



Junos[®] Space

Junos Space OAM Insight

Release
14.3



Modified: 2015-06-07

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2015, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos[®] Space Junos Space OAM Insight
Release 14.3
Copyright © 2015, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Documentation Conventions	xii
	Documentation Feedback	xiv
	Requesting Technical Support	xiv
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xv
Part 1	Overview	
Chapter 1	OAM Insight Overview	3
	Junos Space OAM Insight Overview	3
	RFC2544 Test Overview	5
Part 2	Configuration	
Chapter 2	Prestaging OAM Devices	9
	Understanding the Prestage Devices Workspace	9
	Viewing List of Available Interface per Device	9
	Viewing How Many Services Are in Each Device	10
	Tasks in the Prestage Devices Workspace	11
	Managing OAM Devices	12
	Prestaging OAM Devices	12
	Viewing Device Details	13
	Attaching an Action Profile	15
	Detaching an Action Profile	15
	Attaching an SLA-Iterator Profile	16
	Detaching an SLA-Iterator Profile	17
	Attaching an LFM Configuration	18
	Configuring an LFM Link	19
	Managing LFM Configuration	20
	Viewing Device Configuration Change Log	20

Chapter 3	OAM Service Design	21
	Understanding the OAM Design Workspace	21
	Viewing Services Created from a Service Definition	21
	Viewing How Many Service Definitions Are in Each Service Definition State	22
	Tasks in the OAM Design Workspace	23
	Creating and Viewing CFM Action Profiles	24
	Creating a CFM Action Profile	24
	Viewing a CFM Action Profile	26
	Creating and Viewing LFM Action Profiles	27
	Creating an LFM Action Profile	28
	Viewing an LFM Action Profile	29
	Creating and Viewing SLA-Iterator Profiles	29
	Creating SLA-Iterator Profiles	29
	Viewing SLA Iterator Profile	31
	Creating CFM Profiles	31
	Configuring a CFM Profile-General Tab	32
	Configuring a CFM Profile-MA Settings Tab	33
	Configuring a CFM Profile-MEP Settings Tab	35
	Creating an LFM Profile	36
Chapter 4	OAM Service Provisioning	39
	Understanding the OAM Provisioning Workspace	39
	Creating and Managing CFM Service Orders	41
	Configuring CFM Service Order Information	41
	Configuring CFM Service Order Common Settings	42
	Configuring Endpoint Settings	44
	Deploying a CFM Service Order	45
	Validating a CFM Service Order	46
	Creating an RFC2544 Test Profile	47
Chapter 5	Configuration Example	67
	Configuring CFM on Physical Interfaces	67
Part 3	Administration	
Chapter 6	Managing OAM Service Definitions	77
	Managing CFM Profiles	77
	Publishing a CFM Service Definition	78
	Unpublishing a CFM Service Definition	79
	Deleting a CFM Service Definition	79
Chapter 7	Managing OAM Service Orders	81
	Managing CFM Service Orders	81
	Deleting a CFM Partial Configuration	82
	Viewing the Configuration of a Pending Service Order	83
	Deleting a CFM Service Order	84

Chapter 8	Managing Action Profiles	85
	Managing CFM Action Profiles	85
	Publishing an Action Profile	86
	Unpublishing an Action Profile	87
	Deleting an Action Profile	87
Chapter 9	Managing SLA Iterator Profiles	89
	Managing SLA-Iterator	89
	Publishing an SLA-Iterator Profile	90
	Unpublishing an SLA-Iterator Profile	90
	Deleting an SLA-Iterator Profile	91
Chapter 10	Managing OAM Services	93
	Managing CFM Services	93
	Viewing Provisioned CFM Services	94
	Decommissioning a CFM Service	95
	Modifying a CFM Service	95
	Viewing Service Alarms in OAM Insight	96
Part 4	Troubleshooting	
Chapter 11	Configuration Audit	101
	Performing a Configuration Audit	101
	Viewing Configuration Audit Results	103
Chapter 12	Functional Audit	105
	Performing a Functional Audit	106
	Viewing Functional Audit Results	107

List of Figures

Part 2	Configuration	
Chapter 5	Configuration Example	67
	Figure 1: Ethernet CFM on Physical Interfaces	69

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xii
	Table 2: Text and Syntax Conventions	xiii
Part 4	Troubleshooting	
Chapter 12	Functional Audit	105
	Table 3: Functional Audit Success Status Icons	108
	Table 4: Control Plane and Data Plane Validation Icons	109
	Table 5: Command Status Icons	110

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Documentation Conventions on page xii
- Documentation Feedback on page xiv
- Requesting Technical Support on page xiv

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:







- JA1500
- ACX1000 and ACX1100
- ACX2000 and ACX2100
- ACX4000
- M7i
- M10i
- M320
- MX80
- MX104
- MX240

- [MX480](#)
- [MX960](#)
- [SRX100](#)
- [SRX110](#)
- [SRX210](#)
- [SRX220](#)
- [SRX240](#)
- [SRX650](#)
- [SRX550](#)

Documentation Conventions

[Table 1 on page xii](#) defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

[Table 2 on page xiii](#) defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview

- [OAM Insight Overview on page 3](#)

CHAPTER 1

OAM Insight Overview

- [Junos Space OAM Insight Overview on page 3](#)
- [RFC2544 Test Overview on page 5](#)

Junos Space OAM Insight Overview

The Junos Space OAM Insight application provides capabilities for automated end-to-end network management, monitoring, and troubleshooting. OAM Insight provides a set of functions designed to monitor network operation to detect network faults and measure network performance.

The OAM Insight application allows network operators to configure OAM (Operations, Administration and Maintenance) functionality on all devices and to monitor, detect, isolate and troubleshoot networking faults in a quick and efficient manner. Operators can also measure quality-of-service (QoS) attributes, such as availability, frame delay, frame delay variation, and frame loss. Monitoring and fault isolation can be performed at the Link Layer, Transport Layer, and Session Layer, thus providing a clear demarcation view to the operator, service provider, and customer.

The OAM Insight application is compliant with ITU-T and IEEE standards that support cross-platform link fault management, connectivity fault management (CFM), and performance management on all Juniper Networks devices using the OAM Insight application in Junos Space.

The following standards are supported:

- 802.3ah, *Link Fault Management* which defines OAM link-fault management mechanisms
- 802.1ag, *Connectivity Fault Management*
- Y1731, *Draft, Performance Management*

The OAM Insight application supports service-based CFM provision, LFM provision, and performance measurements of Y.1731 standard frames on the network services. The OAM Insight application also supports the following functions:

- CFM configuration of the following features:

- CFM Action Profile—You can configure a CFM action profile and specify the action to be taken when any of the configured events occur. Alternately, you can configure an action profile and specify default actions when connectivity to a remote maintenance end point (MEP) fails.
- Service Level Agreement (SLA)-Iterator Profile—The OAM application uses the SLA-iterator profile to collect Y.1731 statistics. These iterator profiles have to be configured before starting performance monitoring.
- Remote MEP—You can configure a remote MEP to wait for continuity check messages (CCMs). If autodiscovery is not enabled, the remote MEP must be configured under a MEP. If the remote MEP is not configured under a MEP, the CCMs from the remote MEP are treated as errors.
- CFM Modify Service—You can add or delete new endpoints, as well as modify attributes for remote MEP configuration for MEP.
- LFM configuration
 - LFM Profile—You can define an LFM profile and specify the action to be taken when any of the configured events occur.
 - LFM Action Profile—You can configure an LFM action profile and define event fault flags and thresholds and the action to be taken when any of the configured events occur.

- CFM Integration with Network Activate Services

The CFM is enabled for Point-to-Point (PPP) (E-Line) and virtual private LAN service (VPLS) (E-LAN) services through the Network Activate application. The Network Activate application now detects the availability of CFM service profiles automatically. On availability, the Network Activate application imports the CFM service profiles (CFM service definitions) from the OAM Insight application and attaches them to a Network Activate service order.

- OAM Insight Performance Management

In Performance Management, the OAM Insight application provides an option to measure the frame delay, frame loss, frame delay variation, and service availability. These measurements are achieved in either of the following ways:

- Triggering a one-way delay
- Triggering a two-way delay

Users can also get this information through the Loss Measurement/Delay Measurement (LM/DM) iterator.

The performance measurement is useful for generating periodic service level agreement conformance reports from the deployed network and for studying traffic patterns in the network over a period of time. The iterator profiles are configured on remote MEP for measurement of frame delay (ETH-DM), frame loss (ETH-LM) and statistical frame loss (SFL).

- Related Documentation**
- [Creating CFM Profiles on page 31](#)
 - [Creating an LFM Profile on page 36](#)
 - [Creating and Managing CFM Service Orders on page 41](#)
 - [Creating and Viewing CFM Action Profiles on page 24](#)
 - [Creating and Viewing SLA-Iterator Profiles on page 29](#)
 - [Performance Management Overview](#)
 - [Creating and Viewing LFM Action Profiles on page 27](#)
 - [Managing LFM Configuration on page 20](#)

RFC2544 Test Overview

The testing methodology defined by the RFC2544 standard is intended to assess different parameters included in service-level agreements. By testing service integrity, a service provider can certify that the working parameters of a delivered Ethernet circuit comply with expectations.

The OAM Insight application enables you to create RFC2544 tests to measure the performance of interconnected network devices. You create an RFC2544 test to measure throughput, latency, frame loss, and burstability:

- Throughput tests determine the maximum rate at which no offered frames are dropped by the device under test (DUT) or system under test (SUD). This measurement translates the obtained rate into the available bandwidth of the service.
- Latency tests (for store-and-forward devices) measure the time interval that begins when the last bit of the input frame reaches the input port and ends when the first bit of the output frame is seen on the output port. Latency is the time it takes a bit to go through the network and back. Latency variability can be a problem. With protocols like VoIP, a variable or long latency can cause degradation in voice quality.
- Frame loss tests calculate the percentage of frames that should have been forwarded by a network device under steady state (constant) loads that were not forwarded due to lack of resources. You can use this measurement to report the performance of a network device in an overloaded state. This measurement can indicate how a device would perform under extreme network conditions such as broadcast storms.
- Burst tests calculate the number of frames in the longest burst that the device or network being tested will process without losing any frames.

- Related Documentation**
- [Creating an RFC2544 Test Profile on page 47](#)

PART 2

Configuration

- [Prestaging OAM Devices on page 9](#)
- [OAM Service Design on page 21](#)
- [OAM Service Provisioning on page 39](#)
- [Configuration Example on page 67](#)

CHAPTER 2

Prestaging OAM Devices

- [Understanding the Prestage Devices Workspace on page 9](#)
- [Managing OAM Devices on page 12](#)
- [Prestaging OAM Devices on page 12](#)
- [Viewing Device Details on page 13](#)
- [Attaching an Action Profile on page 15](#)
- [Detaching an Action Profile on page 15](#)
- [Attaching an SLA-Iterator Profile on page 16](#)
- [Detaching an SLA-Iterator Profile on page 17](#)
- [Attaching an LFM Configuration on page 18](#)
- [Configuring an LFM Link on page 19](#)
- [Managing LFM Configuration on page 20](#)
- [Viewing Device Configuration Change Log on page 20](#)

Understanding the Prestage Devices Workspace

The following topics describe viewing statistics and tasks in the Prestage Devices workspace:

- [Viewing List of Available Interface per Device on page 9](#)
- [Viewing How Many Services Are in Each Device on page 10](#)
- [Tasks in the Prestage Devices Workspace on page 11](#)

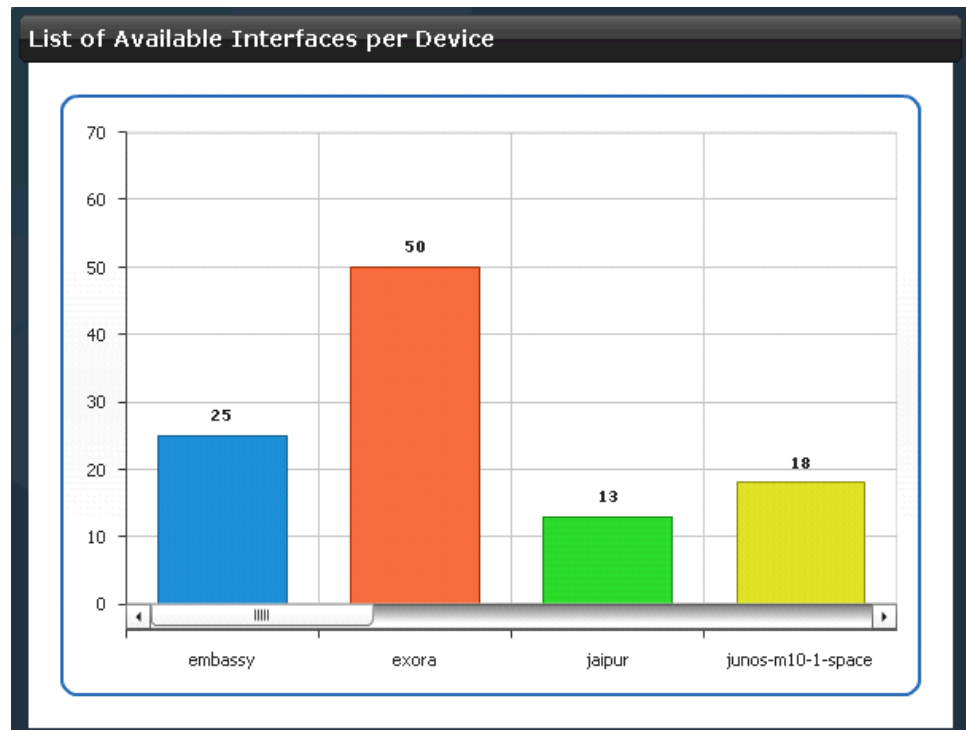
Viewing List of Available Interface per Device

You can view the number of interfaces per device.

To view the number of interfaces for each device:

1. In the OAM Insight task pane, select **Prestage Devices**.

The Junos Space software displays the **List of Available Interfaces per Device** chart.



Each vertical bar represents a device. The number of interfaces is shown on the Y axis. Drag the slider across the bottom of the graph to display all interfaces.

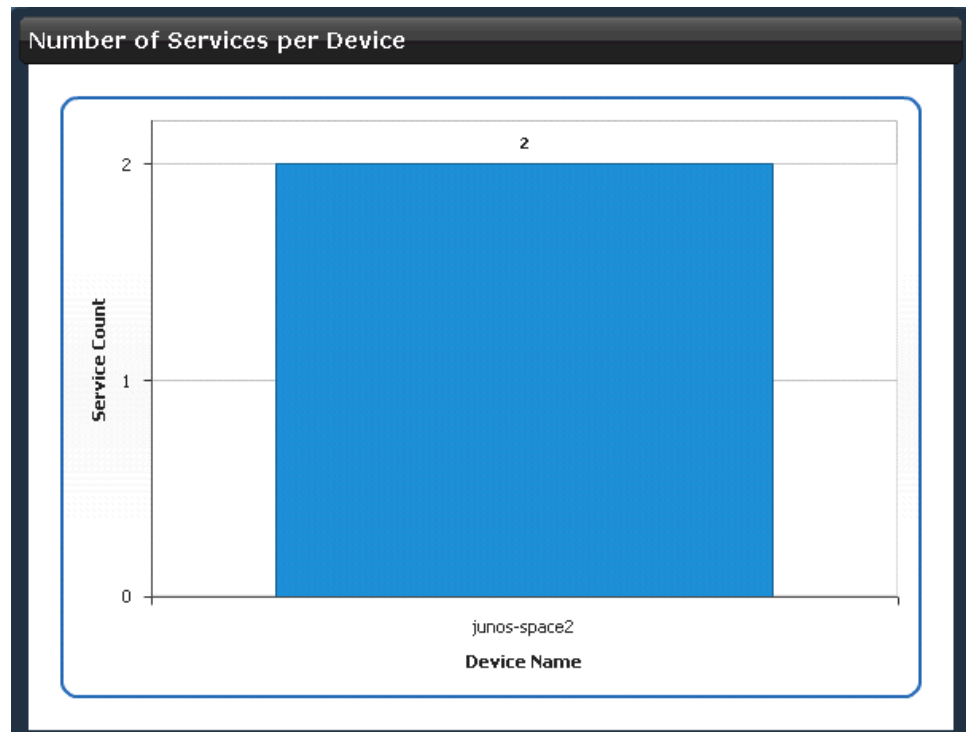
2. To see the interfaces for a device, click the bar that represents the service definition.
The **Manage Services** page shows only the interfaces for that device.

Viewing How Many Services Are in Each Device

To view the number of services that are in each device:

1. In the task pane, select **Prestage Devices**.

The Junos Space software displays the **Number of Services per Device** chart.



Each bar in the chart represents the number of services in a device. In this example, there are two services in the device junos-space2.

To view the number of services in a device, move the mouse pointer over the bar.

2. To see which services are in a device, click a bar in the bar chart.

The **Manage OAM Service Orders** window shows only those services from the selected device segment.

Tasks in the Prestage Devices Workspace

The Prestage Devices workspace includes the following task:

- Manage OAM Devices—The **Manage OAM Devices** page lists the OAM devices. For more information on this page, see [“Managing OAM Devices” on page 12](#)
- Discover Devices—This operation fetches the new devices from the Network Platform Application into the OAM Insight application. For more information on this topic, see [“Prestaging OAM Devices” on page 12](#)

Related Documentation

- [Understanding the OAM Design Workspace on page 21](#)
- [Understanding the OAM Provisioning Workspace on page 39](#)

Managing OAM Devices

The Manage OAM Devices inventory page displays the list of OAM devices.

Viewing OAM Devices—The Manage OAM Devices inventory page provides two views: tabular and tag. Click the view icons at the right of the page name to toggle between the views.

View	Field Description
Tabular	The tabular view displays OAM device information in a table by device name, management address, loopback address.
Tag	The tag view display the OAM device information based on the tags. you can select the tags from the Tags pane.

You can use the search text box to filter the OAM devices by name or by tag names that you create. When you start to type a name in the search box, it automatically completes the name.

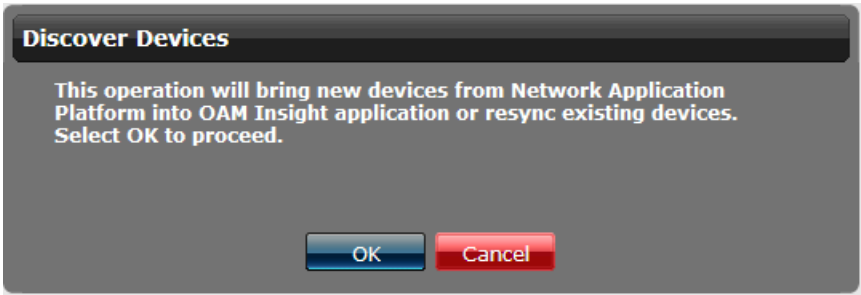
The Manage OAM Devices inventory page includes the following actions:

- **Device Details**—See [“Viewing Device Details” on page 13](#).
- **Attach Action Profile**—See [“Attaching an Action Profile” on page 15](#).
- **Detach Action Profile**—See [“Detaching an Action Profile” on page 15](#).
- **Attach SLA Iterator**—See [“Attaching an SLA-Iterator Profile” on page 16](#).
- **Detach SLA Iterator**—See [“Detaching an SLA-Iterator Profile” on page 17](#).
- **Tag It**—See *Tagging an Object*
- **View Tags**—See *Managing Tags*
- **Untag It**—See *Untagging Objects*

Prestaging OAM Devices

The OAM Insight application aids in discovering the available OAM (Operation, Administration, and Maintenance) domain by discovering the maintenance domains, list of maintenance associations, maintenance end points (MEP), and maintenance intermediate point (MIP) participating in the domain. Before you can prestage OAM devices, you must first run device discovery.

Select **OAM Insight > Prestage Devices > Manage OAM Devices > Discovery Devices**.



To discover devices:

1. To run device discovery, click OK; otherwise, click Cancel.

Field	Action
OK	To discover the OAM devices, click OK . The Job ID dialog box appears The Job Management inventory page appears with the OAM device discovery job displayed. In the State column, you view whether the job was successful. If the OAM discovery job is a failure, you can view a brief summary of the issue.
Cancel	To cancel the discovery of devices in the OAM Insight, click Cancel .

2. Select **Jobs > Job Management** to view the discovered OAM devices on the inventory page.



NOTE: The CFM action profiles and SLA-iterator profiles are also discovered during the OAM discovery.

Related Documentation

- [Junos Space OAM Insight Overview on page 3](#)
- [Creating CFM Profiles on page 31](#)
- [Creating and Managing CFM Service Orders on page 41](#)

Viewing Device Details

You can view the details of each device listed in the Manage OAM Devices page. Select **OAM Insight > Prestage Devices > Manage OAM Devices**.

To view the details of a device:

1. Select a device from the list.
2. Right-click the selected device and select **Device Details**. The Device Details window is displayed.

Device Details

Name: junos-space1
OS version: 12.2R1.3
Platform: ACX2000
Loopback address: 10.216.114.121
Connection status: up

Interfaces | Action Profile | SLA Iterator Profile

Name
ae0
ae1
ae2
ae3
ae4
ae5
ae6
ae7
ae8
ae9

OK

Field	Field Description
Name	Name of the OAM device.
OS version	Junos operating system version.
Platform	Platform type of the OAM device.
Loopback address	IP address of the OAM device.
Connection status	Connection status of the OAM device: <ul style="list-style-type: none"> • up • down
Interfaces	This tab list the interfaces of the selected OAM device.
Action Profile	This tab lists the action profiles attached to the selected OAM device and the profile type.
SLA Iterator Profile	This tab list the SLA iterator profiles attached to the selected OAM device.

- Related Documentation**
- [Attaching an Action Profile on page 15](#)
 - [Attaching an SLA-Iterator Profile on page 16](#)

Attaching an Action Profile

This action attaches an action profile to one or more devices at a time.

To attach an action profile:

1. Select **OAM Insight > Prestage Devices > Manage OAM Devices**.
2. Right-click a device and select **Attach Action Profile**
Or after you select a device, open the **Actions** menu and select **Attach Action Profile**.
The **Attach Action Profile** window appears.
3. Select **CFM** or **LFM** from the **Profile type** list.
4. Select an action profile from the **Profile name** list.



NOTE: In the **Selected Device**, you cannot select the check box of a device, if an action profile is already attached to a device. The application does not attach the action profile to those devices again.

5. Click **Attach**.

The service corresponding to this action profile is modified to attach new devices (end points).

- Related Documentation**
- [Detaching an Action Profile on page 15](#)
 - [Attaching an SLA-Iterator Profile on page 16](#)
 - [Detaching an SLA-Iterator Profile on page 17](#)
 - [Creating and Viewing CFM Action Profiles on page 24](#)

Detaching an Action Profile

This action removes an action profile from the selected device.

To detach an action profile:

1. Select **OAM > Prestage Devices > Manage OAM Devices**.
2. Right-click a device and select **Detach Action Profile**
Or after you select a device, open the **Actions** menu and click **Detach Action Profile**.
The **Detach Action Profile** window appears.
3. Select **CFM** or **LFM** from the **Profile type** list

4. Select the action profile from the **Profile name** list.



NOTE: If the selected device does not have an action profile associated with it, the application takes no action on that node.

5. Click **Detach**.

The corresponding service definition is modified to remove the service elements of selected devices.

**Related
Documentation**

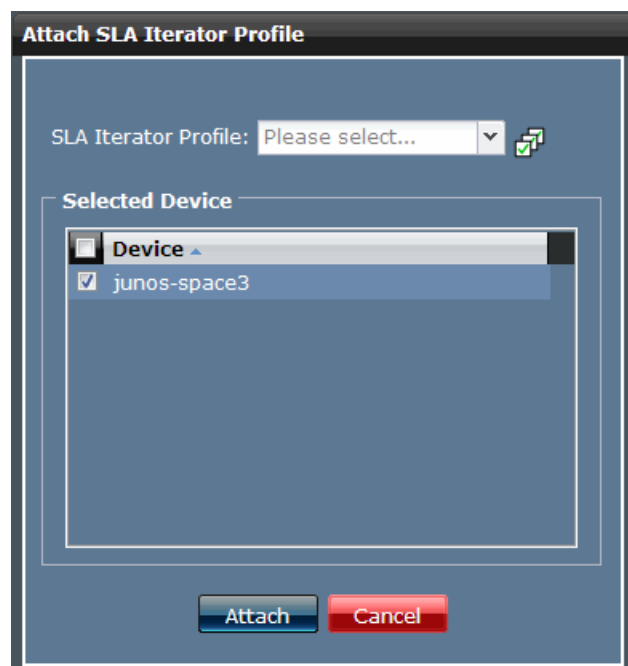
- [Attaching an Action Profile on page 15](#)
- [Attaching an SLA-Iterator Profile on page 16](#)
- [Detaching an SLA-Iterator Profile on page 17](#)
- [Creating and Viewing CFM Action Profiles on page 24](#)

Attaching an SLA-Iterator Profile

This action attaches an SLA-iterator profile on one or more devices at a time. Select **OAM Insight > Prestage Devices > Manage OAM Devices**.

To attach an SLA-iterator profile:

1. Select a device from the **Manage OAM Devices** page.
2. Open the **Actions** menu and click **Attach SLA Iterator**. The **Attach SLA Iterator Profile** window appears.



3. Select the SLA-iterator profile from the list.



NOTE: In the **Selected Device** you cannot select the check box of a device, if an SLA-iterator profile is already attached to a device. The application does not attach the SLA-iterator profile to those devices again.

4. Click **Attach**.

The service corresponding to this SLA-iterator profile is modified to attach new devices (end points).

**Related
Documentation**

- [Attaching an Action Profile on page 15](#)
- [Detaching an Action Profile on page 15](#)
- [Detaching an SLA-Iterator Profile on page 17](#)
- [Creating and Viewing SLA-Iterator Profiles on page 29](#)

Detaching an SLA-Iterator Profile

This action removes an SLA-Iterator profile from the selected device. Select **OAM Insight > Prestage Devices > Manage OAM Devices** landing page.

To detach an SLA-Iterator profile:

1. Select a device from the landing page.
2. Open the **Actions** menu and click **Detach SLA Iterator**. The **Detach SLA Iterator Profile** window appears.



3. Select the SLA-Iterator profile from the list.



NOTE: If the selected device does not have SLA-Iterator profile associated with it, the application takes no action on that node.

4. Click **Detach**.

The corresponding service definition is modified to remove the service elements from selected devices.

Related Documentation

- [Attaching an Action Profile on page 15](#)
- [Detaching an Action Profile on page 15](#)
- [Attaching an SLA-Iterator Profile on page 16](#)
- [Creating and Viewing SLA-Iterator Profiles on page 29](#)

Attaching an LFM Configuration

To attach an LFM Configuration:

1. Select **Prestage Devices > Manage OAM Devices**.
2. Select two devices, right-click, and select **Configure LFM**.

The **Configure LFM** window appears.

3. Select an interface for the device from the list below the **Interface** column.

4. Select the **LFM Profile** from the list and specify a **Link Name**.
5. Click **Attach**.

Configuring an LFM Link

To configure an LFM Link:

1. Add devices to the OAM Insight application. In the OAM Insight task pane, select **Devices > Device Discovery > Discover targets**.
2. In the OAM Insight task pane, select **Prestage Devices > Manage OAM Devices**.
3. In the **Manage OAM Devices** window, select two devices.
4. Right-click, or open the **Actions** menu, and select **Configure LFM Link**.
5. In the **Configure LFM Link** window, select an interface for each device from the list displayed in the **Interface** column.
6. In the **LFM Profile** field, select an LFM profile.
7. In the **Link Name** field, type a name for the link .
8. Click **Attach**.

After you configure an LFM link successfully, if a problem is detected in any of the interfaces, the device generates one of the following alarms, which indicates the reason for the alarm:

- Undefined
- Config disabled
- Removed from AE
- Reserved ifl deleted
- FSM restarted
- Dying gasp
- Local link fault
- Remote link fault
- Critical event
- Local unsatisfied
- Remote unsatisfied
- Adjacency lost

To view alarms associated with the LFM service:

1. In the Network Application Platform task pane, select **Manage LFM Link**.
2. Right-click the link and select **View Service Alarms**.

- Related Documentation**
- [Managing LFM Configuration on page 20](#)

Managing LFM Configuration

From the LFM configuration page, you can perform tasks, such as removing the LFM configuration from a link, updating the link status, manage tags, and so on.

To manage LFM Configuration:

1. Select **Prestage Devices > Manage LFM Link**.
The **Link Status** and **Fault Status** columns display the current status of the links.
2. Select a device and right-click to perform a task.
3. (Optional) Click **Update Link Status** to know the current status of the link.
4. (Optional) Click **Remove LFM Link** to remove the link.

- Related Documentation**
- [Configuring an LFM Link on page 19](#)
 - **Tag It**—See *Tagging an Object*
 - **View Tags**—See *Managing Tags*
 - **Untag It**—See *Untagging Objects*

Viewing Device Configuration Change Log

To view a device configuration change log:

1. Select **Devices > Manage Devices**.
2. Right-click a device and select **Device Configuration > View Config Change Log**.
3. Click **View Change XML** to view the configuration change.

The **View Configuration Change XML** window appears. If no change is made to device configuration, the following message is displayed:

No difference was found in the device configuration.

CHAPTER 3

OAM Service Design

- [Understanding the OAM Design Workspace on page 21](#)
- [Creating and Viewing CFM Action Profiles on page 24](#)
- [Creating and Viewing LFM Action Profiles on page 27](#)
- [Creating and Viewing SLA-Iterator Profiles on page 29](#)
- [Creating CFM Profiles on page 31](#)
- [Creating an LFM Profile on page 36](#)

Understanding the OAM Design Workspace

The following topics describe viewing statistics and tasks in the OAM Design workspace:

- [Viewing Services Created from a Service Definition on page 21](#)
- [Viewing How Many Service Definitions Are in Each Service Definition State on page 22](#)
- [Tasks in the OAM Design Workspace on page 23](#)

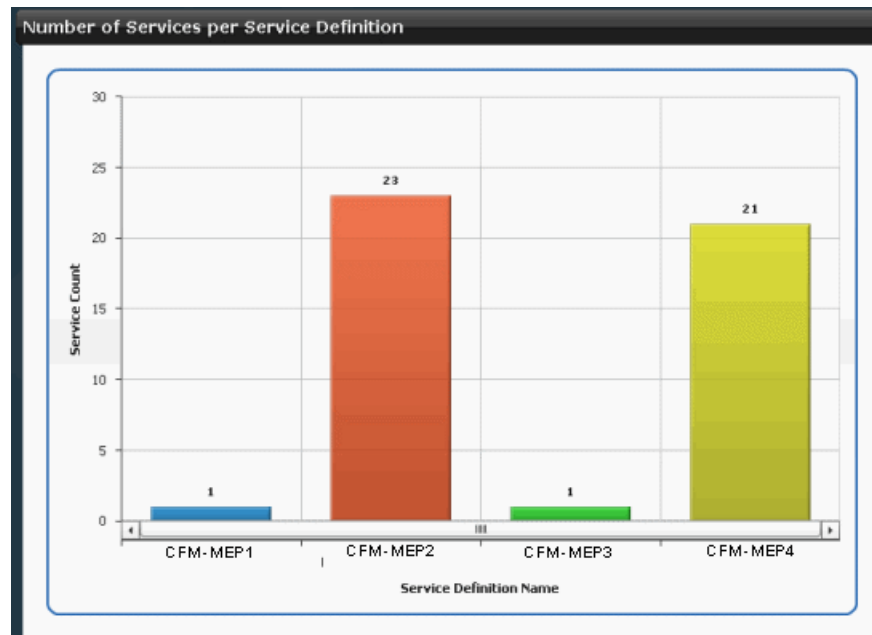
Viewing Services Created from a Service Definition

You can view the services that are associated with a service definition.

To view the number of services made from each service definition:

1. In the OAM Insight task pane, select **OAM Design**.

The Junos Space software displays the **Number of Services per Service Definition** chart.



Each vertical bar represents a service definition. The number of services is shown on the Y axis. Drag the slider across the bottom of the graph to display all service definitions.

- To see which services have been created from a specific service definition, click the bar that represents the service definition.

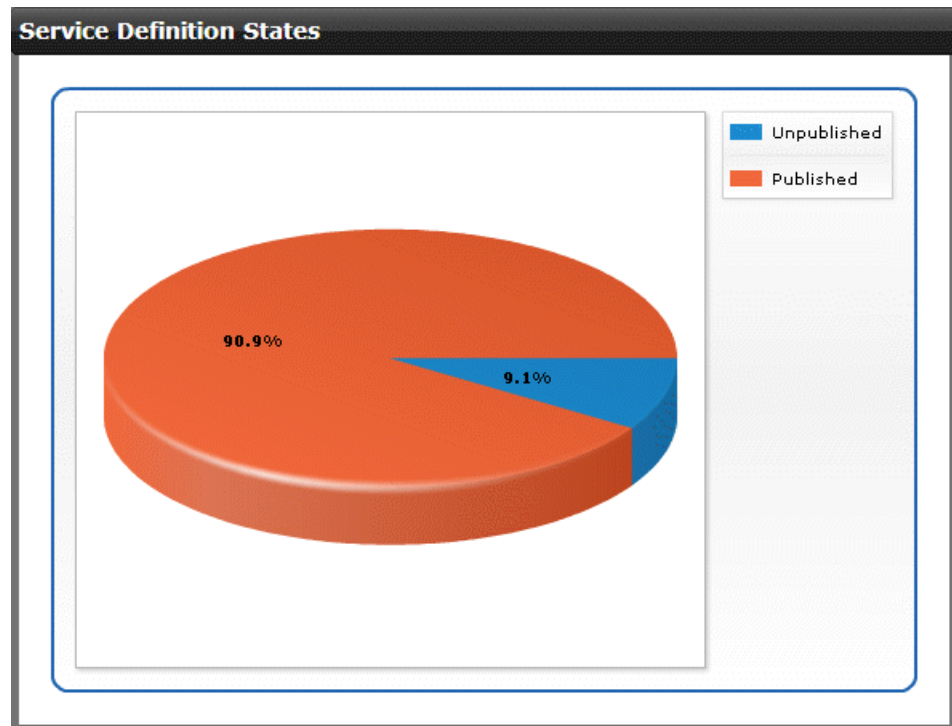
The **Manage Services** page shows only the services created from that service definition.

Viewing How Many Service Definitions Are in Each Service Definition State

To view the percentage or number of service definitions that are in each service definition state:

- In the OAM Insight task pane, select **Service Design**.

The Junos Space software displays the **Service Definition States** chart.



Each segment of the pie chart represents the proportion of service definitions in the indicated state. In this example, 78.8 percent of all completed service definitions are in the Published state.

To view the number of service definitions in a state, move the mouse cursor over the segment.

2. To see which service definitions are in each state, click a segment in the pie chart.

The **Manage Service Definitions** window shows only those service definitions from the selected segment.

Tasks in the OAM Design Workspace

The OAM Design workspace includes the following task:

- **Manage OAM Profiles**—The **Manage OAM Profiles** page displays the list the CFM and LFM profiles created. For more information on this page, see [“Managing CFM Profiles” on page 77](#).

To create a CFM Definition, click **Create CFM Definition**. For more information on creating a service order, see [“Creating and Managing CFM Service Orders” on page 41](#).

- **Manage Action Profiles**—The **Manage Action Profiles** page displays the list the action profiles created. For more information on this page, see [“Managing CFM Action Profiles” on page 85](#).

To create an action profile, click **Create CFM Action Profile**. For more information on creating a service order, see [“Creating and Viewing CFM Action Profiles” on page 24](#).

- SLA Iterator Profile—The **Manage SLA Iterator Profile** page displays the list the SLA-iterator profiles created. For more information on this page, see [“Managing SLA-Iterator” on page 89](#).

To create an action profile, click **Create SLA Iterator Profile**. For more information on creating a service order, see [“Creating and Viewing SLA-Iterator Profiles” on page 29](#).

**Related
Documentation**

- [Understanding the Prestage Devices Workspace on page 9](#)
- [Understanding the OAM Provisioning Workspace on page 39](#)

Creating and Viewing CFM Action Profiles

- [Creating a CFM Action Profile on page 24](#)
- [Viewing a CFM Action Profile on page 26](#)

Creating a CFM Action Profile

You can create a CFM action profile that you can use as a starting point for provisioning OAM Insight services. You can configure an action profile and specify the action to be taken when any of the configured events occur. Alternately, you can configure an action profile and specify default actions when connectivity to a remote MEP fails.



NOTE: Default Action Profile is a predefined action profile.

Select **OAM Design > Manage Action Profiles > Create CFM Action Profile**.

To create a CFM action profile:

1. Fill in the fields as indicated in the table.

Field	Action
Name	Specify the name of the action profile. Range: 1 through 50 characters. Space and special characters are allowed.
Description	Provide a meaningful description for the action profile. Range: 1 through 200 characters. Space and special characters are allowed.
Default Action	If you want to be notified that an interface is down, select this option. NOTE: You can either select Default Action or Configure Event .

Field	Action
Configure Event	<p>If you want notification about any of the following events and actions, select this option. When you select this option, the following fields are displayed:</p> <ol style="list-style-type: none"> Event <ul style="list-style-type: none"> Interface status tlv— Select the type of interface status tlv Connection protection tlv— Select the type of connection protection tlv Port status tlv blocked—Triggers an action when the incoming CCM packet contains port status TLV with value blocked. Adjacency loss—Triggers an action when the link adjacency is lost. Action <ul style="list-style-type: none"> Interface down—Brings the interface down when a remote MEP connectivity failure is detected Propagate remote mac flush—The propagate remote mac flush action is triggered when the incoming CCM packet contains the interface-status TLV with value down <p>Select one or more events or actions. You must select at least one event. On the occurrence of any of these events or actions, the system marks the interface down.</p>

- To create the action profile, click **Create**.

The action profile is saved in the database and appears in the **OAM Design > Manage Action Profiles** inventory page. You can then use the Action drawer to perform additional tasks, such as deleting or modifying action profiles, and applying tags.



NOTE: You can link the action profile to the service definition.

Viewing a CFM Action Profile

To view the list of CFM action profiles, select **OAM Design > Manage Action Profiles**.

To view a CFM action profile:

- Select an action profile.
- Double-click to view the details of an action profile. The **CFM Action Profile Details** window is displayed.

CFM Action Profile Details

General | Device Details

General

Name: StdDef-ActionProfile
Description: Predefined CFM action profile

Event

Interface status tlv: down
Port status tlv:
☒ Adjacency loss
 Connection protection tlv:

Action

☒ Interface down
☒ Propagate remote mac flush

OK

It has two the following two tabs:

- General— Displays action profile configuration
- Device Details— Displays list of devices attached to this action profile



NOTE: The action profile landing page displays the list of action profiles only in tabular view.

Related Documentation

- [Junos Space OAM Insight Overview on page 3](#)
- [Attaching an Action Profile on page 15](#)
- [Detaching an Action Profile on page 15](#)

Creating and Viewing LFM Action Profiles

You use the Ethernet Link Fault Management (LFM) to monitor link operations for physical point-to-point or emulated point-to-point Ethernet links that connect peer OAM entities. LFM is useful to:

- Detect failure on the physical links in both directions, as well as unidirectional failures.
- Put a port in link-loopback mode remotely for diagnostics purposes.

- Monitor a link for critical events.

LFM is a link-layer protocol and does not need a Layer 3 address, such as IPv4 or IPv6, for its operation. When LFM is configured on an aggregated link, it runs on each member link. This helps LFM to function on circuit cross-connect (CCC) or transport cross-connect encapsulated interfaces.

- [Creating an LFM Action Profile on page 28](#)
- [Viewing an LFM Action Profile on page 29](#)

Creating an LFM Action Profile

You use the Link Fault Management to define event fault flags and thresholds and the action to be taken when an event occurs.

To create an LFM Action Profile:

1. Select **OAM Design > Manage Action Profiles > Create LFM Action Profile**.
2. Fill in the fields as indicated in the table.

Field	Action
Name	Specify the name of the action profile. Range: 1 through 50 characters. Space and special characters are allowed.
Description	Provide a meaningful description for the action profile. Range: 1 through 200 characters. Space and special characters are allowed.
Link adjacency loss	Select this check box so that you receive a notification when the link adjacency is lost.
Protocol down	Select this check box so that you receive a notification when the circuit cross-connect, layer 2 circuits or layer 2 VPN are down. CCC-DOWN status is sent when these are down.
Frame error	Specify a rate of receiving frame error events (1–1000 error(s) per 100 millisecond).
Frame period	Specify a rate of receiving frame period events.
Frame period summary	Specify a rate of receiving frame period summary events.
Symbol period	Specify a rate of receiving symbol period events.
Link down	Select this check box to administratively disable the link when the link-fault event occurs.
Send critical event	Select this check box so that the system sends IEEE 802.3ah link event type, length, and values (TLVs) to the OAM Protocol Data Unit (PDU) when a link-fault event occurs.
Syslog	Select this check box so that the system creates a log entry when the link-fault event occurs.

3. Click **Create**.

Viewing an LFM Action Profile

To view an LFM action profile:

1. Select **OAM Design > Manage Action Profiles**.
2. Select an LFM action profile and double-click to view the details.

The **LFM Action Profile Details** window is displayed.

It has the following two tabs:

- General— Displays action profile configuration
- Device Details— Displays list of devices attached to this action profile



NOTE: The Manage Action Profiles window displays the list of action profiles only in tabular view.

Related Documentation

- [Junos Space OAM Insight Overview on page 3](#)
- [Attaching an Action Profile on page 15](#)
- [Detaching an Action Profile on page 15](#)

Creating and Viewing SLA-Iterator Profiles

An iterator periodically transmits service level agreement (SLA) measurement packets as ITU-Y.1731 - compliant frames for two-way delay measurement or loss measurement. For an iterator to form a remote adjacency (pairing of two end points) and to become operational, the continuity check message (CCM) must be active between the CFM local and remote MEP configurations. The OAM Insight application uses SLA-iterator profiles to collect Y.1731 statistics. These iterator profiles have to be configured before starting performance monitoring. The OAM Insight application discovers already configured SLA-iterator profiles while discovering the OAM devices.

There are three predefined SLA-iterator profiles for frame loss, frame delay and two-way delay measurements, respectively. You can also create SLA-iterator profiles through the user interface. The OAM Insight application manages the association between SLA-iterator profiles and devices it has been deployed. You can attach or detach these SLA-iterator profiles to several devices any time.

- [Creating SLA-Iterator Profiles on page 29](#)
- [Viewing SLA Iterator Profile on page 31](#)

Creating SLA-Iterator Profiles

You can create an iterator profile with its parameters to periodically transmit SLA measurement packets as ITU-Y.1731-compliant frames for delay measurement or loss measurement. To create a SLA iterator profile, select **OAM Design > SLA Iterator Profile >**

Create SLA Iterator Profile. The **SLA Iterator Profile** page appears displaying the SLA-Iterator profile information.

To begin to create an SLA-iterator profile:

1. Fill in the fields as indicated in the table.

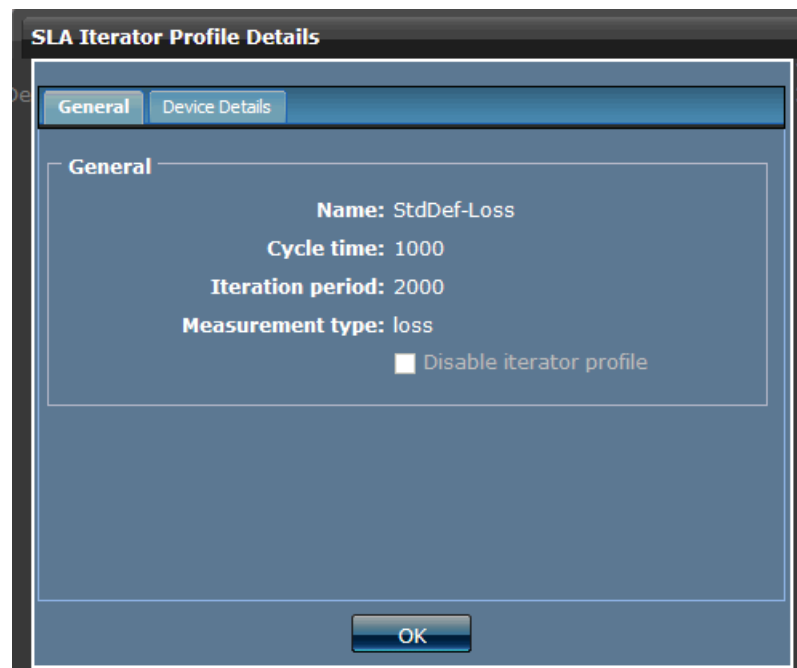
Field	Action
Name	Specify the name of the SLA-iterator profile. Range: 1 through 50. Space and special characters are allowed.
Cycle time	Specify the time period for an iterator profile. Range: 10 through 3600000 milliseconds Default: 10 milliseconds
Iteration period	Specify the maximum services under an iterator profile. Range: 1 through 2000 services Default: 1 service
Disable iterator profile	Disables an iterator profile.
Measurement type	Choice of the type of Y.1731 (SLA measurement) frame to be sent. Select the measurement type: <ul style="list-style-type: none"> • Loss— Y.1731 LM frames are sent for this profile • statistical frame loss— Y.1731 two way DM frames for statistical frame loss are sent for this profile • two way delay— Y.1731 2-way DM frames are sent for this profile

2. To finish creating the SLA Iterator Profile, click **Create**.

The SLA-iterator profile is saved in the database and appears in the **OAM Design > SLA Iterator Profile** inventory page. You can then open the **Actions** menu to perform additional tasks, such as deleting or publishing service definitions and applying tags.

Viewing SLA Iterator Profile

The **SLA Iterator Profile** inventory page lists the SLA-iterator profiles. Double-click an SLA-iterator profile to view its details.



The SLA iterator Profile Details window:

- General tab—Displays the action profile configuration
- Device Details tab—Displays a list of devices attached to an SLA-iterator profile

Related Documentation

- [Junos Space OAM Insight Overview on page 3](#)
- [Attaching an SLA-Iterator Profile on page 16](#)
- [Detaching an SLA-Iterator Profile on page 17](#)

Creating CFM Profiles

You can create CFM profiles that you can use as a starting point for provisioning OAM Insight services. A CFM service is defined as the collection of maintenance end points (MEP), or maintenance intermediate points (MIP) in one maintenance association.

A service definition provides a template upon which services are built. It specifies service attributes that are not specific to a service instance. These service definitions are capable of providing the basis for most of the service orders your organization will need to create. The OAM insight provides a set of predefined service definitions. In case these predefined service definitions are not adequate for all your needs, you can create service definitions of your own.

- [Configuring a CFM Profile-General Tab on page 32](#)
- [Configuring a CFM Profile-MA Settings Tab on page 33](#)
- [Configuring a CFM Profile-MEP Settings Tab on page 35](#)

Configuring a CFM Profile-General Tab

To create a CFM definition, select **OAM Design > Manage OAM Profile > Create CFM Profile**. The **Create CFM Definition** window appears displaying the **General** tab.

To begin to create a CFM profile, from the **General** tab:

1. Fill in the fields as indicated in the table.

Field	Action
Name	Type a unique name that identifies a CFM profile. Range: 1 through 50. Space and special characters are allowed.
Comments	Type a comment that identifies a CFM profile. Range: 1 through 50. Space and special characters are allowed.

Field	Action
Type	Select MEP (maintenance association endpoint configuration).
Domain name	Enter the domain name. Range: The maximum field length is 50. Space and special characters are allowed.
Domain level	Select the level of the domain. Range: 0 through 7 Default: 1
Remote MEP	If you want to enable the MEP settings tab, select this option.

- Go to the **MA Settings** tab.

Configuring a CFM Profile-MA Settings Tab

To continue to configure the CFM profile, select the **MA Settings** tab:

To continue to create a CFM profile, from the **MA Settings** tab:

- Fill in the fields as indicated in the table.

Field	Action
Hold Interval (mts)	Specify the time before flushing MEP database, if no updates occurs. Range: 1 through 256 minutes Default: 1 minute

Field	Action
Message Interval	<p>Select the message interval between the continuity-check messages, where s = seconds, m = minutes, and ms = milliseconds.</p> <ul style="list-style-type: none"> • 1s • 1m • 10m • 10ms • 100ms
Loss Threshold (PDUs)	<p>Specify the number of continuity-check messages lost before marking endpoint as down.</p> <p>Range: 3 through 256</p> <p>Default: 3</p>
Include interface status TLV in CCM	To include the interface status TLV in the CCM, select the check box
Include Port status TLV in CCM	To include the port status TLV in the CCM, select the check box
Include connection protection OUI TLV in CCM	To include the connection protection OUI TLV in the CCM, select the check box
MEP ID Selection	<p>Select the maintenance association endpoint configuration's ID from the list:</p> <ul style="list-style-type: none"> • Auto pick—The system will generate the unique MEP ID. • Select manually—The user has to provide a MEP ID while creating a service order.
Direction	Select the direction of maintenance endpoint.
Priority	<p>Select the 802.1p priority of continuity-check and link-trace packet</p> <p>Range: 0 through 7</p> <p>Default: 0</p>
Accept continuity check messages from all remote MEPS	Select this field to accept the continuity messages from all remote MEPS.



NOTE: Select the **Editable in Service Order** box to modify the CFM service definition setting when configuring the CFM service order.

2. If you have selected the **Remote MEP** check box in the General tab, go to the **MEP settings** tab.



NOTE: If you have not selected the Remote MEP check box in the **General** tab, click **Create**. The CFM definition is saved in the database and appears in the **OAM Design > Manage OAM Profiles** inventory page. You can then use the **Actions** menu to perform additional tasks, such as deleting or publishing service definitions and applying tags.

Configuring a CFM Profile-MEP Settings Tab

To configure the MEP settings, select the **MEP settings** tab:

To complete creating a CFM profile, from the **MEP settings** tab:

1. Fill in the fields as indicated in the table.

Field	Action
Action Profile	Select an action profile.
Add profile	<p>Click the plus icon to specify the following fields:</p> <ul style="list-style-type: none"> • SLA Profile—Select an SLA-iterator profile • Data TLV Size—Specify the size of the data TLV portion of the Y.1731 data frame. Range: 1 through 1400 bytes • Iteration Count—Specify the number of iterations for which the connection should partake in the iterator for acquiring SLA measurements. Range: 1 through 65,535 • Priority—Specify the 802.1p priority of continuity-check and link-trace packet Range: 0 through 7 <p>To delete an SLA-iterator, select a desired row and click the delete icon.</p>

2. To create a CFM Definition, click **Create**.

The CFM profile is saved in the database and appears in the **OAM Design > Manage OAM Profiles** inventory page. You can then open the **Actions** menu to perform additional tasks, such as deleting or publishing service definitions and applying tags.

Related Documentation

- [Junos Space OAM Insight Overview on page 3](#)
- [Prestaging OAM Devices on page 12](#)
- [Creating and Managing CFM Service Orders on page 41](#)

Creating an LFM Profile

To create an LFM Profile:

1. Select **OAM Design > Manage OAM Profiles > Create LFM Profile**.
The **Create LFM Profile** window is displayed.
2. Fill in the fields as indicated in the table.

Field	Action
Name	Type a unique name that identifies an LFM profile. Range: 1 through 50 characters. Space and special characters are allowed.
Comments	Type a comment that identifies an LFM profile. Range: 1 through 200 characters. Space and special characters are allowed.
Link discovery	Select one. <ul style="list-style-type: none"> • Active • Passive
PDU interval	Specify an OAM PDU interval in the range 100-1000 milliseconds. OAM PDUs are slow protocol frames that conforms to IEEE 802.3 and contains OAM control and status information, which is used to monitor, test, and troubleshoot links. OAM PDUs also carry notification of non-critical link events such as errored frame event, errored frame period event, errored frame seconds summary event, and organization-specific event.
PDU threshold	Specify a threshold for fault events that trigger the sending of link event TLVs when the values exceed the threshold.
Remote loop-back	Select this check box to change a remote DTE into loop-back mode.
Action profile	Select an LFM action profile from the list.
Frame error	Specify a threshold for receiving frame error events. Specify a value in the range 1 through 100.

Field	Action
Frame period	Specify a threshold for receiving frame period events. Specify a value in the range 1 through 100.
Frame period summary	Specify a threshold for receiving frame period summary events. Specify a value in the range 1 through 100.
Symbol period	Specify a threshold for receiving symbol period events. Specify a value in the range 1 through 100.
Allow remote loop-back	Select this check box to allow local port to be changed to loop-back mode.
No allow link events	Select this check box to prevent the periodic sending of PDU frames and symbol errors.

3. Click **Create**.

CHAPTER 4

OAM Service Provisioning

- [Understanding the OAM Provisioning Workspace on page 39](#)
- [Creating and Managing CFM Service Orders on page 41](#)
- [Deploying a CFM Service Order on page 45](#)
- [Validating a CFM Service Order on page 46](#)
- [Creating an RFC2544 Test Profile on page 47](#)

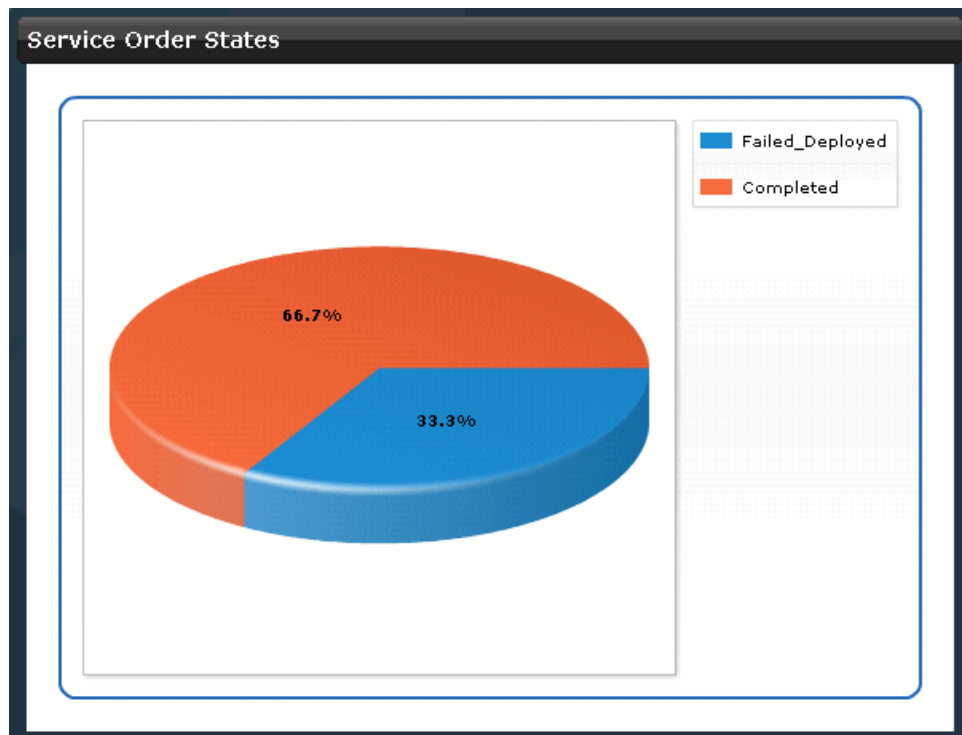
Understanding the OAM Provisioning Workspace

The OAM Provisioning workspace provides a visual overview of the service orders on your network, and enables you to quickly access related and commonly needed information. You can view service orders in a specific state. For example, you can check for failed service orders and then access a list of failed requests so you can begin to take corrective action.

To view service orders by service order state.

1. In the OAM Insight task pane, select **OAM Provisioning**.

The system displays the chart named **Service Order States**.



Each segment of the pie chart represents the proportion of service orders in a specific service order state:

- **Completed**—The service order has been successfully deployed.
- **Deployment Failed**—An attempted service deployment was not successfully completed or failed an audit.

The OAM Provisioning workspace includes the following task:

- **Manage OAM Orders**—The **Manage OAM Service Orders** page lists the OAM service orders created. For more information on this page, see [“Managing CFM Service Orders” on page 81](#).

To create a service order, click **Create CFM Service Order**. For more information on creating a service order, see [“Creating and Managing CFM Service Orders” on page 41](#).

- **Manage OAM Services**—See [“Viewing Provisioned CFM Services” on page 94](#)

Related Documentation

- [Understanding the Prestage Devices Workspace on page 9](#)
- [Understanding the OAM Design Workspace on page 21](#)

Creating and Managing CFM Service Orders

You can view the state of OAM service orders on the OAM Provisioning workspace statistics page. If you have not created a CFM service order, a link appears for you to create one. To create a CFM service order, you need to discover devices that have been configured from the Junos Space network application platform database and create a CFM definition.

The Service Orders pie chart displays the state of all of the CFM service orders you created. The CFM service order states are: completed (deployed) and requested (saved but not deployed).

Use the Service Orders pie chart to filter CFM orders on the Manage OAM Orders. For example, if you click the percentage of orders that are deployed, you view only the deployed orders on the Manage OAM Orders page.

- [Configuring CFM Service Order Information on page 41](#)
- [Configuring CFM Service Order Common Settings on page 42](#)
- [Configuring Endpoint Settings on page 44](#)

Configuring CFM Service Order Information

To create a CFM Service Order, select **OAM Provisioning > Manage OAM Orders > Create CFM Service Orders**. The Create CFM Service Order page appears displaying the Order Information.

To begin to create a CFM service order:

1. Fill in the fields as indicated in the table.

Field	Action
Service Definition	<p>Select the CFM service definition from the list of CFM service definitions available in the database. The OAM Insight provides a predefined service definition that a service provisioner can choose from when creating a service order.</p> <p>NOTE: To view the service definition details, click the icon next to the list menu.</p>
Name	<p>Specify the name of the CFM service order.</p> <p>Range: 1 through 50. Space and special characters are allowed.</p>
Comments	<p>Enter a comment that describes the CFM service order.</p> <p>Range: 0 through 50. Space and special characters are allowed.</p>
Domain name	The maintenance domain specified in the CFM definition is displayed.
Domain level	The priority level of the maintenance domain specified in the CFM definition is displayed.
Select End point devices	Select the available device from the Available box and click the right arrow button to move it to the Selected list box.

2. Click **Next** to go to the **Common Settings** window.

Configuring CFM Service Order Common Settings

Configure the common settings:

Create CFM Service Order

Common Settings

Continuity Check Settings

Hold interval (min):

Message interval:

Loss threshold (PDUs):

☐ Include interface status TLV in CCM

☐ Include Port status TLV in CCM

☐ Include connection protection OUI TLV in CCM

MEP Settings

Direction:

Priority:

☒ Accept continuity check messages from all remote MEPs

Navigation:

Order Information
Common Settings
Endpoint Settings

To continue to create a CFM service order, from the Common Settings window:

1. Fill in the fields as indicated in the table.



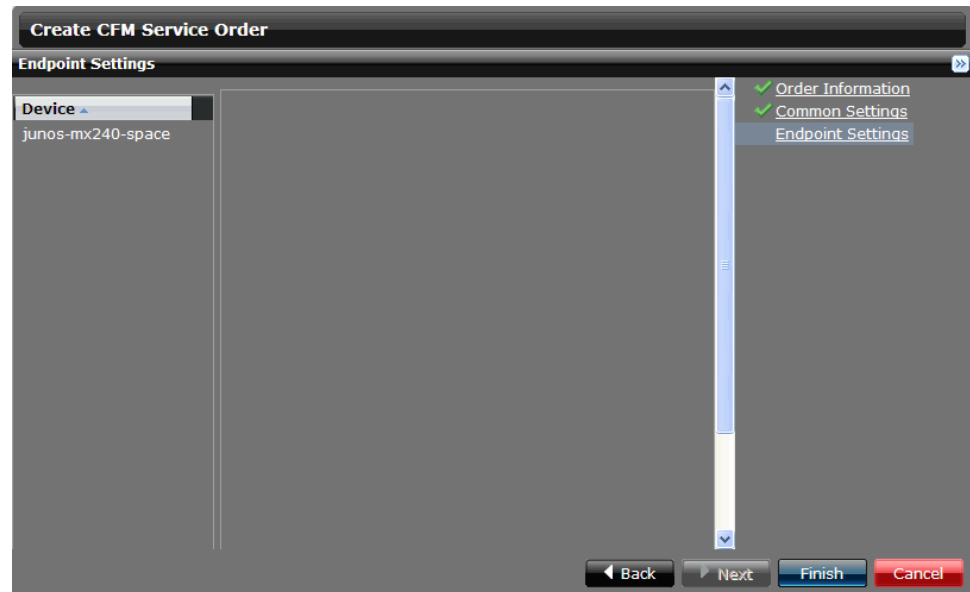
NOTE: You can edit these fields only if you have selected the **Editable in Service Order** in the service definition that you choose while configuring the Order Information.

Field	Action
Hold interval (min)	Specify the time before flushing MEP database, if no updates occurs. Range: 1 through 256 minutes Default: 1 minute
Message interval	Select the message interval between the continuity-check messages, where s = seconds, m = minutes, and ms = milliseconds: <ul style="list-style-type: none"> • 1s • 1m • 10m • 10ms • 100ms
Loss threshold (PDUs)	Specify the number of continuity-check messages lost before marking endpoint as down. Range: 3 through 256 Default: 3
Include interface status TLV in CCM	To include the interface status TLV in the CCM, select the this check box
Include Port status TLV in CCM	To include the port status TLV in the CCM, select the this check box
Include connection protection OUI TLV in CCM	To include the connection protection OUI TLV in the CCM, select the this check box
Direction	Select the direction of maintenance endpoint.
Priority	Select the 802.1p priority of continuity-check and link-trace packets Range: 0 through 7 Default: 0
Accept continuity check messages from all remote MEPs	Select this check box to specify the action profile name.
Action Profile for remote MEP	Select the action profile name. NOTE: This field is required only if Accept continuity check messages from all remote MEPs is unchecked

2. Select **Next** to go to the **Endpoint Settings** window.

Configuring Endpoint Settings

Configure the endpoint settings:



The **Device** panel displays the list of devices. To continue to create a CFM service order, from the Endpoint Settings window:

1. Select a device. Fill in the fields as indicated in the table.

Field	Action
CFM Interface	Select the interface for the device.
MEP ID	ID of the maintenance association endpoint configuration.

2. Configuring Remote MEP:

You can configure remote MEPs for end points only if the **Remote MEP** in the service definition is enabled.

- a. Click the plus icon to add a remote MEP.
- b. Select the remote MEP device from the list. Fill in the fields as indicated in the table.

Field	Action
Action Profile	Select an action profile for a remote MEP device

NOTE: The **Action Profile** lists only the action profiles attached to the selected end point device.

Field	Action
SLA Profile	<p>Click the plus symbol to add a SLA profile and specify the following fields:</p> <ul style="list-style-type: none"> • SLA Profile—Select an SLA-iterator profile from the list • Data TLV Size—Specify the size of the data TLV portion of the Y.1731 data frame. Range: 1 through 1400 bytes • Iteration Count—Specify the number of iterations for which the connection should partake in the iterator for acquiring SLA measurements. Range: 1 through 65,535 • Priority—Specify the 802.1p priority of continuity-check and link-trace packet Range: 0 through 7 <p>NOTE: The SLA Profile lists only the SLA-iterator profiles attached to the selected end point device.</p>

3. To finish creating the CFM service order, click **Create**.

The CFM Service Order is saved in the database and appears in the **OAM Design > Manage CFM Service Order** inventory page. You can then use the Action Drawer to perform additional tasks, such as deleting or publishing service definitions and applying tags.

- Related Documentation**
- [Junos Space OAM Insight Overview on page 3](#)
 - [Prestaging OAM Devices on page 12](#)
 - [Creating CFM Profiles on page 31](#)

Deploying a CFM Service Order

This procedure schedules a service for deployment on the network. Use this procedure to perform the following tasks:

- Deploy a new service.
- Deploy a modified service.
- Redeploy a service order that failed deployment.

You cannot deploy an invalid service order.

To schedule a service for deployment:

1. In the OAM Insight pane, select **OAM Provisioning**.
2. In the **Service Order States** pie chart, click the **Failed_Deployed** segment.

The **Manage OAM Orders** page shows only those service orders in the Failed_Deployed state.

3. Select the service order you want to deploy.
4. Open the **Actions** menu and click **Deploy Service Order**.

OAM Insight displays the **Schedule Service Order** page.

5. Schedule the service deployment.

- To deploy the service immediately, select **Deploy now**, and click **OK**.
- To deploy the service at a later time, select **Deploy later**, and select a date and time for deployment, then click **OK**.

The time field specifies the time kept by the server, but in the time zone of the client.

After scheduling the service order for deployment, the provisioning software begins validating the service order.

6. Use the **Job Management** workspace to monitor the outcome of the deployment. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details about the Jobs workspace.

**Related
Documentation**

- [Managing CFM Service Orders on page 81](#)
- [Validating a CFM Service Order on page 46](#)
- [Deleting a CFM Partial Configuration on page 82](#)
- [Deleting a CFM Service Order on page 84](#)

Validating a CFM Service Order

This procedure validates a service order but does not push the configuration to the device. Use this procedure to perform the following tasks:

- Validate a service request in the REQUESTED state.
- Validate a service request in the INVALID state after making necessary configuration changes on one or more PE devices associated with the service order.

To schedule a service order for validation, follow these steps:

1. In the OAM Insight task pane, select **OAM Provisioning**.
2. In the **Service Orders States** pie chart, click the **Requested** or **Failed Deployment** segment.

The **Manage Service Orders** page shows only those service orders in the Requested state.

3. Select the service order you want to validate and save.
4. Open the **Actions** menu and click **Validate Service Order**.

The **Schedule Service Request Validation** window appears.

5. Validate a service now or at some future time:
 - To validate the service immediately, select **Validate now**, and click **OK**.
 - To validate the service at a later time, select **Validate later**, select a date and time for deployment, and then click **OK**.



NOTE: When specifying a time to validate the service, the time field specifies the time kept by the server, but in the time zone of the client.

After scheduling the service order for validation, the provisioning software begins validating the service order.

6. Click the Job ID in the **Job Details** window to view details about the service validation.
7. Use the Jobs workspace to monitor the outcome of the validation. See *Viewing Jobs* in the *Junos Space Network Application Platform User Guide* for details about the Jobs workspace.

**Related
Documentation**

- [Managing CFM Service Orders on page 81](#)
- [Deploying a CFM Service Order on page 45](#)
- [Deleting a CFM Partial Configuration on page 82](#)
- [Deleting a CFM Service Order on page 84](#)

Creating an RFC2544 Test Profile

To create an RFC2544 test profile:

1. In the OAM Insight task pane, select **RFC2544 Test > Manage Test Configuration > Create RFC2544 Test**.
2. In the **Create RFC2544 Test** window, enter information in the fields of the **General Settings** panel.

General Settings	
Name:	<input type="text"/>
Comments:	<div></div>
<input checked="" type="checkbox"/> Throughput	
Bandwidth:	<input type="text"/> kbps
Packetsize:	<input type="text" value="Please Select..."/>
<input checked="" type="checkbox"/> Frame Loss	
Bandwidth:	<input type="text"/> kbps
Packetsize:	<input type="text" value="Please Select..."/>
Step percent:	<input type="text"/>
<input checked="" type="checkbox"/> Latency	
Bandwidth:	<input type="text"/> kbps
Packetsize:	<input type="text" value="Please Select..."/>
<input checked="" type="checkbox"/> Back-to-Back	
Bandwidth:	<input type="text"/> kbps
Packetsize:	<input type="text" value="Please Select..."/>

Field	Description
Name	A name for the test profile.
Comments	Comments to describe the test profile.
Throughput	Throughput is the maximum rate at which no transmitted frames are dropped by the device or system under test (DUT/SUT). <ul style="list-style-type: none"> Bandwidth (kbps). Packet size—The size of the test frames being transmitted.
Frame Loss	The percentage of frames that should have been forwarded by a network device under steady state (constant) loads that were not forwarded due to lack of resources. <ul style="list-style-type: none"> Bandwidth (kbps). Packet size—The size of the test frames being transmitted. Step percent.
Latency	The time interval that begins when the last bit of the input frame reaches the input port and ends when the first bit of the output frame arrives on the output port. Latency is the time it takes a bit to go through the network and return. <ul style="list-style-type: none"> Bandwidth (kbps). Packet size—The size of the test frames being transmitted.

Field	Description
Back-to-Back	<p>Also called <i>burst</i>, this test reveals the number of frames included in the longest, sustained transmission that the device or network to be tested can manage without losing any frames.</p> <ul style="list-style-type: none"> • Bandwidth (kbps). • Packet size—The size of the test frames being transmitted.

3. When you are done entering information in the **General Settings** fields, click **Next**. The **Test Settings** window appears.

Configuring the Initiator Device

To configure the Initiator device to support operation of the RFC2544 test:

1. Click on **Initiator** in the left panel and enter information in the fields in the **Initiator** panel.



NOTE: The appearance of the Initiator window depends on the value you specify for the Family parameter. The following illustration shows the window that appears when you specify ccc. The subsequent illustration shows the window that appears when you specify inet.

Initiator

Device Name:

Please Select...

Family:

ccq

Test interface:

Please Select...

Source IPv4 address:

Source MAC address:

Source UDP port:

Destination IPv4 address:

Destination MAC address:

Destination UDP port:

Direction:

Please Select...

DSCP code points:

Forwarding class:

Inner VLAN ID:

Outer VLAN ID:

☐ Skip ARP iteration

Test iteration duration:

Initiator

Device Name:

Family:

Source IPV4 address:

Source UDP port:

Destination IPV4 address:

Destination UDP port:

DSCP code points:

Forwarding class:

☐ Halt on prefix down

☐ Skip ARP iteration

Test iteration duration:

Field	Description
Device Name	Name of the device on which the Initiator interface is located.
Family	Family type: <ul style="list-style-type: none"> • inet • ccc
Test Interface	Specify the interface ID on the Initiator device on which the test will be run.
Source IPV4 address	IPV4 address of the interface from which test data originates.
Source MAC address	MAC address of the device from which test data originates, expressed in xx:xx:xx:xx:xx:xx format.
Source UDP port	UDP port from which test data originates. Range: 1 through 65535
Destination IPV4 address	IPV4 address of the interface to which test data is sent.
Destination MAC address	MAC address of the host to which test data is sent, expressed in xx:xx:xx:xx:xx:xx format.
Destination UDP port	UDP port from which test data originates. Range: 1 through 65535

Field	Description
Direction	The direction of the data flow to be tested: <ul style="list-style-type: none"> Egress Ingress
DSCP code points	Specifies the DSCP code points to use in the generated test frames. If not specified, '0' is used in DSCP code point fields in the IP header.
Forwarding Class	Forwarding class assigned to the egress frames of this test: <ul style="list-style-type: none"> assured-forwarding best-effort expedited-forwarding network-control
Halt on prefix down	By default, an RFC2544 test ignores a prefix down event (that is, when the prefix associated with the test goes down) and continues to run. If you specify this parameter, when a prefix goes down, corresponding tests are aborted. The show output for the test indicates that the test was aborted due to prefix going down.
Inner VLAN ID	Inner VLAN ID.
Outer VLAN ID	Outer VLAN ID.
Skip ARP iteration	This parameter is valid only in <i>family inet</i> mode. ARP iteration is a 3-second iteration that is run for all inet tests. The results of this iteration are ignored in test result calculations. Sending test frames for 3 seconds ensures that all devices on the path to the destination build their ARP entries.
Test iteration duration	Duration of each iteration, in seconds. Range: 1 through 172800

- When you are done entering information in the **Initiator** panel, select **Reflector** in the left panel.

Configuring the Reflector Device

To configure the Reflector device to support operation of the RFC2544 test:

- Enter information in the fields in the **Reflector** panel.



NOTE: The appearance of the **Reflector** window depends on the value you specify for the **Family** parameter. The following illustration shows the window that appears when you specify **ccc**. The subsequent illustration shows the window that appears when you specify **inet**.

Reflector

Device Name:

Please Select...

Family:

ccc

Test interface:

Please Select...

Source IPv4 address:

Source MAC address:

Source UDP port:

Destination IPv4 address:

Destination MAC address:

Destination UDP port:

Direction:

Please Select...

Forwarding class:

Inner VLAN ID:

Outer VLAN ID:

Reflect etype:

Reflect mode:

Please Select...

☐ Skip ARP iteration

Reflector

Device Name:

Family:

Test interface:

Source IPV4 address:

Source UDP port:

Destination IPV4 address:

Destination UDP port:

Forwarding class:

☐ Halt on prefix down

☐ Skip ARP iteration

Field	Description
Device Name	Name of the device on which the Reflector interface is located.
Family	Family type: <ul style="list-style-type: none"> inet ccc
Test interface	Specify the interface ID on the Reflector device on which the test will be run.
Source IPV4 address	IPV4 address of the interface from which test data originates.
Source MAC address	MAC address of the device from which test data originates, expressed in xx:xx:xx:xx:xx:xx format.
Source UDP port	UDP port from which test data originates. Range: 1 through 65535
Destination IPV4 address	IPV4 address of the interface to which test data is sent.
Destination MAC address	MAC address of the device to which test data is sent, expressed in xx:xx:xx:xx:xx:xx format.
Destination UDP port	UDP port to which test data is sent. Range: 1 through 65535
Direction	The direction of the data flow to be tested: <ul style="list-style-type: none"> Egress Ingress

Field	Description
DSCP code points	Specifies the DSCP code points to use in the generated test frames. If not specified, '0' is used in DSCP code point fields in the IP header.
Forwarding class	Forwarding class assigned to the egress frames of this test: <ul style="list-style-type: none"> assured-forwarding best-effort expedited-forwarding network-control
Halt on prefix down	By default, an RFC2544 test ignores a prefix down event (that is, when the prefix associated with the test goes down) and continues to run. If you specify this parameter, when a prefix goes down, corresponding tests are aborted. The show output for the test indicates that the test was aborted due to prefix going down.
Inner VLAN ID	Inner VLAN ID.
Outer VLAN ID	Outer VLAN ID.
Reflect etype	Specifies the etype to use for reflection. This parameter is valid only in <i>mode reflect</i> . If not specified, all etypes are reflected. Range: 1 through 65535
Reflect mode	Reflect Mode: <ul style="list-style-type: none"> mac-rewrite mac-swap no-mac-swap
Skip ARP iteration	This parameter is valid only in <i>family inet</i> mode. ARP iteration is a 3-second iteration that is run for all inet tests. The results of this iteration are ignored in test result calculations. Sending test frames for 3 seconds ensures that all devices on the path to the destination build their ARP entries.

- When you are done entering information in the **Reflector** tab fields, click **Finish**.

Starting an RFC2544 Test

To start a configured RFC2544 test:

- In the OAM Insight task pane, select **RFC2544 Test > Manage Test**.
- From the list of tests in the **Manage Test** window, right-click the test you want to run and select **Start Test**.



Stopping an RFC2544 Test

To stop a configured RFC2544 test:

1. In the OAM Insight task pane, select **RFC2544 Test > Manage Test**.
2. From the list of tests in the **Manage Test** window, right-click the test you want to stop and select **Halt Test**.

Viewing RFC2544 Test Results

To view the test results for an RFC2544 test:

1. In the OAM Insight task pane, select **RFC2544 Test > Manage Test**.
2. From the list of tests in the **Manage Test** window, right-click the test for which you want to view results and select **View RFC2544 Test Result**.

The **View RFC2544 Test** window appears, which displays information in four panels:

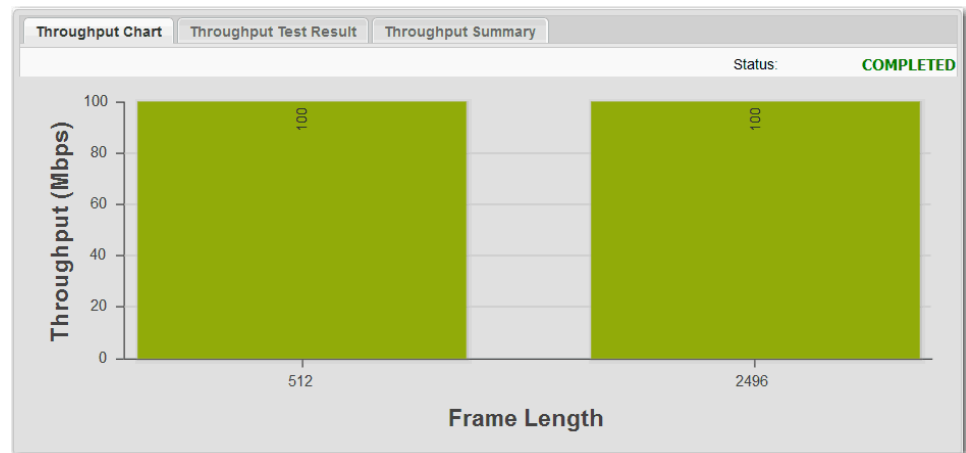
- Throughput (top left panel)
- Latency (bottom left panel)
- Frameloss (top right panel)
- Back Back (bottom right panel)

Each of the four panels includes three tabs. If you click on a tab, the OAM Insight application displays a detailed illustration of the test result for the corresponding test profile. If a parameter was not configured in the RFC2544 test profile, the corresponding panel displays the message, "Test case not configured for this profile."



Throughput Panel Tabs

The following illustration shows the information displayed by the **Throughput Chart** tab.



The following illustration shows the information displayed by the **Throughput Test Result** tab.

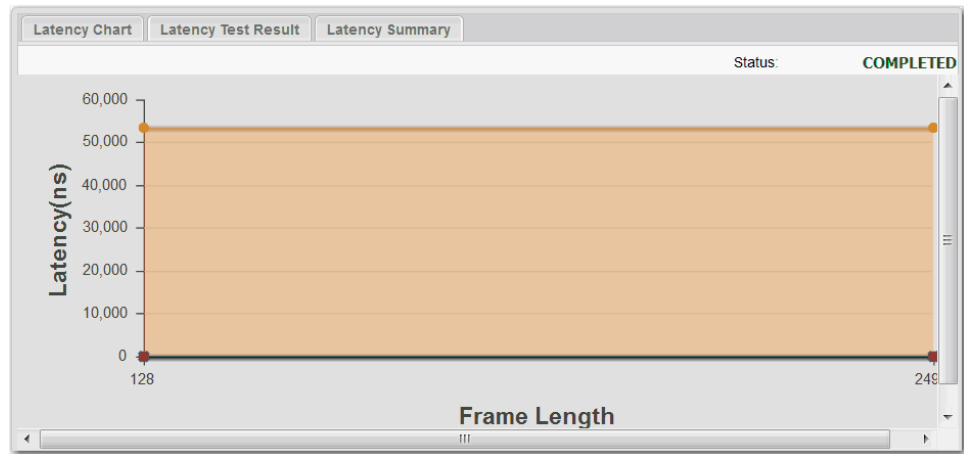
Throughput Chart Throughput Test Result Throughput Summary								
Status: COMPLETED								
Packet Size: 512								
Iteration Count	Duration	TX Packet	RX Packet	TX Bytes	RX Bytes	PPS	Bandwidth	Throughput %
1	3	72	0	36864	0	23	1001	10
2	10	2320	0	1187840	0	231	1001	100
Packet Size: 2496								
Iteration Count	Duration	TX Packet	RX Packet	TX Bytes	RX Bytes	PPS	Bandwidth	Throughput %
1	3	12	0	29952	0	4	1001	10
2	10	500	0	1248000	0	49	1001	100

The following illustration shows the information displayed by the **Throughput Summary** tab.

Throughput Chart Throughput Test Result Throughput Summary	
Status: COMPLETED	
Test Profile Configuration	
Test-profile name:	Test16_throughput
Test packet size:	512,2496
Theoretical max bandwidth:	1001
Test Configuration	
Test mode:	Initiate-and-Terminate
Duration in seconds:	10
Test family:	inet
Routing Instance Name:	default
INET family Configuration	
Egress Interface:	
Source ipv4 address:	20.1.46.2
Destination ipv4 address:	20.1.46.1
Source udp port:	31
Destination udp port:	32

Latency Panel Tabs

The following illustration shows the information displayed by the **Latency Chart** tab.



The following illustration shows the information displayed by the **Latency Test Result** tab.

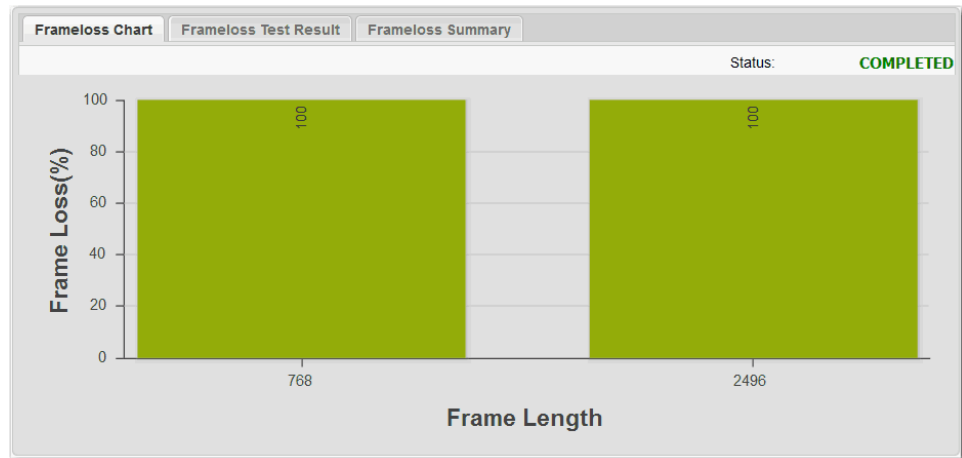
Status: COMPLETED										
Packet Size: 128										
Iteration	Count	Duration	TX Packet	RX Packet	Latency MIN	Latency MAX	Latency AVG	Latency PRC	PPS	Bandwidth
1	3		720	0	0	0	0	53424	240	3001
2	10		24050	0	0	0	0	53424	2404	3001
Packet Size: 2496										
Iteration	Count	Duration	TX Packet	RX Packet	Latency MIN	Latency MAX	Latency AVG	Latency PRC	PPS	Bandwidth
1	3		42	0	0	0	0	53424	14	3001
2	10		1480	0	0	0	0	53424	148	3001

The following illustration shows the information displayed by the **Latency Summary** tab.

Status: COMPLETED	
Test Profile Configuration	
Test-profile name:	Test16_latency
Test packet size:	128,2496
Theoretical max bandwidth:	3001
Test Configuration	
Test mode:	Initiate-and-Terminate
Duration in seconds:	10
Test family:	inet

Frameless Panel Tabs

The following illustration shows the information displayed by the **Frameloss Chart** tab.



The following illustration shows the information displayed by the **Frameloss Test Result** tab.

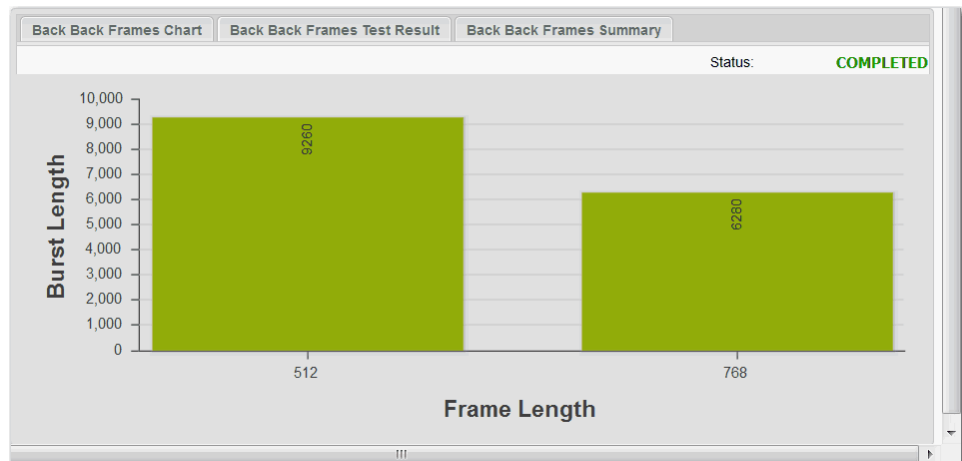
Frameloss Chart										Status: COMPLETED
Frameloss Test Result										
Frameloss Summary										
Packet Size: 768										
Iteration Cou	Duration	TX Packet	RX Packet	TX Bytes	RX Bytes	PPS	Bandwidth	Throughput	Frame Loss %	
1	3	96	0	73728	0	31	2001	10	100	
2	10	3140	0	2411520	0	314	2001	100	100	
Packet Size: 2496										
Iteration Cou	Duration	TX Packet	RX Packet	TX Bytes	RX Bytes	PPS	Bandwidth	Throughput	Frame Loss %	
1	3	30	0	74880	0	9	2001	10	100	
2	10	1000	0	2496000	0	99	2001	100	100	

The following illustration shows the information displayed by the **Frameloss Summary** tab.

Frameless Chart		Frameless Test Result		Frameless Summary	
Status: COMPLE					
Test Profile Configuration					
Test-profile name:	Test16_frame-loss				
Test packet size:	768,2496				
Theoretical max bandwidth:	2001				
Test Configuration					
Test mode:	Initiate-and-Terminate				
Duration in seconds:	10				
Test family:	inet				
Routing Instance Name: default					
INET family Configuration					
Egress Interface:					
Source ipv4 address:	20.1.46.2				
Destination ipv4 address:	20.1.46.1				
Source udp port:	31				
Destination udp port:	32				

Back Back Panel Tabs

The following illustration shows the information displayed by the **Back Back Frames Chart** tab.



The following illustration shows the information displayed by the **Back Back Frames Test Result** tab.

Back Back Frames Chart Back Back Frames Test Result Back Back Frames Summary							
Status: COMPLETED							
Packet Size: 512							
Iteration Count	Duration	TX Packet	RX Packet	TX Bytes	RX Bytes	Bandwidth	Burst %
1	0	276	0	141312	0	4001	276
2	0	9260	0	4741120	0	4001	9260
Packet Size: 768							
Iteration Count	Duration	TX Packet	RX Packet	TX Bytes	RX Bytes	Bandwidth	Burst %
1	0	186	0	142848	0	4001	186
2	0	6280	0	4823040	0	4001	6280

The following illustration shows the information displayed by the **Back Back Frames Summary** tab.

Back Back Frames Chart Back Back Frames Test Result Back Back Frames Summary	
Status: COMPLETED	
Test Profile Configuration	
Test-profile name:	Test16_back-back-frames
Test packet size:	512,768
Theoretical max bandwidth:	4001
Test Configuration	
Test mode:	Initiate-and-Terminate
Duration in seconds:	10
Test family:	inet
Routing Instance Name:	default
INET family Configuration	
Egress Interface:	
Source ipv4 address:	20.1.46.2
Destination ipv4 address:	20.1.46.1
Source udp port:	31
Destination udp port:	32

Viewing Mean Opinion Score

Mean Opinion Score (MOS) is a metric used within the telecommunications industry to assess voice quality. The value range for the MOS metric is:

- 1 = bad
- 2 = poor
- 3 = fair
- 4 = good
- 5 = excellent

Typically, the MOS for Voice over IP is in the range of 3.5 to 4.2. The highest score that most codecs can achieve is in the range of 4.2 to 4.4 because even a perfect connection is affected by the compression algorithms of the codec.

Currently, the Junos Space Release 13.1P1 MOS is based on the E-model ITU-T G.107 Recommendation and implements a Latency test only.

Viewing the MOS

To obtain the MOS for an RFC2544 test:

1. In the OAM Insight panel, select **RFC2544 Test > Manage Test**.
2. In the **Manage Test** window, select the test for which you want to view the test results.
3. Select **Actions > View Test Result**.
4. In the **View RFC2544 Test** window, click the **Latency Test Summary Results** tab.

The MOS metric appears in the far right column of the results table.

View MOS Results									
Status: COMPLETED									
Packet Size	Theoretical rx	TX Packets	RX Packets	Latency MIN	Latency MAX	Latency AVG	Latency PROI	R-Factor	MOS
64	13586	2717200	2717200	17188	18776	18358	17826	75.1022	3.83
128	8012	1602400	1602400	21998	23272	22906	22620	75.1022	3.83
256	4401	880200	880200	26872	28575	27669	27328	75.1022	3.83

5. Click on the **View MOS Results** link in the status bar.

The **View MOS Results** window appears.

View MOS Results

Packetsize: 64

Parameter

Electric circuit noise:

-70

dBm0p

Noise floor:

-64

dBmp

Room noise(send):

35

dB(A)

Room noise(receive):

35

dB(A)

Send loudness rating:

8

dB

Receive loudness rating:

2

dB

Sidetone masking rating:

15

dB

D-factor(Receive):

3

Listener's sidetone rating:

18

dB

D-factor(Send):

3

Mean one-way delay:

0

ms

Absolute delay from (S) to (R):

0

ms

Round trip delay:

0

ms

Talker echo loudness rating:

65

dB

Weighted echo path loss:

110

dB

Quantizing distortion units:

1

dB

Equipment impairment factor:

0

Packet-loss robustness factor:

4.3

Packet-loss probability :

0

%

Burst ratio:

1

Advantage factor:

0

Results

Calculated R-Factor:

147.74033090894147

Calculate

Mean opinion score:

4.5

Reset

The following table provides the abbreviation, unit of measure, default value, and permitted value range for each parameter in the **View MOS Results** window.

Parameter	Abbreviation	Unit	Default Value	Value Range
Electric Circuit Noise		dBm0p		
Noise floor at the receive side	Nfor	dBmp	-64	–
Room noise at the send side	Ps	db(A)	35	35 through 85

Parameter	Abbreviation	Unit	Default Value	Value Range
Room noise at the receive side	Pr	dB(A)	35	35 through 85
Send loudness rating	SLR	dB	+8	0 through +18
Receive loudness rating	RLR	dB	+2	–5 though
Sidetone masking rating	STMR	dB	15	10 through 20
D-Value of telephone, receive side	Dr	–	3	–3 through +3
Listener sidetone rating	LSTR	dB	18	13 through 23
D-Value of telephone, send side	Ds	–	3	–3 through +3
Mean one-way delay of the echo path	T	ms	0	0 through 500
Absolute delay in echo-free connections	Ta	ms	0	0 through 500
Round-trip delay in a 4-wire loop	Tr	ms	0	0 through 1000
Talker echo loudness rating	TELRL	dB	65	5 through 65
Weighted echo path loss	WEPL	dB	110	5 through 110
Number of quantization distortion units	qdu	–	1	1 through 14
Equipment impairment factor	le	–	0	0 through 40
Packet-loss robustness factor	Bpl	–	4.3	4.3 through 40
Random packet-loss probability	Ppl	%	0	0 through 20
Burst ratio	BurstR		1	1 through 8
Advantage factor	A	–	0	0 through 20

Related Documentation • *Creating a Threshold Alarm Profile*

CHAPTER 5

Configuration Example

- [Configuring CFM on Physical Interfaces on page 67](#)

Configuring CFM on Physical Interfaces

This example provides an overview to help you effectively configure connectivity fault management (CFM) on a network of Juniper Networks MX Series 3D Universal Edge Routers.

- [Requirements on page 67](#)
- [Overview on page 67](#)
- [Configuration on page 69](#)
- [Verification on page 73](#)

Requirements

This example uses the following hardware and software components:

- Juniper Networks Junos Space OAM Insight Application
- Juniper Networks MX Series provider edge (PE) routers

Overview

Service provider networks are large and complex with a wide user base, and they often involve different operators that must work together to provide end-to-end services to enterprise customers. While enterprise end-customer demands continue to increase, so do the requirements for service provider Ethernet networks, particularly in the areas of availability and mean time to repair. The Operations, Administration, and Maintenance (OAM) addresses these challenges and more, thereby directly impacting the competitiveness of the service provider.

CFM partitions the service network into various administrative domains. For example, operators, providers, and customers may be part of different administrative domains. Each administrative domain is mapped into one maintenance domain providing enough information to perform its own management, thus avoiding security breaches and making end-to-end monitoring possible. Each maintenance domain is associated with a maintenance domain level from 0 through 7. Level allocation is based on the network hierarchy, where outermost domains are assigned a higher level than the innermost

domains. Customer end points have to highest maintenance domain level. In a CFM maintenance domain, each service instance is called a maintenance association. A maintenance association can be thought as a full mesh of maintenance endpoints (MEPs) having similar characteristics. MEPs are active CFM entities generating and responding to CFM protocol messages. There is also a maintenance intermediate point (MIP), which is a CFM entity similar to the MEP, but more passive (MIPs only respond to CFM messages).

MEPs can be up MEPs or down MEPs. A link can connect a MEP at level 5 to a MEP at level 7. The interface at level 5 is an up MEP (because the other end of the link is at MEP level 7) and the interface at level 7 is a down MEP (because the other end of the link is at MEP level 5).

In a Metro Ethernet network, CFM is commonly used at two levels:

- By the service provider to check the connectivity among its provider edge (PE) routers
- By the customer to check the connectivity among its customer edge (CE) routers

The major features of CFM are:

- Fault monitoring using the continuity check protocol. This is a neighbor discovery and health check protocol which discovers and maintains adjacencies at the VLAN or link level.
- Path discovery and fault verification using the linktrace protocol. Similar to IP traceroute, this protocol maps the path taken to a destination MAC address through one or more bridged networks between the source and destination.
- Fault isolation using the loopback protocol. Similar to IP ping, this protocol works with the continuity check protocol during troubleshooting.

The Junos Space OAM Insight application provides capabilities for automated end-to-end network management, monitoring, and troubleshooting. OAM provides a set of functions designed to monitor network operation to detect network faults and measure network performance.

The OAM Insight application supports service-based CFM provision, and performance measurements of Y.1731 standard frames on the network services. Following are the functionality of the Junos Space OAM Insight application:

- You can create a CFM service definition that you can use as a starting point for provisioning OAM Insight services. A CFM service is defined as the collection of maintenance end points (MEP), or maintenance intermediate points (MIP) in one maintenance association. A service definition provides a template upon which services are built. It specifies service attributes that are not specific to a service instance. These service definitions are capable of providing the basis for most of the service orders your organization will need to create. The OAM Insight provides a set of predefined service definitions. In case these predefined service definitions are not adequate for all your needs, you can create service definitions of your own.
- You can create a service order using the service definition. A service order is an instance of the service definition that completes the definition for a specific customer's use.

You can specify the domain, MEP and physical interfaces during the creation of service order.

- You can functional audit the service that you have deployed. A functional audit determines whether a deployed service instance is functioning.

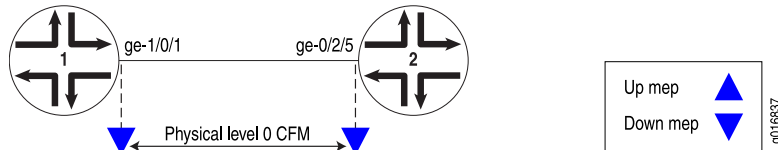
Topology

CFM can be used to monitor the physical link between two routers. CFM over physical interface are deployed in the OAM Insight application. In the OAM Insight application, you can attach an action profile and an SLA-iterator profile to the devices. Once the action profiles and the SLA-iterator profiles are provisioned in devices, they can be referenced in the remote MEP setting during the CFM deployment.

The CFM also supports aggregated Ethernet interfaces. On interfaces configured on Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs) on MX Series routers, CFM is not supported on untagged aggregated Ethernet member links. MPCs and MICs do support CFM on untagged and tagged aggregated Ethernet logical interfaces.

In the following example, two routers (Router 1 and Router 2) are connected by a point-to-point Gigabit Ethernet link. The link between these two routers is monitored using CFM. This is shown in [Figure 1 on page 69](#). The single boundary is a “down mep” in CFM terminology.

Figure 1: Ethernet CFM on Physical Interfaces



Configuration

To configure CFM on the physical interfaces, perform these tasks:

- [Choosing or Creating a Service Definition on page 71](#)
- [Creating and Deploying a CFM Service Order on page 72](#)

CLI Quick Configuration



NOTE: The configurations in this example are only partial examples of complete and functional router configurations. Do not copy these configurations and use them directly on an actual system.

Router 1 Configure the interface and CFM:

```
[edit]
interfaces ge-1/0/1 {
  unit 0 {
    family inet;
  }
}
```

```
protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        maintenance-domain private {
          level 0;
          maintenance-association private-ma {
            continuity-check {
              interval 1s;
            }
            mep 100 {
              interface ge-1/0/1;
              direction down;
              auto-discovery;
            }
          }
        }
      }
    }
  }
}
```

The configuration on Router 2 mirrors that on Router 1, with the exception of the *mep-id*.

Router 2 Configure the interface and CFM:

```
[edit]
interfaces ge-0/2/5 {
  unit 0 {
    family inet;
  }
}

protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        maintenance-domain private {
          level 0;
          maintenance-association private-ma {
            continuity-check {
              interval 1s;
            }
            mep 200 {
              interface ge-0/2/5;
              direction down;
              auto-discovery;
            }
          }
        }
      }
    }
  }
}
```

Choosing or Creating a Service Definition

Step-by-Step Procedure

A service definition provides a template upon which services are built. It specifies service attributes that are not specific to a service instance.

The OAM Insight software ships with standard service definitions. First, we check the standard service definitions to determine whether one already exists that will work.

To create a service definition:

1. In the OAM Insight task pane, select **OAM Design > Manage OAM Definitions > Create CFM Definition**
2. Enter the name of the service definition. For this example, enter **cfm-sd**
3. In **Type**, select **MEP**.
4. In **Domain Name**, specify the name as **DN1**.
5. In **Domain Level**, select **0**.
6. Select the **Remote MEP** check box.
7. Go to the **MA Settings** tab.
8. In **Hold interval**, specify the value as **1**.
9. In **Message interval**, select **1s**.
10. In **Loss threshold (PDUs)**, specify the value as **6**.
11. In **MEP ID Selection**:, select **Auto pick**.
12. In **Direction**, select **down**.
13. In **Priority**, select **1**.
14. Select the **Accept continuity check messages from all remote MEPs** check box.
15. In **Domain Level**, select **0**.
16. Go to the **Remote MEP settings** tab.
17. Select the **StdDef-ActionProfile** action profile.
18. Click the plus icon to add the table.
19. In **SLA profile**, select **StdDef-SFL**.
20. In the **Data TLV size** cell, specify the value as **1300**.
21. In the **Iteration Count** cell, specify the value as **14590**.
22. In the **Priority** cell, specify the value as **4**.
23. Click **Create**. The **Manage OAM Definitions** page includes the new service definition. You have created a customized Service Definition, but it has not yet been published. Before a service definition can be used in provisioning, it must be published.

24. To publish the service definition, in the **Manage Service Definitions** page, select the service definition; then in the **Actions** menu, select **Publish Service Definition**. The **Publish Service Definition** window appears.
25. To confirm that you want to publish this service definition, click **Publish**. In the **Manage OAM Definitions** page, the symbol in the upper left corner of the service definition thumbnail changes to a check mark, indicating that the status has changed to **Published**.

The service definition is now ready for use in provisioning.

Creating and Deploying a CFM Service Order

Step-by-Step Procedure

Now that you have created a suitable service definition you are ready to create and deploy a service order. To create and deploy a service order:

1. In the OAM Insight task pane, select **OAM Provisioning > Manage OAM Orders > Create CFM Service Order**
2. In **Service definition**, select **cfm-sd**.
3. In **Name**, specify the name of the service order as **cfm-so**.
4. Select the end point devices.
5. Click **Next**. The **Common Settings** page appears.
6. In **Hold interval**, specify the value as **1**.
7. In **Message interval**, select **1s**.
8. In **Loss threshold (PDUs)**, specify the value as **6**.
9. In **MEP ID Selection**., select **Auto pick**.
10. In **Direction**, select **down**.
11. In **Priority**, select **1**.
12. Select the **Accept continuity check messages from all remote MEPs** check box.
13. To configure the first device (PE1), select a device in the left pane.
14. In **CFM Interface**, select **ge-1/0/1**.
15. Specify the **MEP** value as **100**.
16. To configure the second device (PE1), select a device in the left pane.
17. In **CFM Interface**, select **ge-0/2/5**.
18. Specify the **MEP** value as **200**.
19. Click **Create**.
20. In the **Deployment Options** window, select **Deploy now**.
21. Click **OK** to start the deployment.
22. To monitor the progress and status of the deployment, in the **Order Information** window, click the job ID. The **Job Management** page shows the status of the job.

23. When you see in the **Job Management** window that the deployment is successful, in the task pane, select the **Service Provisioning** workspace again.
24. In the OAM Insight task pane, select **Manage Services**.
The **Manage Services** page shows the new service.

Verification

Performing a Functional Audit and a Configuration Audit

Purpose Now that your new service is deployed, you should validate its configuration and functional integrity. A functional audit runs operational commands on the device to verify that the service is up or down. A configuration audit verifies whether the configuration that was pushed to the device during deployment is actually on the device.

Action To perform a configuration audit and a functional audit of the service:

1. In the **Manage Services** page, select the service instance you just deployed.
2. Right-click on the service instance or open the **Actions** menu to see the list of available tasks and select **Perform Functional Audit**.
3. In the **Schedule Functional Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, then click **OK**.
4. In the **Order Information** window, click **OK**.
5. Right-click on the service instance or open the **Actions** menu to see the list of available tasks and select **Perform Configuration Audit**.
6. In the **Schedule Configuration Audit** window, you can choose to perform the audit now or schedule it for later. Select **Audit now**, and then click **OK**.
7. In the **Order Information** window, click **OK**.
When the audit jobs have finished, success is indicated by an up arrow in the top right corner of the service thumbnail.
8. To view the functional audit results:
 - a. In the **Manage Services** page, select the **cfm-so** service instance.
 - b. Open the **Actions** menu and select **View Functional Audit Results**.
 - c. In the **Functional Audit Results** window, select each device to view the results.
9. To view the results of the configuration audit:
 - a. Open the **Actions** menu and select **View Configuration Audit Results**.
 - b. In the **Configuration Audit Results** window, select each device in turn and review the results. This report indicates any part of the service configuration that is missing on the device, or is inconsistent with the Junos Space database.

Following successful audit, the service is deployed and ready to be used.

**Related
Documentation**

- [Junos Space OAM Insight Overview on page 3](#)
- [Creating CFM Profiles on page 31](#)
- [Creating and Managing CFM Service Orders on page 41](#)
- [Performing a Functional Audit on page 106](#)
- [Viewing Functional Audit Results on page 107](#)

PART 3

Administration

- [Managing OAM Service Definitions on page 77](#)
- [Managing OAM Service Orders on page 81](#)
- [Managing Action Profiles on page 85](#)
- [Managing SLA Iterator Profiles on page 89](#)
- [Managing OAM Services on page 93](#)

CHAPTER 6

Managing OAM Service Definitions

- [Managing CFM Profiles on page 77](#)
- [Publishing a CFM Service Definition on page 78](#)
- [Unpublishing a CFM Service Definition on page 79](#)
- [Deleting a CFM Service Definition on page 79](#)

Managing CFM Profiles

The Manage OAM Definitions inventory page displays the definitions you created to configure OAMs (Operation, Administration, and Maintenance). The CFM profiles are sorted by name.

Viewing CFM Profiles—The Manage OAM Profiles inventory page provides two views: thumbnail (default) and tabular. Click the view icons at the right of the page name to toggle between the views.

View	Field Description
Thumbnail	<p>The thumbnail view displays CFM definitions graphically by a CFM definition icon and name.</p> <p>The CFM definition icon indicates the CFM order state: published or unpublished.</p>
Tabular	<p>The tabular view displays CFM definition information in a table by definition name, description, state, and creation date.</p> <p>The State column indicates the CFM definition state.</p>

You can use the search text box to filter the CFM profiles by name or by tag names that you create. When you start to type a name in the search box, it automatically completes the name.

Viewing CFM Profile Details—Double-click a CFM profile to view more detailed information. The CFM Profile Details page appears. See [“Creating CFM Profiles” on page 31](#) for CFM profile configuration information.

The Manage OAM Definitions inventory page includes the following actions:

- **Publish a CFM Definition**—See [“Publishing a CFM Service Definition” on page 78](#)
- **Unpublish a CFM Definition**—See [“Unpublishing a CFM Service Definition” on page 79](#)
- **Delete a CFM Definition**—See [“Deleting a CFM Service Definition” on page 79](#)
- **Tag It**—See *Tagging an Object*
- **View Tags**—See *Managing Tags*
- **Untag It**—See *Untagging Objects*

**Related
Documentation**

- [Managing CFM Service Orders on page 81](#)
- [Managing CFM Action Profiles on page 85](#)
- [Managing SLA-Iterator on page 89](#)
- [Managing CFM Services on page 93](#)

Publishing a CFM Service Definition

To publish a CFM definition:

1. Select **OAM Design > Manage OAM Definition**.

The **Manage OAM Definition** inventory page appears.

2. Select the CFM definition that you want to publish.
3. Right-click the CFM definition and select **Publish Service Definition**.

You can also open the **Actions** menu and select **Publish Service Definition**.

The **Publish Service Definition** dialog box appears.

1. Select the CFM definition.
2. Click **Publish**.

The state of the CFM definition changes from unpublished to published.

You see the CFM definition state indicator change on the **OAM Design > Manage OAM Definitions** inventory page.

**Related
Documentation**

- [Creating CFM Profiles on page 31](#)
- [Unpublishing a CFM Service Definition on page 79](#)
- [Deleting a CFM Service Definition on page 79](#)

Unpublishing a CFM Service Definition

Unpublishing places a CFM definition in a state so that you can review or modify it to create a CFM service order.

You can view the service order state in the **Manage OAM Definitions** inventory page in both thumbnail and tabular views.

From the **OAM Design statistics** page, you can view the percentage of unpublished CFM definitions in the **Service Definition States** pie chart. Click the segment of unpublished CFM definition to view them in the **Manage OAM Definitions** inventory page.

To unpublish a CFM definition:

1. Select **OAM Design > Manage OAM Definitions**.
The **Manage OAM Definitions** inventory page appears.
2. Select the OAM Insight definition that you want to unpublish.
3. Right-click the OAM Insight definition and select **Unpublish Service Definition**.

You can also open the **Actions** menu and select **Unpublish Service Definition**.

The **Unpublish Service Definition** dialog box appears.

1. Select the OAM Insight definition.
2. Click **Unpublish**.

The state of the CFM definition changes from published to unpublished.

You see the CFM definition state indicator change on the **OAM Design > Manage OAM Definitions** inventory page.

Related Documentation

- [Creating CFM Profiles on page 31](#)
- [Publishing a CFM Service Definition on page 78](#)
- [Deleting a CFM Service Definition on page 79](#)

Deleting a CFM Service Definition

If a CFM definition is being used by a CFM service order, you cannot delete it.

To delete a CFM definition:

1. Select **OAM Design > Manage OAM Definitions**.
The **Manage OAM Definitions** inventory page appears.
2. Select the OAM Insight definition you want to delete.
3. Either right-click the selected CFM definition and select **Delete Service Definition**, or open the **Actions** menu and select it.

The **Delete Service Definition** dialog box appears.

4. Select the CFM Definition.

The **Manage OAM Definitions** page appears, displaying any remaining definitions.

5. Click **Delete**.

The CFM Definition is removed from the database.



NOTE: Only published CFM definitions can be deleted.

**Related
Documentation**

- [Creating CFM Profiles on page 31](#)
- [Publishing a CFM Service Definition on page 78](#)
- [Unpublishing a CFM Service Definition on page 79](#)

CHAPTER 7

Managing OAM Service Orders

- [Managing CFM Service Orders on page 81](#)
- [Deleting a CFM Partial Configuration on page 82](#)
- [Viewing the Configuration of a Pending Service Order on page 83](#)
- [Deleting a CFM Service Order on page 84](#)

Managing CFM Service Orders

The Manage OAM Service Order inventory page displays the orders you created to configure OAM (Operation, Administration, and Maintenance). The CFM service orders are sorted by name.

Viewing CFM Service Order—The Managing OAM Service Order inventory page provides two views: thumbnail (default) and tabular. Click the view icons at the right of the page name to toggle between the views.

View	Field Description
Thumbnail	<p>The thumbnail view displays CFM service orders graphically by a CFM service order icon and name.</p> <p>The CFM service order icon indicates the CFM order state: published or unpublished.</p>
Tabular	<p>The tabular view displays CFM service order information in a table by service order name, description, state, and creation date.</p> <p>The State column indicates the CFM service order state.</p>

You can use the search text box to filter the CFM service order by name or by tag names that you create. When you start to type a name in the search box, it automatically completes the name.

Viewing CFM Service Order Details—Double-click a CFM service order to view more detailed information. The CFM Service Order Details page appears. See [“Creating and Managing CFM Service Orders” on page 41](#) for CFM order configuration information.

The Managing Service Order inventory page includes the following actions:

- **Deploy CFM Service Order**—See [“Deploying a CFM Service Order” on page 45](#)
- **Validate CFM Service Order**—See [“Validating a CFM Service Order” on page 46](#)
- **Delete Partial Configuration**—See [“Deleting a CFM Partial Configuration” on page 82](#)
- **Delete CFM Service Order**—See [“Deleting a CFM Service Order” on page 84](#)
- **Tag It**—See *Tagging an Object*
- **View Tags**—See *Managing Tags*
- **Untag It**—See *Untagging Objects*

**Related
Documentation**

- [Managing CFM Profiles on page 77](#)
- [Managing CFM Action Profiles on page 85](#)
- [Managing SLA-Iterator on page 89](#)
- [Managing CFM Services on page 93](#)

Deleting a CFM Partial Configuration

A failed service order of type Provisioning can leave parts of the service configuration on the devices. To remove this partial configuration:

1. In the OAM Insight task pane, select **OAM Provisioning > Manage OAM Service Orders**.
2. In the **Manage OAM Service Orders** page, select the failed service order for which you want to delete the partial configuration.
3. Open the **Actions** menu and select **Delete Partial Configuration**.
4. In the confirmation window, select **Delete**.

**Related
Documentation**

- [Creating and Managing CFM Service Orders on page 41](#)
- [Validating a CFM Service Order on page 46](#)
- [Deploying a CFM Service Order on page 45](#)
- [Deleting a CFM Service Order on page 84](#)

Viewing the Configuration of a Pending Service Order

You can view the configuration of a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state.

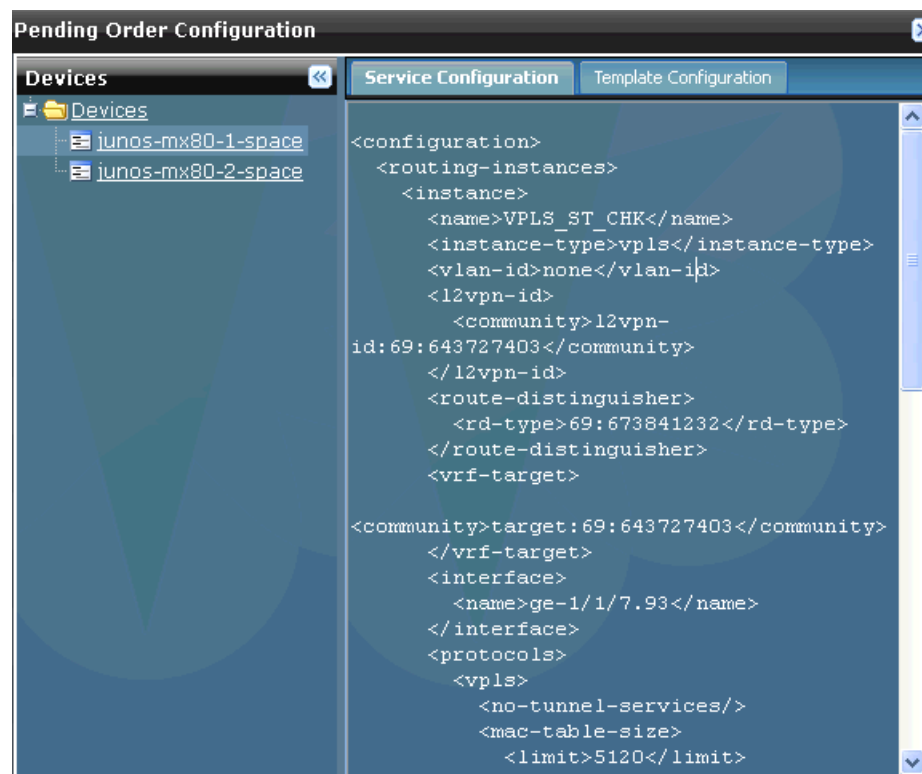
To view the configuration of such service orders:

1. In the Network Activate, select **Service Provisioning > Manage Service Orders**. A list of service orders is displayed.
2. Select a service order that is in either of the following states:
 - Requested
 - Invalid
 - Scheduled
 - Failed deployment



NOTE: The Order State column displays the state of the service order.

3. Right-click the service order and select the **View Pending Order Configuration**. The Pending Order Configuration window is displayed. The configuration is displayed in xml format.





NOTE: The View Pending Order Configuration appears to be dimmed if the service order state is Completed.

4. Select a device to view the configuration details. You can also view the template configuration if a template is attached to the service order.

Based on the application's settings, the configuration is displayed in xml format or in set format. To view the configuration in set format:

1. Select **Platform > Administration > Manage Applications > Network Activate**.
2. Right-click the Network Activate application and select **Modify Application Settings**. The Modify Network Activate Settings window is displayed.
3. Select the **show configuration in set format** check box.

**Related
Documentation**

- [Managing CFM Service Orders on page 81](#)
- [Deleting a CFM Partial Configuration on page 82](#)
- [Deleting a CFM Service Order on page 84](#)

Deleting a CFM Service Order

You can delete a service order that is in the requested state, the scheduled state, the invalid state, or the failed deployment state. To correct a service order in the invalid state, you must delete it and then recreate it; the OAM Insight software does not support modifying the service order directly.

To delete a CFM service order from the database:

1. In the OAM Insight task pane, select **OAM Provisioning > Manage OAM Orders**.
2. In the **Manage OAM Service Orders** inventory page, select the service order you want to delete.
3. Open the **Actions** menu and select **Delete Service Order**.

A window appears requesting confirmation.

4. Click **Delete**.

The **Manage OAM Service Orders** inventory page reappears with the deleted service orders removed.

**Related
Documentation**

- [Creating and Managing CFM Service Orders on page 41](#)
- [Validating a CFM Service Order on page 46](#)
- [Deploying a CFM Service Order on page 45](#)
- [Deleting a CFM Partial Configuration on page 82](#)

CHAPTER 8

Managing Action Profiles

- [Managing CFM Action Profiles on page 85](#)
- [Publishing an Action Profile on page 86](#)
- [Unpublishing an Action Profile on page 87](#)
- [Deleting an Action Profile on page 87](#)

Managing CFM Action Profiles

The Manage Action Profiles inventory page displays the action profiles you created to configure OAMs (Operation, Administration, and Maintenance). The CFM action profiles are sorted by name.

Viewing CFM Action Profile—The Manage Action Profiles inventory page provides two views: thumbnail (default) and tabular. Click the view icons at the right of the page name to toggle between the views.

View	Field Description
Thumbnail	<p>The thumbnail view displays CFM action profile graphically by a CFM action profile icon and name.</p> <p>The action profile icon indicates the CFM action profile state: published or unpublished.</p>
Tabular	<p>The tabular view displays CFM action profiles information in a table by definition name, description, state, and creation date.</p> <p>The State column indicates the action profile state.</p>

You can use the search text box to filter the action profiles by name or by tag names that you create. When you start to type a name in the search box, it automatically completes the name.

Viewing CFM Action Profile Details—Double-click an action profile to view more detailed information. The Action Profile Details page appears. See [“Creating and Viewing CFM Action Profiles” on page 24](#) for CFM action profile configuration information.

The Manage Action Profiles inventory page includes the following actions:

- **Publish CFM Action Profiles**—See [“Publishing an Action Profile” on page 86](#)
- **Unpublish CFM Action Profiles**—See [“Unpublishing an Action Profile” on page 87](#)
- **Delete CFM Action Profiles**—See [“Deleting an Action Profile” on page 87](#)
- **Tag It**—See *Tagging an Object*
- **View Tags**—See *Managing Tags*
- **Untag It**—See *Untagging Objects*

**Related
Documentation**

- [Managing CFM Profiles on page 77](#)
- [Managing CFM Service Orders on page 81](#)
- [Managing SLA-Iterator on page 89](#)
- [Managing CFM Services on page 93](#)

Publishing an Action Profile

To publish a CFM action profile:

1. Select **OAM Design > Manage Action profiles**.

The **Manage Action Profiles** inventory page appears.

2. Select the action profile that you want to publish.
3. Right-click the action profile and select **Publish Action profile**.

You can also open the **Actions** menu and select **Publish Action profile**.

The **Publish Action profile** dialog box appears.

1. Select an action profile.
2. Click **Publish**.

The state of the action profile changes from unpublished to published.

You see the action profile state indicator change on the **OAM Design > Manage Action Profiles** inventory page.

**Related
Documentation**

- [Creating and Viewing CFM Action Profiles on page 24](#)
- [Unpublishing an Action Profile on page 87](#)
- [Deleting an Action Profile on page 87](#)

Unpublishing an Action Profile

To unpublish a CFM action profile:

1. Select **OAM Design > Manage Action Profiles**.
The **Manage Action Profiles** inventory page appears.
2. Select an action profile that you want to unpublish.
3. Right-click the action profile and select **Unpublish Action profile**.

You can also open the **Actions** menu and select **Unpublish Action profile**.

The **Unpublish Action profile** dialog box appears.

1. Select an action profile.
2. Click **Unpublish**.

The state of the action profile changes from published to unpublished.

You see the action profile state indicator change on the **OAM Design > Manage Action Profiles** inventory page.

Related Documentation

- [Creating and Viewing CFM Action Profiles on page 24](#)
- [Publishing an Action Profile on page 86](#)
- [Deleting an Action Profile on page 87](#)

Deleting an Action Profile

To delete a CFM action profile:

1. Select **OAM Design > Manage Action Profiles**.
The **Manage Action Profiles** inventory page appears.
2. Select the CFM action profile you want to delete.
3. Either right-click the selected CFM action profile and select **Delete Action profile**, or mouse over the **Actions** drawer and select it.

The **Delete Action profile** dialog box appears.

4. Select the action profile.

The **Manage Action Profiles** page appears, displaying any remaining CFM action profiles.

5. Click **Delete**.

The action profile is removed from the database.



NOTE: Only published action profile can be deleted.

**Related
Documentation**

- [Creating and Viewing CFM Action Profiles on page 24](#)
- [Publishing an Action Profile on page 86](#)
- [Unpublishing an Action Profile on page 87](#)

CHAPTER 9

Managing SLA Iterator Profiles

- [Managing SLA-Iterator on page 89](#)
- [Publishing an SLA-Iterator Profile on page 90](#)
- [Unpublishing an SLA-Iterator Profile on page 90](#)
- [Deleting an SLA-Iterator Profile on page 91](#)

Managing SLA-Iterator

The Manage SLA-iterator profile inventory page displays the SLA-iterator profile you created to configure OAM (Operation, Administration, and Maintenance). The SLA-iterator profiles are sorted by name.

Viewing SLA-iterator profiles—The Manage SLA-iterator profiles inventory page provides only the tabular view. The tabular view displays SLA-iterator profiles information in a table by SLA-iterator profile name, description, state, and creation date. The State column indicates the SLA-iterator profiles state.

You can use the search text box to filter the SLA-iterator profiles by name or by tag names that you create. When you start to type a name in the search box, it automatically completes the name.

Viewing SLA-iterator profile Details—Double-click an SLA-iterator profiles to view more detailed information. The SLA-iterator Profile Details page appears. See [“Creating and Viewing SLA-Iterator Profiles” on page 29](#) for SLA-iterator profile configuration information.

The Manage SLA Iterator Profiles inventory page includes the following actions:

- **Publish SLA-iterator profiles**—See [“Publishing an SLA-Iterator Profile” on page 90](#)
- **Unpublish SLA-iterator profiles**—See [“Unpublishing an SLA-Iterator Profile” on page 90](#)
- **Delete SLA-iterator profiles**—See [“Deleting an SLA-Iterator Profile” on page 91](#)
- **Tag It**—See *Tagging an Object*
- **View Tags**—See *Managing Tags*
- **Untag It**—See *Untagging Objects*

- Related Documentation**
- [Managing CFM Profiles on page 77](#)
 - [Managing CFM Service Orders on page 81](#)
 - [Managing CFM Action Profiles on page 85](#)
 - [Managing CFM Services on page 93](#)

Publishing an SLA-Iterator Profile

To publish an SLA-Iterator profile:

1. Select **OAM Design > SLA Iterator Profile**.
The **Manage SLA Iterator Profiles** inventory page appears.
2. Select the SLA-Iterator profile that you want to publish.
3. Right-click the SLA-Iterator profile and select **Publish SLA-Iterator Profile**.

You can also open the **Actions** menu and select **Publish SLA-Iterator Profile**.

The **Publish SLA-Iterator Profile** dialog box appears.

1. Select the SLA-Iterator profile.
2. Click **Publish**.

The state of the SLA-Iterator profile changes from unpublished to published.

You see the SLA-Iterator profile state indicator change on the **OAM Design > Manage SLA Iterator Profiles** inventory page.

- Related Documentation**
- [Creating and Viewing SLA-Iterator Profiles on page 29](#)
 - [Unpublishing an SLA-Iterator Profile on page 90](#)
 - [Deleting an SLA-Iterator Profile on page 91](#)

Unpublishing an SLA-Iterator Profile

To unpublish an SLA-Iterator profile:

1. Select **OAM Design > SLA Iterator Profile**.
The **Manage SLA Iterator Profiles** inventory page appears.
2. Select the SLA-Iterator profile that you want to unpublish.
3. Right-click the SLA-Iterator and select **Unpublish SLA Iterator Profile**.

You can also open the **Actions** menu and select **Unpublish SLA Iterator Profile**.

The **Unpublish SLA Iterator Profile** dialog box appears.

1. Select the SLA-Iterator profile.

2. Click **Unpublish**.

The state of the SLA-Iterator profile changes from published to unpublished.

You see the SLA-Iterator profile state indicator change on the **OAM Design > Manage SLA Iterator Profiles** inventory page.

**Related
Documentation**

- [Creating and Viewing SLA-Iterator Profiles on page 29](#)
- [Publishing an SLA-Iterator Profile on page 90](#)
- [Deleting an SLA-Iterator Profile on page 91](#)

Deleting an SLA-Iterator Profile

To delete an SLA-Iterator profile:

1. Select **OAM Design > SLA Iterator Profile**.

The **Manage SLA Iterator Profile** inventory page appears.

2. Select the SLA-Iterator profile you want to delete.

3. Either right-click the selected SLA-Iterator profile and select **Delete SLA-Iterator Profile**, or open the **Actions** menu and select it.

The **Delete SLA Iterator Profile** dialog box appears.

4. Select the SLA-Iterator profile.

The **Manage Service Templates** page appears, displaying any remaining templates.

5. Click **Delete**.

The SLA-Iterator profile is removed from the database.



NOTE: Only published SLA-Iterator profile can be deleted.

**Related
Documentation**

- [Creating and Viewing SLA-Iterator Profiles on page 29](#)
- [Publishing an SLA-Iterator Profile on page 90](#)
- [Unpublishing an SLA-Iterator Profile on page 90](#)

CHAPTER 10

Managing OAM Services

- [Managing CFM Services on page 93](#)
- [Viewing Provisioned CFM Services on page 94](#)
- [Decommissioning a CFM Service on page 95](#)
- [Modifying a CFM Service on page 95](#)
- [Viewing Service Alarms in OAM Insight on page 96](#)

Managing CFM Services

The **Manage OAM Services** inventory page lists CFM services that have been deployed for customers.

Viewing CFM Services—The **Manage OAM Services** inventory page displays a table that presents CFM order information in columns that indicate the definition name, state, description, and creation date.

The search text box enables you to filter the OAM services by name or by tag names that you create. When you start to type a name, the search automatically finishes the name.

Viewing CFM Service Details—Double-click a CFM service to view more detailed information. The **CFM Service Details** page appears.

CFM Service Actions

The **Manage OAM Services** inventory page includes the following actions:

- **Decommission OAM Service**—See [“Decommissioning a CFM Service” on page 95](#)
- **Modify Service**—See [“Modifying a CFM Service” on page 95](#)
- **View Service Alarms**—See [“Viewing Service Alarms in OAM Insight” on page 96](#)
- **Tag It**—See *Tagging an Object*
- **View Tags**—See *Managing Tags*
- **Untag It**—See *Untagging Objects*

Related Documentation

- [Managing CFM Profiles on page 77](#)
- [Managing CFM Service Orders on page 81](#)

- [Managing CFM Action Profiles on page 85](#)
- [Managing SLA-Iterator on page 89](#)

Viewing Provisioned CFM Services

After you have created and deployed OAM Insight services, you can display the services available for management.

Select **OAM Insight > OAM Provisioning > Manage OAM Services**.

From the **Manage OAM Services** page, you can select any service and perform any of the functions available in the **Actions** menu.

The **Manage OAM Services** page displays the following CFM service information:

Column	Description
Name	Name of the CFM service.
Description	Description of the CFM service.
State	Indicates the CFM service state..
FA Status	Functional Audit status of the CFM service: <ul style="list-style-type: none"> • Up—Service passed functional audit • Down—Service failed functional audit • Pending—Service is deployed but a functional audit has not yet been performed, or the service has been modified since the last functional audit was performed.
Fault status	The current status of a service. <ul style="list-style-type: none"> • Down—Service is down • Up—Service is up • None—No status updated
Definition	Name of the definition attached to the CFM service.
Activation Date	The activation date of the CFM service.
Last Modified Date	The last modified date of the CFM service.

Related Documentation

- [Creating and Managing CFM Service Orders on page 41](#)
- [Deploying a CFM Service Order on page 45](#)
- [Decommissioning a CFM Service on page 95](#)

Decommissioning a CFM Service

You can decommission a service that a customer no longer needs.

You cannot decommission a service if it is in the Requested state.

To decommission a service:

1. Select the service you want to decommission.
2. Right-click the service and select **Decommission OAM Service**.
3. Do one of the following:
 - To decommission the service immediately, select **Decommission now**, and click **OK**.
In the Order Information window, click the job ID of the decommission job.
 - To deploy the service at a later time, select **Decommission later**, select a date and time to perform the operation, then click **OK**.

Related Documentation

- [Creating and Managing CFM Service Orders on page 41](#)
- [Deploying a CFM Service Order on page 45](#)
- [Viewing Provisioned CFM Services on page 94](#)

Modifying a CFM Service

You can modify the following entities of an OAM Insight service:

- MEP settings
- Remote MEP settings

After modifying a service, the configuration audit and functional audit information is cleared and the functional audit status is set to pending.

To modify the attributes of a service:

1. In the OAM Insight task pane, select **OAM Provisioning > Manage OAM Services**.
2. In the **Manage OAM Services** page, select the service you want to modify.
3. Open the **Actions** menu and select **Modify Service**.

A graphical image of the service appears, showing the general settings, the **MEP Settings** tab, and the **Remote MEP Settings** tab. The **General Settings** box contains a unique name for the service order that you want to modify.

4. Add or remove remote MEP to an existing MEP, if desired.
5. Click **Modify**.

The OAM Insight software modifies the service.

6. Use the Jobs workspace to check for successful completion of the action.

**Related
Documentation**

- [Creating and Managing CFM Service Orders on page 41](#)
- [Deploying a CFM Service Order on page 45](#)
- [Decommissioning a CFM Service on page 95](#)

Viewing Service Alarms in OAM Insight

The Junos Space Network Application Platform has integrated a third party tool, OpenNMS, to provide network monitoring capabilities. The OpenNMS network management application platform provides solutions for enterprises and carriers. OpenNMS is installed as part of Platform, which exposes some of OpenNMS' functionality through the Network Monitoring workspace. The default performance management configuration of OpenNMS for Space supports generic counters, CPU, memory, temperature, and Mobility counters. For information on this default configuration, see the subset of the OpenNMS documentation included in this Junos Space Network Application Platform User Guide.



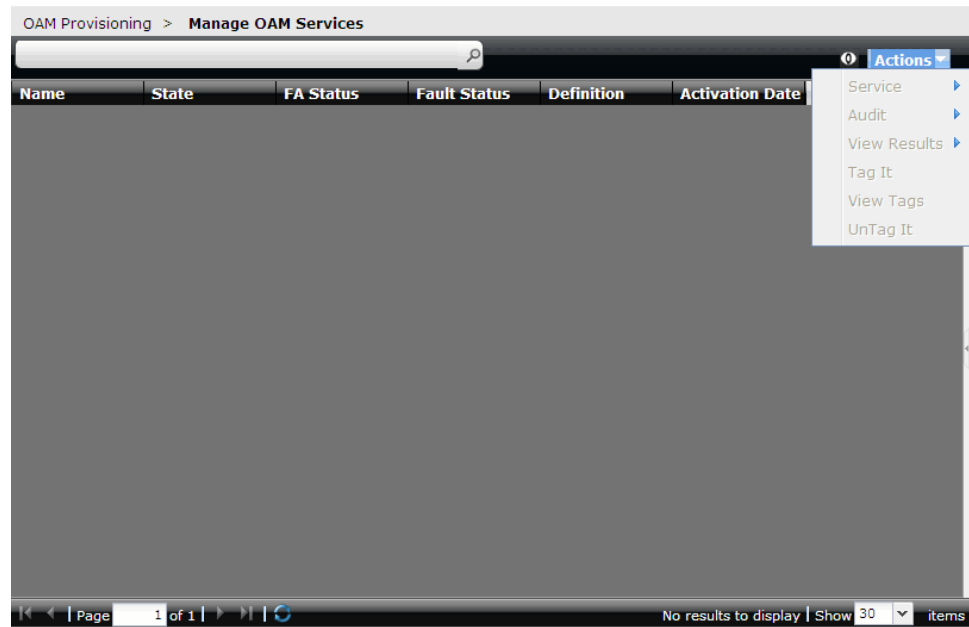
.....

CAUTION: Although additional OpenNMS functionality can be accessed by customizing its XML files, editing these files can affect the functionality of the Network Monitoring workspace. Juniper Networks does not support changes to OpenNMS.

.....

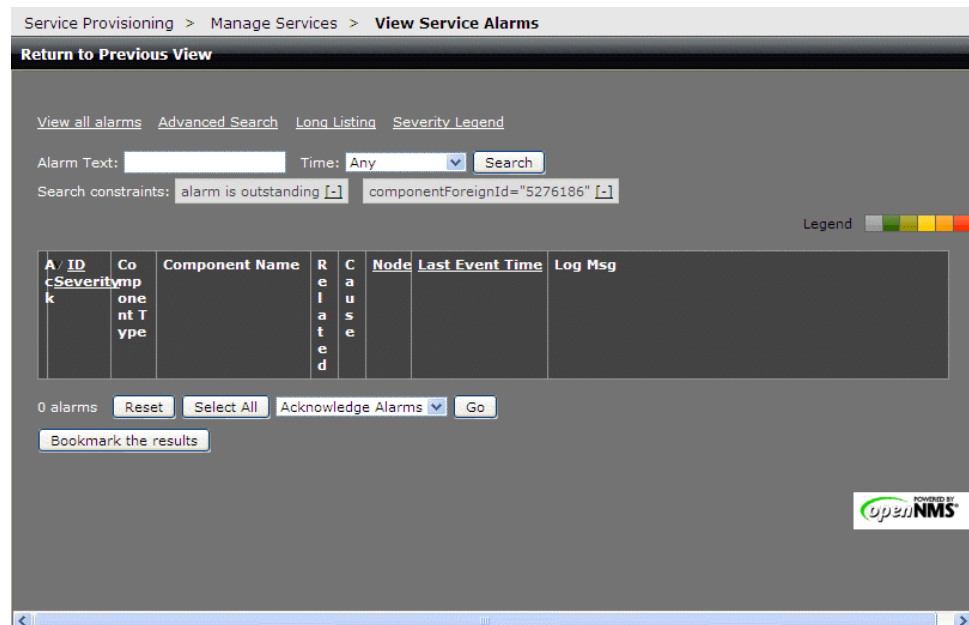
To access the OpenNMS tool in OAM Insight, select **OAM Insight > OAM Provisioning > Manage OAM Services**.

1. When the service inventory window appears, select the entry for the service you want to look at.
2. Right click to display the **Actions** menu.
3. Select **View Service Alarms**.



4. From the **Actions** menu, select **View Service Alarms**.

The OpenNMS **Network Monitoring** window appears.



From this window you can view the alarms associated with the service and search for specific alarms.

For descriptions of the SNMP traps, refer to the Junos OS SNMP MIBs and Traps Reference.

For guidelines on using the OpenNMS interface and services, refer to the Junos Space Network Monitoring reference.

- Related Documentation**
- [Managing CFM Services on page 93](#)
 - [SNMP MIBs and Traps Reference](#)
 - [Junos Space Network Monitoring Reference](#)

PART 4

Troubleshooting

- [Configuration Audit on page 101](#)
- [Functional Audit on page 105](#)

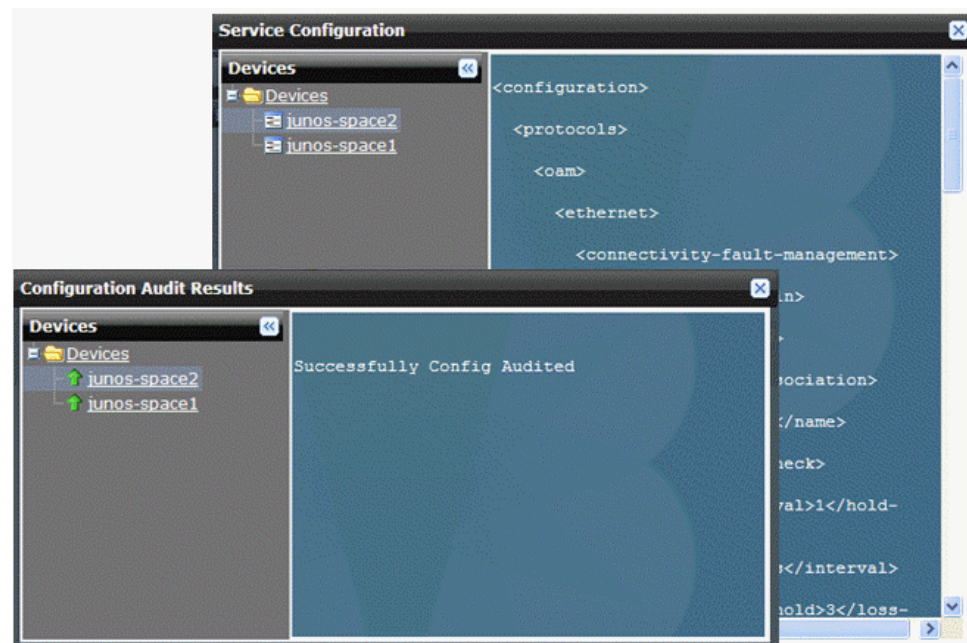
CHAPTER 11

Configuration Audit

- [Performing a Configuration Audit on page 101](#)
- [Viewing Configuration Audit Results on page 103](#)

Performing a Configuration Audit

A configuration audit can help you determine whether the service configuration on the device has been changed out of band. If so, you might need to synchronize the device with the Junos Space database. To this end, you can compare the results of a configuration audit with the service configuration in the Junos Space database. The following example shows a sample comparison:



To perform a configuration audit:

1. In the OAM Insight task pane, select **OAM Provisioning > Manage OAM Services**.
2. In the **Manage OAM Services** inventory page, select the service you want to investigate.
3. Open the **Actions** menu and select **Perform Configuration Audit**.

4. In the **Schedule Configuration Audit** window, either:

- Select **Audit Now**, then click **OK**.

An **Audit Information** window appears, providing a link to details about the audit in the Jobs workspace, and an **OK** button.

- Select **Audit Later**, enter a date and time, then click **OK**.

5. Monitor the progress of an audit.

- To monitor the progress of an audit after selecting Audit Now, click the Job ID in the **Audit Information** window.

The **Job Management** page shows information about the functional audit job. The **State** field indicates whether the service passed or failed the audit. If the service failed the audit, then the **Summary** field provides information about the failure.

- To monitor the progress of an audit after selecting Audit Later, after the scheduled time of the audit:
 - a. In the task pane, select the **Jobs**.
 - b. In the **Job Types** window, select the **Configuration Audit** segment of the pie chart.
 - c. Select the configuration audit of interest from the inventory list.

Summary information about the audit appears in the quick look panel.

- d. In the filter bar, select the table view icon to see additional information about the job. If the service failed the audit, information about the failure appears in the **Summary** field.

6. In the **Audit Information** window, click the job ID of the configuration audit.

The **Job Management** window appears and shows a filtered view of the job inventory, showing only the configuration audit job.



NOTE: If a resynchronization between a device and the Junos Space database is ongoing when the configuration audit job starts, the configuration audit job is suspended until the resynchronization job finishes. If the resynchronization job fails to complete, the audit can be suspended indefinitely. To allow the audit to proceed, go to the **Job Management** workspace and cancel the resynchronization job, as described in *Canceling a Job*.

7. In the **State** column, check the status of the audit to determine whether it succeeded or failed.

Check the **Summary** column, which contains useful service information such as the VC ID and endpoint information. For some failed deployments, this column also contains information about why the deployment failed.

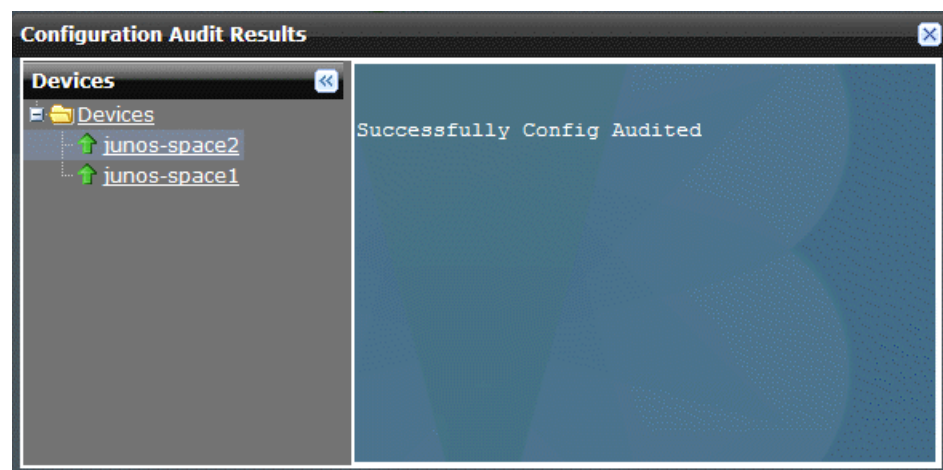
For details about using the Job manager, see *Viewing Jobs* in the *Junos Space Network Application Platform User Guide*.

- Related Documentation**
- [Viewing Configuration Audit Results on page 103](#)
 - [Performing a Functional Audit on page 106](#)
 - [Viewing Functional Audit Results on page 107](#)

Viewing Configuration Audit Results

After performing a configuration audit, check the detailed results of the audit by comparing information in the Configuration Audit Results window with the information in the Service Configuration window:

1. Display the configuration audit results.
 - a. In the OAM Insight task ribbon, select **OAM Service Provisioning > Manage OAM Services**.
 - b. In the **Manage Services** inventory page, select the service you are investigating.
 - c. Either open the **Actions** menu and select **View Configuration Audit Results**, or select that command from the right mouse-click menu.



- d. Examine the audit results for missing configuration information, and keep the window open for later comparison with the service configuration in the Junos Space database.

You can validate policies for the hub and spoke (1 interface).

2. Display the service configuration in the Junos Space database.
 - a. Double-click the service icon in the **Manage Services** inventory page.
 - b. In the **Actions** menu, select **View Service Configuration**.

A new window opens and shows the service configuration.



3. Compare the contents of the **Service Configuration** window with those of the **Configuration Audit Results** window for each device in turn.

If you see discrepancies, then the service configuration was probably modified out-of-band. If so, you might need to synchronize the device with the Junos Space database.

For step-by-step instructions about synchronizing devices, see *Resynchronizing Managed Devices with the Network* for details.

Related Documentation

- [Performing a Configuration Audit on page 101](#)
- [Performing a Functional Audit on page 106](#)
- [Viewing Functional Audit Results on page 107](#)

CHAPTER 12

Functional Audit

- [Performing a Functional Audit on page 106](#)
- [Viewing Functional Audit Results on page 107](#)

Performing a Functional Audit

A functional audit determines whether a deployed service instance is functioning. The functional audit checks the control plane to ensure connectivity among endpoints and that the UNIs are functioning correctly. It also checks the data plane to verify packet transmission between each valid pair of endpoints in the service.

A functional audit works by running commands that perform verification and reporting relevant information.

The following table shows the commands that are used for each service type:

Service Type	XML Command	CLI Command
	Control Plane	Control Plane
CFM	<pre><get-cfm-mep-database> <maintenance-domain> instanceMaintenanceDomain </maintenance-domain> <maintenance-association> instanceMaintenanceAssociate </maintenance-association> </get-cfm-mep-database></pre>	<pre>show oam ethernet connectivity-fault-management mep-database maintenance-domain <i>md-name</i> maintenance-association <i>ma-name</i></pre>
CFM	<pre><get-cfm-interfaces-information> <interface-name> interfaceValue </interface-name> </get-cfm-interfaces-information></pre>	<pre>show oam ethernet connectivity-fault-management interfaces <i>interfaceValue</i></pre>
CFM	<pre><get-interface-information> <terse/> <interface-name> interfaceValue </interface-name> </get-interface-information></pre>	<pre>show interfaces <i>interfaceValue</i> terse</pre>
CFM	<pre><get-cfm-interfaces-information> <interface-name> interfaceValue </interface-name> <detail/> </get-cfm-interfaces-information></pre>	<pre>show oam ethernet connectivity-fault-management interfaces <i>interfaceValue</i> detail</pre>
CFM	<pre><get-cfm-interfaces-information> <level> interfaceLevel </level> </get-cfm-interfaces-information></pre>	<pre>show oam ethernet connectivity-fault-management interfaces level <i>interfaceLevel</i></pre>

To perform a functional audit of a service to find out whether the service is up or down:

1. In the OAM Insight task pane, select **OAM Provisioning > Manage OAM Services**.
2. On the **Manage OAM Services** inventory page, select the service you want to investigate.
3. Either open the **Actions** menu and select **Perform Functional Audit**, or right-click and select **Perform Functional Audit**.

4. In the **Schedule Functional Audit** window, either select **Audit now**, or select **Audit later** and select a date and time.
5. Click **OK**.
6. In the **Job Details** window, click the job ID of the functional audit.

The **Job Management** window appears and shows a filtered view of the job inventory, showing only the functional audit job.
7. In the **State** column, check the status of the audit.

A checkmark indicates that the audit passed. An X indicates that the audit failed. If the **State** field indicates a failed functional audit, the device is down.
8. If the **State** field indicates the device is up, perform a configuration audit. See [“Performing a Configuration Audit” on page 101](#).
9. If the **State** field indicates the device is down, the **Summary** column gives an overview of the problem.
10. For detailed results of the functional audit, see [“Viewing Functional Audit Results” on page 107](#).

**Related
Documentation**

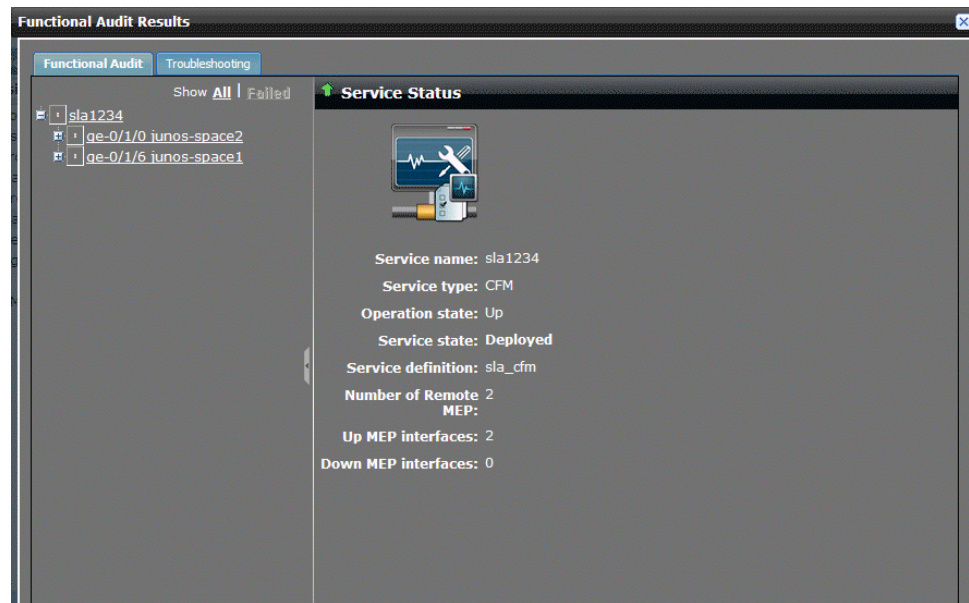
- [Performing a Configuration Audit on page 101](#)
- [Viewing Configuration Audit Results on page 103](#)
- [Viewing Functional Audit Results on page 107](#)

Viewing Functional Audit Results

To view the results of a functional audit of a service, follow this procedure:

1. In the OAM Insight task pane, select **OAM Provisioning > Manage OAM Services**.
2. In the **Manage OAM Services** window, select the service for which you want to view the functional audit results.
3. Either open the **Actions** menu and select **View Functional Audit Results**, or select the same command from the right-click menu.

The **Functional Audit Result** window appears, displaying **Service Status** in the right panel.



A green up-arrow in the **Service Status** header bar indicates that the service has passed the functional audit in both the control plane and the data plane. A red down-arrow indicates that the service failed either or both the control plane validation and the data plane validation.

Depending on the type of service, the left panel lists

- The name of the service
 - Each endpoint in the service
 - Interface name
 - Device name
4. To show all endpoints in the service, in the left panel header, select **All**. To display only the endpoints indicating failed validation, select **Failed**. Failed is dimmed if the functional audit returned no validation errors.
 5. To view details for an individual interface or endpoint, select it in the left panel. The header bar on the right panel changes to **End Point** or **Interface Status**, and details for the selected item are displayed below.
 6. Expand each device to show the link from that device to the other device in the service.

An icon next to each link indicates whether the functional audit commands reported correct functioning of the control plane and data plane. [Table 3 on page 108](#) describes these icons.

Table 3: Functional Audit Success Status Icons



Icon	Meaning
	Control plane and data plane function correctly.

Table 3: Functional Audit Success Status Icons (*continued*)

Icon	Meaning
	Errors were reported in the functioning of either the control plane or the data plane.

7. In the left panel, select a link.

The panel to the right shows the validation results for the control plane validation and data plane validation for the selected link. Icons indicate the success or failure of each of these sets of tests. [Table 4 on page 109](#) describes icons and the textual information provided in the box beside the icon.

Table 4: Control Plane and Data Plane Validation Icons



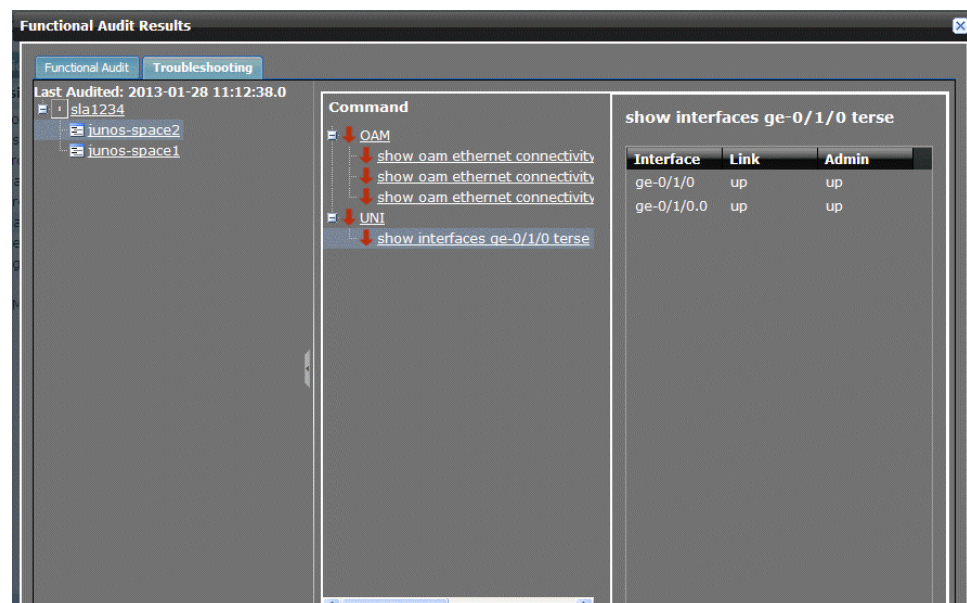
Icon	Meaning	Explanation
	Control plane up	The text box shows the name of the remote N-PE device and confirms that the data plane is operational.
	Control plane down	The text box shows the name of the configured remote N-PE device and, in the Command status field, explains why the test failed.
	Control plane status unknown	The text box indicates the name of the configured remote N-PE device and, in the Result field, an explanation as to why the functional audit operation was unable to test the control plane—for example, configuration was missing on the device.
	Data plane up	The text box indicates the number of packets transmitted and received, and confirms that no data packets were lost during the audit.
	Data plane down	The text box indicates that data packets were lost during the audit.

Table 4: Control Plane and Data Plane Validation Icons (*continued*)

Icon	Meaning	Explanation
	Data plane status unknown	The functional audit was unable to complete the data plane test. The Result field in the text box indicates the reason—for example, the platform does not support data plane testing, or the connection to the remote N-PE device is down.



The control plane and data plane validation checks must both show operational status for the link to be considered operational.

- To troubleshoot a service, open the **Troubleshooting** tab. To select the status you want to check, click the device from the device list on the left, and select the show command from the **Command** list. This figure shows the Ethernet OAM CFM information for the interface.



An icon next to each command indicates whether the command execution is successful or failed. [Table 5 on page 110](#) describes these icons.

Table 5: Command Status Icons

Icon	Meaning
	Command execution is successful and the command status is up.
	<ul style="list-style-type: none"> Command execution is failed, or, In case of multiple rows, one of the status value is down



NOTE: Junos OS Release 9.3 and Junos OS Release 9.4 do not support data plane validation. The Functional Audit Results window do not display data plane validation information if any device in the service is running one of these Junos OS releases.

**Related
Documentation**

- [Performing a Configuration Audit on page 101](#)
- [Viewing Configuration Audit Results on page 103](#)
- [Performing a Functional Audit on page 106](#)

