7701 CPAA and vCPAA
CONTROL PLANE ASSURANCE APPLIANCE

Release 10.0 R5

Setup and Installation Guide

3HE-12020-AAAE-TQZZA
Issue 3
September 2022

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

About this document

Purpose

The *7701 CPAA and vCPAA Setup and Installation Guide* provides information about the 7701 CPAA hardware and vCPAA.

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Please send your feedback to documentation.feedback@nokia.com.

1 CPAA Overview

1.1 CPAA overview

1.1.1 CPAA route analyzer

The CPAA collects and analyzes routing data from the routing areas to which it is connected. Traffic on the CPAA is restricted to control data and packages directly destined to the CPAA. Because no other traffic can pass through it, the CPAA only advertises itself to its neighbor routers and does not re-advertise link-state data received from its neighbors.

The CPAA uses a passive version of the 7750 SR OS, and acts as a special-purpose routing element that passively peers with the network to capture a real-time view. The 7701 CPAA and vCPAA are managed by the NFM-P like any other NE. Management procedures such as timing synchronization, polling, deployments, and NE resynchronization are similar to procedures for other SR OS devices. See the *NSP NFM-P User Guide* for information about general device management functions.

The following are the main functions of a CPAA:

- listening to routing data from the routing protocols that are running on it
- providing route calculation for routes passing through the routing areas the CPAA is responsible for
- performing routing analysis and providing the results to the CPAM, so the CPAM can generate network-wide reports or alarms

For information about CPAA functions and deployment under the NFM-P CPAM feature set, see the *NSP NFM-P Control Plane Assurance Manager User Guide*.

1.1.2 7701 CPAA hardware and vCPAA

The CPAA exists as a hardware chassis and as a virtual CPAA (vCPAA).

This guide describes software installation and upgrade, commissioning and discovery, and redundancy for both the 7701 CPAA hardware and vCPAA.

For information about specifications and setup of the 7701 CPAA hardware, consult the *7701 CPAA Setup and Installation Guide* that corresponds to the original hardware and software release at time of purchase.

1.1.3 CPAA alarm support

All alarms supported in CPAA Release 8.0 are also supported in CPAA Release 9.0 and CPAA Release 10.0.

The 7701 CPAA hardware rev.2 and vCPAA do not support power supply alarms or power failure alarms. The CPAA OS has no visibility of the power supply, and cannot detect power interruptions.

2 7701 CPAA hardware Revision 2 installation and upgrade

2.1 Installation and upgrade overview

2.1.1 Purpose

This chapter provides information and procedures for software installation and upgrades on the 7701 CPAA Hardware Revision 2.

For information about installation and upgrades for vCPAA, see Chapter 4, “vCPAA installation and upgrade”.

2.1.2 Important information

The first installation of a software image on the 7701 CPAA must be performed using a CLI.

If you are upgrading from a 7701 CPAA release prior to 8.0 R5, you must update the BOOTROM.SYS file on the 7701 CPAA.

WARNING

Equipment Damage

Do not update the BOOTROM.SYS file unless it is required.

If you update the BOOTROM.SYS file, use a reliable method to transfer the file. Confirm that the transfer and update are successful before you reboot the device.

2.1.3 Upgrade methods

You can upgrade the software on 7701 CPAA Rev. 2 hardware by the following methods:

- Using a CLI; see 2.3 “To install or upgrade the 7701 CPAA Hardware Revision 2 OS software using a CLI” (p. 12).
- Using the NFM-P software upgrade functionality; see 2.4 “To upgrade the 7701 CPAA Hardware Revision 2 OS software using the NFM-P client GUI” (p. 17). This method allows you to upgrade the image on multiple CPAAs at one time. However, a CLI must be used to modify the NVRAM.DAT and bof.cfg files for each device, and to verify the upgrade and reboot the device.

  For information about the NFM-P NE upgrade functionality; see the “NE software upgrades” chapter in the *NSP NFM-P User Guide*

2.2 7701 CPAA software

2.2.1 7701 CPAA Hardware Revision 2 software contents

The 7701 CPAA Hardware Revision 2 must contain the files listed in Table 2-1, “7701 CPAA files” (p. 9) . When you first boot the 7701 CPAA Hardware Revision 2, you must upgrade the 7701 CPAA generic software load. See 2.3 “To install or upgrade the 7701 CPAA Hardware Revision 2 OS software using a CLI” (p. 12) for information.

2.2.2 Software files

The following table describes the 7701 CPAA software files:

Table 2-1 7701 CPAA files

File	Description	Parameters Hardware Revision 2 (solid state memory)
BOOTROM.SYS	VxWorks boot program	—

Table 2-1 7701 CPAA files (continued)

File	Description	Parameters Hardware Revision 2 (solid state memory)
NVRAM.DAT	Used to inform the system of the location of the 7701 CPAA images. The contents of the NVRAM.DAT file can be changed only at reboot time.	• boot device — the options are: - network (fei) When fei is configured, other parameter configurations are required; see below. - device flash (ata). The flash location is identified by numerals. • processor number — must be set to 0. • host name — name of the host machine from which to boot. • file name — full pathname of the boot.tim. • inet on ethernet (e) — Internet address of the Ethernet interface. • inet on backplane (b) — Internet address of the backplane interface. Not used. • host inet (h) — IP address of the host from which to boot. • gateway inet (g) — IP address of a gateway node if the host is not on the same network as the target. • user (u) — username used to ftp the boot load. • ftp password (pw)— password used to ftp the boot load. • target name (tn)— name of the 7701 CPAA system. The target name is the name of the system which is displayed in the CLI prompt and the NFM-P. The system name can later be changed using the following CLI command: configure>system>name • flags (f) — sets the boot options. • startup script (s)

Table 2-1 7701 CPAA files (continued)

File	Description	Parameters Hardware Revision 2 (solid state memory)
bof.cfg	Boot options file. The contents of the bof.cfg file can later be changed in a CLI session to the 7701 CPAA.	• primary-image — the full pathname of the preferred both.tim. Configure the pathname of the upgrade load when you perform an upgrade. • secondary-image — the full pathname of the both.tim to use if the primary image fails. When you perform an upgrade, Nokia recommends that you configure the pathname for the previous image as the secondary-image. • primary-config—full pathname of the 7701 CPAA configuration. • secondary-config—full pathname of the alternate configuration. • address—Internet address of the Ethernet interface. • primary-dns and dns-domain—domain name that is used when performing DNS address resolution. This is a required parameter if DNS address resolution is required. • static-route—allows the manual configuration of static routing table entries. These static routes are only used by traffic generated by the Ethernet management port.
boot.tim	CPAA image file	—
both.tim	CPAA image file	—

Note: Do not copy the BOOTROM.SYS file when upgrading unless it is required. See 2.1.2 “Important information” (p. 9).

2.3 To install or upgrade the 7701 CPAA Hardware Revision 2 OS software using a CLI

WARNING

Equipment Damage

Do not add, modify, or delete the content of the last stable version of the boot files. They must be preserved in case they are required as a secondary image.

2.3.1 Before you begin

The following procedure describes Nokia’s recommendations for using a CLI to install or upgrade the software on a 7701 CPAA. Variations on this procedure are possible, depending on your system and requirements.

Place the installation or upgrade files in a location that is accessible using FTP or SCP.

Do not copy the BOOTROM.SYS file when upgrading unless it is required. See 2.1.2 “Important information” (p. 9).

2.3.2 Steps

1

Back up the existing configuration files for the CPAA that you are planning to upgrade. Ensure that the following files are backed up:

- bof.cfg
- CPAA configuration file

See “To create a 7701 CPAA backup policy” in the *NSP NFM-P Control Plane Assurance Manager User Guide*.

2

Ensure that the COM1 serial port is connected to a terminal server, then open a Telnet session on that connection.

3

If you are performing an upgrade, proceed to Step 4.

If you are performing an initial installation, you must change the management port IP address and assign a static route. Use the following CLI commands, and insert the IP address, mask, and file names required for your network:

```
A:CPAA_name# bof↵

A:CPAA_name>bof# no static-route IP_address/mask next-hop IP_address↵

A:CPAA_name>bof# address management_port_IP_address/mask active↵

A:CPAA_name>bof# static-route IP_address/mask next-hop gateway_IP_
address↵

A:CPAA_name>bof# save↵
```

Note: The default SNMP Engine ID is derived from the management IP that you specify in the bof.cfg file. If you specify the same management IP address for two different 7701 CPAAs, they have the same SNMP Engine ID.
The SNMP Engine ID of the 7701 CPAA is used for SNMPv3. To use SNMP, you must ensure that you specify a unique management port IP address for each 7701 CPAA.

The following is a sample configuration:

```
A:CPAA# bof↵

A:CPAA>bof# no static-route 198.51.0.0/16 next-hop 198.51.185.1↵
```

```
A:CPAA>bof# address 198.51.9.8/24 active↵

A:CPAA>bof# static-route 198.51.0.0/16 next-hop 198.51.9.1↵

A:CPAA>bof# save↵
```

4

Create a directory on the CPAA for the upgrade files. Use the following commands:

```
A:CPAA_name# file↵

A:CPAA_name>file cf1:\ # md new_load↵

A:CPAA_name>file cf1:\ # cd new_load↵

A:CPAA_name# exit↵
```

5

Use FTP or SCP to copy the new boot.tim and both.tim files to the directory created in Step 4.

If you use FTP, you must enable FTP on the CPAA. Use the following commands:

```
A:CPAA_name# configure system security↵

A:CPAA_name>config>system>security#  ftp-server↵

A:CPAA_name>config>system>security# user user_name↵

A:CPAA_name>config>system>security>user$ password password↵

A:CPAA_name>config>system>security>user$ access ftp↵

A:CPAA_nameconfig>system>security>user$ exit all↵

A:CPAA_name# admin save↵
```

For FTP, use binary mode.

6

Confirm that the file transfer is successful.

7

Modify the bof.cfg to designate the primary and secondary image locations. Use the existing primary-image path as the secondary-image path. Use the *new_load* path created in Step 4 as the primary-image path.

Use the following commands:

```
A:CPAA_name# bof↵
```

A:*CPAA_name*>bof# secondary-image cf1:*previous primary-image path*\both.tim↵

A:*CPAA_name*>bof# primary-image cf1:*new_load*\both.tim↵

A:*CPAA_name*>bof# save↵

You can view the current bof.cfg configuration by using the **show bof** command.

8

Reboot the appliance, then stop the boot process to configure the boot parameters by clicking on any key when the following message appears:

Press any key to stop auto-boot...↵

This may take several minutes.

9

Type p (for print) to view the content of the NVRAM.DAT file.

You can enter ? to view other command options and information.

10

Type c (change) to change the content of the NVRAM.DAT file. Configure the parameters:

boot device : ata=0,0 ↵

unit number : 0 ↵

processor number : 0 ↵

host name : *host_name*↵

file name : *boot_load_pathname*/boot.tim↵

inet on ethernet (e) : *management_port_IP_address*:*ffffffff*↵

inet on backplane (b): *ftp_server_IP_address*↵

host inet (h) : *ftp_server_IP_address*↵

gateway inet (g) : *gateway_IP_address*↵

user (u) : *ftp_username*↵

ftp password (pw) : *ftp_password*↵

flags (f) : 0x0↵

```
target name (tn)      : CPAA_name↲
```

Some of the NVRAM.DAT parameters are optional, depending on the option configured for **boot device**. For example, the inet on backplane, host inet, gateway inet, user, and ftp password parameters apply when you boot from the network, when the boot device is fei. However, the inet on ethernet (e) parameter is not optional. See Table 2-1, “7701 CPAA files” (p. 10).

The following is a sample configuration:

```
boot device           : ata=0,0↲

unit number           : 0↲

processor number      : 0↲

host name             : ↲

file name             : cf1:\new_load\boot.tim↲

inet on ethernet (e)  : management_port_IP_address:ffffffff↲

inet on backplane (b): 0.0.0.0↲

host inet (h)         : 0.0.0.0↲

gateway inet (g)      : 0.0.0.0↲

user (u)              : ↲

ftp password (pw)     : ↲

flags (f)             : 0x0↲

target name (tn)      : CPAA_name↲
```

11

Enter @ to save the changes and continue the boot process.

12

Wait for the system to reboot. The system is fully rebooted when the login prompt appears.

Note: The contents of the NVRAM.DAT file can be changed during a reboot, as required. See Table 2-1, “7701 CPAA files” (p. 10) for a description of the parameters.

13

Verify that the upgrade was successful by using the **show version** command:

END OF STEPS

2.4 To upgrade the 7701 CPAA Hardware Revision 2 OS software using the NFM-P client GUI

2.4.1 Important information

For the 7701 CPAA Revision 2 hardware, software upgrades performed from the NFM-P client GUI use the software download method. Ensure that the Software Download option is selected when you create a software upgrade policy for the 7701 CPAA Revision 2 hardware. The software download method does not provide automatic reboot of the NE; you must perform a manual reboot using a CLI. You must also use a CLI to modify the NVRAM.DAT and bof.cfg files.

See the “NE software upgrades” chapter in the *NSP NFM-P User Guide* for more information about NE software upgrades.

Do not copy the BOOTROM.SYS file when upgrading unless it is required. See 2.1.2 “Important information” (p. 9).

You must configure the system IP address and enable SNMP and the FTP server on the 7701 CPAA Hardware Revision 2. See the “Device commissioning and management” chapter in the *NSP NFM-P User Guide* for information.

2.4.2 Steps

1

The 7701 CPAAs you are upgrading must be administratively down. To turn down the 7701 CPAA, perform the following:

1. Choose Tools→Route Analysis→Admin Domains/CPAAs from theNFM-P main menu. The Admin Domains/CPAAs form opens.
2. Choose CPAA (CPAM: Topology) from the object drop-down and click Search. A list of discovered 7701 CPAAs appears.
3. For each 7701 CPAA that you need to turn down, double-click on the entry in the list. The CPAA (Edit) form opens.
4. Set the Administrative State parameter to Down and click Apply.
5. Close the CPAA (Edit) form.
6. Close the Admin Domains/CPAAs form.

2

Import the new 7701 CPAA software image into the NFM-P database.

1. Copy or move the files to a location that is accessible to the NFM-P.

   The required files are:

   - boot.tim
   - both.tim
   - md5sums.txt

   Ensure that the required files are all within the same folder. For more information see “To import device software files to the NFM-P” in the *NSP NFM-P User Guide*.

2. Choose Administration→NE Maintenance→Software Upgrade from the NFM-P main menu. The Software Upgrade form opens.
3. Click on the Software Images tab, then on the SR Software Images subtab, if required.
4. Click on the Import button. The Open form opens.
5. Navigate to the directory that contains the software image and click Open. The Open form closes.

   The NFM-P verifies the file set, imports the files to the database, and displays an entry for the imported image in the list on the Software Images tab.

   For the 7701 CPAA, the Target Product name is Alcatel-SR/ESS-7XXX by default.
6. Confirm that the image is valid, and is the correct version.

3

Create a 7701 CPAA software upgrade policy.

1. Click on the Software Upgrade Policy tab, then click Create. The Software Upgrade Policy (Create) form opens.
2. Configure the following parameters:
   - Policy ID
   - Auto-Assign ID
   - Name
   - Policy Type
   - CFlash Image Root Path
   - CFlash Backup Root Path

   You must choose SR Based Node as the Policy Type.

   The 7701 CPAA Revision 2 hardware supports only one compact flash, designated as cf1. Ensure that you specify cf1 when you configure the CFlash Image Root Path and CFlash Backup Root Path parameters.
3. Enable the Software Download parameter and click Apply. The Software Upgrade Policy (Create) form refreshes with additional tabs, and the form name changes to Software Upgrade Policy (Edit).

4

Assign the policy to the required 7701 CPAAs.

1. Click on the Software Upgrade Policy Assignment tab. The Software Upgrade Policy (Edit) Filter form opens.
2. Configure a filter, if required, and click OK. A list of CPAAs is displayed in the Unassigned Sites panel.
3. Select one or more 7701 CPAAs in the Unassigned Sites list and click on the right-arrow button to move them to the Assigned Sites list.
4. Click OK and confirm the action. The policy is assigned to the NEs, and the Software Upgrade Policy (Edit) form closes. The Software Upgrade form is displayed.

5

Perform the 7701 CPAA upgrade.

1. On the Software Upgrade form, click on the Software Images tab.
2. Select the new 7701 CPAA software image that you imported in Step 2 and click Upgrade Sites. The Select Sites form opens.
3. Select one or more 7701 CPAAs from the list and click OK, then confirm the action.

The NFM-P downloads the software to the selected 7701 CPAAs, in the directory TiMOS-B-*Release number*, where *Release number* is the version of the downloaded software.

6

Open a CLI session on each CPAA to perform the following:

- Modify the NVRAM.DAT and bof.cfg files to point to the new files in TiMOS-B-*Release number*.
- Verify that the upgrade was successful
- Reboot the upgraded 7701 CPAAs

See 2.3 “To install or upgrade the 7701 CPAA Hardware Revision 2 OS software using a CLI” (p. 12) .

END OF STEPS

3 vCPAA setup

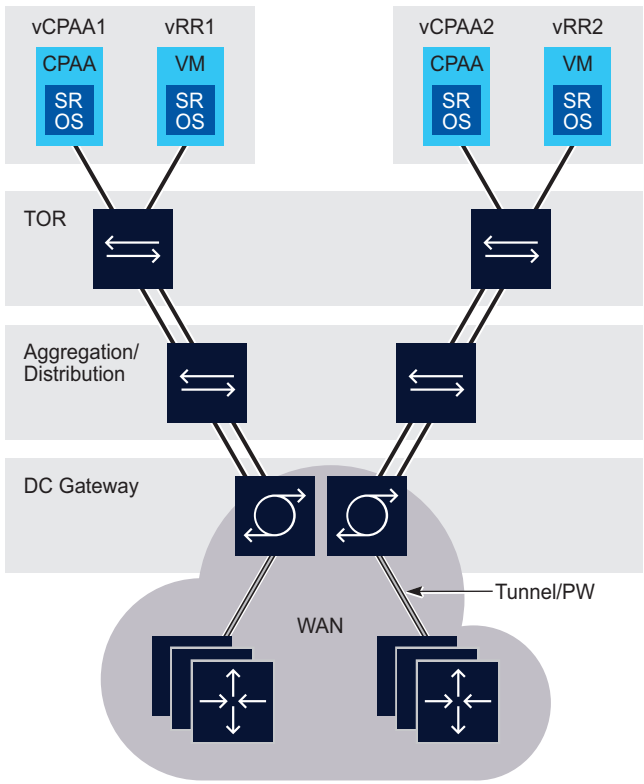
3.1 vCPAA setup overview

3.1.1 Introduction

The vCPAA, or virtual CPAA, is designed to run as a virtual machine on a host that supports virtualization. Each vCPAA corresponds to one virtual machine, and multiple virtual machines can be deployed on a single host. The vCPAA provides the same control and management plane features as a hardware-based 7701 CPAA.

The vCPAA can be deployed in data centers, WAN POPs, or a combination of both. When deployed in data centers, IGP and BGP traffic must be leaked from the WAN into the data centers, so that the vCPAA can establish IGP adjacencies and IBGP sessions. vCPAA control traffic can be tunneled from the DC edge to an arbitrary WAN location to analyze CP changes remotely. vCPAA can connect to the vRR via internal bridge mechanisms to obtain all information (IGP and BGP) directly from the vRR. See the DC deployment example in the following figure:

Figure 3-1 vCPAA DC deployment



The licensing model for the vCPAA is identical to that of the hardware-based 7701 CPAA. See the *NSP Installation and Upgrade Guide* for more information.

The NFM-P discovers vCPAAs and hardware-based 7701 CPAAs in the same way. See the *NSP NFM-P Control Plane Assurance Manager User Guide* for more information.

Scalability and performance for the vCPAA are subject to limitations. For information about IGP and BGP scalability and performance, see the *NSP Planning Guide*.

The 7701 CPAA hardware rev.2 and vCPAA do not support power supply alarms or power failure alarms. The CPAA OS has no visibility of the power supply, and cannot detect power interruptions.

VM backup is not supported for vCPAA.

The vCPAA does not support packet forwarding.

3.2 Host hardware requirements

3.2.1 Overview

Prior to installing the vCPAA, the user must ensure that the host meets the specified hardware requirements. See the following table:

Table 3-1 Host hardware and system requirements

Spec	Supported (Intel x86)	Supported (IntelXeon)	Recommended
CPU type	Intel x86	IntelXeon	IntelXeon
CPU architecture	Sandy Bridge, Ivy Bridge, Haswell, Skylake-Client	Sandy Bridge, Ivy Bridge, Haswell, Skylake-Client-IBRS. Cascade Lake	Skylake-Client
CPU - number of processors	1-2	1-2	1-2
CPU - number of cores [threads]	2 [4], 4 [8], 6 [12]	4 [8], 6 [12], 8 [16]	4 [8], 6 [12], 8 [16]
Memory	8 GB+	8 GB+	8 GB+
Interfaces (NIC controller)	GigE 10GigE	GigE	GigE
KVM Hypervisor	Centos 6.4; RHEL 7.3, 7.5, and 7.9	Centos 6.4; RHEL 7.3, 7.5, and 7.9	RHEL 7.9
VMware Hypervisor	ESXi 5.5, 6.0, 6.5, 6.7, and 7.0	ESXi 5.5, 6.0, 6.5, 6.7, and 7.0	ESXi 7.0

Note: Intel GigE is the recommended NIC controller, or any other NIC controller not using the tg3v3.124 driver.

The user is responsible for host selection, maintenance, and support.

3.3 Host software requirements

3.3.1 Overview

Prior to installing the vCPAA, the user must ensure that the host meets the following software requirements:

- Kernel Virtualization is supported
- KSDM (kernel shared memory daemon) is disabled

3.4 Virtual hardware configuration

3.4.1 Overview

The vCPAA mimics an SR-12 chassis equipped with:

- One SFM3-12 installed in slot A
- No SFM installed in slot B
- One IOM installed in slot 1 (iom-ra1)
- One 4-port GE SFP MDA installed in slot 1/1 (m4-1gb-tx)
- One CF3 disk (additional CF devices can be added)

Each vCPAA should be configured as follows, where KVM or VMware is configured as the hypervisor:

Table 3-2 Virtual machine configuration

Parameter	Supported	Recommended
Memory	4GB+	4GB+
Virtual CPUs - mode	Custom	Custom
Virtual CPUs - number	1 with dual core	1 with dual core
Virtual CPUs - pinning	Required	Required
Virtual disks - number	1	1
Virtual disks - type	KVM: QCOW2 image file VMware: OVF image file	KMV: QCOW2 image file VMware: OVF image file
Virtual disks - driver	KVM: virtIO VMware: vmhba	KMV: virtIO VMware: vmhba
Virtual NIC - interfaces	1-5	1-5
Virtual NIC - type	KVM: bridge or direct VMware: vSwitch, bridge, or direct	KVM: bridge or direct VMware: vSwitch
Virtual NIC - model	KVM: virtIO VMware: vmnic	KVM: virtIO VMware: vmnic

Table 3-2 Virtual machine configuration (continued)

Parameter	Supported	Recommended
Console serial port	KVM: physical serial port, or bind to available host TCP port VMware: bind to available host TCP port	Bind to available host TCP port

Note: Nokia recommends providing 1 GB of HDD space for each virtual machine, in addition to any HDD space required to run the host OS or hypervisor.

The vCPAA must be shutdown before performing certain tasks on the host, such as increasing or decreasing the amount of virtual CPUs, changing CPU pinning information, increasing or decreasing the VM memory, adding or removing a disk, or adding or removing network interfaces.

The setup process for vCPAA on VMware is user-specific, and may vary depending on your system configuration. For issues that are not resolved by existing resources, contact your Nokia representative for assistance.

3.5 Virtual software configuration

3.5.1 Software packages

You can install the vCPAA using either a KVM or a VMware hypervisor. Each hypervisor requires a specific file package.

For KVM installations the image file is cpaa-vm.qcow2. For VMware installations, the image file is cpaa-vm.ova. Each file package contains boot-loader files, image binaries for CPAA, a minimal/generic configuration file, and a minimum/generic BOF (boot options file). Each vCPAA needs a copy of this image file, which it considers equivalent to its CF3 disk, which is the boot disk of the vCPAA. New file packages are built for every release, containing the features, bug fixes, and enhancements delivered in the corresponding hardware load.

You can download the latest software from OLCS, under the NSP product hierarchy.

4 vCPAA installation and upgrade

4.1 vCPAA installation overview

4.1.1 General information

The vCPAA is supported on the following hypervisors:

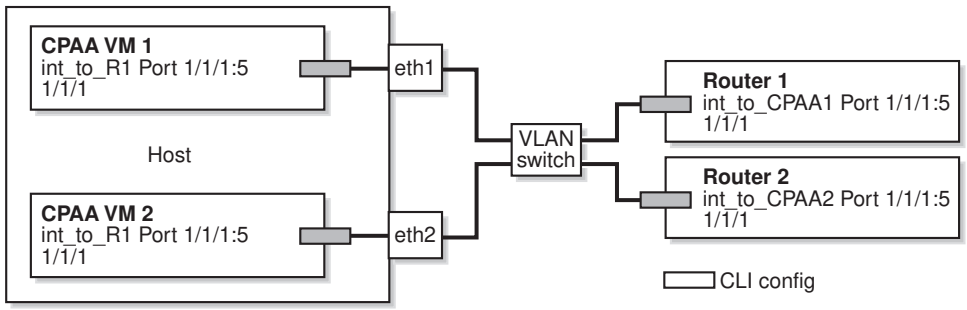
- KVM, using a QCOW2 image file
- VMware, using an ova image file

The vCPAA supports two interface models: direct and bridge.

4.1.2 Direct interface model

When the vCPAA is configured using the direct interface model, the hypervisor creates a one-to-one binding between the VM network interface and a physical network interface on the host. As such, the number of vCPAAs is limited to the number of physical network interfaces assigned on the host. Multiple interfaces may be specified per vCPAA using qtags (dot1.q). See the direct interface model deployment example in the following figure:

Figure 4-1 vCPAA direct interface model deployment



24490

where

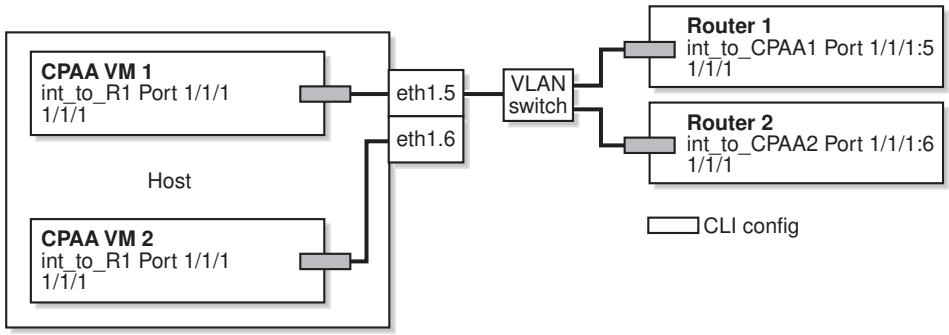
int_to_*port* is a sample interface configured inside the VM

Note: IP management port diagrams are not shown.
VLAN switch programming is operator-dependent.

The direct interface model can also be deployed using sub-interfaces on the host rather than physical network interfaces. This allows the number of vCPAAs to exceed the number of physical

network interfaces assigned on the host, however, each vCPAA has only four logical ports and therefore, only four interface adjacencies. See the direct interface model using sub-interfaces deployment example in the following figure:

Figure 4-2 vCPAA direct interface model using sub-interfaces deployment



where

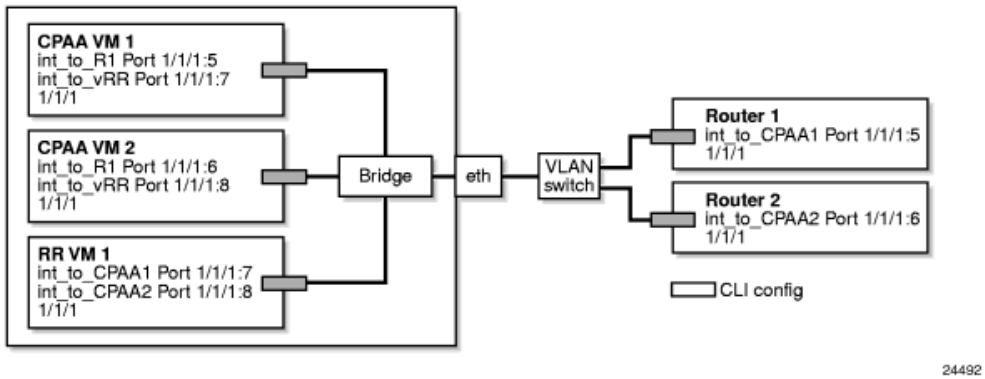
int_to_*port* is a sample interface configured inside the VM

Note: IP management port diagrams are not shown.
VLAN switch programming is operator dependent.

4.1.3 Bridge interface model

When the vCPAA is configured using the bridge interface model, the hypervisor connects the VM network interface to a host bridge. Physical network interfaces are also connected to the host bridge, allowing vCPAAs to share physical network interfaces and communicate internally. Logical ports configured on these vCPAAs must have different tag values. The bridge interface model is required for host programming, and is recommended for eth0 VM network interfaces (associated with the A/1 management port). See the bridge interface model deployment example in the following figure:

Figure 4-3 vCPAA bridge interface model deployment



where

int_to_*port* is a sample interface configured inside the VM

Note: IP management port diagrams are not shown.
VLAN switch programming is operator dependent.

4.1.4 vCPAA installation

You can install the vCPAA using either a KVM or a VMware hypervisor.

If you are using VMware, see 4.4 “To deploy a vCPAA on VMware using the vSphere Client” (p. 30).

Note: The process for installing a vCPAA on VMware is user-specific, and may vary depending on your system configuration. For issues that are not resolved by existing resources, contact your Nokia representative for assistance.

If you are using KVM, see 4.2 “vCPAA installation workflow for KVM” (p. 27).

4.2 vCPAA installation workflow for KVM

4.2.1 Stages

1

Copy the cpaa-vm.qcow2 image file to a directory on the host machine, for example: /var/lib/libvirt/images/. See the 3.5 “Virtual software configuration” (p. 24) section for more information.

2

Create the vCPAA. See 4.3 “To create a vCPAA on a KVM hypervisor” (p. 28) for more information.

3

Start the VM using the following command: virsh create /var/lib/libvirt/images/vcpaa.xml

Note: The above command is an example only. The actual command must reflect the directory in which the XML file was saved, and the name of the XML file.

4

Connect to the console port of the vCPAA using a Telnet session to the host.

5

If prompted, enter BOF data (management port IP address, static routes).

4.3 To create a vCPAA on a KVM hypervisor

4.3.1 Steps

1

Navigate to the desired directory on the host machine.

2

Create the XML file as follows:

Note: The values used in this procedure are specific to this example. The actual values must reflect the user's setup.

```
    <domain type="kvm">
<memory>4194304</memory>
<currentMemory>4194304</memory>
<name>vsim98_66</name>
<uuid>df806b10-c863-40fd-2187-dead98066001</uuid>
<cpu mode="custom" match="minimum">
<model>SandyBridge</model>
<vendor>Intel</vendor>
</cpu>
<vcpu current="4">4</vcpu>
<os>
<type arch="x86_64" machine="rhel7.3.0">hvm</type>
<boot dev="hd"/>
<smbios mode="emulate"/>
</os>
<clock offset="utc">
<timer name="pit" tickpolicy="delay"/>
<timer name="rtc" tickpolicy="delay"/>
</clock>
<devices>
<emulator>/usr/libexec/qemu-kvm</emulator>
```

```
<disk type="file" device="disk">
<driver name='qemu' type='qcow2' cache="none"/>
<source file="/var/lib/libvirt/images/cpaa-vm.qcow2"/>
<target dev="hda" bus="virtio"/>
</disk> -->
```

3

In the XML file, configure the following lines to map the host physical interface to the vCPAA IP management port A/1:

```
<interface type="bridge">
<mac address="DE:AD:98:66:01:01:/>
<source bridge="breth0/>
<model type="virtio/>
</interface>
```

4

Perform one of the following:

a. In the XML file, configure the following lines to map the host physical interface(s) to the vCPAA logical network interface port(s) 1/1/1...1/1/4 with the bridge interface model:

```
<interface type="bridge">
<mac address="DE:AD:98:66:01:02/>
<source bridge="breth1"/>
<model type="virtio"/>
</interface>
```

b. In the XML file, configure the following lines to map the host physical interface(s) to the vCPAA logical network interface port(s) 1/1/1...1/1/4 with the direct interface model:

```
<interface type="direct">
<mac address="DE:AD:98:66:01:02/>
<source dev="eth1" mode=passthrough"/>
<model type="virtio"/>
</interface>
```

5

In the XML file, configure the following lines to specify the console port of the vCPAA:

```
<console type="tcp">
<source mode="bind" host="198.51.98.62" service="40066"/>
<protocol type="telnet"/>
<target port="0"/>
<alias name="serial0"/>
</console>
```

6

In the XML file, configure the following lines to close the configuration of the vCPAA:

```
</devices>
<seclabel type="none"/>
</domain>
```

7

Save and close the XML file.

END OF STEPS

4.4 To deploy a vCPAA on VMware using the vSphere Client

4.4.1 Preliminary information

This procedure is intended for administrators who are familiar with the creation of VMware virtual machines and the deployment of applications on those machines.

This procedure provides recommendations for vCPAA deployment that allow an administrator to configure a Telnet console, which is then used to edit the bof.cfg file and assign a management IP address. Subsequent vCPAA configurations are performed using the management address.

This procedure assumes the following:

- VMware is installed on the required server, with default settings
- The vSphere client is functional and has access to that server
- The vCPAA OVF file package is accessible
- Telnet is enabled

Note: The process for installing a vCPAA on VMware is user-specific, and may vary depending on your system configuration. For issues that are not resolved by existing resources, contact your Nokia representative for assistance.

Nokia recommends using the vSwitch interface model for VMware.

Nokia is not responsible for changes in the VMware application that may render these instructions inaccurate or obsolete.

If you are unable to open a Telnet session to the TCP port that is being used as serial connection to the vCPAA, you may need to add a firewall exception on the VMware hypervisor for that port.

4.4.2 Steps

1

Open the vSphere client. In the inventory panel, select the server where you want to deploy the virtual CPAA.

2

Enable a serial port connection on the server:

1. Click on the Configurations tab and select Security Profile in the Software menu.
2. Ensure that the **VM serial port connected over network** parameter is enabled.

   On later versions of EXSi, you may have to open the Firewall Properties form to enable the check box.

   Enabling the serial port connection allows a Telnet session on the server.

3

Choose File→Deploy OVF Template from the vSphere main menu. The Deploy OVF Template step form opens.

4

Ensure the following selections and settings as you go through the steps:

1. When selecting the **Source**, specify the location of the vCPAA OVF package file.
2. When selecting the **Disk Format**, choose Thin Provision.
3. When configuring **Network Mapping**, the first port in the list must be mapped to your management network.

5

Click Finish to deploy the OVF template. This may take a few minutes.

6

On the vSphere client, in the inventory panel, select the newly deployed vCPAA VM.

7

Configure a TCP console on the VM:

1. Click Edit virtual machine settings. The Virtual Machine Properties form opens. The Hardware tab displays a list of provisioned hardware.
2. Click Add. The Add Hardware step form opens.
3. Select Serial Port and click Next.
4. Select Connect via Network and click Next.
5. In the Network Backing panel, select Server (VM listens for connection) and enter the Port URI. For example:

   telnet://:<*port #*>

   where <*port #*> is an available TCP port. This port will enable a Telnet connection to the vCPAA through the VMware server IP address.
6. Complete the configuration.
7. Verify that the newly configured serial port is displayed in the list on the Hardware tab.

8

Power up the vCPAA.

9

Telnet to the VMware server using the port number specified in Step 7. The VMware server will forward the session to the newly created vCPAA, allowing configuration of the vCPAA.

10

Edit the bof.cfg file to add a management IP address and a static route for the vCPAA, to provide independent access through the management network.

11

Save the vCPAA configuration, and reboot.

12

Open a Telnet session on the vCPAA using the management IP address in the bof.cfg file, to confirm management connectivity.

END OF STEPS

4.5 vCPAA Upgrades

4.5.1 Upgrade methods

You can upgrade the software on the vCPAA by the following methods:

- Using a CLI; see 4.6 “To upgrade the vCPAA software using a CLI” (p. 32).
- Using the NFM-P software upgrade functionality; see 4.7 “To upgrade the vCPAA OS software using the NFM-P client GUI” (p. 36). This method allows you to upgrade the image on multiple CPAAs at one time. However, a CLI must be used to modify the NVRAM.DAT and bof.cfg files for each device, and to verify the upgrade and reboot the device.

  For information about the NFM-P NE upgrade functionality; see the “NE software upgrades” chapter in the *NSP NFM-P User Guide*.

4.6 To upgrade the vCPAA software using a CLI

WARNING

Equipment Damage

Do not add, modify, or delete the content of the last stable version of the boot files. They must be preserved in case they are required as a secondary image.

4.6.1 Before you begin

The following procedure describes Nokia's recommendations for using a CLI to install or upgrade the software on a vCPAA. Variations on this procedure are possible, depending on your system and requirements.

Place the installation or upgrade files in a location that is accessible using FTP or SCP.

For information about 7701 CPAA software files, see Table 2-1, "7701 CPAA files" (p. 10).

4.6.2 Steps

1

Back up the existing configuration files for the CPAA that you are planning to upgrade. Ensure that the following files are backed up:

- bof.cfg
- CPAA configuration file

See "To create a 7701 CPAA backup policy" in the *NSP NFM-P Control Plane Assurance Manager User Guide*.

2

Ensure that the serial port is connected to a terminal server, then open a Telnet session on that connection.

3

Create a directory on the CPAA for the upgrade files. Use the following commands:

```
A:CPAA_name# file↵

A:CPAA_name>file cf3:\ # md new_load↵

A:CPAA_name>file cf3:\ # cd new_load↵

A:CPAA_name# exit↵
```

4

Use FTP or SCP to copy the new boot.tim and both.tim files to the directory created in Step 3.

If you use FTP, you must enable FTP on the CPAA. Use the following commands:

```
A:CPAA_name# configure system security↵

A:CPAA_name>config>system>security#  ftp-server↵

A:CPAA_name>config>system>security# user user_name↵

A:CPAA_name>config>system>security>user$ password password↵
```

A:*CPAA_name*>config>system>security>user$ access ftp↵

A:*CPAA_name*config>system>security>user$ exit all↵

A:*CPAA_name*# admin save↵

For FTP, use binary mode.

5

Confirm that the file transfer is successful.

6

Modify the bof.cfg to designate the primary and secondary image locations. Use the existing primary-image path as the secondary-image path. Use the *new_load* path created in Step 3 as the primary-image path.

Use the following commands:

A:*CPAA_name*# bof↵

A:*CPAA_name*>bof# secondary-image cf1:*previous primary-image path*\both.tim↵

A:*CPAA_name*>bof# primary-image cf1:*new_load*\both.tim↵

A:*CPAA_name*>bof# save↵

You can view the current bof.cfg configuration by using the **show bof** command.

7

Reboot the appliance, then stop the boot process to configure the boot parameters by clicking on any key when the following message appears:

Press any key to stop auto-boot...↵

This may take several minutes.

8

Type p (for print) to view the content of the NVRAM.DAT file.

You can enter ? to view other command options and information.

9

Type c (change) to change the content of the NVRAM.DAT file. Configure the parameters:

boot device : ata=0,2 ↵

unit number : 0 ↵

processor number : 0 ↵

```
host name            : host_name↵

file name            : boot_load_pathname/boot.tim↵

inet on ethernet (e) : management_port_IP_address:ffffffff↵

inet on backplane (b): ftp_server_IP_address↵

host inet (h)        : ftp_server_IP_address↵

gateway inet (g)     : gateway_IP_address↵

user (u)             : ftp_username↵

ftp password (pw)    : ftp_password↵

flags (f)            : 0x0↵

target name (tn)     : CPAA_name↵
```

Some of the NVRAM.DAT parameters are optional, depending on the option configured for **boot device**. For example, the inet on backplane, host inet, gateway inet, user, and ftp password parameters apply when you boot from the network, when the boot device is fei. However, the inet on ethernet (e) parameter is not optional. See Table 2-1, “7701 CPAA files” (p. 10).

The following is a sample configuration:

```
boot device          : ata=0,2↵

unit number          : 0↵

processor number     : 0↵

host name            : ↵

file name            : cf3:\new_load\boot.tim↵

inet on ethernet (e) : management_port_IP_address:ffffffff↵

inet on backplane (b): 0.0.0.0↵

host inet (h)        : 0.0.0.0↵

gateway inet (g)     : 0.0.0.0↵

user (u)             : ↵

ftp password (pw)    : ↵
```

```
flags (f)              : 0x0↵

target name (tn)       : CPAA_name↵
```

10

Enter @ to save the changes and continue the boot process.

11

Wait for the system to reboot. The system is fully rebooted when the login prompt appears.

Note: The contents of the NVRAM.DAT file can be changed during a reboot, as required. See Table 2-1, “7701 CPAA files” (p. 10) for a description of the parameters.

12

Verify that the upgrade was successful by using the **show version** command.

END OF STEPS

4.7 To upgrade the vCPAA OS software using the NFM-P client GUI

4.7.1 Important information

For the vCPAA, software upgrades performed from the NFM-P client GUI use the software download method. Ensure that the Software Download option is selected when you create a software upgrade policy for the vCPAA. The software download method does not provide automatic reboot of the NE; you must perform a manual reboot using a CLI. You must also use a CLI to modify the NVRAM.DAT and bof.cfg files.

See the “NE software upgrades” chapter in the *NSP NFM-P User Guide* for more information about NE software upgrades.

You must configure the system IP address and enable SNMP and the FTP server on the vCPAA. See the “Device commissioning and management” chapter in the *NSP NFM-P User Guide* for information.

4.7.2 Steps

1

The vCPAAs you are upgrading must be administratively down. To turn down the vCPAA, perform the following:

1. Choose Tools→Route Analysis→Admin Domains/CPAAs from theNFM-P main menu. The Admin Domains/CPAAs form opens.
2. Choose CPAA (CPAM: Topology) from the object drop-down and click Search. A list of discovered CPAAs appears.
3. For each vCPAA that you need to turn down, double-click on the entry in the list. The CPAA (Edit) form opens.

4. Set the Administrative State parameter to Down and click Apply.
5. Close the CPAA (Edit) form.
6. Close the Admin Domains/CPAAs form.

2

Import the new CPAA software image into the NFM-P database.

1. Copy or move the files to a location that is accessible to the NFM-P

   The required files are:
   - boot.tim
   - both.tim
   - md5sums.txt

   Ensure that the required files are all within the same folder. For more information see “To import device software files to the NFM-P” in the *NSP NFM-P User Guide*.
2. Choose Administration→NE Maintenance→Software Upgrade from the NFM-P main menu. The Software Upgrade form opens.
3. Click on the Software Images tab, then on the SR Software Images subtab, if required.
4. Click on the Import button. The Open form opens.
5. Navigate to the directory that contains the software image and click Open. The Open form closes.

   The NFM-P verifies the file set, imports the files to the database, and displays an entry for the imported image in the list on the Software Images tab.

   For the CPAA, the Target Product name is Alcatel-SR/ESS-7XXX by default.
6. Confirm that the image is valid, and is the correct version.

3

Create a CPAA software upgrade policy.

1. Click on the Software Upgrade Policy tab, then click Create. The Software Upgrade Policy (Create) form opens.
2. Configure the following parameters:
   - Policy ID
   - Auto-Assign ID
   - Name
   - Policy Type
   - CFlash Image Root Path

   You must choose SR Based Node as the Policy Type.

   The vCPAA does not require a CFlash Backup Root Path.
3. Enable the Software Download parameter and click Apply. The Software Upgrade Policy (Create) form refreshes with additional tabs, and the form name changes to Software Upgrade Policy (Edit).

4

Assign the policy to the required vCPAAs.

1. Click on the Software Upgrade Policy Assignment tab. The Software Upgrade Policy (Edit) Filter form opens.
2. Configure a filter, if required, and click OK. A list of CPAAs is displayed in the Unassigned Sites panel.
3. Select one or more vCPAAs in the Unassigned Sites list and click on the right-arrow button to move them to the Assigned Sites list.
4. Click OK and confirm the action. The policy is assigned to the NEs, and the Software Upgrade Policy (Edit) form closes. The Software Upgrade form is displayed.

5

Perform the CPAA upgrade.

1. On the Software Upgrade form, click on the Software Images tab.
2. Select the new CPAA software image that you imported in Step 2 and click Upgrade Sites. The Select Sites form opens.
3. Select one or more vCPAAs from the list and click OK, then confirm the action.

The NFM-P downloads the software to the selected CPAAs, in the directory TiMOS-B-*Release number*, where *Release number* is the version of the downloaded software.

6

Open a CLI session on each CPAA to perform the following:

- Modify the NVRAM.DAT and bof.cfg files to point to the new files in TiMOS-B-*Release number*.
- Reboot the upgraded vCPAAs
- Verify that the upgrade was successful

See 4.6 “To upgrade the vCPAA software using a CLI” (p. 32) .

END OF STEPS

5 CPAA commissioning and discovery

5.1 CPAA commissioning and discovery overview

5.1.1 Introduction

The discovery process is similar to the discovery process of the 7750 SR and 7450 ESS. The NFM-P discovers CPAAs using SNMP. During the discovery process, the NFM-P scans the network for devices according to user-defined IP addresses or IP address ranges. When the system IP address, or ID, is used to discover the device, management is in-band. After you discover the CPAAs, you can create network interfaces and routing instances to discover OSPF and ISIS network topologies and BGP networks.

The 7701 CPAA and vCPAA are managed by the NFM-P like any other NE. Management procedures such as timing synchronization, polling, deployments, and NE resynchronization are similar to procedures for other SR OS devices. See the *NSP NFM-P User Guide* for information about general device management functions.

5.2 Device commissioning and network discovery workflow

5.2.1 Purpose

The following workflow outlines the high-level steps necessary to commission devices and discover the network. This workflow assumes that the CLI has been used to verify that each CPAA to be discovered and managed using SNMPv2c or SNMPv3 has a unique engine ID, and to configure the SNMP security parameters on those CPAAs. Mediation must also be configured.

5.2.2 Stages

1

Perform one of the following:

a.

To discover CPAAs:

1. Create discovery rules.
2. Discover CPAAs by scanning the network according to discovery rules.
3. Set each discovered CPAA to a managed state.
4. Reconcile device elements into the NFM-P database.
5. Check the discovery, management, and reconciliation status of the CPAAs.

b.

To manage device discovery:

1. Modify the discovery rules.

2. Add or modify rule elements.
3. Enable or disable the discovery rules.
4. Delete the discovery rules.
5. Scan the network according to a discovery rule.
6. Manage or unmanage the CPAAs.
7. Reconcile device elements into the NFM-P database.

c.

To configure managed routers:

1. Configure IP interfaces to designated routing domains.
2. Configure OSPF interfaces.
3. Configure ISIS interfaces.

See 5.3 “To discover CPAAs” (p. 41) for more information.

2

Create OSPF and ISIS instances on the CPAA. See 5.4 “To configure OSPF and ISIS on a CPAA” (p. 43) for more information.

3

Create an IGP administrative domain. See 5.5 “To configure an IGP administrative domain” (p. 44) for more information.

4

To configure route listening and analysis functions:

1. Configure the IGP role for OSPF or ISIS.
2. Associate the CPAA to an IGP administrative domain.
3. Enable CPAM-CPAA event history registration or retrieve IGP data from the CPAA.

   See 5.6 “To configure route listening and analysis on a CPAA” (p. 46) for more information.

5

As required, deploy a CPAA to monitor a BGP AS. See 5.7 “To deploy a CPAA to monitor a BGP AS” (p. 47) for more information.

6

As required, configure CPAM-CPAA event registration. See 5.8 “To configure CPAM-CPAA event registration” (p. 49) for more information.

7

As required, view the update times on a CPAA for IGP and BGP information. See 5.9 “To view CPAA update times information” (p. 49) for more information.

8

As required, delete an IGP administrative domain. See 5.10 “To delete an IGP administrative domain” (p. 50) for more information.

9

Configure redundancy. See Chapter 6, “CPAA Redundancy” for more information.

5.3 To discover CPAAs

5.3.1 Steps

1

Choose Administration→Discovery Manager from the NFM-P main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

2

Create one or more discovery rules to discover the CPAA devices. Perform the following:

1. Click on the Create button. The Create Discovery Rule - Specify General Attributes form opens.
2. Configure the parameters:
   - ID
   - Auto-Assign ID
   - Description
   - Administrative State

     When you set the Administrative State parameter to Up, the network is scanned according to the discovery rule when the discovery rule is saved. The network is also scanned according to the discovery rule as specified by the Discovery Rule Scan Interval parameter in the PollerManager form. When you set the administrative state to Down, the network is not scanned as specified by these conditions.
   - OLC State
3. Click on the Next button. The Add Rule Elements form opens.
4. Click on the Create button. The Topology Discovery Rule Element (Create) form opens.
5. Configure the parameters:
   - IP Address
   - Mask Bits
   - Usage

   Note:

   You should track the IP addresses used to discover devices. When the IP address used to discover the device is the system IP address, or ID, management is out-of-band.
6. Click on the OK button. The Topology Discovery Rule Element (Create) form closes. The discovery rule is saved.
7. Perform substeps 4 to 6 to add more rule elements.

8. Click on the Next button. The Configure Mediation Security form opens.
9. Specify the mediation policies for read access, write access, and SNMP trap access. See the “Mediation and event notification policies” topic in the *NSP NFM-P User Guide* for information about how to configure mediation policies. Click on the Select button if you need to specify mediation security policies specific to the discovery rule. The Configure Mediation Security form opens. You can:
   - Select an existing mediation security policy and click on the OK button.
   - Select an existing mediation security policy and click on the Properties button. The MediationPolicy (Edit) form opens.
   - Configure the parameters and click on the OK button to save the changes.
   - Do not specify a policy to apply the default policy.
10. Click on the Next button. The Configure Management Ping Policy form opens.
11. Specify the management ping policies for each of the following management IP addresses, if required:
    - the management IP address on the management port, called an out-of-band management interface
    - the system IP address, called an in-band management interface
    - the IP address of the standby Control card, also called a CPM

    Note:

    Management ping policies are created using the PollerManager configuration form. These are the policies applied during discovery rule creation. You must apply a ping policy, even for interfaces that do not exist.
12. Click on the Select button for each ping policy ID parameter. The Configure Management Ping Policy form opens.
13. Choose a ping policy. If there is no interface, choose a ping policy that has the Schedule Enabled parameter set to disabled.
14. Click on the OK button. The ping policy ID appears in the Policy ID parameter.

    The NFM-P generates alarms if the ping fails.
15. Click on the Next button. The Configure Stats Polling Policy form opens with the default statistics polling policy displayed.
16. Click on the Select button to choose another statistics polling policy, if required. The Configure Stats Polling Policy - Topology Discovery Rule form opens. Select a statistics polling policy in the list and click on the OK button.
17. Click on the Finish button. The Create Discovery Rule - Configure Management Ping Policy form closes and a dialog box opens.
18. Click on the OK button to close the dialog box. The Discovery Manager form reappears.

3

Save the discovery rule and discover devices by scanning the network as specified by the discovery rule.

1. Click on the Discovery Rules tab on the Discovery Manager form.
2. Click on the Apply button.

   New and modified discovery rules are saved. The NFM-P discovers devices by scanning

the network as specified by the discovery rules. After a device is discovered, the NFM-P sets the device in a managed state and reconciles the device elements into its database.

Discovery rules that are disabled or shut down are not applied.

4

Verify that the device is discovered and is managed by the NFM-P by clicking on the Managed State tab on the Discovery Manager form. A list of managed devices opens.

The management state of the device is displayed in the Site State column. Managed is the default state. If the device is unmanaged, choose the device and click on the Manage button.

5

From the Managed State tab, you can also perform management IP address pings to ensure connectivity to all of the managed devices. Do not ping devices without an interface.

1. Click on one of the managed devices in the list.
2. Click on the appropriate ping button.
3. Review the ping information to verify connectivity.

6

Click on the Resync Status tab to verify that the device configuration has been reconciled with the NFM-P database.

The status is displayed in the Resync Status column.

To initiate manual reconciliation of a device, choose a device or devices and click on the Resync button.

Devices that are successfully reconciled appear in the NFM-P navigation tree and the Equipment Manager form.

7

Close the Discovery Manager form.

END OF STEPS

5.4 To configure OSPF and ISIS on a CPAA

5.4.1 Steps

1

Configure OSPF; see the “OSPF configuration workflow and procedures” section in the *NSP NFM-P User Guide*.

Note: The Traffic Engineering parameter must be set to OSPF/ISIS to receive traffic engineering data.

2

Configure ISIS; see the “IS-IS configuration workflow and procedures” section in the *NSP NFM-P User Guide*.

END OF STEPS

5.5 To configure an IGP administrative domain

5.5.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Perform one of the following:

a. Click on the Create button and choose Create IGP Admin Domain from the contextual menu. The IGP Administrative Domain (Create) form opens with the General tab displayed.

b. Specify a filter for the search, if required, and click on the Search button. A list of IGP administrative domains appears. Choose an entry and click on the Properties button. The IGP Administrative Domain (Edit) form opens with the General tab displayed.

3

WARNING

Equipment Damage

The IGP administrative domain should generally be public IP address spaces, and not private IP address spaces. If two IGP administrative domains have duplicate router IDs, for example, some operations—such as the IP Path Monitor and Managed Routes—may not function correctly.

Configure the parameters:

- IGP Admin Domain Name
- IGP Admin Domain Number
- Description

Note: To prevent upgrade problems, verify that the IGP Admin Domain Number parameter is correctly configured.
The IGP Admin Domain Name and IGP Admin Domain Number parameters are not configurable if you configure for an existing IGP administrative domain.

4

Configure the Enabled Menus parameter.

5

Click on the Reference tab to view the OSPF and ISIS reference times.

6

Click on the CPAAs tab to view the associated CPAAs.

7

Click on the BGP AS tab to view the associated BGP AS.

8

Click on the Static Routes tab to view static routes in the administrative domain.

1. Click on the All tab to view all static routes in a non-routed edge discovery policy within the administrative domain.
2. Click on the Active Primary tab to view primary static routes that are operationally up.
3. Click on the Inactive Primary tab to view primary static routes that are operationally down.
4. Click on the Active Secondary tab to view secondary static routes that are operationally up.
5. Click on the Inactive Secondary tab to view secondary static routes that are operationally down.

   Note:

   Primary static routes are static routes in the administrative domain which have the lowest metric among source nodes, destination addresses, or destination address prefix lengths. Secondary static routes are all other static routes in the administrative domain.

9

To create or manage OSPF checkpoints, see the *NSP NFM-P Control Plane Assurance Manager User Guide*.

10

To create or manage ISIS checkpoints, see the *NSP NFM-P Control Plane Assurance Manager User Guide*.

11

Click on the OK button to save the configuration and close the form.

END OF STEPS

5.6 To configure route listening and analysis on a CPAA

5.6.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose CPAA (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered CPAAs appears

3

Configure each CPAA by performing the following:

1. Double-click on an entry in the list of discovered CPAAs. The CPAA (Edit) form opens with the General tab displayed.
2. Set the Administrative State parameter to Down.

   Note:

   Nokia recommends that you apply a reference to the CPAA before you change the configuration. See the *NSP NFM-P Control Plane Assurance Manager User Guide* for more information.
3. Click on the Administrative Domains tab.

   Note:

   See 5.7 “To deploy a CPAA to monitor a BGP AS” (p. 47) for information about how to configure a CPAA to monitor a BGP administrative domain.
4. Configure the Role parameter. You must enable the IGP option.
5. Click on the Select button next to the IGP Admin Domain Number to associate the CPAA with an IGP administrative domain.

   The Select IGP Administrative Domain - CPAA form opens with a list of configured IGP administrative domains.

   Note:

   For CPAAs with ISIS enabled, you cannot add a CPAA to an IGP administrative domain if the area ID of one the ISIS instances of the CPAA is associated to another CPAA in the IGP administrative domain.
6. Choose an entry and click on the OK button. The Select IGP Administrative Domain - CPAA form closes and the CPAA (Edit) form refreshes with the IGP administrative domain information.
7. Click on the Apply button.
8. Click on the General tab.
9. Configure the Protocol Events parameter by selecting one or both of the following options:
   - OSPF / OSPF-TE
   - ISIS / ISIS-TE

The CPAM retrieves the LSDB and receives change notifications for the selected protocols only.

Note:

For monitored LSPs, monitored IP paths, ABM/SAC-managed routes, and other highlights, the appropriate protocols must be enabled to ensure that the topology map view is up-to-date.

10. Configure the Keep Event History parameter by selecting one or more of the following options:
    - OSPF
    - OSPF-TE
    - ISIS-TE

    Note:

    Alternatively, you can view and configure the route listening and analysis parameters from the CPAA tab of the CPAA Network Element (Edit) form. Right-click on a CPAA in the NFM-P equipment view of the navigation tree and choose Properties from the contextual menu. Click on the CPAA Properties button.
11. Set the Administrative State parameter to Up.
12. Click on the Apply button. The area topology is sent to the CPAM from the CPAA.
13. Click on the Retrieve From CPAA button, then either OSPF LSDB or ISIS LSDB if a forced topology resynchronization is required. If the Retrieve From CPAA button is not visible, click on the More Actions button and choose Retrieve From CPAA.
14. Click on the Close button to close the CPAA (Edit) form.

4

Close the Admin Domains / CPAAs form.

END OF STEPS

5.7 To deploy a CPAA to monitor a BGP AS

5.7.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose CPAA (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered CPAAs appears.

3

Configure each CPAA by performing the following:

1. Double-click on an entry in the list of discovered CPAAs. The CPAA (Edit) form opens with the General tab displayed.
2. Set the Administrative State parameter to Down.

   Note:

   Nokia recommends that you apply a reference to the CPAA before you make any configuration changes. See the *NSP NFM-P Control Plane Assurance Manager User Guide* for more information.

   Alternatively, you can view and configure the route listening and analysis parameters from the CPAA tab of the CPAA Network Element (Edit) form. Right-click on a CPAA in the NFM-P equipment view of the navigation tree and choose Properties from the contextual menu. Click on the CPAA Properties button.

   See 5.6 “To configure route listening and analysis on a CPAA” (p. 46) for information about how to configure a CPAA to monitor an IGP administrative domain.

4

Click on the Administrative Domains tab.

5

Configure the Role parameter. You must enable the BGP option.

Note: To remove a role from a CPAA that is assigned to an administrative domain, set the Administrative State parameter to Down, remove the role, and click on the Apply button. The CPAM automatically removes the selected administrative domain.

6

Click on the Select button next to the Type parameter to associate the CPAA with a BGP AS.

The Select BGP AS/Sub-AS - CPAA form opens with a list of configured BGP AS.

7

Click on the General tab.

8

Set the Administrative State parameter to Up.

9

Click on the Apply button. The area topology is sent to the CPAM from the CPAA.

10

Close the Admin Domains / CPAAs form.

END OF STEPS

5.8 To configure CPAM-CPAA event registration

5.8.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose CPAA (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered CPAAs appears.

3

Choose a CPAA and click on the Search button. The CPAA (Edit) form opens with the General tab displayed.

4

Configure the CPAM-CPAA event registration parameters:

- Event Types
- Keep Event History

5

Click on the OK button. A dialog box appears.

6

Click on the Yes button. The CPAA (Edit) form closes.

7

Close the Admin Domains / CPAAs form.

END OF STEPS

5.9 To view CPAA update times information

5.9.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose CPAA (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered CPAAs appears.

3

Choose an entry and click on the Properties button. The CPAA (Edit) form opens.

4

Click on the Update Times tab to view the following information:

- OSPF LSDB update time
- ISIS LSDB update time
- BGP AS path data update time
- BGP RIB information update time
- BGP VPN IPv4 RT update time

5

Close the CPAA (Edit) form.

6

Close the Admin Domains / CPAAs form.

END OF STEPS

5.10 To delete an IGP administrative domain

WARNING

Equipment Damage

When you delete an IGP administrative domain, the objects that are contained within the IGP administrative domain—such as routers, links, LSAs, and LSPs—are also deleted.

5.10.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

From the Filter drop-down menu, expand the Administrative Domain (CPAM:Topology) object and choose IGP Administrative Domain (CPAM:Topology).

3

Click on the Search button. A list of IGP administrative domains appears.

4

Choose one or more entries and click on the Delete button. A dialog box appears.

5

Click on the Yes button. The dialog box closes and the IGP administrative domains are deleted from the CPAM.

END OF STEPS

6 CPAA Redundancy

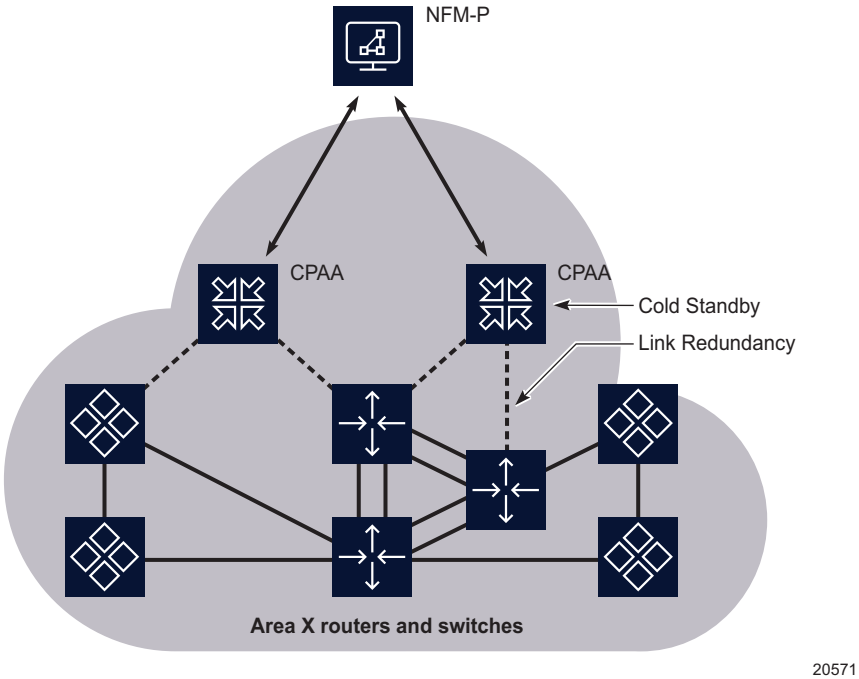
6.1 CPAA Redundancy overview

6.1.1 Introduction

You can use the NFM-P to create a cold standby CPAA for ISIS and OSPF protocols. In a redundant configuration, each CPAA must have exactly the same peering configuration within the network. For example, when the CPAA 10.1.1.7/32 peers in 0.0.0.0, 0.0.1.0 and 0.0.2.0 OSPF areas, the CPAA 10.1.7.6/32 needs the same peering arrangements to be a standby for CPAA 10.1.1.7/32.

The following figure shows CPAA redundancy:

Figure 6-1 CPAA redundancy



6.1.2 CPAA switchover

The NFM-P supports a manual switchover, initiated by the user. The OSS developers can use the XML API interface to create XML scripts to automate this manual switchover. The CPAAs are pre-configured in a redundancy pair (the pair must have visibility of the same OSPF areas, ISIS routing domains and BGP AS). The alarm configuration, BGP prefix monitor, IGP shortcuts and IP paths

are automatically distributed to the newly active CPAA. Note that the BGP routing change statistics must be configured on both CPAAs.

For redundant CPAAs, the deployment rules described in 6.2 “CPAA redundancy workflow” (p. 53) must be followed to correctly back up one another. Because the NFM-P does not support two active CPAAs in the same IGP administrative domain, the standby CPAA must be administratively down and IGP administrative domains must not be configured.

6.2 CPAA redundancy workflow

6.2.1 Purpose

This workflow outlines the high-level steps necessary to configure CPAA redundancy. It assumes that the active and standby CPAAs have been configured for active peering with the same IGP areas (OSPF) or levels (ISIS), and that the standby CPAA does not have a configured IGP administrative domain (duplicate IGP administrative domains that are configured on the active and standby CPAAs are not supported and can corrupt the IGP topology). The active CPAA is configured to be administratively up and the standby CPAA is configured to be administratively down.

6.2.2 Stages

1

Assign the standby CPAA to the active CPAA. See 6.3 “To assign a standby CPAA to an active CPAA” (p. 54) for more information.

Note: Set checkpoints for all of the IGP areas or levels that are managed by the active CPAA. Otherwise, you may lose the layout of network links and NEs on the map.

2

As required, switchover to a standby CPAA from an active CPAA. See 6.4 “To switchover to a standby CPAA from an active CPAA” (p. 55) for more information.

Note: Auditing of the active and standby CPAA configurations can be automated using the XML script capability of the NFM-P or the XML API OSS interface. The provision of the scripts or XML interface tools is an Nokia contracted design service.

6.3 To assign a standby CPAA to an active CPAA

Note: You can only assign one standby CPAA. The standby CPAA must not be assigned to any IGP administrative domains or BGP AS.

6.3.1 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose CPAA (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered CPAAs appears.

3

Choose an entry and click on the Properties button. The CPAA (Edit) form opens.

4

Click on the Select button in the Standby CPAA panel. The Select Standby CPAA form appears.

5

Click on the Search button. A list of CPAAs appears.

6

Choose a CPAA and click on the OK button. The Select Standby CPAA form closes. The Standby CPAA panel refreshes with the CPAA information.

7

Click on the OK button. The CPAA (Edit) form closes.

END OF STEPS

6.4 To switchover to a standby CPAA from an active CPAA

6.4.1 Important information

The CPAM performs the following during a switchover:

- verifies whether the protocol configuration is compatible (OSPF areas and ISIS levels and instances, BGP AS). If the protocols are administratively up on active, the protocols must be operationally up on the standby CPAA. The CPAM does not verify interface configuration, connectivity, or reachability.
- administratively brings down the active CPAA and removes the IGP administrative domain and BGP AS from the CPAA.
- adds the standby CPAA to the same IGP administrative domain and BGP AS.
- ensures that the standby CPAA has the same event registration and keep event history configuration as the previously active CPAA.
- ensures that the appropriate alarms are propagated to the new CPAA.
- initiates the switchover of all of the relevant IP path monitors and ABM managed routes to use the standby CPAA, where applicable.
- administratively enables the standby CPAA, which initiates the following:
  - The standby CPAA becomes the active CPAA. The previously active CPAA becomes the standby CPAA.
  - distributes the alarm configuration to the CPAA.

- distributes the BGP monitored prefixes to the CPAA.
- distributes the IGP shortcuts to the CPAA.

Note: Before a CPAA switchover, the CPAM verifies whether the same ISIS instances with similar ISIS level capabilities are configured on both the active and standby CPAA. The CPAM does not verify the ISIS interfaces or adjacencies for each instance, but does verify whether the same area IDs are configured on the similar instances of the active and inactive CPAAs.

You must ensure that the standby CPAA has the same ISIS configuration as the active CPAAs. Similar instances on both CPAAs have adjacencies to the same L1 domain with the same area ID.

6.4.2 Steps

1

Choose Tools→Route Analysis→Admin Domains / CPAAs from the NFM-P main menu. The Admin Domains / CPAAs form opens.

2

Choose CPAA (CPAM: Topology) from the object drop-down menu and click on the Search button. A list of discovered CPAAs appears.

3

Choose the activeCPAA and click on the Properties button. The CPAA (Edit) form opens.

4

Click on the Switchover button. If the Switchover button is not visible, click on the More Actions button and choose Switchover. A dialog box appears.

5

Click on the Yes button to confirm the switchover.

6

Click on the OK button. The CPAA (Edit) form closes.

END OF STEPS