HPSP VPN Technology Extension

Delivery Guide

Release v7.0



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 2015 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.

Java[™] is a registered trademark of Oracle and/or its affiliates.

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

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

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

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.

Table of Contents

1 Introduction	7
1.1 L3 VPN Services	7
1.2 The HPSP VPN TE Solution	7
1.2.1 Functionality covered	7
1.2.2 Architecture	8
2 Installation & Configuration	10
2.1 Prerequisites	10
2.1.1 HPSA	10
2.1.1.1 Installation	10
2.1.1.2 Configuration	10
2.1.2 HPSA VPN Solution	10
2.1.2.1 Installation	10
2.1.2.2 Configuration	10
2.1.3 HP Service Provisioner	10
2.1.3.1 Installation	10
2.1.3.2 Configuration	11
2.1.4 OSS Console	11
2.1.4.1 Installation	11
2.1.4.2 Configuration	11
2.2 HPSP VPN TE Installation	11
2.2.1 Web service connectivity module	11
2.2.2 HPSP VPN TE Core	13
2.2.3 HPSP VPN TE UI	14
2.3 Configuration	14
2.3.1 HPSP Microworkflow configuration	14
2.3.2 Import the VPN Catalog	17
2.4 Start and Stop the solution	18
2.5 Putting the solution to work	18
2.5.1 CSP Network configuration	18
2.5.1.1 CSP Core Network	18
2.5.1.2 L2 Access Networks	19
2.5.1.3 IP Pool	20
2.5.1.4 Preview	21
2.5.2 Access the HPSP VPN TE UI	21
2.6 Uninstall the solution	21
3 Appendix I: Customize the solution	24
3.1 UI Customization	24
3.2 Logic Customization	24

In This Guide

This document explains installation and administration processes for the HPSP VPN Technology Extension.

Audience

The audience for this guide is the Solutions Integrator (SI). The SI has a combination of some or all of the following capabilities:

Understands and has a solid working knowledge of:

- UNIX® commands
- Windows® system administration

Understands networking concepts and language

Is able to program in Java™ and XML

Understands security issues

Understands the customer's problem domain

Conventions

The following typographical conventions are used in this guide.

Font	What the Font Represents	Example
Italic	Book or manual titles, and man page names	Refer to the HP Subscription Repository and the Javadocs man page for more information.
	Provides emphasis	You <i>must</i> follow these steps.
	Specifies a variable that you must supply when entering a command	Run the command: javac <i><sourcefiles></sourcefiles></i>
	Parameters to a method	The <i>assigned_criteria</i> parameter returns an ACSE response.
Bold	New terms	The distinguishing attribute of this class
Computer	Text and items on the computer screen	The system replies: Press Enter
	Command names	Use the javac command
	Method names	The get_all_replies() method does the following
	File and directory names	Edit the file \$Installation_dir/config/conf.xml
	Process names	Check to see if system is running.
	Window/dialog box names	In the Test and Track dialog
	XML tag references	Use the <dbtable> tag to</dbtable>
Computer Bold	Text that you must type	At the prompt, type: ls -l
Кеусар	Keyboard keys	Press Return .
[Button]	Buttons on the user interface	Click [Delete].
		Click the [Apply] button.
Menu ltems	A menu name followed by a colon (:) means that you select the menu, then the item. When the item is followed by an arrow (->), a cascading menu follows	Select Locate:Objects->by Comment.

Abbreviations

HPSP: HP Service Provisioner HPSP VPN TE: HP Service Provisioner Technology Extension HP TV: HP Trueview resource inventory HPSA VPN: HPSA VPN activation solution HP SR: Subscription Repository

1 Introduction

1.1 L3 VPN Services

The current version of the HPSP VPN TE covers the L3 VPN Services. An L3 VPN is an IP based network delivering private network services over the CSP infrastructure.



Figure 1: High level view

Internally, it uses layer 3 VRF (VPN/virtual routing and forwarding) to segment routing tables for each "customer" using the service. Protocol BGP is required in the CSP.



Figure 2: Technical view

1.2 The HPSP VPN TE Solution

The HPSP Technologies Extensions provide, on top of the HPSP, the modules needed to cover the provisioning process for a concrete technology/business domain, in this case, the L3 VPNs.

1.2.1 Functionality covered

The functionality covered by the solution is:

- Management of L3 VPN services, including:
 - Selection of the VPN topology to apply:
 - Full Mesh
 - Hub & Spoke
 - o Selection of the Class of Service to apply and rate limit available per site
 - Configuration of the connectivity between the CE and correspondent PE, including the following protocols:
 - RIP
 - BGP
 - OSPF
 - Static Routes
 - Configuration and provisioning of the L2 access network (vlan path between the CE and the PE), including:
 - L2 direct connections
 - L2 ring networks
 - L2 star networks
 - Provisioning of the PE including the VRF configuration.
 - Monitor the installation task of the CE equipment
 - Remote configuration of the CE equipment
- The available models of equipments that can be managed by the solution are the ones covered by the HPSA VPN solution.

1.2.2 Architecture



Figure 3: HPSP VPN TE Architecture

Modules included in the solution:

Module	Description
VPN Service Catalog	Product and Service Catalog for the L3 VPN services, including the decomposition of the customer services in technical services.
Associated provisioning workflows	Workflows in charge of managing the provisioning process, associated to the technical services in the catalog.
TV VPN Inventory Adaptor	Out-of-the-box adaptor to interact with HP TV, in charge of the network resource inventory.
HPSA VPN Adaptor	Out-of-the-box adaptor to interact with HPSA VPN, in charge of the service activation.
Customer Agent UI	Order entry and service monitor functionality. Integrated into the HP OSS Console platform.
Operator UI	Manual task management and technical monitoring. Integrated into the HPSP default UI.

2 Installation & Configuration

This part of the guide will try to summarize the installation process of the Technology Extension solution, specifying also the rest of components it requires to work properly.

2.1 Prerequisites

This chapter describes the list of steps to install and configure the different solutions integrated by the application.

Please consult the documentation of each solution for details on how to install the different components.

2.1.1 HPSA

The following actions are required to properly install and configure the HPSA solution.

2.1.1.1 Installation

Install the HPSA v7.0.

2.1.1.2 Configuration

Deploy the 'CRM Model' solution on top of the HPSA.

2.1.2 HPSA VPN Solution

The following actions are required to properly install and configure the HPSA VPN solution.

2.1.2.1 Installation

Install the HPSA VPN v7.0.

2.1.2.2 Configuration

In order to configure the HPSA VPN ready for the HPSP VPN TE solution, execute the script 'resetVPNAdaptativeMode' located in \$HP\OpenView\ServiceActivator\solutions\SAVPN\etc\config

2.1.3 HP Service Provisioner

The following actions are required to properly install and configure the HP Service Provisioner solution.

2.1.3.1 Installation

Deploy the HP Service Provisioner v7.0 solution on top of the installed HPSA.

2.1.3.2 Configuration

No configurations are required.

2.1.4 OSS Console

The following actions are required to properly install and configure the HP OSS Console solution.

2.1.4.1 Installation

Install the OSS Console v2.0

2.1.4.2 Configuration

No configurations are required.

2.2 HPSP VPN TE Installation

Once the prerequisites have been followed, the HPSP VPN TE installation process can start.

2.2.1 Web service connectivity module

This module is required for the solution to interact with the TV platform via web service.

The first step is to install the patch 'HPSA Extension Pack v7.0' on top of the installed HPSA. Once installed, the following module has to be deployed:

Go to Local Deployment -> Import solution and select the MSA_WSC.zip located in the directory 'binaries' of the ISO file. Click on import.

💢 HP Service Activator Deploy	/ment Manager	
File Deployment Verification	Configuration Wizards Help	
🚿 🚠 🧔 🍄 🧔 🎓 🛙	R	
Local Deployment	Import Solution	
Solution Operations	- Select mode	
Create Solution Skeleton		
Deploy Local Solution	From zip/tar file	
Ondepioy Local Solution Delate Local Solution	C: (HP (OpenView (ServiceActivator (SolutionPacks (MSA_WSC.zip Browse	
Import Solution	From directory	
Export Solution	Browse	
Patch Operations		
Create Patch Skeleton Deploy Patch		
Undeploy Patch		
Delete Patch		
 Import Patch 		
Export Patch		
Customization Operations		
Create Customization Skeleton		
 Deploy Customization 		
 Undeploy Customization 		
Delete Customization	Import	
Import Customization Export Customization		
Export Customization	Log	
Preferences		
List Solutions		
Local Deployment		
Remote Deployment		
Verification		
Configuration		
Local Deployment - Import Solution		

Go to Local Deployment -> Deploy local solution and select the imported solution. Then select the appropriate deployment file. Check the option "Create inventory tables" and click on Deploy solution.

🔯 HP Service Activator Deploy	rment Manager	
File Deployment Verification	Configuration Wizards Help	
🌋 🕹 🦃 🦃 🌾	Ř	
Local Deployment	Deploy Solution on Local Server	
Solution Operations		
Create Solution Skeleton	Solution name: MSA 🗸	
Deploy Local Solution		
Delete Local Solution	Deployment file: "OpenView ServiceActivator (solutions WSA (deploy_6_1_oracle.xm) Browse	
Import Solution		
Export Solution	Do not deploy workflows, plug-ins, inventory trees, compound tasks, umm data, queues or xmaps	
Detth Occurrence		
Create Batch Skeleten	Do not deploy SQL	
Deploy Patch	🕅 Do not back up	
Undeploy Patch		
Delete Patch	Force	
 Import Patch 	Provide Investment Address	
 Export Patch 	V Create inventory tables	
Customization Operations		
Create Customization Skeleton		
 Deploy Customization 		
 Undeploy Customization 		
Delete Customization	Deploy solution	
Import Customization Export Customization	· · · · · · · · · · · · · · · · · · ·	
Export Customization		
Preferences		
List Solutions		
Local Deployment		
Remote Deployment		
Verification		
Configuration		
Local Deployment - Deploy Local So	lution	

2.2.2 HPSP VPN TE Core

Deploy the HPSP VPN TE solution included in the ISO:

Go to Local Deployment -> Import solution and select the VPNTech.zip located in the directory 'binaries' of the ISO file. Click on import.



A manual interaction is required at this point. Access the file 'populate_poc_data_xxx.sql' (where xxx represents the installed data base) located in

'\$HP\OpenView\ServiceActivator\solutions\VPNTech\etc\sql', open it and replace the values <tvuser>, <tvpassword>, <host:port> with the appropriate values to connect to TV Inventory. Save it.

-- Replace the fields in bold letter with the appropiate TV connectivity values INSERT INTO WSC_ENDPOINT (ENDPOINTID, TARGETEQUIPMENT, USERNAME, PASSWORD, URL, WSCSERVICEID, NETWORKELEMENTID, ISPARENT_) VALUES (WSC_ENDPOINT_SEQ.nextVal, 'TV', tvuser, tvpassword, 'http://host:port/tnp-ws/services', (SELECT WSCSERVICEID FROM WSC_SERVICE WHERE SERVICENAME='TV'), (SELECT NETWORKELEMENTID FROM CR_NETWORKELEMENT WHERE NAME='TV'), '0');

Then, go to Local Deployment -> Deploy local solution and select the imported solution. Then select the appropriate deployment file. Check the option "Create inventory tables" and click on Deploy solution.



2.2.3 HPSP VPN TE UI

Put the file 'GUI_VPN_Technology_Extension_v7.0.0.zip' included in the 'binaries' directory of the ISO file, in the 'dist' directory of the HP OSS Console. Please consult the HP OSS Console documentation on more details on how to deploy solutions on top.

2.3 Configuration

This chapter describe the steps needed to configure the solution once the installation process has been done.

2.3.1 HPSP Microworkflow configuration

Edit the mwfm.xml located at \$HP\OpenView\ServiceActivator\etc\config to match this configuration:

• Add or uncomment this line:

<Generate-Service-ID>**true**</Generate-Service-ID>

• Uncomment authenticator module:

```
<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="mwfm remote url" value="//localhost:2000/wfm"></Param>

<Param name="mwfm remote url" value="/localhost:2000/wfm"></Param>

<Param name="mwfm remote url" value="90"></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>
```

• Configure the socket sender module:

• Add the JMS listener and sender module, changing the user/password if necessary:

```
<Module>
        <Name>jms_listener_queue</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.JMSListenerModule</Class-Name>
        <Param name="workflow" value="Example_Controller"/>
        <Param name="jndi url" value="remote://primary:4447"/>
        <Param name="jndi initial context factory"
                value="org.jboss.naming.remote.client.InitialContextFactory"/>
        <Param name="connection factory name" value="ConnectionFactory"/>
        <Param name="jms_trans_mode" value="queue"/>
<Param name="jms_destination" value="HPSAQueue"/>
        <Param name="username" value="hpsa"/>
        <Param name="password" value="s5/HIIXk9NIZdrwnw6tSmA=="/>
        <Param name="header" value="true"/>
        <Param name="dtd" value="exchange.dtd"/>
        <Param name="dtd root tag" value="msg"/>
        <Param name="min threads" value="1"/>
        <Param name="max threads" value="3"/>
        <Param name="max queue length" value="50"/>
        <Param name="write message to" value="db"/>
</Module>
<Module>
        <Name>jms sender queue</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.JMSSenderModule</Class-Name>
<Param name="jndi_url" value="remote://primary:4447"/>
        <Param name="jndi_initial_context_factory"
                value="org.jboss.naming.remote.client.InitialContextFactory"/>
        <Param name="connection factory name" value="ConnectionFactory"/><Param name="jms destination" value="HPSAQueue"/>
        <Param name="username" value="hpsa"/>
        <Param name="password" value="s5/HIIXk9NIZdrwnw6tSmA=="/>
</Module>
```

• Configure the conflict module:

```
<Module>

</Module>

</Module>
</Module>
</Module>
</Module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
</module>
```

• Add the following modules, reviewing that the user/password fields match your own configuration:

```
<Module>
       <Name>SOFAModuleTV</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.sofa.SOFAModule</Class-Name>
       <!-- Adapter package -->
       <Param name="implementation package"
       value="com.hp.ov.activator.mwfm.engine.module.sofa.inventory.tv"/>
       <!-- RMI Port -->
       <Param name="rmi_service_port" value="9998"></Param>
<!-- Maximum interval to wait for a ws request in seconds-->
       <Param name="max ext waiting response" value="60"></Param><!-- default value is 60-->
       <!-- WS Parameters-->
       <Param name="wsc module name" value="wsc"></Param>
       <Param name="target equipment" value="TV"></Param>
       <Param name="service name" value="TV"></Param>
</Module>
<Module>
       <Name>SOFAModuleSAVPN</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.sofa.SOFAModule</Class-Name>
       <!-- Adapter package -->
       <Param name="implementation package"
               value="com.hp.ov.activator.mwfm.engine.module.sofa.activation.savpn"/>
       <Param name="rmi service port" value="9997"></Param>
       <Param name="mwfm remote url" value="//localhost:2000/wfm"></Param>
       <Param name="mwfm_remote_user" value="hpsa"></Param>
       <Param name="mwfm_remote_password" value="s5/HIIXk9NIZdrwnw6tSmA=="></Param>
       <!-- Socket listener parameters -->
       <Param name="wait latency" value="1000"></Param><!-- default value is 1000 -->
       <Param name="max ext waiting response" value="60"></Param><!-- default value is 60 -->
       <Param name="listener_port" value="5099"></Param>
       <Param name="terminal_codes" value="200;500;501;306;307;201;402;401"></Param>
       <Param name="ok codes" value="200;210"></Param>
       <Param name="database module" value="db"></Param>
</Module>
<Module>
       <Name>wsc</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.sofa.WSCModuleVPNTech</Class-Name>
       <Param name="database module" value="db"/>
       <Param name="retry count" value="1"/>
       <Param name="retry interval" value="20"/>
</Module>
```

```
<!-- SOM Config modules -->
</Module>
</Name>som_jms_listener_queue</Name>
</Class-Name>com.hp.ov.activator.mwfm.engine.module.JMSListenerModule</Class-Name>
</Param name="workflow" value="Example Controller"/>
</Param name="jidi_url" value="remote://primary:4447"/>
</Param name="jidi_initial_context_factory"
value="org.jboss.naming.remote.client.InitialContextFactory"/>
</Param name="connection factory name" value="ConnectionFactory"/>
</Param name="jims_trans_mode" value="queue"/>
</Param name="jims_destination" value="HPSAQueue"/>
```

```
<Param name="username" value="hpsa"/>
       <Param name="password" value="s5/HIIXk9NIZdrwnw6tSmA=="/>
       <Param name="header" value="true"/>
       <Param name="dtd" value="exchange.dtd"/>
       <Param name="dtd root tag" value="msg"/>
       <Param name="min threads" value="1"/>
       <Param name="max threads" value="3"/>
       <Param name="max queue length" value="50"/>
       <Param name="write message to" value="db"/>
</Module>
<Module>
       <Name>som_jms_sender_queue</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.JMSSenderModule</Class-Name>
       <Param name="jndi url" value="remote://primary:4447"/>
       <Param name="jndi initial context factory"
               value="org.jboss.naming.remote.client.InitialContextFactory"/>
       <Param name="connection factory name" value="ConnectionFactory"/>
       <Param name="jms destination" value="HPSAQueue"/>
       <Param name="username" value="hpsa"/>
       <Param name="password" value="s5/HIIXk9NIZdrwnw6tSmA=="/>
</Module>
<Module>
       <Name>ServiceOrderManagement</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.som.SRModule</Class-Name>
       <Param name="username" value="sruser"/>
       <Param name="password" value="sruser"/>
       <Param name="encrypted password" value="false"/>
       <Param name="ws url" value=" http://localhost:8180/subscriptionrepository/operations"/>
<Param name="retry_count" value="3"/>
       <Param name="retry interval" value="10000"/>
       <Param name="min threads" value="1"/>
       <Param name="max_threads" value="3"/>
</Module>
<Module>
       <Name>trueview</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.TrueviewModule</Class-Name>
       <Param name="username" value="admin"/>
       <Param name="password" value="admin1001"/>
       <Param name="encrypted password" value="false"/>
       <Param name="ws_url" value="http://portov4.gre.hp.com:8011/tnp-ws/services"/>
       <Param name="retry_count" value="3"/>
       <Param name="retry interval" value="10000"/>
       <Param name="min threads" value="1"/>
       <Param name="max threads" value="3"/>
</Module>
```

2.3.2 Import the VPN Catalog

To import the VPN catalog, the HPSP must be running. Then, go to \$HP\OpenView\ServiceActivator\bin and execute the next command, specifying the path to the catalog file (the file called catalogVPNTE.xml located in \$HP\OpenView\ServiceActivator\solutions\VPNTech\docs)

SOMData -import -user hpsa -password hpsa -filePath C:\HP\OpenView\ServiceActivator\solutions\VPNTech\docs\catalogVPNTE.xml

2.4 Start and Stop the solution

The HPSP VPN TE is deployed as a solution on top of the HPSP. For information on stopping and starting the HPSP, refer to the HPSP Installation Guide.

2.5 Putting the solution to work

2.5.1 CSP Network configuration

The Technology Extension solution requires some previous population of the TV Inventory System in order to work:

2.5.1.1 CSP Core Network

At least on available BGP Network has to be configured. The BGP Network contains the PE and P equipments that will compose the CSP Network. This network requires the following configuration:

- The CSP has to be defined as a valid customer in TV
- All the BGP components (PE and P equipments) will be associated to this customer, as it is the owner of the core network.
- All the equipments will be well configured in the TV Inventory including a valid location.
- All the connections and IP links have to be configured, connecting the equipments (following the CSP network design).
- The IP links have to be added to the already created BGP network.
- Some UDAs (user defined attributes) have been added to the standard TV configuration in order to complete the basic information of the network elements. The PE equipments require the configuration of the following UDAs:

Module	Description
Role	Fixed value: "PE"
Default Network	Identifier of the BGP Network
Username	User name to access the equipment remotely via Telnet/SSH
Password	User name to access the equipment remotely via Telnet/SSH
Username enable	User enable to access the equipment remotely via Telnet/SSH. Optional
Password enable	Password enable to access the equipment remotely via Telnet/SSH. Optional
Management IP	IP to access the equipment remotely via Telnet/SSH

Management IF	Name of the interface to be accessed remotely. Optional, only informative.
Element Type	Element type of the equipment. Compatible with the field 'Element type' of network elements in the HPSA VPN solution*
OS Version	OS Version of the equipment. Compatible with the field 'OS Version' of network elements in the HPSA VPN solution*
Vendor	Vendor of the equipment. Compatible with the field 'Vendor' of network elements in the HPSA VPN solution*

*Consult the HPSA VPN documentation to know the available network element models Once configured, the BGP network has to be in active state.

2.5.1.2 L2 Access Networks

The access networks are Ethernet networks that will connect the CE equipments to the CSP core network.

Each access network is composed of Access and Aggregation switches. The Aggregation switches transport the traffic of the customers to the PEs. The configuration of each Ethernet network requires the following configuration:

- All the equipments (Access switches and Aggregation switches) will be well configured in the TV Inventory including a valid location.
- All the equipments will be associated to the CSP customer, as it is the owner of the network.
- All the connections (facilities and Ethernet links) have to be configured, connecting the equipments (following the CSP network design).
- The Ethernet connections have to be added to the already created Ethernet network (including the connections between the aggregation switches and the PEs)
- An Ethernet circuit has to be defined connecting each access switch to the PE (this circuit will go through the access network in order to reach the core network). This circuit will be used to calculate the physical path to reach the core network.
- Some UDAs (user defined attributes) have been added to the standard TV configuration in order to complete the basic information of the network elements. These equipments require the configuration of the following UDAs:

Module	Description
Role	Fixed value: "ACCSWITCH" for access switches and "AGGSWITCH" for aggregation switches.

Default Network	Identifier of the Ethernet network
Access Circuit	Identifier of the access circuit to reach the core network.
Username	User name to access the equipment remotely via Telnet/SSH
Password	User name to access the equipment remotely via Telnet/SSH
Username enable	User enable to access the equipment remotely via Telnet/SSH. Optional
Password enable	Password enable to access the equipment remotely via Telnet/SSH. Optional
Management IP	IP to access the equipment remotely via Telnet/SSH
Management IF	Name of the interface to be accessed remotely. Optional, only informative.
Element Type	Element type of the equipment. Compatible with the field 'Element type' of network elements in the HPSA VPN solution*
OS Version	OS Version of the equipment. Compatible with the field 'OS Version' of network elements in the HPSA VPN solution*
Vendor	Vendor of the equipment. Compatible with the field 'Vendor' of network elements in the HPSA VPN solution*

*Consult the HPSA VPN documentation to know the available network element models

Once configured, the Ethernet network has to be in active state.

2.5.1.3 IP Pool

An IP pool has to be created in TV. This IP pool will be used to obtain the available IPs in order to provisioning the L3 connectivity between the customers (and core network). IP pools in TV are defined as number pools. The HPSP solution, by default, will use an IP pool called 'Simple-VPN-Pool'. This pool has to be created and configured in the Inventory with the appropriate IP ranges.

2.5.1.4 Preview

This is an example of a view in the TV Inventory, containing a BGP core network and three access networks located in different areas:



2.5.2 Access the HPSP VPN TE UI

Once the Inventory has been configured, the solution can be accessed and customer VPN services created and managed. Access the solution in this URL:

http://<hostname>:<port>

Where <host>:<port> are the host and port (typically 3000) on which the OSS Console has been deployed.

Please consult the HPSP VPN TE User's Guide for details on how to use the tool.

2.6 Uninstall the solution

Undeploy the HPSP VPN TE solution.

Go to Local Deployment -> Undeploy local solution, and select the 'VPNTech' solution. Check the option 'Delete inventory tables'. Click on Undeploy the solution.

🙀 HP Service Activator Deploy	/ment Manager
File Deployment Verification	Configuration Wizards Help
% 🔝 🦃 📽 🦪 🎦 👒	
Local Deployment	Undeploy Solution from Local Server
Solution Operations	
Create Solution Skeleton	Sch jon name: VPNTech 🗸
Deploy Local Solution	To be bet underlay workflows, plustics, investory trace, compared tacks, your data, graves or years
 Undeploy Local Solution 	Do not undeploy worknows, plag-ins, inventory alees, compound tasks, unin data, queues or kinaps
Delete Local Solution	🗇 Do not undeploy SQL
Export Solution	
· Export solution	Do not restore
Patch Operations	Force
Create Patch Skeleton	
Deploy Patch	V Delete inventory tables
Ondepioy Patch Delete Batch	E Saran delata disastarian
Import Patch	proce delete directories
Export Patch	
Customization Operations	
Create Customization Skeleton	
Undeploy Customization	
Delete Customization	
Import Customization	Undeploy solution
 Export Customization 	Log
Preferences	
List Solutions	
Local Deployment	
Remote Deployment	
Verification	
Configuration	
Local Deployment - Undeploy Local	Solution

Go to Local Deployment -> Delete local solution, and select the VPNTech solution. Click on Delete solution.

W HP Service Activator Deploy	ment Manager
File Deployment Verification	Configuration Wizards Help
\lVert 🚠 🐼 隆 🕼 🕼	×
Local Deployment	Delete Solution from Local Server
Solution Operations	
Create Solution Skeleton	Solution name: NPNTech
Deploy Local Solution	
Undeploy Local Solution	
Import Solution	
Export Solution	
Patch Operations	
Create Patch Skeleton	
 Deploy Patch 	
Undeploy Patch	
Delete Patch Tragent Database	
Import Patch Export Patch	
• Export Pater	
Customization Operations	
 Create Customization Skeleton 	
 Deploy Customization 	
 Undeploy Customization 	
Delete Customization	Delete solution
Import Customization	
 Export Customization 	\hpsa.ear\activator.war\jsp\inventory\VPNTech
Preferences	[20-ene-2015 17:22:22]Delete the directory: C:\HP\jboss\standalone\deployments
List Solutions	\hpsa.ear\activator.war\javascript\VPNTechExt
	[20-ene-2015 17:22:22]Delete the directory: C:\HP\jboss\standalone\deployments
Local Deployment	\hpsa.ear\activator.war\jsf\VPNTechExt
Remote Deployment	[20-ene-2015 17:22:22]Delete the directory: C:\HP\OpenView\ServiceActivator\et
Verification	[20-ene-2015 17:22:22]Undeployment was completed successfully.
Configuration	▼
Local Deployment - Delete Local Sol	ution

Please consult the guides of the different solutions included in the requirement list in order to uninstall the whole environment.

3 Appendix I: Customize the solution

3.1 UI Customization

The HPSP VPN TE UI is deployed on top of the HP OSS Console solution. Visual customizations are available out-of-the-box with this solution. Please consult the HP OSS Console documentation for more details about how to customize the look&feel of the solution.

3.2 Logic Customization

It's strongly recommended to use the services included in the HPSP VPN TE Catalog as they are. If a modification/extension of the logic is required, create your own products combining the existing services or use the pre-workflow and post-workflow functionality included in the HPSP, this way, the users can develop their own workflows and assign them to the CFSs and Products in the Catalog without changing the basic functionality and ensuring the backward compatibility for next versions.