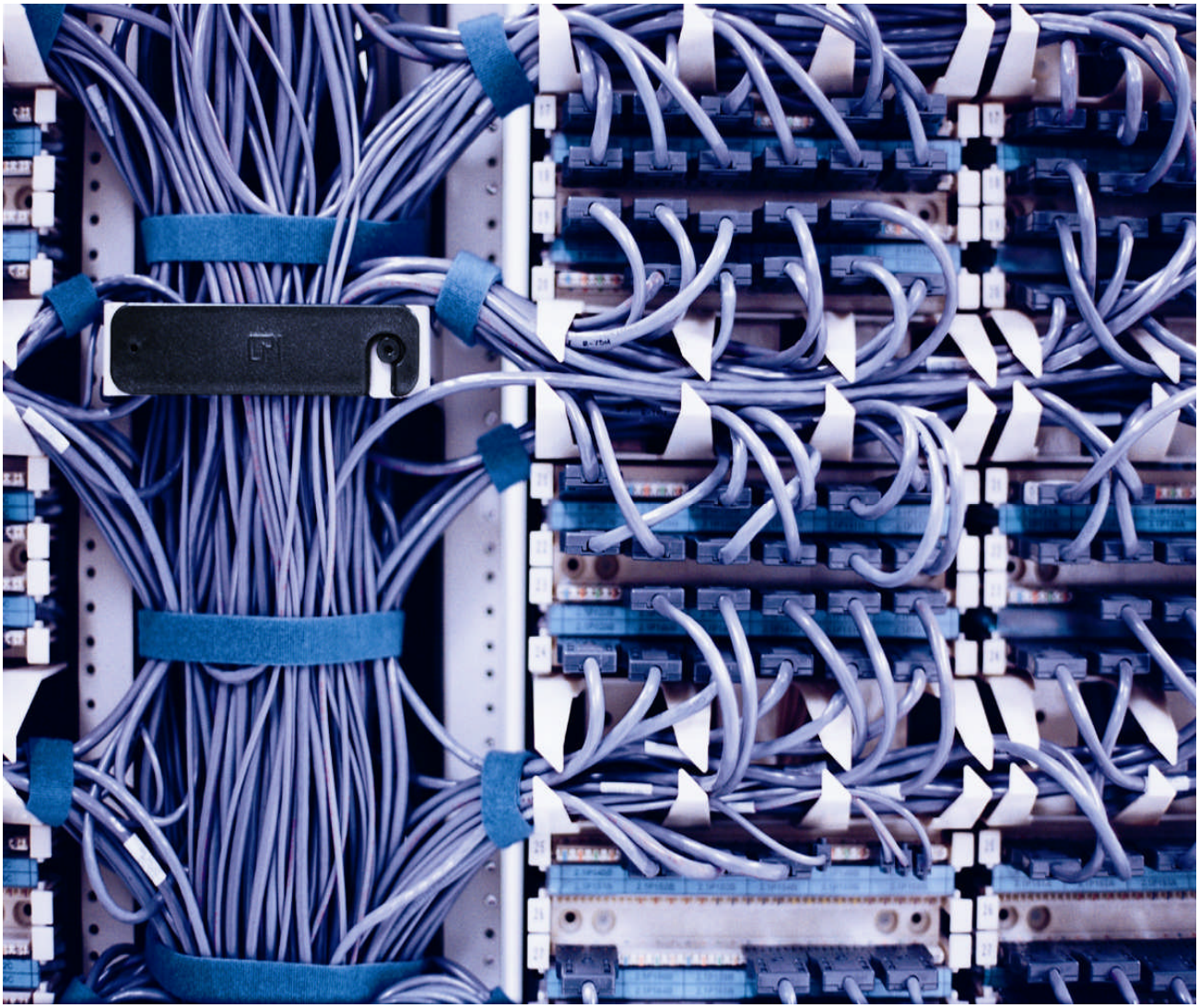
HPSA - VPN SVP 5.1 SP1

Administrator's Guide



Reference number: p175-pd000208

Edition: March 2011

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company

United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

©Copyright 2001-2011 Hewlett-Packard Development Company, L.P., all rights reserved.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Trademark Notices

Linux is a U.S. registered trademark of Linus Torvalds

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

MS-DOS® is a U.S. registered trademark of Microsoft Corporation.

Oracle® and Java™ are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of the Open Group.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Printed in the DK

Contents

1 Introduction
1-1 In This Guide 5
1-2 Audience 5
1-3 Software Versions 5
1-4 Manual Organization 5
1-5 Install Location Descriptors 6
1-6 References 7

2 Introduction to HP Service Activator VPN Solution Pack
2-1 What is the VPN_SVP? 8
2-2 Content of VPN_SVP 8
2-3 Services of VPN_SVP 10
2-4 Activation Process of VPN_SVP 13
2-4-1 CRM Portal 13
2-4-2 HPSA Portal 13

3 Main GUIs of VPN_SVP
3-1 CRM Portal GUI 15
3-2 HPSA Portal GUI 16

4 Service Order Interface
4-1 Service Request Messages 20
4-2 Service Response Messages 21

5 Configuration of Network and Network Elements
5-1 Provider network pre-configuration 25
5-2 Configuration of adminVPN 28
5-3 Managed L3 Site CE Activation 29
5-4 NE Password Encryption 30
5-5 SSH as NE Management Protocol 31

6 Configuration of Inventory
6-1 Initial Configuration of ‘Parameters’ View 32
6-1-1 SP Parameters 33
6-1-2 LSP Parameters 36
6-1-3 VPLS Parameters 39
6-1-4 VPWS Parameters 39
6-1-5 Layer 3 Parameters 39
6-1-6 Service mappings 41
6-1-7 Action templates 41
6-1-8 Upload Templates 42
6-1-9 Backup Parameters 42
6-2 Initial Configuration of ‘Equipment’ View 43
6-3 Network Upload 48

7 Configuration of QoS
7-1 Overview 50
7-2 EXP Mappings 50
7-3 Traffic Classification 51
7-4 QoS Profiles 53
7-5 Template Hooks 54
7-6 Multi-AS backbone QoS 54
7-7 LSP Configuration 55

8 Configuration of Roles
8-1 Roles in HPSA 59
8-1-1 Roles and Inventory GUI 63

8-1-2 Roles and Workflows 64
8-2 Roles in CRM 65

9 Backup Tool

10 Integration with NNMi

10-1 NNMi Integration Configuration 68
10-1-1 HPSA mwfm.xml NNMRequestModule configuration 68
10-1-2 HPSA CRModel→Parameters NNMi configuration 69
10-1-3 SSH installation and configuration 69
10-1-4 NNMi Liaison plugin configuration 70
10-1-5 VPN_SVP CrossLaunch configuration 72
10-1-6 VPN_SVP→Parameters NNMi Queue configuration 72
10-2 Dataload 73
10-2-1 HPSA CRModel configuration of OSVersions, Element Types, Region and Locations 74
10-2-2 HPSA mwfm.xml NNMiDataloadModule configuration 76
10-2-3 Scope configuration 76
10-2-4 Enrichment configuration 77

11 Integration with NA

11-1 NA Integration Configuration 80
11-1-1 MWFM 80
11-1-2 CR Model Inventory Parameters 81
11-1-3 NA Queue 81
11-2 Service Configuration Integrity 82
11-2-1 NA Parent Group Name: 83
11-2-2 Pattern reading from Properties file 83

1 Introduction

1-1 In This Guide

This document is the Administrator's Guide to HP Service Activator (HPSA) based VPN Solution Pack. The VPN solution suite manages MPLS based VPN services, from order entry to activation in the network.

The objective of this guide is to offer assistance to the administrators that must configure and maintains the HP Service Activator VPN Solution Pack (VPN_SVP) for network service provisioning work.

The guide contains detailed information about:

- The components and structure of the HPSA VPN_SVP
- The initial steps of network equipment configuration assumed completed before VPN service activations may take place
- The initial configuration of the VPN_SVP itself before VPN service activations may take place
- The initial configuration of the VPN_SVP for the integration with HP Network Node Manager (NNMi) and HP Network Automation (NA)
- This guide does not contain a full user's or operator's manual

1-2 Audience

The audience for this guide is:

- Systems Administrator or the installer of the VPN_SVP
- Systems Integrator, using it as a resource for building a new solution or extending the existing solution.

The reader must understand the architecture, tools, and service delivery processes described in *HP Service Activator– Overview* and in *HP Service Activator - User* and the reader must in general be familiar with the HP Service Activator version 5.1.

In addition, the reader has a combination of some or all of the following:

- Has a basic knowledge of Network configuration tasks
- Has a basic knowledge of MPLS based VPN configurations and setup
- Has a detailed knowledge of the provider network topology

1-3 Software Versions

The software versions referred to in this document are:

- HP ServiceActivator version 5.1
- HP Service Activator Common Resource Model Solution CRModel V1-1-2
- HP ServiceActivator version 5.1 Hotfix V51-1A-4 (See [*REL*] for detailed software requirements)
- VPN 5.1 Service Pack 1 (V51-1A) (referred to as VPN_SVP).

1-4 Manual Organization

This guide contains the following chapters:

Chapter 2 Introduction to HP Service Activator VPN Solution Pack describes the structure of the VPN_SVP solution, and its features.

Chapter 3 Main GUIs of VPN_SVP describes the main operator interfaces of the CRM Portal and the HPSA server.

Chapter 4 Service Order Interface contains a description of the north-bound service request interface of the VPN_SVP solution used by the CRM Portal.

Chapter 5 Configuration of Network provides detailed description on the expected level of pre-configuration of the provider network.

Chapter 6 Configuration of Inventory provides detailed instructions on how to configure the VPN_SVP to make it ready for use.

Chapter 7 Configuration of QoS explains some details around the QoS features and the configuration process required to setup these before provisioning

Chapter 8 Configuration of Roles contains a description of the default association of operator Roles with Regions and the effect on different views and operations.

Chapter 9 Backup Tool contains an overview of the transfer protocol related configuration of the Backup Tool.

Chapter 10 Configuration of NNMi liaison provides detailed instruction on how to configure VPN_SVP for the integration with HP NNMi.

Chapter 11 Configuration of NA liaison provides detailed instruction on how to configure VPN_SVP for the integration with HP NA.

1-5 Install Location Descriptors

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

Table 1-1 Install Location Descriptors

Descriptor	What the Descriptor Represents
$ACTIVATOR_ETC	The install location of specific Service Activator files. The UNIX location is `/etc/opt/OV/ServiceActivator` The Windows location is `<install drive>:\HP\OpenView\ServiceActivator\etc`

$JBOSS_DEPLOY	The install location of the Service Activator J2EE components.
	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

1-6 References

List of References

Reference	Document Title	FileName
USR	HPSA - VPN SVP 5.1 SP1 User's Guide	UsersGuide.pdf+
SDG	HPSA - VPN SVP 5.1 Service Discovery Guide	SDGuide.pdf+
REL	HPSA – VPN SVP 5.1 Release Notes	ReleaseNotes.pdf+
INTRO	HP Service Activator User's and Administrator's Guide. Edition V51-1A-3	HPSA-User.pdf**
HPSA_INSTALL	HP Service Activator Installation Guide. Edition V51-1A	InstallationGuide.pdf**
PLUGIN	HP Service Activator Developing Plug-Ins and Compound Tasks. Edition V51-1A	Plug-ins.pdf**
NA_USR	HP Network Automation User's Guide	User_guide.pdf*
INTEGRATE	HP Service Activator System Integrator's Overview. Edition V51-1A-3	Overview.pdf**

NOTE1: * Documents available in the HP Network Automation docs folder.

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

NOTE3: + Documents available in the HPSA VPNSVP solution docs folder.

2 Introduction to HP Service Activator 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
- Include 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.

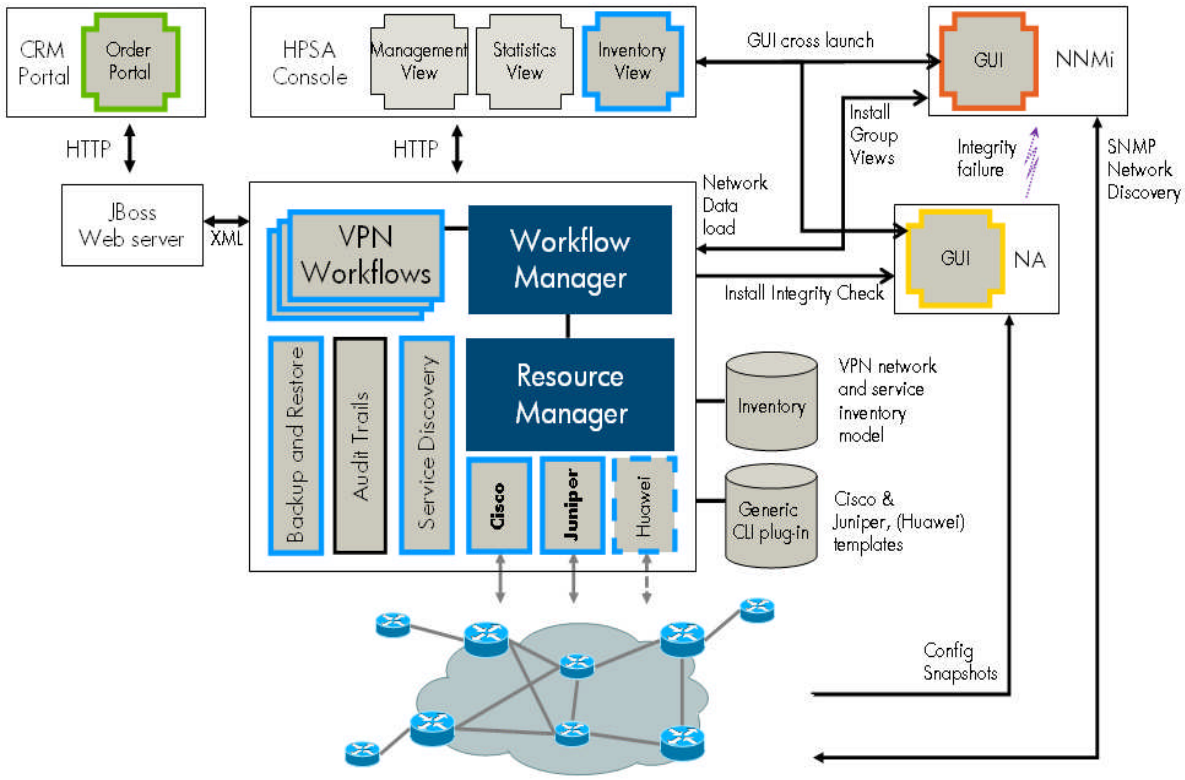
2-2 Content of VPN_SVP

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

- A simple CRM Portal GUI, which provides an easy-to-use interface for Customer Order related personnel to manage the services ordered by the Customer to be provisioned or activated in the Provider's network. List customer displays a summary of the states of various services requested by the various customers.
- An Inventory repository which keeps 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 can not 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.
- An example SOAP client that allows remote operators to interact with the CE provisioning process (i.e. to confirm the completion of the CE installation and pre-configuration).
- 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 component



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.
- Creation and deletion of 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 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
- 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 (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 (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 P2P 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.
- Service Integrated LSP feature. This enables enhanced treatment of MPLS cross-core data according to the customer/ingress data classification. This strategic Traffic Engineering component builds a full mesh of LSPs between the PE routers hosting VPN sites. The LSPs are created, modified and/or deleted according the requirement and topology of the site services. This is currently only supported on Juniper PE devices.
- 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 to fail the service request.
    - Temporary connectivity failures to the provider's network infra-structure (e.g. 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.
- Service Discovery from network element configurations. Analyzes the configuration files of the NEs and discovers the configured L3 services (Cisco or Juniper devices). 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 the 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	÷	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.

2-4-1 CRM Portal

It is assumed that the operators of CRM portal may be different personnel 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, entering service specific parameters based on the customer's requirements, submitting the completed service orders for activation by Service Activator.

The services 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.

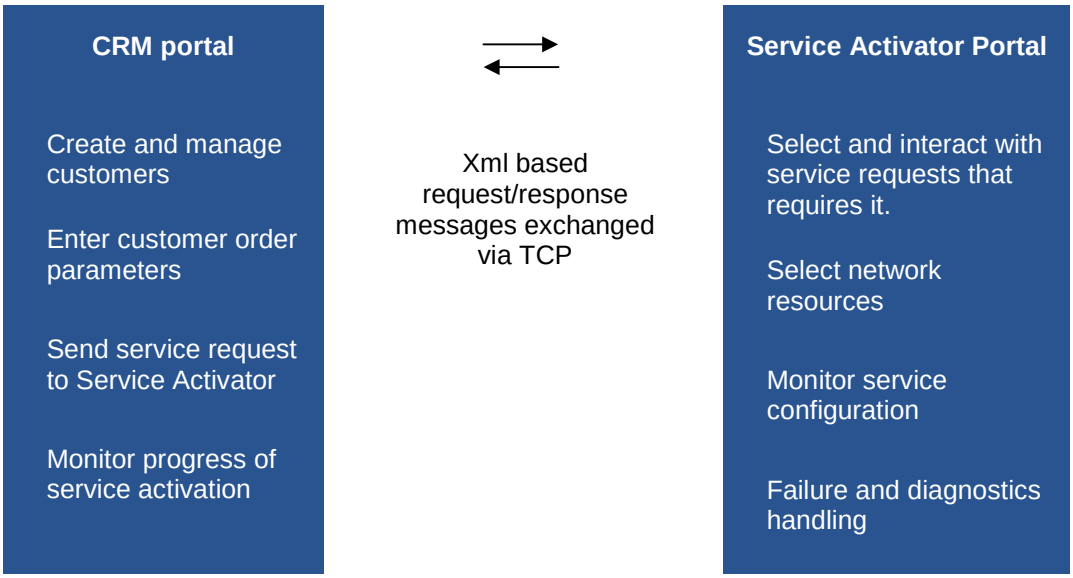
The initial creation of a site service requires the network operator to select the attachment point of the service, i.e. the router/switch and interface that the customer's site gets connected to. This is requested via an interaction form that automatically pops-up when required.

But often a received service request will not required 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 be reported back to the CRM Portal 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 and if the caused may be identified and even repaired, the request my be re-submitted from HPSA Portal. Otherwise, the request may be failed and the responsibility of the process returns to the CRM Portal.

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



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

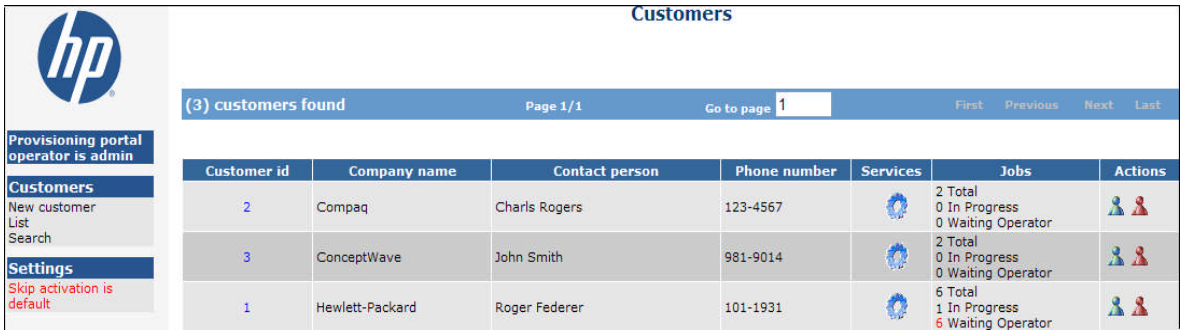
3 Main GUIs of VPN_SVP

3-1 CRM Portal GUI

The simple CRM Portal GUI for Customer Order provides an easy-to-use interface to request the services ordered by the Customer to be provisioned or activated in the Provider's network. This component is optional and could be substituted by an existing Provider CRM system.

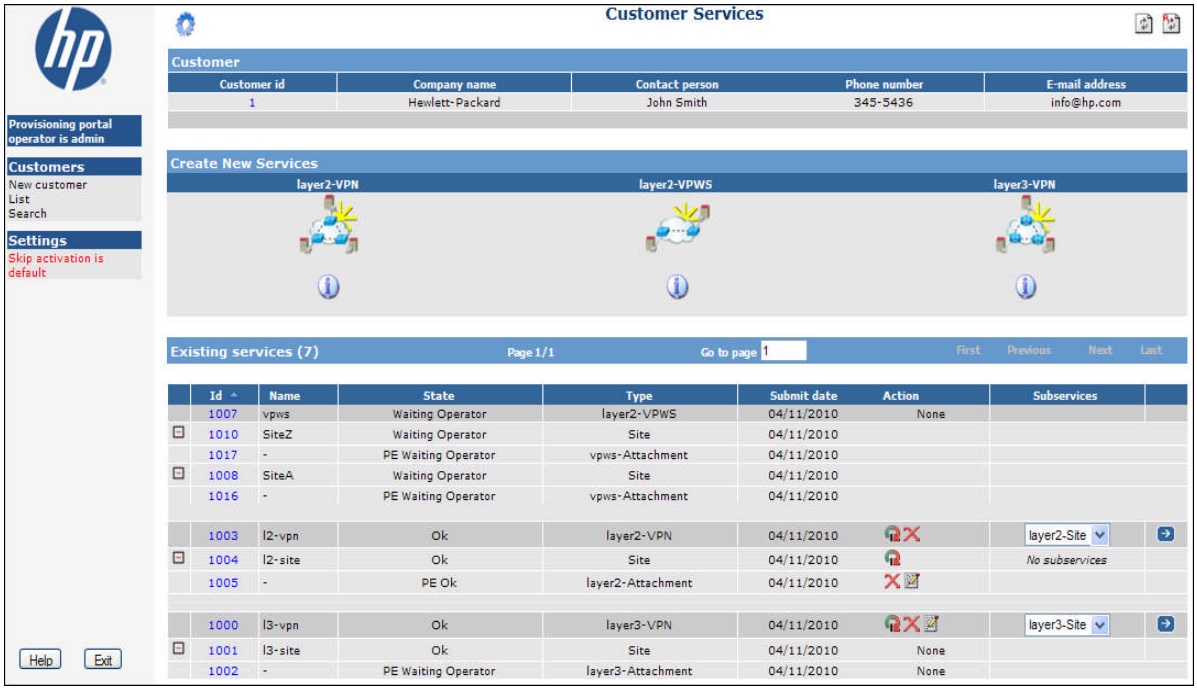
In the main CRM Portal GUI, list of existing customers can be viewed, as shown in **Figure 3-1**. The 'Jobs' column gives a summary of the states of various service requests requested by the customer, represented by 'Company Name'.

Figure 3-1 CRM List Customers



Detailed list of various services and their state, for a specific customer can be viewed by clicking on the 'Services' icon. See **Figure 3-2**.

Figure 3-2 The CRM Portal GUI. VPNs and some associated Sites are being or have been created.



The authentication mechanism is very primitive out-of-the-box. There is basically no check on the password supplied, only that some string is entered. To enhance the authentication mechanism, some more advanced authentication module must be implemented and the CRM portal must be re-generated using the required mechanism.

The CRM Portal is role based and provides three roles of interactions.

- A user with Operator role may perform the following tasks:
  - Creation/deletion of a customer
  - Creation/deletion of customer's L3 VPN, L2 VPLS and L2 VPWS services, addition/removal of VPN/VPLS/VPWS Sites and modification of specific VPN and Site parameters
  - Timed creation and deletion of VPN Site and VPWS services, timed VPN Site modification
  - Browsing of services' information
  - Re-issuing of failed requests.
- A user with role Admin can perform the above tasks plus enable 'skip activation' mode which may be used for debug and repair.

NOTE: Unless you are absolutely sure about what you are doing, don't manipulate 'skip activation' mode on a production system!

- All other users will be assigned the role Guest and may only view the above information

NOTE: See more about configuration of CRM portal roles in section 8-2 below.

.

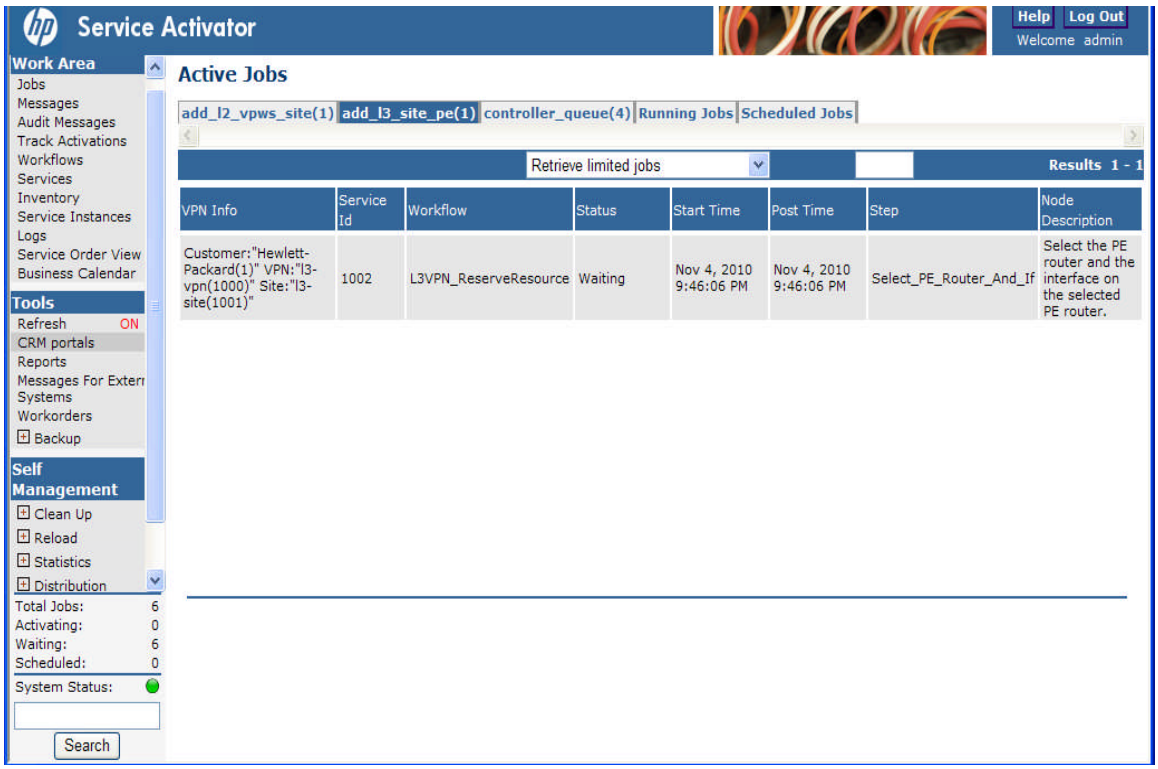
The CRM system is responsible for allocation of unique service ids and for requesting the activation of services by sending xml based service requests to the HPSA server. These requests must adhere to the message dtd defined by the VPN_SVP (see section 4-1).

3-2 HPSA Portal GUI

The HPSA Portal consists of the standard HPSA GUI and VPN_SVP specific extensions. The HPSA Portal is the main GUI of the network operators.

The Jobs view of the standard HPSA GUI represents one of the two main views used by the network operator, see **Figure 3-3**.

Figure 3-3 Portal Jobs View. A job is currently awaiting network operator interaction.



The service requests received from the CRM Portal may be of two types with respect to network operator interactions, Flow-through or Interactive:

- Flow-through

  Several types of requests do not need any further information to be provided by the network operator to complete. These jobs will only shortly be visible in the Jobs list and not allow any interaction. These include:

  - Creation/Deletion of VPNs
  - Creation/Deletion of VPN Sites.
  - Modifications of existing services attachments
  - Enabling/disabling of services
  - Removal of existing services

- Interactive

  Not all information may be determined automatically by the VPN_SVP and some requests may therefore require the network operator to supply the additional information. These include:

  - Addition of new Site services.

    The network Operator has to select which PE router and interface the service should be attached to among the possible resources, and possibly the encapsulation type and related parameters of the selected interface and attachment type.

  - Setup CE

    When provisioning a managed CE, the initial configuration of the CE to obtain connectivity to the Provider network has to be specified.

  - Confirmation of the continuation of the activation process

    Some activation types require the explicit confirmation of the network operator to continue. These include:

    – Confirmation that L3 Managed CE router that is specified as present, actually is in place and ready for activation

    – Confirmation of continuing with the de-activation of a scheduled modify rate-limit request.

The responsibility of the network operator is to assign network resources such as edge devices, and interfaces for the services and to specify their encapsulation and related connectivity properties. Therefore, a network operator is required to have a detailed knowledge of the provider network and its resources.

The Jobs view allow for the interactions with the pending jobs, so the network operator may select edge devices and interfaces for the attachment of services.

Additional HPSA left-pane GUI components are augmented by the VPN_SVP. These GUIs are used for:

- Instantiation of the CRM Portal
- Report generation
- Display of messages queued for distribution to external system
- Display of manual work-orders used for the pre-configuration of CE routers
- Management of router configuration Back and Restore

The standard HPSA GUIs are used for display and searches of audit trails, display of messages, logs, etc., and are available from the HPSA Main view.

The Inventory viewer of the HPSA is the other main GUI used by the network operator. It provides two main types of views, class views and the instance views. The views available are made specifically for a solution. The class views are mainly used to specify advanced searches in the inventory database and will not be described further in this guide.

In the following the instance views available in the inventory GUI of the VPN_SVP (SAVPN) solution are described. These instance views provides an easy interface for the network operator to inspect services and their associated properties and allocated resources.

The views have been divided into 3 main views (or presentation trees) (see **Figure 3-4** below):

- SAVPN/Services

  Displays the Customers and their associated services such as VPNs and their Sites, and the resources associated the services. As this view represents the activated services, only limited modification capabilities of these entries are allowed.

- SAVPN/Equipment

  This view contains the network resources such as PEs and CEs and their Interfaces, divided into Regions, AS and Networks. This view allows extensive addition and modification of network resources and provides upload capabilities to automatically populate the Inventory with the interfaces of e.g. a newly added NE.

NOTE: If NNMi liaison is configured and enabled, the dataload functionality automatically populates the network resources into the VPN_SVP SAVPN/Equipment inventory. See section 1-1 for more details.

- SAVPN/Parameters

  This view contains the configured parameters and resources, such as Regions, IP address pools, QoS profiles, etc. which are necessary for successful provisioning of services. It is via this section that most of the (pre-) configuration of VPN_SVP takes place.

Certain operations related to the equipment resources are done by the network operator interacting directly with the Inventory views:

- Creation of Channelized interfaces

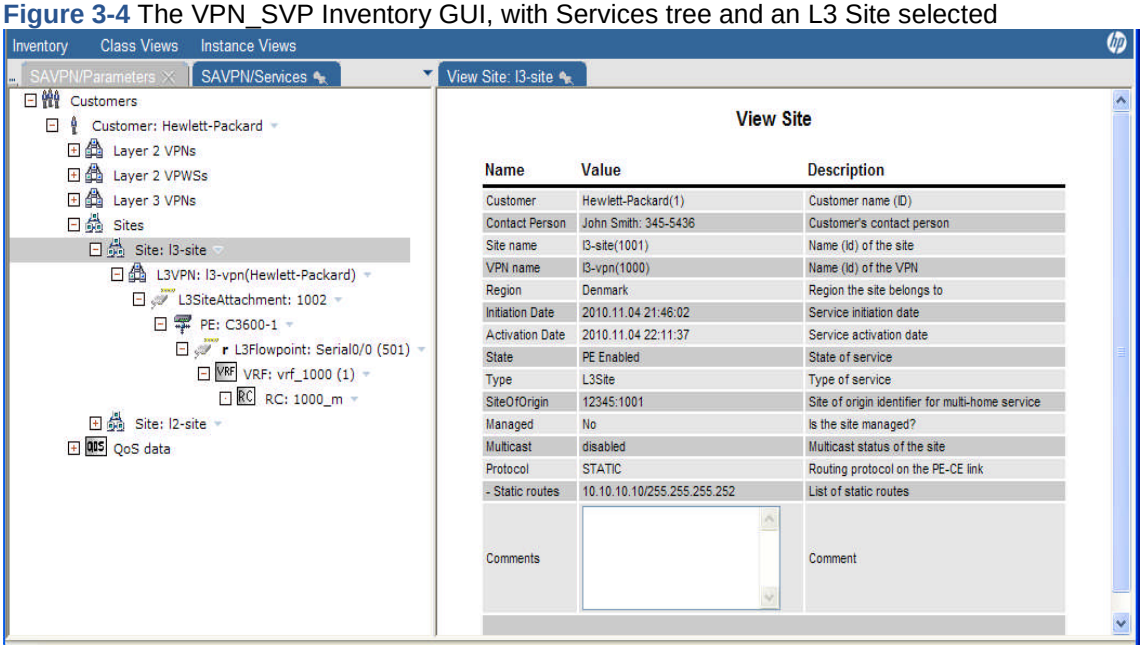
  The network operator has to select the Time Slots and framing parameters when the need to create new interfaces from the available controllers arises

- Creation of Bundled interfaces

  The network operator has to select the individual interfaces to be bundled (aggregated) into a virtual interface.

In addition to the three views described above, a 4th view, SAVPN/ServiceUpload is available. This view is used in connection with the Service Discovery tool as described in [*SDG*].

Figure 3-4 The VPN_SVP Inventory GUI, with Services tree and an L3 Site selected



4 Service Order Interface

This section contains information about the HPSA based north-bound interface used to request service activation from external system (e.g. the CRM Portal) and the response that's optionally communicated back to the requestor.

4-1 Service Request Messages

The service request messages sent from CRM portal to the HPSA server (see **Figure 2-2** above) to request activation, modification or deletion of services are xml based. See **Figure 4-1** below for an example request message.

Figure 4-1 Example service request message as received from CRM portal by HPSA

```
<msg Message_id="18">
  <header>
    <Service_request Skip_activation="default" Service_response="true">
      <Service_id>1007</Service_id>
      <Activation_name>add</Activation_name>
      <Deactivation_name>remove</Deactivation_name>
      <Service_name>L3Site</Service_name>
      <Region>Denmark</Region>
    </Service_request>
  </header>
  <body>
    <VPNSite>
      <Site>
        <VPN_Service_id>1006</VPN_Service_id>
        <Site_name>Sales1</Site_name>
        <Site_address/>
        <Contact_person>John Smith: 328-4650</Contact_person>
        <Comment/>
        <Managed_CE_router>false</Managed_CE_router>
      </Site>
    </VPNSite>
  </body>
</msg>
```

The service request messages are received by the HPSA server and passed to the Controller workflow for validation. The configuration of the listener module and association of the controller workflow is made using HPSA standard procedures.

The Controller workflow uses the <header> information to identify the service specific workflow which should handle the received request.

The header contains the <Service_request> element which again contains the <Activation_name> and <Service_name> elements. In the inventory GUI → Parameters view, the table 'Service mappings' defines the Workflows that is to be instantiated based on these two header fields.

The identified workflow is initiated as a child workflow and the request message passed along. The service specific child workflow will primarily use the parameters included in the <body> part of the request message to control the activation process.

If some customer specific changes are required to the request messages, e.g. addition of some extra parameters, the message.dtd file (*$ACTIVATOR_ETC*`/config/message.dtd`) must be updated accordingly (and also the workflows which would need this extra information). **Figure 4-2** below illustrates the top level structure of the message.dtd of request messages.

Figure 4-2 Top level elements of message.dtd

```
<!--
  A request message consists of a header and a body.
  The header contains the elements necessary to identify the workflow which implements
  the requested service.
  The body consists of the service specific parameters necessary to activate the service.
  An optional Service_schedule element is also part of the request header.

  - Message_id: Unique identifier of the request message  that must be included in the
    optional response. May be useful for the requestor (sender) to identify responses of
    multiple outstanding requests.
-->
<!ELEMENT msg (header, body)>
<!ATTLIST msg
  Message_id CDATA #REQUIRED
>
<!ELEMENT header (Service_request, Service_schedule?)>
<!--
  A service request consists of a target (Service_name) and an operation (Activation_name).

  - Service_name: L3VPN | L3Site | L2VPN | L2Site | L2VPWS
  - Activation_name:
    create | delete | modify | add | remove | join | leave| disable
  - modify: Represents the following specific modification types:
    L3VPN:  modify_VPNTopology, modify_Multicast
    L3Site: modify_Rate_limit, modify_QoS, modify_StaticRoutes,
      modify_ConnectivityType, modify_Multicast
    L2Site: modify_Rate_limit, modify_QoS
    L2VPWS: modify_Rate_limit

  - Service_id: The service is uniquely identified by the requesting system using the
    Service_id, must to be an integer.
  - Deactivation_name:  Used for scheduled services. May be: delete | remove
  - Region: This element specifies a region (an operator area of responsibility) and is
    used to associate a role for the service request. Only used for site services.
  - Service_response: This element indicates whether the requestor wants specific responses
    or not (silent) to the request.
  - Skip_activation: This element is used in e.g. test environments where the actual equipment
    may not be presents and hence, the activation on the equipment is to be skipped but
    everything else execute normally.
-->
<!ELEMENT Service_request (Service_id, Activation_name, Deactivation_name?, Service_name, Region?)>
<!ATTLIST Service_request
  Service_response (true | false) #REQUIRED
  Skip_activation (true | false | default) #REQUIRED
>
<!--
  The Service_schedule allows timed services. Two timed service types are currently supported:
  Scheduled and Recurrent. Scheduled supports a StartTime and an optional EndTime. Recurrent
  support a StartTime, EndTime (i.e. basically a duration) and a Recurrency interval.
  Not all services are currently supported as timed service:
  Scheduled:
    L3Site: add-L3Site, modify_Rate_limit
    L2Site: add-L2Site, modify_Rate_limit
    L2VPWS: create-L2VPWS, modify_Rate_limit
  Recurrent:
    L3Site: modify_Rate_limit
    L2Site: modify_Rate_limit
    L2VPWS: modify_Rate_limit

  - StartTime: The time when the requested services is to be activated
  - EndTime: The (optional) time when the service is de-activated
  - Recurrency: Daily | Weekly | Monthly. Only modify_Rate_limit is currently supported as recurrent.
-->
<!ELEMENT Service_schedule ((StartTime, EndTime, Recurrency) | (StartTime, EndTime?))>
<!-- Header tags -->
<!ELEMENT Service_id (#PCDATA)>
<!ELEMENT Activation_name (#PCDATA)>
<!ELEMENT Deactivation_name (#PCDATA)>
<!ELEMENT Service_name (#PCDATA)>
<!ELEMENT Region (#PCDATA)>
<!ELEMENT StartTime (#PCDATA)>
<!ELEMENT EndTime (#PCDATA)>
<!ELEMENT Recurrency EMPTY>
```

4-2 Service Response Messages

It may be noted, that a Service_response attribute is available. This may be used to enable (true) or disable (false) the generation of response messages from HPSA server to be send back to the CRM system. If the CRM portal supplied with the VPN_SVP is used, this attribute should always be ‘true’. If an existing CRM system is used, it is strongly recommended to always request responses to allow the CRM system and the HPSA server to stay synchronized with respect to the state of the requested services.

The structure of the Response messages are defined by the xsl template illustrated in **Figure 4-3** below and may be found in *$SOLUTION/*`etc/template_files/Common/Crm_status.xsl`.

Figure 4-3 The generic structure of response messages send to the CRM Portal.

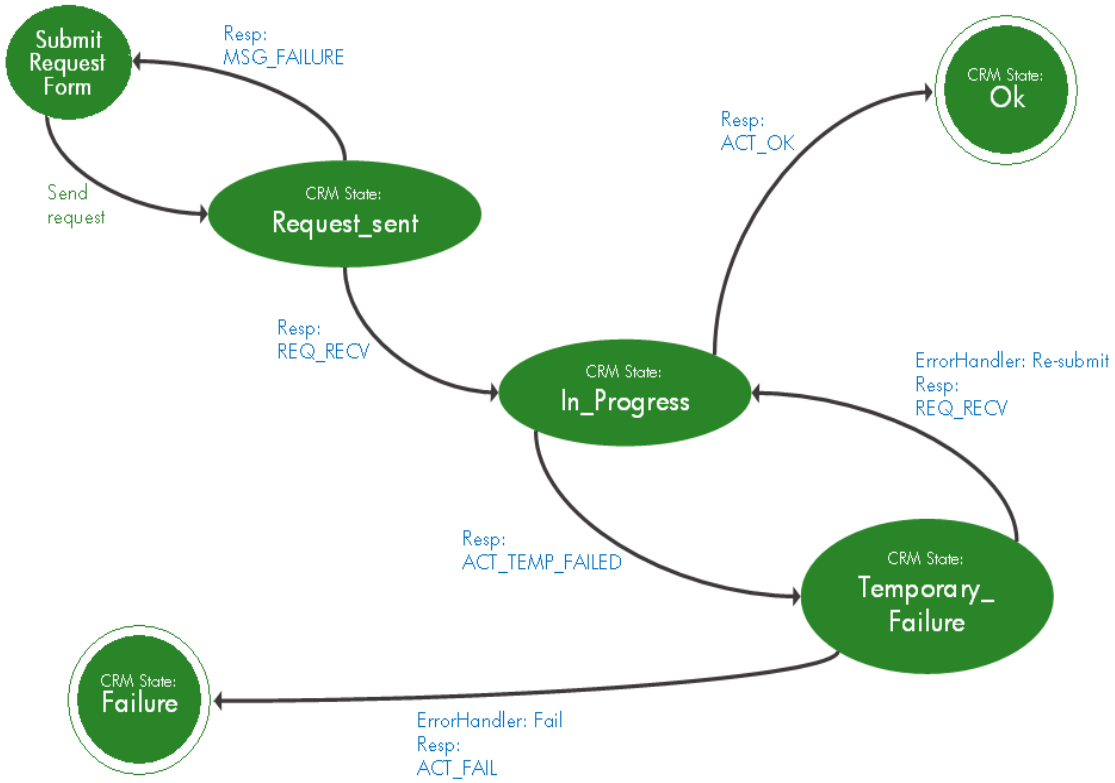
```
<xsl:param name="message_id" />
<xsl:param name="SERVICE_ID" />
<xsl:param name="crm_response" />
<xsl:param name="crm_response_data" />

<xsl:template match="/">

<Resp_mesg>
   <Message_id>
      <xsl:value-of select="$message_id" />
   </Message_id>
   <Service_id>
      <xsl:value-of select="$SERVICE_ID" />
   </Service_id>
   <Response>
      <Resp_status>
         <xsl:value-of select="$crm_response" />
      </Resp_status>
      <Resp_data>
         <xsl:value-of select="$crm_response_data" />
      </Resp_data>
   </Response>
</Resp_mesg>
</xsl:template>
</xsl:stylesheet>
```

The four parameters are substituted at run-time with their actual values when the xml message is created by the SendCrmSyncHandler in the Controller work-flow.

The <Resp_status> element may take the following values:

- **MSG_FAILURE**
- **WF_FAILURE**
- **REQ_RECV**
- **ACT_OK**
- **ACT_SCHED**
- **END_SCHED**
- **CONFIRM**
- **ACT_TEMP_FAILED**
- **ACT_PARTIAL**
- **ACT_FAILED**
- **DONE**
- **ACT_DONEWAIT**
- **ACT_WAITOPER**
- **VALID_FAILURE**

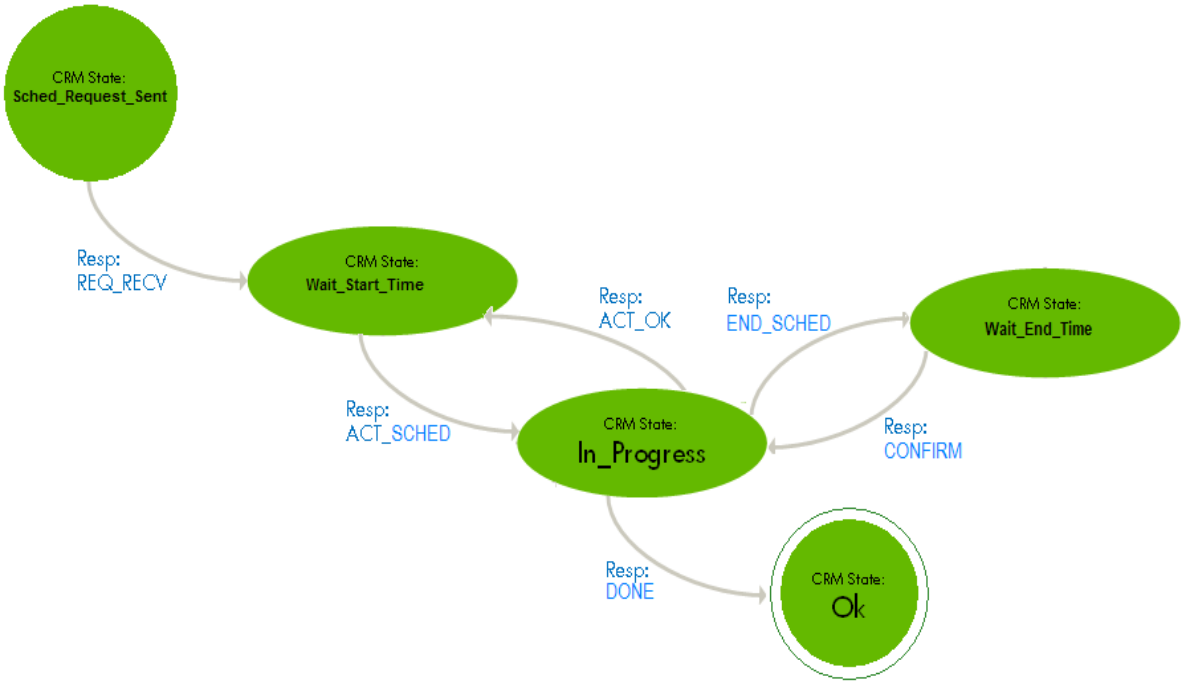
Figure 4-4 An example of the normal sequences of states in the CRM portal as driven by some of the response messages/events sent from HPSA.



These values represent different states and completion codes of the activation process and drive a state-event machine in the CRM Portal. **Figure 4-4** illustrates a general example of the normal state transitions observed during a normal activation process.

Scheduled and timed services are also supported and the state-event automata for these cases are a little more involved. Below **Figure 4-5** illustrates a set of normal transitions for a scheduled service operation.

Figure 4-5 Typical state-event transitions for a scheduled activation process



The number of state-event transitions specified in the database of the CRM portal (table CRM_STATEMAPPING) contains quite a large number of entries. These are mainly duplicates of the above illustrated basic transition types but replicated one time for each of a number of different initial states, some of which are:

- **Request_Sent**
- **PE_Request_Sent**
- **CE_Request_Sent**
- **CE_Failure**
- **Proceed_CE_Request_Sent**
- **Proceed_CE_In_Progress**
- **Proceed_CE_Failure**
- **Proceed_PE_and_CE_In_Progress**
- **Proceed_PE_and_CE_Request_Sent**
- **Proceed_PE_and_CE_Temporary_Failure**
- **Periodic_Modify_Wait_Start**
- **Periodic_Modify_PE_Request_Sent**
- **Delete_Requested**
- **Modify_Request_Sent**
- **Modify_PE_Request_Sent**
- **Undo_Modify_PE_Sent**
- **Undo_Modify_Sent**
- **Disable_Request_Sent**
- **Disable_PE_Request_Sent**
- **Enable_Request_Sent**
- **Enable_PE_Request_Sent**
- **Sched_Request_Sent**
- **Sched_PE_Request_Sent**
- **Sched_CE_Request_Sent**
- **Sched_Modify_Request_Sent**
- **Periodic_Modify_Request_Sent**
- **Periodic_Modify_PE_Request_Sent**
- **Partial**
- **Ok_Wait_Mod_End_Time**
- **Ok_Wait_End_Time**
- **Waiting_Operator**
- **Wait_Start_Time**
- **Temporary_Failure**

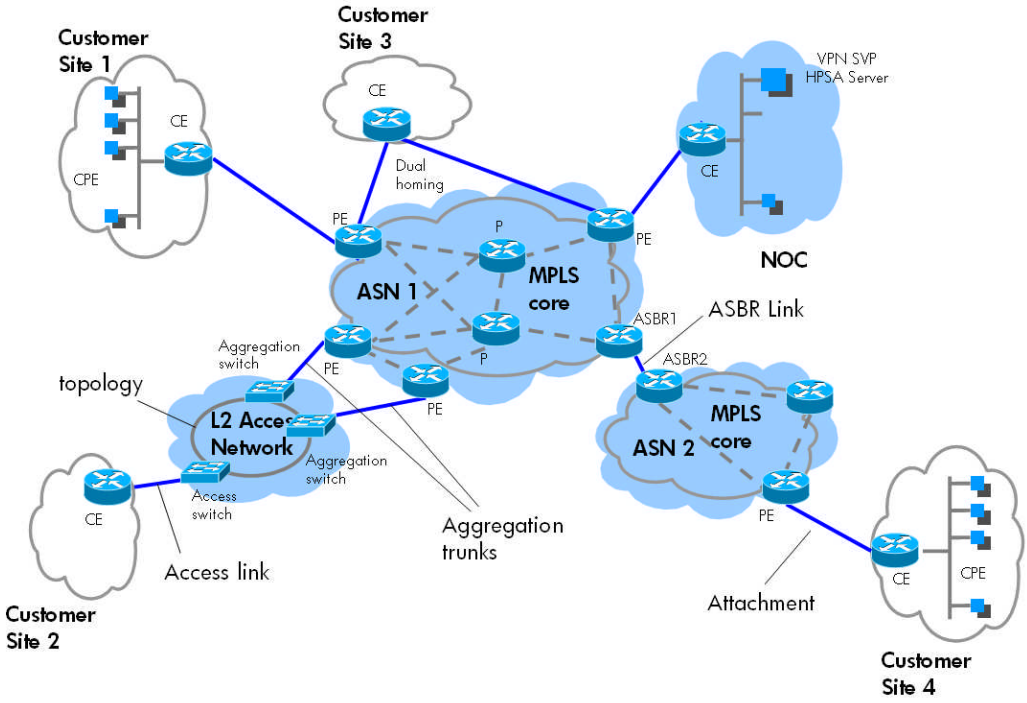
5 Configuration of Network and Network Elements

This chapter explains the assumptions made concerning the configuration of the provider network and its network elements.

5-1 Provider network pre-configuration

Figure 5-1 below illustrates the general network topology and the type of network elements relevant for the activation of MPLS based VPN services in a provider network using VPN_SVP.

Figure 5-1 Generic Service Provider Network Architecture



The Provider Edge (PE) routers are facing the Customer Edge (CE) routers. The attachment (access flows) between the CE and the PE router is associating a Customer Site with a VPN service. The type of attachments may be direct or via an L2 switched access network. The termination points (flow points) are the PE interface(s) and the CE interface.

L3 VPN services are supported across a provider Multi-AS backbone core network, 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** 5-1 above 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. This is currently done in accordance with model a) in RFC 4364 which is the simplest and security wise the preferable model.

The NOC represents the network operations center (or management network) of the Provider and is typically connected to the core network similar to a Customer Site. The HPSA server running VPN_SVP is located in the NOC.

The operation of VPN_SVP is related to the configuration of the site attachments, its parameters (IP addresses, encapsulation, VLAN IDs, routing protocols, CoS, QoS, trunks ports, allowed VLans in access network, etc.), the PE and optionally the CE interfaces.

For L3 services also the Virtual Routing and Forwarding (VRF) instances on the PE router that defines the L3 VPN membership/connectivity of the site attachment and for L2 VPLS services the Virtual Forwarding Instance (VFI) is configured. Additionally, the peering of sites across the MPLS core must be configured for P2P L2 services (VPWS).

The MPLS core network is not configured by the VPN_SVP. The MPLS core network consists of the core facing interfaces of the PE router as well as all the Provider (P) core routers and their interconnections.

NOTE: The ASBR links are also configured by the VPN_SVP but only for L3 services.

The following steps represent the assumed pre-configuration of the provider network and MPLS core:

- P routers are setup and inter-connected in the core network and has been made operational
- PEs are setup including their management IP addresses and login authorization and interconnected with the P routers (and possibly other PE routers) via core facing interfaces.
- The core Autonomous System Numbers (ASNs) has been configured and the Border gateway Protocol (BGP) has been setup with peering and possibly Route Reflectors
- The ASBR links are connected as required between the ASBRs in a Multi-AS backbone environment.
- The necessary MPLS configuration of the P and PE routers have been completed, including the QoS related configuration which is related to MPLS EXP classification and policing
- The access networks, consisting of access switches, topologies (e.g. rings), aggregation switches and trunks are configured and connected as required. Currently no Spanning Tree configurations are made by VPN_SVP.
- Telnet (or SSH) connectivity from VPN_SVP server and to the PE routers in the Provider network must be configured and assured.
- Telnet (or SSH) connectivity from VPN_SVP server and to the NE/switches in the access networks must be configured and assured. Normally some predefined management VLans are assigned to this usage.
- Connectivity from NEs and to the VPN_SVP server must be configured and assured for the support of configuration backup. This depends on the backup transfer protocol selected and installed by the provider.
- To support L3 Managed CEs, an adminVPN (or grey VPN) must be manually configured on the PE router connecting the NOC (see section 5-2 below for more information). The corresponding configuration in the Inventory-Parameters→ISP object must be done to assure that the correct RC automatically gets included in the VPN sites attachment configuration (see section 6-1 below for more information)

Basically, all Access switches, PEs and P routers are assumed interconnected and fully operational and the core setup completed. The VPN_SVP supports network equipment in state Planned, but before VPN configuration is permitted, the NE must be fully operational (Ready).

The VPN_SVP Inventory Equipment part must be initialized and configured correspondingly so it reflects the provider network structure correctly, as describe in section 1-1

The described setup of the provider network may represent a considerable effort but is in nature a once-only configuration which then stays relatively unchanged over time with the more occasional addition/modification of NEs. Therefore this type of configuration is not the target for VPN_SVP automation, which focuses on the more repetitive tasks in the VPN activation process.

The initialization of interfaces in each NE is a relatively big task as potentially thousands of interfaces may exists on e.g. a PE router. This task is accomplished by using the VPN_SVP interface upload facility, which automatically extracts that information from the devices and then populates the Inventory correspondingly.

The VPN_SVP focus areas are:

- L3 VPN Services
  - Configuration of the PE interface(s) facing towards the Customer Site's CE routers, optionally the access port and trunks of an access network, including IP addresses, routing protocols and QoS and VPN membership/connectivity, including adminVPN Spoke RC in case of Managed CEs
  - On Managed CEs, the configuration of the CE interface facing towards the Provider's PE router, including IP address, routing protocol, optionally QoS and the CE management address (loopback address)
  - Configuration of the ASBR links interconnecting a Multi-AS backbone environment.
  - Configuration of LSPs according to the service request.
- L2 VPN (VPLS) Services
  - Configuration of the PE interface facing towards the Customer Site, optionally the access port and trunks of an access network, including customer VLAN ID and QoS.
  - Configuration of the full-mesh PE-PE peering across the MPLS core of all sites in a L2 VPN without BGP auto discovery.
  - Configuration of LSPs according to the service request.
- L2 VPWS (point-to-point) Services
  - Configuration of the PE interface facing towards the Customer Site. In case of an Ethernet attachment circuit, optionally configuration of a customer VLAN ID. In case or frame relay, configuration of a customer DLCI. And configuration of a single CoS and its rate limit.
  - Configuration of the PE-PE peering across the MPLS core of the two sites attachment endpoints in a L2 VPWS
  - Configuration of LSPs according to the service request.

5-2 Configuration of adminVPN

If the configuration of adminVPN is not already done in the provider network, an example is included here to illustrate what must be done. The example assumes that the PE connecting the NOC is a Cisco router.

The adminVPN is a Hub&Spoke topology VPN and the PE interface attaching the NOC to the MPLS network must be manually configured including the VRF associated containing the Hub Routing Community (RC). This is a once-only manual task.

The individual customer sites, that are specified as managed (i.e. the CE router is managed by the Provider) must have the corresponding Spoke RC included in their associated VRF. That is automatically done by VPN_SVP when the site service is added.

The number of route prefixes that the Provider wants to import into the adminVPN and make available for the NOC should be limited as much as possible. Importing all the internal route prefixes related to the customer's network infra structure is not desirable - only the prefixes that create connectivity into the CE routers are relevant for creating connectivity from the NOC to the CE. I.e. the prefixes related to the PE-CE link addresses and the CE loopback addresses.

This limitation or filtering of the route prefixes received from a Customer site is implemented as part of adminVPN Spoke configuration that is automatically done by VPN_SVP. This involves the configuration of prefix lists (filters) and route maps that associates the admin Route Targets to only the selected prefixes.

As VPN_SVP manages the address pools related to CE-PE links and CE loopback addresses this necessary information is available at activation time and the configuration necessary for the particular customer site is automatically done by VPN_SVP. **Table 5-1** below displays a generic example on how to configure the VRF associated the NOC attachment, i.e. the Hub site and the corresponding configuration of the VRF associated the customer sites (Spoke part).

The assumptions in **Table 5-1** below are:

- The Provider Autonomous System number is <ASN>
- The NOC attachment interface uses export route target <ASN>:1 and import route target <ASN>:2.
- The PE-CE link addresses are assumed allocated from IP net number <PE.CE.IP.Net> and the CE loopback addresses are assumed allocated from IP net number <CE.Loop.Back.Net>.

Table 5-1 Admin VPN related VRF configuration (in grey) related to a Managed Customer site VRF (in green)

Hub site in an admin VPN. **I.e. the NOC attachment. Must be manually created and associated the interface.**	**Spoke site in an admin VPN.** **I.e. any managed customer site. Done automatically by VPN_SVP**

`vrf adminVRF`
` rd <ASN>:1`
` route-target export <ASN>:1`
` route-target import <ASN>:2`
	`ip prefix-list adminVPN permit <CE.Loop.Back.Net>/16 le 32`
	`ip prefix-list adminVPN permit <PE.CE.IP.Net>/16 le 32`
	
	`route-map adminVPN`
	`  match ip address prefix-list adminVPN`
	`  set extcommunity rt <ASN>:2 additive`
	
	`vfr VPN-GREEN`
	`  rd <ASN>:10010`
	`  route-target import <ASN>:10000`
	`  route-target export <ASN>:10000`
	`  route-target import <ASN>:1`
	`  export map adminVPN`

The actual values of ASN and the Hub export and import RT must be configured in the inventory as described in section 6-1 below before provisioning of managed CE sites. This configuration should not be changed after sites have been provisioned!

As different managed sites may have been allocated PE-CE link addresses from different address pools, the prefix-list can not be a single common definition but depends upon the used pool. Hence, the actual prefix-list names and router-map names configured are appended the name of the used address pool.

5-3 Managed L3 Site CE Activation

The activation of the CE router of a managed L3 site follows in time the activation of the access network/PE interface. This assures that the customer data is confined into the proper L3 VRF which then is in place before the CE is connected.

Generally, when the HPSA platform connects to the CE router to perform activation tasks, the CE router needs to know how to route IP packets back to the HPSA server to assure connectivity. But at the very initial activation, routing protocols, etc. is not yet configured on the CE router. Hence, often an initial default route entry on the CE router pointing to the PE router interface needs to be part of the initial and manual pre-configuration of the CE router.

To circumvent the need of having such a default route configured on the CE router as part of the manual pre-configuration, VPN_SVP supports a two-step CE activation process:

1) VPN_SVP VPN_SVP (HPSA) connects to the PE router where the VRF is already configured on the attachment point (interface) facing the CE router.

2) The connection from PE to the CE is then done within the vrf. E.g. on Cisco this could be:
telnet <if_ipaddr_CE> /vrf <vrf_name>

To the CE router it now appears that the packets are originating from the PE router interface IP address and because this is the other end of one of its directly connected networks and therefore no routing is required, no default route entry is required!

NOTE: Please note, that when the CE connection protocol is selected as SSH, that not all PE device types may support a similar way of connecting to the CE router from the PE router within the VRF as for telnet. In such cases, the CE activation templates may need to be changed, and a default route pointing at the PE interface may have to be added to the initial CE configuration before connections/activations from VPN_SVP (and from the NOC) may be possible via the adminVPN connectivity.

E.g. the activation template Cisco/Cisco-CE-MPLS-Add-VPN.xsl uses the parameter “direct_to_CE” to control the form of connection made to the CE router. If it is ‘false’ the template will use the above described “jump-host” technique making the connection via the PE’s vrf. If it is ‘true’ it will connect directly from VPN_SVP to CE.

This parameter may be overwritten in the specific template files or, its default assignment to false in the L3VPN_AddSiteAttachment_CE.xml workflow may be changed if it is to take effect for all CE types.

This “jump-host” technique allows VPN_SVP to activate the CE router with fewer requirements to the CE router’s initial configuration and actually even the adminVPN configuration described above is not required by VPN_SVP. But please note, that other OSS systems in the NOC may require connectivity to the managed CE routers and as these systems may have no specific knowledge of the PE routers and their configured VRFs, etc., the adminVPN must be setup and used as described above to provide access in general from the NOC to the managed CEs.

5-4 NE Password Encryption

The HPSA frame work supports optional encryption of passwords so in no circumstances, like Inventory GUI, log files, database, etc. does a password appear in clear text. This feature is used to protect the passwords to access the network elements (NE). Only on the actual connection established at activation time when VPN_SVP needs to login to the NE to perform the activation is the password decrypted and send to the NE in the clear. But if you specify the connection protocol as ssh, even this occurrence of the password is protected.

As this feature must be specified at production time, it has been decided to enable password encryption by default in VPN_SVP. This you may e.g. observe in the resource definition files. E.g. in inventory/NetworkElement.xml where the snippet in **Figure 5-2** is taken from.

Figure 5-2 Configuration snippet from the CRModel NetworkElement.xml resource definition file

```
<Field mandatory="false" encrypt="true" password="true">
  <Name>Password</Name>
  <Type>String</Type>
  <Description>Password for management connection</Description>
</Field>
```

This enforces the password to be encrypted before inserting the row in the database. And it is then decrypted in the CLI-Plugin when sending it to the device.

To enable decryption of the password in the CLI-Plugin, the templates must indicate to the plugin which commands corresponds to passwords. In the following **Figure 5-3** a snippet from template_files/Cisco/Cisco-ConnectDisconnect.xsl template let you observe that when telnet is the management protocol.

Figure 5-3 Configuration snippet from the CLI-Plugin Cisco-ConnectDisconnect template

```
<Confirm>
    <Pattern>Password: $</Pattern>
    <Command isPassword="yes" isEncrypted="yes">
     <xsl:value-of select="$passwd"/>
  </Command>
</Confirm>
```

This allows the CLI-Plugin to decrypt the $passwd parameter and to avoid logging the clear text password.

These configuration snippets in **Figure 5-2** and **Figure 5-3** must go hand-in-hand. If one indication of the usage of encrypted passwords is missing the behavior of the system will be erroneous.

If SSH is used as the management protocol, the password pattern is not expected and used in the login dialog with the NE. But the server (NE) may still request SSH to supply a password. Hence, the usage of encrypted password in case of SSH as the management protocol is defined via the ssh.isEncrypted attribute shown in section 5-5 below.

NOTE: For details on setting the password policy, refer to [*INTEGRATE*] and [*INTRO*]

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

5-5 SSH as NE Management Protocol

The NE management protocol may be specified as telnet or SSH. When it is specified as SSH, certain defaults have been preconfigured into the activation templates. In **Figure 5-4** you may see a snippet from template_files/Cisco/Cisco-ConnectDisconnect.xsl template that illustrates these defaults.

Figure 5-4 Snippet from Cisco-ConnectDisconnect template

```
<Connect protocol="{$connection_protocol}"
         ssh.username="{$username}"
         ssh.password="{$passwd}"
         ssh.isEncrypted="yes"
         ssh.known_hosts="/.ssh/known_hosts"
         ssh.identity="-"
         ssh.allow_host = "true">
```

NOTE: VPN_SVP VPN_SVP sets the ssh.allow_host attribute true by default. This avoids that an initial SSH connection to the device requires a manual acceptance of its identity. By setting ssh.allow_host to true, the identity of the remote host (the NE) is automatically accepted.

If this is not acceptable, the attribute has to be set to false, and some initial acceptance of the NEs identities must be made before successful connections may be established by the CLI-Plugin.

NOTE: Consult the HPSA documentation for more information about the usage of these SSH attributes.

NOTE: Consult section 5-3 above for more information on using SSH as CE management protocol

---

6 Configuration of Inventory

This chapter explains the initial configuration/customization of the VPN_SVP that must be completed before VPN services may be provisioned.

The major part of the configuration and customization of the VPN_SVP that is required to match the needs of a specific service provider is done via the Inventory GUI.

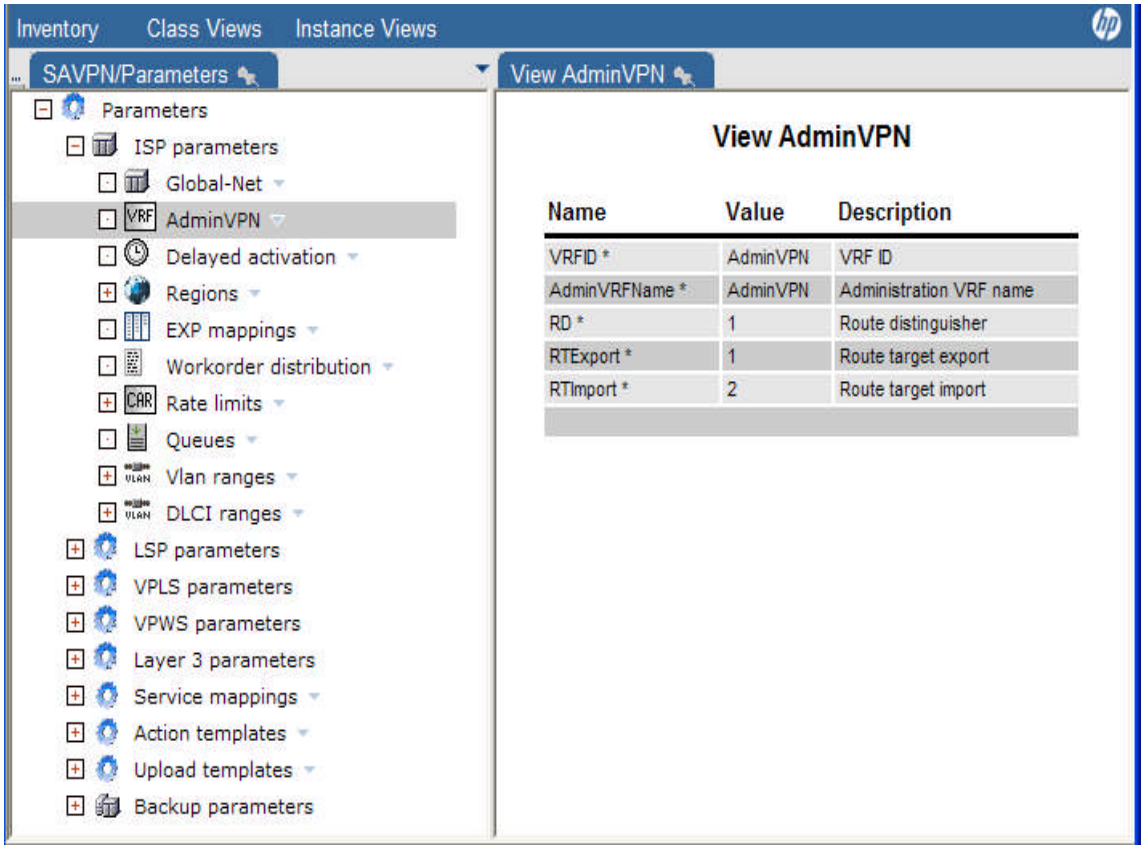
The Inventory GUI is instantiated by selecting the Work Area menu item ‘Inventory’ displayed in HPSA Main GUI, left pane menu.

6-1 Initial Configuration of ‘Parameters’ View

Figure 6-1 below shows the three available instance views of the Inventory GUI: SAVPN/Services, SAVPN/Equipment and SAVPN/Parameters.

The Initial configuration of VPN_SVP consists of configuring the Parameters section and the Equipment sections.

Figure 6-1 Inventory GUI – SAVPN/Parameters Instance view



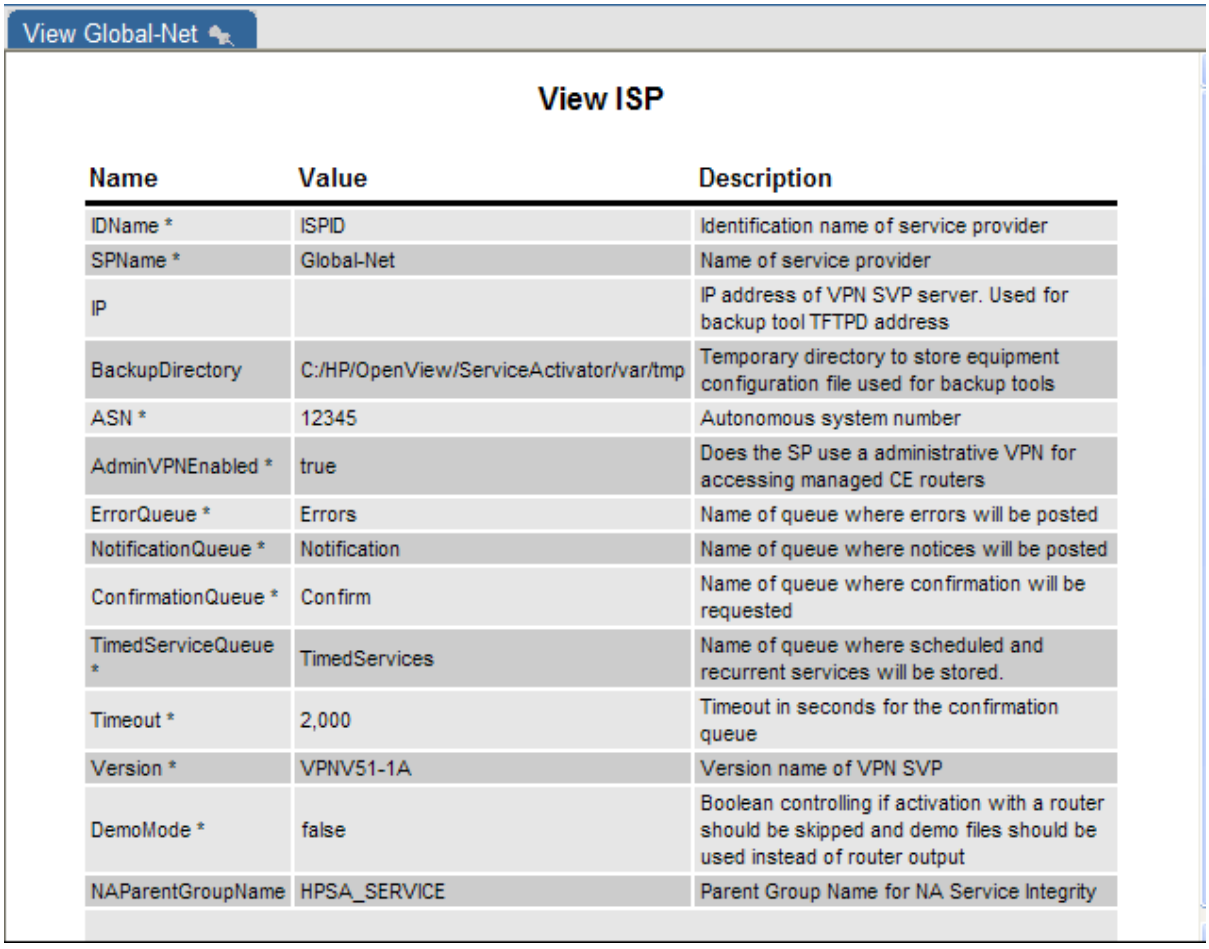
The initial configuration of VPN_SVP Parameters consists of configuring objects described in the following sections.

6-1-1 SP Parameters

- **Global-Net** - Select Edit function on 'SP' (Global-Net) and set the following parameters:
  - **SPName** - set the name of the Provider (i.e. change Global-Net to the actual provider name)
  - **IP –** optionally, but if the VPN_SVP server is multi-homed (i.e. has several IP addresses), select the IP address to be used from the NEs to access the backup protocol process on the VPN_SVP server
  - **BackupDirectory –** optionally, used for backup tool to agree between VPN_SVP VPN_SVPand the installed backup protocol where equipment configuration files are temporarily placed in the file system
  - **ASN** – sets the default Autonomous System Number allocated to the Provider. This will be used as the ASN in case the networks configured in Equipment Tree doesn't configure a specific ASN or in case the Provider's core network is not of Multi-AS backbone type.
  - **AdminVPNEnabled –** set to 'Yes', if the provisioning commands must add Managed CE connectivity with an AdminVPN (which is normally the case).
  - **DemoMode** – make sure this is set to 'No' before activation on real equipment!
  - Leave the remaining parameters as is

NOTE: NAParentGroupName – This represents the Parent Group Name that needs to be set in the HP NA. For more details see section 11-2-1

Figure 6-2 Inventory GUI – View ISP



- **Admin VPN** - If AdminVPNEnabled was selected 'Yes', select the Edit function on 'Admin VPN' and set the following parameters:

- **RD –** Route Distinguisher used for the AdminVPN VRF associated the Hub site (NOC attachment point), e.g. 1. The actually value will get the "<ASN>:" pre-pended depending upon the ASN value of the network where the NOC is connected, or the default value of the Provider's ASN set above.

NOTE: AdminVPN's Hub site is assumed to be manually preconfigured according to these values.

- **RTExport –** the Route Target Export value defines the tag added to the routing information send from the Hub site (NOC) and which is to be imported by the Spoke sites (Customer VPN Sites). E.g. set to 1. The actually value will get the "<ASN>:" pre-pended depending upon the ASN value of the network where the NOC is connected, or the default value of the Provider's ASN set above.
- **RTImport -** the Route Target Import value defines the filter used on the Hub site (NOC) when receiving routing information from the Spoke (Customer VPN Sites) or other Hub sites (other NOCs). E.g. set to 2. The actually value will get the "<ASN>:" pre-pended depending upon the ASN value of the network where the NOC is connected, or the default value of the Provider's ASN set above.

NOTE: The AdminVPN constitutes a Hub&Spoke type VPN which every Managed CE Sites is automatically joined into as Spokes.

The RTExport and RTImport values above are from the HUB (NOC attachment) site point of view. Hence, sites that are joined into the AdminVPN as Spoke sites will use the opposite values, e.g. <ASN>:1 as RT import and <ASN>:2 as RT export (see section 5-2 above) where the ASN value is extracted from the configuration of the network where the site is connected, or extracted from the default value of the Provider's ASN set above.

The HUB site is assumed manually pre-configured. The Spoke sites (i.e. managed CE sites) will get the corresponding Spoke RT import/export automatically joined into their VRF by the VPN_SVP activation process.

- **Delayed Activation –** set the parameters that control automatic retries of service request that fails to connect to the NE.
  - **NumberOfRetries -** Total number of activation retries to be performed - for no retries value is 0
  - **Days -** Time Period between activation retries - Days
  - **Hours -** Time Period between activation retries - Hours
  - **Minutes -** Time Period between activation retries – Minutes

NOTE: If a service request does not successfully connect to a NE within the specified number of reties, the request will be redirected to the Error Handler WF.

- **Regions –** Expand the 'Regions' branch and select the 'Create Region' action to define the Regions of the Provider Network.
  - **WODistribution** – Work-orders may be automatically distributed by e.g. email to 3rd party technicians that perform the initial installation/configuration of CE routers. This configuration item allows you to configure a recipient email address valid for the work-orders within that region. If no Region level WoDistribution configuration is found, the global level WoDistribution item is used when the recipient address is to be determined for distributing work-orders.
  - **Locations –** Regions may consist of Locations. Use the 'Create Location' action to define the Locations under each Region.
    - **WODistribution** – same as above but at the granularity of the Locations. If no Location level WoDistribution configuration is found, the Region level item is used when the recipient address is to be determined for distributing work-orders.

NOTE: Regions and Locations provide a hierarchical structure to the Provider's Network. The provider's network may be sub-divided into Regions and for each region the PE routers may be situated at different Locations.

Operators may be associated Region based roles which confines and restricts the network operator's task to be related to equipment within the associated Region(s). A VPN create service request will specify a Region and a Location. Hence, only network operators having a Role associated that corresponds to the requested Region may interact with that specific request and when selecting a PE interfaces for the Site's attachment circuit, only PE routers from the requested Location will be selectable.

NOTE: See chapter 8 for information related to configuring the operator's login ids and their associated roles.

  - **Vlan Ranges –** For each Region a Vlan allocation scheme used by Ethernet based services may be specified. If no Region level Vlan Ranges configuration is found, the global level Vlan Ranges are used when validating the Vlan id.
  - **DLCI Ranges –** For each Region a DLCI allocation scheme used by FrameRelay links may be specified. If no Region level DLCI Ranges configuration is found, the global level DLCI Ranges are used when validating the DLCI.

- **EXP Mappings –** Here the fundamental Class of Service (CoS) and QoS related configurations and mappings are specified. For each of up to 8 CoS, the Class name, its mapping to MPLS EXP marking in the MPLS core network, the DSCP marking used to identify the CoS when classifying the traffic on the CE router, the Loss Priority used and the queue names used (particular on Juniper PE devices). The Loss Priority combined with the Queue may provide more CoSs than the number of available queues otherwise would allow.
- **Rate Limits –** An initial set is provided. But more or other Rate Limits may be defined. Rate limits are used in the QoS policing configuration to limit the data rate that a customer site may send into the provider network. Also it may be used to shape the traffic towards the customer site. The associated average bits per second, normal and maximum burst sizes must be specified. These entries are vendor independent but some devices/vendors may restrict the acceptable burst values. Such specific restrictions are normally best implemented in the device/vendor specific configuration templates (.xsl templates)
- **Queues –** The queues are optional components that may or may not be used. These objects are used to temporary store information that must be distributed to e.g. external systems. This is typically used to decouple the service activation work-flows from the distribution tasks. Each queue may be associated a distribution mechanism, e.g. SMTP. See [*USR*] for detailed information. The various types of queues that can be created are:
  - Workorder: This type of queue is set when the CE workorders generated during creation of Layer 3 Sites needs to be distributed
  - NA: This type of queue is set to send across the service information to NA, so that appropriate policies can be created on HP NA.
  - NNM: This type of queue is set to send across the service information to NNMi, so that appropriate annotation operations can be performed on HP NNMi.

Queue States could be in one of the active, disable, or suspended states.

- Active: Enqueue and dequeue of message happens
- Suspended: Enqueue of message happens. Dequeue is not allowed.
- Disable: Enqueue and dequeue of messages are not allowed. In this state, the messages can be deleted.

In case of communication issues with external systems, the network operator should inspect the queue contents and take appropriate action, like deleting the message..

NOTE: See sections 10-1-6 and 11-1-3 for details on queue setup for NA and NNMi liaison

- **Vlan ranges –** These objects allows for a global Ethernet Vlan id allocation scheme for Ethernet based attachments to be defined. Currently a single scheme is supported for all PEs/Access networks, but a specific Vlan id may be reused on independent PEs/Access networks. The allocation scheme allows for dividing the total range of 4094 Vlan ids into ranges which are then assigned to specific usage.
  - **Usage –** Assign a usage type or purpose of a Vlan range that then allows for specific usage/treatment by VPN_SVP of that range. The following types are supported:
    - **Management –** Represents the Vlans used for management purposes, e.g. to provide management access to the NEs in an access network. This Vlan range will not be used or allocated by VPN_SVP for any services.
    - **BridgeGroup** - Represents Vlans used in certain VPWS service scenarios where a bridge-group/bridge-domain Vlan id is used.
    - **Attachment –** This range is used to allocate Vlan ids for services attached via an L2 switched access network or directly to PE routers.
  - **Allocation** – Specifies how the allocation is made. The **internal** is used for auto-allocation by VPN_SVP and **external** is used for customer/operator specified VLan ids.

Figure 6-3 Inventory GUI – View Vlan Ranges

Usage	Allocation	StartValue	EndValue	Description
Management	Internal	171	200	
Attachment	Internal	501	750	
Attachment	External	751	1000	
Attachment	Internal	2001	3000	
Attachment	External	3001	4000	
BridgeGroup	Internal	201	500	

- **DLCI ranges –** Similar in purpose to the VLan ranges described above but addressing DLCI allocation of Frame Relay encapsulated attachments. These objects are simpler as only direct attachments are supported, so DLCI range of 1024 values are sub-divided into an internal and external allocation range.

NOTE: Normally only the DLCI range from 16 – 991 is allowed.

Figure 6-4 Inventory GUI – View DLCI Ranges

Usage	Allocation	StartValue	EndValue	Description
Attachment	Internal	200	511	
Attachment	External	512	999	

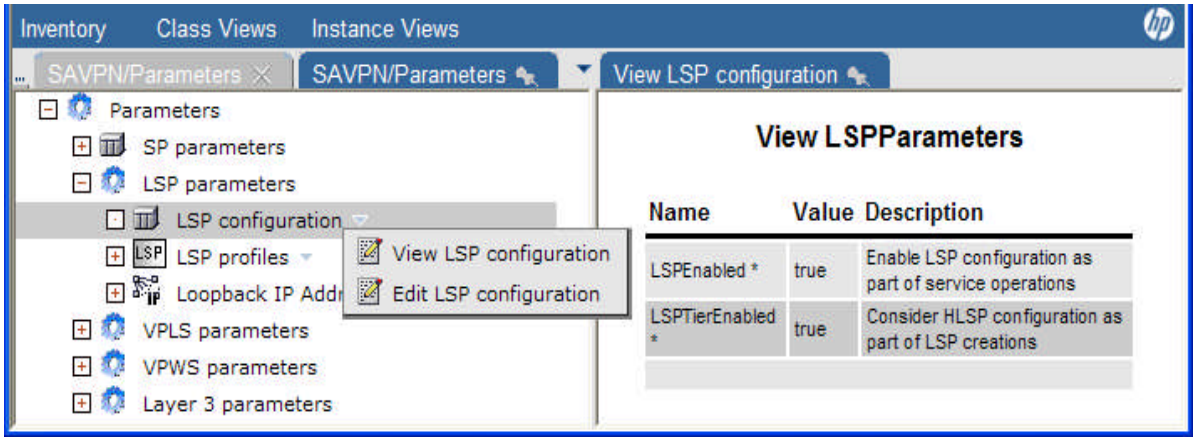
6-1-2 LSP Parameters

The LSP Parameters section contains the objects relevant for enabling and usage of the Traffic Engineering LSP feature. Before using this feature, it must be enabled, the required profiles must be created, and the LSP loopback pool must be created as described below. If the feature is not to be used, no actions in this section are required.

- **LSP configuration** – The LSP feature is by default disabled but may be enabled via the Edit action.
  - LSPEnabled – controls whether the LSP feature is globally enabled or not. When ‘true’ the service integrated LSP feature is enabled and LSP will be created/modified/deleted as required by the service requests.
  - LSPTierEnabled – controls whether hierarchical LSP needs to be considered while activating LSPs. If the LSPEnabled is ‘true’, and this flag is set to ‘true’, the PEs in the

MPLS network can be logically separated into up to 3 tiers. PE's with Tier1 are closest to the MPLS core, and the higher Tiers are successively farther from the MPLS core.

Figure 6-5 Inventory GUI – View LSP Parameters



- **LSP profiles** – The LSP profiles keep attributes common for a specific usage or type of LSPs and support variability in how LSPs should be configured and used, still maintaining generality and simplicity in the provisioning process. In this release only a subset of the attributes are used but included for future enhancements. The Operator defines the basic profiles in the Inventory, initially or later in the process when required by the following steps:
  - Select the 'Create LSP profiles' action on LSP profiles and set the following parameters:
    - **LSPProfileName –** Set to any Operator selected value e.g. to 'DataLSP'.
    - **Type –** Select the type from the selection list. Currently only 'VPN' is supported.
    - **CT –** Select the LSP's Class Type from the selection list. The values ct0, ct1, ct2 and ct3 are supported. This is the key used by the LSP creation process to select among the LSP profiles when the required CT is known. All LSPs created for this specific CT will use this profile.
    - **bwAllocation** – LSP Profiles can be created with either 'Manual' or 'Auto' bandwidth allocation mode. Only one version for a given Class Type (CT) is allowed. The 'Manual' mode interaction allows operator to assign bandwidth to each LSP as well as to determine whether the LSP should be created or not. The LSPs assigned 'Auto' allocation mode requires no operator interaction. Further addition of VPN sites or modifications of rate limits of existing VPN sites will automatically update the associated LSP's bandwidth accordingly. When set to 'manual' the service integrated automatic modifications of the LSP's bandwidth will be disabled and the Operator is required to change the bandwidth.

NOTE: If a LSP is created with 'Manual' bwAllocation mode, and then LSP is modified to 'Auto' mode, the LSPs in both directions get modified to 'Auto'.

If a LSP is created with 'Auto' bwAllocation mode, and then LSP is modified to 'Manual' mode, the LSPs in both directions get modified to 'Manual', and the bandwidth gets set to the assigned value.

    - **bwAlgorithm** – Currently only the 'Sum' algorithm is supported. When an LSP is created/modified, its bandwidth is set to the (class type specific fraction) sum of the ingress rate_limits over the VPN sites on the head end PE.
    - **CoS** – When setting up a VPN service, a number of CoSs may be included in the QoS profile sharing the total rate limit of the service. The LSPs need to be created per Class Type. This attribute specifies the mapping from CoSs to the specific CT defined above so the solution can assign the bandwidth and CT correctly to LSPs.
    - **LSPFilter** – The Operator provides the name of the LSPFilter that is to be associated LSPs created with this profile.

NOTE: It is assumed, that the configured LSPFilter name may need to be extended with VPNid information to make it VPN specific and that this extension is done by local customizations.

It is also assumed, that the LSPFilters are preconfigured on the PE routers as part of their base-line.

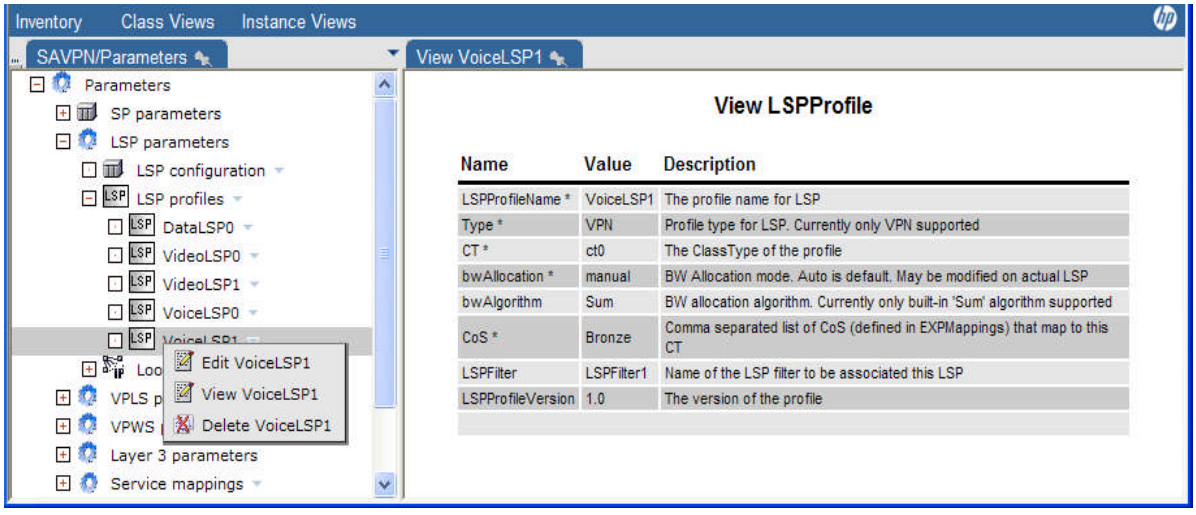
- **LSPProfileVersion** – This attribute is maintained automatically. It will by default be set to '1.0' and will not be modifiable. It allows modifications to the profile itself without changing the already deployed instances but only following created services. It will automatically be incremented if the CoS field or LSPFilterName is reconfigured while LSP exists having the previous version associated. A history of profiles in active use can then be kept so e.g. a profile may not be deleted as long as services (LSPs) are using it.

NOTE: LSPProfileVersion is not supported in this version.

- Select the 'Edit' action on a created LSP profile to modify it defined attributes. This currently only allows you to modify the assigned CoS that maps to the set CT:
  - **CoS** – This attribute specifies the mapping from CoS to the specific CT set on the profile so the solution can assign the bandwidth and CT correctly on created LSPs.

NOTE: The other attributes are not currently modifiable. Hence, you may be required to Delete a profile and then re-create it with modified attribute values.

Figure 6-6 Inventory GUI – View LSP Profile



- **Loopback address pool** – The creation of LSPs require IP addresses to be assigned to LSP endpoints. This pool allows you to define the range of these addresses
  - Select the 'Create AddressPool' action on 'Loopback address pool' and set the following parameters for LSP loopback address pool:
    - **Name –** Set e.g. to 'Loopback' for the address pool to be used for allocation of LSP loopback IP numbers
    - **IPNet –** The IP Network number from which the individual IP Network addresses are to be drawn. E.g. a class-A private address like 10.14.0.0
    - **Mask –** The corresponding IP Network mask where e.g. 16 is representing 255.255.0.0.

- **Type –** Select ‘LSP’ for LSP loopback IP Network address pool.

6-1-3 VPLS Parameters

The VPLS parameters consists of QoS related objects: Traffic classifier and QoS profiles for VPLS services. The predefined VLPS Parameters may be sufficient or used as examples for how more/other Classifiers and Profiles may be created.

- **Traffic classifiers** – A traffic classifier is used specify the criteria that data traffic/packets must fulfill to be consider belonging to a specific class of service out of a total of 8. Each class may then be given specific/different treatment according to the profile. VPLS supports classification based on the COS bits (p-bits) in the Ethernet tag.
- **VPLS Profiles** – A QoS profile specifies how the total amount of data (the rate limit) associated the customer site, is distributed among the defined CoS. The amount is specified in percentages of the rate limit. When a L2VPN site service is requested in the CRM portal, a QoS profile defined here may be selected

NOTE: A QoS profiles can not be deleted, when services exists that have been provisioned using that profile. You may create new at will.

6-1-4 VPWS Parameters

The VPWS parameters consists of QoS related objects: Traffic classifier and QoS profiles for VPWS services. The predefined VPWS Parameters may be sufficient or used as examples for how more/other Classifiers and Profiles may be created.

- **Traffic classifiers** – A traffic classifier is used specify the criteria that data traffic/packets must fulfill to be consider belonging to a specific class of service out of a total of 8. Each class may then be given specific/different treatment according to the profile. Currently only a single CoS may be associated VPWS traffic.
- **VPWS Profiles** – For VPWS only a single CoS is currently supported. Hence all (100%) of the traffic may be assigned to a single of the 8 CoS available. When a L2VPWS service is requested in the CRM portal, a QoS profile defined here may be selected.

NOTE: A QoS profiles can not be deleted, when services exists that have been provisioned using that profile. You may create new at will.

6-1-5 Layer 3 Parameters

The Layer 3 specific parameters consist of QoS related objects (Traffic classifiers and QoS profiles) , IP address pools and enabling the VRRP for redundancy configuration. The predefined Layer 3 QoS parameters may be sufficient or used as examples for how more/other Classifiers and Profiles may be created

- **Traffic classifiers –** L3 traffic may be classified according to DSCP values or according to IP addresses and TCP/UDP ports. To create a classifier, select the **Create TrafficClassifier** action on ‘Traffic classifiers’. You must create the classifiers before they be associated the profiles
- **Profiles –** L3 QoS profiles specifies how the total amount of data (the rate limit) associated the customer site, is distributed among the defined CoS. The amount is specified in percentages of the rate limit. In the profiles you associate up to 8 classifiers with a CoS and the percentage (of rate limit) amount of the traffic that may be transferred in this CoS. When a site service is requested in the CRM portal, a QoS profile defined here may be selected.

NOTE: A QoS profiles can not be deleted, when services exists that have been provisioned using that profile. You may create new at will.

- **Address pools** - The IP Address Pools must be defined. These pools are use for allocation of IP Network numbers to the attachments (access flows), for CE Loopback addresses, for Multicast service (MDT Default, MDT Data and Multicast Loopback interface addresses). The following section describes how to create an address pool for attachment circuits and for CE Loopback addresses.
  - Select the 'Create AddressPool' action on Address pools and set the following parameters for attachment circuit IP Network address pool:
    - **Name –** Set e.g. to 'PE-CE Default' for the default address pool to be used for allocation of attachment circuit IP Network numbers
    - **IPNet –** The IP Network number from which the individual IP Network addresses are to be drawn. E.g. a class-B private address like 172.17.0.0
    - **Mask –** The corresponding IP Network mask where e.g. 16 is representing 255.255.0.0.
    - **Type –** Select IPNet for attachment circuit IP Network address pool.
  - Submit (OK) the values to create the pool parameters
  - Select the 'Create Address' action of the newly created pool and set the following parameters:
    - **First IP network** – The starting IP Network address and mask for the entries (in address/mask notation). It is possible to use /31 to maximize the number of network numbers and minimizing the consumed IP address space though /30 is the recommended mask.
    - **Number -** The needed number of entries. This should correspond to the number of attachment circuits expected to have network address allocated from this pool.
    - Submit (OK) to create the address pool entries
  - This procedure must be repeated for the different address pool needed. So e.g. select the 'Create AddressPool' action again and now set the following parameters for the CE Loopback IP address pool:
    - **Name –** Set to 'CE loopback' for the address pool to be used for allocation of CE loopback IP addresses
    - **IPNet –** The IP Network number from which the individual IP Network addresses are to be drawn. E.g. a class-A private address like 10.1.0.0
    - **Mask –** The corresponding IP Network mask. E.g. 16 representing 255.255.0.0.
    - **Type –** Select IPHost for CE Loopback IP address pool
  - Submit (OK) the values to create the pool parameters
  - Select the 'Create Address' action of the newly created pool and set the following parameters:
    - **First IP address** – The starting IP host address for the entries (the mask is assumed to be /32).
    - **Number -** The needed number of entries. This should correspond to the number of Managed CE routers expected to have a loopback address allocated from this pool.
    - Submit (OK) to create the address pool entries

NOTE: Only one address pool of Type IPHost, multicast pools (MDT Data, MDT Default, Multicast loopback) and LSP Loopback can be created.

Below tables provide some sample IP Address pools to serve as examples.

Table 6-2 Sample IP Address Pools

Address Pool Type	IPNet	Mask
IPHost (CE loopback)	10.20.30.0	24
IPNet (PE-CE Default)	172.17.0.0	16
IPNet (Slash31)	192.168.70.0	24
MDT Data	226.0.0.0	8
MDT Default	225.0.0.0	8
Multicast loopback	99.0.0.0	8
Loopback (LSP)	12.14.6.0	24

Table 6-3 Sample IP Addresses in different address pools

Pool Name	IPNet Address	Netmask	Hostmask
IPNet (Slash31)	192.168.70.0	255.255.255.254	0.0.0.1
IPNet (PE-CE Default)	172.17.0.0	255.255.255.252	0.0.0.3
MDT Data	226.0.0.0	255.255.255.0	0.0.0.255

- **VRRP** - The VPN_SVP supports configuration of Virtual Router Redundancy Protocol (VRRP) which provides a first hop redundancy in a LAN environment which e.g. has static route configured for the default gateway. This may be relevant when attaching L3 services via an L2 access network that terminates in two or more PE routers. This configuration item determines whether VRRP is enable or not by default. It is possible for the network operator in the Router and interface selection form to change the default assigned VRRP mode. If it is enabled, the master PE and the VRRP Group id may optionally be modified from the default selected values.
- **Multicast Bandwidth Policy** – This flag determines the bandwidth allocated to the multicast sites.

6-1-6 Service mappings

The Service mappings provided represents the service catalog of VPN_SVP and contains the currently supported services that may be requested from external systems (e.g. CRM Portal). Each entry corresponds to a possible <Action_name> (service operation) and <Service_name> (service object) combination in the <header> element of a request message (see section 4-1). For each entry, the workflow implementing the corresponding service request is specified.

The Controller workflow uses this table to lookup and instantiate the workflow to handle a particular service request.

Normally there should be no need to change the provided service mappings. But if new services/workflows are created, corresponding entries must be made to allow a remote system to request the new services.

6-1-7 Action templates

The action templates provided represents the set of device activations currently supported by VPN_SVP. An action template represents the device/equipment specific configuration commands which must be executed to configure the associated Action or service (e.g. Add, for adding a L3 VPN site).

If new vendors and /or element types are to be supported, the new Vendor, OS version and/or Element Type must be created as described below under Equipment Parameters.

When that is done and the new action template files (xsl format) have been created, select ‘Create Action Templates’ and fill-in the form. Use the existing definitions for guidance.

NOTE: If devices have been created in the inventory Equipment section but have not been associated some action templates, these devices will be unavailable for selection by the network operator for provisioning of that associated Action or service

6-1-8 Upload Templates

The Upload templates provided represents the set currently support by VPN_SVP. Upload of interfaces, controllers and description keywords (UPLINK, RESERVED) is supported. Also the SNMP ifIndex may be uploaded and associated the interfaces.

NOTE: See section 6-3 for more information.

6-1-9 Backup Parameters

Backup Parameters represents the configuration necessary to support the backup and restore of the router configurations.

- **Memory Type –** This represents the device specific name of the type of configuration that is associated the selected generic Target Type (see below). So e.g. on Cisco, if Target Type ‘Startup’ is selected, the device/vendor specific configuration memory type must be set to: startup-config.

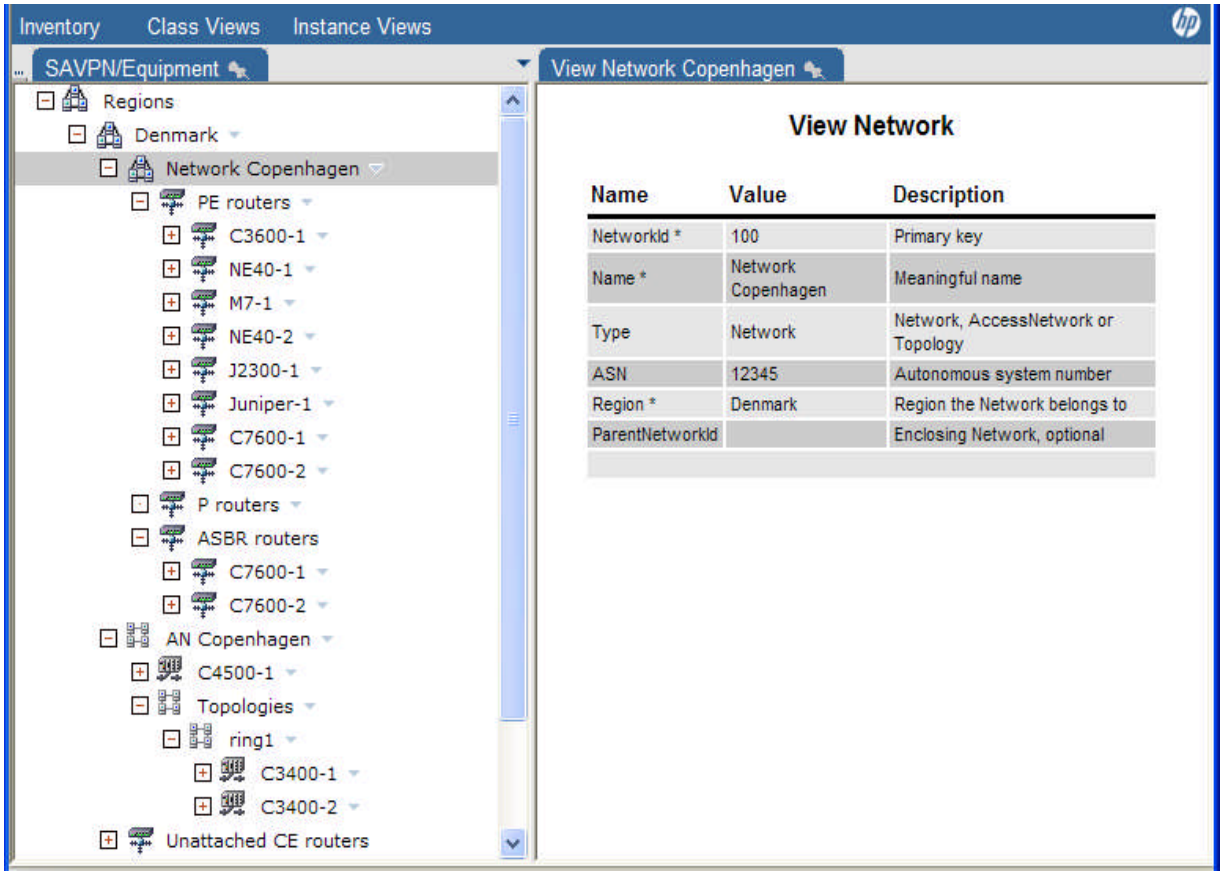
NOTE: Failing to define memory types for new element types will prevent support for configuration backup/restore for those devices.

  - **OS** - select the relevant OS version. Different OS version may have different Memory Type.
  - **Target Type** - select the generic target type corresponding to the Memory Type. Currently ‘Startup’ and ‘Running’ are the supported generic Target Types.
  - Submit the form to associate the defined Memory Type with the Element Type.

6-2 Initial Configuration of ‘Equipment’ View

Figure 6-7 below shows the inventory SAVPN/Equipment view. The shown example has already been configured with some Networks and Routers.

Figure 6-7 The SAVPN/Equipment instance view



The Equipment view contains the top-level Regions consisting of one or more networks. Network may be of type Network (normal) or of type AccessNetwork that may contain sub-networks (topologies) representing e.g. rings in an access network.

To support Multi-AS backbone networks, each network of type network may be associated an Autonomous System Number (ASN). This will be used in the configuration/activation items that require an ASN value. If it is not specified on the network, the global/default ASN value configured as described in section 6-1-1 above will be used.

For each network a number of PE routers and optionally P routers may be defined. For an Access Network, Aggregation Switches and Access Switches may be defined. The PE routers and Access Switches are used for the attachment points of customer services. The PE routers represent the MPLS edge of the provider’s core network.

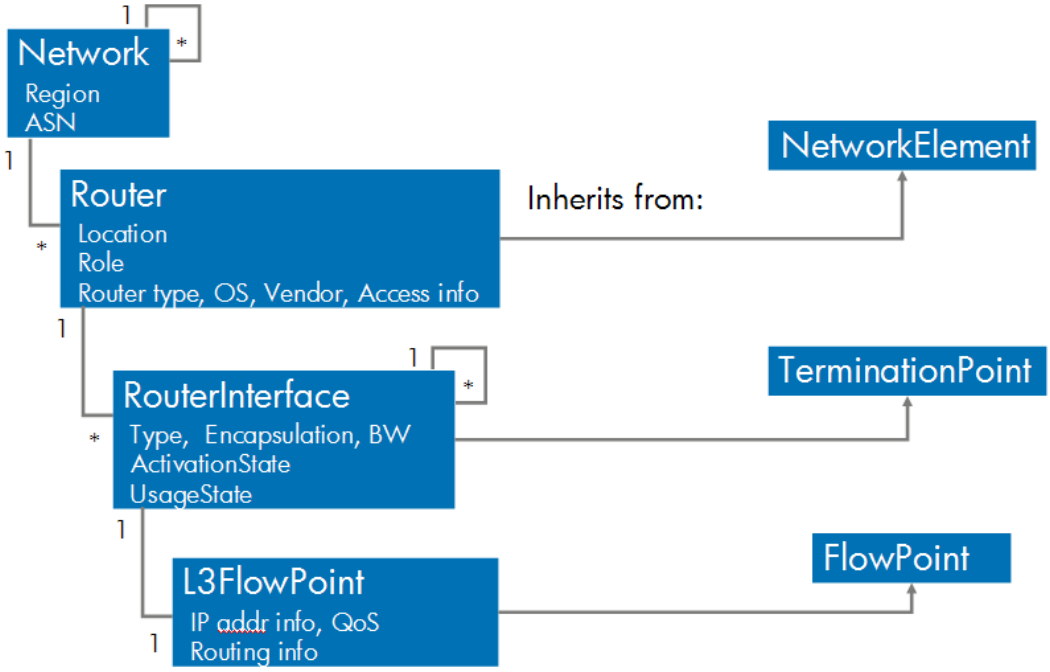
The P routers are included for the purpose of enabling the backup tool to manage their configurations. The P routers will not be selectable nor activated for any services.

When services are provisioned which include managed CE routers, these CE routers will also be populated into the inventory.

Each device may contain interfaces, and optionally controllers, uploaded from the network. Among the switches and between the aggregating devices and the PE routers, trunks may be created that represents the interconnection between the switches and the connection of the access network to the PE routers (MPLS edge).

When services are terminated on an interface, a flowpoint object representing the attachment of the service to a device interface will be created. This represents the lowest level in the Equipment tree. This model is illustrated in **Figure 6-8**.

Figure 6-8 Simplified view of the equipment model



The initial configuration of VPN_SVP Equipment consists of configuring the following objects:

- **Regions -** The Regions constitutes the top level branch and expanding these will display the individual Regions that where defined in the previous section 6-1-1 . The association of Roles corresponding to these Regions may be used to restrict the display of Region branches (see Chapter 8), so only specific operators may inspect specific Regions in the Inventory GUI.
- **Networks -** For each defined Region, select the ‘Create Network’ action and set the following parameters:
  - **Name** - set the name of the network.
  - **Type** - the type will be fixed as Network. Submit (OK) the form to create the defined Network. Repeat this in each Region for each network to be created
  - **ASN** – set the ASN associated this network. If not specified, the global/default value will be inserted.
- **Access network -** for each defined Region, select the ‘Create AccessNetwork’ action and set the following parameters:
  - **Name** - set the name of the network.
  - **Type** - the type will be fixed as AccessNetwork.
  - **State** – will be initialized as ‘Planned’. Modify the state to Ready when the construction of the access network is complete and it is ready for activation.
  - **ManagementVlans** – specify the Vlans used for management of this access network. Only values within the range ‘Management’ specified in section 6-1-1 Vlan ranges. Submit (OK) the form to create the defined Network. Repeat this in each Region for each network to be created

- **PE Routers**

  For a defined Network, expand the branch and select the 'Create PE routers' action and set the following parameters (the full sets of parameters are illustrated in **Figure 6-9** below):

  - **Name** - set to the name of the router
  - **Location** – select among the earlier defined Locations under that Region
  - **Loopback IP** and **Management IP** – these two addresses represent the IP address used between PE routers (i.e. the loopback IP) and the IP address used to configure the PE router (i.e. the Management IP used by VPN_SVP)
  - **Management Protocol** – select among 'telnet' or 'ssh' as the protocol to be used by VPN_SVP to connect to the PE router when activating services.
  - **UsernameEnabled** – set to 'Yes', if the router is configured to prompt for a Username upon logon. Set to 'No' if a Password prompt is the first to appear
  - **BGPDiscovery** – set to 'Yes' for e.g. Juniper routers supporting BGP Auto-discovery of VPLS sites
  - **LifeCycleState** – is default set to 'Planned'. When the router has been physically placed in the Network and is actually accessible using the defined IP address and authentication information, the LifeCycleState must manually be set to 'Accessible'. When the core facing interfaces have been assigned a description field of UPLINK and possibly other interfaces not to be used for service attachments or otherwise to be reserved have been assigned a description field of RESERVED, the LifeCycleState must be manually set to 'Preconfigured'. In this state, the interface Upload function may be selected and will automatically set LifeCycleState to 'Ready' (see section 6-3). When the router is Ready it as available for selection when services has to be attached.
  - The remaining parameters are more or less self-explanatory
  - Submit (press OK) the form to create the defined PE router

  Repeat this in each Region and each Network for each PE router to be created.

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.

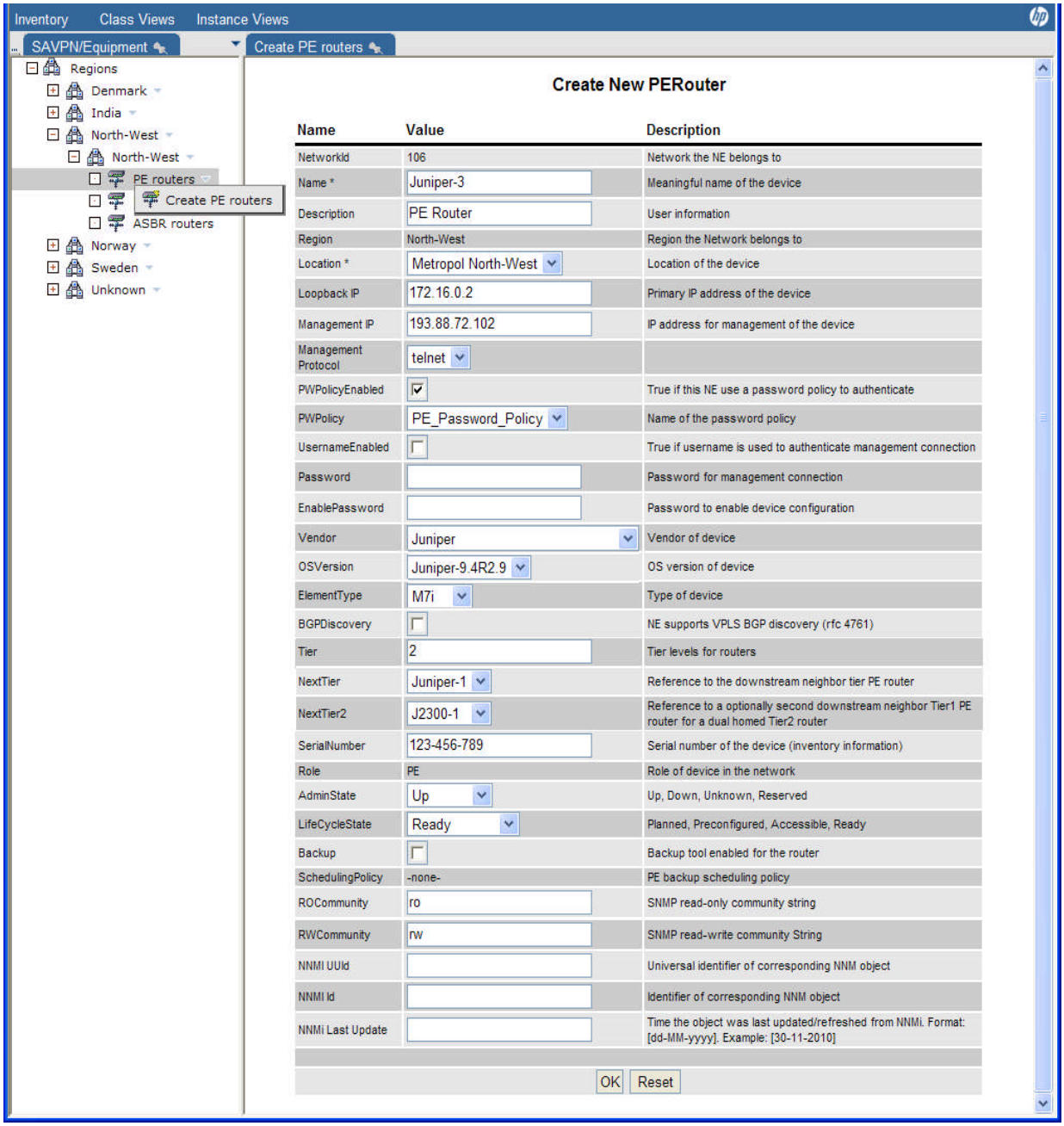
When adding a PE router, the form accepts entering a Tier value. If the value "1" is entered, nothing further happens and the form may be submitted.

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.

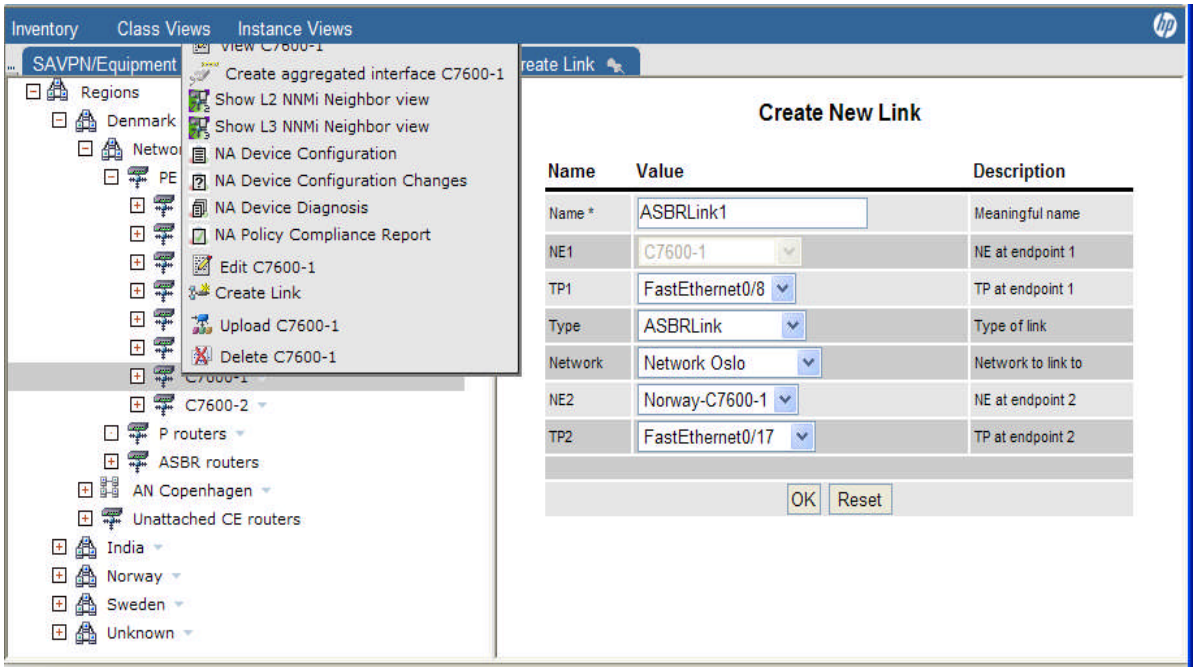
Figure 6-9 Equipment view. Create PE router form



When the PE routers of your networks have been created and they are physically present in the network and accessible, you may modify the LifeCycleState to ‘Accessible’ (or ‘Preconfigured’) and perform an interface upload function. This will extract the interface information from the router configuration and populate the inventory with the interfaces on the access devices. See section 6-3

- **ASBR routers –** For a Multi-AS backbone networks, the Autonomous System Border Routers (ASBR) must be identified and the interconnecting links created. This is done by selecting from the routers in the ‘PE routers’ branch, the ‘Create Link action (see **Figure 6-10**). In the form, choose the Link Type as ASBRLink. When completed these selected PE routers will also appear in the ASBR routers branch. The ASBR routers interface to ASBR routers in neighboring ASNs via the created ASBR links. The ASBR routers have Role as PE as they may also be used to attach to services as normal PE routers.

Figure 6-10 Create ASBR Link Form.



- **Aggregation Switches -** For a defined Access Network, right-click and select the 'Create Aggregation switch' action. The form is similar to the Create PE router form and is to be filled out similarly as described above.
  - Submit (press OK) the form to create the defined Aggregated Switch.

  Repeat this for each Access Network and for each Aggregation Switch to be created. Usually two aggregation switches are used for attaching and access network to two PE routers.
  - Trunks - Trunks can be created to attach this Aggregated Switch to Access Switch or to the PE router.
    - AggregationTrunk: Create a Trunk of Type "AggregationTrunk" to attach this Aggregated Switch to the PE router or another Aggregated Switch.
    - AccessTrunk: Create a Trunk of Type "AccessTrunk" to attach this Aggregated Switch to the Access Switch.
- **Topologies** – Expand the Access Network branch and right-click the Topologies branch and select the 'Create Access Topology' action to create e.g. a ring topology in your access network. Repeat this for each topology (e.g. ring) to be created.
- **Access Switches** - Expand the Topologies branch and right-click one of your created topologies. Select the 'Create Access Switch' action. The form is similar to the Create Aggregation Switch' form and is to be filled out similarly as described above.
  - Submit (press OK) the form to create the defined Access Switch

  Repeat this for each Access Switch to be created.

When the devices of your access networks have been created and they are physically present in the network and accessible, you may modify the LifeCycleState to Accessible (or Preconfigured) and perform an interface upload function. This will extract the interface information from the router configuration and populate the inventory with the interfaces on the access devices. The final steps in setting up the access network may then be completed:

- **Trunks** – Trunks can be created to attach this Access Switch to the UPE router or Aggregation Switch or another Access Switch.
  - AccessLink: Create a Trunk of Type "AccessLink" to attach this Access Switch to a UPE router.
  - AccessTrunk: Create a Trunk of Type "AccessTrunk" to attach this Access Switch to another Access Switch or to an Aggregated Switch.

- **Attach the Topologies** –Right-click an aggregation switch in your access network and select the 'Attach Access Topology' action. In the form specify the two end-points of the trunk connecting the aggregation switch to one of the access switches in the topology. For a ring topology repeat this operation to attach the other end (access switch) to an (possibly another) aggregation switch to close the ring.
  - AggregationTrunk: If the aggregation switch needs to be connected to a PE, or to another aggregation switch, choose the Type field as AggregationTrunk
  - AccessTrunk: If the aggregation switch needs to be connected to the access switch, choose the Type field as AccessTrunk.

    Attach the Access Network - Finally, the access networks have to be connected to the MPLS edge devices. Typically a PE device per Aggregation switch will be used. Right-click on the PE device in the Region that is to be used for terminating the aggregation trunk from the aggregation switch. Select the 'Create Link' action. In the form, choose the Type as 'AggregationTrunk', so that you may select the two end-points of the aggregation trunk connecting the aggregation switch to the chosen PE router.

NOTE: See section 10-2 for details on NNMi dataload.

6-3 Network Upload

The VPN_SVP includes network equipment upload functionality. As described above in section 1-1 NEs may be entered into the Equipment Inventory and when connectivity to these NEs are assured, and the NEs are configured their LifeCycleState may manually be set to 'PreConfigured. In this state, all the interfaces available on a PE router may be uploaded from the device and into the Equipment Inventory which gets automatically populated with these objects.

As part of the pre-configuration of the NEs, the description field on a router interface may be used to control the UsageState of the interface created in the Inventory: Core facing interfaces may be assigned a description field of 'UPLINK' (appearing as the first word in the description). Other interfaces not to be used for service attachments or which otherwise are to be reserved for other purposes and therefore to be excluded from provisioning may be assigned a description field of 'RESERVED' (appearing as the first word). These interfaces will automatically be assigned a UsageState of 'Uplink' or 'Reserved', respectively by the Upload function.

The interfaces that are used as ASBR Links between the two ASBR routers can be assigned a interface description of 'ASBRLINK'. These interfaces will automatically be assigned a UsageState 'Reserved' by the Upload function.

Interface having UsageState 'Reserved' or 'Uplink' will automatically be exclude from selection lists from where the Operator selects an interface for provisioning. There are no other implications of these states and both are handled the same way. The difference between 'Reserved' and 'Uplink' is only in its interpretation by the Operator.

The configuration example in **Figure 6-11** shows a Cisco router interface having RESERVED set in its description field.

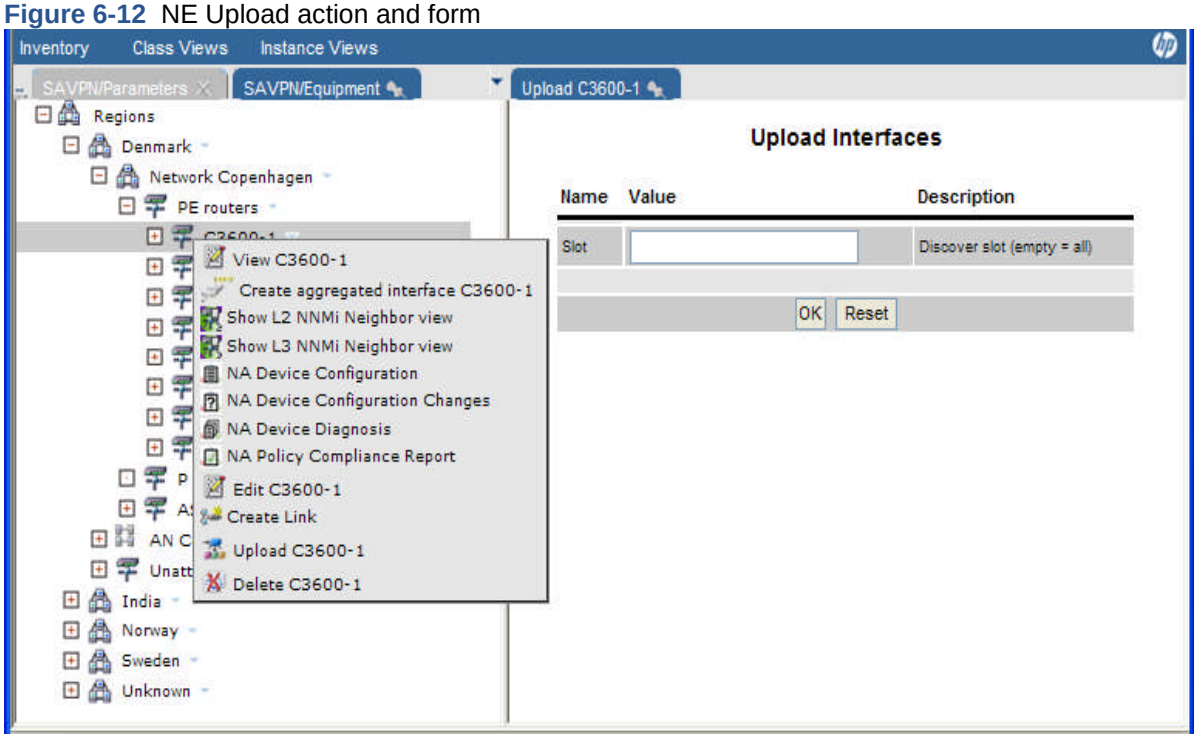
Figure 6-11 Illustration of description field with RESERVED keyword on a Cisco router

```
interface Serial0/1
  description RESERVED interface on a Cisco router
  ip unnumbered Loopback0
  encapsulation ppp
  no ip mroute-cache
  clockrate 2000000
!
```

The procedure for Upload of interfaces is:

In the Inventory→Equipment section on the PE router that is to be uploaded, select the Upload action and the form displayed in **Figure 6-12** will appear.

Figure 6-12 NE Upload action and form



In the form, an optional Slot may be specified to restrict the scope of the upload, or it may be left unspecified in which case all interfaces is uploaded.

Interfaces, controllers of type E1 and STM1/STM4 (SONET), and SNMP IfIndex are uploaded.

Interfaces, which have already been manually configured and are in use on the router for some reason, are uploaded as 'Reserved' to protect these from being overwritten by VPN_SVP. The detection of an interface being in use covers scenarios like having an assigned IP address, an assigned Vlan id and others.

NOTE: The detection mechanism may not detect all possible kinds of configuration.

NOTE: If a specific interface is being uploaded as 'Reserved' and it is verified that it actually should be 'Available', the configuration on the router must be cleaned up manually. Then remove the interface from the Inventory before a new upload may re-create it as 'Available'.

NOTE: The upload function does not update (modify) objects already existing in the inventory with the exception of IfIndex values.

NOTE: See section 10-2 for details on NNMi dataload.

---

7 Configuration of QoS

The configuration of QoS related items is generally a complicated matter and many concerns and issues are involved in this. This section provides an attempt to describe the capabilities available in the VPN_SVP, the constraints and special issues that must be considered.

7-1 Overview

The VPN_SVP supports up to 8 Classes of Service (CoS) for L3 VPN and L2 VPN services. A CoS is an identifiable type of traffic flowing between the Customer's Edge device (CE) and the Provider's Edge device (PE). The VPWS service only supports a single CoS.

To identify a specific CoS, a Traffic Classifier (TC) must be defined that contains the defining criteria or characteristics of the CoS.

When the CoS is identified, specific treatment to that CoS may then be required and that is specified via the QoS Profiles.

The classification of data is typical done at the ingress PE but VPN_SVP optionally supports CE based classification of L3 services.

The basic treatment that the VPN_SVP supports is rate/limiting of the ingress traffic, and marking of the CoS with its required MPLS EXP bits when forwarding the data into the MPLS core. It is assumed that the provider's MPLS core network is configured with respect to the treatment of traffic according to its EXP marking.

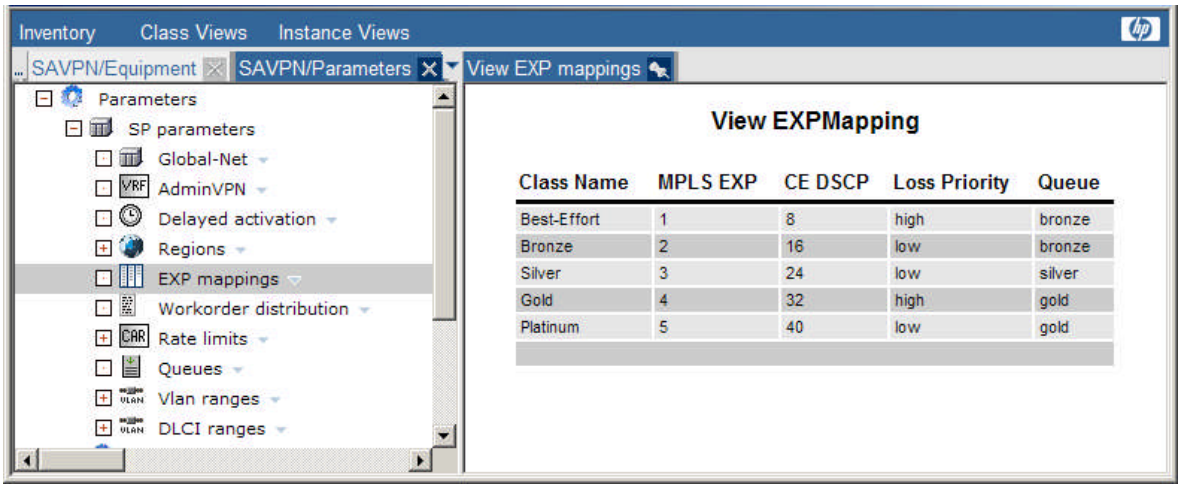
7-2 EXP Mappings

The basic definition of the required CoS takes place via the global configuration item: **EXP mappings** (see section 6-1-1 SP Parameters above).

The number of CoS, their names and corresponding MPLS EXP bit markings are all issues decided by the provider at his network planning stage. **Figure** 7-1 below illustrates an example configuration of the EXP mappings table with 5 CoS defined.

The VPN_SVP supports CE based classification and re-marking of the traffic towards the PE router of L3 data and uses the IP headers DSCP field to contain these marks. This allows the PE router to implement an effective (and often hardware based) re-classification of the ingress data. The CE DSCP values desired to be used on the CE-PE attachment is defined by the provider at his network planning stage and also specified in the EXP mappings table.

Figure 7-1 Example EXP Mappings configuration with 5 CoS defined



The two reaming values, Loss Priority and Queue are not applicable to all router vendors. Some vendors (e.g. Juniper), allow the association of different loss priorities to data and increases in this way the number of CoS. Traffic with a higher loss priority is more likely to be dropped in case of network congestion than data being of a lower loss priority.

Management and configuration of the forwarding queues of a PE router is not supported by VPN_SVP. This is a very diverse subject that has not yet been found suitable for automation. But basically it is via the forwarding queues that the devices implement their QoS capabilities. For some vendors (e.g. Juniper), the forwarding queues may be named which provides a more obvious association between a CoS and the forwarding queue to be used.

The forwarding queue names are decided by the provider at his network planning stage and are assumed preconfigured on the relevant network devices.

Hence, the **EXP mappings** table is a very important object that should be configured/edited before any other QoS related configuration or activation is performed.

NOTE: Existing EXP mappings entries, used by some QoS profile, can not be deleted.

NOTE: An EXP mapping entry can be deleted by choosing the EXP mappings → Edit EXP mappings option. On the Update form, remove the “Class Name” entry for the row to be deleted, and click on OK.

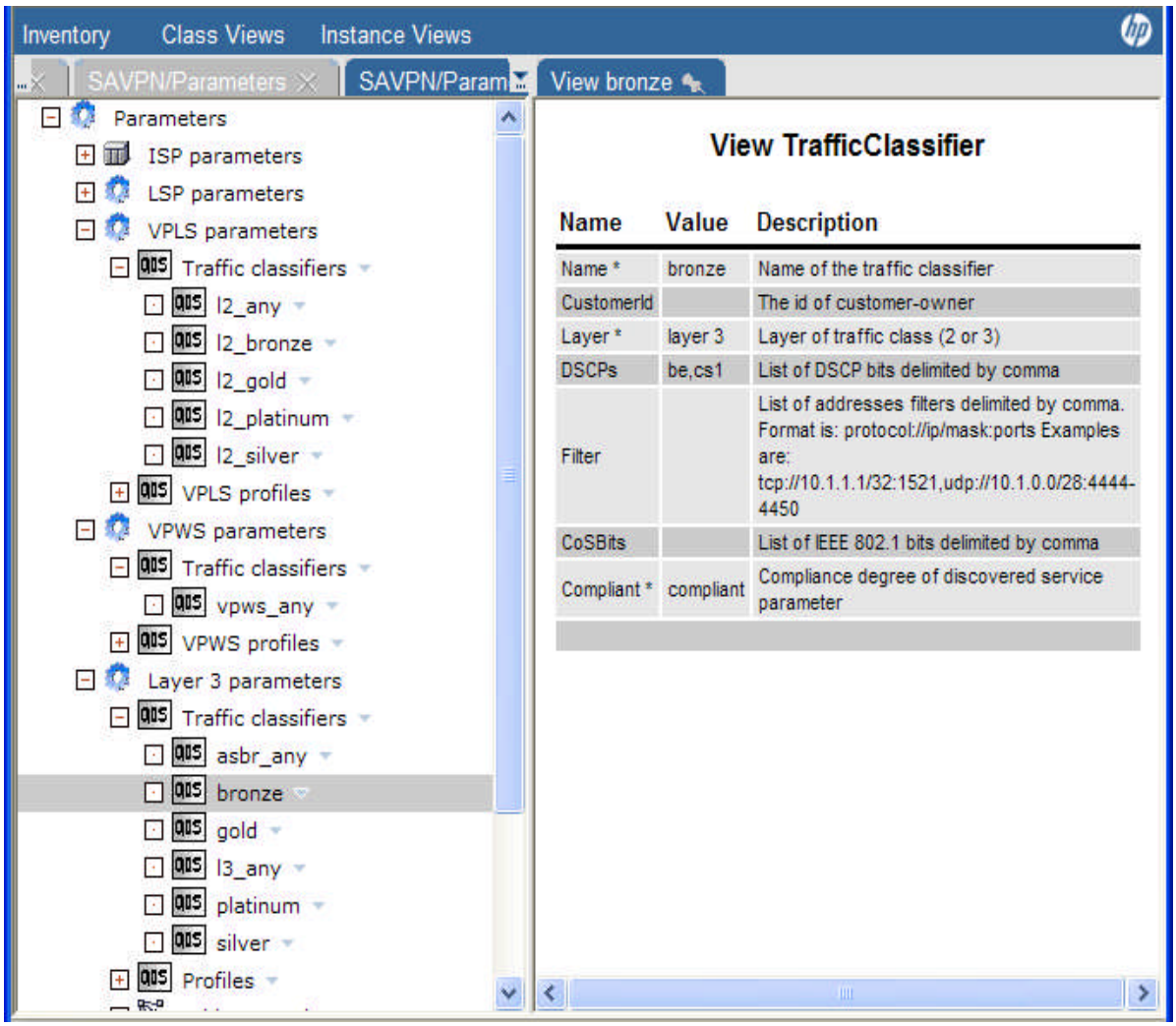
7-3 Traffic Classification

As mentioned above, to associate data traffic with a CoS, a classifier has to be defined that contains the defining criteria or characteristics of the CoS.

Traffic classifiers are specific to the service type and must be defined as a Layer 3, VPLS or VPWS classifiers. L3 traffic contains an IP header and therefore the DSCP filed and other IP header fields may by used to classify L3 traffic. L2 VPLS traffic contains an Ethernet header but not necessarily a L3 header and therefore the IEEE 3 bit field 802.1p that contains priority bits (or CoS bits) may be used to classify L2 traffic.

As only a single CoS is supported for VPWS, only a build-in vpws_any classifier is available.

Figure 7-2 Example of VPLS, VPWS and Layer 3 Traffic Classifiers



Traffic classifiers may be defined using the ‘Create TrafficClassifier’ action defined on the Traffic classifiers branch.

For L3 services both DSCP and filter based classification is available. The DSCP field (previously known as the TOS filed) is a field and encoding defined in the IP header that carries CoS information according to the differential services architecture defined by IETF. The filter based classification supports the definition of filters or access lists that contains protocol type (TCP and/or UDP), IP addresses and/or application types (port numbers).

NOTE: The term ‘be’ is used for the DSCP ‘best effort’ code point. Some vendor devices do not support this term, and it may have to be translated in the configuration templates by a dedicated customization task.

In **Figure 7-3** below is an example of a Cisco access list created to support filter based classification corresponding to the example provided in the description field of the filter attribute.

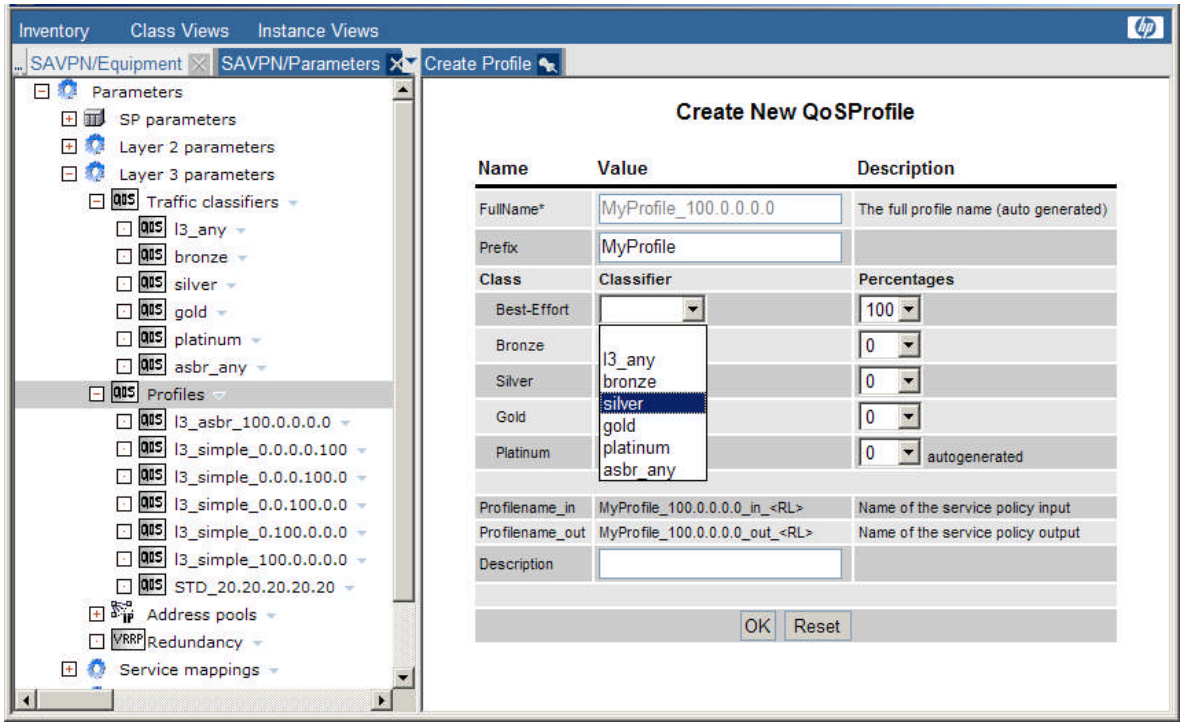
Figure 7-3 Example of a filter based classifier

```
ip access-list extended <name>
  permit tcp 10.1.1.1 0.0.0.0  any eq 1521
  permit tcp any 10.1.1.1 0.0.0.0  eq 1521
  permit udp 10.1.0.0 240.0.0.0  any range 4444 4450
  permit udp any 10.1.0.0 240.0.0.0  range 4444 4450
```

7-4 QoS Profiles

The final step in configuring QoS is the creation of the QoS profiles. The QoS profile ties together the CoSs, the traffic classifiers and the requested total rate limit available to a site attachment.

Figure 7-4 Example of QoS profile creation



The QoS profile may be named by specifying a prefix, but its full name as it will be configured on the devices will be constructed out from the prefix and the requested CoS and their associated percentages of the rate limit.

For each CoS defined in the EXP mappings table, a corresponding line is available in the QoS Profile form. For each class, its defining classifier and the percentage allocation of the total rate limit may be specified.

A received service request for e.g. creation of a site service includes the rate limit. The rate limit represents the total amount of data that a customer site may inject into the providers network (data rate). This is the main QoS parameters managed by the VPN_SVP and provides both a definition/limitation of the customer's available bandwidth and a limitation/protection of the provider's core network against overload problems, DoS attacks, etc.

The VPN_SVP implements policing on ingress side (direction from customer to provider). This means, that certain bursts may be acceptable within configurable limits, but the average data rate will not exceed the specified rate limit.

On the egress side the VPN_SVP implements shaping (when devices otherwise support this). This means that data arriving from other sites and which has to be forwarded to this site will be sent with a maximum rate corresponding to the requested rate limit. Bursts will be queued and buffered (within the PE's available buffer capacity) and sent when possible.

When defining a QoS profile, the total rate limit to be requested is not know yet, but it may be subdivided into the percentages that should be made available to the different CoS specified (see **Figure 7-4**). A specific profile for ingress (in) and for egress (out) traffic is created, but currently the same rate limit will be associated both direction.

NOTE: QoS profiles, used by some service, can not be deleted from Inventory.

NOTE: Traffic Classifiers, used by some QoS profile, can not be deleted from Inventory.

NOTE: Existing QoS profiles or classifiers will not be affected by later EXP mappings changes. Only new profiles take EXP mappings changes into account.

NOTE: Existing EXP mappings entries, used by some QoS profile, can not be deleted.

7-5 Template Hooks

Some assumptions are made in the configuration templates about QoS configuration.

Mapping between queue name and queue number is done in the templates and will be used to create any forwarding class for Juniper devices. In the below **Figure 7-5** an example of the default mapping implemented in the delivered templates is displayed. You may see that queue names bronze, silver and gold queue names are mapped to queue numbers 1, 2 and 3 respectively.

Figure 7-5 Default queue name to queue number mapping

```
<xsl:template name="QoS_MapQueueName">
    <xsl:param name="queue_name"/>
    <xsl:choose>
        <xsl:when test="$queue_name = 'bronze'">1</xsl:when>
        <xsl:when test="$queue_name = 'silver'">2</xsl:when>
        <xsl:when test="$queue_name = 'gold'">3</xsl:when>
    </xsl:choose>
</xsl:template>
```

NOTE: This mapping from queue name to number must be changed in the QoS templates to fit the requirements of the provider and the queue names specified in the EXP mappings table before service activation is started.

NOTE: A flag “_configure_fc”, is introduced in the Juniper QoS related XSL templates. The flag will state if VPN_SVP must create forwarding classes and queues when the first site service is added to the router. VPN_SVP will create forwarding classes only if the flag is set to true. If the flag is set to false it is assumed that the required forwarding classes are all preconfigured on the device and VPN_SVP will skip this configuration.

7-6 Multi-AS backbone QoS

When the provider deploys a Multi-AS backbone network, the physical ASBR links between the ASs have to be pre-created and configured before service activation may commence (see section 1-1 above).

A virtual ASBR link (ASBRAttachment) is created when a new site service requires it (e.g. when a L3 site service is created for the first time in an additional AS). This link is specific for the service (i.e. for the L3 VPN). The rate-limit requested for this site service will be the initial rate limit associated the ASBRAttachment.

The QoS features currently supported on the ASBRAttachments are quite limited. Only a single CoS is supported and only a single classifier (asbr_any) may be associated. The asbr_any simply identifies all traffic as belonging to this single class.

The required QoS profiles must use the asbr_any classifier and must be created before ASBRAttachment are requested to be configured using VPN_SVP.

Later additions of site services in the interconnected ASs may cause an ASBRAttachment to carry increased traffic from several sites among the interconnected ASs and the QoS parameters on these links become important to manage.

Currently the initial configure rate-limit on an ASBRAttachment is not modified when more site services are added. This rate-limit may be modified manual via the Inventory GUI using the ‘Modify Ratelimit ASBRAttachment’ action available on the ASBRAttachment branch.

7-7 LSP Configuration

A Service Integrated LSP provisioning feature which represents a strategic Traffic Engineering approach is supported. This enables enhanced treatment of MPLS cross-core data according to the customer/ingress data classification.

This component builds a full mesh of LSPs between the PE routers hosting sites specific for a particular VPN and specific for a particular Class Type. See **Figure 7-9** below.

The creation/deletion/modification of LSPs is integrated with the normal service activation process according to the requirements and topology of the site services. i.e. when a service request is received and completed successfully, it is followed with a corresponding LSP activation process which has to complete before the status is responded back to the requestor.

The QoS related LSP parameters consist of the class of traffic that is to be exchanged by the LSP, the so called Class Type and the bandwidth associated the LSP for a specific Class Type. Up to 8 CoS supported by the QoS profiles are mapped to a maximum of 4 LSP Class Types according to the CoS list defined on the LSP profile as described above in section 6-1-2 above.

The bandwidth associated an LSP depends on the rate-limit associated the individual CoS in the QoS profile (based on the specified percentage of the total rate-limit) and which maps to the Class Type. This association of bandwidth is made automatically at LSP creation time according to the following simple procedure:

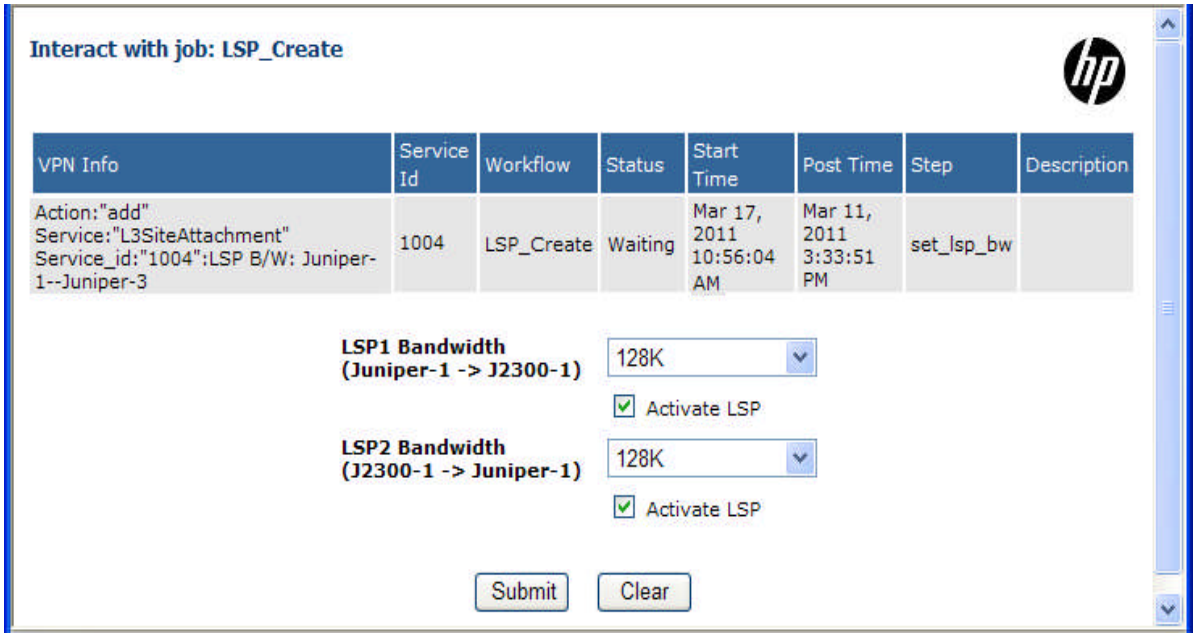
- When a LSP profile is created, by default the bwAllocation mode is set to manual. Any LSP that gets created using the LSP profile that has bwAllocation 'manual' waits for the operator to set the LSP bandwidth. An option is also provided to NOT create the LSPs between the two PEs. The job waits in the set_lsp_bw queue.

The VPN Info in the job queue indicates that the LSP creation between Juniper-1 and Juniper-3 is waiting for the operator interaction to provide the LS bandwidth, as shown in the figure below.

Figure 7-6 Set LSP bandwidth manually

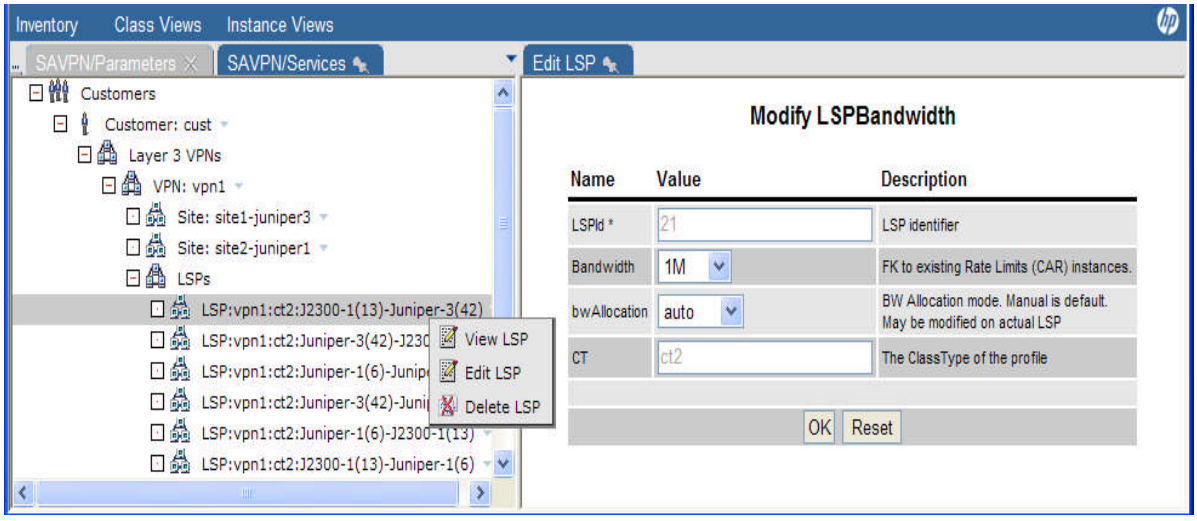
Figure 7-7 indicates that the LSPs need to be created between the two PEs. The LSP bandwidth between Juniper-1→J2300-1 and J2300-1→Juniper-1 can be manually set. Also, if the Operator chooses not to create LSPs between these PE's, the checkbox 'Activate LSP' can be unchecked. These LSPs will never be created again

Figure 7-7 Interact with Job: Set LSP bandwidth manually



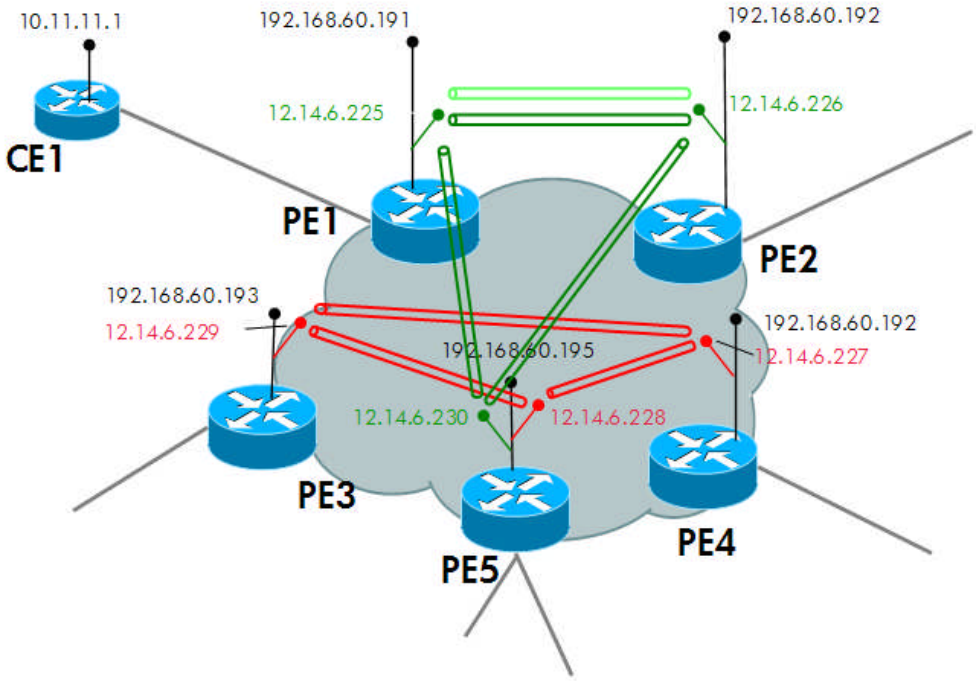
- Initially when a LSP is created, if the LSPProfile has the bwAllocation set to ‘auto’, it is automatically assigned a bandwidth value equal to the (class type specific fraction) sum of the ingress rate-limits over the VPN sites on the head-end PE. If the bwAllocation in LSPProfile is set to ‘manual’, the LSP is assigned a bandwidth value equal to the value set by the Operator in the ‘set_lsp_bw’ form, as shown in **Figure 7-7** above.
- Later changes to services, like adding more sites, modifying QoS/Ratelimit and Multicast enabling operations, automatically modifies the bandwidth according to the same algorithm - if bwAllocation mode is set to ‘auto’. If the bwAllocation mode is set to ‘manual’, LSP bandwidth assignment is then under full control and responsibility of the Operator and no further automated modifications will be made.
- LSP bandwidth and bwAllocation mode modifications are supported via the Inventory GUI by direct Operator interaction.

Figure 7-8 Modify LSP bandwidth GUI example from Inventory Service Tree.



- LSPs may be deleted manually by the Operator through the ‘Delete LSP’ option. Deleted LSPs will not be re-created in case of further service operations that otherwise would have updated these LSPs.

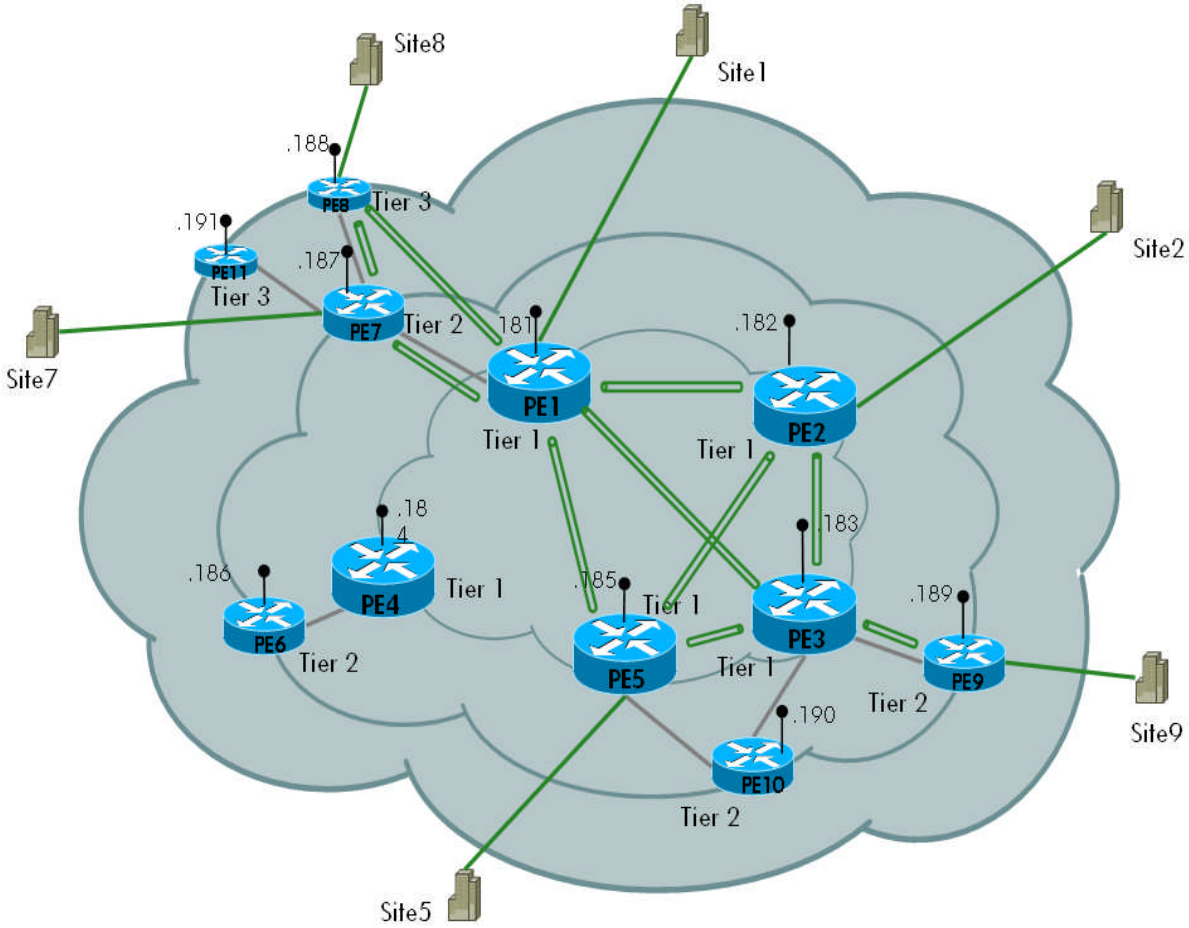
Figure 7-9 LSP topology example for 2 VPNs, Red and Green. A pipe in the figure represents 2 uni-directional LSPs or a tunnel. Green VPN has two tunnels created between PE1 and PE2, one for each of 2 Class Type.



A LSP tier (or hierarchical LSP) feature allows significant reduction in the number of MPLS LSPs that otherwise would have to be created across the MPLS core to create a full mesh of LSPs. The tier defines a hierarchy among the PE routers with Tier1 being the PE routers closest to the MPLS core and higher Tiers being successively farther away from the MPLS core.The higher tier LSPs share the Tier1 LSPs.

The tiers/hierarchy can be defined among the PE routers – See Section 6-2 for details on tier fields.

Figure 7-10 Illustration of a PE multi Tier structure or hierarchy.



The Tiers determine the PEs between which the LSPs are created, e,g. when a new site is added to a VPN on some PE router.

When sites are added to Tier1 routers, a full mesh of LSPs among the other Tier1 routers hosting sites must be created.

When adding a VPN site to a Tier2 router, a new LSP pair between the Tier2 router and its downstream root Tier1 router, must be created. LSP pairs towards other Tier routers in the same Tier tree that hosts sites are also added. Similar principle is also applied on a Tier3 router.

8 Configuration of Roles

The HPSA core product support user roles. A user may be associated one or more roles. The particular roles may be checked in the GUI views and with respect to which WF operations are permitted and that enables role dependent behavior and therefore the behavior of the VPN_SVP as experienced by a particular user.

8-1 Roles in HPSA

VPN_SVP implements out-of-the-box a Region based role concept, which enables the restriction of Workflow interaction and the display of Region branches in the Inventory GUI to users having the specific Region role associated. See [*INTRO*] for more information about Roles, Privileges, and Authentication. An example is the best way to describe this functionality:

Assume that the following Regions: 'Denmark', 'Sweden' and 'Norway' have been defined in the SAVPN/Parameters tree as described above in 6-1-1 , and that we have added users 'dk', 'se' and 'no', which should be restricted to operate only within their associated Regions.

We also assume that the DB Authentication module has been enabled as illustrated in **Figure** 8-1.

Figure 8-1 Example authenticator definition in HPSA `mwfm.xml`

```
<Module>
  <Name>authenticator</Name>
  <Class-Name>com.hp.ov.activator.mwfm.engine.module.umm.DatabaseAdvancedAuthModule</Class-Name>
  <Param name="mwfm_remote_url" value="//localhost:2000/wfm"></Param>
  <Param name="expiry_days" value="90"></Param>
  <Param name="expiry_alert_days" value="10"></Param>
  <Param name="reuse_interval" value="3"></Param>
  <Param name="password_validation" value="true"></Param>
</Module>
```

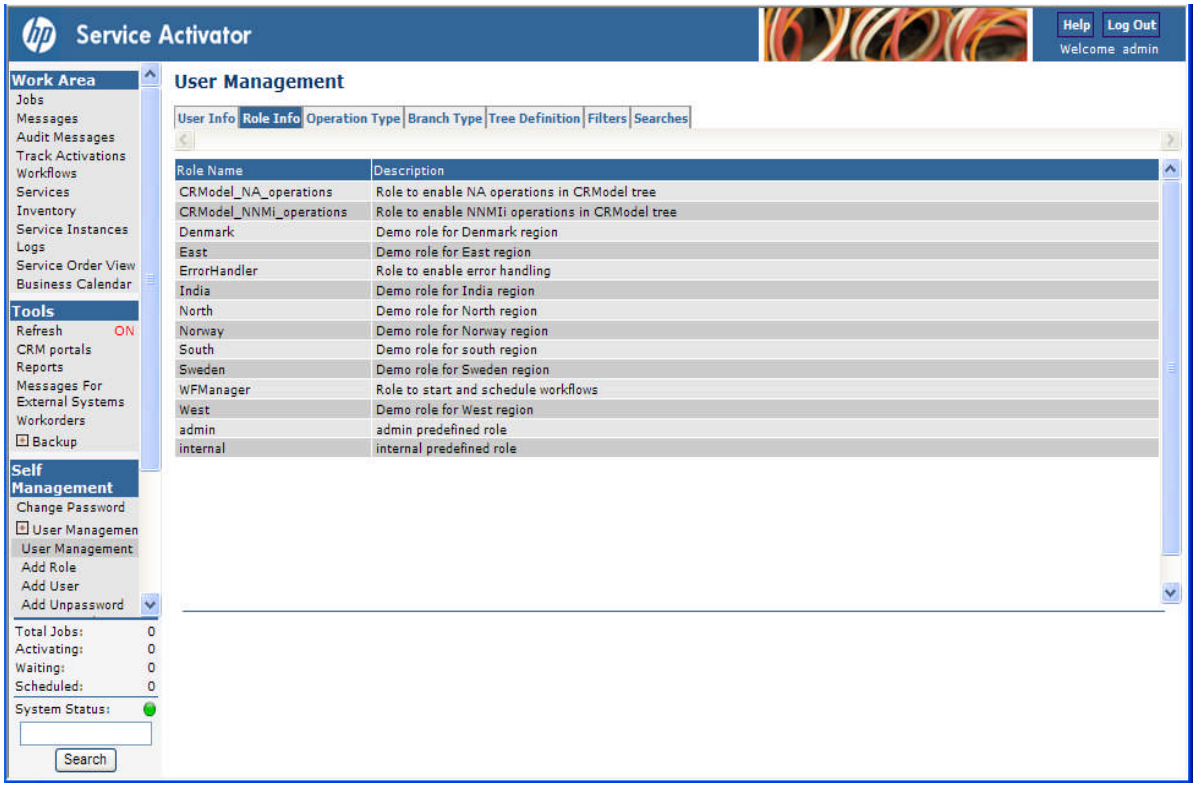
First, the roles have to be defined. Use the HPSA Self management→User Management interface and select the 'Add Role' action. The following roles must be defined:

- Denmark
- Norway
- Sweden

Use the User Management 'Role Info' tab to display the created roles. It should appear as in below.

NOTE: Only the roles Denmark, Norway and Sweden are part of the example. The other roles (WFManager, ErrorHandler, admin, internal) must be initially defined.

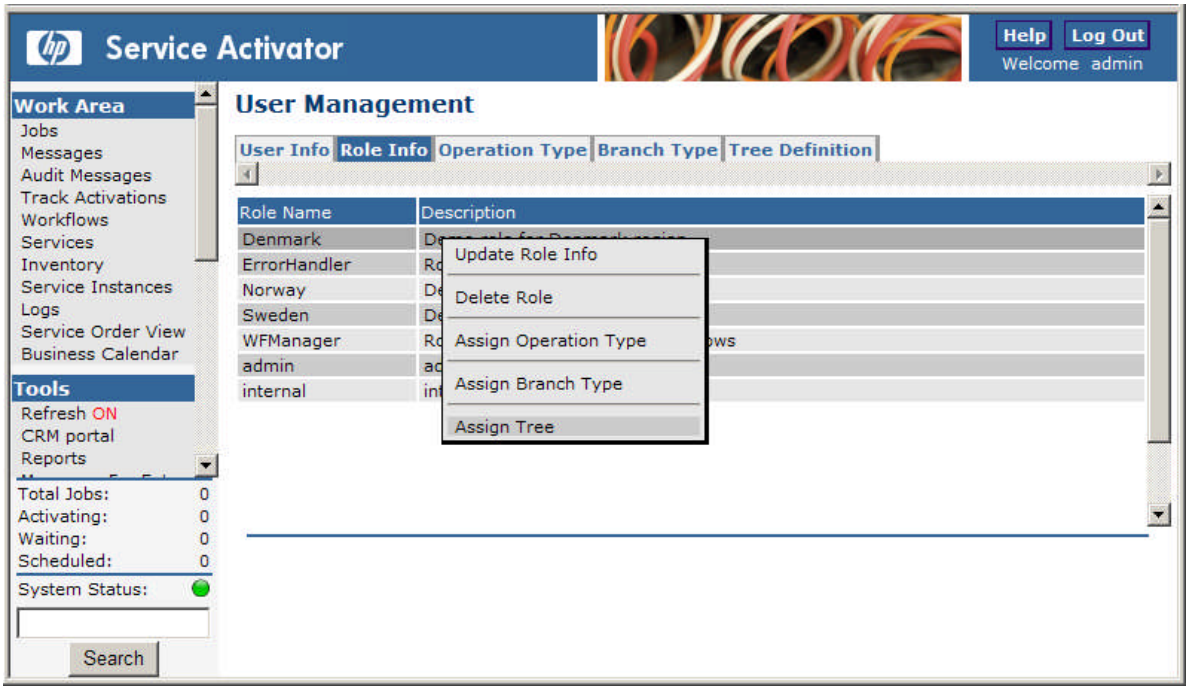
Figure 8-2 Roles defined for VPN_SVP example



NOTE: The roles CRModel_NA_operations and CRModel_NNMi_operations are necessary in order to edit the HPSA inventory attributes related to NA and NNMi respectively

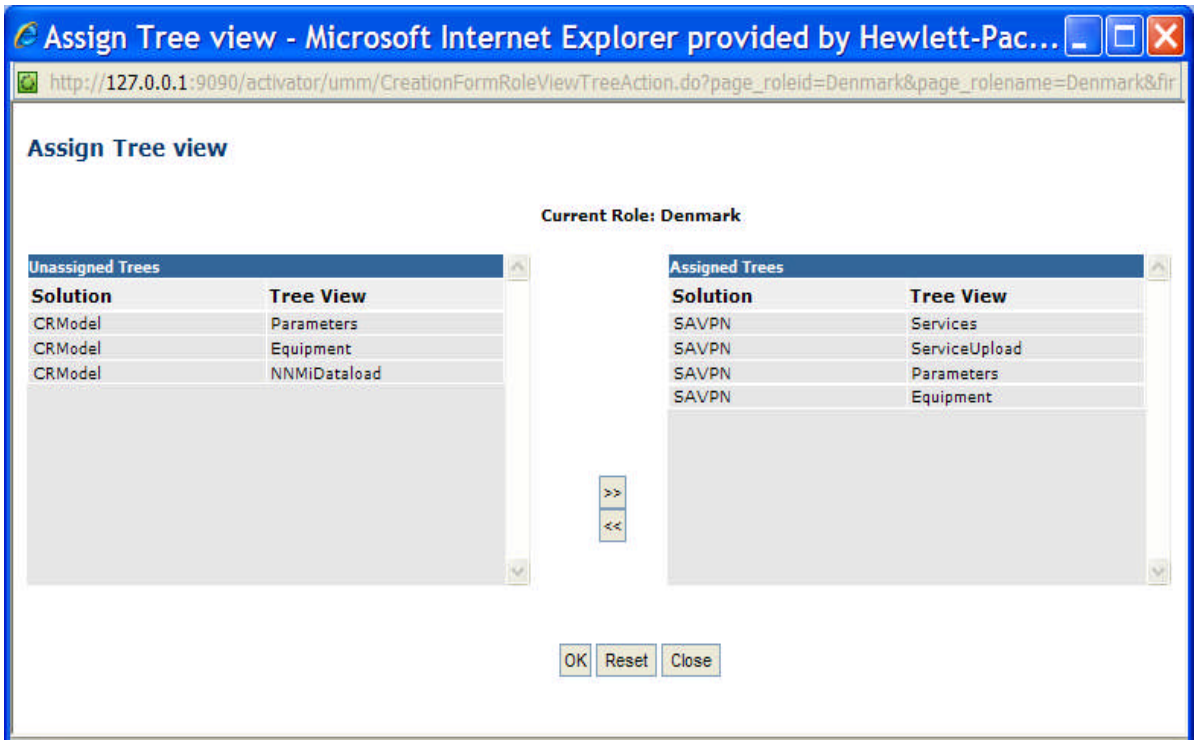
Secondly, the Inventory Tree views must be assigned the roles that are supposed to view these. Select the 'Role Info' tab and right-click the role to be assigned a Tree view. The GUI illustrated in **Figure 8-3** below shows the resulting pop-up menu.

Figure 8-3 Assigning Inventory Tree to Role



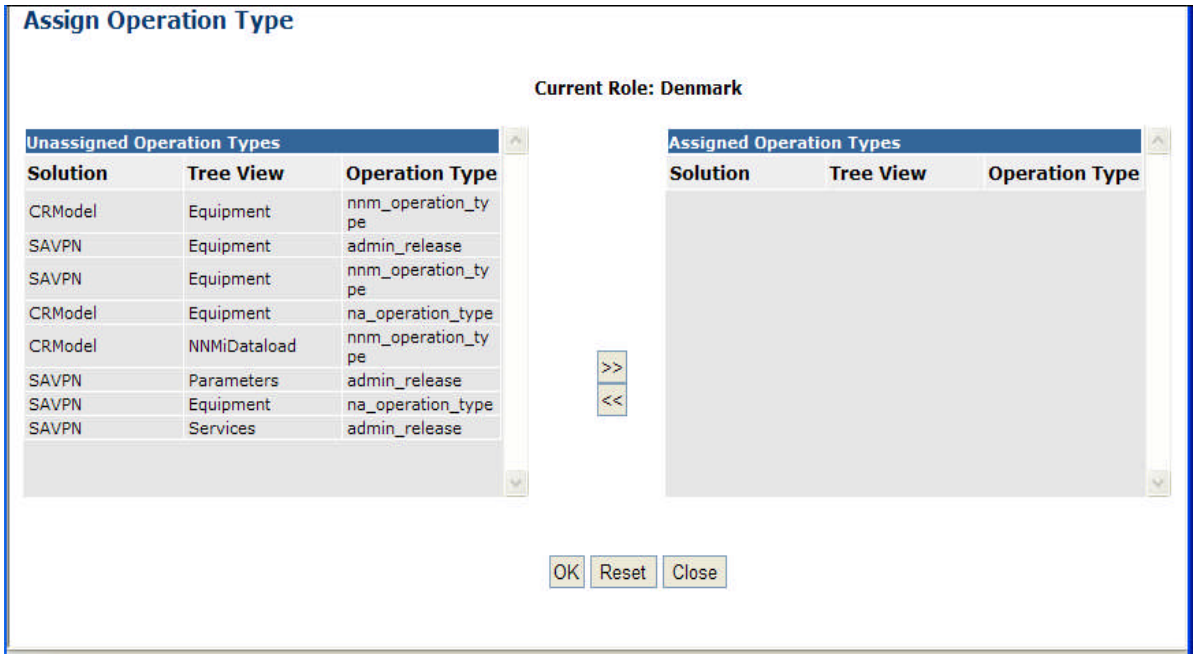
Select the 'Assign Tree' action and the resulting GUI allows you to assign Inventory Tree views to the selected role. You may assign all the available Tree Views to the selected role. The resulting view should be as illustrated in **Figure 8-4** below.

Figure 8-4 Tree views assigned to Role Denmark



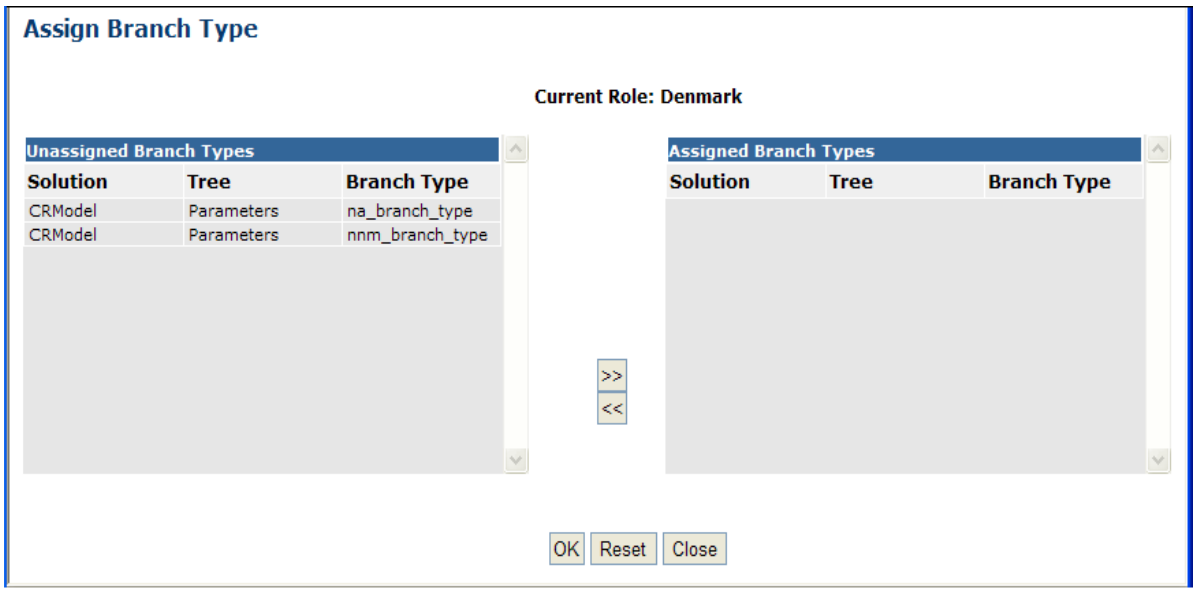
Next, the defined role can be assigned different operations. Right click on Denmark Role, select 'Assign Operation Type'. Assign the appropriate operations to the chosen role.

Figure 8-5 Operation Types assigned to Role Denmark



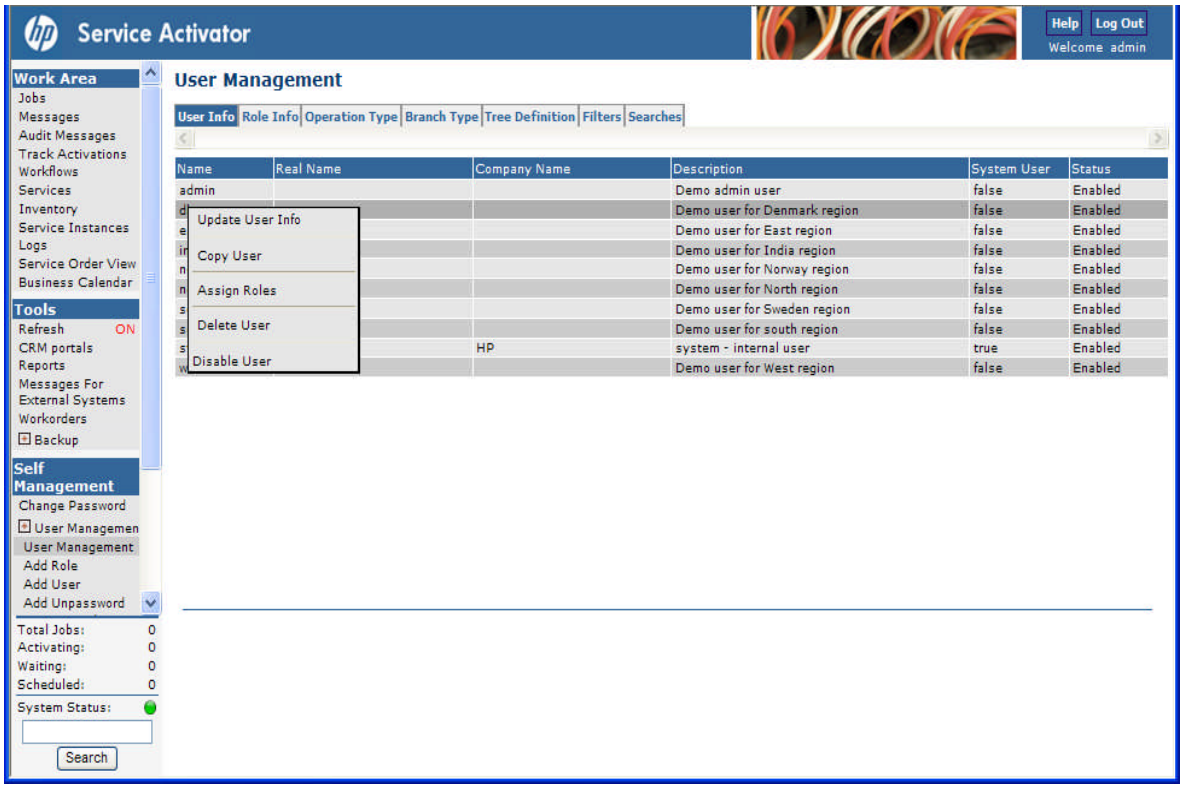
Next, the NA/NNM configuration parameters can be modified by certain roles. These privileges can be associated to a role by right-click on Role, and choose 'Assign Branch Type'.

Figure 8-6 Branch Types assigned to Role Denmark



Finally, the defined roles must then be assigned to the defined users. Use the User Management 'User Info' tab to list the users. Select e.g. dk and right-click. From the pop-up menu select 'Assign Roles' (see **Figure 8-7**).

Figure 8-7 Assign Roles to Users



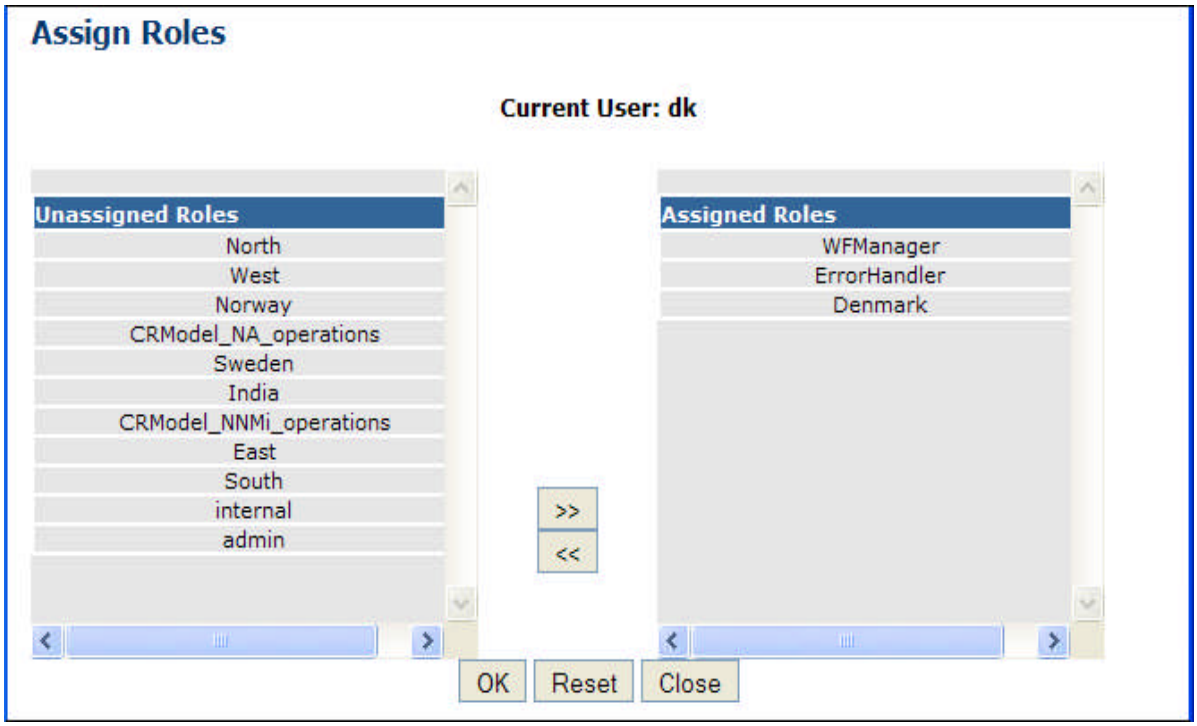
Assign the roles: Denmark, to user dk in the 'Assign Roles' GUI. The resulting view should be as shown in **Figure 8-8** below. Additionally, the user dk is also associated the WFManager role and the ErrorHandler role.

The WFManager role allows the user to select the Workflows menu in HPSA left pane and to interact with the displayed workflows.

NOTE: None of the Workflows supplied with the VPN_SVP requires direct interaction as this WFManager role allows as all are automatically instantiated. This form of interaction must actually be avoided!

The ErrorHandler role allows the user to interact with failed jobs and use the ErrorHandler GUI to diagnose and re-submit failed requests.

Figure 8-8 Example of Roles assign to a user



Likewise, role Sweden should be assigned to user se, and role Norway to user no.

Assign **all** defined roles including 'admin' (except role 'internal' !) to user admin, so user admin will have no restrictions in viewing nor interacting with neither Jobs nor Self Management GUI except activation queues. The role 'admin' is pre-defined in HPSA.

Assign **all** defined roles (including 'internal' and 'admin') to the system user (e.g. system). The role 'internal' is pre-defined in HPSA.

NOTE: You must select Reload → Configuration after defining the users and assigning their roles.

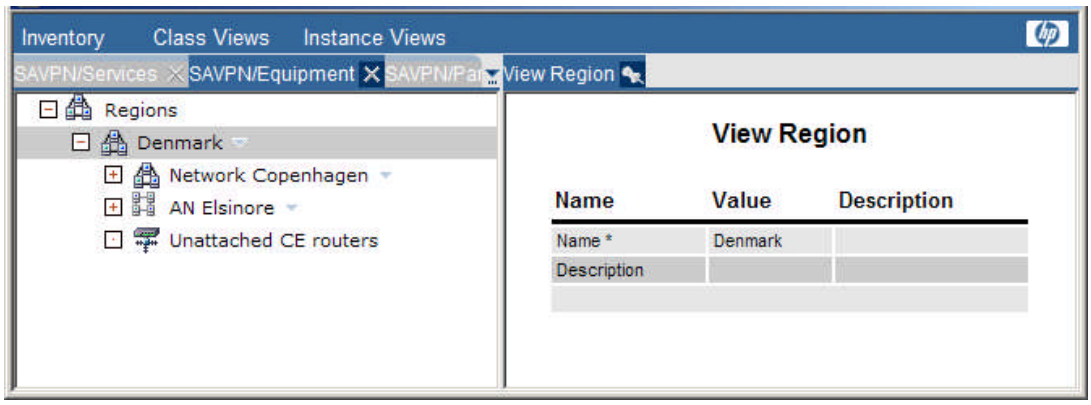
NOTE: For more information on User Management, refer to *INTRO*.

8-1-1 Roles and Inventory GUI

If you log in as user dk now, you will only be able to observe the Region branch 'Denmark'. If you log in as user no, you will likewise only be able to observe the Region branch 'Norway'. Role dependent branch selection in the presentation trees of the Inventory GUI is used by VPN_SVP to achieve this behavior.

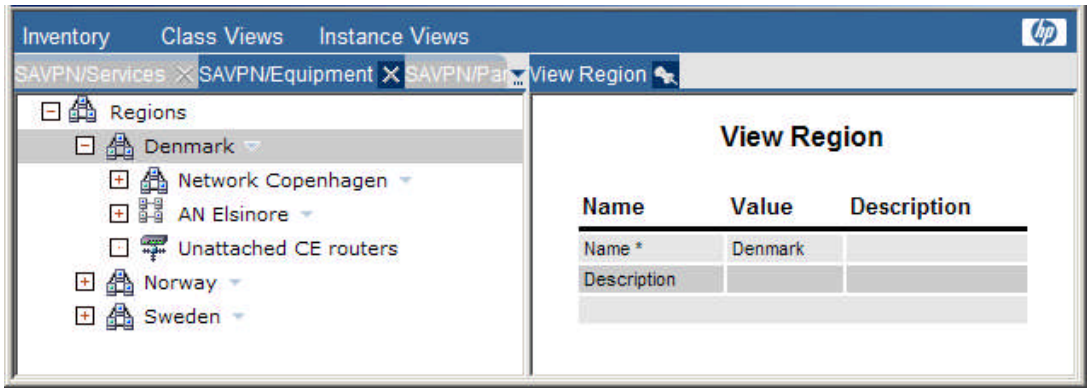
Hence, by associating roles to users corresponding to the defined region(s), the user's Inventory view of the SAVPN/Equipment → Region branches is restricted to include only those regions. E.g. user dk's view may be as illustrated in **Figure 8-9** below.

Figure 8-9 User dk's view of the Region branch. Only region Denmark is visible.



User admin would have a view as e.g. illustrated in below which includes all Region branches as admin has been assigned all corresponding roles.

Figure 8-10 User admin's view of the Region branch. All regions are visible



8-1-2 Roles and Workflows

The HPSA also implements role dependent workflow functionality (see [*INTRO*]). A workflow may specify role dependent behavior via the following attributes:

- Start-role
  This attribute allows the specification of the role required to start a workflow via the HPSA Workflows menu.
- Trace-role
  This attribute allows the specification of the role required to view the job (i.e. workflow) in the HPSA Jobs view.
- Kill-role
  This attribute allows the specification of the role required to kill (i.e. Stop) the workflow from the HPSA Jobs view.
- Default-role
  This attribute allows the specification of the role required to interact with a job, i.e. it is the Interact-role. But it is also role used as the default value for the above attributes in case these more specific role attributes has not been assigned any value, hence its name Default-role.

The requests submitted from the CRM Portal include the Region element in the request message. The Controller workflow which receives the requests sets the value of this Region element to the workflow's <Default-role>. This role is passed on to child workflows, so all the workflows instantiated for a specific service request will all have the same <Default-role> set. See the "Operator User Interface" in [*INTRO*] for more information on workflows and their role setting.

Operators will only be able to observe and interact with the workflows having a role set to one of the operator's roles. Hence, a job received for region Denmark will only be visible to operator dk (and to admin, as admin also have role Denmark assigned).

8-2 Roles in CRM

In the CRM Portal, a role concept is also present. Currently, it is allowing three modes of operation: Admin, Operator and Observer. The name of the role mapping file is configured in:

`$JBOSS_DEPLOY/crmportal.sar/crm.war/WEB-INF/web.xml`

as an init parameter:

Figure 8-11 web.xml snippet

```
<init-param>
  <param-name>roles_file</param-name>
  <param-value>roles.xml</param-value>
</init-param>
```

The location is relative to `$JBOSS_DEPLOY/crmportal.sar/crm.war/WEB-INF/`. An example configuration is illustrated in **Figure 8-12**.

Figure 8-12 Example Role definition of CRM Portal in `WEB-INF/roles.xml`

```
<Users>
  <User name="admin" roles="admin,operator"/>
  <User name="operator" roles="operator"/>
  <User name="dk" roles="operator"/>
  <User name="visitor" roles="observer"/>
  <Default-roles>observer</Default-roles>
</Users>
```

Every time a user logs into the CRM Portal, the user name is matched against the Users defined in the `roles.xml` file. If the user is found, the corresponding role(s) are saved into the session.

If a user is having the 'admin' or 'operator' role associated, then this user is permitted to create customers and services and to modify these.

If a user is not having the 'admin' nor 'operator' role associated, then this user is not permitted to create customers and services nor allowed to modify these. This user is only allowed to view the Customers and their associated services.

If no matching entry is found, the Default-roles are used. If Default-roles are not defined and no matching entry is found, the user is denied access to the CRM Portal.

The role 'observer' is used just for this example; it is not used anywhere in the CRM Portal.

NOTE: The authentication mechanism included in the CRM portal as delivered is very simple and must in most cases be replaced by a mechanism that provides a proper level of security. This replacement is unfortunately not currently configurable but must be re-compiled into the CRM portal.

---

9 Backup Tool

The VPN_SVP solution includes a Backup Tool that in earlier versions included a TFTPD process used as the transfer protocol between HPSA and a network device. In these versions only the TFTP transfer protocol was supported.

In versions from 5.0-3A the Backup Tool does not any more include any transfer protocol. It is now assumed the responsibility of the provider to install any preferred transfer protocol that the network devices may support. Hence, now basically any transfer protocols are supported.

In order to use transfer protocol different from TFTP, some modifications are required to be made to the backup related templates under the solutions/$SOLUTION/etc/template_files folder. These templates are:

```
<vendor>/<vendor>_Manual_Backup_Config.xsl
<vendor>/<vendor>_Save_Config.xsl
```

and as delivered these are prepared for TFTP as the transfer protocol. Hence, to use another protocol the templates must be updated accordingly.

The integration point between the transfer protocol and the VPN_SVP is the directory where the transfer protocol stores received files and reads files to be transmitted. VPN_SVP will transfer configuration backups to/from this point and the database; the transfer protocol will transfer the configuration backups between this point and the network devices.

This directory must be configured as described in section 6-1-1 by assigning it to the SP Parameters→ISP **BackupDirectory** attribute**.** This could e.g. on a windows platform be configured as:

BackupDirectory C:\tmp

On HPSA servers that have multiple configured IP interfaces, the IP address used by the transfer protocol to listen for transfer requests from the network devices must be assigned to the SP Parameters→ISP **IP** attribute. This could e.g. on a windows platform be configured as:

IP 120.130.140.151

NOTE: In a clustered HPSA environment, the IP address configured this way effectively becomes a floating IP address. HPSA 5.1 core product supports floating IP, but not in Windows.

In a clustered environment, the HPSA server address sent to router devices must be the physical address.

---

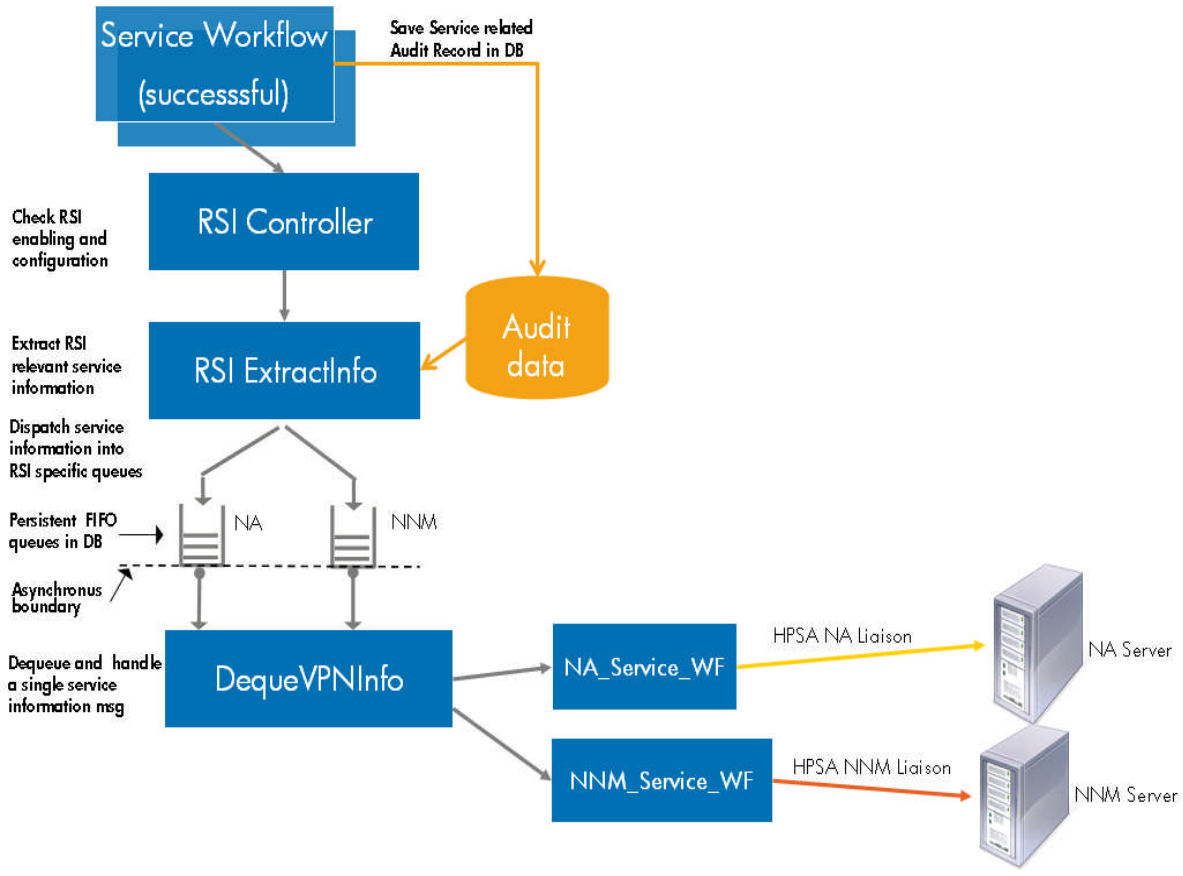
10 Integration with NNMi

Integration of HPSA VPN solution with NNMi brings the following benefits to the user 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 with easy access to NNMi's network resource status. This allows inspection of the status of the resources used by activated services and help in e.g. determining the cause of activation errors.

The following figure depicts the overall architecture of VPN_SVP-NA/NNMi integration,

Figure 10-1 VPN_SVP-NA/NNM Integration Architecture



10-1 NNMi Integration Configuration

The various steps involved in VPN_SVP– NNMi integration configuration are:

1. HPSA mwfm.xml NNMRequestModule configuration
2. HPSA CRModel→Parameters NNMi Configuration
3. SSH installation and configuration
4. NNMi Liaison plugin configuration
5. VPN_SVP CrossLaunch configuration
6. VPN_SVP→Parameters NNMi Queue Configuration

The following section details the configurations to be performed by the administrator.

10-1-1 HPSA mwfm.xml NNMRequestModule configuration

Dataload and NNMi modules should be configured in the mwfm.xml file as follows:

```
<Module>
    <Name>nnm_request</Name>
    <Class-Name>com.hp.ov.activator.mwfm.engine.module.nnmrequest.NNMRequestModule</Class-Name>

    <Param name="nnm_username" value="admin"/>
    <Param name="nnm_password" value="secret"/>
    <Param name="nnm_pass_is_encrypted" value="false"/>
    <Param name="nnm_hostname" value="HPSA-NNMiv9"/>
    <Param name="nnm_protocol" value="http"/>
    <Param name="nnm_port" value="80"/>
    <Param name="nnm_keystore" value="C:\HP\OpenView\ServiceActivator\etc\mwfmSSL.keystore"/>
    <Param name="nnm_keystore_pass" value="changeit"/>

    <Param name="queue_class" value="com.hp.ov.activator.mwfm.engine.module.WeightedEngineQueue"/>
    <Param name="queue_name" value="nnm_request_queue"/>
    <Param name="retry_count" value="4"/>
    <Param name="retry_interval" value="10"/>
    <Param name="min_threads" value="2"/>
    <Param name="max_threads" value="5"/>
</Module>
```

The parameters for this module are:

- nnm_username: NNM server username for authentication.
- nnm_password: NNM server password for authentication. It may be encrypted.

NOTE: Encrypted value for nnm_password must be specified if the value for the parameter nnm_pass_is_encrypted is set to true.

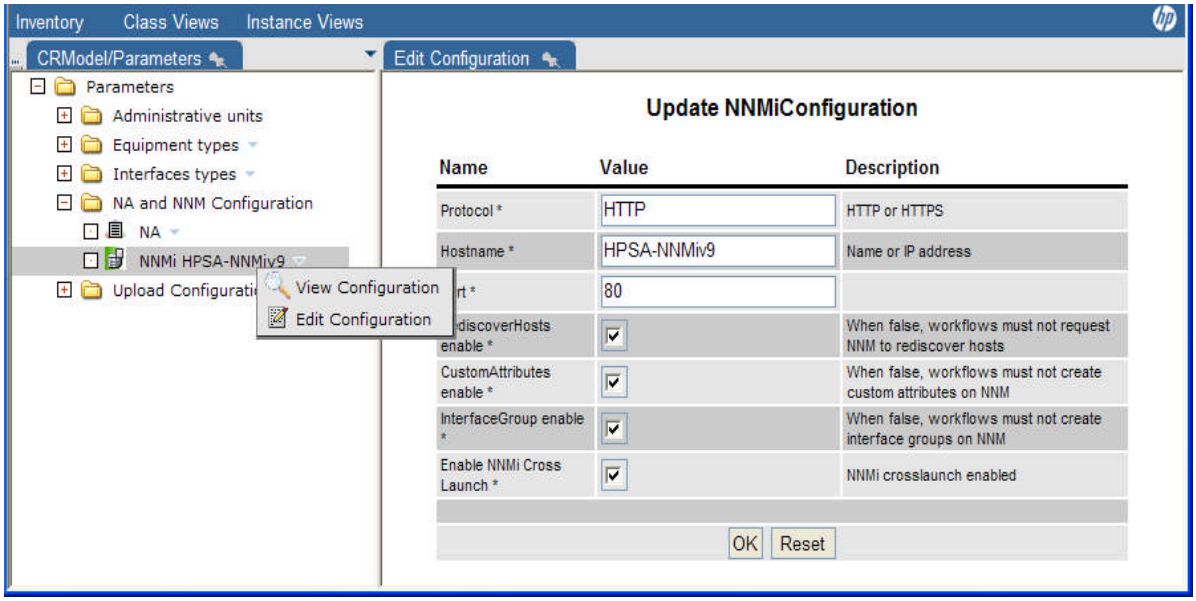
You can generate the encrypted password using the HPSA core utility $ACTIVATOR_BIN\generateEncryptedPassword.

- nnm_pass_is_encrypted (optional): Specifies if the provided nnm_password is encrypted. The default value is 'false'.
- nnm_hostname: NNM server hostname or IP address.

10-1-2 HPSA CRModel→Parameters NNMi configuration

In order to enable various SAVPN – NNMi integration configurations, the following menu items found under CRModel Parameters → NA and NNM Configuration → NNM should be configured:

Figure 10-2 NNMi CRModel Parameter configuration



The different parameters include protocol for communication with NNMi, NNMi hostname, NNMi Port, enable / disable rediscover hosts, custom attribute annotation, interfaceGroup creation and cross launch features.

10-1-3 SSH installation and configuration

The Interface Groups helps the NNMi 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.

In order to configure the creation of interface groups the following configuration needs to be done:

- SSH Setup: SSH communication needs to be setup between HPSA host and NNMi host.
- HPSA Configuration : HPSA needs to be configured to use that user, key pair and ssh client in the “/etc/config/resmgr.xml” file as shown below :

Following snippet represents the configuration sample on Windows system

```
<Deployer>
  <ClassName>com.hp.ov.activator.deployment.SSHScriptDeployerFactory</ClassName>
  <Param name="username" value="ovactusr"/>
  <Param name="identity" value="C:/cygwin/home/ovactusr/.ssh/identity"/>
  <Param name="sshbindir" value="C:/cygwin/bin"/>
</Deployer>
```

Where:

- username: The username of the user allowed to log in to the NNMi host through ssh.
- identity: absolute path to the ssh identity file
- sshbindir: absolute path to the cygwin bin directory

These parameters can also be set during HPSA installation..

NOTE: The SSH configurations must be performed on the NNMi server too.

Refer to [*HPSA_INSTALL*] “Installing and Configuring Secure Shell” for further details.

10-1-4 NNMi Liaison plugin configuration

- NNMi Plugin Configuration : Set the NNMiLiaison plug-in configuration parameters described below using HPSA Service Builder:
  - NNM_TMP_DIR: Full path to a temporary directory in NNMi host on which the SSH user has read/write access. This would be generally /tmp on UNIX systems and C:/cygwin/tmp on Windows systems.
  - NNM_PERL_DIR: Full path to the NNMi instance perl “bin” directory on the NNMi host. This would be generally /opt/OV/nonOV/perl/a/bin on UNIX systems and C:\Program Files (x86)\HP\HP BTO Software\nonOV\perl\a\bin on Windows systems.
  - NNM_BIN_DIR: Full path to the NNMi instance “bin” directory on the NNMi host. The perl script “nnmconfigimport.ovpl” must exist in the path. This is generally /opt/OV/bin on UNIX systems and C:\Program Files (x86)\HP\HP BTO Software\bin on Windows systems.
  - NNM_USER: The NNMi instance user which will be used to log in to NNMi application to perform InterfaceGroup View import.
  - NNM_PASS:The NNMi instance user password which will be used to log in to the NNMi application to perform InterfaceGroup View import.
  - HPSA_TMP_DIR: The HPSA temporary directory [path local to HPSA host]. This would be generally $ACTIVATOR_OPT\var\tmp..

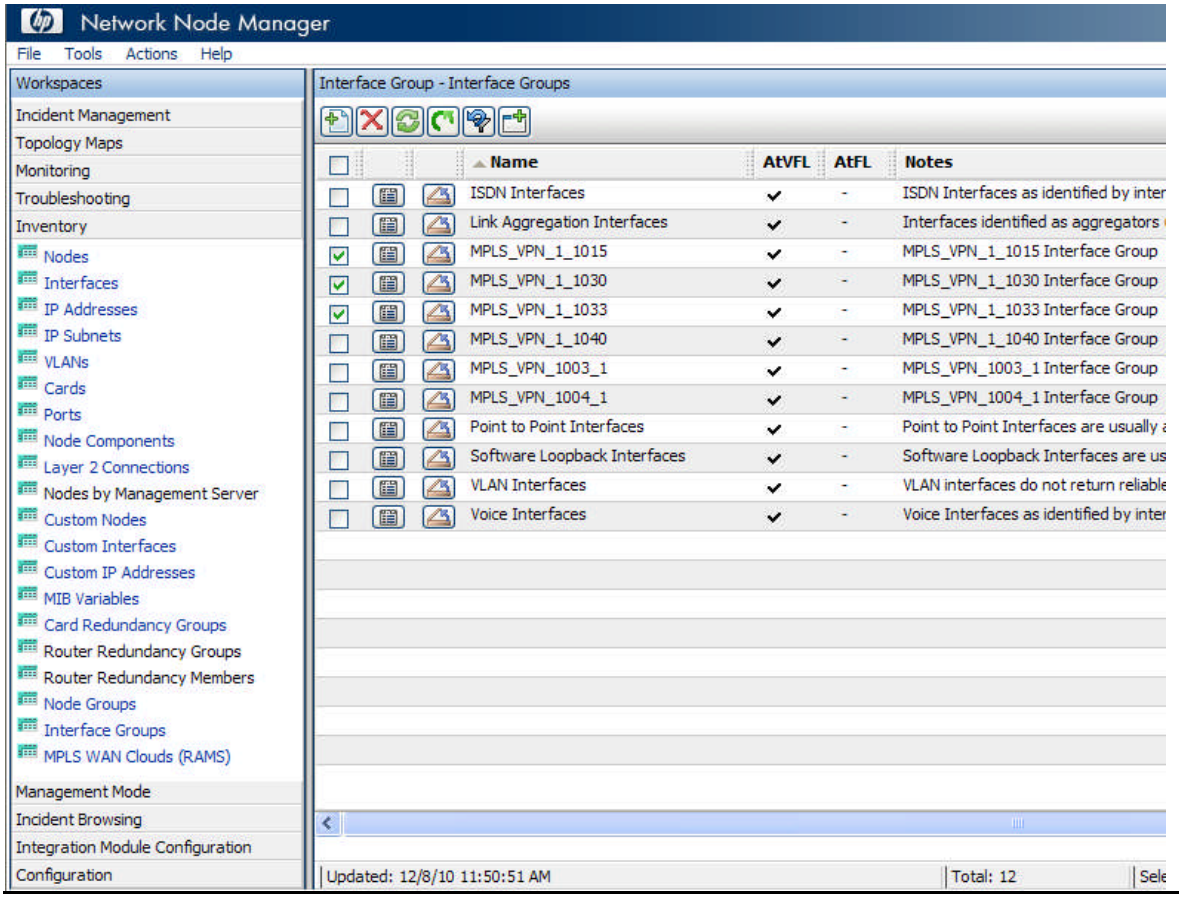
NOTE: The systems NNMi and HPSA can provide better usability with Single Sign On [SSO] configuration. For details on the configuration and usage of SSO, refer to Chapter 2 of [*HPSA_INSTALL*] and Chapter 4 of [*INTRO*].

Once the NNMi Liaison plug-in is configured, install the plug-in using the HPSA Service Builder.

NOTE: Refer to Appendix B “NNM Liaison” in [*PLUGIN*] for further details..

NOTE: The interface groups which are created on NNMi when a service is created – are not automatically deleted when the service is deleted. This has to be done manually on the NNMi system, as follows:

- Login to NNMi
- Click on the Workspace→Inventory→Interface Groups
- Click on the check boxes for Interface Groups that needs to be deleted, and delete them.



10-1-5 VPN_SVP CrossLaunch configuration

This would help the NNMi operator to launch service related L3 / L2 flow point views by choosing a specific Interface on NNMi. VPN_SVP supports the menu item "*Show HPSA VPN FlowPoint View*" under the actions menu. This menu is context sensitive and would be enabled only when the operator chooses an interface – and the interface is appropriately annotated with service attributes.

In order for the operator to enable this feature the file "***custom_hpsavpn_cl_conf***" present under the directory $SOLUTION/etc/config/nnm_liaison should be transferred to the configured NNMi system. Once done, the file should be imported to the NNMi database by executing the below command on NNMi server.:

nnmconfigimport.ovpl –u <nnmi_user> -p <nnmi_passwd> -f custom_hpsavpn_cl_conf.xml

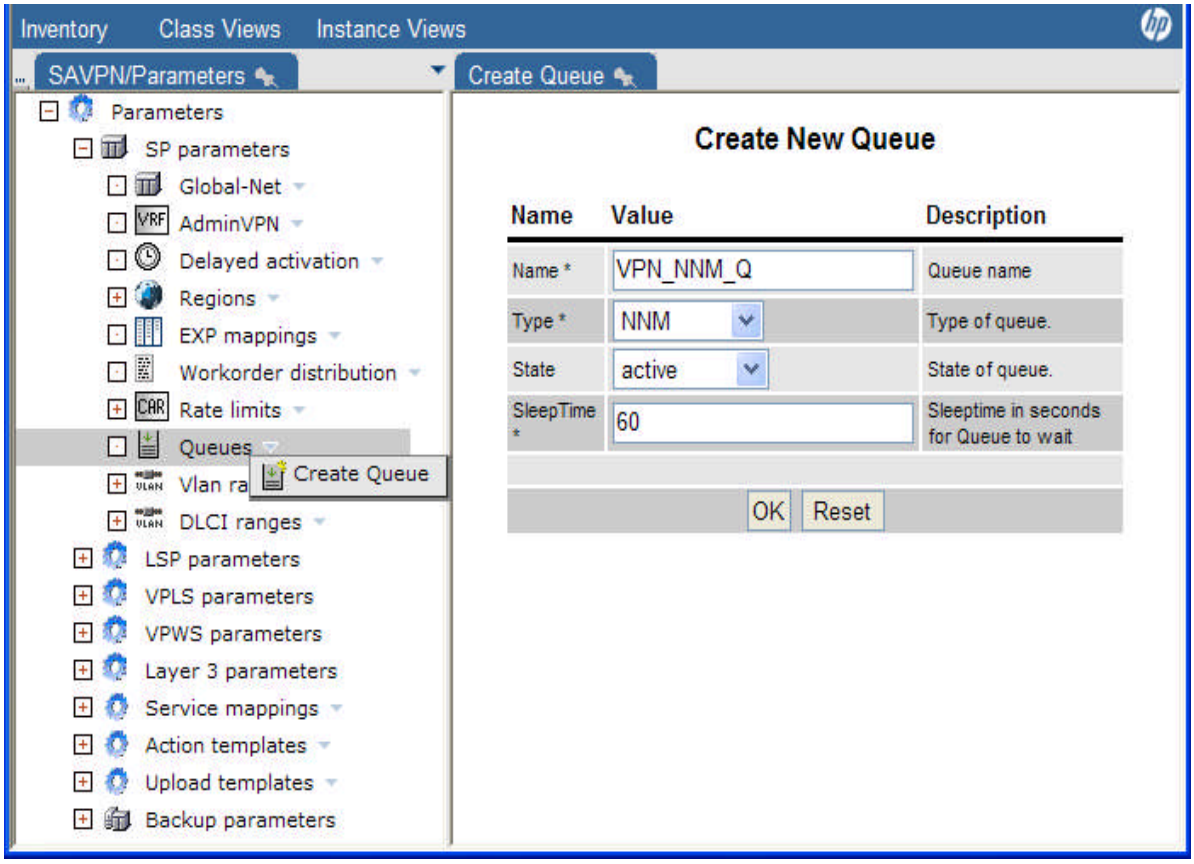
NOTE: The file nnmconfigimport.ovpl would be generally present under /opt/OV/bin directory in case of UNIX systems and under C:\Program Files\OpenView\bin in case of windows systems.

10-1-6 VPN_SVP→Parameters NNMi Queue configuration

The initial configuration to complete for successful NNMi integration is the creation of the internal NNM queue through which all service activation related information exchange towards NNMi happens. This queue decouples the activation process from the remote system integration process so service activations may proceed independently from updating the remote NNMi system."

. Navigating from SAVPN/Parameters inventory tree, expand SP parameters to find the option for creating the queue. Create the queue with a name of your choice by doing a right click on the "Queues" item as shown in the following figure.

Figure 10-3 Creation of VPN NNM Queue



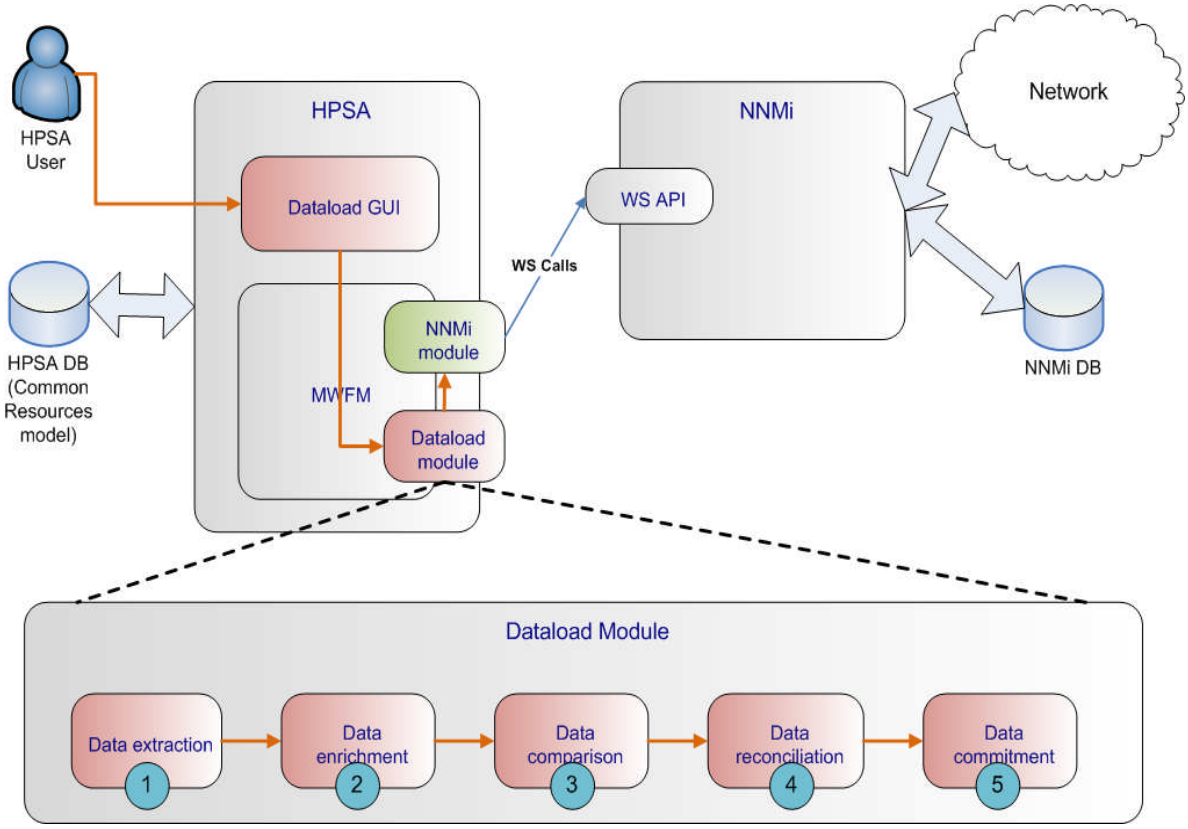
10-2 Dataload

The term dataload refers to the population of HPSA CRNModel's Equipment inventory with data discovered from the network by NNMi's discovery engine. Dataload in HPSA core is implemented as a MWFM module and it requires the NNMi request module and the CRNModel as dependencies. It is launched through a workflow and only one instance can be running at any given point in time. From Inventory tree we can trigger the NNM dataload workflow.

NOTE: The SAVPN/Equipment model is extended from the HPSA CRModel Equipment model. For details on CRModel Equipment model, refer to [*INTRO*]

The dataload process comprises several steps as shown in the following diagram:

Figure 10-4 Dataload process overview



Dataload process involves the following steps:

1. Data Extraction: HPSA extracts network information from NNMi via web-service interface.
2. Data Enrichment: Fills the service relevant information not provided by NNMi
3. Data Comparison: Compares NNMi extracted data with the existing data in HPSA database.
4. Data Reconciliation: Let's the operator to "Accept" or "Reject" the NNMi extracted data before committing to HPSA database.
5. Data Commitment: Commits the data in to HPSA database.

The various steps involved in VPN_SVP– NNMi integration configuration are:

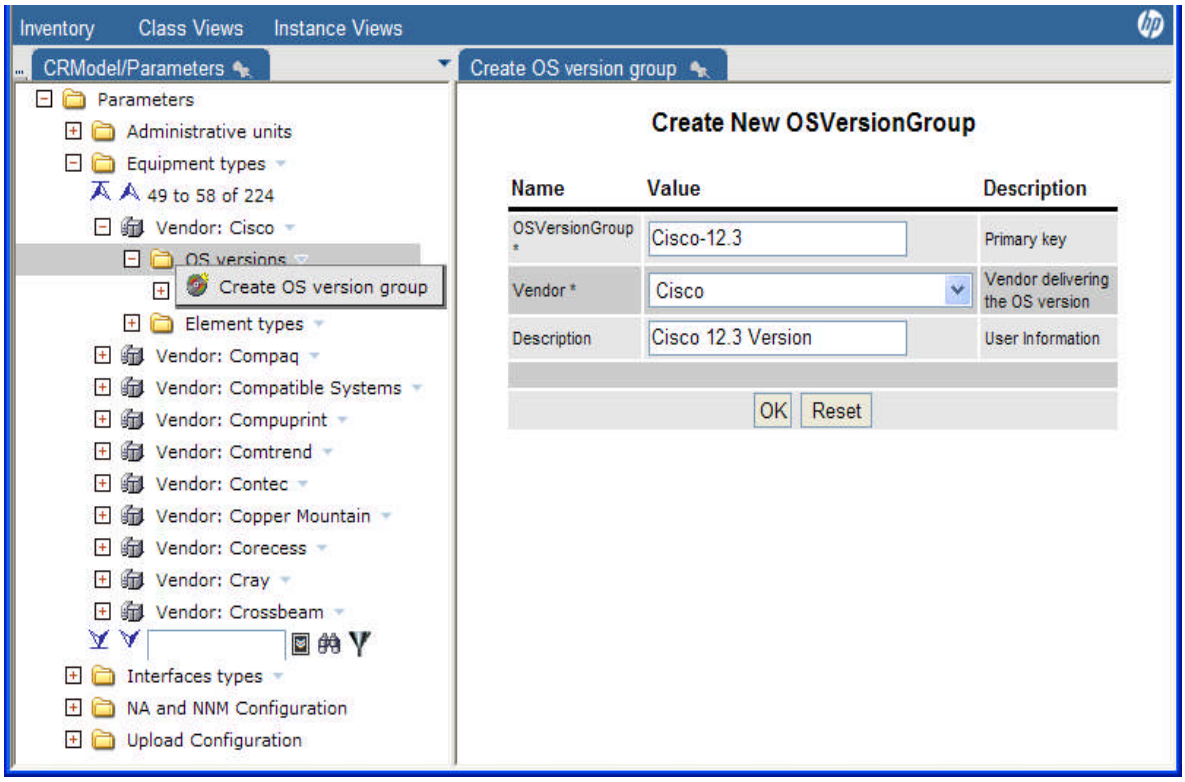
1. HPSA CRModel configuration of OSVersions, Element Types, Region and Locations
2. HPSA mwfm.xml NNMiDataloadModule configuration
3. Scope configuration
4. Enrichment configuration

The following section details the configurations to be performed by the administrator.

10-2-1 HPSA CRModel configuration of OSVersions, Element Types, Region and Locations

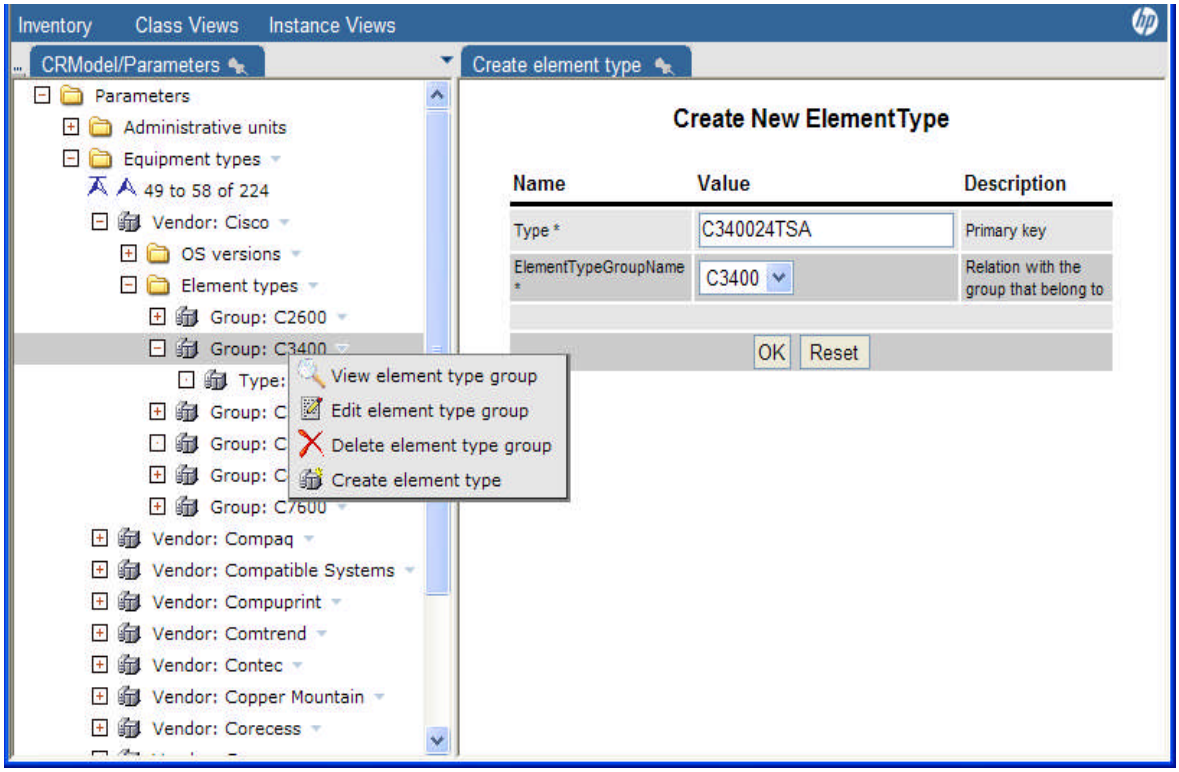
- Pre-populate the OS Version group details for the vendor, Open HPSA Inventory, CRModel Parameters→Parameters→Equipment types→Vendor<Vendor Name>→OS versions, and create the OS version group, as shown in the figure below.

Figure 10-5 Create OS version group



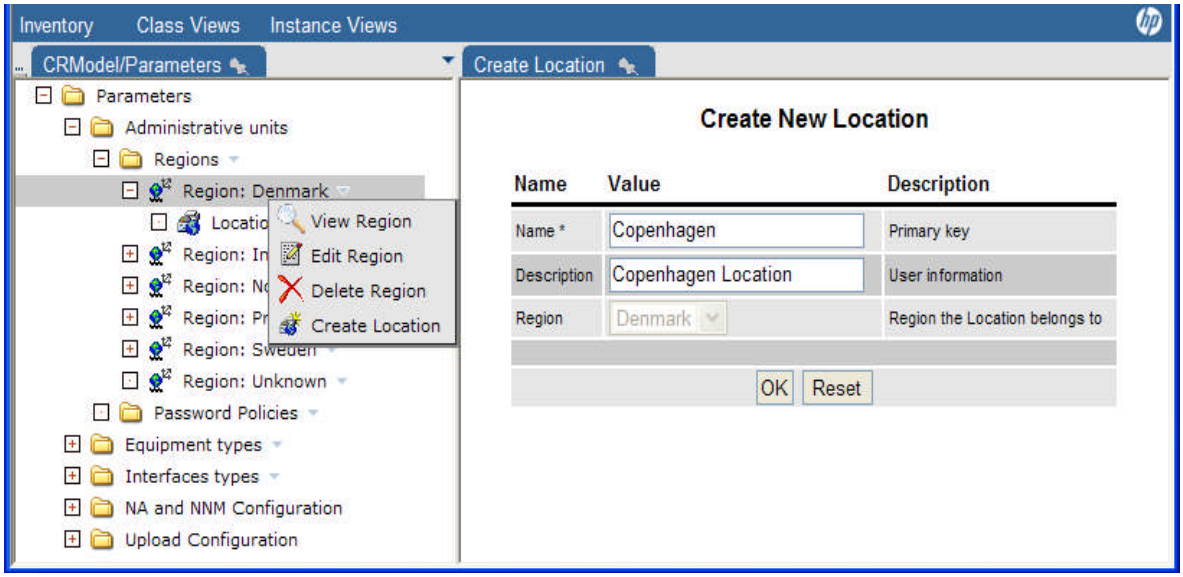
- Pre-populate the Element Types for the vendor. Open HPSA Inventory, CRModel Parameters→Parameters→Equipment types→Vendor<Vendor Name>→Element types, and create or use existing Group, and create element type within the Group, as shown in the following figure

Figure 10-6 Create element type



- Pre-populate the regions and locations. Open HPSA Inventory, CRModel Parameters→Parameters→Administrative units→Regions, choose or create a new Region, and create a new location, as shown in the following figure

Figure 10-7 Create Location



NOTE: For more details, refer to [*INTRO*].

10-2-2 HPSA mwfm.xml NNMiDataloadModule configuration

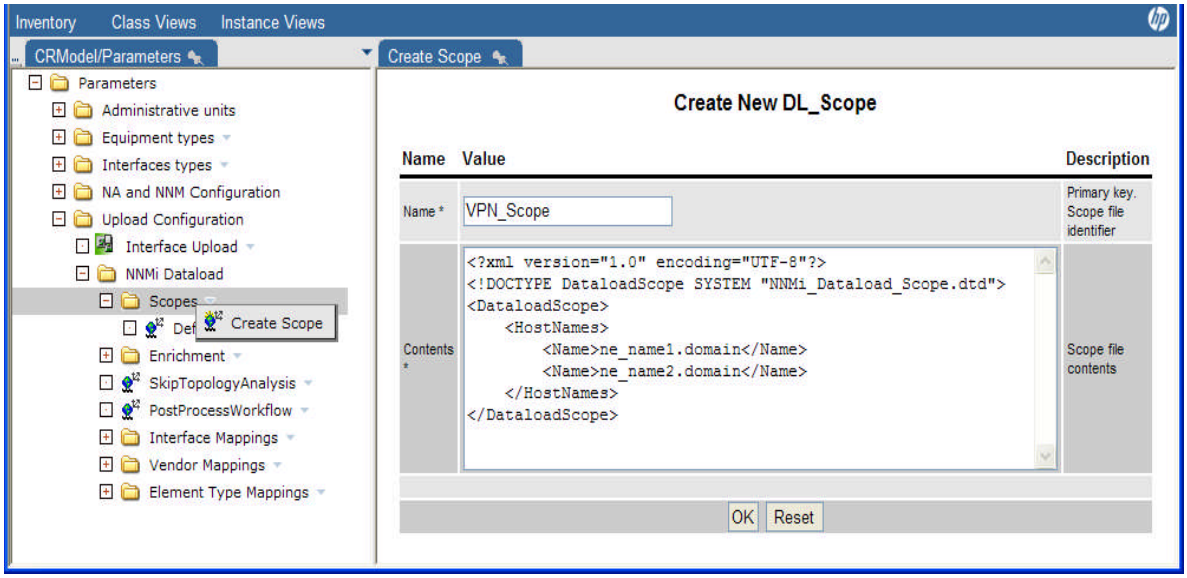
The Dataload Module must be appropriately configured. Ensure that the mwfm.xml file contains a single instance of the following module configuration:

```
<Module>
    <Name>NNMIDataloadModule</Name>
    <Class-Name>com.hp.ov.activator.mwfm.engine.module.dataload.NNMiDataloadModule</Class-Name>
    <Param name="nnmi_module_name" value="nnm_request"/>
</Module>
```

10-2-3 Scope configuration

The term scope in the context of dataload feature refers to the list of Network Elements that would be considered for the dataload process. The scope file is an XML file persisted in the HPSA database. In order to edit the scope, go to CRModel/Parameters→Parameters→Upload Configuration→NNMi Dataload→scopes, as shown in the figure below :

Figure 10-8 Create dataload Scope



NOTE: Name representing the hostname in the scope file should be the same name as identified by the NNMi 'Node Name' or 'Node Long Name'.

NOTE: HPSA dataload mechanism from NNMi discovers only the L2 link between different NEs and not the L3 Links.

NOTE: Scope also supports the wildcarding for hostnames.

The percent character '%' matches any sequence of 0 or more characters, and the underscore character '_' matches any single character. Devices which are not in the specified scope will be disregarded by the NMMi dataload operation.

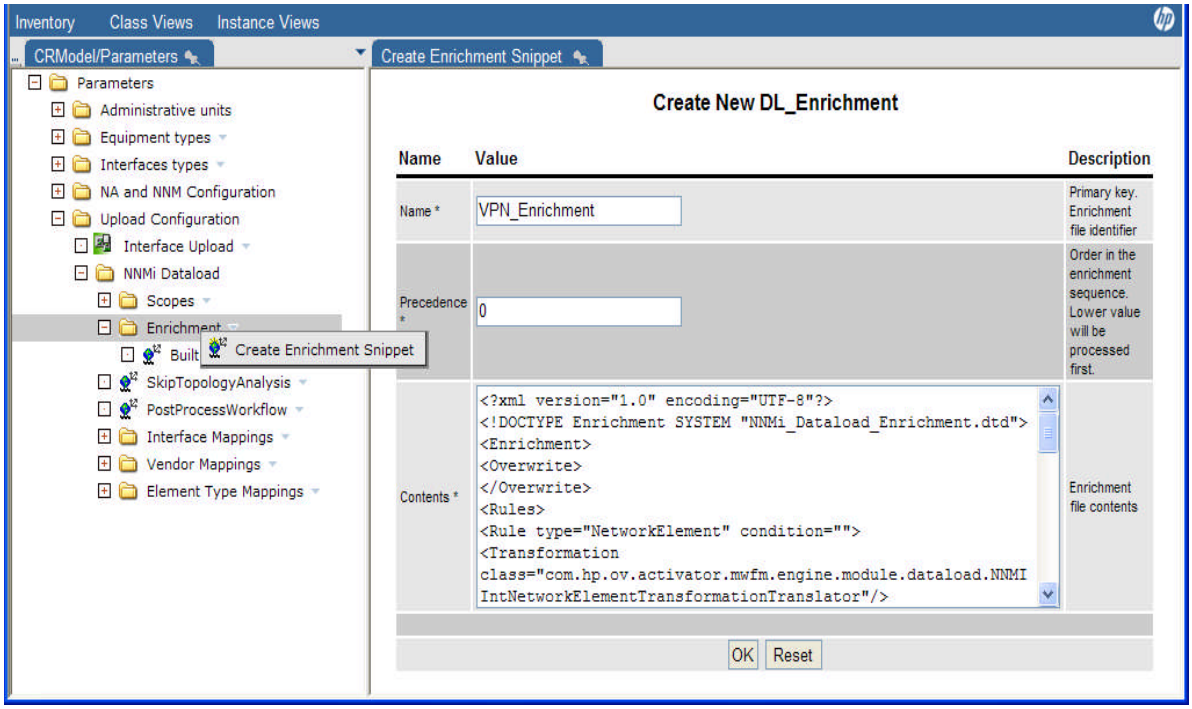
An example that matches all the hostnames is as given below

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE DataloadScope SYSTEM "NNMi_Dataload_Scope.dtd">
<DataloadScope>
        <HostNames>
                <WName>%%</WName>
        </HostNames>
</DataloadScope>
```

10-2-4 Enrichment configuration

The raw network data coming from NNMi during the dataload process can be enriched as per the needs of HPSA VPN before populating the same to VPN database. Enrichment is an XML file persisted in the HPSA DB – and can be edited by navigating through CRModel ParameterTree→Parameters→Upload Configuration→NNMi Dataload→Enrichments as shown below:

Figure 10-9 Create dataload enrichment snippet



NOTE: The best way to edit the enrichment file is to use cut-and-paste from the Inventory GUI and into the preferred editor- and vice versa when the file updates are completed..

VPN Solution service creation depends upon the correct values of some of the Network Element and Interface attributes like location, NetworkID, AdminState etc. All this data needs to be provided in the enrichment file so that, correct values of all these attributes are set as a part of the dataload process. The purpose of creating an enrichment file is that these properties can not be discovered by NNMi's network discovery engine. Following are the various blocks in the enrichment file:

- Setting the correct value of NetworkId and Location for each Network Element. Following is an example entry on how this can be done. In case of large number of network elements, proper naming convention with wild-carding feature will ease the effort of integration to a great extent:

```
<Rule type="NetworkElement"
    Condition="NetworkElement.NAME=='ne_name1.domain'">
        <Relation type="Network" name="ID" value="100"/>
        <Assignment name="Location" value="Denmark"/>
</Rule>
```

- Setting the correct value of AdminState and LifeCycleState. For all the network elements on which the services need to be created, the values of these attributes should be “Up” and “Ready” respectively. Following is an example of how this can be done:

```
<Rule type="NetworkElement" Condition="">
        <Assignment name="AdminState" value="Up" />
        <Assignment name=" " value="Ready" />
</Rule>
```

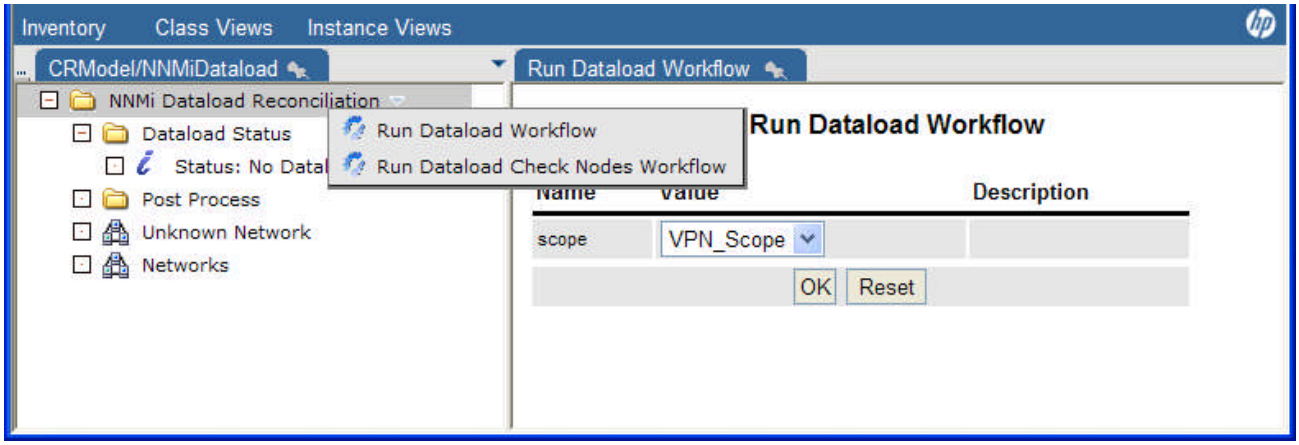
- Setting UserName, Password, Narrowing down to specific instance of PE/CE Router /Switch for each of the network element is an important activity prior to dataload. Following is an example on how this can be done:

```
<Extensions>
        <Rule type="NetworkElement"
                condition="NetworkElement.NAME=='ne_name1.domain'">
                <Narrowing class="com.hp.ov.activator.vpn.inventory.PERouter">
                        <Field name="UsernameEnabled" value="true"/>
                        <Field name="Username" value="safe"/>
                        <Field name="Password" value="OkhPR4cQf/XsRTmq0bA=="/>
                        <Field name="EnablePassword" value="OkhPR4cQf/XsRTmq0bA=="/>
                </Narrowing>
        </Rule>
        <Rule type="NetworkElement"
                condition="NetworkElement.NAME=='ne_name2.domain'">
                <Narrowing class="com.hp.ov.activator.vpn.inventory.Switch">
                        <Field name="PWPolicyEnabled" value="true"/>
                        <Field name="PWPolicy" value="100"/>
                </Narrowing>
        </Rule>
</Extensions>
```

In order to run the dataload using the scope and the enrichment files created, following are the steps:

- Select CRModel/NNMiDataload→NNMi Dataload Reconciliation, right click and choose ‘Run Dataload Workflow’.
- Select the scope ‘VPN_Scope’ as created earlier, as shown in the following figure:

Figure 10-10 Run Dataload WF



- All the enrichment files available in the system will be used in the sequence depending on the “Precedence*” value set in the enrichment.

NOTE: Enrichment also supports the wildcarding as follows.

For example, if the service provider has followed a consistent naming convention for different network elements based on role, the following enrichment snippet will identify all NetworkElement names with ‘*Switch*’ as AggregationSwitch. Similar wildcarding can be used to assign different attributes to the network element.

```
<Rule type="NetworkElement"
        condition="NetworkElement.NAME like '*Switch*'">
        <Assignment name="Role" value="AggregationSwitch" />
</Rule>
```

NOTE: For a sample enrichment file, refer to $SOLUTION/etc/config/nnm_liaison/enrichment_example.xml.

---

11 Integration with NA

Unintended or unauthorized modification of VPN connectivity can create serious security breaches which will lower or eliminate end-users' trust to the provider's ability to manage a MPLS VPN network. And the detection of changes to the service configuration on the network elements that e.g. could create unwanted connectivity can be very difficult.

The VPN_SVP-NA integration provides a Service Integrity check that will detect such changes by automatic creation and installation of NA Policies for the service activations done by VPN_SVP.

NA's policy manager validates regularly, by operator command or automatically when any changes are made to the device configurations, the installed Policies against the network device configurations. Failure of a Policy check implies that changes to the related service configuration have been made "behind the back" of VPN_SVP and such changes could be unintended or unauthorized."

11-1 NA Integration Configuration

11-1-1 MWFM

Interactions with NA from workflows take place through workflow manager modules, the NA Request modules. These modules must be configured in the Workflow Manager Configuration file, mwfm.xml as shown below:

```
<Module>
    <Name>na_request</Name>
    <Class-Name>com.hp.ov.activator.mwfm.engine.module.narequest.NARequestModule</Class-Name>
    <Param name="na_username" value="admin"/>
    <Param name="na_password" value="secret"/>
    <Param name="encrypted_password" value="false"/>
    <Param name="na_url" value="server1:1099;server2:1099"/>
    <Param name="queue_class" value="com.hp.ov.activator.mwfm.engine.module.WeightedEngineQueue"/>
    <Param name="queue_name" value="na_request_queue"/>
    <Param name="retry_count" value="4"/>
    <Param name="retry_interval" value="10"/>
    <Param name="min_threads" value="2"/>
    <Param name="max_threads" value="5"/>
</Module>
```

The parameters for this module are:

- na_username: NA server username for authentication.
- na_password: NA server password for authentication. It may be encrypted.
- Encrypted_password (optional): Specifies if the provided na_password is encrypted. The default value is 'false'.
- na_url: NA server url containing hostname and port.
- queue_name (optional): Name of the queue to be used by HPSA MWFM module to interact with the external NA system.

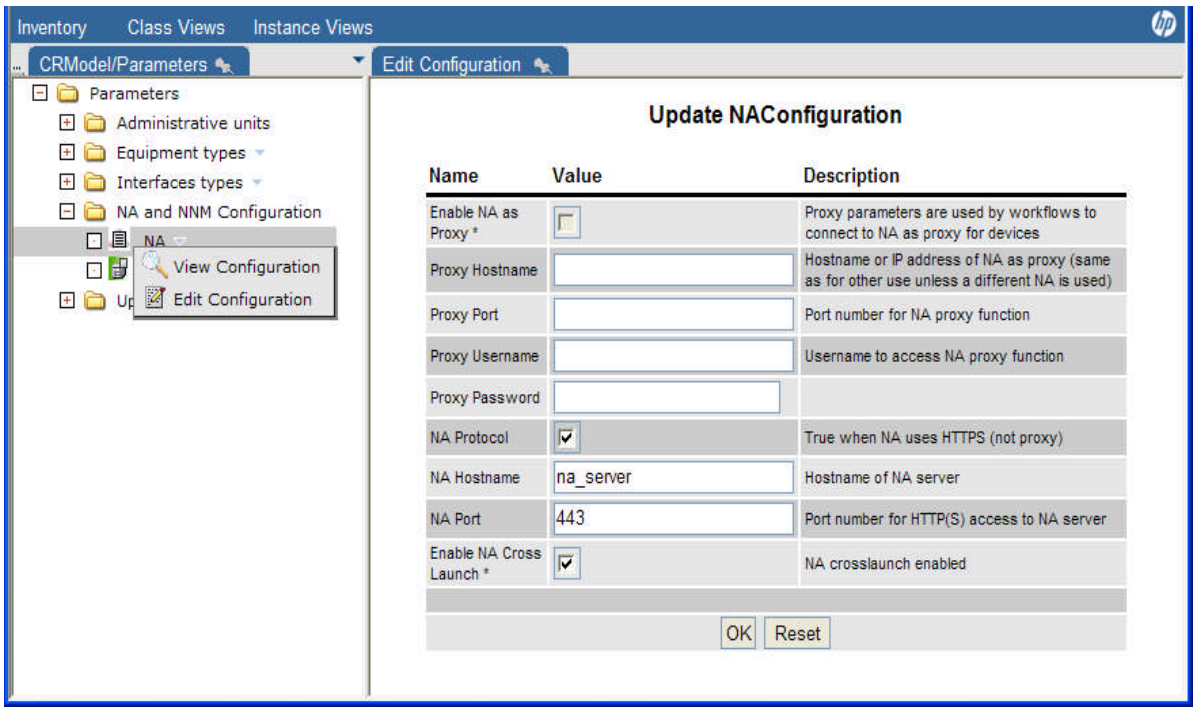
NOTE: As the Single Sign On [SSO] feature is not supported by NA, it cannot be used between HPSA and NA.

11-1-2 CR Model Inventory Parameters

In order to enable various VPN_SVP→NA integration features, the following menu items found under CRModel Parameters→NA and NNM Configuration→NA should be configured.

The configuration parameters NA protocol, NA hostname,NA Port, and Enable NA Cross Launch are used for the UI cross launch. User can enable/disable cross launch by setting the enabling/disabling a cross launch flag.

Figure 11-1 Update NA Configuration



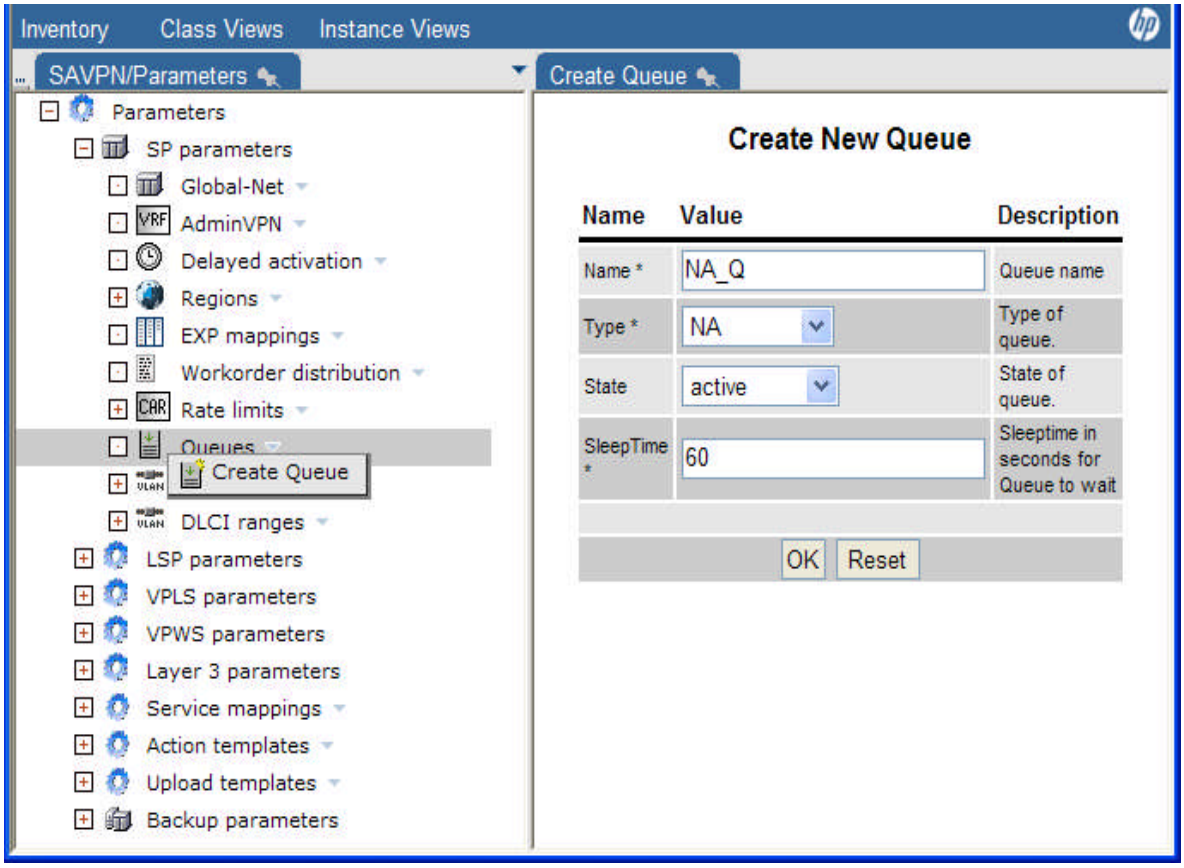
NOTE: The Proxy parameters are intended to be used by workflows to access devices through NA as a proxy, but this feature is not supported in this version. See Parameter Tree Section of [*INTRO*] for more details.

11-1-3 NA Queue

The initial configuration to complete for successful NA integration is the creation of the internal NA queue through which all service activation related information exchange towards NA happens. This queue decouples the activation process from the remote system integration process so service activations may proceed independently from updating the remote NA system

Navigating from SAVPN/Parameters menu item, expand SP parameters to find the option for creating the queue. Create the queue with a name of your choice by doing a Right click on the “Queues” item as shown in the following figure.

Figure 11-2 Create NA Queue



11-2 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 Product User Guide 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.

11-2-1 NA Parent Group Name:

VPN_SVP provides an Option to configure Parent Group Name for the Policies that are created by VPN_SVP. This could be done by navigating through SAVPN→ Parameters →SP Parameters→ Global-Net inventory tree branch. User can specify ParentGroup Name by editing the SP object.

NOTE: All the PE Routers should be added to the NA with the valid driver details. See [*NA_USR*] chapter “Adding Devices and Device Groups” .

11-2-2 Pattern reading from Properties file

VPN_SVP uses regular expression to extract info from the set of <DO> commands to form the policies on NA. These patterns are described in the property files cisco.properties and juniper.properties placed under the directory $SOLUTION/etc/config/na_liasion. cisco.properties and juniper.properties contains patterns for the Cisco and Juniper network elements respectively.

Default value of a pattern is used if a property is not found in the property file. Customization of VPN_SVP SI module can be done by modifying these patterns in property files.