Oracle® Communications IP Service Activator

Network and SLA Monitoring Guide

Release 7.5
F59531-01
September 2022

Oracle Communications IP Service Activator Network and SLA Monitoring Guide, Release 7.5

F59531-01

Contents

A TopologyExporterConfig.xml Fields

Preface

This guide provides information about how Oracle Communications IP Service Activator can be integrated with third-party reporting systems to offer network and SLA monitoring.

Audience

This guide is intended for network administrators who want to integrate IP Service Activator with third-party reporting systems and applications that offer network and SLA monitoring.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1 Overview

This chapter provides a brief overview of the use of network and SLA monitoring with Oracle Communications IP Service Activator.

Introduction

IP Service Activator integrates with a wide range of third-party reporting systems and applications to offer network and SLA monitoring. To do this, network measurement parameters are first configured in IP Service Activator to generate network statistics from the devices. A third-party reporting tool is then set up to collect and process the performance data.

> **Note:**
>
> Measurement and SLA monitoring are currently supported on Cisco IOS-based devices only.

Measurement Types

IP Service Activator supports a range of measurement types that enable the measurement of point-to-point performance, or performance at a specific point in the network. The following measurement types are supported:

- **Service Assurance Agent (SAA)**: A Cisco technology that performs point-to-point measurement based on key SLA metrics such as response time, network resources, availability, jitter, connect time and packet loss.
- **CAR MIB statistics**: Report on performance of CAR-enabled interfaces. Used to monitor bandwidth usage.
- **MIB2 statistics**: Report on Management Information Bases (MIBs) in MIB2 format. Their variables indicate the basic state of the network, such as load, availability, discards, broadcast rate.
- **NetFlow:** A Cisco technology that enables you to characterize and analyze an IP flow on an interface. It is often used as a metering base for other applications, including accounting and billing, network planning, and marketing.

SAA measurements can be collected for pairs of peer devices (CE to CE, or between Virtual CEs, or between a CE and Virtual CE) within a VPN, either an MPLS VPN or a measurement-only VPN, with no MPLS configuration applied. Measurement is applied by defining an SAA template that holds one or more SAA operations and applying the template to a VPN.

NetFlow and MIB-based measurements can be collected for any IP Service Activator policy target; that is, a domain, network, customer, VPN, site, device, interface, sub-interface or VC endpoint. Measurement is applied using a measurement template which can be selectively

inherited to lower level policy targets using device and interface roles. This means that you can apply measurement at a high level, such as the network, and implement measurement only at selected points in the network.

External Systems

IP Service Activator uses external systems to model third-party applications in the user interface and object model. When setting up reporting and measurement, one or more external systems must be modelled through the IP Service Activator user interface.

The type and number of external systems that must be modelled depends on the reporting software used.

If Concord's eHealth Suite is used for reporting, a single eHealth suite must be modeled.

For complete information about modelling external systems, see "Modeling External Systems".

Configurable XML Exporter

The Configurable XML Exporter runs as a client of the OSS Integration Manager (OIM). Based on information contained in a local configuration file, the Configurable XML Exporter creates an export file that can be used by a third-party reporting tool to collect data for report purposes.

The local configuration file specifies the following information:

- The IP Service Activator IP address
- The data, including type and scope, to extract from the object model
- The number of XSL style sheets to apply to the XML data
- The name of the final export file

Getting Started

To set up network and SLA monitoring in IP Service Activator, you must first configure the devices in IP Service Activator to generate statistics for the various measurement types. To do this, see "Service Assurance Agent Measurement " and "MIB-based and NetFlow Measurements ".

After the devices are configured to generate statistics, you can then set up the third-party reporting tool to collect the statistics and generate reports. For more information, see "Setting Up IP Service Activator for Integration ".

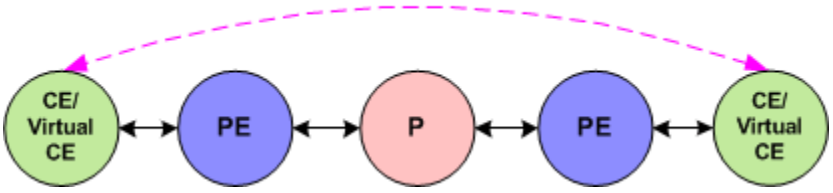
2
Service Assurance Agent Measurement

This chapter provides information about using Service Assurance Agent (SAA) Measurement with Oracle Communications IP Service Activator.

About Service Assurance Agent

Service Assurance Agent (SAA) is a Cisco technology that measures key SLA metrics, such as response time, network resources, availability, jitter, connect time, and packet loss between two devices (CE to CE, or between Virtual CEs, or between a CE and Virtual CE - in this chapter, the term ‘device' can refer to a CE or a Virtual CE). Figure 2-1 illustrates this concept.

Figure 2-1 SAA Monitoring SLA Metrics Between CE Devices



For measurements to or from a Virtual CE, you drag the CE device into the SAA VPN site and you also add the Virtual CE object. After this is completed, you can perform measurements between Virtual CEs and between CEs and Virtual-CEs in addition to CE to CE measurements.

SAA is also referred to as Response Time Reporter (RTR).

> **Note:**
>
> IPv6 SAA is implemented as IP SLA rather than RTR.

SAA's measurement features are built into the Cisco IOS software, supporting response time monitoring without the need to purchase and deploy additional equipment and software in the network. This feature may represent significant cost and management savings.

For information about device and IOS support, see *IP Service Activator Cisco IOS Cartridge Guide*.

SAA Operations

When you apply SAA to a VPN, Oracle Communications IP Service Activator tests the connection between pairs of sites in the VPN. The SAA operation that performs the test is configured at the device level.

Also known as probes, SAA operations collect response time and availability information. An operation is configured on a device and tests the connection to a target device by placing synthetic packets in the network. The packets simulate other forms of network traffic, depending on the type of operation that has been configured. Each SAA operation has a unique ID number that enables tracking of the operation.

This section details how different VPN configurations can affect the implementation of SAA operations. The SAA operations supported by IP Service Activator are also covered.

Configuration Considerations

The number of operations that are configured when you apply SAA to a VPN depends on the topology of the VPN and whether you choose to configure one or two-way tests.

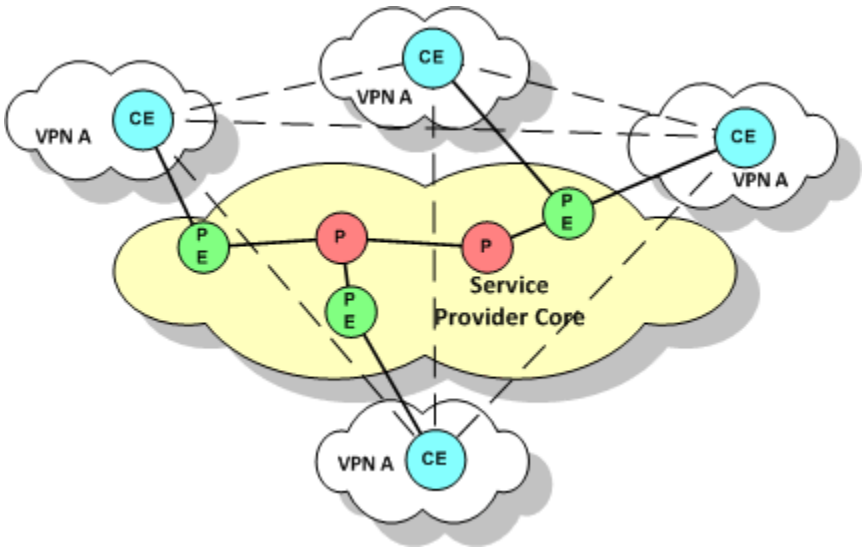
Unmanaged devices can also be configured for SAA measurement by modelling the device as a virtual device in IP Service Activator.

Topology

The number of tests performed depends on the VPN's topology and whether the probe properties are set to half or full duplex:

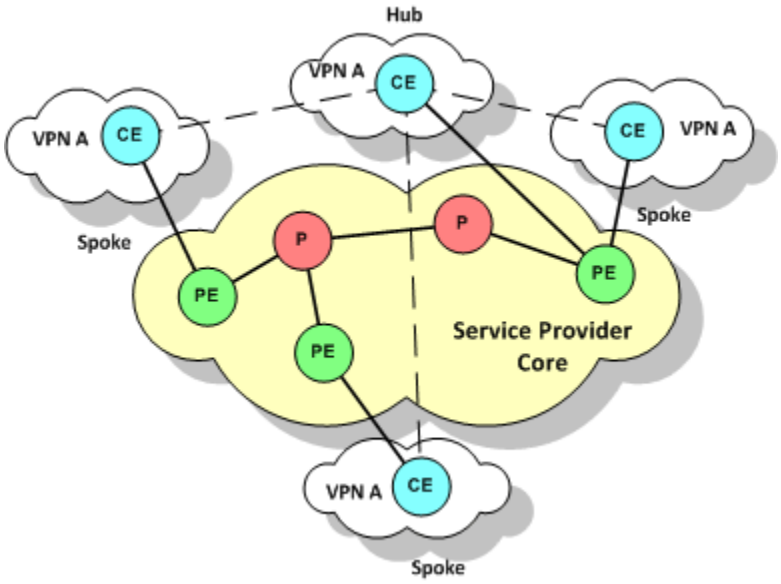
- In a fully-meshed VPN, IP Service Activator tests the connection between each pair of sites, as shown in Figure 2-2.

Figure 2-2 Connection Tests in a Fully-Meshed VPN



- In a hub and spoke VPN, IP Service Activator tests the connection between the hub site and each spoke site, as shown in Figure 2-3.

Figure 2-3 Connection Tests in a Hub and Spoke VPN



If there are multiple hub sites and they are meshed, IP Service Activator also tests the connection between each pair of hub sites.

One-way and Two-way Probes

When you apply SAA to a VPN, you can specify whether the probe configured for each pair of sites is:

- A one-way (half duplex): An operation is configured on only one device in the connection
- A two-way (full duplex): An operation is configured on both devices in the connection

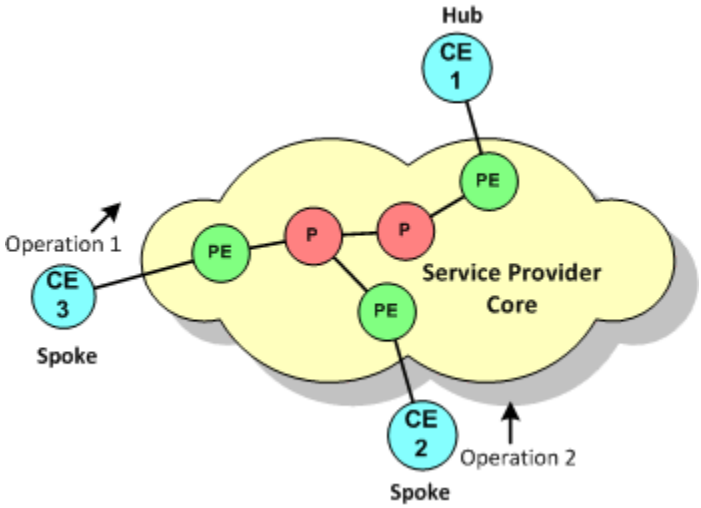
For TCP Connect, UDP Echo and Jitter operations, IP Service Activator also configures SAA Responder on target devices probed by one of these operations.

One-way Probes

For a one-way probe, IP Service Activator configures the operation on only one device for each A to B pair.

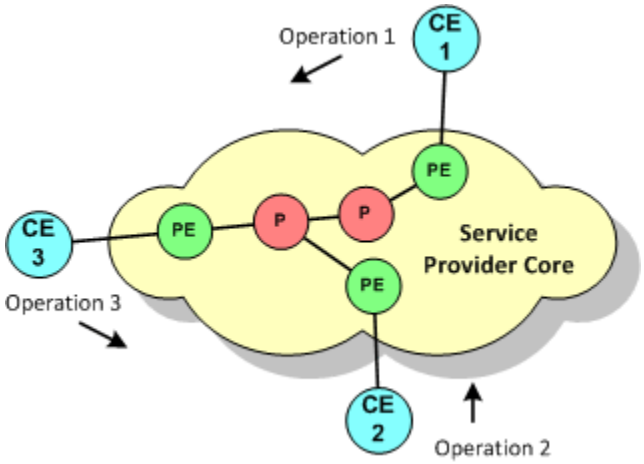
For hub and spoke VPNs, a probe is configured on each spoke, testing the connection from the spoke to the hub. These probes are shown in Figure 2-4.

Figure 2-4 One-way Probes in a Hub and Spoke VPN



For fully-meshed VPNs, IP Service Activator chooses one of the devices in each pair and configures the probe on that device only, ensuring that the load imposed by SAA is evenly distributed between devices. These probes are shown in Figure 2-5.

Figure 2-5 One-way Probes in a Fully-Meshed VPN

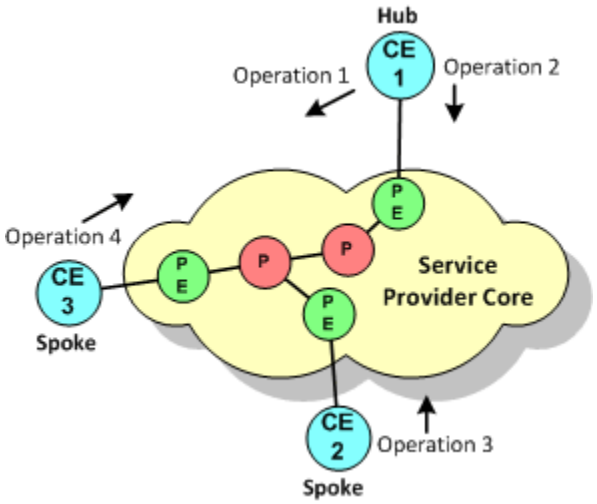


Two-way Probes

For a two-way probe, IP Service Activator configures the operation on both devices for each A to B pair.

For hub and spoke VPNs, an operation is configured on each spoke, with the hub as the target, and on the hub an operation is configured to probe each spoke connection. These operations are shown in Figure 2-6.

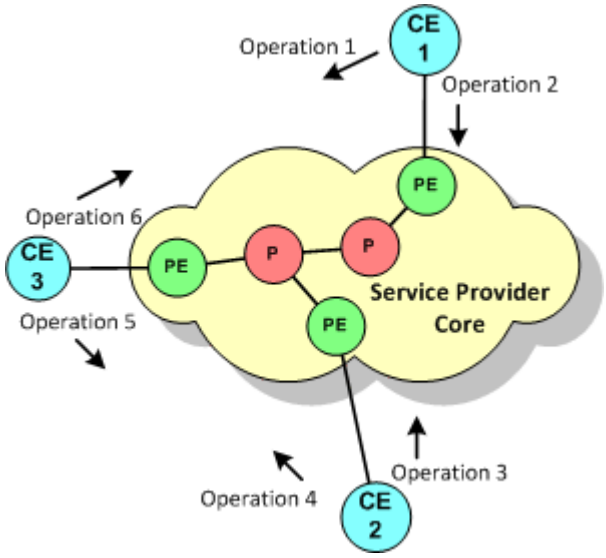
Figure 2-6 Two-way Probes in a Hub and Spoke VPN



If there are multiple hub sites and they are meshed, IP Service Activator probes the connection between each pair of hub sites.

For fully-meshed VPNs, probes are performed between each pair of sites. These probes are show in Figure 2-7.

Figure 2-7 Two-way Probes in a Fully-Meshed VPN



Unmanaged Devices

An unmanaged device is a device that is not managed by IP Service Activator. It is possible to test the connection from a managed device to an unmanaged device by modelling the unmanaged device as a virtual router. The virtual device is set up as the destination device in a one-way probe. One or more managed devices can then send test packets to the virtual device.

For information about modelling a virtual device, see *IP Service Activator User's Guide*.

> **Note:**
>
> When testing the connection to a virtual device, Jitter, UDP Echo and TCP Connect operations require the manual configuration of rtr responder on the target device. IP Service Activator cannot configure rtr responder on an unmanaged (virtual) device.
>
> The connection to a virtual device can be tested in one direction only; that is, from the managed to the unmanaged device.

SAA Probe Calculations

The following is a breakdown of the SAA probe calculation method. Figure 2-8 demonstrates how the calculation is broken down into its components and Table 2-1 explains the individual components.

Figure 2-8 Example of SAA Probe Calculation

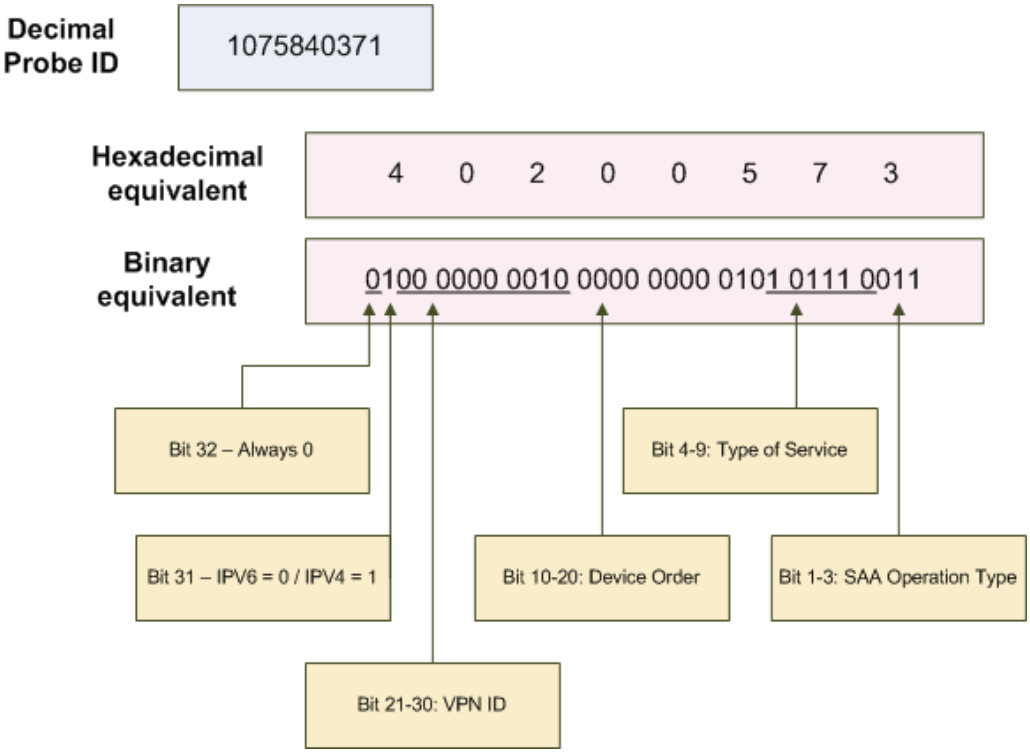


Table 2-1 Components of the SAA Probe Calculations

Component	Description
VPN ID	This is taken from the VpnId attribute of the SAA VPN object.
Device order	This is taken from the VpnOrder attribute of the hub-site concrete object in the SAA VPN.
Type of service	This is the DSCP value for the class of probe.
SAA Operation type	This is the value for the type of operation.

Supported Operations

Table 2-2 summarizes IP Service Activator support for SAA operations.

Table 2-2 Supported SAA Operations

Operation	Description
ICMP Echo	Measures end-to-end response time between a Cisco router and devices using IP.
UDP Echo	Calculates UDP response times between a Cisco router and an IP-enabled device.
TCP Connect	Discovers the time it takes to connect to a target device.
Jitter	A super set of the UDP Echo operation. The Jitter operation additionally measures per-direction packet-loss and jitter (inter-packet delay variance).

For detailed information about these operations, see the Cisco documentation.

> **Note:**
>
> The number of SAA operations that can be configured on a Cisco device is limited by the router's IOS and hardware specification. Devices running IOS 12.1 or later support a maximum of 500 operations.

For UDP Echo, ICMP and Jitter operations, the target device may not natively provide the service. You can specify whether the operation sends a control message to the target device to enable the destination port prior to sending a packet.

When you push ICMP probe to the device IP Service Activator doesn't activate RTR responder on the device. In this case, you must manually activate the RTR responder on the device.

For all operations, you can define the rising or falling threshold for response times to the operation's test packets. A variety of algorithms are available for calculating a violation. You can also specify how long the operation waits for a response, whether error checking is performed and whether loss of connection is reported for connection-oriented protocols. You can specify what happens when a threshold is violated or a timeout or error condition occurs, either sending an SNMP trap or an SNA NMVT alert. An SNA NMVT alert is an SNA message that conveys network management specific information.

> **Note:**
>
> IP Service Activator does not configure the target address for an SNMP trap or SNA NMVT alert. To send an SNMP trap or SNA NMVT alert, you must manually configure the target address details on the relevant devices.

SAA Responder

UDP Echo, Jitter and TCP Connect operations use non-native services to test the connection to a target device. The SAA Responder enables a router to respond to these operation types and must be configured on target devices. IP Service Activator automatically configures an SAA Responder on the relevant devices.

SAA Templates

In IP Service Activator, an SAA template acts as a container for one or more SAA operations. A template may contain configuration details for different operation types, such as UDP and Jitter, or TCP Connect and Jitter. Once defined, a template can be applied to any number of VPNs.

For information on the limits that operate when defining an SAA template and applying SAA to a VPN, see "Creating an SAA Template".

Applications in IP Service Activator

IP Service Activator can apply SAA measurements to both MPLS and measurement-only VPNs.

MPLS VPN

When you apply SAA to a VPN, IP Service Activator configures operations between pairs of devices within the VPN. The number of operations configured depends on the VPN's topology and whether connections are tested in one or both directions. For more information, see "Configuration Considerations".

Applying SAA to an MPLS VPN is suitable only where the VPN has a small number of sites or has a hub and spoke topology. If the VPN topology is fully-meshed, IP Service Activator configures a full mesh of SAA operations. The number of operations configured on each device will therefore be one less than the number of sites in the VPN.

SAA is processor intensive and significantly affects device performance. The greater the number of sites in the VPN, the greater the number of operations configured on each device.

If you choose to deploy more than one SAA operation, for example, Jitter and TCP Connect, operations are configured for each type.

Measurement-only VPN

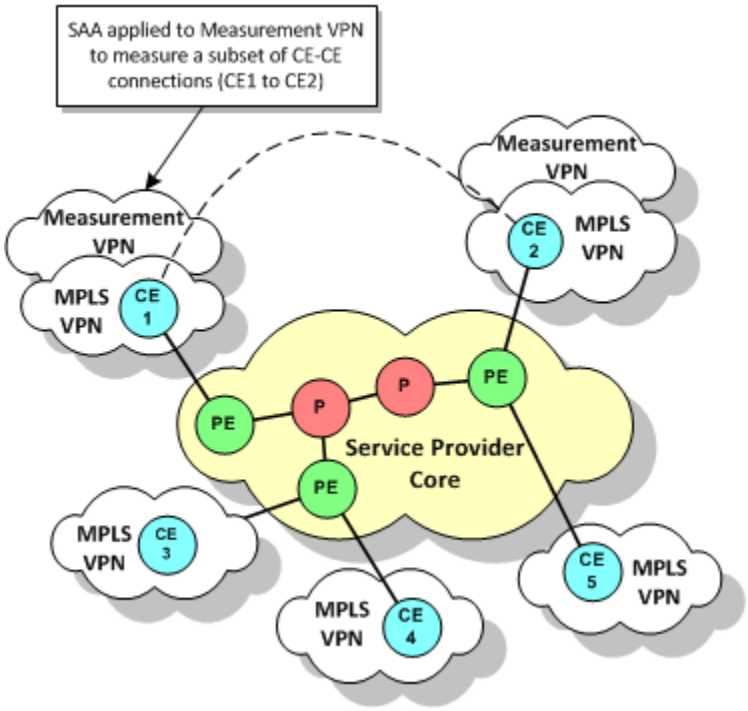
A measurement-only VPN allows you to apply SAA to a subset of devices in an MPLS VPN or to apply SAA without configuring an MPLS VPN. A measurement-only VPN can be used to:

- Group a subset of devices that belong to an MPLS VPN and apply SAA to those devices.

  This enables you to measure the connection between selected devices in an MPLS VPN, where the size of the VPN or its topology makes measuring all connections unfeasible.

  Figure 2-9 illustrates this concept. All CE devices are members of an MPLS VPN. To reduce the number of operations configured, however, only the connection between CE1 and CE2 is measured. This is achieved by overlaying the MPLS VPN with a measurement-only VPN and applying SAA to the measurement-only VPN.

Figure 2-9 Measurement-only VPN Overlay



- Group devices that do not participate in an MPLS VPN and apply SAA measurement.

  This enables you to measure a connection between any pair of devices without the need to configure MPLS.

Configuring SAA

SAA Measurement is configured in IP Service Activator by defining an SAA template that holds one or more SAA operations and applying the template to a VPN.

This section covers the following topics:

- Configuration Prerequisites

- Deployment Considerations
- Configuring SAA Measurements for Different VPN Connections
- Configuring SAA Measurement in IP Service Activator

For more information on the Service Assurance Agent, refer to the Cisco documentation.

Configuration Prerequisites

Before configuring SAA in IP Service Activator, ensure that the following pre-requisites are implemented:

- The RTT-MON MIB v2.1.0 or later must be present on the devices that you want to configure an SAA operation.
- Given that memory problems are common, the following command should be run on CE devices before configuring the SAA probes:

  ```
  Global config mode
  rtr low-memory #
  ```

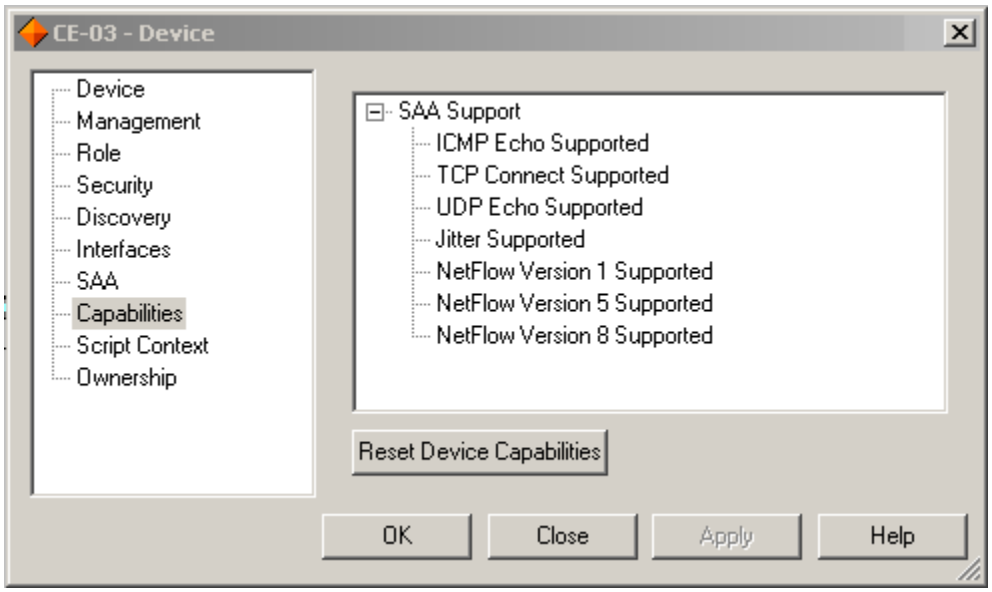
  Where # is an integer that is equal to 25% of the memory available in the system. For more information, see Cisco documentation.
- If you intend to generate reports based on the SAA measurement, there may be additional pre-requisites associated with the reporting tool. For more information about the reporting tool's measurement requirements, see "Generic Exporter".

Deployment Considerations

This section highlights some of the deployment considerations associated with applying SAA using IP Service Activator.

- Check the device's capabilities to determine which operation types are supported. The operation types can be found on the device object's Properties page in the Capabilities section, as shown in Figure 2-10.

Figure 2-10 Device Capabilities



- Make sure that you specify the correct device roles when defining data collection points. For more information, see "Creating Collectors".
- Ensure that you apply SAA templates only to the VPNs that you want to measure.

Configuring SAA Measurements for Different VPN Connections

SAA measurement can be set up for the following VPN connections:

- Configuring SAA for a CE to CE Connection
- Configuring SAA for a PE to PE Connection using Shadow Routers
- Configuring SAA for a PE to CE Connection using a Shadow Router

You can also test the connection to an unmanaged device by modelling it as a virtual router. For more information, see "Unmanaged Devices".

A shadow router is a device dedicated to SAA measurements in a service provider's Points of Presence (POP). Deploying shadow routers enables realistic PE to PE or PE to CE metrics to be gathered and protects measurement routers from customers. A PE device may have any number of shadow routers attached to it.

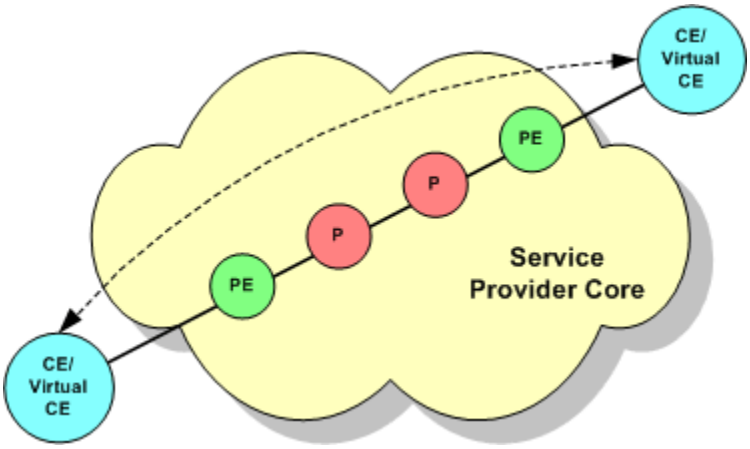
When configuring SAA measurements for different VPN connections, you may need to refer to the following additional references:

- For information about setting up a VPN, see *IP Service Activator VPN User's Guide*.
- See "Configuring SAA Measurement in IP Service Activator" for procedures on how to do the following:
  - Create an SAA template and apply it to a VPN.
  - Create a measurement-only VPN.

Configuring SAA for a CE to CE Connection

By deploying SAA on CE devices (or Virtual CEs), as shown in Figure 2-11, you can capture information about the complete end-to-end performance of a VPN service.

Figure 2-11 SAA for CE to CE Connections



You can only test a CE to CE connection where one or both CE devices are managed. An unmanaged device may be modelled as a virtual router and a one-way test performed. See "Unmanaged Devices".

There are two alternatives for monitoring a CE to CE connection:

- Apply SAA to the MPLS VPN: this setup is feasible only in some scenarios. See "Configuration Considerations" and "MPLS VPN".
- Overlap an MPLS VPN with a measurement-only VPN populated by a subset of the CE devices and apply SAA to the measurement-only VPN

To apply SAA to a CE to CE connection in an MPLS VPN:

1. Create a Management VPN populated by the CE devices and the management station.
2. Create an MPLS VPN where each site consists of a CE device and a PE interface.
3. Apply an SAA template to the MPLS VPN.

To apply SAA to a CE to CE connection in a measurement-only VPN:

1. Create a Management VPN populated by the CE devices and the management station.
2. Create an MPLS VPN where each site consists of a CE device and a PE interface.
3. Create a measurement-only VPN, populated by a subset of the MPLS VPN's CE devices.

   You do not need to associate the PE interface with the measurement-only VPN's sites.
4. Apply an SAA template to the measurement-only VPN.

For information about setting up a VPN, see *IP Service Activator VPN User's Guide*.

For information about creating and applying an SAA template and creating a measurement only VPN, see "Configuring SAA Measurement in IP Service Activator".

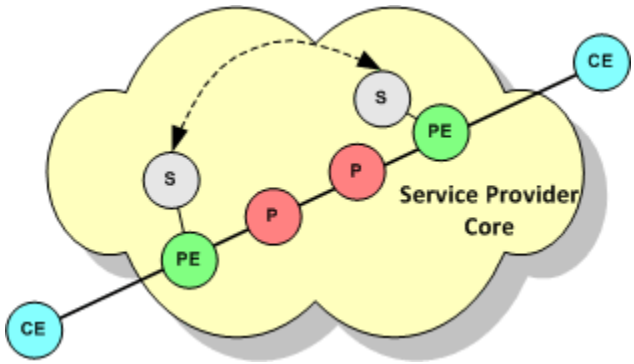
Configuring SAA for a PE to PE Connection using Shadow Routers

PE to PE measurement provides information about the performance across the network backbone.

To collect PE to PE metrics, you must deploy shadow routers. In IP Service Activator, a shadow router behaves in a similar way to a CE device: it may be associated with a site and have a VRF table associated with it, a protocol may be specified for connection to the PE device, and so on.

IP Service Activator includes a system-defined Shadow role which must be assigned to the shadow devices. For information about assigning a role to a device, see *IP Service Activator User's Guide*.

Figure 2-12 SAA for PE to PE Connections using Shadow Routers



The PE device to which a shadow router is attached may participate in more than one MPLS VPN, where each VPN belongs to a different customer. If you wish to view performance metrics per customer in IP Service Activator using an integrated reporting tool, you must create a measurement-only VPN for each customer. Populate the measurement-only VPN with the relevant shadow routers and apply SAA to the VPN.

To apply SAA to a PE to PE connection using shadow routers:

1. Create a Management VPN populated by the shadow routers and the management station.
2. Create an MPLS VPN where each site is a shadow router and a PE interface.
3. If you want to group a subset of shadow routers by customer, create a measurement-only VPN populated by the relevant shadow routers.
4. Apply an SAA template to the MPLS VPN and, if created, each measurement-only VPN.

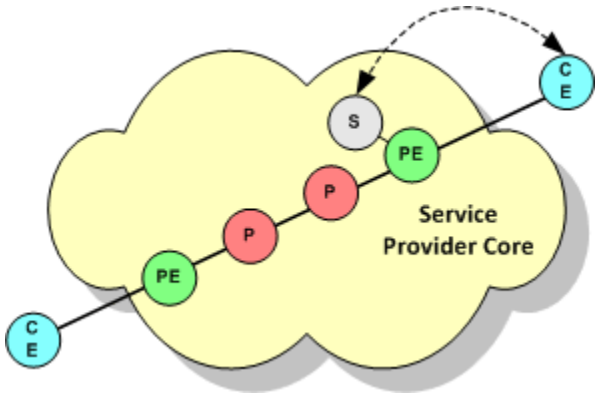
For information about setting up a VPN, see *IP Service Activator VPN User's Guide*.

For information about creating and applying an SAA template and creating a measurement only VPN, see "Configuring SAA Measurement in IP Service Activator".

Configuring SAA for a PE to CE Connection using a Shadow Router

PE-CE metrics provide information about the connection between the service provider's POP and a customer site. A shadow router must be deployed at the PE device, as shown in Figure 2-13.

Figure 2-13 SAA for PE to CE Connections using a Shadow Router



If the CE device is not managed it is possible to test the connection to it by modelling the device as a virtual router. See "Unmanaged Devices".

To apply SAA to a PE to CE connection using a shadow router:

1. Create a Management VPN that contains the shadow routers and the management station and, optionally, the CE devices.

   Alternatively, you can create two Management VPNs: one for the shadow routers and one for the CE devices.
2. Create an MPLS VPN where each site is a CE device and a PE interface.
3. Create a measurement-only VPN populated by a shadow router attached to one of the MPLS VPN's PE devices and one or more of the CE devices attached to the PE device.
4. Apply an SAA template to the measurement-only VPN.

For information about setting up a VPN, see *IP Service Activator VPN User's Guide*.

For information about creating and applying an SAA template and creating a measurement only VPN, see "Configuring SAA Measurement in IP Service Activator".

Configuring SAA Measurement in IP Service Activator

This section covers the following procedures:

- Creating an SAA Template
- Adding an SAA Operation to a Template
- Creating a Measurement-only VPN
- Applying an SAA Template to a VPN

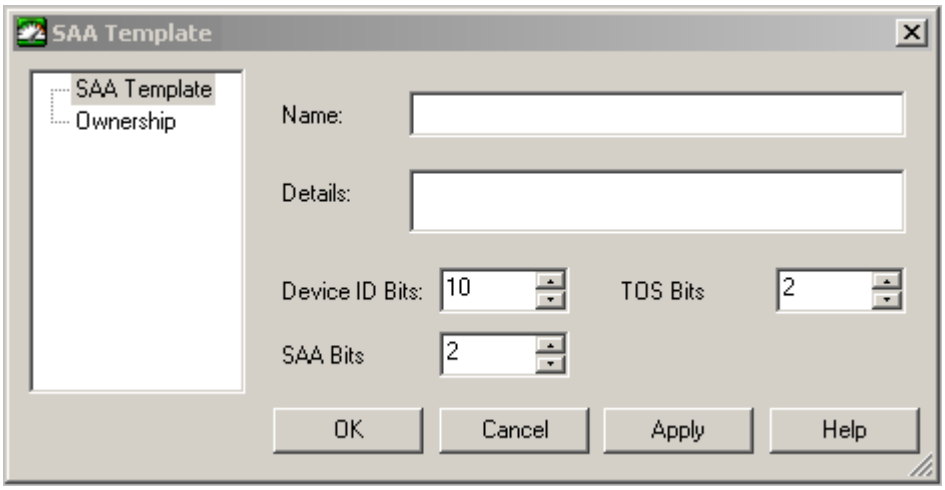
Creating an SAA Template

By default, an SAA template has the following:

- A maximum of 1024 devices that can participate in the VPN
- A maximum of 4 Type of Service (ToS) values that can be used within the VPN
- A maximum of 4 operation types that can be applied to the VPN

However, you can adjust these VPN-specific limits by specifying the amount of space that IP Service Activator allocates to store device, ToS value, or operation type data.

Figure 2-14 Adjusting the SAA Template Values



By adjusting the values of Device ID Bits, TOS Bits, and SAA Bits, you can increase the number of devices within the VPN, the number of operations, or the number of operation types that can be applied. The values specified for these three fields must add up to exactly 14. If you choose to increase the number of bits allocated to the device ID, you must reduce either the number of bits allocated to the ToS value or the SAA operation type.

If you want to apply more than one operation to a single peer-to-peer connection in a VPN, you must ensure that either the ToS value or the operation type differs between the operations. This is because IP Service Activator bases each operation's unique RTR (Round Time Response) number on the ToS value and operation type (in combination with other types).

To create an SAA template:

1. On the **System** tab, right-click the **SAA Templates** folder.
2. Select **Add SAA Template**.

   The SAA Template dialog box opens.
3. Specify values including **Name**, **Details**, **Device ID Bits**, **TOS Bits**, and **SAA Bits**.
4. Click **OK** and commit the transaction.

Adding an SAA Operation to a Template

You can only configure SAA operations to test the connection between two devices that are in the same customer VPNs.

To add an SAA operation to a template:

1. On the **System** tab, open the **SAA Templates** folder.
2. Right-click the SAA template and select **Add SAA Operation**.

   The SAA Operation dialog box opens.
3. On the SAA Operation property page, specify values including **Type**, **Source port**, **Destination Port**, **Request size**, **ToS, Control**, **Packets in sequence**, **Inter-packet interval**, **History lives kept**, **History filter**, **History buckets**, and **Tag Value**.
4. Select the Threshold property page.
5. Specify values including **Type**, **Rising**, **Falling**, **Repetitions**, **X**, **Y**, **Average**, and **Action**.
6. Select the Other property page.
7. Specify values including **Period**, **Timeout**, **Lifetime**, **Half duplex**, **Full duplex**, **Error checking**, **Connect checking**, and **Timeout checking**.

Creating a Measurement-only VPN

You can use SAA to measure the point-to-point connection between any pair of devices without configuring an MPLS VPN.

To apply SAA without configuring an MPLS VNP:

1. Apply the appropriate roles to the relevant devices.

   You can associate devices tagged with the Access or Shadow role with sites in a VPN.
2. Associate each device with a site. For Virtual CE measurements, you also associate the Virtual CE to the site.

   You do not need to associate an interface with the site.
3. If needed, specify the device's (or Virtual CE's) SAA destination and source measurement address as follows:
   a. Open the Device/Virtual CE dialog box.
   b. Select the SAA property page. Note that attributes on the Virtual CE SAA property page are different than those on the Device SAA property page.
   c. Configure Measurement Probe Destination Address in one of two ways:
      - Select **Use device management address** to use the device management IP address set up on the Device property page as the SAA destination measurement address.
      - Select **Use**, and from the list choose one of the interfaces previously discovered on the device.
   d. Configure Measurement Probe Source Address in one of four ways:

- Select **Use Measurement Probe Destination Address** to use the Measurement Probe Destination Address as the Measurement probe source address in the device.
- Select **Use Device Management Address** to use the Device Management Address as the Measurement probe source address in the device.
- Select **Use** and from the menu select an address from the other available addresses in the device as the Measurement probe source address.
- Select **Not configured** to avoid configuring the Measurement probe source address in the device.

e. Select **Use** and select an IP address from the list of interfaces that have been discovered by the device.

4. For each site:
   a. Right-click the site and select **Properties** from the menu.

      The Site dialog box opens.

   b. Select the Connectivity property page.
   c. In the **Routing Type** field, select **None**.
5. Create a VPN by right-clicking the VPN folder and selecting **Add MPLS VPN** from the menu.
6. Ensure that the **Use MPLS** option on the VPN property page of the VPN dialog box is cleared to effectively create a measurement-only VPN.
7. Add the relevant sites to the VPN.

Applying an SAA Template to a VPN

To apply an SAA template to a VPN:

1. On the **Service** tab, select the relevant VPN and select **Properties** from the VPN menu.

   VPNs are listed in the VPNs folder beneath the relevant customer.
2. Select the Measurement property page.
3. In the **SAA Measurement** field, select an SAA template from the list.

If a site is a member of more than one VPN to which SAA measurement is applied, there may potentially be one operation per VPN configured on the device, depending on the VPN's topology and whether one or two-way tests are performed. For information about the factors that affect the number of operations configured within a VPN, see "SAA Operations".

3
MIB-based and NetFlow Measurements

This chapter provides information about measuring performance in Oracle Communications IP Service Activator using MIB-based and NetFlow measurements.

Overview of MIB and NetFlow-based Measurements

Oracle Communications IP Service Activator allows you to measure performance based on various information sources other than SAA probes. You can apply CAR MIB, MIB2 and NetFlow measurement types to any policy target, including a customer, VPN, device or VC endpoint.

Measurement is set up by applying a measurement parameter to a policy target. Measurement types are inherited in the same way as rules and PHB groups. Device and interface roles provide fine-grained control over the application of NetFlow and MIB-based measurements.

After you configure the measurement parameters, you can set up a third-party reporting tool to collect and process the performance data. For more information, see "Setting Up IP Service Activator for Integration ".

About Committed Access Rate MIB

Committed Access Rate (CAR) is configured on router interfaces. It is used to limit the input and output traffic rates, control bandwidth usage and implement a selective IP entry policy.

CAR MIB reports provide a clear picture of the performance of each interface channel based on its CAR configuration. CAR MIB polls the following MIBs:

- CISCO-CAR-MIB
- CISCO-SMI-MIB

About MIB2

MIB2 measurement polls variables defined in any MIB2 format MIB. The MIB and the variables polled depend on the reporting tool used to generate reports.

Applying MIB2 measurement provides information about the basic state of the network; for example, load, availability, discards, broadcast rate. Monitoring MIB2 values can provide useful information for detecting escalating error conditions and to determine trends that aid in capacity planning.

There is no device configuration associated with MIB2 measurement.

About NetFlow

NetFlow is a Cisco-specific feature that enables you to characterize and analyze an IP flow on an interface with minimal impact on router performance. Often used as a metering base

for other applications, including accounting and billing, network planning, and marketing, NetFlow generates flow-based statistics per interface and the information produced is highly granular. NetFlow is often deployed at the PE interface within an MPLS VPN but can be applied at any point in the network.

Flow-based statistics are gathered on the router and stored in a cache. At intervals, the router exports its stored information in the form of NetFlow UDP datagrams to collector software; the software varies, depending on which reporting tool you wish to use (see "Creating Collectors"). A range of UDP formats is supported; later versions minimize bandwidth usage by aggregating data before export from the device.

The NetFlow measurement parameter specifies which version of UDP to use for exporting flow data and any aggregation that should be applied before export. The device driver configures NetFlow on the device according to the parameters defined in IP Service Activator.

For information on IP Service Activator support for NetFlow by device and IOS, see the IP Service Activator Cisco cartridge guides.

This section covers the following NetFlow topics:

- NetFlow Architecture and Components
- About Flows
- About UDP Formats
- About Aggregation

NetFlow Architecture and Components

In any NetFlow deployment, collection software gathers exported flow data from monitored devices. IP Service Activator currently supports the following collection software:

- Vista Plug-in for NetFlow
- Cisco's NetFlow FlowCollector

Oracle recommends that you install the collection software on a dedicated host machine. A number of collectors may be distributed throughout the network, with each collector gathering data from a subset of devices.

About Flows

A flow is a unidirectional stream of packets between a source and a destination. Both of these parameters are defined by a network-layer IP address and a transport-layer source and destination port number. A flow is identified by the combination of the following seven field values:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- ToS byte

- Input logical interface (ifIndex)

Together, these key fields define a unique flow. Additional accounting fields appear in the flow and these vary depending on which UDP format version packets have been selected for export from the device (see "About UDP Formats").

Flows are processed in a NetFlow cache. NetFlow creates a NetFlow cache entry that contains information for all active flows. Within the cache, a flow record is maintained for each active flow. Each flow record contains key fields that can be used for exporting to a collection device.

The router checks the cache once per second and expires the flow if one or more of the following conditions are met:

- Transport is completed
- The cache is full
- The inactive timer has expired after traffic inactivity for the specified number of seconds
- The active timer has expired after traffic activity for the specified number of minutes

About UDP Formats

NetFlow data is exported from the router as a UDP datagram in one of the five formats: Version 1, Version 5, Version 7, Version 8, or Version 9. The datagram consists of a header and one or more flow records.

IP Service Activator supports the following formats:

- **Version 1:** The first released version and should only be used if you need to support a legacy collection system. Typically, records are exported when the NetFlow cache is full or the flow or the timer has expired.
- **Version 5:** Based on version 1 with the addition of BGP AS information and flow sequence numbers.
- **Version 8**: Supports router-based aggregation of flows in additional aggregation caches. As flows expire from the main cache, they are added to each enabled aggregation cache. This format allows for export datagrams to contain a subset of Version 5 export data, which is valid for a particular aggregation cache scheme.
- **Version 9**: A flexible and extensible means to carry NetFlow records from a network node to a collector. The version has definable record types and is self-describing for easier NetFlow Collection Engine configuration. In this version:
  - Record formats are defined using templates.
  - Template descriptions are communicated from the router to the NetFlow Collection Engine.
  - Flow records are sent from the router to the NetFlow Collection Engine with minimal template information so that the NetFlow Collection Engine can relate the records to the appropriate template.
  - The version is independent of the underlying transport (UDP, TCP, SCTP, and so on).

IP Service Activator indicates which UDP versions are supported by the device in the device capabilities. For information on retrieving and viewing device capabilities, see *IP Service Activator User's Guide*.

For detailed information on which UDP versions are supported by a particular device, consult the Cisco documentation.

About Aggregation

Aggregating NetFlow data on the router before exporting in Version 8 format provides a number of benefits:

- It reduces the bandwidth required between the router and the machine that collects the exported NetFlow data.
- It reduces the amount of flows sent to the collector software for processing.
- It improves the scalability of high-flow-per-second routers, such as the Cisco 7500 series routers.

A range of aggregation schemes is available and you can configure each aggregation scheme with a cache size, timeout value, export destination IP address and export destination UDP port.

As flows expire in the main NetFlow cache, relevant information is extracted from the expired flow and the relevant flow entry in an aggregation cache is updated. One or more aggregation caches may be maintained, depending on the number of aggregation schemes selected for export. Each aggregation cache contains different field combinations that determine which data flows are grouped.

> **Note:**
>
> In IP Service Activator you can implement only one aggregation scheme on a device. The aggregation cache parameters (size, timeout value, and so on) are the same as those defined for the main NetFlow cache.

Data is always exported from an aggregation cache in v8 format.

The following aggregation schemes are available:

- **AS aggregation**: Generates AS-to-AS traffic flow data. The scheme groups data flows by source BGP AS, destination BGP AS, input interface and output interface.
- **Destination prefix**: Supports examination of flows by destination. The scheme groups data flows by destination prefix, destination prefix mask, destination BGP AS and output interface.
- **Prefix aggregation**: Supports examination of flows by source and destination. The scheme groups data flows by source prefix, destination prefix, source prefix mask, destination prefix mask, source BGP AS, destination BGP AS, input interface and output interface.
- **Protocol port aggregation**: Supports examination of network usage by traffic type. The scheme groups data flows by IP protocol, source port number and destination port number when applicable.
- **Source prefix aggregation**: Supports examination of flows by source. The scheme groups data flows by source prefix, source prefix mask, source BGP AS and input interface.

> **Note:**
>
> If you are generating NetFlow reports in IP Service Activator, note that some aggregation schemes may not be supported by the integrated reporting software. Consult the relevant SLA monitoring guide or third-party documentation for details of supported schemes.

Configuring Measurement Types in IP Service Activator

This section gives conceptual and procedural information about configuring measurement types in IP Service Activator.

Configuration Considerations

Depending on the type of measurement being configured and its intended use, any one of the following considerations should be taken into account when configuring a measurement parameter in IP Service Activator:

- Reports
- Policy Target Levels
- CAR MIBs
- NetFlow

Reports

If you intend to generate reports based on these measurement types, there may be additional requirements associated with the reporting tool. For more information about the reporting tool's measurement requirements, see "Generic Exporter".

Policy Target Levels

Measurement is automatically inherited to policy targets at a lower level, down to the device level. Below this level, device and interface roles specify where measurement is inherited to.

When you configure a measurement parameter, you must specify at which level measurement is activated, and this varies depending on the measurement type, as shown in Table 3-1.

Table 3-1 Measurement Levels by Type

Measurement	Device Level	Interface Level	Sub-interface Level	PVC Level
CAR MIB	N/A	Select one or more options (mandatory)	Select one or more options (mandatory)	Select one or more options (mandatory)
MIB2	Select one or more options (mandatory)	Select one or more options (mandatory)	Select one or more options (mandatory)	Select one or more options (mandatory)

Table 3-1 (Cont.) Measurement Levels by Type

Measurement	Device Level	Interface Level	Sub-interface Level	PVC Level
NetFlow	Mandatory	Select one or more options (mandatory)	Select one or more options (mandatory)	Select one or more options (mandatory)

NetFlow is generally applied to Access interfaces on PE devices; that is, as close to the customer site as possible.

CAR MIBs

If you want to apply the CAR MIB measurement on an IP Service Activator object, the following MIBs must be present on the devices where measurement is implemented:

- CISCO-CAR-MIB
- CISCO-SMI

NetFlow

When applying NetFlow measurement, you can specify in which version of UDP packets are exported from the device to the NetFlow collector. Later versions support aggregation of flows before export, minimizing bandwidth usage. For more information on UDP and aggregation, see "About UDP Formats" and "About Aggregation".

> **Note:**
>
> If you are monitoring NetFlow measurements using an integrated reporting tool, check which aggregation schemes are supported. A tool may not support all of the available aggregation types. For information on supported aggregation types, consult the reporting tool's documentation.

The following limitations apply to the NetFlow measurement parameter:

- NetFlow data cannot be exported to more than one collection system.
- When configuring NetFlow measurement, you cannot configure multiple aggregation schemes on a device.
- Check the device's capabilities; device-level capabilities indicate support for NetFlow.

  To do this, right-click on the device object and select Properties from the context menu. Then select the Capabilities property page.
- Oracle recommends that you configure a dedicated interface between the router and the collection device to prevent loss of packets.
- The collection device should be a dedicated host machine.

Applying NetFlow or MIB-based Measurements to a Policy Target

Measurement Parameters can be applied to policy targets including networks, devices, interfaces, and sub-interfaces.

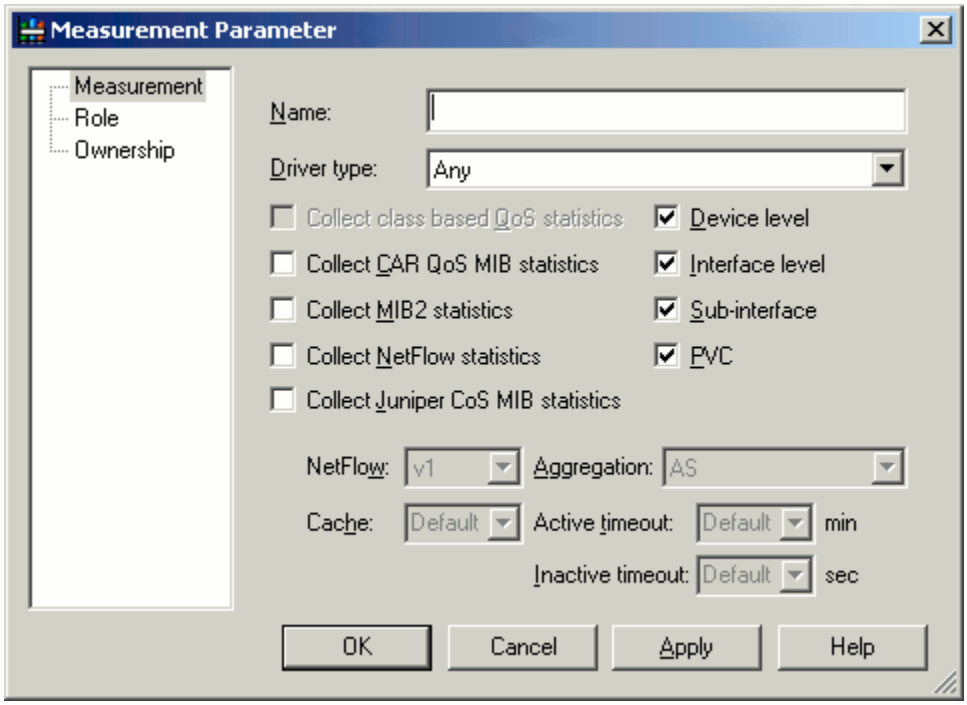
To apply NetFlow or MIB-based measurements (on device driver) to a policy target:

1. From the policy target's pop-up menu, select Add Measurement Parameter.

   The Measurement Parameter dialog box appears.

2. Select the Measurement property page, shown in Figure 3-1.

Figure 3-1 The Measurement Property Page on the Measurement Parameter Dialog Box



3. In the Name field, enter an identifier for the measurement parameter.
4. From the Driver type drop-down menu, select a driver type or select Any to apply measurement to all vendor devices.
5. As needed, specify options including **Collect class-based QoS statistics**, **Collect CAR QoS MIB statistics**, **Collect MIB2 statistics**, **Collect NetFlow statistics**, **Collect Juniper CoS MIB Statistics**, **Device level**, **Interface level**, **Sub-interface**, **PVC**.
6. If you select NetFlow properties, specify values for **Netflow**, **Cache**, **Aggregation**, **Active timeout**, and **Inactive timeout**.
7. On the Role property page, specify the device and interface roles to which measurement applies.

If you are using Network Processor, you can apply Netflow parameters using Netflow Parameters and Collector Parameters configuration policies that are packaged within the Service Assurance module.

To apply NetFlow or MIB-based measurements to a policy target using NetFlow parameters:

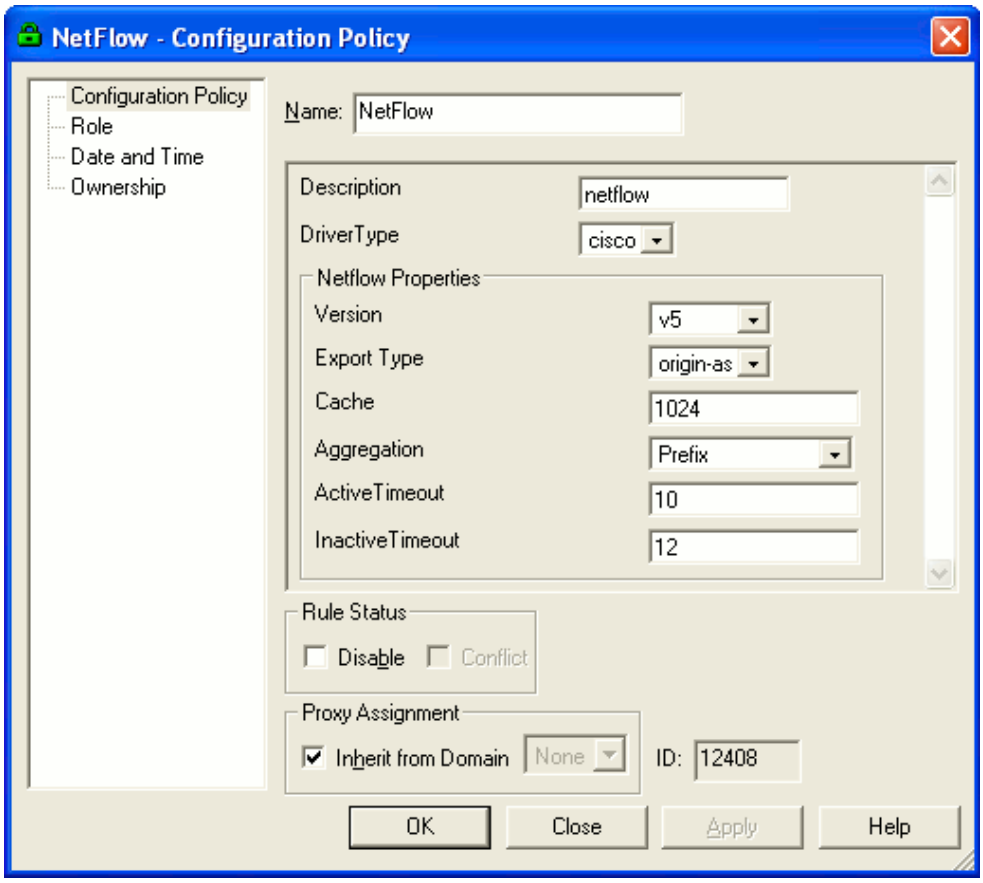
1. On the Domain dialog box, load the **ServiceAssurancePolicyTypes.policy** configuration policy.

   For information on loading a configuration policy file, see *IP Service Activator QoS User's Guide*.

2. On the Topology tab, right-click a policy target, select **Add Configuration Policy**, select Service Assurance, then select **Netflow Parameters**.

   The Configuration Policy dialog box appears, shown in Figure 3-2.

Figure 3-2 NetFlow Configuration Policy Dialog Box



3. In the Name field, enter a name for the configuration policy.
4. In the Description field, enter a description for the configuration policy.
5. From the DriverType list, select the appropriate vendor device to which you want to apply the configuration policy.

   Netflow is supported only on Cisco cartridge.

6. From the Version list, select one of the following:
   - Select **AG Only** to export data from the aggregation cache only.
   - Select **v1** to export data in v1 format.

- Select **v5** to export data in v5 format.
- Select **v9** to export data in v9 format.

7. From the Export Type list, select one of the following:
   - Select **Origin-as** to specify that export statistics include the origin autonomous system (AS) for the source and destination.
   - Select **Peer-as** to specify that export statistics include the peer AS for the source and destination.
8. From the Aggregation list, select one of following:
   - **AS**: Indicates the scheme groups' data flows by source BGP AS, destination BGP AS, input interface, and output interface.
   - **Destination-Prefix**: Indicate the scheme groups' data flows by destination prefix, destination prefix mask, destination BGP AS, and output interface.
   - **Prefix**: Indicates the scheme groups' data flows by source prefix, destination prefix, source prefix mask, destination prefix mask, source BGP AS, destination BGP AS, input interface, and output interface.
   - **Protocol-Port**: Indicates the scheme groups' data flows by IP protocol, source port number and destination port number when applicable.
   - **Source-Prefix**: Indicates the scheme groups' data flows by source prefix, source prefix mask, source BGP AS, and input interface.
9. Specify the values including **Cache**, **ActiveTimeout**, and **InactiveTimeout**.
10. On the Role property page, specify the device and interface roles to which the configuration policy applies.

For more information, see IP Service Activator online Help.

To apply NetFlow or MIB-based measurements to a policy target using Collector Parameters:

1. On the Domain dialog box, load the **ServiceAssurancePolicyTypes.policy** configuration policy.

   For information on loading a configuration policy file, see *IP Service Activator QoS User's Guide*.
2. On the Topology tab, right-click a policy target, select **Add Configuration Policy**, select **Service Assurance**, then select **Collector Parameters**.
3. In the Name field, enter a name for the configuration policy.
4. In the Description field, enter a description for the configuration policy.
5. From the Type list, select Cisco Netflow FlowCollector to allow device-generated statistics to be exported to Cisco Netflow Collector.
6. Under Collector Properties, specify values of the primary IP to which the statistics are exported. You may also specify the values of secondary IP.
7. On the Role property page, specify the device and interface roles to which the configuration policy applies.

For more information, see IP Service Activator online Help.

4
Setting Up IP Service Activator for Integration

This chapter provides information about modeling external systems and creating collectors in Oracle Communications IP Service Activator.

Modeling External Systems

IP Service Activator's SLA monitoring capability is provided through integrated third party reporting software. Before you configure IP Service Activator to support the third party reporting tool, it is important to understand the reporting tool's architecture and functionality.

To enable IP Service Activator's support for third party reporting software, you must model the reporting software's components as external systems through the IP Service Activator client. The type and number of components to be modelled depends on which reporting software you are using.

Types of External System

IP Service Activator supports NetFlow Flow Collector as an external system for reporting purposes.

As shown in Table 4-1, NetFlow works with a Cisco device.

Table 4-1 External Systems

External System Type	Reporting Tool	Statistics Type
NetFlow FlowCollector	Third party tool that reports on Cisco's NetFlow data	NetFlow

An external system does not have to be dedicated to collecting one particular data type.

Creating an External System

To create an external system:

1. On the System tab, select the External Systems folder and select **Add External System** from the folder's context menu.

   The External System dialog box appears.

2. Select the External System property page and specify values including **Name**, **Remarks**, **Type**, **Primary IP**, **Port**, **Secondary IP**, **Port** and **URL**.

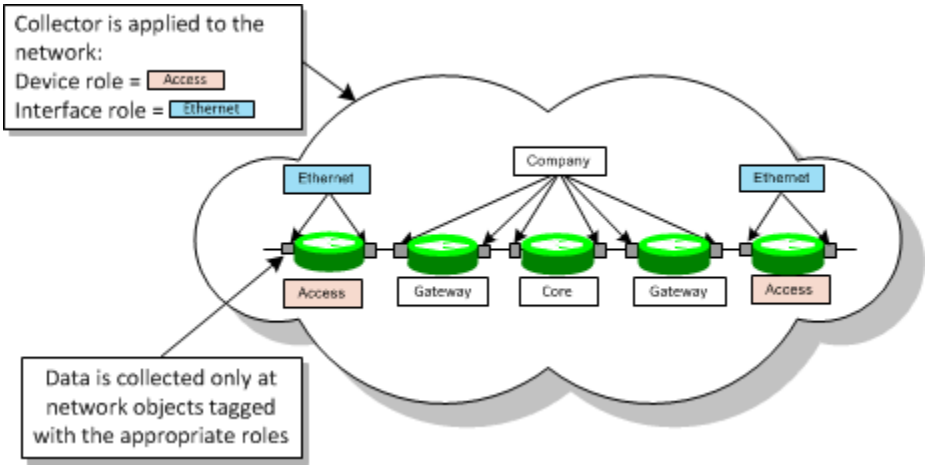
3. Select the Security property page, and select values including **Username** and **Login password**.

Creating Collectors

One or more collectors must be added to each device that you want to monitor. The collector links the device to the external system that performs data collection and aggregation. In IP Service Activator, the link between the device and the external system is called a collector parameter.

A collector behaves in a similar way to IP Service Activator's PHB groups in that it may be applied to any number of policy targets, and is inherited through IP Service Activator's policy inheritance hierarchy. Device and interface roles specify the points from which data is collected. Figure 4-1 illustrates this concept. For more information on defining and using roles, see *IP Service Activator User's Guide*.

Figure 4-1 Collectors and IP Service Activator Device Roles



Roles and Measurement Parameters

The roles that you associate with a collector depend on the type of data to be collected and from which devices.

For NetFlow and MIB-based measurement, the roles should be the same as those associated with at least one measurement parameter.

SAA is configured at device level and so only the device role that you associate with a collector is significant.

> **Note:**
>
> Though only device role is significant, you must also specify an interface role when you apply a collector that collects SAA data. Oracle recommends that you use the system-defined **Any Role**.

SAA measurement can be applied to an MPLS VPN or to a measurement-only VPN.

If SAA is applied to devices that participate in an MPLS VPN, the device role you associate with a collector depends on which connection you are measuring:

- For CE to CE, the device role must be **Access** or **Shadow**

  It is possible to monitor the CE to CE connection by applying SAA to the CE device, or by deploying shadow routers.

- For PE to PE, the device role is **Shadow**

  Shadow routers must always be deployed when monitoring the PE to PE connection.

- For PE to CE, data must be collected from devices tagged with two different roles: **Shadow** and **Access**.

  It is not possible to associate two device roles with a collector. Oracle recommends that you assign an additional user-defined role to the relevant Shadow and Access devices and associate this role with the collector.

If you have applied SAA to devices that do not participate in an MPLS VPN, the device role must be **Access** or **Shadow**, depending on which role you have assigned to the monitored devices.

> **Note:**
>
> If you apply a collector at domain level, the collector is inherited through IP Service Activator's logical inheritance line; that is, through customer, VPN, and site. Do not apply the collector at domain level unless you have created at least one customer and VPN, populated by the devices from which you wish to collect data.

When you have associated a collector with a policy target, the measurement component exports the relevant topology details to the collector. For example, if the collector is associated with a VPN, the component exports topology details for all devices participating in the VPN. If the topology changes, the measurement component exports the updated details to the collector.

Creating a Collector in IP Service Activator

If you are creating more than one collector, and if you are creating a Vista Plug-in for Netflow, ensure that you create the plug-in collector first.

To create a collector in IP Service Activator:

1. From a policy target's context menu, select **Add Collector Parameter**.

   The Collector Parameter dialog box appears.

2. On the Collector property page, specify values including **Name**, **Collector**, and **Driver Type**.

   Measurement data may be collected from Cisco devices only.

3. On the Role property page, specify the device and interface roles to which the collector applies.

   You must specify both a device and an interface role for the collector to be applied. If necessary, you can use the system-defined **Any Role** as the device or interface role which effectively acts as a wildcard.

5
Generic Exporter

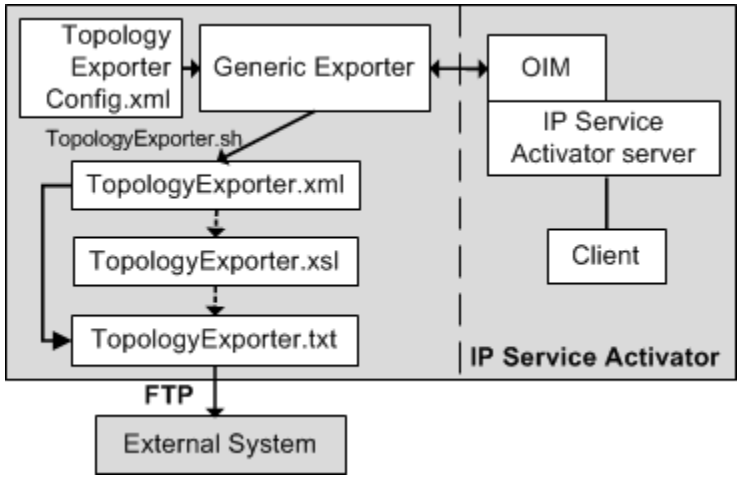
This chapter describes the Oracle Communications IP Service Activator Generic Exporter.

Generic Exporter Integration with IP Service Activator

Integration between IP Service Activator and the Generic Exporter occurs in the following way:

- IP Service Activator's Generic Exporter reads an XML export file (**TopologyExporterConfig.xml**) that identifies which data to collect for external reporting.
- This file is used to guide data collection from the IP Service Activator object model through the OSS Integration Manager (OIM) to create **TopologyExporter.xml**, which contains raw object model data.
- An XSL file (**TopologyExporter.xsl**) is then used to filter the **TopologyExporter.xml** file to create an export file.

Figure 5-1 Generic Exporter and IP Service Activator Integration



Key Integration Components

Table 5-1 provides a brief description of the key components used with the Generic Exporter.

Table 5-1 Key Integration Files

File	Description
TopologyExporterConfig.xml	When the Generic Exporter is invoked, it reads this configuration file that includes variables indicating: • IP Service Activator server to connect to. • Name of the output XML file to be used when extracting data from IP Service Activator. • Transformation directives indicating the number of XSLs to be called and what sequence they are to be called in. • Root tag to be used in XML output. • Rules specifying which objects, attributes and children are to be extracted and which are to be filtered out from the IP Service Activator object model.
TopologyExporter.xml	An object model file filtered by **TopologyExporter.xsl** to produce final output file **TopologyExporter.txt**.
TopologyExporter.xsl	An XML schema file used to transform **TopologyExporter.xml**. Executes filtering and formatting commands to localize data to meet output requirements.
TopologyExporter.txt	Contains filtered object model information to be transmitted by FTP to the Vista Provisioner.
Archive files	Whenever IP Service Activator creates a new **TopologyExporter.txt** file, the previous one is archived with the date and time of creation incorporated into the filename.

These files can be customized to meet the requirements of the third-party components that you are integrating IP Service Activator data with. For more information, see "Customizing Integration".

TopologyExporter.xml Filtering

The Generic Exporter filters the object model to process only the entities described in the table below. It exports an XML file containing a filtered version of the object model for both customer and network topology trees:

- Policy/Domain*/Customer*/VPN*/, Site*, ParameterSetInstance*
- Policy/Domain*/Network*/Device*, ParameterSetInstance*

Customizing Integration

A service provider can customize the Generic Exporter integration between IP Service Activator and a third party component by modifying the following files:

- **TopologyExporterConfig.xml**
- **TopologyExporter.xsl**
- **TopologyExporter.txt**

TopologyExporterConfig.xml

The content of the **TopologyExporter.xml** file is controlled by the **TopologyExporterConfig.xml** file. The Generic Exporter utility uses **TopologyExporterConfig.xml** to generate **TopologyExporter.txt**.

As needed, a service provider can modify the **TopologyExporterConfig.xml** file to customize the topology information exported.

The **TopologyExporterConfig.xml** file is located in the following directory:

*ServiceActivator_Home***/modules/TopologyExporterIntegrationModule/**

For a description of the fields included in the **TopologyExporterConfig.xml** file, see "TopologyExporterConfig.xml Fields ".

TopologyExporter.xsl

The **TopologyExporter.xsl** file applies formatting and filter rules to the **TopologyExporter.xml** file to generate a **TopologyExporter.txt** file. If **TopologyExporterConfig.xml** is modified, the filters in **TopologyExporter.xsl** should also be modified accordingly.

The **TopologyExporter.xsl** file is located in the following directory:

*ServiceActivator_Home***/modules/TopologyExporterIntegrationModule/**

The default transform file, **TopologyExporter.xsl**, applies the following filters to **TopologyExporter.xml** to generate the output **TopologyExporter.txt** file:

- **Domains**: Applies the domains filter.
- **Networks**: When a device is nested in multiple networks, only the immediate parent of the device appears in the output network folder.
- **Devices**: Must be managed and must not be virtual.
- **Interfaces and Sub-Interfaces**: Must have interface and parent device roles assigned, must have measurement parameter MIB2 selected, must have measurement parameter Juniper CoS selected for Juniper CoS data export.
- **PVCs**: Must have measurement parameter MIB2 selected.

TopologyExporter.txt

The **TopologyExporter.txt** file is derived from the **TopologyExporter.xml** file based on format instructions provided by the **TopologyExporter.xsl** file.

The **TopologyExporter.txt** file is deposited in the following directory:

*ServiceActivator_Home***/modules/TopologyExporterIntegrationModule/**

Invoking the Generic Exporter

The XML data export function of the Generic Exporter is run by using the **TopologyExporter.sh** script, which resides on the IP Service Activator server on which the Integration Manager is installed.

You can run it by using a manually entered command, or set it up by using a UNIX cron job to run automatically at appropriate intervals.

The command has the following syntax:

```
ServiceActivator_Home/modules/bin/TopologyExporter.sh username password
[ftp_server_name] [ftp_user_name] [ftp_pwd] [remote_directory_name]
```

Where *username* is the user ID used to access IP Service Activator, *password* is the password for *username*, *ftp_server_name* is the destination FTP server to send the output file to, *ftp_user_name* is the user ID for the destination FTP server, *ftp_pwd* is the password for *ftp_user_name*, and *remote_directory_name* is the destination FTP server directory in which to place **TopologyExporter.txt**.

Configuring the Generic Exporter SNMP Community String

The OSS Integration Manager does not pass the device SNMP write community string in open text (acting as a password) and therefore it is not available for **TopologyExporter.xsl** to process. A hard coded value of private is used for this value.

If your devices are configured to use a different value for the SNMP write community string, you can replace the string private by editing the **TopologyExporter.xsl** file.

If your devices are all configured with individual write community strings, you would have to implement a look up method which integrates with the **TopologyExporter.xsl** file. This is beyond the scope of this document.

Error Reporting

During the filtering of the **TopologyExporter.xml** file by the **TopologyExporter.xsl** file, if there is missing data or incorrect data, a message will be output to the Error console. The error will also be included in the XML output file as an XML comment. This allows you to confirm if any of the required data is missing or if the data is incorrectly filled.

A

TopologyExporterConfig.xml Fields

This appendix describes fields included in the default Oracle Communications IP Service Activator **TopologyExporterConfig.xml** files, located in the following directory:

*ServiceActivator_home***/modules/Config/**

TopologyExporterConfig.xml Fields

Table A-1 describes the configuration fields.

Table A-1 Configuration Fields

Type	Configuration Field	Description
ipsaServer	ipAddress	The IP address where the IP Service Activator Integration Manager is running.
ipsaServer	port	The port where the IP Service Activator Integration Manager is running.
primaryEntry	filenameToWrite	The filename of the XML export file.
transformations	--	Multiple transformations can be performed by surrounding each transformation with the <item> </item> element.
transformations	fileNameToRead	The filename that acts as the source document for the transformation. This entry is usually the filenameToWrite from the primaryEntry.
transformations	xslToCall	The filename of the XSL document that is used for the transformation.
transformations	filenameToWrite	The filename where the transformation is written to.
rootTagName	--	The root XML tag (top-level) that is inserted into the output XML document. The default is 'root'.

Table A-2 describes the output rules fields.

Table A-2 Output Rules Fields

Field Type	Output Rules Field	Description
startFromObject	--	The object type in IP Service Activator that the export starts the cascade from.
objectSubscription	--	Filters which objects are exported.
objectSubscription	subscribe	Identifies which object types to export. If all objects should be exported, insert object type 'all'.
objectSubscription	unsubscribe	Identifies which object types not to export.

Table A-2 (Cont.) Output Rules Fields

Field Type	Output Rules Field	Description
attributeSubscription	--	Filters which attributes to export.
attributeSubscription	subscribe	Identifies what attributes to export. If all attributes should be exported, then enter the single subscribe 'all'.
requiresAttributeValue	--	Filters which objects to export based on an attribute value.
requiresAttributeValue	objectType	Type of object the attribute is on.
requiresAttributeValue	attribute name	The name of the attribute.
requiresAttributeValue	attribute value	The value the attribute must have for the object to be exported.
requiresChild	--	Filters which objects to export based on associated child type.
requiresChild	objectType	Identifies type of object to export based on child type.
requiresChild	requires	The type of child object that is required for the above object type to be exported. For example, if the objectType is Customer and requires is set to VPN, only Customers that have VPNs will be exported.
ignoreChild	--	Filters which objects not to export based on whether they are the child of a given parent.
ignoreChild	objectType	Identifies the object type of the parent.
ignoreChild	ignore	Type of child object type that will not be exported based on the above parent type. For example, if the parent objectType is Customer and ignore is set to VPN, any VNP object with a parent of Customer will not be exported.
stopChildCascade	--	Stops cascading one level below a certain object type. For example, if stopChildCascade is given for object type Site, only direct children of the Site object are exported.
stopChildCascade	item	The object type to stop cascading on. **Note**: You still get one level of children below this object type.
requiresCollectorParameter	--	Filters which objects to export based on whether they are associated with a collector of a certain type.
requiresCollectorParameter	objectType	The object type, typically Device, that is associated with a collector type.
requiresCollectorParameter	collectorType	The collector type that the above object type is associated with.

Table A-2 (Cont.) Output Rules Fields

Field Type	Output Rules Field	Description
cascadeMeasurementParameter	--	This is not really a filter. Measurement parameters are not children of objects, but instead have targets to which they apply. To make Measurement Parameters appear as children, the exporter can cascade the xml definition of the MeasurementParameter down to the object which it targets. For example, if cascadeMeasurementParameter is applied to the object type Interface, the measurement parameter will appear under the interface object when it is exported.
cascadeMeasurementParameter	item	The object type that measurement parameters are cascaded on.