Quantum Policy Suite 5.5.1 Operations Guide

Version 5.5.1

September 30, 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-29748-01

CONTENTS

Preface

Revised: September 30, 2013, OL-29748-01

Welcome to Cisco's Quantum Policy Suite 5.5.1 Operations Guide for Quantum Policy Server.

This document describes operations, maintenance, and troubleshooting activities for the various VM servers in the Cisco's Quantum Policy Suite. This document assists system administrators and network engineers to operate and monitor the Quantum Policy Server 5.5 and its parts.

This preface covers the following topics:

Readers

This guide is best used by these readers:

- Deployment engineers
- System administrators
- Network administrators
- Network engineers
- Network operators
- Implementation engineers

This document assumes a general understanding of network architecture, configuration, and operations. Instructions for installation and use of QPS 6.0 and related equipment assume that the reader has experience with electronics and electrical appliance installation.

Additional Support

For further documentation and support:

- Contact your Cisco, Inc. technical representative.
- Call the Cisco, Inc. technical support number.

- Write to Cisco, Inc. at support@cisco.com
- Refer to your other documents.

Terms and Definitions

This document uses certain terms and definitions specific to the QPS software application. Please refer to our common Glossary.

Quantum Policy Server Operations

Revised: September 30, 2013, OL-29748-01

This chapter covers the following topics:

Starting and Stopping

On the advisement of your support staff, you may want restart the Quantum Policy Server because of troubles seen in logs or perhaps performance issues. This section describes several start and stop tasks for the Quantum Policy Server.

Restarting the Quantum Policy Server

This operation stops and restarts the software modules and components.

Step 1 Restart sessionmgr, the session database, with these commands:

service sessionmgr-27717 stop

service sessionmgr-27717 start

service sessionmgr-27718 stop

service sessionmgr-27718 start

service mongodb-27719 stop

service mongodb-27719 start

service mongodb-27720 stop

service mongodb-27720 start

service mongodb-27731 stop

service mongodb-27731 start

Step 2 Restart the Quantum Policy Server with this command:

service qns restart

Step 3 Restart SVN with this command:

service httpd restart

Step 4 Restart the Quantum Policy Builder client with these commands:

service qns restart

Step 5 Restart Load Balancer with these commands:

- RADIUS: service qns restart
- SSL: service stunnel restart
- DHCP: service ldirectord restart
- HA VIP Failover: service heartbeat restart
- All Other: service haproxy restart

Shutting Down the Quantum Policy Server

If you need to shut down the Quantum Policy Server, you can do so from the console or logged in as the root user.

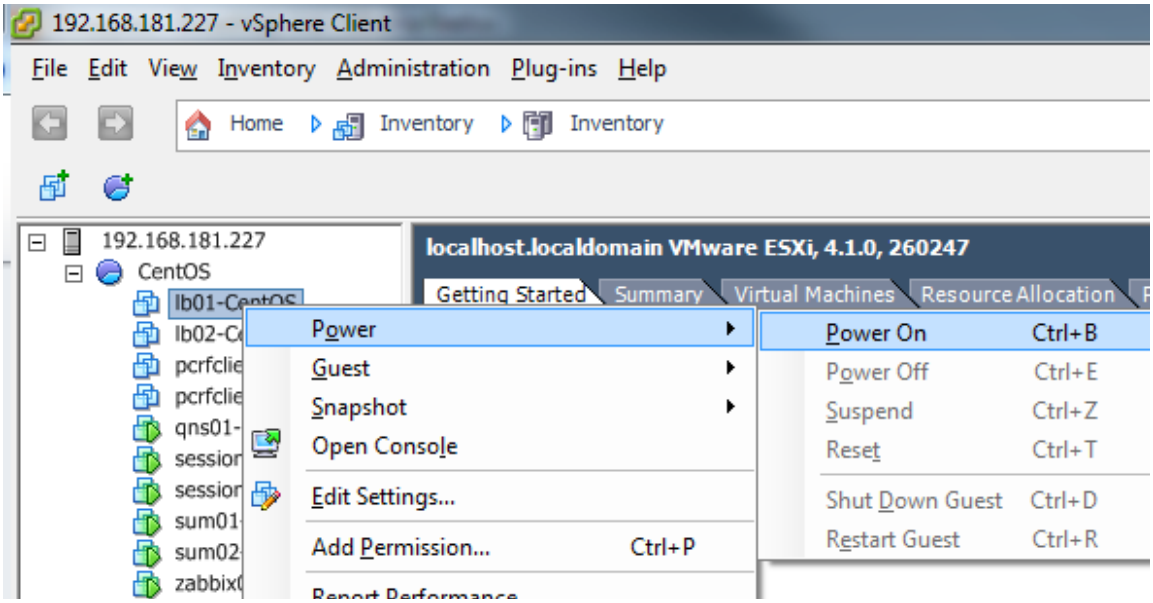
To shutdown from the Linux command line, log in as `root` and use the `init` command:

init 0

Starting VMware

Step 1 Start a VMware vSphere session.

Step 2 Right-click on the VMware ESXi IP address on the left and select Power On.



Rebooting a VM

Occasionally, you may be asked to bounce a VM server. To stop and restart a VM from the Linux command line, use the `init` command as shown:

```
init 6
```

Switching Active and Standby

In QPS, the active and standby strategy applies only to the secondary (02) load balancers. Recall that the four load balancers are in the system are these:

lb01

lb02

portallb01

portallb02

Determining the Active Load Balancer

- For the couples lb01 and lb02 and portallb01 and portallb02, the active load balancers have the Virtual IPs (vips) active.
- Run the command `ifconfig` to return the addresses assigned to the interfaces eth0:0 (or eth0:1) and eth1:0 (or eth1:1).
- Equivalently, run the command `ip addr` to return secondary IP addresses (the VIPs) assigned to eth0 and eth1.

Determine the Standby Load Balancer

The passive or standby load balancer is the system which does not have active VIPs.

Determine Standby Function and Statefulness

- The standby load balancer is available via tcp/udp (or icmp). Ping or ssh to the machine.
- The standby load balancer shows "running..." as the return to the command `service heartbeat status`.

Backing Up and Restoring

As a part of routine operations, you will need to have backups and may need to restore them. This section describes several backup and restore tasks for the databases for Quantum USuM, SessionMGR, and SVN.

- Backing Up and Restoring the Databases
- Backing Up SVN

Backing Up and Restoring the Databases

For more information, see the document *Quantum Policy Suite 6.0 Backup and Restore Guide*.

Backing Up SVN

Backup up the SVN repository is performed within SVN itself.

Step 1 Download and install Tortoise SVN (or any other SVN client).

Step 2 Connect to `http://<svn_IP_here>/repos/`.

Step 3 Check out the configuration and run directories.

The run directory contains the runtime information for the Quantum Policy Server. The configuration directory contains the Quantum Policy Builder client information.

Step 4 The default login for this is broadhop/broadhop.

Adding or Replacing Hardware

Hardware replacement is usually performed by the hardware vendor with whom your company holds a support contract.

Hardware support is not provided by Cisco. The contact persons and scheduling for replacing hardware is made by your company.

Before replacing hardware, see if you have a recent backup. If not, try to make a backup now. See Backing Up and Restoring.

Unless you have a readily available backup solution, use VMware Data Recovery. This solution, provided by VMware under a separate license, is easily integrated into your QPS environment.

New installations to new hardware can be performed a couple of different ways, but the most common is to install via virtual machine templates VMware ESXi.

See Quantum Policy Server Deployment Start to Finish.

The templates you download from the Cisco repository are partially pre-configured but require further configuration. Your Cisco technical representative can provide you with detailed instructions.

Note You can download the VMware software and documentation from the following location:

www.VMware.com

Publishing Data

This section describes publishing Quantum Policy Builder data to the Quantum Policy Server.

Publishing data occurs in the Quantum Policy Builder client interface, but affects the Quantum Policy Server.

The Configuration Guide for Quantum Policy Builder, discusses publishing to the server in detail. Please refer to that document. You will have to log in to the Quantum Policy Builder to publish data.

Quantum Policy Builder manages data stored in three areas:

- The Client Repository stores data captured from the Policy Builder GUI locally. This is a place where trial configurations can be developed and saved without affecting Quantum Policy Builder server data.
- The Updates Repository stores information on where to find software updates, including their URIs.
- This is the area that affects the Quantum Policy Server:

  The Server Repository stores configuration data about policies, system configuration, and subscriber servers after it is checked into a version control software. The server takes its data from this repository after you have used the Publish option.

You are concerned with the Server Repository data for this operation.

Version Control Software

Before setting up your client repository sites, version control software is installed and available. Users do not use version control software directly. Rather, the Quantum Policy Server uses is for publishing of repository data.

In the Quantum Policy Server, a Subversion server is located at http://pcrfclient01/repos/trunk/main.

QPS comes with the Subversion version control software. You can use your own copy of Subversion server, but not another version control software product such as IBM® ClearCase®.

Setting Debug Levels

Setting debug levels for QPS occurs in Zabbix, the third-party monitoring software QPS uses. Open a Zabbix session and set them there.

You can also edit the logback.xml file to set QPS debugging levels.

Step 1 Edit the logback.xml file in the `/etc/broadhop` directory and the `logback.xml` in the `/etc/broadhop/controlcenter` directory.

Start by looking at the `/etc/broadhop/logback.xml`. It will have a section that looks similar to this:

```
<!-- Configure Loggers -->

 <!-- Hide 'Could not load class...' noise. -->

 <logger
    name="org.springframework.osgi.extensions.annotation.ServiceReferenceDependencyBeanFa
    ctoryPostProcessor" level="error" />

 <logger name="org.springframework" level="warn" />

 <logger name="com.broadhop.resource.impl" level="warn" />

 <logger name="com.danga" level="warn" />

 <logger name="httpclient.wire" level="warn" />

 <logger name="org.apache.commons.httpclient" level="warn" />

 <logger name="sun.rmi.tranrsport.tcp" level="warn" />

 <logger name="org.apache.activemq.transport.InactivityMonitor" level="warn" />


  <!-- Configure default Loggers -->

  <root level="warn">

    <appender-ref ref="FILE" />

    <appender-ref ref="SOCKET" />

 </root>
```

Note The level is configurable to error, warn, info, or debug in order of least logging to most logging. When debugging an issue or upon initial installation, it is most helpful to set the logging level to debug.

- To change logging level, change one of the levels or add additional categories, which may involve help from a Cisco support representative.

Step 2 Look at the `/etc/broadhop/controlcenter/logback.xml`. It will have a section that looks similar to this:

```
<!-- Configure Remote Logger -->

<logger name="remote" level="info" additivity="false">

  <appender-ref ref="CONSOLIDATED-FILE" />

  <appender-ref ref="CONSOLIDATED-JMX" />

</logger>
```

Again, it may be helpful to set this level to `debug` for initial installation purposes, but no other changes are necessary for this file.

After your system is up and running, it is most useful to turn the system to either `error` or `warn`. The levels `debug` or `info` usually have logs rollover very quickly. After the log rolls over, the information is lost. For this reason, `warn` or `error` generates a substantially smaller amount of logging, and gives you the ability to look for issues over a longer period of time in the system.

Synchronizing Times

This section explains how to synch time between all of the QPS services so they all have the same clock reading.

System times are synchronized from lb01 and lb02.

All VMs point their NTP to lb01 and lb02 for time sync. Both load balancers are preconfigured to look out to internet-based NTP pools. If pools are unavailable, you must set this manually, as follows:

- If lb01 and lb02 HAVE access to a valid NTP server, log in to lb01 and lb02 as root and run:

  service ntpd stop

  ntpdate -b <ntpserverip>

- Replace `<ntpserverip>` with a valid IP. This sets the system date.

  hwclock --systohc

  This will sync the hardware clock (VMWare BIOS) to the system time.

  `date` (to check if the date is actually correct)

  `hwclock` (to check if the hw clock is actually correct)

- Edit `/etc/ntp.conf` and search for lines beginning with server.

  There should be 3 lines pointing to NTP pools. Replace these lines by the <ntpserverip> above (i.e., if <ntpserverip>=172.31.32.33, then the only server line in the .conf file should read: server 172.31.32.33

  service ntpd start

- If lb01 and 02 DO NOT HAVE access to a valid NTP server, log in to lb01 and lb02 as root and run:

service ntpd stop

date -s "2004-02-29 16:21:42

- Replace the example date with the real one. This sets the system date.

  hwclock --systohc

  This syncs the hardware clock (VMWare BIOS) to the system time.

  `date` (to check if the date is actually correct)

  `hwclock` (to check if the hw clock is actually correct)

  service ntpd start

Minor Time Synch Result

The system times on the remaining QPS servers will slowly, over hours or days, be brought into proper time by NTP if the system time is slightly off, slightly meaning maybe 30 minutes or so.

Major Time Sync Result

If other system times are off by more than 30 minutes, NTP may never converge times. Better practice is to set the system times manually for each individual server. Run the script below from lb01. Time will be in sync as close as the time it takes you to type the root password.

lb02	portal01	sessionmgr01	qns01
	portal02	sessionmgr02	qns02
pcrfclient01	portallb01		qns03
pcrfclient02	portallb02		qns04

Log in to each server as listed above and run this command:

```
MYDATE=$(date); ssh $server "service ntpd stop;date -s
\"${MYDATE}\";service ntpd start;hwclock --systohc";done
```

Quantum Policy Server Deployment Start to Finish

An operation that all deployments use, but usually only once or twice, is the deployment process. This operation is provided here in the event you are asked to reinstall the Quantum Policy Server, perhaps to move it to another piece of hardware.

Note In a full-environment, this operation needs to be performed on each of the VMs.

Use these two procedures to do a basic Quantum Policy Server deployment at your site:

- VMware® vSphere™ Hypervisor™ Install and Configuration
- OVF Template Deployment

VMware® vSphere™ Hypervisor™ Install and Configuration

Install VMware ESXi 4.1+

Step 1 Download and request a free license from VMware at:

http://www.vmware.com/go/get-free-esxi

For further clarification, refer to the VMware vSphere Hypervisor Install Guide at:

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esxi_i_vc_setup_guide.pdf

Step 2 Burn the ISO to a disk.

Step 3 Boot your server off of the ISO disk.

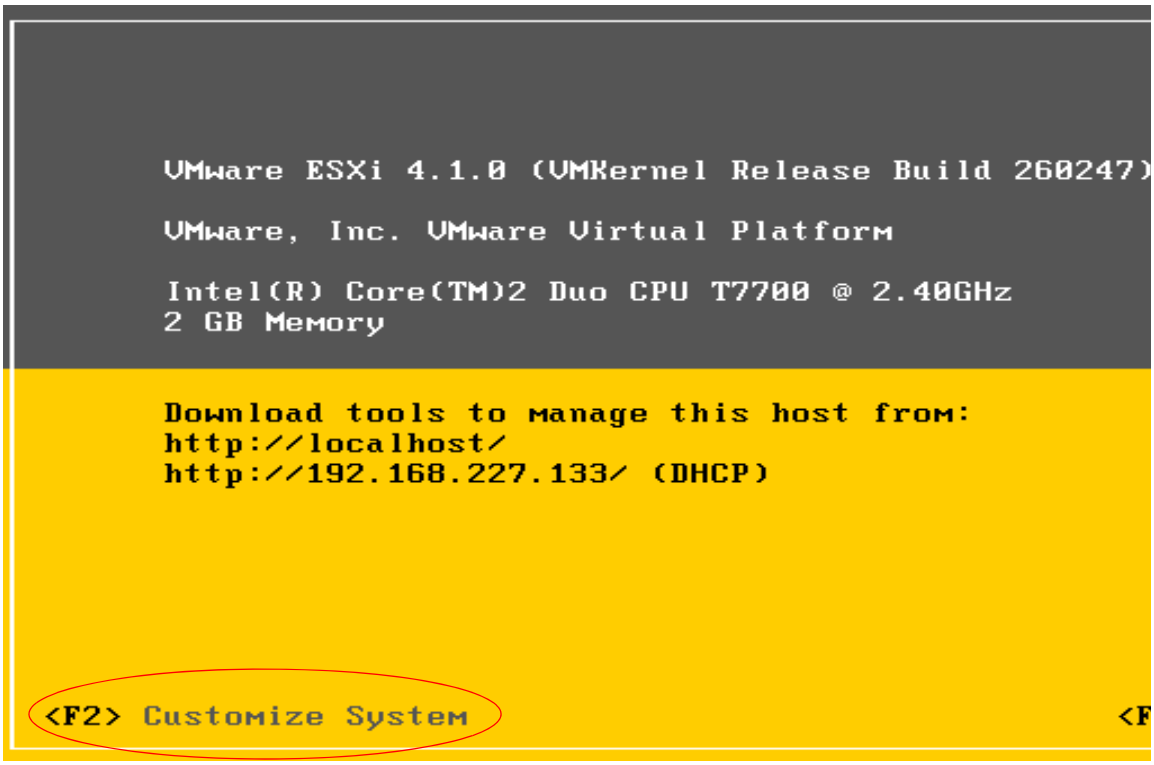
Please refer to your server's owners manual for directions on how to change the boot order.

Step 4 Run the installer and accept all the defaults.

Configure VMware ESXi 4.1+

Step 1 Connect a keyboard and monitor to your newly installed ESXi server.

Step 2 Press F2 to customize the system.

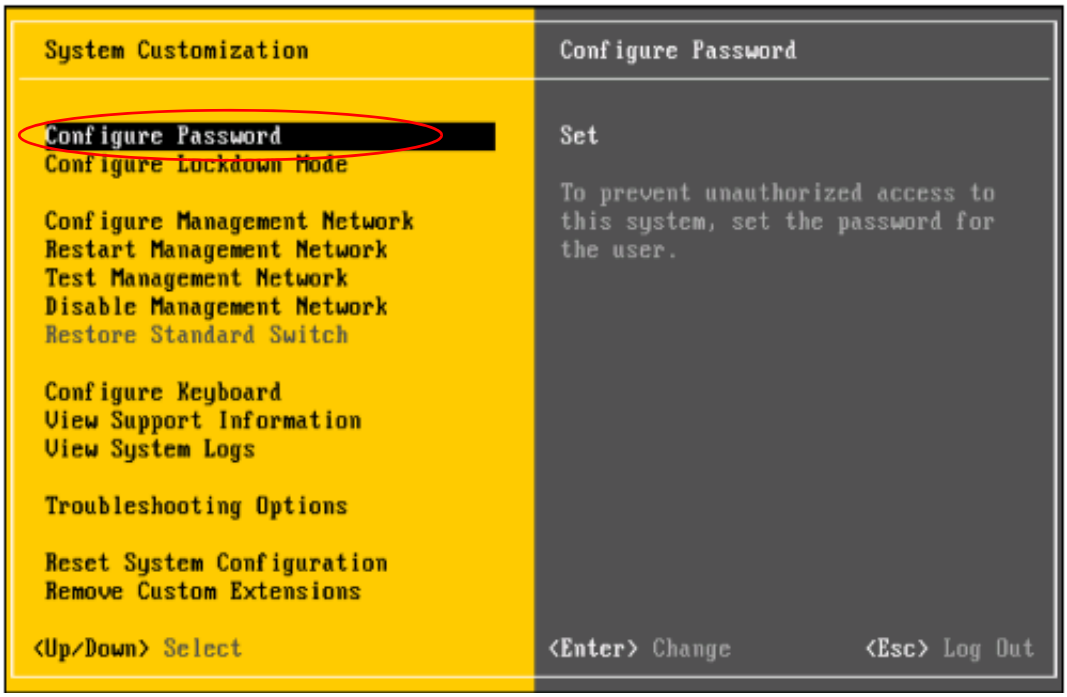


Step 3 When prompted for a user name and password:

- Type `root` as the user name.

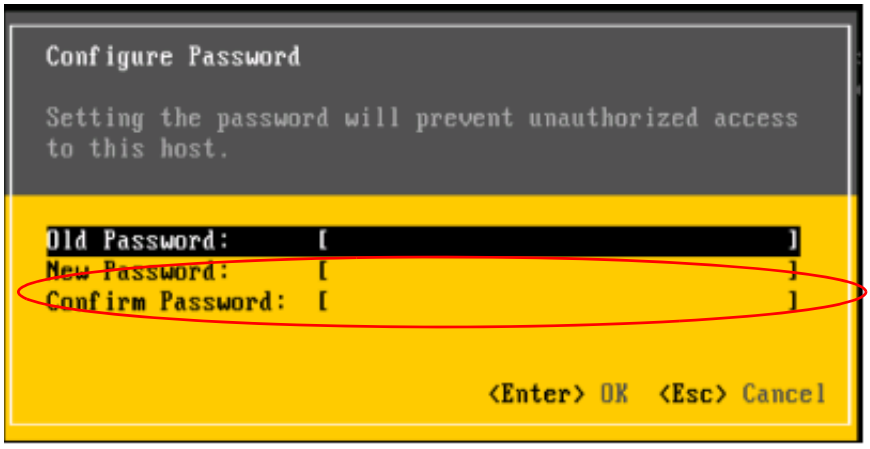
- Leave the password blank.
- Press OK.

Step 4 Select Configure Password from the System Customization menu to configure the password to broadhop.



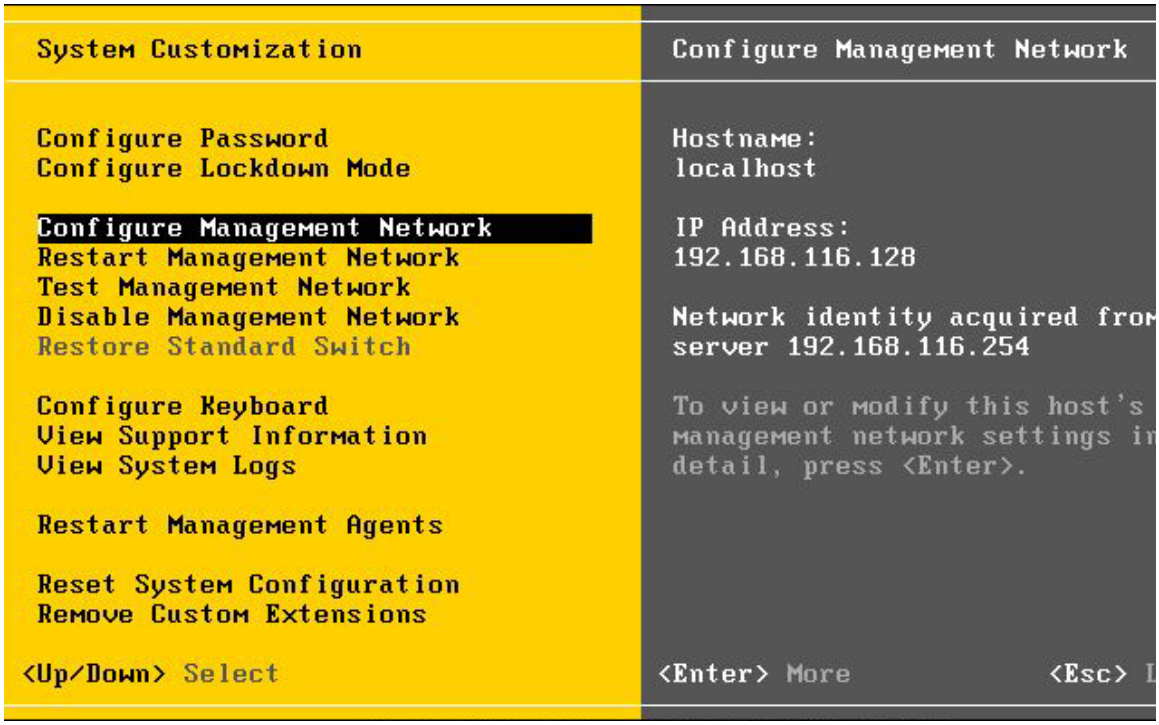
The Old Password is blank.

Step 5 For the New Password and Confirm Password, type broadhop.

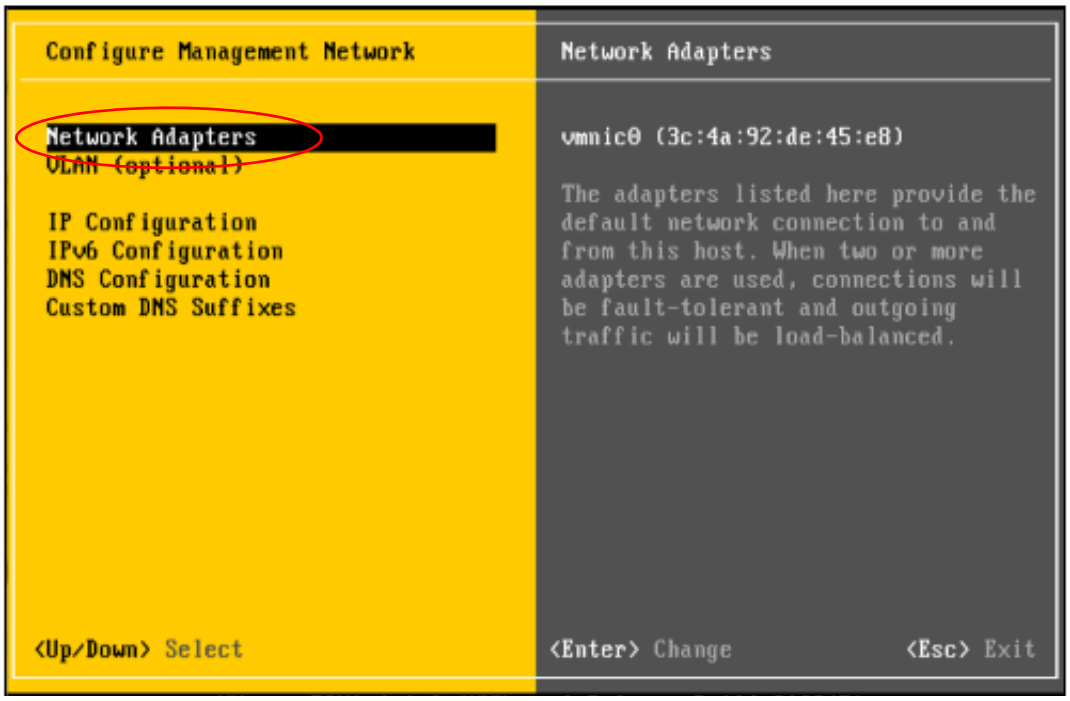


Step 6 Configure the network interface to which you will connect your ESXi client.

Step 7 Select Configure Management Network from the System Configuration menu.



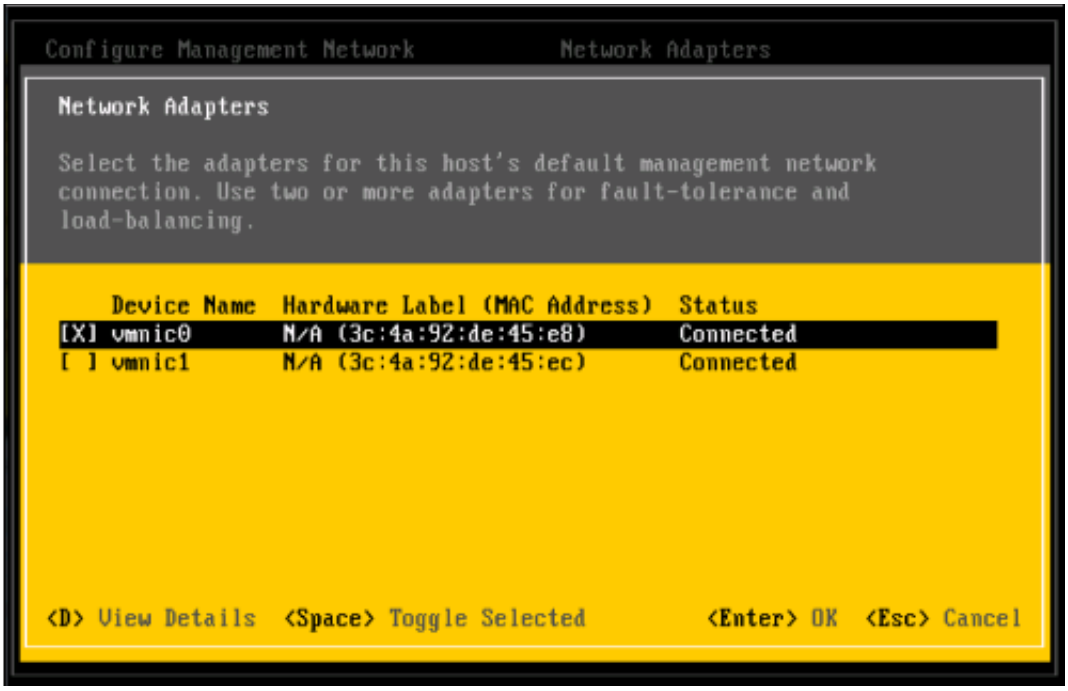
Step 8 Make sure you select the correct Network Adapter on which your management interface will reside.



In this example, there are only two network interfaces.

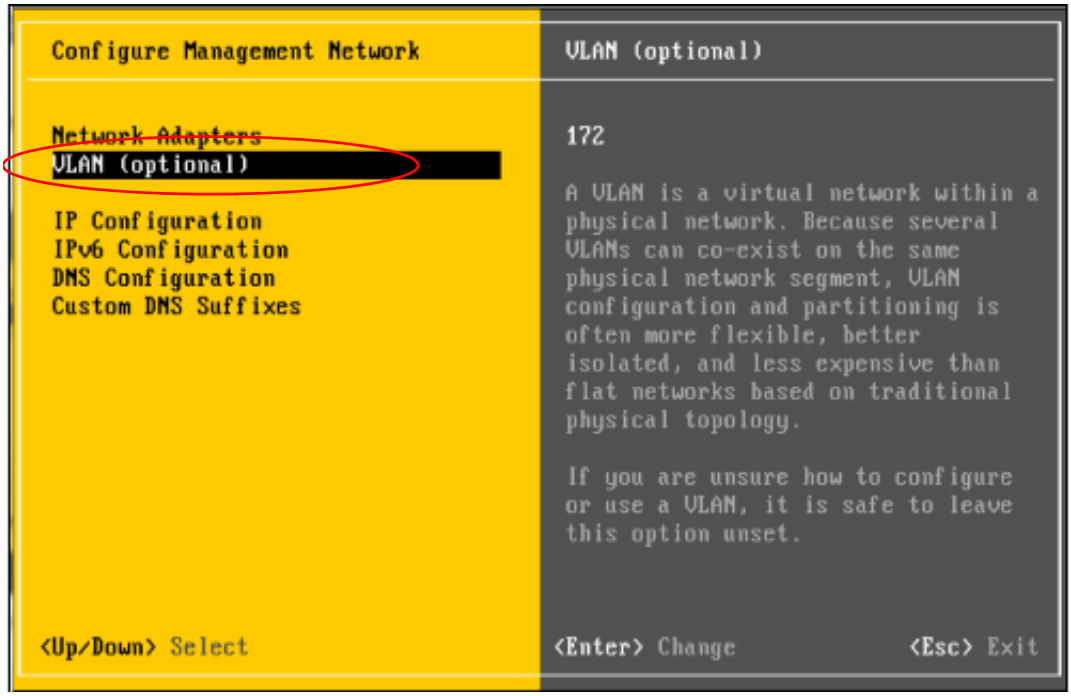
Define the first physical network interface as the management interface.

Step 9 Highlight the physical interface you wish to use and select it with the spacebar.



Step 10 Optional: If there is a flat network there is no need to configure a VLAN.

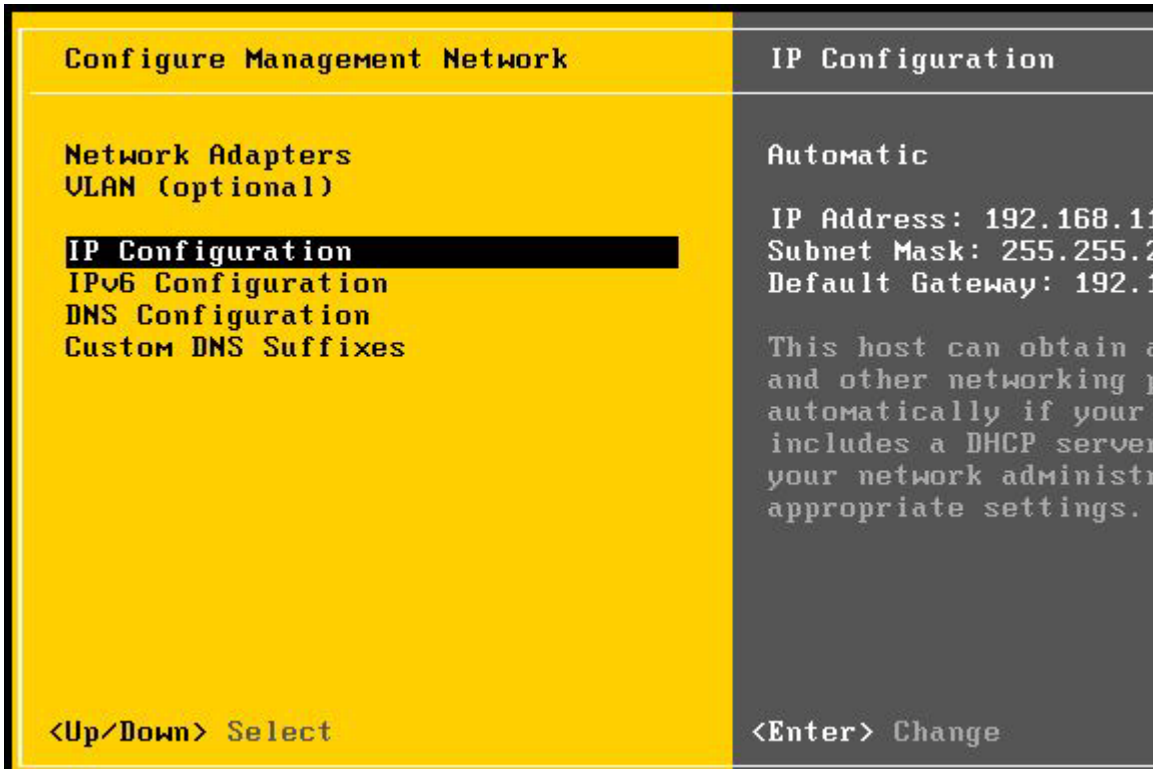
To configure a VLAN, select VLAN from the Configure Management Network menu.



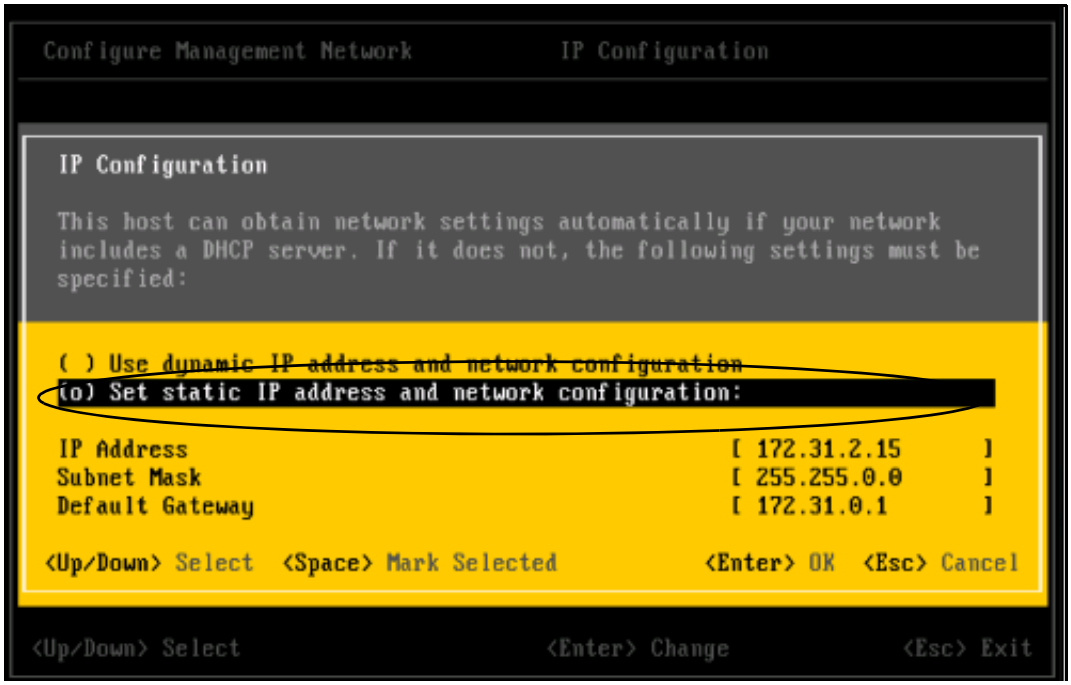
For this example the ESXi host's management interface is on vlan 172.

Step 11 Type your own interface ID and press Enter.

Step 12 Setup the IP address for the ESXi server. Select IP Configuration from the Configure Management Network.



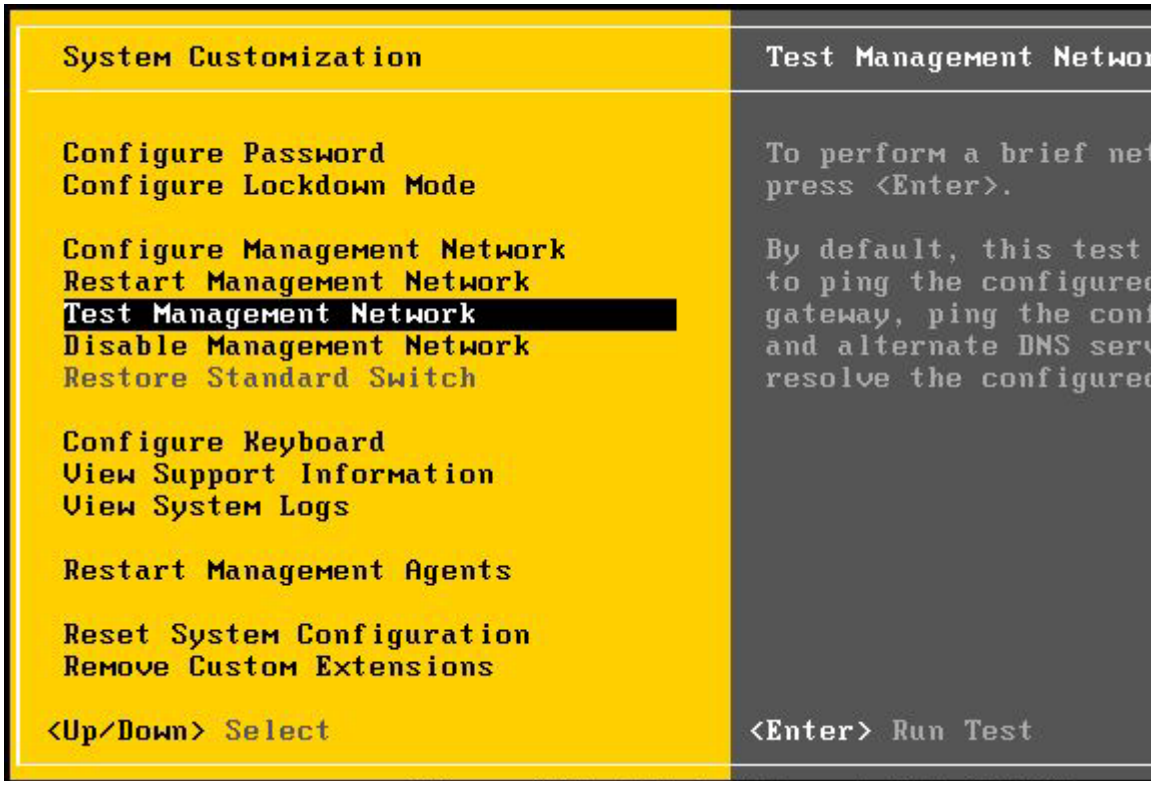
Step 13 On the IP Configuration screen, make sure Set static IP address and network configuration is selected, then fill out the IP address, subnet mask, and gateway information.



Step 14 Select yes or OK to restart the network management agents.

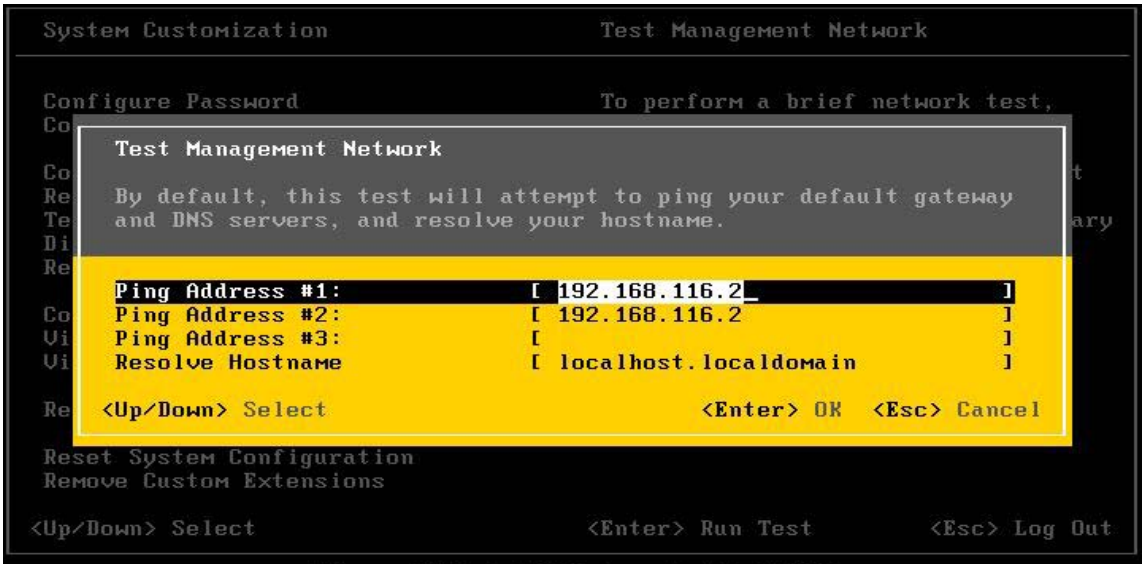
Test your management network and make sure you can ping the default gateway.

Step 15 Select "Test Management Network" from the configuration screen.



Step 16 Enter the gateway IP address and press OK.

The reply should come back OK.



Step 17 If you get a ping reply, then continue on to OVF Template Deployment.

OVF Template Deployment

This section helps you deploy or install the OVF templates required to run the virtual machines at your site.

- Install vSphere Client
- OVF Template Location
- Import OVF Templates

Install vSphere Client

Step 1 When your ESXi server is connected to your network, open a browser and point to the IP address of your ESXi server:

https://esxi_ip_address_here/

Step 2 Click on the "Download vSphere Client" link.

Step 3 Run the installer and accept the defaults.

OVF Template Location

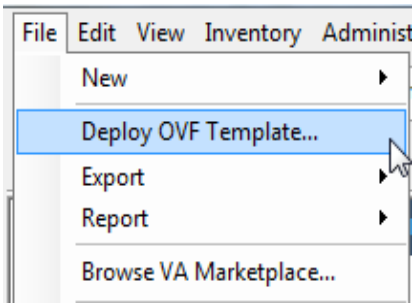
To obtain the OVF templates, contact your Cisco technical staff. These templates are kept inside the Cisco firewall on Confluence for security and ease of update.

Import OVF Templates

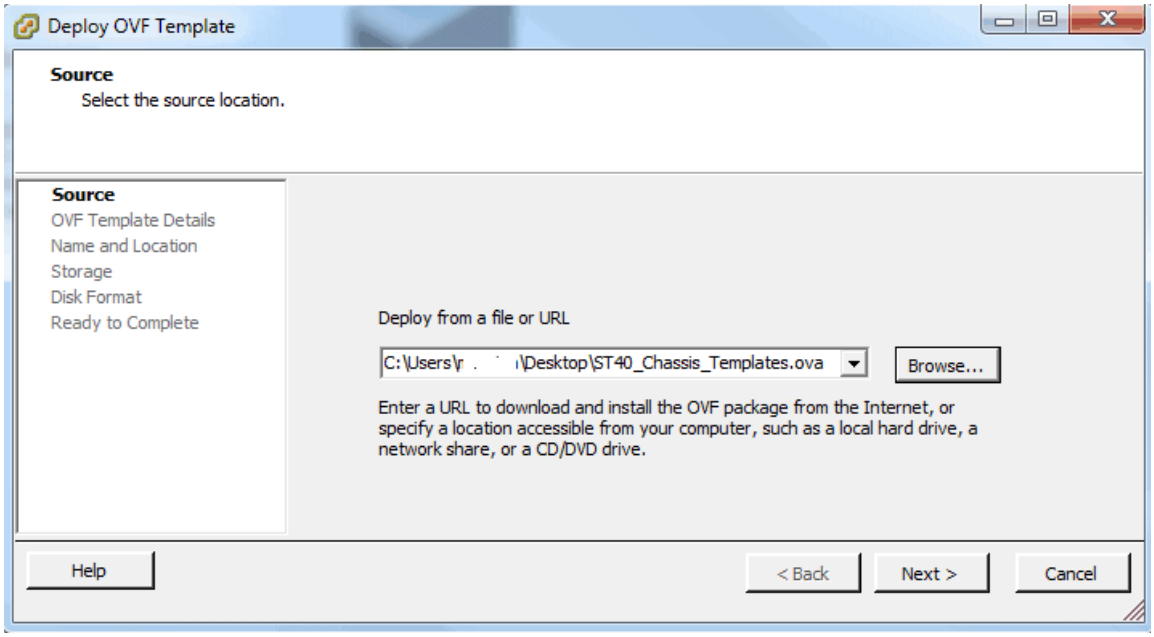
Step 1 Start your vSphere Client.

Step 2 Enter the IP address of your vSphere Hypervisor Server along with the user name and password.

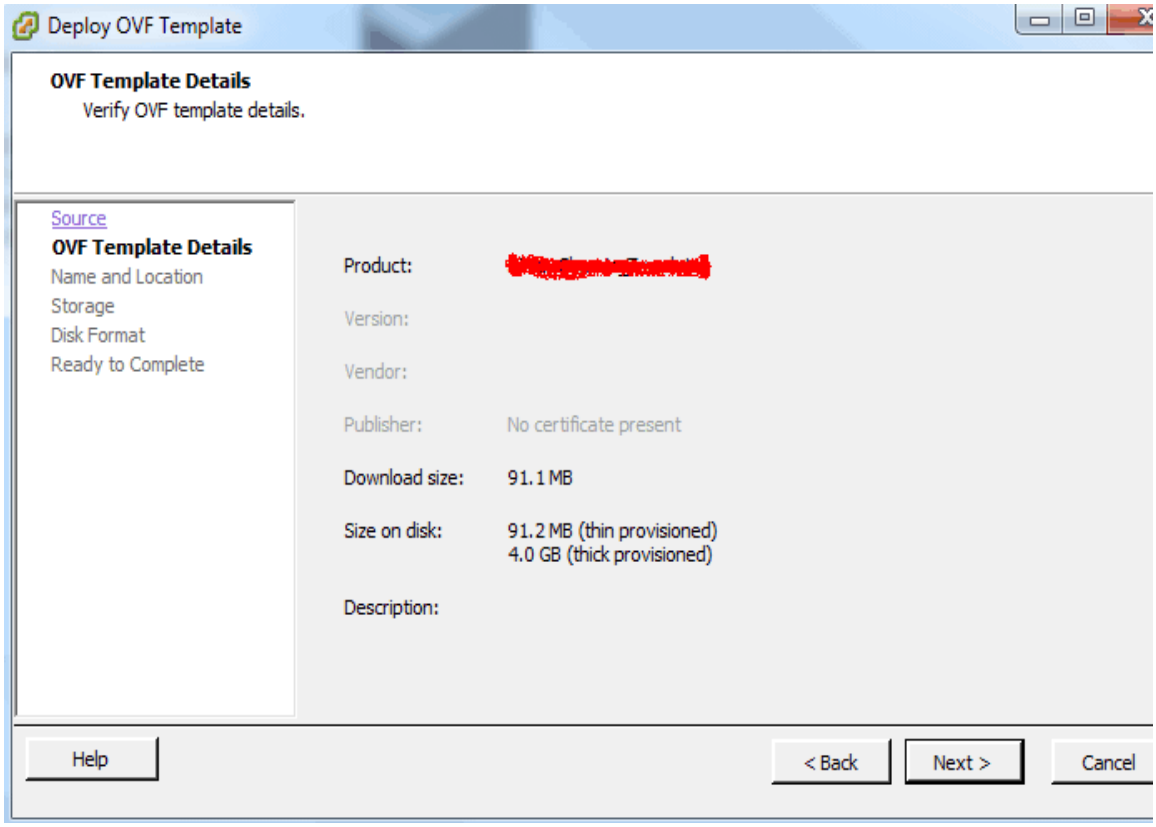
Step 3 When authenticated, select File > Deploy OVF Template.



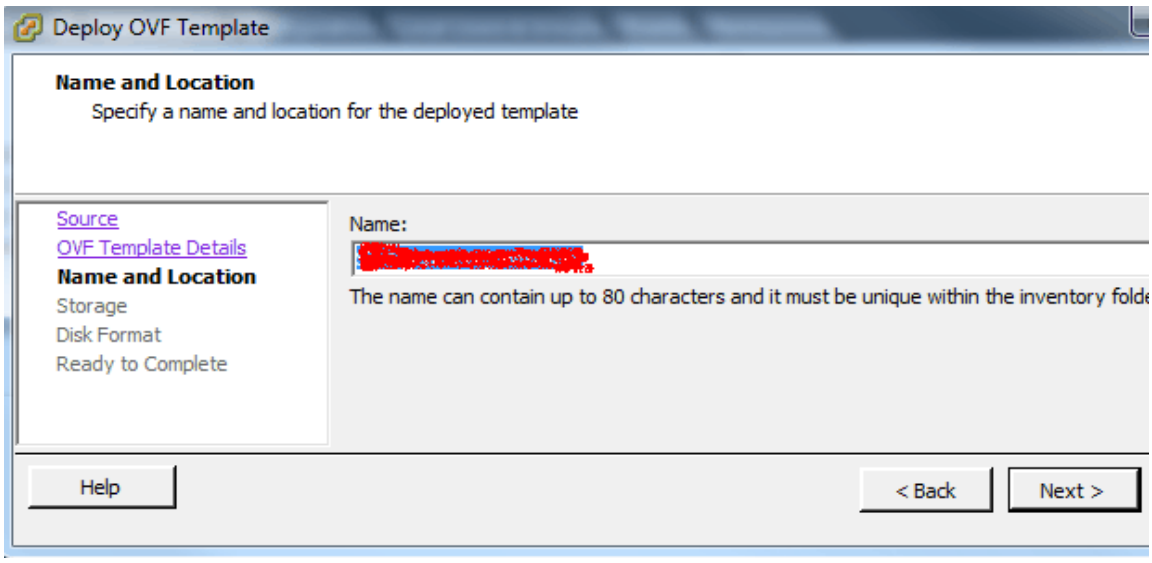
Step 4 Select the location of the OVF Template on your local machine.



Step 5 Press Next to verify the details of the OVF Template.



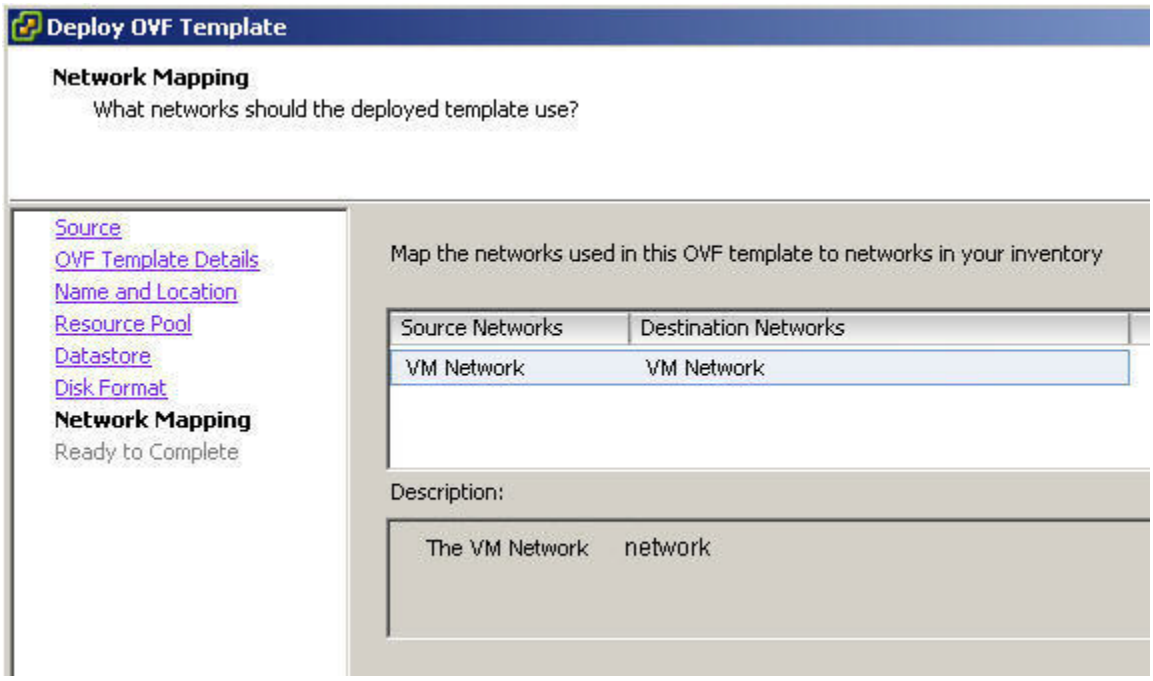
Step 6 Press Next to enter a name for this OVF Template in the Name field.



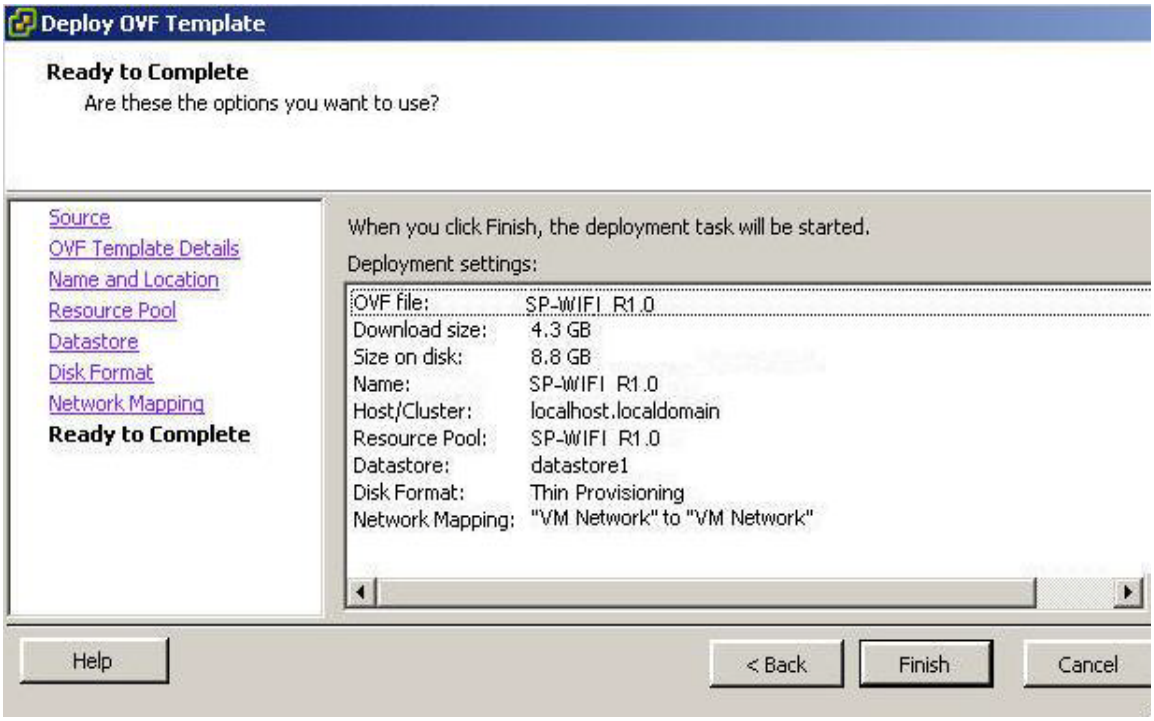
Step 7 Define which datastore to deploy on. In most situations, deploy on datastore1.

Step 8 Decide if you want to deploy the images in Thin Mode or Thick Mode and choose that radio button. All VMs can be deployed in Thin Mode except for the SessionMGR VMs.

Step 9 Map the physical interfaces to the virtual networks configured in VMware. This example assumes a flat network with a single network interface, although this value can be changed later.



Step 10 Confirm all of your options and press Finish.



Managing Subscriber Data

Subscriber Management with AAA

Please see the documentation for your AAA server.

Subscriber Management with USuM

Please use the documentation that comes with Cisco Unified SuM, available through your Cisco technical representative.

Additional Documents

Other documents are available for your use as a Quantum Policy Server administrator.

In addition to this guide, you may want to have these documents available:

- Alarming and SNMP Guide
- QNS Troubleshooting Guide
- Blueprint Solution documents specific to your enterprise
- Monitoring Guide

Updating the Installation

Revised: September 30, 2013, OL-29748-01

This chapter describes how to perform software updates for QPS 6.0. Installation steps must be performed before any updates.

This chapter covers the following topics:

Initial Upgrade

Use these steps if you have never performed an install.

These steps are for an initial installation, that is, from versions of 5.3 pre-Feb 10th, 2012.

Note Release 5.1/5.2 upgrade is currently unsupported. If you have a version obtained before this, use the previous install guide, version 2.0.

If you do not currently have the updated /opt/broadhop/installer directory (check for /opt/broadhop/installer/.git), you can use these installation instructions.

In summary:

- get update tar.gz and cisco-sp-wifi.tar.gz into /var/tmp
- Unzip and use the stage_updates.sh script inside to bootstrap the install (after this update you can use: /opt/broadhop/installer/stage_updates.sh without unzipping)

  cd /var/tmp

- Find the latest yum repository (System RPM updates)

  wget
  http://updatesite.broadhop.local/dev/yum.repository/trunk_zip/broadhop_3p_repository-latest.tar.gz

- Grab the latest SP Wifi (QPS/Portal/Installer) Software

  wget http://updatesite.broadhop.local/customer/cisco-sp-wifi.tar.gz

Note Please contact your local Cisco Technical representative in case you are not able to download the software.

- Unzip

  tar zxvf cisco-sp-wifi.tar.gz

  tar zxvf cisco-sp-wifi/installer-r*.tar.gz

- Install software

  installer/update_rpm_repo.sh

  broadhop_3p_repository-latest.tar.gz

- Stage updates (say yes to update_vms and update_qps)

  installer/stage_update.sh cisco-sp-wifi.tar.gz

Normal Update Procedure

Use these steps if you have performed an initial installation as above.

- Stash existing changes - needed until scripts are updated
- Grab the latest SP Wifi

  cd /var/tmp

Note Before doing the `wget` below, make sure that a cisco-sp-wifi.tar.gz files does not exist or the `wget` will create a cisco-sp-wifi.tar.gz.1

  wget http://updatesite.broadhop.local/customer/cisco-sp-wifi.tar.gz

Note Please contact your local Cisco Technical representative in case you are not able to download the software.

- Tell QPS to update (say 'y' to all steps)

  /opt/broadhop/installer/stage_update.sh

  /var/tmp/cisco-sp-wifi.tar.gz

Expanding the Deployment

Revised: September 30, 2013, OL-29748-01

This chapter covers the following topics:

Note The host addresses used in the examples may be different for your deployment.

Expanding Architecture for Scalability

For future installations and network upgrades, this section proposes what hardware and components you should consider as you grow your network.

The Quantum Policy Server solution is a robust and scalable software-based solution that can be expanded by adding additional hardware and software components. The following sections explain typical scenarios of when to expand the hardware and software to effect such growth.

Typical Scenarios When Expansion is Necessary

Your network may grow for the following reasons:

- The subscriber base has grown or will grow beyond the initial installation specifications.

  In this case, the number of active or non-active subscribers becomes larger than the initial deployment. This can cause one or more components to reach capacity. New components must be added to accommodate the growth.

- The services or subscriber scenarios have changed, or new services have been introduced, and the transactions per second on a component no longer meet requirements.

  When a new service or scenario occurs, often there is a change in the overall Transactions Per Second (TPS), or in the TPS on a specific component. When this occurs, new components are necessary to handle the new load.

- The operator notices that there are factors outside of the initial design that are causing either the overall system or a specific component to have a high resource load.

  This may cause one or multiple components to reach its capacity for TPS. When this occurs, new components are necessary to handle the new factors.

Hardware Approach to Expanding

Adding a new component may require adding additional hardware. However, the addition of more hardware depends on the physical resources already available, plus what is needed for the new component.

High Availability (HA) Consequences

When adding more hardware, the design must take into consideration the high availability needs (HA) of the system. The HA design for a single-site system is N+1 at the hardware and application level. As a result, adding a new blade incrementally increases the HA capacity of the system.

For example, in a basic installation there are 2 Quantum Policy Server blades handling the traffic. The solution is designed so that if one of the blades fails, the other blade can handle the entire capacity of the system. When adding a third blade for capacity expansion, there are now 2 blades to handle the system load if one of the blades fails. This allows for a more linear scaling approach because each additional blade can be accountable for being able to use its full capacity.

Note When adding new blades to a cluster, the blades in the cluster must be co-located to achieve the proper throughput between other components.

Adding a New Blade

To add new blade hardware,

Step 1 Log in to the Control Center 01 component on the Control Center Blade 1.

Step 2 Through SSH or through the vSphere Client console, go to the directory

/etc/broadhop/scripts/installation

and make sure the esx.conf file has the extra lines needed for the components. See Appendix A, “File Examples” for an example of the `esx.conf` file.

Step 3 When the configuration file changes are complete, run the `install_esx.sh` script to install the new blade and components. The script recognizes the additional components and installs them into the environment.

Step 4 After the script finishes, go to the new blade(s) and log in using the vSphere Client, and start each component.

Component Approach to Expanding

The most common components to be expanded are on the Quantum Policy Servers. As your system begins to scale up, you will need to add more QPS nodes and more SessionMgrs. Expansion for other components can follow the same pattern as described here. The next sections discuss the configurations needed for those specific components to be active in the system.

Adding Additional Component

All new components must be added to the `/etc/hosts` file on Control Center 01 and synchronized to all of the other components using `/opt/broadhop/qns/bin/synconfig.sh`.

Note For specific components, additional configuration is necessary.

Additional portal components must be added to the Portal Load Balancer configuration.

Step 1 Use `ssh` or the vSphere Client console to access the command line on the Portal Load Balancer 01. Edit the `/etc/haproxy/haproxy.conf` file.

```
listen portal_proxy lbpvip01:80

mode http

source 0.0.0.0 usersrc client

cookie SERVERID insert nocache indirect

server portal01 portal01:80 weight 1 cookie portal01 check

server portal02 portal02:80 weight 1 cookie portal02 check
```

Step 2 If another portal03 and portal04 are added, the following lines need to be added to the file:

```
server portal03 portal03:80 weight 1 cookie portal03 check

server portal04 portal04:80 weight 1 cookie portal04 check
```

Step 3 To complete the task, run this command from the CLI:

```
service haproxy restart
```

Step 4 Next, perform the same steps on the Portal Load Balancer 02.

As new features or fixes to the solution become available, Cisco posts newer software to the Cisco web site for download. Use the Cisco web site to download `a.tgz` file to your local machine and then upload to the Control Center 01 system into the `/var/broadhop/repositories/cisco-sp-wifi` directory. Untar it using `tar xfz` and a compatible file name.

Expanding Architecture for Geographic Redundancy

To handle a complete failure of a QPS cluster or the loss of a data center hosting a QPS, the QPS may be deployed in geo-redundant QPS clusters in which two or more QPS clusters are deployed in multiple sites and linked together for redundancy purposes.

QPS supports both active-standby and active-active geo-redundant architectures. In an active-standby model, one site is the designated primary site carrying load (active). The secondary, backup sites are only used in the event of failure of the active site.

In an active-active model, all sites within the geo-redundant cluster actively carry traffic, but are dimensioned with sufficient capacity to handle the additional traffic load in the event of a site failure of geographic proportion.

In the event of a site failure, the PCEFs need to be treated as follows:

- They must be configured to automatically detect a site failure and switch to the standby QPS cluster

  or

- They must be able to be switched through manual intervention

Similarly, it is the responsibility of northbound systems (for example, provisioning systems) to detect site failures and support either switching or reconfiguration to the standby QPS cluster as necessary.

Data Synchronization

Geo-redundancy is achieved by synchronizing data across the sites in the cluster. Three types of data is replicated across sites:

- Service and policy rule configurations
- Subscriber data that are stored in the Quantum Unified SuM component
- Balance data stored in the Quantum MsBM component

In addition, active session data stored in the Session Manager component may also be synchronized across sites when network conditions permit. Active session data is the most volatile data in QPS and has the most stringent synchronization requirements. Session replication across sites has these requirements:

- Internal QPS VMs in both of the geographically dispersed sites must exist in the same VLAN.
- Bandwidth must be on a 40MBps link or faster.
- Latency must be less than 10 milliseconds.
- Packet loss must be less than 0.1%.

QPS utilizes a unicast heartbeat between sites in the geographic redundant solution. The heartbeat allows the session manager components to

- Know which is the currently active component.
- Protect against a split-logic scenario where data is accepted at more than one session manager component, possibly causing data corruption.

An additional external component called an arbiter provides a tie-breaking vote as to which of the session managers is the current master. This external component is required to reside on a separate site from the primary and secondary sites and must be routable from both sites. An arbiter ensures that if one of the sites is lost, the arbiter has the ability to promote the standby site's session manager to be the master.

To support this architecture, sessionmgr01, sessionmgr02, sessionmgr03, sessionmgr04 and arb01 must be able to route to each other across the sites across the following ports:

27717 - sessions

27718 - balance

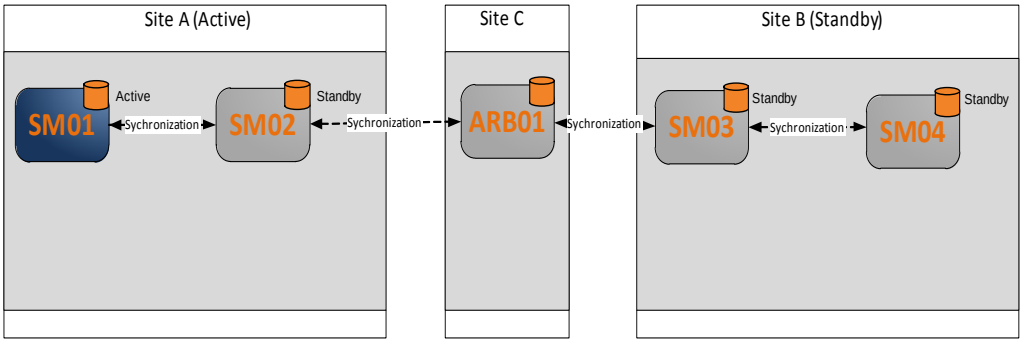
27719 - SPR

27720 – SPR

Typically this routing is done over the signaling traffic interface because there are other requirements relating to the Policy Directors that have the same routing requirements.

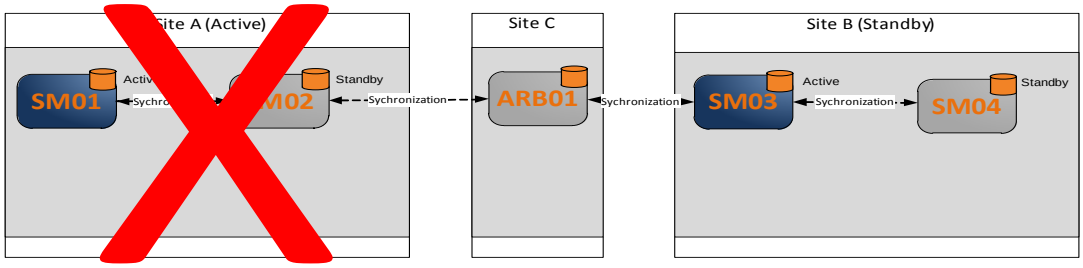
Figure 4-1 shows a detailed example of the data synchronization architecture for subscriber, balance, and session data.

Figure 4-1 Synchronization Architecture for Subscriber, Balance, And Session Data



In the case of Site A failure, Site B's session manager will become master as shown in Figure 4-2.

Figure 4-2 Session Manager Becoming Master



Active-Standby Mode

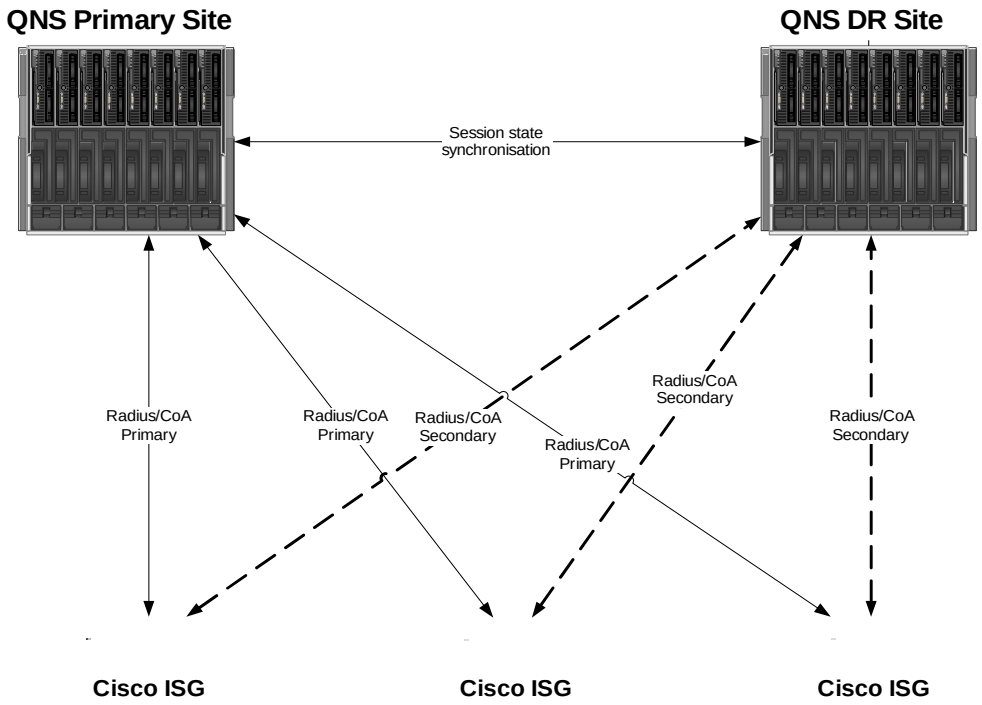
In active-standby mode, one QPS system is active while the other QPS system, often referred to as the Disaster Recovery (DR) site, is in standby mode. In the event of a complete failure of the primary QPS cluster or the loss of the data center hosting the QPS, the standby site takes over as the active QPS cluster. All PCEFs use the active QPS system as primary, and have the standby QPS system configured as secondary.

The backup QPS system is "standby" in the sense that it does not receive any requests from connected PCEFs unless the primary QPS system fails, or in the event of a complete loss of the primary site. The backup QPS system is not configured as passive.

If your system uses an external load balancer or Diameter Routing Agent (DRA), the QPS in the active cluster is typically configured in one group and the QPS in the standby cluster is configured in a secondary group. The load balancer/DRA may then be configured to automatically fail over from active to passive cluster.

The active-passive, or Disaster Recovery mode is illustrated in Figure 4-3.

Figure 4-3 Active/Passive HA without External Load Balancer



Active-Active Geographic Clusters

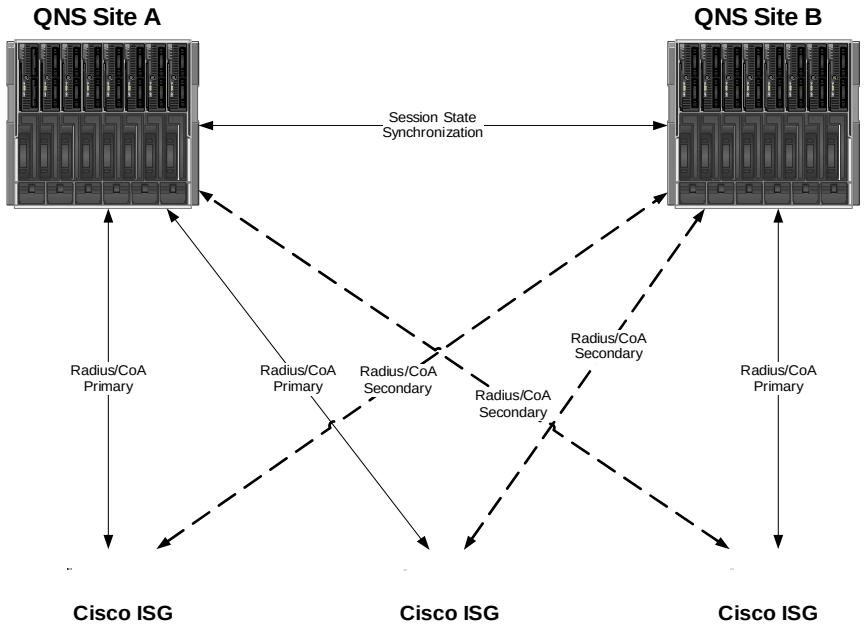
The most common QPS geographically redundant architecture supports two or more QPS active-standby clusters deployed in an active-active configuration across multiple PCEFs. Each site contains the active for the local PCEFs and the other site contains the standby for the remote PCEFs. Each PCEF is configured in active-passive mode with one QPS cluster as primary and another QPS cluster as standby.

As such, the PCEF automatically switches over to the standby QPS cluster if the primary QPS cluster fails. The failure detection is supported in the PCEF or NAS device, perhaps as a result of a connection failure or server busy message.

In the case of either a complete QPS system failure or the loss of the data center in which the QPS system is installed, the second QPS system will process all requests from all subscribers. If the subscriber session state is synchronized between the sites, the failover is stateful and no sessions need to be re-established.

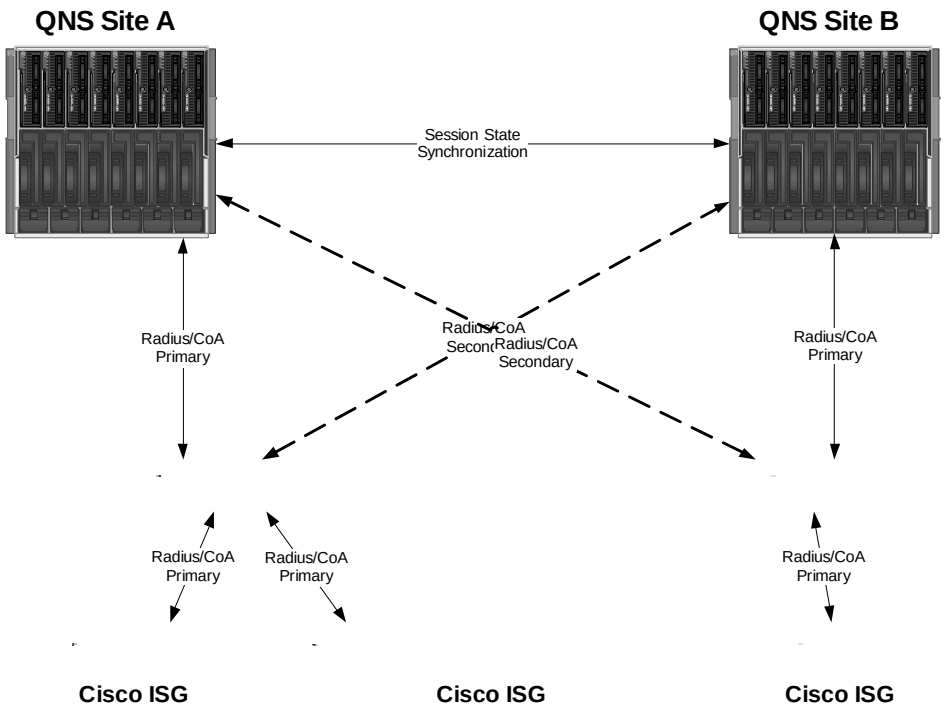
The active-active mode is illustrated in Figure 4-4. Each PCEF is configured with a primary and a secondary RADIUS connection to the deployed QPS systems.

Figure 4-4 Active/Active QPS HA Without External Load Balancer



In the following diagram, Figure 4-5, two external load balancers send traffic to the QPS installations.

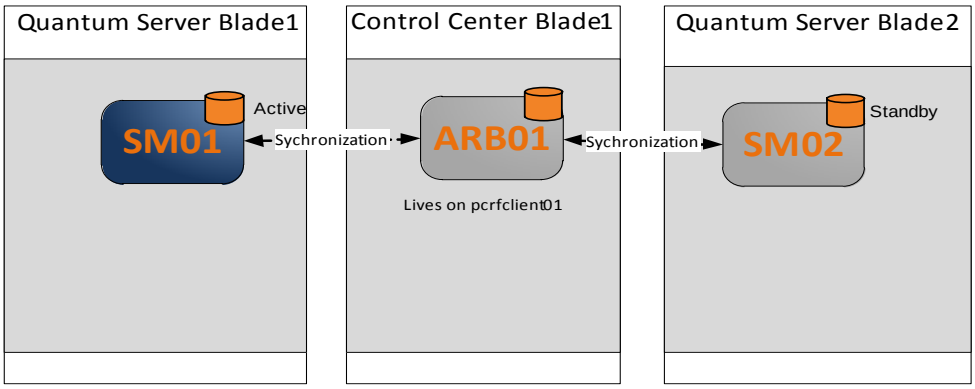
Figure 4-5 Active/Active QPS HA with External Load Balancer



Session Manager Configuration

After the base install has been completed on both sites, the standard Session Manager configuration on each site will be as shown in Figure 4-6.

Figure 4-6 Standard Session Manager Configuration at Installation



Verifying Session Manager Cluster

These steps verify the session manager cluster.

Step 1 To verify that the session manager cluster is up, use the command line interface on sessionmgr01, and run the following commands:

```
[root@sessionmgr01 ~]# /usr/bin/mongo --port 27717

MongoDB shell version: 2.2.0

connecting to: 127.0.0.1:27717/test

set01:PRIMARY> rs.status()
```

The result should look like the following code response, where one of the session manager instances is the PRIMARY, one is the SECONDARY, and the arbiter is running on pcrfclient01.xxxx

```
{
        "set" : "set01",
        "date" : ISODate("2013-01-25T22:33:18Z"),
        "myState" : 1,
        "members" : [
                {
                        "_id" : 0,
                        "name" : "sessionmgr02:27717",
                        "health" : 1,
                        "state" : 2,
                        "stateStr" : "SECONDARY",
                        "uptime" : 957076,
                        "optime" : Timestamp(1359153189000, 18),
                        "optimeDate" : ISODate("2013-01-25T22:33:09Z"),
                        "lastHeartbeat" : ISODate("2013-01-25T22:33:16Z"),
                        "pingMs" : 0
                },
                {
                        "_id" : 1,
                        "name" : "sessionmgr01:27717",
                        "health" : 1,
                        "state" : 1,
```

```
                    "stateStr" : "PRIMARY",
        "uptime" : 957930,
                    "optime" : Timestamp(1359153189000, 18),
                    "optimeDate" : ISODate("2013-01-25T22:33:09Z"),
                    "self" : true
                },
                {
                    "_id" : 2,
                    "name" : "pcrfclient01:27717",
                    "health" : 1,
                    "state" : 7,
                    "stateStr" : "ARBITER",
                    "uptime" : 781693,
                    "lastHeartbeat" : ISODate("2013-01-25T22:33:16Z"),
                    "pingMs" : 0
                }
            ],
            "ok" : 1
        }
```


Step 2 To verify the setup, repeat these steps for the other instances on 27718, 27719 and 27720.

Step 3 After verification:

- Procure five IP routable IP addresses on the Management/Signaling network. In the examples listed in this document, this will be in the 192.168.2.0/24 IP range.
- Procure a hostname to be used for external arbiter.
- Two new hostnames for site B's sessionmgr03 and sessionmgr04.
- For reference, we will call the new arbiter arbiter01, and the IP will be 192.168.2.10. The new sessionmgr01 and sessionmgr02 IPs in site A will be 192.168.2.11 and 192.168.2.11. The new sessionmgr03 and sessionmgr04 IPs in site B will be 192.168.2.12 and 192.168.2.13.

The next steps install the Arbiter on site C hardware.

Step 1 Start by cloning the pcrfclient01 VM and install it on the new hardware containing VMWare ESX.

Step 2 When this is complete, IP the VM and change the hostname to be arbiter01 in the `/etc/hostname` file and the `/etc/hosts` file.

Step 3 Because this was originally a pcrfclient, stop some of the services on it. To do this, issue these commands:

service qns stop

chkconfig qns off

Step 4 Add the management sessionmgr01 and sessionmgr02 and IP the new interfaces in site A. This may require you to restart the VM. See the VMware documentation for specific instructions on how to do this. See http://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc_50%2FGUID-662B9537-23D2-446B-9DCF-6A66E09B0B27.html

Step 5 Add the management sessionmgr01, sessionmgr02, and IP the new interfaces in site B. This addition may require to restart the VM.

Step 6 Add the host name of the arbiter01, sessionmgr03 (originally site B sessionmgr01), sessionmgr04 (originally site B sessionmgr02) and their appropriate IPs to the /etc/hosts of the pcrfclient01 and synch it to all systems.

Step 7 Check all of the configurations by pinging arbiter01, sessionmgr01, sessionmgr02, sessionmgr03 and sessionmgr04 from each of those respective VMs.

Step 8 If all of those can be pinged, the next check is to make sure that all of the ports can be opened from all of the VMs to each other. Run this command:

/usr/bin/mongo --port 27717 --host arbiter01

Step 9 Replace the port for ports 27717, 27718, 27719, 27720 and the host with arbiter01, sessionmgr01, sessiongmr02, sessionmgr03, sessionmgr04 from each respective VM.

The result should look like this:

MongoDB shell version: 2.2.0

connecting to: arbiter01:27717/test

Step 10 Run these commands on pcrfclient01 to stop its mongo instances since they will be running on arbiter01.

chkconfig sessionmgr-27717 off

chkconfig sessionmgr-27718 off

chkconfig sessionmgr-27719 off

chkconfig sessionmgr-27720 off

Step 11 Run these commands from pcrfclient01 to build the new replica sets.

build_set.sh set01

/data/sessions.1

arbiter01:27717

sessionmgr01:27717

sessionmgr02:27717

sessionmgr03:27717

sessionmgr04:27717

build_set.sh set02

/data/sessions.2

arbiter01:27718

sessionmgr01:27718

sessionmgr02:27718

sessionmgr03:27718

sessionmgr04:27718

build_set.sh set03

/data/sessions.3

arbiter01:27719

sessionmgr01:27719

sessionmgr02:27719

sessionmgr03:27719

sessionmgr04:27719

build_set.sh set04

/data/sessions.4

arbiter01:27720

sessionmgr01:27720

sessionmgr02:27720

sessionmgr03:27720

sessionmgr04:27720

Step 12 After the replica set is fully online (wait about 10 minutes to be sure or tail the log file or run rs.status() (to check the status), retest the original cluster or if this a new deployment try running some basic tests to confirm all of the connectivity is set.

Policy Director Configuration

When an active-active cluster is deployed, both sides have active sessions that will be replicated only to the other cluster as a standby. When back office systems need to make changes to subscribers (SPR) or their balances (MsBM), they will not always know which cluster the subscriber's active session will be on. To facilitate the decision, the QPS system has the ability to broadcast the messages resulting from subscriber or balance changes to other clusters.

To configure this feature, you will need the lb01 and lb02 IP addresses of the remote active cluster. For this example, assume these are IPs 192.168.22.2 and 192.168.22.3.

Step 1 Open a command line on pcrfclient01.

Step 2 Add these IPs to the /etc/hosts file as remote-lb01 and remote-lb02.

Step 3 After adding those, find the `/etc/broadhop/iomanager01/qns.conf` and `/etc/broadhop/iomanager02/qns.conf`.

Find the section in both that looks like this:

```
QNS_OPTS="
-DbrokerUrl=vm://localhost
-DjmsFlowControlHost=localhost
-DjmsFlowControlPort=9045
-DembeddedBrokerEnabled=true
-DembeddedBrokerNetworkUri=static:(tcp://lb02:61616)?useExponentialBackOff=false
"
```

Step 4 After the `-DembeddedBrokerNetworkUri` property, add a new property like this:

```
-DclusterPeers=failover:(tcp://remote-lb01:61616,tcp://remote-lb02:61616)?updateURIsSupported
    =false!cluster-1.default
```

The new configuration should look like this:

```
QNS_OPTS="
-DbrokerUrl=vm://localhost
-DjmsFlowControlHost=localhost
-DjmsFlowControlPort=9045
-DembeddedBrokerEnabled=true
-DembeddedBrokerNetworkUri=static:(tcp://lb02:61616)?useExponentialBackOff=false


-DclusterPeers=failover:(tcp://remote-lb01:61616,tcp://remote-lb02:61616)?updateURIsSupported
    =false!cluster-1.default
```

"

Step 5 After these changes, synch all of the `/etc/hosts` and configuration files to all of the other VMs and then restart iomanager01 and iomanager02 to get the changes to take effect.

Step 6 After the configuration changes, test by starting a session on the remote cluster and then change the subscribers profile in SPR in the local cluster.

The session should be changed in the remote cluster, and any network device changes should be made as well.

Step 7 After confirming the tests, repeat the procedure in the remote cluster.

Quantum Policy Server Blade Hardware

Revised: September 30, 2013, OL-29748-01

This section describes the blade hardware used in Quantum Policy Suite, and the number of blades needed to deploy. Specifically, look at these sections for information on what your hardware consists of and how to grow your QPS solution.

This chapter covers the following topics:

Server Prerequisites

For specific hardware recommendations, see the document Quantum Policy Suite System Sizing Guide,

The Quantum Policy Suite can be installed on a variety of non-specific hardware. For example, a deployment site might use blade hardware or an HP DL 380 Generation 7.

You can obtain hardware directly from Cisco Systems, Inc. or through your own purchasing department.

5Blade Server Requirements

The Quantum Policy Suite is optimized for a commercial off-the-shelf (COTS) blade server and ATCA environment, such as those from IBM, Sun Microsystems, HP, Cisco, and RadiSys (Continuous Computing).

Blade Server Minimum Hardware Requirements	
Processor	2 x Intel Xeon X5650 or higher speed processor
Memory	Minimum RAM Requirement: • 48 GB RAM for less than 1,000,000 subscribers • 72 GB RAM for greater than 1,000,000 subscribers
Storage	• 2 x 200 GB SSD Drives • Supporting Hardware RAID 1 with write backed cache
Interconnect	Dual Gigabit Ethernet ports

Blade Server Minimum Hardware Requirements	
Virtualization	Must be listed on the VMware HCL http://www.vmware.com/resources/compatibility/search.php
Chassis Minimum Hardware Requirements	
Device Bays	4 Minimum
Interconnect	Redundant interconnect Support
Power	Redundant AC or DC power supplies (as required by Service Provider)
Cooling	Redundant cooling Support
Quantum Network Suite Minimum Requirements	
Redundant System	4 blade servers: • 2 Quantum Control Centers plus • 2 Quantum Servers

Revised: September 30, 2013, OL-29748-01

3G systems 3G is the third generation of mobile phone standards and technology. It is based on the international Telecommunication Union (ITU) family of standards under the International Mobile Telecommunications Programme, MT-2000.

3GPP Third Generation Partnership Project

4G System 4G is the fourth generation of cellular wireless standards, a successor to the 3G and 2G families of standards. In 2008, the ITU-R organization specified the IMT-Advanced (International Mobile Telecommunications Advanced) requirements for 4G standards, setting peak speed requirements for 4G service at 100 Mbit/s for high mobility communication (such as from trains and cars) and 1 Gbit/s for low mobility communication (such as pedestrians and stationary users.

A

AAA Command for an AA Answer

AAR Command for an AA Request

ADC Application Detection and Control

ADN Application Delivery Network

AF Application Function

Element offering application(s) that use IP bearer resources. NOTE: One example of an AF is the P-CSCF of the IM CN subsystem.

AF Session Application-level session established by an application-level signaling protocol offered by the AF that requires a session set-up with explicit session description before the use of the service.

Note: One example of an application session is an IMS session.

AN Gateway Access Network Gateway

answer service template A service template for Diameter; answering a request.

API Application Programming Interface

application A Diameter application that defines the data needed to perform various related actions.

Application Service Provider A business entity responsible for the application that is being/will be used by a UE, which may be either an AF operator or has an association with the AF operator.

ARAC-F Access Resource Admission Control Function

ARP Allocation and Retention Priority

ASA Command for an Abort Session Answer

ASP Application Service Provider

ASR Command for an Abort Session Request

authorised QoS The maximum QoS that is authorized for a service data flow. In case of an aggregation of multiple service data flows within one IP-CAN bearer (e.g. for GPRS a PDP context), the combination of the "Authorized QoS" information of the individual service data flows is the "Authorized QoS" for the IP-CAN bearer. It contains the QoS class identifier and the data rate.

AVP Attribute Value Pair

See RFC 3588 [5], corresponds to an Information Element in a Diameter message.

B

BBERF Bearer Binding and Event Reporting Function

BBF Bearer Binding Function

BG Border Gateway

binding PCRF process of associating IP flows described in AF Service Information with IP-CAN bearers. The association between a service data flow and the IP-CAN bearer (for GPRS the PDP context) transporting that service data flow.

binding mechanism The method for creating, modifying and deleting bindings.

blueprint Predefined packages of data (Policies, Reference Data, and so on) managed by Quantum Policy Builder 6.0 and used to start an implementation project quickly.

BNG Broadband Network Gateway

BSS Block Started by Symbol/Business Support Systems

bursting Subscriber session where periods of rapid and high transmission spiking are followed by quiescent, silent, periods.

C

calculated session class A calculated session class stores attributes and recalculates them each time a policy references the calculated session objects. A calculated session class sets its own data. It can calculate what a value should be and will evaluate that data whenever asked rather than waiting for other policies to set its information.

calculator decorator A Calculator Decorator stores attributes that are recalculated each time the policies reference the calculator object. A Calculated Decorator sets its own data. It can calculate what a value should be and will evaluate that data whenever asked, e.g. TimeSpentThisSession.

CAPEX Capacity Expansion/Capital Expense

CAR CDR Analysis and Reporting from Cisco Systems

CCA Credit Control Answer

CCR Credit Control Request

CDR Call Detail Record

charging control The process of associating packets, belonging to a service data flow, to a charging key and applying online charging and/or offline charging, as appropriate.

charging key Information used by the online and offline charging system for rating purposes.

child Some other subcomponent on the hierarchy tree, which occupies the left pane.

class In object-oriented programming, a class is a construct that is used as a blueprint (or template) to create objects of that class. This blueprint describes the state and behavior that the objects of the class all share.

An object of a given class is called an instance of the class. The class that contains that instance can be considered as the type of that object, e.g. a type of an object of the “Fruit” class would be “Apple”.

CLI Command Line Interface

CMS In Subscriber Services Portal (SSP), this means Content Management System. The CMS helps the provider develop skins for subscriber pages.

CNR Cisco Network Registrar from Cisco Systems

CoA Change of Authentication/Change of Authorization/Certificate of Authority

CoA shared secret A piece of data such as a password or pass phrase, known only by the entities involved in a secure communication for the purposes of authentication.

CODEC Coder-decoder

condition phrase A Condition which can be used by a policy. For example, A user exists with name X.

configured blueprint An implementation of a blueprint (either initial or and extension) to which configured extension points will be added.

configured extension point A configured extension point provides a way to add policies to your Quantum Network Suite system, augmenting the standard policies Quantum Network Suite provides.

configured trigger extension point Configured trigger extension points let you specifically start and stop a session, based on criteria you specify.

COPS Common Open Policy Service

COTS Common Off-the-shelf

CRF Charging Rules Function

CSG Closed Subscriber Group

CSG ID Closed Subscriber Group Identity

D

DCCA Diameter Credit-Control Application

decision table A type of policy which can simplify the creation of similar policies using a table/spreadsheet format. For example, if username='A' then bandwidth='B' - Table (A,B): (jdoe, superhigh) (jdoe,superlow) (*, default)

DHCP Dynamic Host Configuration Protocol, one of the protocols in the TCP/IP networking suite.

Diameter Diameter is a computer networking protocol for AAA (authentication, authorization and accounting). It is a successor to RADIUS. Diameter controls communication between the Secure Ticket Authority (STA) and any network entity requesting authentication.

DRA Diameter Routing Agent

DRA binding The PCRF routing information stored per UE or per PDN in the DRA, which include the user identity (UE NAI), the UE IPv4 address and/or IPv6 prefix, the APN (if available) and the selected PCRF identity for a certain IP-CAN Session.

DSL Digital Subscriber Line

DWR/DWA DW Request/DW Acknowledgment

dynamic PCC Rule A PCC rule for which the definition is provided in the PCEF via the Gx reference point.

E

ECUR Event Charging with Unit Reservation

ESXi An operating system from VMWare permitting placement of the hypervisor onto a dedicated compact storage device.

event report A notification, possibly containing additional information of an event which occurs that corresponds with an event trigger. Also, an event report is a report from the PCRF to the AF concerning transmission resources or requesting additional information.

event trigger A rule specifying the event reporting behavior of a PCEF or BBERF. Also, a trigger for credit management events.

extension A software extension is a computer program designed to be incorporated into another piece of software in order to enhance, or extend, the functionalities of the latter. On its own, the program is not useful or functional.

extension blueprint A blueprint that depends on data from another blueprint.

extension point A place in a Cisco Systems blueprint which can be extended with additional policies and policy groups for a given client implementation. For example, Extension Point: 'Set User bandwidth' which would allow a client to add specific policies to set bandwidth.

F

FON Fiber Optic Network

FTTx Fiber To The Wherever

G

Gateway Control Session An association between a BBERF and a Quantum Network Suite (when GTP is not used in the EPC), used for transferring access-specific parameters, BBERF events, and QoS rules between the Quantum Network Suite and BBERF. In the context of this specification, this is implemented by use of the Gxx procedures.

gating control The process of blocking or allowing packets, belonging to a service data flow, to pass through to the desired endpoint.

GBR Guaranteed Bit Rate

GBR bearer An IP-CAN bearer with reserved (guaranteed) bit rate resources.

GGSN Gateway GPRS Support Node/Gateway General Support Node

GPRS IP-CAN This IP-CAN incorporates GPRS over GERAN and UTRAN, see TS 23.060 [12].

GPRS_Core_Network The General Packet Radio Service (GPRS) system is used by GSM mobile phones, the most common mobile phone system in the world, for transmitting IP packets. The GPRS core network is the centralized part of the GPRS system. It also provides support for WCDMA-based 3G networks. The GPRS core network is an integrated part of the GSM network switching subsystem.

group of applications In usage monitoring, a set of ADC rules sharing a common monitoring key.

GSM - Groupe Spécial Mobile GSM is a cellular network. Mobile phones connect to it by searching for cells in the immediate vicinity. GSM (Global System for Mobile communications: originally from Groupe Spécial Mobile) is the most popular standard for mobile phones in the world.

GTP GPRS Tunneling Protocol

Gxx Gx extension

H

H-AF Home Application Function

H-DRA Home Diameter Routing Agent

H-PCEF A PCEF in the HPLMN

H-PCRF Home Policy Charging Rules Function

Home Routed Access Roaming scenario where the PCEF is located in the HPLMN. In a Home Routed roaming scenario, the UE obtains access to the packet data network from the HPLMN.

HPLMN Home Public Land Mobile Network

HR Home-Routed

HRPD High Rate Packet Data

HSGW HRPD Serving Gateway

HTTP Hypertext Transfer Protocol

I

I-WLAN IP-CAN This IP-CAN incorporates 3GPP IP access of I-WLAN, see TS 23.234 [13].

IMS A database system from IBM consisting of IMS/Data Base and IMS/Data Communications.

IMS IP Multimedia Subsystem, a set of specifications from 3GPP for delivering IP multimedia to mobile users.

initial blueprint A root-level blueprint. This type of blueprint does not depend on data from another blueprint to exist. The initial blueprint contains Policy Groups, Policies and Extension Points relating to a given piece of functionality.

IP flow Unidirectional flow of IP packets with the same Source IP address and port number, Destination IP address and port number, Transport protocol. Port numbers are only applicable if used by the transport protocol.

IP-CAN IP connectivity Access Network

An IP transmission path of defined capacity, delay, and bit error rate.

IP-CAN bearer IP transmission path of defined capacity, delay and bit error rate, etc. See 3GPP TS 21.905 [1] for the definition of bearer.

IP-CAN session The association between a UE and an IP network. The association is identified by one or more UE IP addresses (one IPv4 and/or one IPv6 address) together with a UE identity information, if available, and a PDN represented by a PDN ID (e.g. an APN). An IP-CAN session incorporates one or more IP-CAN bearers. Support for multiple IP-CAN bearers per IP-CAN session is IP-CAN specific. An IP-CAN session exists as long as the related UE IP addresses are assigned and announced to the IP network.

IPHK Internet Protocol Host Key

ISG Intelligent Services Gateway, a Cisco Systems policy enforcement point.

ISO An ISO image (International Organization for Standardization) is an archive file (also known as a disc image) of an optical disc, composed of the data contents of every written sector of an optical disc, including the optical disc file system.

J

Java Action Phrase An action a policy that is based on Java code.

Juniper Juniper Networks provides high-performance network infrastructure.

L

LDAP Lightweight Directory Access Protocol/Lightweight Data Access Protocol

Location In Subscriber Services Portal (SSP) a location is the URL that a subscriber logs in to.

LTE Long Term Evolution

MAC A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment.

MBR Maximum Bit Rate

MMSC Multimedia Message Service Center

Monitoring key Information used by the PCEF and PCRF for usage monitoring control purposes as a reference to a given set of service data flows that all share a common allowed usage on a per UE and APN basis.

MPS Multimedia Priority Service

MPS session A session for which priority treatment is applied for allocating and maintaining radio and network resources to support the Multimedia Priority Service (MPS). MPS is defined in 3GPP TS 22.153 [31]

N

network session information All the information that Quantum Network Suite knows about a subscriber. The information is set by Policies.

NGN Next Generation Network

non-GBR bearer An IP-CAN bearer with no reserved (guaranteed) bit rate resources.

O

object action phrase An action a policy can use that is based on Session objects in the Policy Builder GUI.

OCS Online Charging System

OFCS Offline Charging System

operator-controlled service A service for which complete PCC rule information, including service data flow filter information, is available in the PCRF through configuration and/or dynamic interaction with an AF.

OSS Open Source Software

OVF Open Virtualization Format

P

P-CSCF Proxy-Call Session Control Function

The P-CSCF is the entry point to the IMS domain and serves as the outbound proxy server for the UE.

PA Proxy Agent

packet flow A specific user data flow carried through the PCEF. A packet flow can be an IP flow.

PBHK - Port-bundle Host-key This provides an apparatus and method to associate a subscriber with one of many port bundles in an aggregation device. The method reserves one of the port bundles for the subscriber if the subscriber was not assigned a port bundle, changes the original source port number in a data packet to a port bundle number, modifies the subscriber address to an assigned aggregation address, and issues a request to a remote management device for authentication of the subscriber. Once a response is received from the management device including the authentication or unauthentication of the subscriber, the subscriber is mapped with the reserved port bundle in a port bundle object and the reserved port bundle is then assigned to the subscriber. The apparatus has at least one source port to receive a data packet, several port bundles coupled to the source port, each port bundle having a memory with a port bundle object to associate the subscriber with one of the port bundles, a processor coupled to the port bundles, and an output port coupled to the processor.

PCC Policy and Charging Control

PCC decision A PCC decision consists of PCC rules and IP-CAN bearer attributes, which are provided by the PCRF to the PCEF for policy and charging control.

PCC rule A set of information enabling the detection of a service data flow and providing parameters for policy control and/or charging control.

PCEF Policy and Charging Enforcement Function

PDF Policy Decision Function

PDN Packet Data Network/Public Data Network/Process Data Network

PGW PDN-Gateway

PME Policy Management Engine

PMS Payment Management System

An electronic payment method such as PayPal.

policy The policy is the building block of the Quantum Network Suite. A policy checks if a certain set of conditions is true and if so, executes actions. For example, if username='jdoe' then bandwidth='superhigh'.

policy control The process where the PCRF indicates to the PCEF how to control the IP-CAN bearer. Policy control includes QoS control or gating control or both.

policy counter A mechanism within the OCS to track spending applicable for a subscriber.

policy counter status A label whose values are not standardized and that is associated with a policy counter's value relative to the spending limit(s) (the number of possible policy counter status values for a policy counter is one greater than the number of thresholds associated with that policy counter, i.e policy counter status values describe the status around the thresholds). This is used to convey information relating to subscriber spending from OCS to PCRF. Specific labels are configured jointly in OCS and PCRF.

PEP - Policy Enforcement Point PEP is a component of policy-based management. When a user tries to access a file or other resource on a computer network or server that uses policy-based access management, the PEP describes the user's attributes to other entities on the system. The PEP gives the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user's attributes. Applicable policies are stored on the system and are analyzed by the PDP. The PDP makes it's decision and returns the decision. The PEP lets the user know whether or not they have been authorized to access the requested resource.

policy group A logical grouping of policies that will be evaluated at the same time.

For example, Policy Group: 'Set User Bandwidths' could contain all policies which set bandwidth. They would all be re-evaluated if something important to bandwidth changed.

Port-bundle Key Length For PBHK, the port bundle number:

Includes a range of sequential port numbers starting with a base port number.

Is approximated by range of sequential port numbers=$2^{\text{port bundle length}}$.

The port bundle length is an integer between 1 to 16.

predefined PCC rule A PCC rule that has been provisioned directly into the PCEF by the operator.

publish Represents sending the configuration data from the Quantum Policy Builder Client and 'publishing' it into the QNS environment.

Q

QCI QoS Class Identifier. A scalar that is used as a reference to a specific packet forwarding behavior, for example, packet loss rate, packet delay budget, to be provided to an SDF.

QME Quota Management Engine

QNS Quantum Network Suite, Cisco Systems, Inc. collection of policy, PCRF, and PCEF software.

QoE Quality of Experience

QoS Quality of Service

QoS class identifier (QCI) A scalar used as a reference to a specific packet forwarding behavior (e.g. packet loss rate, packet delay budget) to be provided to a SDF. This may be implemented in the access network by the QCI referencing node specific parameters that control packet forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.), that have been pre-configured by the operator at a specific node(s) (e.g. eNodeB).

QoS rule A set of information enabling the detection of a service data flow and defining its associated QoS parameters.

QPS Quantum Policy Suite, Cisco Systems, Inc. collection of policy, PCRF, and PCEF software.

Query Map Parameters that are passed during initial redirection to be saved in the subscriber's browser session and included in QNS API calls.

R

RAA Re-Authenticate Answer

RADIUS Remote Authentication Dial in User Service

RADIUS service template A service template for RADIUS. This template can be either a request or answer.

RAN Radio Access Network

RAR Re-authorization Request

RCP version QNS uses the R9 PCRF specification.

R9 includes the Gx, Gy, Rx, Sp, Gxx, and S9 interfaces. The Gxx and S9 interfaces were new in R8 and are for roaming scenarios. The Cisco Systems, Inc. GA release is focusing on Rx, Gx, Gy, and Sp (where Sp is not defined by the specification).

RDBMS Relational Data Base Management System

Redback Redback Networks Inc. provides networking solutions for IP-based services and communications. Redback products create solutions that address building a next generation network.

Redirection Redirect the detected service traffic to an application server (e.g. redirect to a top-up / service provisioning page).

Repository A software repository is a storage location from which software packages may be retrieved and installed on a computer.

In the case of Quantum Policy Suite, we store the configuration and use data in a repository and manage it with Subversion, a version control software.

Subversion maintains current and historical versions of the Quantum Policy Suite configuration and policy files. You may use your own version Subversion control software if you have it.

Response service template A service template for Diameter used for answering a request.

RFC - Request for Comments One of a series of numbered Internet informational documents and standards widely followed by commercial software and freeware in the Internet and Unix communities. Few RFCs are standards but all Internet standards are recorded in RFCs. Perhaps the single most influential RFC has been RFC 822, the Internet electronic mail format standard.

root configured blueprint In Quantum Policy Builder, the Root Blueprint is the starting blueprint for a policy framework. In general, this is always the starting blueprint used when configuring the policies. When first installed, the root blueprint is selected and becomes known as the initial blueprint, which can then be added to or modified, leaving the root blueprint unchanged.

RTCP RTP Control Protocol

RTP Real-time Transport Protocol

S

S-GW Serving Gateway

S5/S8 PMIP Proxy Mobile IP

Sandvine Sandvine helps DSL, FTTx, cable, fixed wireless, and mobile operators understand network traffic, mitigate malicious traffic, manage network congestion, and deliver QoS-prioritized multimedia services.

SCUR Session Charging with Unit Reservation

SDF Service Data Flow

SDK Software Development Kit

SDM Subscriber Data Management

Service An individual service defined by VSAs within the VSA. Contained in a service bundle as an offering to a customer.

service bundle A group of services that are offered to customers in a specific service location.

service data flow An aggregate set of packet flows that matches a service data flow template.

service data flow filter A set of packet flow header parameter values or ranges, used to identify one or more of the packet flows constituting a service data flow.

service data flow filter identifier A scalar that is unique for a specific service data flow (SDF) filter (used on Gx and Gxx) within an IP-CAN session.

service data flow template The set of service data flow filters in a PCC rule, required for defining a service data flow.

service identifier An identifier for a service. The service identifier provides the most detailed identification, specified for flow based charging, of a service data flow. A concrete instance of a service may be identified if additional AF information is available (further details to be found in clause 6.3.1).

service information Set of information conveyed from the AF to the Quantum Network Suite over the Rx interface, to be used as a basis for PCC decisions at the Quantum Network Suite, including information about the AF session (e.g. application identifier, type of media, bandwidth, IP address and port number).

service management The integrated set of functions that together enable a service provider to effectively define, deploy and manage advanced multi-service offerings on their packet-based network. Key elements include: identification and authentication, subscriber service profile management, service and policy management, dynamic service portal, billing and payments. These functions form the critical service management layer in the IMS framework, linking network applications with network infrastructure and control.

service template A template that defines what data needs to be sent for a given service.

Service construct that contains the basic VSAs required to create a service. Additional information, such as access policies, billing rules and pricing are applied to a service template to create a specific service.

session based service An end user service requiring application level signaling, which is separated from service rendering.

session class A logical grouping of fields into an object on the Session. Session classes allow having an “Address” on the session, rather than listing “Street Name”, “ZIP”, “City”, for example, on the session.

A session class is used as a blueprint to create other session objects. In Quantum Network Suite, it is possible to define more than one type of session.

Session classes populate the Conditions phrase list from which you set up policies.

session domain Session domains track and hold data for later use. Classes make up the session domains. You can configure what data to track and hold about a session.

session domain decorator Session Domain Decorators provide additional attributes to pre-existing domains. These are objects that add (decorate) additional fields to the root network session.

Session Domain Decorators are of two types:

Session Domain Decorators—the static attributes from a subscriber session.

Calculator Decorators—the computable values that are available for use within a session period.

session info Information about what data is currently in the session.

session key A key or index or a field of the session that speeds up searching on that field, if needed.

Session Manager - sessionmgr The database used by Quantum Policy Suite.

SGSN Serving GPRS Support Node

shard A method of horizontal partitioning in a database or search engine. Each individual partition is referred to as a shard or database shard.

shared secret A piece of data, that is, a password or pass phrase, only known by the entities involved in a secure communication.

SLA Spending-Limit-Answer (SL-Answer)

SLR Spending-Limit-Request (SL- Request)

SME Cisco Systems's Service Management Engine

SMSC Short Message Service Center

SNA Spending-Status-Notification-Answer (SN-Answer)

SNMP Simple Network Management Protocol

SNR Spending-Status-Notification-Request (SN- Request)

SOAP Simple Object Access Protocol

SP Wi-Fi Service Provider Wi-Fi

SPDF Server-based Policy Decision Function

spending limit A spending limit is the usage limit of a policy counter (e.g. monetary, volume, duration) that a subscriber is allowed to consume.

spending limit report A notification, containing the current policy counter status generated from the OCS to the PCRF via the Sy reference point.

SPR Subscriber Profile Repository, a general name for a system or a database schema that holds information about subscribers.

SQL Structured Query Language/Standard Query Language/Search and Query Language

SRS Software Requirements Specifications

SSL Secure Socket Layer

STA Session Termination Answer

Startup Action An action that runs on startup.

STR Session Termination Request

subscribed guaranteed bandwidth QoS The per subscriber, authorized cumulative guaranteed bandwidth QoS which is provided by the SPR/UDR to the PCRF.

subscriber The end user customer of a service provider.

subscriber category A means to group the subscribers into different classes, e.g. gold user, the silver user and the bronze user.

subscriber data source The specified locale that stores the subscriber data. This could be SME, SuM, Unified SuM, an AAA server, or an LDAP system.

subscription A recurring service offering, usually on a monthly basis, purchased by the customer, requiring the creation of a personal profile including a username and password.

SuM/Unified SuM/USuM Subscriber Management, the Cisco Systems solution for a subscriber data source.

svn Tortoise Subversion, a version control software used as a data repository.

T

TDF Traffic Detection Function

TDF session For a TDF, an association, made by the PCRF, between an IP-CAN session and the assigned TDF.

TISPAN Telecommunications and Internet-converged Services and Protocols for Advanced Networking

trigger extension point A place in a blueprint which allows adding conditions to indicate when a Policy Group should be re-triggered.

For example, Trigger Extension Point: 'Set User bandwidth' allows a client to add a condition, 'new user added to system' which will rerun the policies for setting user bandwidth.

TS Technical Specification

U

UDC User Data Convergence

UDR User Data Repository

UE	User element, a subscriber's hardware.Wireless telephone as user equipment in 3G mobile telephone systems
UMTS	Universal Mobile Telephony System
uplink bearer binding verification	The network enforcement of terminal compliance with the negotiated uplink traffic mapping to bearers.
Use Case Template	In Quantum Policy Suite, the easily defined parts that are put together to form a Service. Fair Usage and Quality of Service are examples of a use cases which are templatized in the Quantum Policy Builder interface.
user-subscribed service	A service provided to an end user as a subscription. Services may exist, but have no users subscribed to them.

V

V-AF	Visited Application Function. thefreedictionary.com
V-DRA	Visited Diameter Routing Agent. thefreedictionary.com
V-PCEF	A PCEF in the VPLMN
V-PCRF	Visited PCRF
VA	Visited Access
vendor	A vendor of Diameter. In Quantum Network Suite a vendor can represent a business in general, for example, Cisco, HP, or Sun.
VIPlan	Virtual IP LAN
Virtual IP	Virtual IP address. A virtual IP address (VIP or VIPA) is an IP address that is not connected to a specific computer or network interface card (NIC) on a computer. Incoming packets are sent to the VIP address, but they are redirected to physical network interfaces.
Visited Access (also known as local breakout)	Roaming scenario where the PCEF is located in the VPLMN. In a Visited Access Roaming scenario, the UE obtains access to the packet data network from the VPLMN.
VLAN	Virtual LAN
VPLMN	Visited Public Land Mobile Network
VSA	Vendor Specific Attribute
vSRVCC	Video Single Radio Voice Call Continuity

W

WISPr	Wi-Fi Internet Service Provider roaming

X

XML Extensible Markup Language

Interfaces in the GPRS network

Ga The interface server's CDRs (accounting records) which are written in the GSN and sent to the charging gateway (CG). This interface uses a GTP-based protocol, with modifications that supports CDRs (called GTP' or GTP prime).

Gb Interface between the base station subsystem and the SGSN. The transmission protocol could be Frame Relay or IP.

Gd Interface between the SGSN and the SMS Gateway. Can use MAP1, MAP2 or MAP3.

Ge The interface between the SGSN and the service control point (SCP); uses the CAP protocol.

Gi IP-based interface between the GGSN and a public data network (PDN), either directly to the Internet or through a WAP gateway.

Gmb The interface between the GGSN and the broadcast-multicast service center (BM-SC), used for controlling MBMS bearers.

Gn IP-based interface between SGSN and other SGSNs and (internal) GGSNs. DNS also shares this interface. Uses the GTP Protocol.

Gp IP based interface between internal SGSN and external GGSNs. Between the SGSN and the external GGSN, there is the border gateway (which is essentially a firewall). Uses the GTP Protocol.

Gr Interface between the SGSN and the HLR. Messages going through this interface uses the MAP3 protocol.

Gs Interface between the SGSN and the MSC (VLR). Uses the BSSAP+ protocol. This interface allows paging and station availability when it performs data transfer. When the station is attached to the GPRS network, the SGSN keeps track of which routing area (RA) the station is attached to. An RA is a part of a larger location area (LA). When a station is paged this information is used to conserve network resources. When the station performs a PDP context, the SGSN has the exact BTS the station is using.

Gx The interface between the GGSN and the Cisco Systems Quantum Network Suite. It is used for provisioning service data flow based policy and charging rules. Uses the Diameter protocol.

The on-line policy interface between the GGSN and the charging rules function (CRF). It is used for provisioning service data flow-based charging rules. Uses the Diameter protocol.

Gx Plus A vendor-specific Gx interface.

Gy The on-line charging interface between the GGSN and the online charging system (OCS). Uses the Diameter protocol (DCCA application).

Gz The off-line (CDR-based) charging interface between the GSN and the CG. Uses GTP.

Ro Interface to the RCP.

Rx Interface to the RCP.

Sp 3GPP Release 9 interface that has no protocol associated with it.

Sy The Sy reference point connects two ePDSNs in the 3GPP2 HRPD network.