Monitoring Switches, Routers, and Firewalls with SNMP

SL1 version 10.1.4

Table of Contents

Introduction ... 3
What Switches, Routers, and Firewalls Can be Monitored "Out of the Box"? ... 3
Dynamic Applications ... 4
Discovery ... 5
PowerPacks ... 5
Discovering SNMP Routers, Switches, and Firewalls ... 6
Prerequisites ... 6
Creating an SNMP Credential ... 7
Creating an SNMP Credential for Monitoring Multiple VRFs ... 10
Discovery for SNMP-Enabled Routers, Switches, and Firewalls ... 11
Adding Devices Using Unguided Discovery ... 12
Running Discovery in the SL1 Classic User Interface ... 17
Interfaces and Networks ... 25
Viewing All Interfaces Discovered by the ScienceLogic Platform ... 25
Viewing Interfaces for a Single Device ... 29
Overview of Network Records ... 33
IPv4 Networks ... 33
Viewing the List of IPv4 Networks ... 34
Browsing a Network ... 36
Viewing Used and Unused IP Addresses in a Network ... 36
Viewing Devices Aligned with a Network ... 37
Viewing Interfaces Aligned with a Network ... 37
Device Relationships and Topology Collection ... 38
Overview of Device Relationships ... 38
Viewing the List of Device Relationships ... 39
Viewing the Relationships for a Single Device ... 41
The Device View Page ... 43
Layer-2 Topology Collection ... 44
CDP Topology Collection ... 45
LLDP Topology Collection ... 47
Layer-3 Topology Collection ... 49
Configuring Cisco IOS Devices for SNMP and Syslog ... 51
Configuring a Cisco IOS Router or Cisco IOS Switch to Use SNMPv1 and SNMPv2 ... 51
Configuring a Cisco IOS Firewall to Use SNMPv1 and SNMPv2 ... 52
Configuring Cisco IOS Devices for Syslog ... 53
Dynamic Applications for Routers, Switches, and Firewalls ... 55
PowerPack: Generic Switch/Router MIB Support ... 55
PowerPack: Alteon Base Pack ... 58
PowerPack: Cisco: Base Pack ... 60
PowerPack: Cisco IPSLA ... 77
PowerPack: Force 10 Base Pack ... 95
PowerPack: Juniper Base Pack ... 96
PowerPack: Netscreen Base Pack ... 103
Dashboards ... 106
PowerPack: Juniper Base Pack ... 106
Juniper Network ... 107

Chapter 1

Introduction

Overview

This manual describes how to monitor network devices (specifically routers, switches, and firewalls) with SL1. The instructions in this manual are intended for System Administrators and Network Administrators responsible for deploying SL1 and can also be applied to other network devices, like hubs and VPNs, that support SNMP.

The following sections describe the types of switches, routers, and firewalls that SL1 can monitor using the built-in discovery processes and Dynamic Applications that are delivered with SL1:

What Switches, Routers, and Firewalls Can be Monitored "Out of the Box"? 3

Dynamic Applications 4

Discovery 5

PowerPacks 5

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What Switches, Routers, and Firewalls Can be Monitored "Out of the Box"?

SL1 can discover and monitor most routers, switches, and firewalls using the built-in discovery processes and the default Dynamic Applications.

Dynamic Applications

SL1 can monitor most switches, routers, and firewalls using the default Dynamic Applications included with the product. You can install additional Dynamic Applications from the ScienceLogic portal at no cost.

Using the default Dynamic Applications, SL1 can monitor switches, routers, and firewalls from most vendors, either using a vendor-specific Dynamic Application and a vendor-specific MIB or a generic Dynamic Application for switches, routers, and firewalls using generic MIBs.

The default version of the SL1 includes vendor-specific Dynamic Applications for:

- Alteon
- Brocade
- Cisco
- Force 10
- Fortinet
- Foundry
- HP ProCurve
- Juniper
- Netscreen
- Nokia

The default version of the SL1 includes a PowerPack called ***Generic Switch/Router MIB Support*** that can collect details from devices for which there are no vendor-specific Dynamic Applications.

NOTE: If neither the vendor-specific Dynamic Applications nor the generic Dynamic Applications monitor one or more routers or switches in your network, you can create custom Dynamic Applications using SNMP and the the user interface. For details, see the manual ***Dynamic Application Development***.

Discovery

During initial discovery, SL1 can discover device information, interfaces, IP addresses, and networks and create topology maps for devices that support the following MIBs:

- BRIDGE-MIB
- CISCO-CDP-MIB
- CISCO-ETHERNET-FABRIC-EXTENDER-MIB
- CISCO-FCOE-MIB
- CISCO-PORT-CHANNEL-MIB
- CISCO-PROCESS-MIB
- CISCO-SYSTEM-EXT-MIB
- HOST-RESOURCES-MIB
- IF-MIB
- IP-MIB
- SYSTEM-MIB
- UCD-SNMP-MIB

PowerPacks

This manual describes content from the following PowerPack versions:

- Generic Switch/Router MIB Support, version 103
- Alteon Base Pack, version 1.4
- Cisco: Base Pack, version 212
- Cisco: IPSLA, version 102
- Force 10 Base Pack, version 1.3
- Juniper Base Pack, version 102
- Netscreen Base Pack, version 7.3.6

Chapter 2

Discovering SNMP Routers, Switches, and Firewalls

Overview

The following sections describe how to create SNMP credentials and discover SNMP network devices in SL1:

Prerequisites 6

Creating an SNMP Credential 7

Creating an SNMP Credential for Monitoring Multiple VRFs 10

Discovery for SNMP-Enabled Routers, Switches, and Firewalls 11

Adding Devices Using Unguided Discovery 12

Running Discovery in the SL1 Classic User Interface 17

Prerequisites

If you configure your network device to respond to SNMP requests from SL1, you can discover your devices as SNMP devices. When SL1 discovers a device as an SNMP device, SL1 will automatically collect data supplied by the SNMP agent.

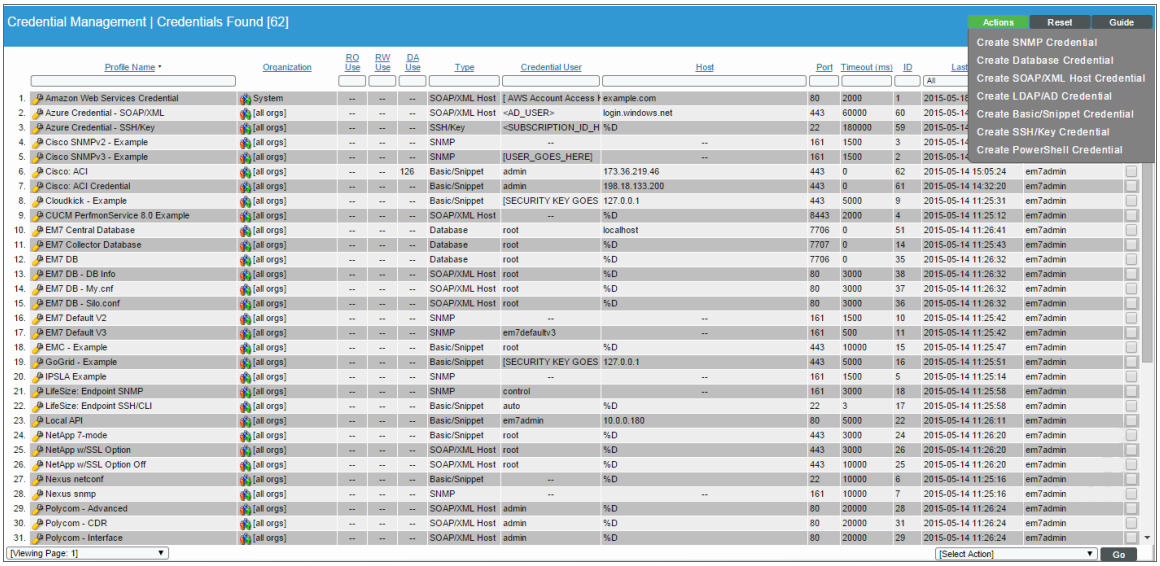
- To configure your devices to respond to SNMP requests, see the documentation for your devices.
- To use events in SL1, configure your devices to send syslog messages and traps to the SL1 system. See the documentation for your devices to determine how to configure syslog and trap forwarding.

Creating an SNMP Credential

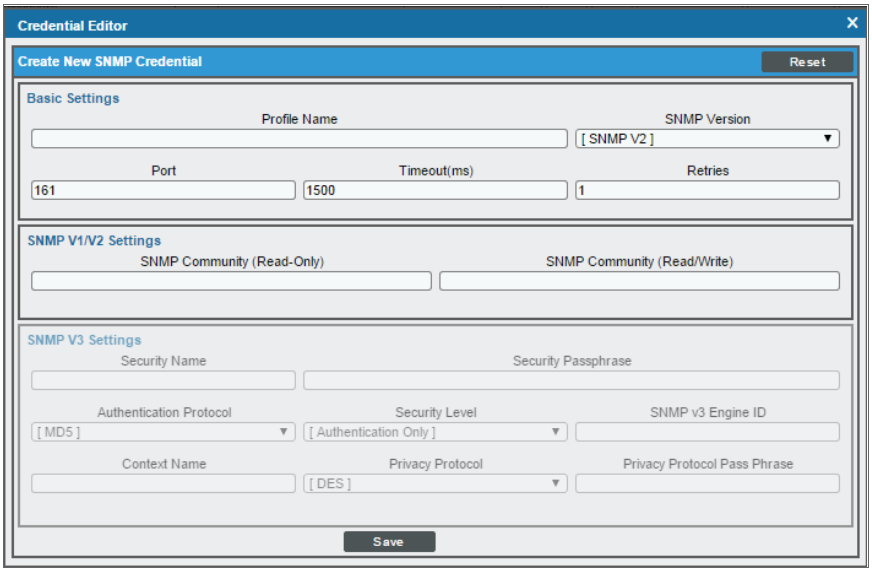
SNMP Credentials allow SL1 to access SNMP data on a managed device. SL1 uses SNMP credentials to perform discovery, run auto-discovery, and gather information from SNMP Dynamic Applications.

To create an SNMP credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).



2. Click the **[Actions]** button and select *Create SNMP Credential*. The **Credential Editor** page appears.



3. Supply values in the following fields:
    - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters.
    - ***SNMP Version***. SNMP version. Choices are *SNMP V1*, *SNMP V2*, and *SNMP V3*. The default value is *SNMP V2*.
    - ***Port***. The port SL1 will use to communicate with the external device or application. The default value is *161*.
    - ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the SNMP device. The default value is *1500*.
    - ***Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*.

    SNMP V1/V2 Settings

    These fields appear if you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field. The fields are inactive if you selected SNMP V3.

    - ***SNMP Community (Read-Only)***. The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read/Write)*** field.
    - ***SNMP Community (Read/Write)***. The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read Only)*** field.

    SNMP V3 Settings

    These fields appear if you selected *SNMP V3* in the ***SNMP Version*** field. These fields are inactive if you selected SNMP V1 or SNMP V2.

    - ***Security Name***. Name for SNMP authentication. This field is required.
    - ***Security Passphrase***. Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a ***Security Level*** that includes authentication.

- ***Authentication Protocol***. Select an authentication algorithm for the credential. This field is required. Choices are:
    - *MD5*. This is the default value.
    - *SHA*
    - *SHA-224*
    - *SHA-256*
    - *SHA-384*
    - *SHA-512*

NOTE: The *SHA* option is SHA-128.

- ***Security Level***. Specifies the combination of security features for the credentials. This field is required. Choices are:
    - *No Authentication / No Encryption*.
    - *Authentication Only*. This is the default value.
    - *Authentication and Encryption*.
- ***SNMP v3 Engine ID***. The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID.) This field is optional.
- ***Context Name***. A context is a mechanism within SNMPv3 (and AgentX) that allows you to use parallel versions of the same MIB objects. For example, one version of a MIB might be associated with SNMP Version 2 and another version of the same MIB might be associated with SNMP Version 3. For SNMP Version 3, specify the context name in this field. This field is optional.
- ***Privacy Protocol***. The privacy service encryption and decryption algorithm. This field is required. Choices are:
    - *DES*. This is the default value.
    - *AES-128*
    - *AES-192*
    - *AES-256*
- ***Privacy Protocol Passphrase***. Privacy password for the credential. This field is optional.

4. Click the **[Save]** button to save the new SNMP credential.
5. Repeat steps 1-4 for each SNMP-enabled device in your network that you want to monitor with SL1.

NOTE: When you define an SNMP Credential, SL1 automatically aligns the credential with all organizations of which you are a member.

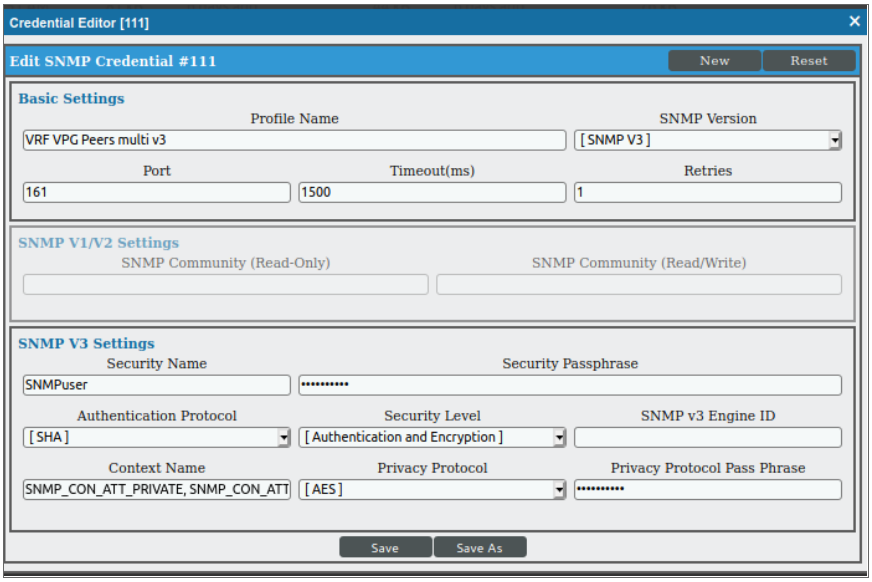
For more details on creating credentials, see the manual ***Discovery and Credentials***.

Creating an SNMP Credential for Monitoring Multiple VRFs

To monitor multiple VRFs on your Nexus devices, you must create the SNMP credential with SNMP v2 or SNMPv3 settings and then manually align the "Cisco: VRF BGP Peers" Dynamic Application.

To create the SNMP credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** button and select *Create SNMP Credential*. The **Credential Editor** page appears.



3. Supply values in the following fields:
   - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters.
   - ***SNMP Version***. SNMP version. Select *SNMP V2* or *SNMP V3*. SNMP v1 is not supported for monitoring multiple VRFs.
   - ***Port***. The port SL1 will use to communicate with the external device or application. The default value is *161*.
   - ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the SNMP device. The default value is *1500*.
   - ***Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*.

SNMP V2 Settings

Supply values in the following field if you selected *SNMP V2* in the ***SNMP Version*** field:

- ***SNMP Community (Read-Only)***. Type the SNMP community string (password) required for read-only access of SNMP data on the remote device or application. If you are specifying more than one community string, separate them with a comma.

SNMP V3 Settings

Supply values in the following fields if you selected *SNMP V3* in the ***SNMP Version*** field:

- ***Security Name***. Name for SNMP authentication. This field is required.
- ***Security Passphrase***. Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a ***Security Level*** that includes authentication.
- ***Authentication Protocol***. Select *SHA*.

NOTE: The *SHA* option is SHA-128.

- ***Security Level***. Select *Authentication and Encryption*.
- ***Context Name***. Specify the context(s) in this field. If you are adding more than one, separate each with a comma.
- ***Privacy Protocol***. Select *AES-128*.
- ***Privacy Protocol Pass Phrase***. Privacy password for the credential. This field is optional.

4. Click the **[Save]** button to save the new SNMP credential.

To align the "Cisco: VRF BGP Peers" Dynamic Application:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Locate your Cisco device and click its wrench icon ( ).
3. In the **[Collections]** tab, click the **[Actions]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears.
4. In the ***Dynamic Applications*** field, select the "Cisco: VRF BGP Peers" Dynamic Application.
5. In the ***Credentials*** field, select the SNMP credential you just created.
6. Click the **[Save]** button.

Discovery for SNMP-Enabled Routers, Switches, and Firewalls

To maximize the data that can be collected from SNMP-enabled routers and switches, ensure that your devices include the following MIBs:

- BRIDGE-MIB
- CISCO-CDP-MIB
- CISCO-ETHERNET-FABRIC-EXTENDER-MIB
- CISCO-FCOE-MIB
- CISCO-PORT-CHANNEL-MIB
- CISCO-PROCESS-MIB
- CISCO-SYSTEM-EXT-MIB
- HOST-RESOURCES-MIB
- IF-MIB
- IP-MIB
- SYSTEM-MIB
- UCD-SNMP-MIB

During initial discovery, SL1 automatically performs the following actions to gather information from each SNMP-enabled router and switch:

- Uses the SYSTEM-MIB to retrieve a system description, SysObject ID, system uptime, system contact, system name, and system location
- Uses the IF-MIB to retrieve information about all network interfaces on the device
- Uses the IP-MIB to determine the IP address and netmask associated with each interface
- Uses the retrieved SysObject ID to assign a device class to each device
- Assigns a device ID, a device name, a primary IP address for use in SL1, and a primary credential
- Checks each discovered device against the list of already-defined Dynamic Applications. SL1 searches each discovered device to find "discovery objects" and aligns devices with the appropriate Dynamic Application(s).
- Immediately after the initial discovery session is completed, SL1 will use the aligned Dynamic Applications to collect additional data from devices.
- Shortly after the initial discovery session, SL1 uses internal processes to create network records for each IP address and interface.
- Shortly after the initial discovery session, SL1 uses the BRIDGE-MIB and the CISCO-CDP-MIB to create topology relationships for routers and switches.

For details on discovery, see the manual ***Discovery and Credentials***.

Adding Devices Using Unguided Discovery

Instead of running a Universal Discovery for a specific discovery type, you can run an "unguided" discovery to find a range of devices using core credentials such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or PowerShell credentials.

To run an unguided discovery:

1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:
2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears.
4. Complete the following fields:

    - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
    - ***Description***. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab. Optional.
    - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.

5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:
6. On the **Credentials** page, you can optionally do one of the following:

    - If the credential you need is not in the list, click the **[Create New]** button to open the **Create Credential** window, where you can specify the name and organization for the credential, the third-party username and password, and other data such as Cloud Type and Proxy information. Click **[Save & Close]** to save the credential and return to the **Credentials** page of the **Add Devices** wizard. For more information on creating new credentials, see the ***Discovery and Credentials*** manual.
    - To edit a credential on the **Credentials** page, click the **[Actions]** button ( ) for the credential, select *Edit*, and edit that credential as needed. Click the **[Save & Close]** button on the **Edit Credential** window to save your updates. For more information on editing credentials, see the ***Discovery and Credentials*** manual.

7. On the **Credentials** page of the **Add Devices** wizard, select one or more credentials to allow SL1 to access a device's SNMP data and click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:
8. Complete the following fields:

    - ***List of IPs/Hostnames***. Provide a list of IP addresses, hostnames, or fully-qualified domain names for SL1 to scan during discovery. This field is required. In this field, you can enter a combination of one or more of the following:

        - One or more *single IPv4 addresses* separated by commas and a new line. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20."
        - One or more *ranges of IPv4 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 – 10.20.30.254".

- One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
- One or more *ranges of IPv6 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0:0-2001:DB8:0:0:0:0:0:0003".
- One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0:0/117".
- One or more hostnames (fully-qualified domain names). Separate each item in the list with a comma.

TIP: You can also click the **[Upload File]** button to upload a comma-separated list of IPs.

- ***Which collector will monitor these devices?***. Select an existing collector to monitor the discovered devices. Required.
- ***Run after save***. Select this option to run this discovery session as soon as you click **[Save and Close]**.
- ***Advanced options***. Click the down arrow icon ( ) to access additional discovery options.

  In the **Advanced options** section, complete the following fields as needed:

  - ***Initial Scan Level***. For this discovery session only, specifies the data to be gathered during the initial discovery session. The options are:
    - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface of SL1.
    - *1. Model Device Only*. Discovery will discover if the device is up and running and if so, collect the make and model of the device. SL1 will then generate a device ID for the device so it can be managed by SL1.
    - *2. Initial Population of Apps*. Discovery will search for Dynamic Applications to associate with the device. The discovery tool will attempt to collect data for the aligned Dynamic Applications. Discovery will later retrieve full sets of data from each Dynamic Application. Discovery will also perform *1. Model Device Only* discovery.
    - *3. Discover SSL Certificates*. Discovery will search for SSL certificates and retrieve SSL data. Discovery will also perform *2. Initial Population of Apps* and *1. Model Device Only*.
    - *4. Discover Open Ports*. Discovery will search for open ports. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

NOTE: If your system includes a firewall and you select *4. Discover Open Ports*, discovery might be blocked and/or might be taxing to your network.

    - *5. Advanced Port Discovery*. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

NOTE: If your system includes a firewall and you select *5. Advanced Port Discovery*, some devices might remain in a pending state (purple icon) for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

- *6. Deep Discovery*. Discovery will use nmap to retrieve the operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *3. Discover SSL Certificates, 2. Initial Population of Apps*, and *1. Model Device Only*.

NOTE: For devices that don't support SNMP, option *6. Deep Discovery* allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable". Note that option *6. Deep Discovery* is compute-intensive.

- ***Scan Throttle***. Specifies the amount of time a discovery process should pause between each specified IP address (specified in the ***IP Address/Hostname Discovery List*** field). Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for SL1.
  - *Disabled*. Discovery processes will not pause.
  - *1000 Msec to 10000 Msec*. A discovery process will pause for a random amount of time between half the selected value and the selected value.
- ***Port Scan All IPs***. For the initial discovery session only, specifies whether SL1 should scan all IP addresses on a device for open ports. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for SL1.
  - *Enabled*. SL1 will scan all discovered IP addresses for open ports.
  - *Disabled*. SL1 will scan only the primary IP address (the one used to communicate with SL1) for open ports.
- ***Port Scan Timeout***. For the initial discovery session only, specifies the length of time, in milliseconds, after which SL1 should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - Choices between 60 to 1,800 seconds.

- ***Scan Ports***. Specify a list of ports to scan, separated by colons (:). The default is *21:22:25:80:136*.

- ***Interface Inventory Timeout (ms)***. Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).

  - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).

  - If you specify a value in this field and do not apply a device template to this discovery session, the ***Interface Inventory Timeout*** setting in the **Device Thresholds** page (Registry > Devices > Device Manager > wrench icon > Thresholds) is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).

- ***Maximum Allowed Interfaces***. Specifies the maximum number of interfaces per devices. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.

  - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page.

  - If you specify a value in this field and do not apply a device template to this discovery session, the ***Maximum Allowed Interfaces*** setting in the **Device Thresholds** page is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page.

- ***Bypass Interface Inventory***. Specifies whether or not the discovery session should discover network interfaces.

  - *Selected*. SL1 will not attempt to discover interfaces for each device in the discovery session. For each discovered device, the ***Bypass Interface Inventory*** checkbox on the **Device Investigator [Settings]** tab will be selected.

  - *Not Selected*. SL1 will attempt to discover network interfaces, using the ***Interface Inventory Timeout*** value and ***Maximum Allowed Interfaces*** value.

- ***Discover Non-SNMP***. Specifies whether or not SL1 should discover devices that don't respond to SNMP requests.

  - *Selected*. SL1 will discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** field. These devices will be discovered as "pingable" devices.
  - *Not Selected*. SL1 will not discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** fields.

- ***Model Devices***. Determines whether or not the devices that are discovered with this discovery session can be managed through SL1. Choices are:
  - *Enabled*. When a device is modeled, SL1 creates a device ID for the device; you can then access the device through the **Device Manager** page and manage the device in SL1.
  - *Disabled*. If a device is not modeled, you cannot access the device through the **Device Manager** page, and you cannot manage the device in SL1. However, each discovered device will still appear in the Discovery Session logs. For each discovered device, the discovery logs will display the IP address and device class for the device. This option is useful when performing an initial discovery of your network, to determine which devices you want to monitor and manage with SL1. For the amount of time specified in the ***Device Model Cache TTL (h)*** field, a user can manually model the device from the **Discovery Session** window.
- ***Enable DHCP***. Specifies whether or not the specified range of IPs and hostnames use DHCP.
  - *Selected*. SL1 will perform a DNS lookup for the device during discovery and each time SL1 retrieves information from the device.
  - *Not Selected*. SL1 will perform normal discovery.
- ***Device Model Cache TTL (h)***. Amount of time, in hours, that SL1 stores information about devices that are discovered but not modeled, either because the ***Model Devices*** option is not enabled or because SL1 cannot determine whether a duplicate device already exists. The cached data can be used to manually model the device from the **Discovery Session** window.
- ***Log All***. Specifies whether or not the discovery session should use verbose logging. When you select verbose logging, SL1 logs details about each IP address or hostname specified in the ***IP Address/Hostname Discovery List*** field, even if the results are "No device found at this address."
  - *Selected*. This discovery session will use verbose logging.
  - *Not Selected*. This discovery session will not use verbose logging.
- ***Apply Device Template***. As SL1 discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in SL1. For more information on device templates, see the manual on ***Device Groups and Device Templates***.

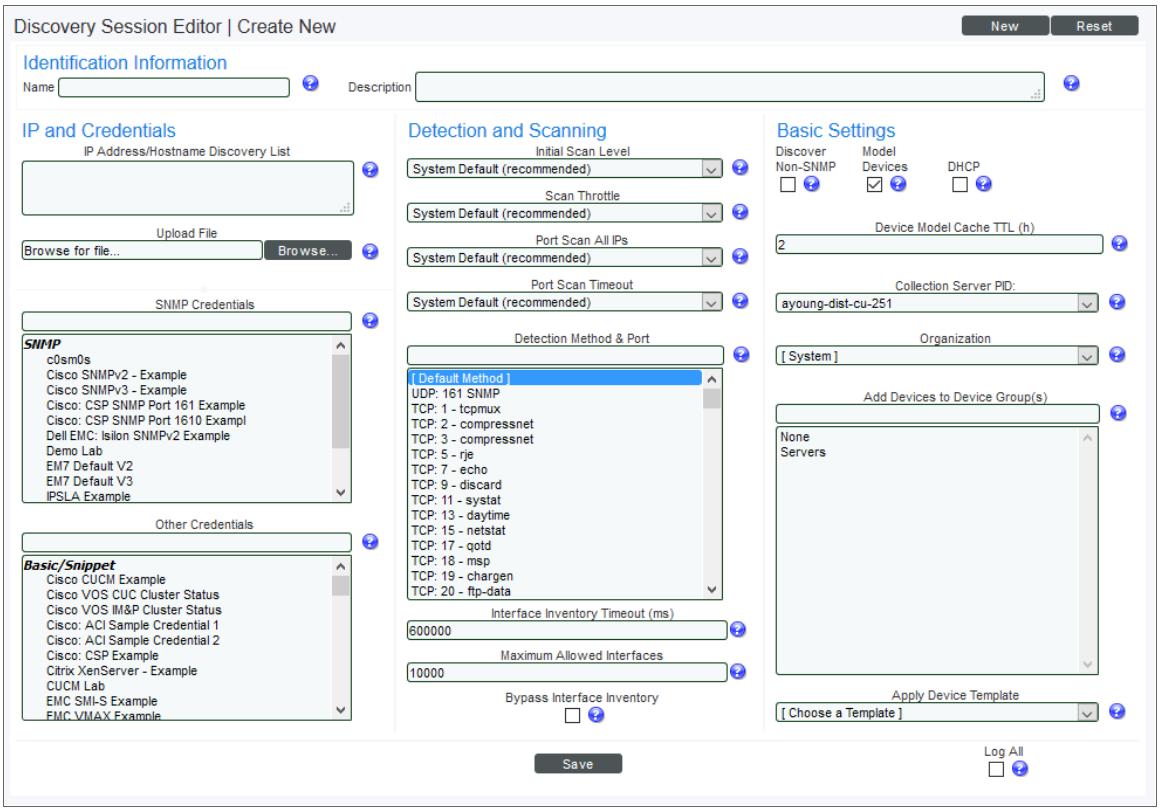
9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device:

Running Discovery in the SL1 Classic User Interface

To perform a discovery session for one IP address, multiple IP addresses, or a range of IP addresses on the **Classic Discovery** page:

NOTE: To discover all the devices in your network, you must first know the range of IP addresses used in your network. If you need help, ask your network administrator.

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. In the **Discovery Control Panel**, click **[Create]**. The **Discovery Session Editor** page appears:



3. Supply values in the following fields:

   - ***Name***. Type a name for the discovery session. This name is displayed in the list of discovery sessions in the **Discovery Control Panel** page.
   - ***Description***. Optionally, type a description of the discovery session.

- ***IP Address/Hostname Discovery List***. Provide a list of IP addresses or fully-qualified domain names for SL1 to scan during discovery. In this field, you can enter a combination of one or more of the following:

NOTE: Instead of manually entering a list of IP addresses and hostnames, you can upload a file that contains the list of IP addresses and hostnames. See the description of the ***Upload File*** field.

  - One or more *single IPv4 addresses* separated by commas. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20.30.3".
  - One or more *ranges of IPv4 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 – 10.20.30.254".
  - One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
  - One or more *ranges of IPv6 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0:0-2001:DB8:0:0:0:0:0:0003".
  - One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0:0/117".
  - One or more hostnames (fully-qualified domain names). Separate each item in the list with a comma.

CAUTION: If you enter both the hostname and IP address of the same devices, SL1 will discover two duplicate devices.

NOTE: The following types of notation are **not supported**: IPv4 netmask with comma notation (e.g., 192.168.168.0,24); a list of single IPv6 addresses, separated by comma.

NOTE: SL1 will display an error if your discovery session exceeds the maximum size for optimum performance. SL1 will display a warning message if your discovery session includes 100 or more IP addresses. The warning message will tell you that discovery with more than 100 IP addresses might "take a long time to discover".

- ***Upload File***. Instead of manually entering a list of IP addresses and hostnames in the ***IP Address/Hostname Discovery List*** field, you can upload a file that contains a list of IP addresses and hostnames. The IP addresses and hostnames in the file must be in a format that is allowed for the ***IP Address/Hostname Discovery List*** field. Each address or range of addresses in the file must be separated by a newline character instead of a comma. You can browse to the file and then select it. After uploading the file, the ***IP Address/Hostname Discovery List*** field will display the IP addresses and hostnames from the file.

- ***SNMP Credentials***. A community string that allows SL1 to access a device's SNMP data. SNMP credentials are defined in the **Credential Management** page (System > Manage > Credentials). If you want to retrieve SNMP data from one or more devices, you must select one or more working SNMP credentials in this field. You can select multiple credentials from this field. SL1 will try each selected credential when discovering devices and retrieving device data.
- ***Other Credentials***. A username and password pair (among other fields) that allows SL1 to access a device's database data, SOAP data, XML data, WMI data, WBEM data, or data that is monitored with a Snippet Dynamic Application. These credentials are defined in the **Credential Management** page (System > Manage > Credentials). You can select multiple credentials from this field. SL1 will try each selected credential when searching for Dynamic Applications to align with each discovered device.

NOTE: You can use the field at the top of the ***SNMP Credentials*** field and the ***Other Credentials*** field to filter the list of credentials. If you enter an alpha-numeric string in the field, the ***SNMP Credentials*** field or the ***Other Credentials*** field will include only credentials that match the string.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***SNMP Credentials*** field and the ***Other Credentials*** field.

- ***Initial Scan Level***. For this discovery session only, specifies the data to be gathered during the initial discovery session. The options are:
    - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
    - *0. Model Device Only*. Discovery will discover if the device is up and running and if so, collect the make and model of the device. SL1 will then generate a device ID for the device so it can be managed by SL1.
    - *1. Initial Population of Apps*. Discovery will search for Dynamic Applications to associate with the device. The discovery tool will attempt to collect data for the aligned Dynamic Applications. Discovery will later retrieve full sets of data from each Dynamic Application. Discovery will also perform *0. Model Device Only* discovery.
    - *2. Discover SSL Certificates*. Discovery will search for SSL certificates and retrieve SSL data. Discovery will also perform *1. Initial Population of Apps* and *0. Model Device Only*.
    - *3. Discover Open Ports*. Discovery will search for open ports. Discovery will also perform *2. Discover SSL Certificates*, *1. Initial Population of Apps*, and *0. Model Device Only*.

NOTE: If your system includes a firewall and you select *3. Discover Open Ports*, discovery might be blocked and/or might be taxing to your network.

- *4. Advanced Port Discovery*. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *2. Discover SSL Certificates*, *1. Initial Population of Apps*, and *0. Model Device Only*.

NOTE: If your system includes a firewall and you select *4. Advanced Port Discovery*, some devices might remain in a pending state (purple icon) for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

- *5. Deep Discovery*. Discovery will use nmap to retrieve the operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *2. Discover SSL Certificates, 1. Initial Population of Apps*, and *0. Model Device Only*.

NOTE: For devices that don't support SNMP, option *5. Deep Discovery* allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable". Note that option *5. Deep Discovery* is compute-intensive.

- ***Scan Throttle***. Specifies the amount of time a discovery process should pause between each specified IP address (specified in the ***IP Address/Hostname Discovery List*** field). Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - *Disabled*. Discovery processes will not pause.
  - *1000 Msec to 10000 Msec*. A discovery process will pause for a random amount of time between half the selected value and the selected value.
- ***Port Scan All IPs***. For the initial discovery session only, specifies whether SL1 should scan all IP addresses on a device for open ports. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - *0. Disabled*. SL1 will scan only the primary IP address (the one used to communicate with SL1) for open ports.
  - *1. Enabled*. SL1 will scan all discovered IP addresses for open ports.

- ***Port Scan Timeout***. For the initial discovery session only, specifies the length of time, in milliseconds, after which SL1 should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are:
    - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
    - Choices between 60,000 to 1,800,000 milliseconds.
- ***Detection Method & Port***. During discovery, SL1 will scan the list of ports selected in this field to determine if the range of devices is up and running and which ports are open on each discovered device. If a device does not respond to SNMP or ICMP, SL1 uses an open port to collect availability data for that device. If you are not sure which ports are used by the range of devices, select the entry *Default Method*. SL1 will check ICMP (ping), FTP, SSH, Telnet, SMTP, and HTTP ports.

NOTE: You can use the field at the top of the ***Detection Method & Port*** field to filter the list of ports. If you enter an alpha-numeric string in the field, the ***Detection Method & Port*** field will include only ports that match the string.

- ***Interface Inventory Timeout (ms)***. Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
    - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
    - If you specify a value in this field and do not apply a device template to this discovery session, the ***Interface Inventory Timeout*** setting in the **Device Thresholds** page (Registry > Devices > Device Manager > wrench icon > Thresholds) is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
- ***Maximum Allowed Interfaces***. Specifies the maximum number of interfaces per devices. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
    - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page.
    - If you specify a value in this field and do not apply a device template to this discovery session, the ***Maximum Allowed Interfaces*** setting in the **Device Thresholds** page is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page.

- ***Bypass Interface Inventory***. Specifies whether or not the discovery session should discover network interfaces.
    - *Selected*. SL1 will not attempt to discover interfaces for each device in the discovery session. For each discovered device, the ***Bypass Interface Inventory*** checkbox in the **Device Properties** page will be selected.
    - *Not Selected*. SL1 will attempt to discover network interfaces, using the ***Interface Inventory Timeout*** value and ***Maximum Allowed Interfaces*** value.

NOTE: If a device has already been discovered and then is rediscovered through the **Discovery Session Editor** page, the ***Bypass Interface Inventory.*** checkbox in the **Device Properties** page will retain its previous value, regardless of what is selected in the **Discovery Session Editor** page.

- ***Discover Non-SNMP Devices***. Specifies whether or not SL1 should discover devices that don't respond to SNMP requests.
    - *Selected*. SL1 will discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** field. These devices will be discovered as "pingable" devices.
    - *Not Selected*. SL1 will not discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** fields.
- ***Model Devices***. Determines whether or not the devices that are discovered with this discovery session can be managed through SL1. Choices are:
    - *Enabled*. When a device is modeled, SL1 creates a device ID for the device; you can then access the device through the **Device Manager** page and manage the device in SL1.
    - *Disabled*. If a device is not modeled, you cannot access the device through the **Device Manager** page, and you cannot manage the device in SL1. However, each discovered device will still appear in the Discovery Session logs. For each discovered device, the discovery logs will display the IP address and device class for the device. This option is useful when performing an initial discovery of your network, to determine which devices you want to monitor and manage with SL1. For the amount of time specified in the ***Device Model Cache TTL (h)*** field, a user can manually model the device from the **Discovery Session** window.
- ***DHCP***. Specifies whether or not the specified range of IPs and hostnames use DHCP.
    - *Selected*. SL1 will perform a DNS lookup for the device during discovery and each time SL1 retrieves information from the device.
    - *Not Selected*. SL1 will perform normal discovery.
- ***Device Model Cache TTL (h)***. Amount of time, in hours, that SL1 stores information about devices that are discovered but not modeled, either because the ***Model Devices*** option is not enabled or because SL1 cannot determine whether a duplicate device already exists. The cached data can be used to manually model the device from the **Discovery Session** window.

- ***Collection Server PID***. This field contains a list of all Data Collectors on the network. Select the Data Collector that is local or closet to the devices to be discovered.
    - For SL1 appliances, only the name of the appliance will appear in this field.

NOTE: After initial discovery, each device will use the collector group that contains this Data Collector for collection and rediscovery.

- ***Organization***. This field contains a list of all organizations defined in SL1. Devices discovered during the discovery session will be assigned to the selected organization.

NOTE: Make sure you have the desired organization created and selected before running the discovery process. This field assigns all devices and networks in the specified IP range to a single organization. However, you can later assign individual devices and networks to different organizations.

- ***Add Devices to Device Group(s)***. When SL1 discovers a device in the IP discovery list, that device is added to each selected device group. You can select one or more device groups from a list of device groups in SL1 that have "Discovery" selected in the ***Visibility*** field. For more information on device groups, see the manual on ***Device Groups and Device Templates***.

NOTE: You can use the field at the top of the ***Add Devices to Device Group(s)*** field to filter the list of device groups. If you enter an alpha-numeric string in the field, the ***Add Devices to Device Group(s)*** field will include only device groups that match the string.

- ***Apply Device Template***. As SL1 discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in SL1. For more information on device templates, see the manual on ***Device Groups and Device Templates***.
- ***Log All***. Specifies whether or not the discovery session should use verbose logging. When you select verbose logging, SL1 logs details about each IP address or hostname specified in the ***IP Address/Hostname Discovery List*** field, even if the results are "No device found at this address."
    - *Selected*. This discovery session will use verbose logging.
    - *Not Selected*. This discovery session will not use verbose logging.

4. Click the **[Save]** button **to save the discovery session**. Close the **Discovery Session Editor** page.
5. In the **Discovery Control Panel** page, click the **[Reset]** button. The new discovery session will appear in the **Session Register** pane.
6. To launch the new discovery session, click its ***Queue this Session*** icon ( ).
7. If no other discovery sessions are currently running, the session will be executed immediately. If another discovery session is currently running, your discovery session will be queued for execution.

Chapter 3

Interfaces and Networks

Overview

The following sections describe how to view the interfaces and networks for the routers, switches, and firewalls that SL1 discovers:

Viewing All Interfaces Discovered by the ScienceLogic Platform *25*

Viewing Interfaces for a Single Device *29*

Overview of Network Records *33*

IPv4 Networks *33*

Viewing the List of IPv4 Networks *34*

Browsing a Network *36*

Viewing Used and Unused IP Addresses in a Network *36*

Viewing Devices Aligned with a Network *37*

Viewing Interfaces Aligned with a Network *37*

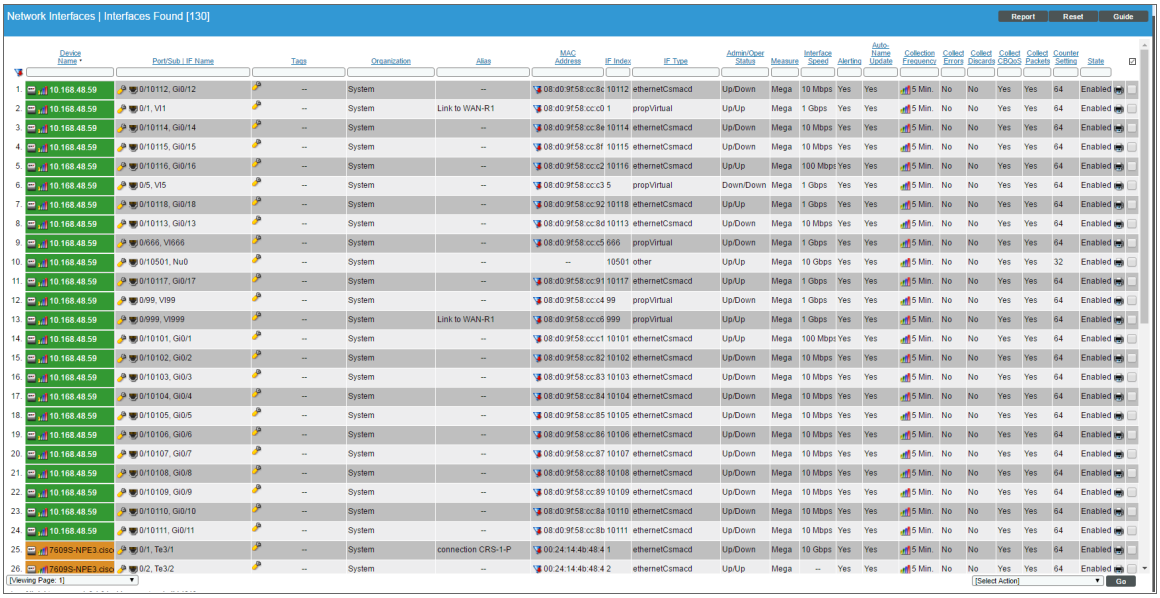
Viewing All Interfaces Discovered by the ScienceLogic Platform

During discovery, SL1 discovers all interfaces on each discovered device. The list of all interfaces is displayed in the **Network Interfaces** page.

The **Network Interfaces** page allows you to view a list of all interfaces, view details about each interface, define a monitoring policy for an interface, and view bandwidth reports for each interface.

To view a list of all interfaces discovered by SL1:

1. Go to the **Network Interfaces** page (Registry > Networks > Interfaces).
2. The **Network Interfaces** page displays a list of all network interfaces discovered by SL1.



3. The **Network Interfaces** page displays the following for each interface:

TIP: To sort the list of interfaces, click on a column heading. The list will be sorted by the column value, in ascending order. To sort the list by descending order, click the column heading again.

- ***Device Name***. Name of the device where the interface resides.
- ***Port/Sub***. Port and sub-port (if applicable) of the interface.
- ***IF Name***. The name of the network interface. The auto-name, generated by SL1, is device_name:interface_number. You can define a different name in the **Interface Properties** page.
- ***Tags***. Displays a comma-delimited list of descriptive tags that have been manually defined for the interface. Interface tags are used to group interfaces in an IT service policy. To add or edit the tags for an interface, click its wrench icon (). In the **Edit Network Interface Tags** modal that appears, supply a comma-delimited list of tags in the ***Tags*** field, and then click the **[Save]** button.
- ***Organization***. Organization associated with the network interface. This can be the organization associated with the device where the interface resides, or it can be an organization that has emissary rights to the interface.
- ***Alias***. User-defined name assigned to the interface.
- ***MAC Address***. A unique number that identifies the interface. MAC Addresses are defined by the hardware manufacturer.

- ***IF Index***. A unique number (greater than zero) that identifies each interface on a device. These numbers are defined within the device.
- ***IF Type***. A string that describes the type of interface, as defined by the standards group Internet Assigned Numbers Authority (IANA).
- ***Status***. Consists of two parts:
    - *Administration Status*. Specifies how the network interface has been configured on the device. Can be one of the following:
        - Up. Network interface has been enabled.
        - Down. Network interface has been disabled.
    - *Operation Status*. Specifies current state of the network interface. Can be one of the following:
        - Up. Network interface is transmitting and receiving data.
        - Down. Network interface cannot transmit or receive data.

NOTE: SL1 generates an event when a network interface has an administrative status of "up" and an operation status of "down".

- ***Measure***. Unit of measurement for bandwidth reports for the interface. The choices are:
    - Mega
    - Giga
    - Kilo
    - Tera
    - Peta
- ***Interface Speed***. The number of megabits per second that can pass through the network interface.
- ***Alerting***. Specifies whether or not events will be generated for the selected interfaces.
    - *Yes*. SL1 monitors the network interface and generates events when the required conditions are met.
    - *No*. SL1 monitors the network interface, but events are not generated for the interface.
- ***Auto-Name Update***. Specifies whether or not SL1 will update and/or overwrite the interface name during auto-discovery.
    - *Yes*. SL1 can update and/or overwrite the interface name during auto-discovery.
    - *No*. SL1 will not update and/or overwrite the interface name during auto-discovery.

- ***Collection Frequency***. When you define a monitoring policy for an interface, you must specify how frequently you want SL1 to collect data from the interface. Your choices are every:
    - 1 Minute
    - 5 Minutes
    - 10 Minutes
    - 15 Minutes
    - 30 Minutes
    - 60 Minutes
    - 120 Minutes
- ***Collect Errors***. Specifies whether or not SL1 will collect data about packet errors on the interface. Packet errors can occur when packets are lost due to network outages or faulty adapter hardware. Your choices are:
    - *Yes*. SL1 will collect data on packet errors that occur on the interface.
    - *No*. SL1 will not collect data on packet errors that occur on the interface.
- ***Collect Discards***. Specifies whether or not SL1 will collect data about interface discards. Discards can occur when an interface receives more traffic than it can handle. Discards can also occur when an interface has been specifically configured to discard packets. For example, a network administrator might configure a router's interface to discard packets from an unauthorized IP. Your choices are:
    - *Yes*. SL1 will collect data about packet discards that occur on the interface.
    - *No*. SL1 will not collect data about packet discards that occur on the interface.
- ***Collect CBQoS***. Specifies whether SL1 will collect CBQoS (Class-Based Quality-of-Service) data for this interface. This column appears only if you have enabled the field ***Enable CBQoS Collection*** in the **Behavior Settings** page (System > Settings > Behavior). If ***Collect CBQoS*** is enabled for an interface, SL1 will display the collected CBQoS data in Device Performance reports associated with the device that contains this interface. Choices are:
    - *Yes*. SL1 will collect CBQoS data for this interface.
    - *No*. SL1 will not collect CBQoS data for this interface.

    For more information about CBQoS, see the ***Infrastructure Health*** manual.
- ***Collect Packets***. Specifies whether SL1 will collect network traffic data, in packets, for this interface. If ***Collect Packets*** is enabled for an interface, SL1 will display the collected data in Device Performance reports associated with the device that contains this interface. Choices are:
    - *Yes*. SL1 will collect packet data for this interface.
    - *No*. SL1 will not collect packet data for this interface.
- ***Counter Setting***. Specifies whether the interface uses a 32-bit counter or a 64-bit counter to measure bandwidth on the interface.

NOTE: If an interface has a status of "down" during initial discovery, SL1 will discover the interface but assign the interface the default Counter Setting of "32". During re-discovery or nightly auto-discovery, SL1 will update Counter Setting to "64" if applicable.

- ***State***. Specifies whether SL1 monitors the network interface and collects data about the network interface for reports. Can be either *Enabled* or *Disabled*.
- ***Edit Date***. Date and time the monitoring policy for the interface was created or last edited. If the interface is using the default monitoring policy, the edit date reflects the date that the interface was discovered by SL1.

Viewing Interfaces for a Single Device

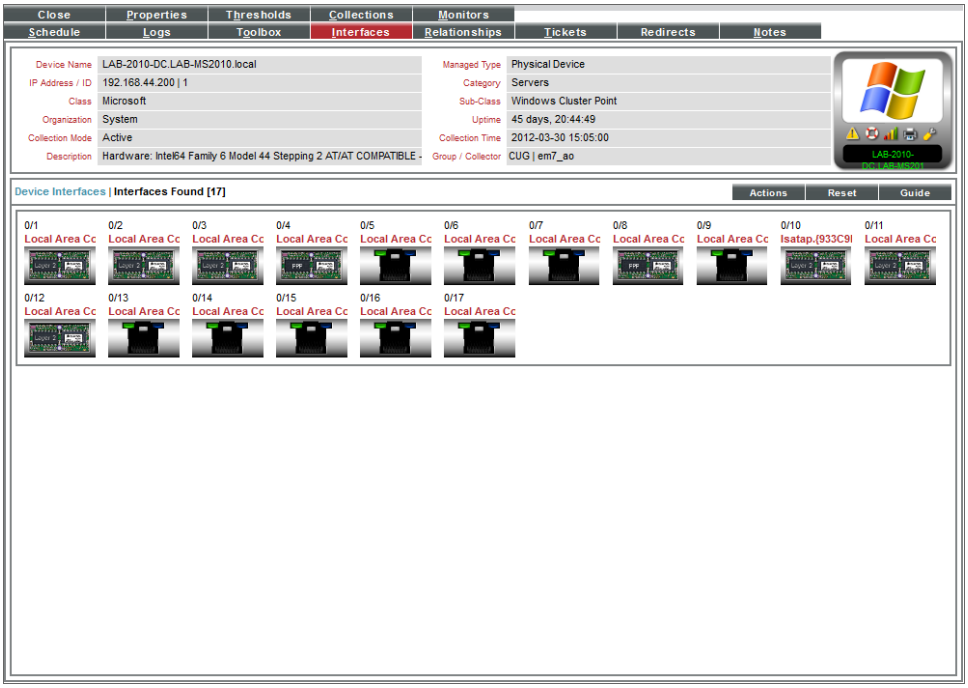
In the **Device Administration** panel for a device, you can view the **Device Interfaces** page. The **Device Interfaces** page displays detailed information about each network interface on the device and allows you to define monitoring policies for interfaces on the device. When you define a monitoring policy for an interface, SL1 will monitor the interface and gather usage data from the interface. SL1 uses the data retrieved from the interface to generate bandwidth reports for the interface.

In the **Device Reports** panel for a device, you can view the **Interfaces Found** page. The **Interfaces Found** page displays detailed information about each network interface on the device. The **Interfaces Found** page allows you to view a list of all interfaces on the device, view details about each interface, and view bandwidth usage reports for each interface.

To view details about the network interfaces on a device:

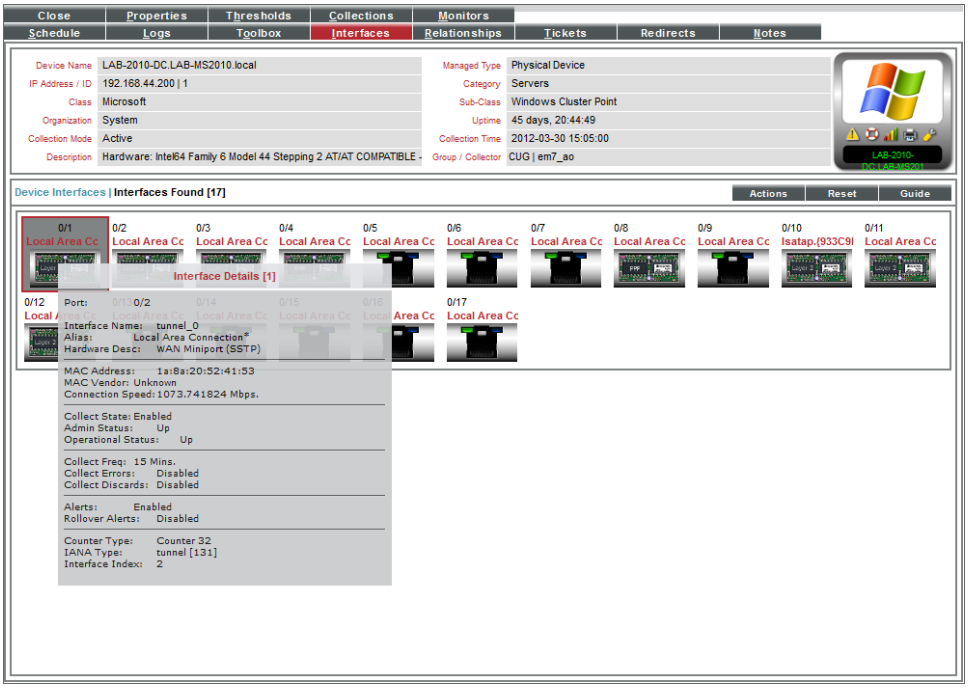
1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device for which you want to view the list of network interfaces, then do one of the following:
   - Click its wrench icon (), followed by the **[Interfaces]** tab, to view the **Device Interfaces** page.
   - Click the bar graph icon (), followed by the **[Interfaces]** tab, to view the **Interfaces Found** page.

3. Both pages display icons to represent the interfaces on the device:



4. The page displays an icon for each interface on the device. Each icon provides a visual overview of the interface.
5. For details on interface icons, click the **[Legend]** button, or in the **[Actions]** menu, select ***Interface Legend***. The **Interface Legend** modal page displays each type of interface icon with explanatory callouts.

6. When you mouse over the icon for that interface, the **Interface Details** pop-up window appears. This window displays details about the interface and its current monitoring policy.



7. The **Interface Details** pop-up window displays the following about an interface:

   - ***Port / Sub***. Port and sub-port (if applicable) of the interface.
   - ***Interface Name***. The name of the network interface. The auto-name, generated by SL1, is device_name:interface_number.
   - ***Alias***. Easy-to-remember, human-readable name for the network interface.
   - ***Hardware Desc***. Description of the network interface. Usually a description of a network-interface card.
   - ***MAC Address***. A unique number that identifies network hardware. MAC Addresses are defined by the hardware manufacturer.
   - ***MAC Vendor***. Manufacturer of the network interface.
   - ***Connection Speed***. The amount of data per second that can pass through the network interface.
   - ***Collect State***. Specifies whether or not SL1 monitors the network interface and collects data from the network interface for reports.
   - ***Admin Status***. Specifies how the network interface has been configured on the device. Can be one of the following:
     - *Up*. Network interface has been configured to be up and running.
     - *Down*. Network interface has been disabled.

- ***Operational Status***. Specifies current state of the network interface. Can be one of the following:
  - *Up*. Network interface is transmitting and receiving data.
  - *Down*. Network interface cannot transmit or receive data.
- ***Collect Freq***. Frequency at which SL1 will poll the interface to collect data. Choices are 1 minute, 5 minutes, 10 minutes, 30 minutes, 60 minutes, and 120 minutes.
- ***Collect Errors***. Specifies whether or not SL1 will collect data about packet errors on the interface. Packet errors occur when packets are lost due to hardware problems such as network outages or faulty adapter hardware.
- ***Collect Discards***. Specifies whether or not SL1 will collect data about interface discards. Discards occur when an interface receives more traffic than it can handle. Discards can also occur when an interface has been specifically configured to discard. For example, a network administrator might configure a router's interface to discard packets from an unauthorized IP address.
- ***Alerts***. Specifies whether or not SL1 will generate events for the interface. When disabled, the interface is monitored, but events are not generated for the interface.
- ***Rollover Alerts***. Specifies whether or not SL1 will generate an event when the counter for the interface rolls over.

NOTE: Rollovers and ***Rollover Alerts*** apply only to 32-bit counters and not to 64-bit counters.

- ***IP***. IP address and network mask assigned to the interface.
- ***Counter Type***. Specifies whether the interface uses a 32-bit counter or a 64-bit counter to measure bandwidth on the interface.

NOTE: If an interface has a status of "down" during initial discovery, SL1 will discover the interface but assign the interface the default ***Counter Type*** of "32". During re-discovery or nightly auto-discovery, SL1 will update the ***Counter Type*** to "64" if applicable.

- ***IANA Type***. A string that describes the type of interface, as defined by the standards group Internet Assigned Numbers Authority.
- ***Interface Index***. A unique number (greater than zero) that identifies each interface on a device. These numbers are defined by the device.

8. In the **Device Interfaces** page, clicking on an interface icon leads to the **Interface Properties** page.
9. In the **Interfaces Found** page, clicking on an interface icon leads to the Network Bandwidth Usage report in the **Device Performance** page.

Overview of Network Records

During discovery of an SNMP-enabled device, SL1 collects information about the network interfaces on that device using the standard IF-MIB. After collecting information about each interface, SL1 collects information about the IP addresses associated with those interfaces using the standard IP-MIB.

After discovery, SL1 runs a process that classifies each IP address associated with that device. The classification process calculates the network address by performing a bitwise "AND" operation using the IP address and the network mask. SL1 determines whether the IP address for the device needs to be associated with an existing network record or whether to create a new network record.

After an IP address is associated with a network record, the interface associated with that IP address appears in the **Network Browser** page for that network record. To access the **Network Browser** page for a network record, go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks) and select the desired interface icon.

IPv4 Networks

The **IPv4 Networks** page (Registry > Networks > IPv4 Networks) lists all networks and subnets detected by ScienceLogic auto-discovery and all manually defined (new) networks.

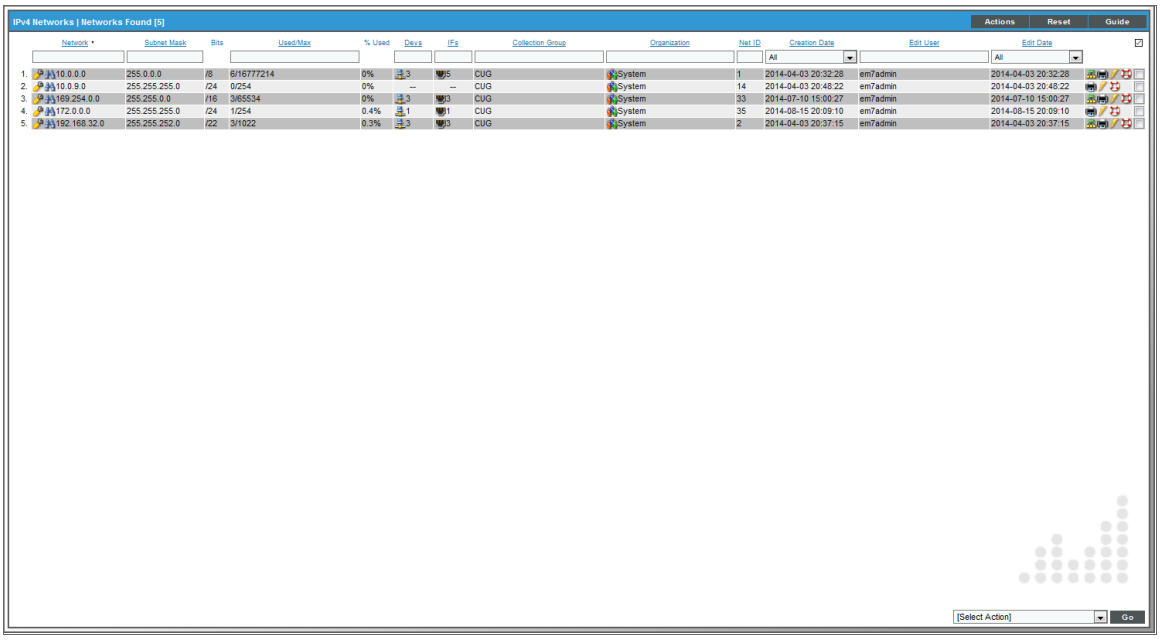
The **IPv4 Networks** page allows you to easily manage networks and IP addresses. From the **IPv4 Networks** page, you can view detailed data about the network, keep records of subnets, and determine which IP addresses are in use and which IP addresses are available.

NOTE: Users of type "user" can view only IPv4 networks that are aligned with the same organization(s) to which the user is aligned. Users of type "administrator" can view all IPv4 networks.

Viewing the List of IPv4 Networks

The table in the **IPv4 Networks** page (Registry > Networks > IPv4 Networks) contains an entry for each network managed by SL1:

NOTE: Users of type "user" can view only IPv4 networks that are aligned with the same organization(s) to which the user is aligned. Users of type "administrator" can view all IPv4 networks.



The **IPv4 Networks** page displays the following about each managed network:

TIP: To sort the list of networks, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The ***Edit Date*** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

- ***Network***. IP address of the entire network.
- ***Subnet Mask***. Subnet mask for the subnet.
- ***Bits***. The number of bits used for the network address.
- ***Used/Max***. Number of IP addresses discovered and monitored by SL1 and the maximum number of IP addresses allowed in the subnet.

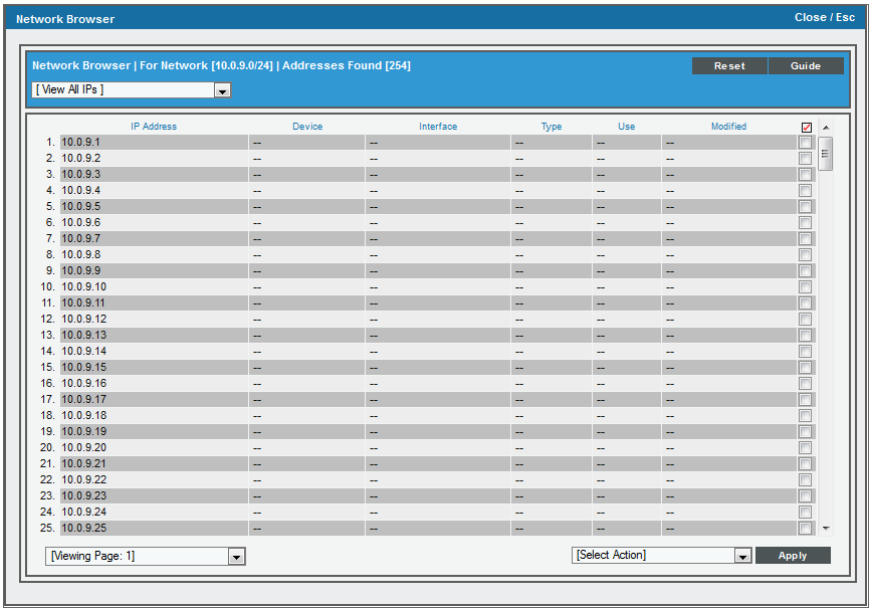
- ***% Used***. Percentage of total addresses in the network that have been discovered and monitored by SL1. In the **Account Preferences** page, you can specify whether or not you want to include empty networks (networks with no devices or interfaces) in the list of networks. These networks will have 0% in the % Used column.
- ***Devs***. Number of devices in the subnet.
- ***IFs***. Number of interfaces in the subnet.
- ***Collection Group***. The collector group associated with the network. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups).
- ***Organization***. Organization associated with the network.
- ***Net ID***. Unique network ID, assigned by SL1.
- ***Creation Date***. Date the network was discovered or manually defined.
- ***Edit User***. User who created or last edited the network's properties.
- ***Edit Date***. Date the network was created or last edited, whichever is later.
- ***Tools***. For each network in the table, the following tools are available:
    - *View/Edit Network Properties ()*. Displays the **Network Properties** modal page, where you can view and edit the basic properties of an IPv4 network.
    - *Browse Network ( )*. Leads to the **Network Browser** page. From this page, you can view a list of IP addresses (used and unused) included in a network, a list of devices included in a network, and a list of interfaces included in a network.
    - *View/Edit Aligned Devices ( )*. Leads to the **Network Browser** page, where you can view a list of devices associated with a network.
    - *View/Edit Aligned Interfaces ( )*. Leads to the **Network Browser** page, where you can view a list of interfaces associated with a network.
    - *View/Edit Organization ( )*. Leads to the **Organizational Summary** page, where you can view and edit information associated with the organization.
    - *View Network Map ( )*. Leads to the **Layer-2 Maps** page, where you can view and edit a graphical representation of a layer-2 network.
    - *View a Network Report ( )*. Opens the **Report Creator** modal page, where you can specify information to include in the report and the format in which to generate the report.
    - *Add Network to Dynamic Discovery ( )*. Adds the network to the dynamic-discovery queue. SL1 will perform dynamic-discovery on all of the IP addresses in the network and gather information about any devices and interfaces in the network. Leads to the **Discovery Control Panel** page, with the selected network as the value in the discovery list.
    - *Create a Ticket ( )*. Leads to the **Ticket Editor** page, where you can create a ticket that will be associated with the selected network.
    - *Delete (☑)*. To delete the network, select this checkbox and then click the **[Delete]** button. To select all the checkboxes, click the large red check icon.

Browsing a Network

From the **IPv4 Networks** page, you can browse a network and view the IPs, devices, and interfaces within the network. To do this:

> **NOTE**: Users of type "user" can view only devices that are aligned with the same organization(s) to which the user is aligned. Users of type "administrator" can view all devices. Users of type "user" can view only interfaces that are aligned with the same organization(s) to which the user is aligned or have been emissaried to the user's organization(s). Users of type "administrator" can view all interfaces.

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to browse.
3. Click the binocular icon ( ) for that network.
4. The **Network Browser** page appears.



5. In the drop-down menu in the upper left, you can choose to view all IP addresses in the network, all devices in the network, or all interfaces in the network.

Viewing Used and Unused IP Addresses in a Network

From the **IPv4 Networks** page, you can view a list of all IP addresses, used and unused, in a network. To do this:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to view.

3. Click the binocular icon ( ) for that network.
4. The **Network Browser** page appears.
5. In the drop-down menu in the upper left, you can choose to view all IP addresses in the network, all devices in the network, or all interfaces in the network.

Viewing Devices Aligned with a Network

From the **IPv4 Networks** page, you can view a list of all devices in a network To do this:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to view.
3. Click the devices icon ( ) for that network.
4. The **Network Browser** page appears and displays the list of devices in the network.
5. In the drop-down menu in the upper left, you can choose to view all IP addresses in the network, all devices in the network, or all interfaces in the network.

Viewing Interfaces Aligned with a Network

From the **IPv4 Networks** page, you can view a list of all interfaces in a network To do this:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to view.
3. Click the interface icon ( ) for that network.
4. The **Network Browser** page appears and displays the list of interface in the network.
5. In the drop-down menu in the upper left, you can choose to view all IP addresses in the network, all devices in the network, or all interfaces in the network.

Chapter 4

Device Relationships and Topology Collection

Overview

During discovery, SL1 automatically defines parent and child relationships for certain devices and discovers all networks and subnets in your infrastructure. SL1 then creates graphical representations of these discovered devices, networks, and subnets to create topology maps.

The following sections describe the device relationships and topology maps created by the SL1:

Overview of Device Relationships 38
Viewing the List of Device Relationships 39
Viewing the Relationships for a Single Device 41
The Device View Page 43
Layer-2 Topology Collection 44
CDP Topology Collection 45
LLDP Topology Collection 47
Layer-3 Topology Collection 49

Overview of Device Relationships

SL1 automatically defines parent and child relationships for certain devices. Users can also manually define some types of relationships. Devices can have the following types of relationships:

- Layer-2 devices and their clients. Layer-2 relationships are automatically discovered by SL1 and can be created in the **Subnet Map (L2)** page (Maps > Classic Maps > Topology Maps > Layer-2).

- Layer-3 devices and layer-2 devices. Layer-3 relationships are automatically discovered by SL1 and can be created in the **Layer 3 Map** page (Maps > Classic Maps > Topology Maps > Layer-3).
- Network devices that use CDP (Cisco Discovery Protocol) and devices that are specified as neighbors in the CDP tables. CDP relationships are automatically discovered by SL1 and can be created in the **Subnet Map (CDP)** page (Maps > Classic Maps > Topology Maps > CDP).
- Network devices that use LLDP (Link Layer Discovery Protocol) and devices that are specified as neighbors in the LLDP tables. LLDP relationships are automatically discovered by SL1 and can be created in the **Classic Maps > Topology Maps > LLDP** page (Maps > Classic Maps > Topology Maps > LLDP).
- Component devices and their parent devices using Dynamic Application data. For example, virtual machines and their hypervisors.
- Device relationships between root devices, parent devices, and component devices (Component Mapping).
- Device relationships created using Dynamic Application data. For example, the Dynamic Applications in the VMware vSphere and NetApp PowerPacks are configured to create relationships between VMware Datastore component devices and their associated NetApp Volume component devices.
- Generic parent-child relationships, sometimes referred to as Event Correlation relationships or Ad-Hoc relationships, can be manually created. These relationships can be created in the **Device Children** page for the parent device.

NOTE: SL1 also automatically discovers relationships between VMWare hypervisors and VMWare virtual machines using SNMP data, but ***only for legacy versions VMWare ESX 3.5 and VMWare ESX 4.x***.

All device relationships are displayed as child and parent relationships. For example:

- A layer-2 switch is a parent device and a firewall attached to the switch is a child device.
- A layer-3 router is a parent device and a layer-2 switch attached to the router is a child device.
- A VMware ESX server is a parent device and a Linux VM on that server is a child device.

Viewing the List of Device Relationships

The **Device Relationships** page displays information about every parent-child relationship that has been automatically created by SL1 or manually defined by a user.

For each child device, the **Device Relationships** page displays at least the MAC address of the child interface and, if possible, the device name of the child device, the IP address associated with the child interface, the name of the child interface, and the manufacturer of the child interface.

For each parent device, the **Device Relationships** page displays the device name, the name of the parent interface, the MAC address of the parent interface, and the manufacturer of the parent interface.

For example, suppose a switch has been discovered by SL1. Suppose that 12 interfaces on that switch are in use. Suppose that only three of those 12 interfaces are connected to child interfaces that have been discovered by SL1. The **Device Relationships** page will display whatever ARP information SL1 can retrieve about the remaining nine child interfaces. In most cases, SL1 can retrieve the MAC address and manufacturer associated with the child interface, even if the child interface has not been discovered by SL1.

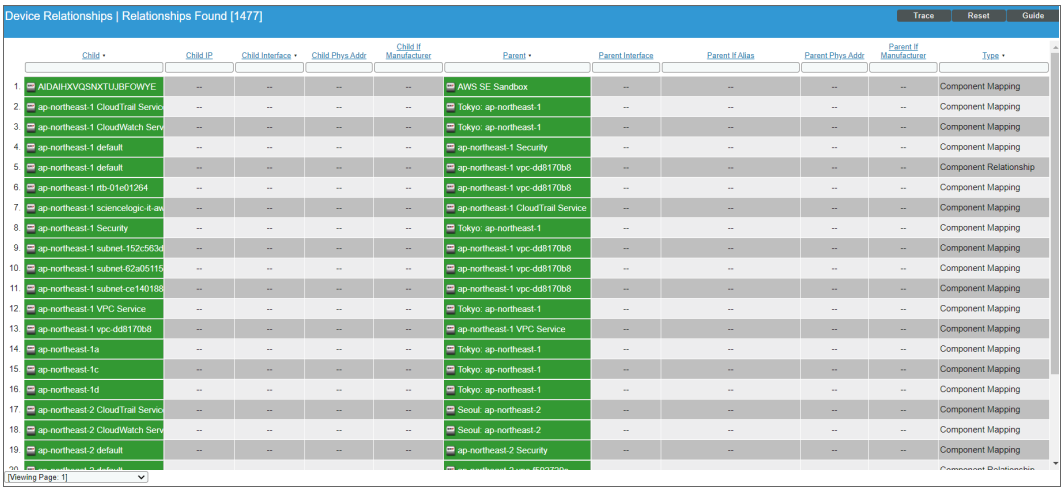
The relationships in the **Device Relationships** page are dynamically updated. If SL1 discovers a new relationship, SL1 updates the **Device Relationships** page.

You can view information for each parent-child relationship between two devices managed by SL1 or for a single parent device managed by SL1 and an unknown child device. To view information on **Device Relationships**:

1. Go to the **Device Relationships** page (Registry > Networks > Device Relationships).
2. The **Device Relationships** page displays the following information:

TIP: You can sort the list of user device relationships by column. To sort by ascending column value, click on a column heading. To sort by descending column value, click on the same column heading a second time.

NOTE: The **Device Relationships** page respects multi-tenancy rules. This means that you can view relationships in this page only if both devices are aligned with an organization of which you are a member.



- ***Child***. If the child device has been discovered by SL1, this column contains the name of the device and a link to the **Device Relationships** page for the child device.
- ***Child IP***. If the child device has been discovered by SL1, this column contains the IP address through which the child communicates with the parent device.
- ***Child Interface***. If the child device has been discovered by SL1, this column contains the name of the interface through which the child device communicates with the parent device and a link to the **Interfaces Found** page for the child interface.

- ***Child Phys Addr***. The physical address (MAC address) for the interface through which the child device communicates with the parent device.
- ***Child IF Manufacturer***. If included in the MAC address, the manufacturer of the child interface.
- ***Parent***. The name of the parent device and a link to the **Device Relationships** page for the parent device.
- ***Parent Interface***.The name of the interface through which the parent device communicates with the child device and a link to the **Interfaces Found** page for the parent interface.
- ***Parent IF Alias***. Easy-to-remember, human-readable name for the interface on the parent device.
- ***Parent Phys Addr***. The physical address (MAC address) for the interface through which the parent device communicates with the child device.
- ***Parent IF Manufacturer***. If included in the MAC address, the manufacturer of the parent interface.
- ***Type***. Describes the relationship between the parent device and child device. Possible values are:
  - CDP
  - LLDP
  - Component Mapping
  - Component Relationship
  - Event Correlation
  - Layer-2
  - Layer-3
  - VMware

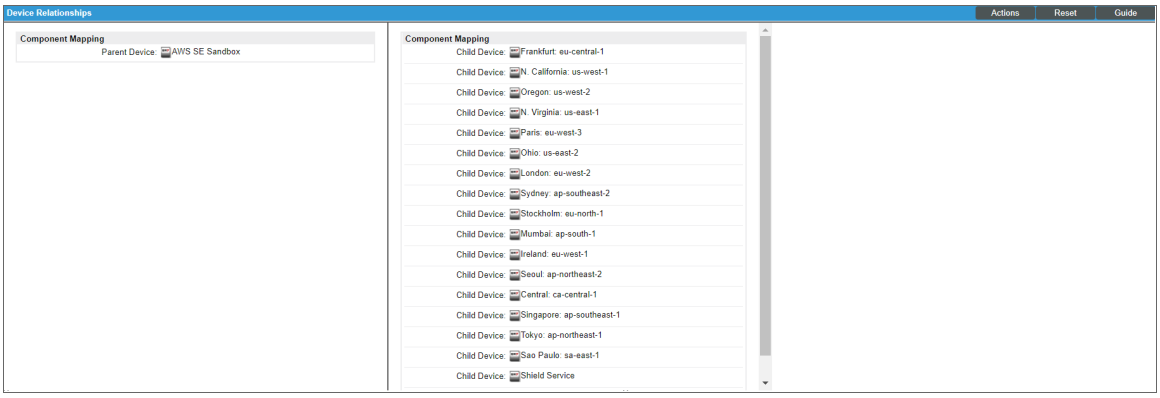
Viewing the Relationships for a Single Device

You can view all links for a single device on the **Relationships** tab of the **Device Investigator** (or on the **Device Relationships** page in the **Device Properties** panel in the classic SL1 user interface).

To view all links for a single device:

1. Go to the **Relationships** tab of the **Device Investigator**. (Alternatively, in the classic SL1 user interface, go to the **Device Manager** page (Devices > Device Manager), click the wrench icon for a device ( ) and click the **[Relationships]** tab in the **Device Properties** pane.) The **Device Relationships** page appears.

2. The left pane of the **Device Relationships** page displays links to parent devices. The right pane of the **Device Relationships** page displays links to child devices. For each relationship, the **Device Relationships** page displays the following information:

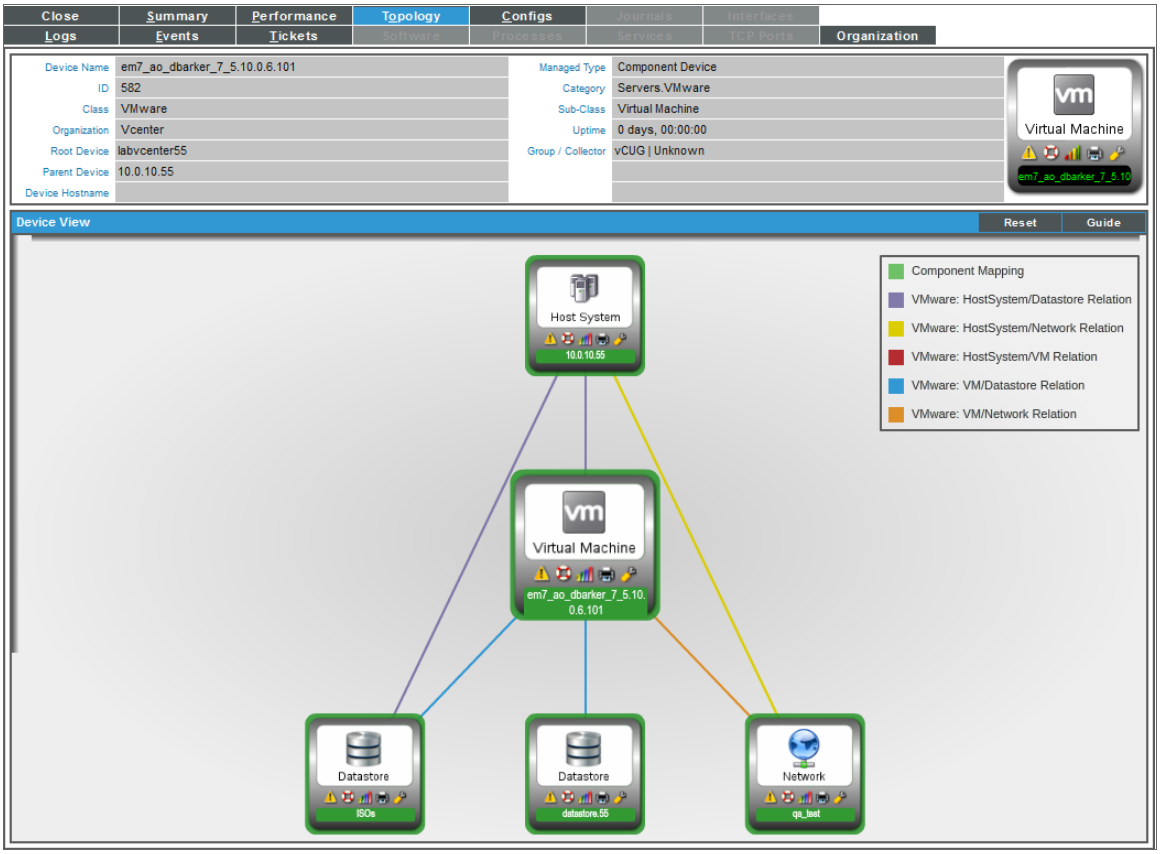


- ***Type of relationship***. Possible values are:
  - *Layer 2*. Layer-2 devices and their clients.
  - *Layer 3*. Layer-3 devices and layer-2 devices.
  - *VMware*. Hypervisors and their virtual machines.
  - *CDP*. Network devices that use CDP (Cisco Discovery Protocol) and devices that are specified as neighbors in CDP tables.
  - *LLDP*. Network devices that use LLDP (Link Layer Discovery Protocol) and devices that are specified as neighbors in LLDP tables.
  - *Event Correlation*. Relationships defined manually by users through the user interface.
  - *Component Mapping*. Relationships defined using Dynamic Applications.
- ***Parent Device***. The name of the parent device and a link to the **Device Properties** page for the parent device.
- ***Parent Interface***. The name of the interface through which the parent device communicates with the child device and a link to the **Interfaces Found** page for the parent interface.
- ***Child Device***. The name of the child device and a link to the **Device Properties** page for the child device.
- ***Child Interface***. The name of the interface through which the child device communicates with the parent device and a link to the **Interfaces Found** page for the child interface.

NOTE: Clicking on a device reloads the **Device Relationships** page and makes the selected device the primary device.

The Device View Page

The **Device View** page appears when a user clicks the **Topology** tab in the Device Reports panel. The **Device View** page displays a map of the device and all of the devices with which the device has relationships.



These relationships include:

- Layer-2 devices and their clients
- Layer-3 devices and Layer-2 devices
- Component devices and their parent devices. For example, virtual machines and their hypervisors and their virtual machines.
- Network devices that use CDP (Cisco Delivery Protocol) and devices that are specified as neighbors in CDP tables
- Links between network devices that use CDP (Cisco Discovery Protocol) and devices that are specified as neighbors in CDP tables
- Network devices that use LLDP (Link Layer Delivery Protocol) and devices that are specified as neighbors in LLDP tables

- Links between network devices that use LLDP (Link Layer Discovery Protocol) and devices that are specified as neighbors in LLDP tables
- Device relationships between root devices, parent devices, and component devices (Component Mapping)
- Device relationships created with Dynamic Applications
- Manually created parent-child relationships that affect event correlation

> **NOTE**: Double-clicking on a device reloads the **Device View** page and makes the selected device the primary device.

For details on the toolbars that appear in this page, see the ***Views*** manual.

Layer-2 Topology Collection

A layer-2 topology record describes a direct network connection between a parent device (a Network Switch or Network Bridge) and a child device. The child device is either:

- Another bridge device discovered in SL1
- Another type of device that is discovered in SL1
- A device that is not discovered in SL1

Every hour, SL1 collects information from the Bridge-MIB from all discovered network switches and bridges. Network switches and bridges that support the Bridge-MIB report information about all MAC addresses for which that network switch or bridge has forwarding information.

During collection, SL1 performs the following steps:

- Compiles a list of all devices to poll. SL1 polls devices that have a ***Device Category*** of "Network.Switches" (ID 2) or "Network.Bridges" (ID 19). The ***Device Category*** is defined in the Device Class assigned to the device.
- If the ***Enable Community String Indexing (VLAN Topology)*** checkbox is selected in the **Behavior Settings** page (System > Settings > Behavior), SL1 compiles a list of vLANs for which data should be collected using the CISCO-VTP-MIB. A vLAN is added to the list of vLANs only if the vLAN state is 1 (operational) and the vLAN type is 1 (ethernet). If the ***Enable Community String Indexing (VLAN Topology)*** option is disabled, SL1 performs collection for vLAN 1 only.
- For each vLAN on each device, SL1 polls the Bridge-MIB to collect the list of all MAC addresses for which that network switch or bridge has forwarding information.
- SL1 stores a MAC address record if:
    - The status of the record is "3" (learned).
    - An ifIndex value was collected successfully for the associated port index.

The information collected from the Bridge-MIB does not explicitly indicate which devices are directly connected to a network switch or bridge; switches and bridges will report forwarding information for MAC addresses that are several network hops away from the switch or bridge. A second "crunch" process creates layer-2 topology relationships by evaluating all of the collected MAC address records holistically.

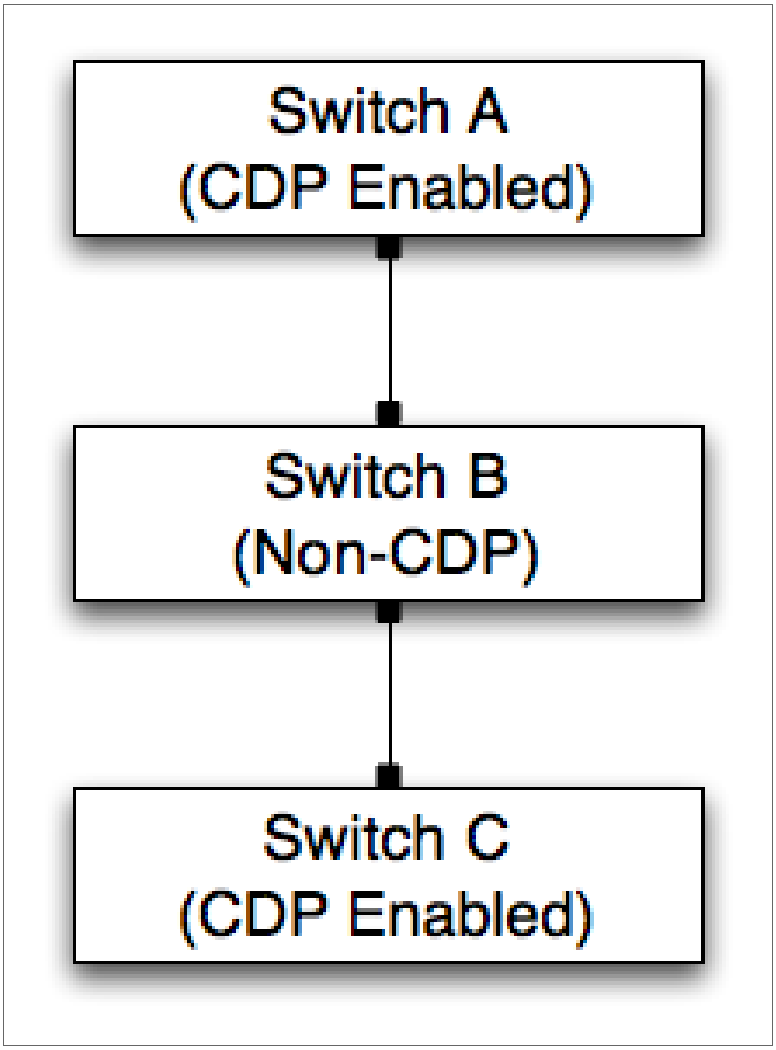
To view layer-2 maps, go to the **Subnet Map (L2)**page (Classic Maps > Topology Maps > Layer-2). For details on viewing layer-2 maps, see the***Views*** manual.

CDP Topology Collection

A CDP Topology record describes a direct network connection between a parent device (a Network Switch or Network Router) and a child device. CDP stands for "Cisco Discovery Protocol," a proprietary standard that is used by networking devices to communicate configuration information to the other devices in the network. Devices that support CDP store and report information received about their immediate neighbors.

CDP is a proprietary protocol developed by Cisco and is not supported by all network hardware. If your network includes both CDP-enabled and non-CDP network switches and routers, the topology data reported by the CDP-enabled devices might not be accurate.

Suppose a network includes three switches connected in the following way:



- Switch A and Switch C, which are both CDP-enabled, broadcast CDP messages.
- Because Switch B is not CDP-enabled, the broadcast messages from Switch A will reach Switch C. Therefore, Switch C will report that it is directly connected to Switch A.
- Conversely, the broadcast messages from Switch C will reach Switch A. Therefore, Switch A will report that it is directly connected to Switch C.

In addition to the CDP data collected from the switches in this example, SL1 might also collect layer-2 topology data that can be used to create correct topology links. However, each discovered interface can be associated with only one topology record of ***any*** type. If a conflict exists between the collected CDP topology data and the collected layer-2 topology data, the CDP topology data takes precedence. In the example above, the CDP topology data will be inaccurate, but the layer-2 data might be accurate. Therefore, if your network includes both CDP-enabled and non-CDP network switches and routers, you might want to disable CDP topology collection in the **Behavior Settings** page (System > Settings > Behavior).

If CDP collection is enabled, SL1 collects information from the Cisco-CDP-MIB from all discovered network switches and routers. SL1 polls devices that have a ***Device Category*** of "Network.Switches" (ID 2) or "Network.Routers" (ID 1). The ***Device Category*** is defined in the Device Class assigned to the device. Network switches and routers that support the Cisco-CDP-MIB report the IP address and interface information for all directly connected devices that are CDP-enabled.

> **NOTE:** Although SL1 polls all network switches and routers for CDP information, not all network switches and routers support CDP.

Each discovered interface can be associated with only one topology record of ***any*** type. Therefore, the same "crunch" process that creates layer-2 topology records is also responsible for creating the CDP records based on the collected data. However, unlike layer-2 topology records, the Cisco-CDP-MIB reports only directly connected devices. Therefore, if all associated interfaces are valid and available, there is a 1:1 mapping between collected CDP relationships and the CDP relationships created by the "crunch" process.

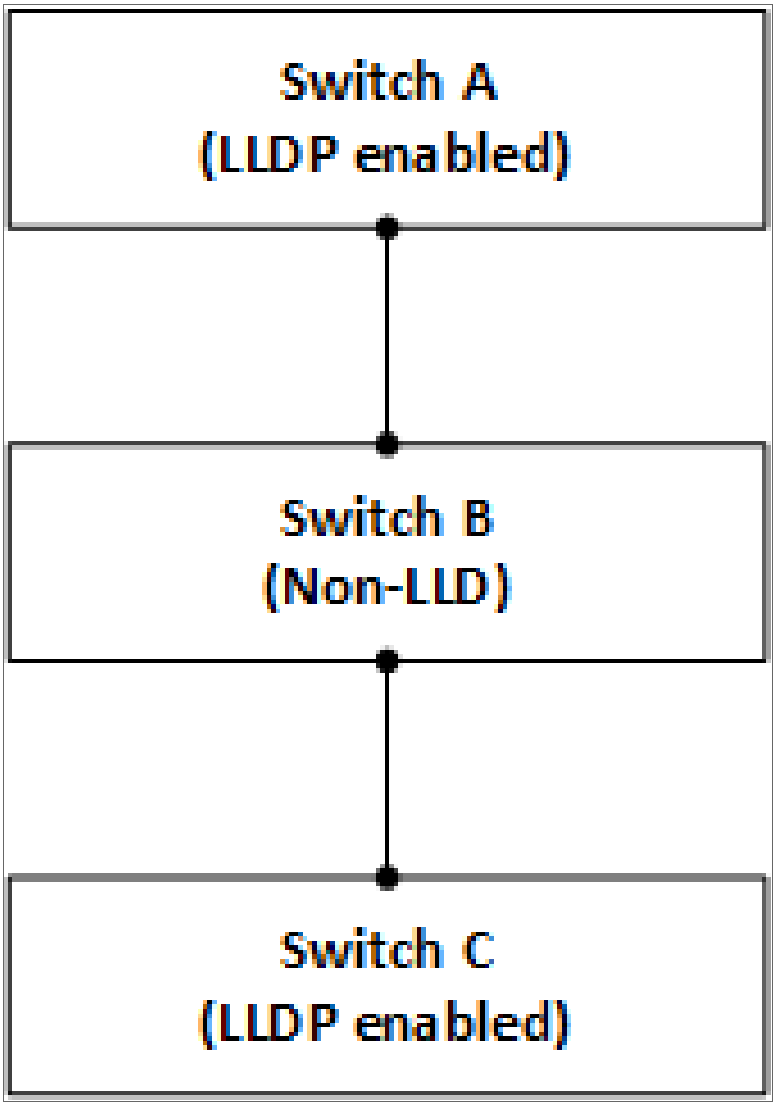
To view CDP maps, go to the **Subnet Map (CDP)** page (Views > Topology Maps >CDP). For details on viewing CDP maps, see the ***Views*** manual.

LLDP Topology Collection

An LLDP topology record describes a direct network connection between a parent device (a Network Switch or Network Router) and a child device. LLDP stands for "Link Layer Discovery Protocol," a standard used by networking devices to communicate configuration information to the other devices in the network. Devices that support LLDP store and report information received about their immediate neighbors.

If your network includes both LLDP-enabled and non-LLDP network switches and routers, the topology data reported by the LLDP enabled devices might not be accurate.

Suppose a network includes three switches connected in the following way:



- Switch A and Switch C, which are both LLDP-enabled, broadcast LLDP messages.
- Because Switch B is not LLDP-enabled, the broadcast messages from Switch A will reach Switch C. Therefore, Switch C will report that it is directly connected to Switch A.
- Conversely, the broadcast messages from Switch C will reach Switch A. Therefore, Switch A will report that it is directly connected to Switch C.

In addition to the LLDP data collected from the switches in this example, SL1 might also collect Layer-2 topology data that can be used to create correct topology links. However, each discovered interface can be associated with only one topology record of ***any*** type. If a conflict exists between the collected LLDP topology data and the collected Layer-2 topology data, the LLDP topology data takes precedence. In the example above, the LLDP topology data will be inaccurate, but the Layer-2 data might be accurate. Therefore, if your network includes both LLDP-enabled and non-LLDP network switches and routers, you might want to disable LLDP topology collection in the **Behavior Settings** page (System > Settings > Behavior).

If LLDP collection is enabled, SL1 collects information from the LLDP MIB from all discovered network switches and routers. SL1 polls devices that have a ***Device Category*** of "Network.Switches" (ID 2) or "Network.Routers" (ID 1). The ***Device Category*** is defined in the Device Class assigned to the device. Network switches and routers that support the Cisco-LLDP-MIB report the IP address and interface information for all directly connected devices that are LLDP-enabled.

NOTE: Although SL1 polls all network switches and routers for LLDP information, not all network switches and routers support LLDP.

Each discovered interface can be associated with only one topology record of ***any*** type. Therefore, the same "crunch" process that creates Layer-2 topology records is also responsible for creating the LLDP records based on the collected data. However, unlike Layer-2 topology records, the -LLDP MIB reports only directly connected devices. Therefore, if all associated interfaces are valid and available, there is a 1:1 mapping between collected LLDP relationships and the LLDP relationships created by the "crunch" process.

Layer-3 Topology Collection

Layer-3 topology records are created by performing a traceroute command from a Data Collector or the All-In-One Appliance to the discovered network hardware every two hours:

- For each "hop" in a traceroute that specifies an IP address associated with a discovered device, SL1 creates a layer-3 topology record that connects the device from the previous hop to the device for the current hop.
- Layer-3 topology records are created only when both devices are discovered; layer-3 topology records are not created when one or both of the two devices is unknown.
- If the IP address associated with a hop is associated with an unknown device, SL1 does not store that hop or any subsequent hops for that traceroute.
- Layer-3 topology records describe only that two devices are connected; layer-3 topology records do not describe which interfaces on those devices are connected.

For SL1 to create layer-3 topology records, the following requirements must be met:

- All traceroute commands for layer-3 topology collection originate from Data Collectors or an All-In-One Appliance. Therefore, the parent node(s) in the layer-3 topology is always a Data Collector or the All-In-One Appliance. For SL1 to create layer-3 topology records, all Data Collectors and All-In-One Appliances must be discovered.

- SL1 performs traceroute commands to devices that have the ***L3 Topology*** option enabled. The ***L3 Topology*** option is defined in the device class assigned to a device. For SL1 to perform layer-3 topology collection, at least one device in your system must have the ***L3 Topology*** option enabled in the device class.
- Your network configuration must allow the traffic generated by the traceroute commands. To test whether your network allows this traffic, go to the **Device Toolbox** page (by clicking the **[Toolbox]** tab in the **Device Administration** panel) for a device with the ***L3 Topology*** option enabled, and then click the **Traceroute** icon.

NOTE: A device that has the ***L3 Topology*** option disabled can still be associated with a layer-3 topology record. If an IP address associated with a device that has the ***L3 Topology*** option disabled appears as a "hop" in a traceroute command performed for a different device, the device with the ***L3 Topology*** option disabled will be associated with the layer-3 topology records that represent the hops to and from that device.

To view layer-3, go to the **Layer 3 Map**page (Classic Maps > Topology Maps > Layer-3). For details on viewing layer-3 maps, see the***Views*** manual.

Appendix

A

Configuring Cisco IOS Devices for SNMP and Syslog

Overview

If you configure your Cisco IOS device to respond to SNMP requests from SL1, you can discover your Cisco IOS device as an SNMP device. When SL1 discovers a Cisco IOS device as an SNMP device, SL1 will automatically collect data supplied by the SNMP agent.

The following sections describe how to configure your Cisco IOS devices for SNMP and Syslog:

Configuring a Cisco IOS Router or Cisco IOS Switch to Use SNMPv1 and SNMPv2 ..... *51*

Configuring a Cisco IOS Firewall to Use SNMPv1 and SNMPv2 ..... *52*

Configuring Cisco IOS Devices for Syslog *53*

Configuring a Cisco IOS Router or Cisco IOS Switch to Use SNMPv1 and SNMPv2

To configure a Cisco Router or Cisco Switch to use SNMP, perform the following steps:

1. Telnet to the device, enter "enable", and then enter the enable password to start configuration mode. From configuration mode, you can use the ***snmp-server*** commands. When you execute the first snmp-server command, that command enables the SNMP agent on the device.
2. To set the SNMP server location, execute the following command:

```
snmp-server location ScienceLogic HQ Chantilly, VA
```

3. To set the SNMP server contact, execute the following command:

```
snmp-server contact Rollins, Henry 571-555-6482
```

4. To set the community string on your Cisco device, execute the following command:

> **NOTE:** The community string is used in credentials for SNMPv1 and SNMPv2 to authenticate communication with the Cisco Router.

```
snmp-server community <community string> RO <access_list_number>
```

5. To enable SNMP traps, execute the following commands:

   - If you are using an All-In-One Appliance, use the IP address of the All-In-One Appliance when executing these commands.
   - If you are using a Distributed System and the Collector Group that will monitor your Cisco router includes a Message Collector, use the IP address of the Message Collector when executing these commands.
   - If you are using a Distributed System and the Collector Group that will monitor your Cisco router includes a single Data Collector that performs the message collection function, use the IP address of the Data Collector when executing these commands.

```
snmp-server enable traps

snmp-server host <ip_address> <snmp_string>
```

Configuring a Cisco IOS Firewall to Use SNMPv1 and SNMPv2

To configure a Cisco Firewall to use SNMP, perform the following steps:

1. To set the SNMP server location, execute the following command:

```
Firewall(config)# snmp-server location ScienceLogic HQ Chantilly, VA
```

2. To set the SNMP server contact, execute the following command:

```
Firewall(config)# snmp-server contact Rollins, Henry 571-555-6482
```

3. To set the community string on your Cisco device, execute the following command:

> **NOTE:** The community string is used in credentials for SNMPv1 and SNMPv2 to authenticate communication with the Cisco Firewall.

```
Firewall(config)# snmp-server community <your community string>
```

4. To enable SNMP traps, execute the following commands:

    - If you are using an All-In-One Appliance, use the IP address of the All-In-One Appliance when executing these commands.
    - If you are using a Distributed System and the Collector Group that will monitor your Cisco router includes a Message Collector, use the IP address of the Message Collector when executing these commands.
    - If you are using a Distributed System and the Collector Group that will monitor your Cisco router includes a single Data Collector that performs the message collection function, use the IP address of the Data Collector when executing these commands.

```
Firewall(config)# snmp-server enable traps

Firewall(config)# snmp-server host <if_name> <EM7 appliance IP> poll
```

Configuring Cisco IOS Devices for Syslog

To configure a Cisco IOS Device to use syslog, perform the following steps:

1. To make sure logging is enabled, use the **logging on** command.

```
router(config)# logging on
```

2. To specify the IP address that is to receive the router syslog messages, use the **logging *ip_address*** command, where *ip_address* is the IP address of the SL1 appliance collecting the syslog messages. For example:

    - If you are using an All-In-One Appliance, use the IP address of the All-In-One Appliance when executing this command.
    - If you are using a Distributed System and the Collector Group that will monitor your Cisco router includes a Message Collector, use the IP address of the Message Collector when executing this command.
    - If you are using a Distributed System and the Collector Group that will monitor your Cisco router includes a single Data Collector that performs the message collection function, use the IP address of the Data Collector when executing this command.

```
router(config)# logging 172.16.23.140
```

3. To limit the types of messages that can be logged to the SL1 appliance, set the appropriate logging trap level using the **logging trap informational** command, where **informational** signifies severity level 6. This means all messages from levels 0-5 (from emergencies to notifications) will be logged to the SL1 appliance. Best practices recommend setting the system to the **error** level so that only levels 0-4 are logged to the syslog server.

```
router(config)# logging trap informational error
```

4. Valid logging facilities are local0 through local7. Valid levels can be:
    - emergency
    - alert
    - critical
    - error
    - warning
    - notification
    - informational
    - debug
5. To check if the device is sending syslog messages, run the **sh logging** command.
6. You should see the syslog messages being sent. If you are having problems seeing syslog messages, ensure that the following is configured:
    - logging on
    - logging console debug
    - logging monitor debug
    - logging trap debug

To see a device's syslog messages in SL1, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Find the device for which you want to see syslog messages. Select its wrench icon ( ).
3. Click the **[Logs]** tab to see the device's log messages, which will include any syslog messages the device has sent.

In a distributed system, it can take up to five minutes to view syslog messages not associated with an event policy.

NOTE: By default, SL1 includes multiple event policies based on syslog messages. ScienceLogic recommends that you review these policies to ensure that they suit your business needs. To view these policies, go to Registry > Events > Event Manager. Use the sort and filter tools to view all policies of type "syslog." From the same page, you can edit these event policies or create your own event policies based on syslog messages. For more information on event policies, see the manual on ***Events***.

Appendix

B

Dynamic Applications for Routers, Switches, and Firewalls

Overview

The default version of the SL1 includes several vendor-specific PowerPacks that enable you to discover and monitor routers, switches, and firewalls from those vendors. It also includes a *Generic Switch/Router MIB Support* PowerPack that can collect additional data from your network devices.

The following sections describe the Dynamic Applications that are included in these PowerPacks:

PowerPack: Generic Switch/Router MIB Support 55
PowerPack: Alteon Base Pack 58
PowerPack: Cisco: Base Pack 60
PowerPack: Cisco IPSLA 77
PowerPack: Force 10 Base Pack 95
PowerPack: Juniper Base Pack 96
PowerPack: Netscreen Base Pack 103

PowerPack: Generic Switch/Router MIB Support

If the SL1 does not include vendor-specific Dynamic Applications for your routers and switches, you can use the following Dynamic Applications to collect additional data from your routers and switches.

CAUTION: Some of the Dynamic Applications in this section are not automatically aligned to devices. You must manually align these Dynamic Applications to devices. Do not align these Dynamic Applications to device that include more than 200 indexes (either more than 200 peers or more than 200 interfaces, depending on the Dynamic Application. Doing so will significantly slow the performance of your SL1 system. For details on manually aligning a Dynamic Application with a device, see the ***Device Management*** manual.

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
BGP Peer Statistics	BGP4-MIB	Number of inbound updates	5 Minutes	**Yes** **NOTE:** This Dynamic Application can collect and report data for up to 200 peers by default. The Dynamic Application will not collect and report data for peers beyond the threshold. If the threshold is exceeded, a device log entry will be generated. To change the threshold from the default, go to the **Device Thresholds** page (Registry > Devices > Device Manager > wrench icon > Thresholds), update the ***Maximum BGP Peer Statistics*** value, and then click **[Save]**.
		Number of outbound updates		
		Total inbound messages		
		Total outbound messages		
		FSM Transitions		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
BGP Peers	BGP4-MIB	Remote IP Address	5 minutes	**Yes**
		Remote Port		
		Remote AS		
		Local Port		
		Local IP Address		
		Peer State		
		Peer Admin Status		
		BGP Peer Version		
		BGP Last Error		
		FSM Established Time		
		Alerts will be generated when the Peer state is not established and the admin state is "start"		
Interface Extended Statistics	IF-MIB	Multicast Packets In	15 minutes	**No** This Dynamic Application must be manually aligned to each device. CAUTION: Do not align this Dynamic Application to devices that include more than 200 interfaces. Doing so will significantly slow performance of your SL1 system.
		Multicast Packets Out		
		Unicast Packets In		
		Unicast Packets Out		
		Broadcast Packets In		
		Broadcast Packets Out		
		The ifName is used as the label		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
OSPF Neighbors Configuration	OSPF-MIB	Neighbor IP	5 minutes	**Yes**
		Neighbor Priority		
		Neighbor Router ID		
		Neighbor State		
		Neighbor State Changes		
		Retx Q Len		
		Alerts will be generated when the Neighbor State is not 'full'.		
		OSPF Type		
		Designated Router		
		Backup Designated Router		

PowerPack: Alteon Base Pack

If your network includes Alteon devices, you can use the following Dynamic Applications to collect additional data from your routers and switches.

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Alteon: Configuration	ALTEON-TIGON-SWITCH-MIB ALTEON-TS-NETWORK-MIB	pending changes	2 hours	Yes
		status of redundant power		
		backup links		
		storage of current configuration		
		port tables		
		second syslog host		
		IP tables		
		secondary RADIUS server		
		enabled software		
		SMTP host		
		errors		
		software version		
		local network definitions		
		spanning tree status		
		offset from GMT in hours		
		syslog host IP		
		status of power supply		
		temperature data		
		IP address, authentication string, authentication status, and authentication timeout for RADIUS server		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Alteon: Load Trending	ALTEON-TS-NETWORK-MIB ALTEON-TS-LAYER4-MIB ALTEON-CHEETAH-LAYER4-MIB	current number of ARP entries	15 minutes	Yes
		concurrent connections per port		
		connection rate per virtual server		
		port bindings		
		real server current sessions		
Alteon: Performance	ALTEON-TS-NETWORK-MIB ALTEON-TS-LAYER4-MIB ALTEON-CHEETAH-LAYER4-MIB	current number of ARP entries	15 minutes	Yes
		concurrent connections per port		
		real server current sessions		
		port bindings		
		connection rate per virtual server		

PowerPack: Cisco: Base Pack

If your network includes Cisco devices, you can use the following Dynamic Applications to collect additional data from your routers and switches.

CAUTION: Some of the Dynamic Applications in this section are not automatically aligned to devices. You must manually align these Dynamic Applications to devices. Do not align these Dynamic Applications to device that include more than 200 indexes (either more than 200 peers or more than 200 interfaces, depending on the Dynamic Application. Doing so will significantly slow the performance of your SL1 system. For details on manually aligning a Dynamic Application with a device, see the ***Device Management*** manual.

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: BGP Peer Stats	CISCO-BGP4-MIB	Number of time the BGP FSM transitioned	5 minutes	Yes This Dynamic Application includes a threshold that limits the collection to a default of 200 BGP Peers to keep from slowing the performance of your SL1 system.
		Label for the peer		
		Number of accepted route prefixes		
		Number of route prefixes that have been advertised		
		Number of route prefixes that have been denied		
		Number of route prefixes that have been suppressed		
		Number of route prefixes that have been withdrawn		
		Number of messages received		
		Number of messages sent		
		Number of BGP updates received		
		Number of BGP updates sent		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: BGP Peers	CISCO-BGP4-MIB	Most recent error code and subcode	5 minutes	Yes This Dynamic Application includes a threshold that limits the collection to a default of 200 BGP Peers to keep from slowing the performance of your SL1 system.
		Label for peer		
		Version of BGP running between two peers		
		Amount of time peer has been in established state		
		BGP identifiers		
		Local IP address		
		Local port		
		Administrative status of peer		
		Status of peer		
		Remote autonomous system number		
		Remote IP address		
		Remote port		
Cisco: CPU	CISCO-PROCESS_MIB, CISCO-SYSTEM-EXT-MIB, or OLD-CISCO-CPU-MIB	CPU busy percentage in the last five minutes	5 minutes	Yes
		Label for the CPU		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: Environmental Entity Status	CISCO-ENTITY-SENSOR-MIB	Description of the fan	15 minutes	Yes
		State of the fan		
		Label for the fan		
		Index for the fan		
		Description of the power supply		
		State of the power supply		
		Label for the power supply		
		Index for the power Supply		
		Description of temperature test point		
		Status of temperature test point		
		Label for temperature test point		
		Index for temperature test point		
Cisco: Environmental Status	CISCO-ENVMON-MIB	Description of the fan	30 minutes	Yes
		State of the fan		
		Label for the fan		
		Label for the power supply		
		Description of the power supply		
		State of the power supply		
		Description of temperature test point		
		Status of temperature test point		
		Label for temperature test point		
Cisco: Fan Configuration	CISCO-ENVMON-MIB	Description of the fan	30 minutes	Yes
		State of the fan		
		Status configuration of the fan		
		Percentage of fans in a Critical or Shutdown state		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: FCoE Configuration	CISCO-FCOE-MIB	Ethernet interface name	15 minutes	Yes
		FCoE information		
		Ethernet interface admin status		
		VFC bind MAC address		
		Ethernet interface operational status		
		VFC bind type		
		VFC name		
		VFC failure cause		
		VFC admin status		
		VFC FCF priority		
		VFC operational state		
		VCF interface index		
		Ethernet interface index		
Cisco: Feature Set Configuration	CISCO-FEATURE-CONTROL-MIB	Feature name	1 hour	Yes
		Feature information		
		Current operating status		
		Reason for current operating status		
		Last action triggered		
		Last action result		
		Reason for last action failure		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: FEX Configuration	CISCO-ETHERNET-FABRIC-EXTENDER-MIB	Extender name	15 minutes	Yes
		Fabric port name		
		Creation time		
		Identify serial number string		
		Pinning max links		
		Fabric port admin status		
		Pinning mode		
		Fabric port interface index		
		Row status		
		Fabric port operational status		
		Enable serial number check		
		FEX information		
		Cisco Ethernet Fabric Extender Binding Extender Index		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: Fibre Channel Configuration	CISCO-FC-FE-MIB	Interface name	1 hour	Yes
		Current port operating FEC state		
		Administrative FEC state		
		Current interface operating state		
		Administrative port mode		
		Current port operating status cause		
		Administrative port speed		
		Current port operating status cause description		
		Administrative trunking mode		
		Current port trunking mode		
		BB_Credit model		
		Port channel name		
		Beacon mode		
		Interface service state		
		Port connector module type		
		Port World-Wide name		
		Interface label		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: Fibre Channel Performance	CISCO-FC-FE-MIB	8b10b disparity errors	5 minutes	Yes
		Framing errors		
		Address ID errors		
		b2b credit transition to zero		
		b2b credit transition from zero		
		Interface name		
		Class 2 frames discarded		
		Invalid CRCs		
		Class 2 frames received		
		Invalid transmission words		
		Class 2 frames sent		
		Frames received that were too long and had a CRC error		
		Class 2 frame octets received		
		Link failures		
		Class 2 frame octets sent		
		Link reset protocol errors received		
		Class 3 frames received		
		link reset protocol errors sent		
		Class 3 frames sent		
		F8 LIP errors received		
		Class 3 frame octets received		
		F8 LIP errors sent		
		Class 3 frame octets sent		
		Link reset responses received		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: Fibre Channel Performance ***(continued)***		Class F frames received		
		Link reset responses sent		
		Class F frames sent		
		Non-F8 LIP errors received		
		Class F frame octets received		
		Non-F8 LIP errors sent		
		Class F frame octets sent		
		Non-operational sequences received		
		Link resets due to unavailable credits		
		Non-operational sequences sent		
		Delimiter errors		
		Offline sequence errors received		
		Egress packets discarded		
		Offline sequence errors sent		
		EISL frames discarded		
		Primitive sequence protocol errors		
		ELP failures		
		Frames received that were too short, regardless of CRC status		
		Frames with EOF aborts		
		Signal losses		
		Blocks corrected by FEC decoder		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: Fibre Channel Performance ***(continued)***		Fragmented frames received		
		Loss of synchronization failures		
		Blocks not corrected by FEC decoder		
		Packets dropped due to timeouts		
		Wait times due to lack of transmission credits		
		Frames discarded		
		Credit transitions to zero for 100 ms		
		Frames received that were too long		
		Unknown class frames		
		Frames received that were too short		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: FRU Control Configuration	CISCO-ENTITY-FRU-CONTROL-MIB	Status of the FRU	5 minutes	Yes
		Name of module		
		Administrative status of the FRU		
		Name of FRU		
		Amount of current drawn for inline operation		
		Name of fan		
		Amount of current drawn for system operation		
		Operational status of module		
		Fan label		
		Operational status of FRU		
		Current supplied by the FRU		
		Operational status of fan		
		Model name of FRU		
		Power label		
		Model name of fan		
		Total current available from FRU for inline operation		
		Module label		
		Total current available from FRU for system operation		
		Cause of last module state change		
		sysUpTime value		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: Interface Errors Performance	CISCO-IF-EXTENSION-MIB	Number of times carrier signal transitioned	15 minutes	**No** This Dynamic Application must be manually aligned to each device. CAUTION: Do not align this Dynamic Application to devices that include more than 200 interfaces. Doing so will significantly slow performance of your SL1 system.
		Number of framing errors per interface		
		Number of packets dropped due to large size		
		Interface label		
		Number of times interface was reset		
		Number of input packets dropped		
		Number of output packets dropped		
		Number of packets dropped due to small size		
Cisco: IPSEC Global Ph1 Performance	CISCO-IPSEC-FLOW-MONITOR-MIB	Number of currently active IPsec Phase-1 IKE tunnels	5 minutes	Yes
		Number of previously active IPsec Phase-1 IKE tunnels		
		Number of IPsec Phase-1 IKE tunnels which were locally initiated		
		Number of IPsec Phase-1 IKE tunnels that were locally initiated and failed to activate		
		Number of IPsec Phase-1 IKE tunnels that were remotely initiated and failed to activate		
		Number of authentications that ended in failure		
		Number of decryptions that ended in failure		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: IPSEC Global Ph1 Performance ***(continued)***		Number of hash validations that ended in failure		
		Number of packets received		
		Number of packets dropped during receive processing		
		Number of packets sent		
		Number of packets dropped during send processing		
		Number of notifications received		
		Number of notifications sent		
		Number of octets received		
		Number of octets sent		
		Number of IPsec Phase-2 exchanges received		
		Number of IPsec Phase-2 exchanges received and rejected		
		Number of IPsec Phase-2 exchanges received and found to be invalid		
		Number of IPsec Phase-2 exchanges sent		
		Number of IPsec Phase-2 exchanges sent and rejected		
		Number of IPsec Phase-2 exchanges sent and found to be invalid		
		Number of IPsec Phase-2 security association delete requests		
Cisco: IPSEC Global Ph1 Performance ***(continued)***		Number of non-existent security association inbound failures that occurred during processing		
		Number of system capacity failures that occurred during processing		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: Old Interface Details	OLD-CISCO-INTERFACES MIB	Count for ARP protocol input, in octets	15 minutes	**No** This Dynamic Application must be manually aligned to each device. CAUTION: Do not align this Dynamic Application to devices that include more than 200 interfaces. Doing so will significantly slow performance of your SL1 system.
		Count for ARP protocol output, in octets		
		Count for ARP protocol input, in packets		
		Count for ARP protocol output, in packets		
		Number of times carrier signal transitioned		
		Number of packets with cyclic redundancy checksum errors		
		Number of packets dropped due to large size		
		Interface label		
		Number of times interface was reset		
		Number of input packets dropped		
		Number of output packets dropped		
		Number of packets dropped due to small size		
Cisco: Physical Memory	CISCO-ENHANCE_MEMPOOL-MIB or CISCO-MEMORY-POOL-MIB	Unused I/O memory, in bytes	5 minutes	Yes
		Used I/O memory, in bytes		
		I/O memory accuracy		
		Memory label		
		Unused processor memory, in bytes		
		Used processor memory, in bytes		
		Processor memory accuracy		
		Sum of all unused memory, in bytes		
		Sum of all used memory, in bytes		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: Port Channel Configuration	CISCO-PORT-CHANNEL-MIB	Interface name	15 minutes	Yes
		Last action status		
		Admin channel mode		
		Last action time		
		Channel add compatibility check		
		Member port		
		Channel creation time		
		Forwarding status of member port		
		Interface index		
		Port operating channel mode		
		Index		
		Port channel information and channel member list		
		Last action cause		
		Row status		
Cisco: Swap	CISCO-MEMORY-POOL MIB	Unused swap, in bytes	15 minutes	**No** This Dynamic Application must be manually aligned to each device. CAUTION: Do not align this Dynamic Application to devices that include more than 200 interfaces. Doing so will significantly slow performance of your SL1 system
		Used swap, in bytes		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: Temperature Sensor Performance	CISCO-ENTITY-SENSOR-MIB	Temperature Sensor Index	5 minutes	Yes
		Major severity threshold value		
		Temperature sensor name		
		Minor severity threshold value		
		Operational status		
		Most recent value		
Cisco: VLAN Configuration	CISCO-VTP-MIB	VLAN ID	24 hours	Yes
		Number of errors for revision numbers		
		Number of errors for revision numbers		
		Number of advert requests received		
		Number of subset adverts received		
		Number of summary adverts received		
		Maximum number of VLANs after reboot		
		Number of advert requests sent		
		Number of subset adverts sent		
		Number of summary adverts sent		
		MTU size		
		Name of VLAN		
		VLAN type		
		VTP version		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: VRF BGP Peers	CISCO-BGP4-MIB	Most recent error code and subcode	5 minutes	**No** This Dynamic Application must be manually aligned to each device.
		Label for peer		
		Version of BGP running between two peers		
		Amount of time peer has been in established state		
		BGP identifiers		
		Local IP address		
		Local port		
		Administrative status of peer		
		Status of peer		
		Remote autonomous system number		
		Remote identifier		
		Remote IP address		
		Remote port		
		TCP state		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco: VSAN Configuration	CISCO-VSAN-MIB	VSAN name	5 minutes	Yes
		VSAN administrative status		
		VSAN operational status		
		InorderDelivery guarantee flag		
		Interoperability		
		Load balancing type		
		Network media type		
		Interface name		
		Number of subset adverts sent		
		Number of summary adverts sent		
		MTU size		
		VSAN ID		
		VSAN index label		
		VSAN interface ifIndex		
Device Software Version	ENTITY-MIB	IOS version	24 hours	Yes

PowerPack: Cisco IPSLA

If your network includes Cisco devices and you want to collect network performance data for those devices, you can use the following Dynamic Applications to do so.

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA ICMP JITTER Performance	CISCO-RTTMON-MIB	Label for the RTT target	1 minute	Yes
		Minimum one-way trip time, destination to source		
		Average positive and negative jitter values, destination to source		
		Minimum one-way trip time, source to destination		
		Average positive and negative jitter values, source to destination		
		Sum of squares of one-way trip time, destination to source		
		Average positive and negative jitter values in both directions		
		Sum of squares of one-way trip time, source to destination		
		Interarrival jitter at source		
		Sum of one-way trip time, destination to source		
		Interarrival jitter at responder		
		Sum of one-way trip time, source to destination		
		Maximum negative jitter value, destination to source		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA ICMP JITTER Performance ***(Continued)***		Maximum positive jitter value, source to destination		
		Number of packets arrived after timeout		
		Maximum absolute negative jitter value, source to destination		
		Number of packets lost		
		Maximum positive jitter value, destination to source		
		Number of packets unable to initiate due to internal error		
		Maximum RTTs successfully measured		
		Maximum successive lost packets		
		Minimum RTTs successfully measured		
		Minimum negative jitter value, destination to source		
		Sum of RTTs successfully measured		
		Minimum absolute negative jitter value, source to destination		
		Sum of squares of RTTs successfully measured		
		Minimum positive jitter value, destination to source		
		Application-specific sense code for the completion status		
		Minimum positive jitter value, source to destination		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA ICMP JITTER Performance ***(Continued)***		Number of successful one-way trip time measurements		
		Sum of squares of all negative jitter values, destination to source		
		Minimum successive lost packets		
		Sum of squares of all negative jitter values, source to destination		
		Number of all negative jitter values, destination to source		
		Sum of squares of all positive jitter values, destination to source		
		Number of all negative jitter values, source to destination		
		Sum of squares of all positive jitter values, source to destination		
		Sum of all negative jitter values, destination to source		
		Number of all positive jitter values, destination to source		
		Sum of all negative jitter values, source to destination		
		Number of all positive jitter values, source to destination		
		Sum of all positive jitter values, destination to source		
		Number of RTTs successfully measured		
		Sum of all positive jitter values, source to destination		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA ICMP JITTER Performance ***(Continued)***		Average one-way trip time, source to destination		
		Average one-way trip time, destination to source		
		Number of out-of-sequence packets in both directions		
		Average one-way trip time, source to destination		
		Number of out-of-sequence packets, destination to source		
		Maximum one-way trip time, destination to source		
		Number of out-of-sequence packets, source to destination		
		Maximum one-way trip time, source to destination		
Cisco IPSLA Configuration	CISCO-RTTMON-MIB	Round Trip Time Monitoring application version string	1 hour	Yes
		Explicit-null label added to LSP echo requests		
		RTP session duration		
		LSP echo reply IP header DSCP value		
		Number called		
		LSP echo requests reply mode		
		Codec inter-packet delay, in milliseconds		
		127/8 address for load balancing		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA Configuration ***(Continued)***		ICPIF advantage factor		
		Codec payload		
		NTP sync tolerance value		
		Codec type		
		Acceptable NTP clock synchronization error tolerance percentage		
		Control message status		
		Non-volatile memory "show running" command		
		HTTP or FTP RTT operation type		
		Post-dial delay detect point		
		Table row owner		
		DNS name server IP address		
		Packet data request size		
		Minimum router free memory to configure RTR		
		Packet data response size		
		Duration between each RTT operation		
		Router probe capacity		
		FTP RTT operation type		
		Probe ID		
		HTTP cache status		
		Probe packet priority		
		HTTP proxy server information		
		Protocol for the RTT operation		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA Configuration ***(Continued)***		IPSLA probe configuration label		
		HTTP raw request content, string 1		
		HTTP raw request content, string 2		
		HTTP raw request content, string 3		
		HTTP raw request content, string 4		
		HTTP raw request content, string 5		
		Router RTR responder status		
		Echo probe response time status		
		Source IP address		
		Source port number		
		Source voice port		
		HTTP server version number		
		Conceptual RTT control row status		
		Index of supported "RttMonProtocol" protocols		
		IPSLA HTTP probe configuration label		
		Supported "RttMonProtocol" protocols definition		
		IPSLA jitter configuration label		
		Index of supported "RttMonRttType" types		
		IPSLA jitter probe configuration label		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA Configuration ***(Continued)***		Maximum echo packet data size		
		Supported "RttMonRttType" types definition		
		IPSLA MPLS configuration label		
		Target IP address		
		Target port number 1		
		Target port number 2		
		Target URL		
		IPSLA Probes configuration label		
		IPSLA supported configuration label		
		IPSLA VoIP configuration label		
		Jitter inter-packet delay, in milliseconds		
		Administrative threshold limit, in milliseconds		
		Jitter statistics accuracy, in microseconds		
		Time of last set operation		
		Last set error message description		
		Timeout duration, in milliseconds		
		Object lifetime, decremented every second		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA Configuration ***(Continued)***		Terms of service		
		Maximum number of entries that can be added to the rttMonCtrlAdminTable		
		Total clock synchronization error threshold		
		Number of packets to be transmitted (jitter probe using codec type)		
		MPLS echo request packet TTL setting		
		Number of packets to be transmitted (jitter probe)		
		MPLS echo request EXP value		
		RTT operation type		
		FEC target type for RTT echo and pathEcho operations		
		Data verification status		
		VoIP GK registration delay		
		VRF name		
Cisco IPSLA DHCP Performance	CISCO-RTTMON-MIB	RTT operation type	1 minute	Yes
		Latest RTT operation completion status sense code		
		RTT target label		
		Number of RTT operation timeouts		
		Latest successful RTT operation completion time		
Cisco IPSLA ECHO Performance	CISCO-RTTMON-MIB	RTT target label	1 minute	Yes
		Latest RTT operation completion status sense code		
		Latest successful RTT operation completion time		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA FTP Performance	CISCO-RTTMON-MIB	RTT target label	1 minute	Yes
		Latest RTT operation completion status sense code		
		Latest successful RTT operation completion time		
Cisco IPSLA HTTP Performance	CISCO-RTTMON-MIB	RTT target label	1 minute	Yes
		Latest RTT operation completion status sense code		
		Round-trip time to perform DNS query within the HTTP operation		
		Round-trip time to connect to the HTTP server		
		Round-trip time to perform HTTP operation		
		Round-trip time to download object specified by the URL		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA JITTER Performance	CISCO-RTTMON-MIB	RTT target label	1 minute	Yes
		Maximum one-way latency, source to destination		
		Average positive and negative jitter values for latest operation, destination to source		
		Minimum one-way latency, destination to source		
		Average positive and negative jitter values for latest operation, in both directions		
		Minimum one-way latency, source to destination		
		Average positive and negative jitter values for latest operation, source to destination		
		Sum of squares of one-way latency, destination to source		
		Inter-arrival jitter at source		
		Sum of squares of one-way latency, source to destination		
		Inter-arrival jitter at responder		
		Sum of one-way latency, destination to source		
		ICPIF value for the latest jitter operation		
		Sum of one-way latency, source to destination		
		Maximum negative jitter value, destination to source		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA JITTER Performance ***(Continued)***		Maximum positive jitter value, destination to source		
		Number of packets that arrived after timeout		
		Maximum absolute value of all negative jitter values, source to destination		
		Packet loss, destination to source		
		Packet loss, source to destination		
		Maximum positive jitter value, source to destination		
		Packet loss, direction undetermined		
		Minimum negative jitter value, destination to source		
		Number of packets arrived out of sequence		
		Minimum absolute value of all negative jitter values, source to destination		
		Maximum of successfully measured RTTs		
		Minimum positive jitter value, destination to source		
		Minimum of successfully measured RTTs		
		Minimum positive jitter value, source to destination		
		Sum of successfully measured jitter RTTs		
		Latest jitter operation MOS value, in hundreds		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA JITTER Performance ***(Continued)***		Total of all negative jitter values, source to destination		
		Sum of squares of successfully measured RTTs		
		Latest jitter operation NTP sync status		
		Latest jitter RTT operation completion status sense code		
		Total of all negative jitter values, destination to source		
		Sum of squares of RTTs of all negative jitter values, destination to source		
		Sum of squares of RTTs of all negative jitter values, source to destination		
		Number of successful one-way latency measurements		
		Sum of squares of RTTs of all positive jitter values, destination to source		
		Total of all positive jitter values, destination to source		
		Sum of squares of RTTs of all positive jitter values, source to destination		
		Total of all positive jitter values, source to destination		
		Sum of RTTs of all negative jitter values, destination to source		
		Number of RTTs successfully measured		
		Sum of RTTs of all negative jitter values, source to destination		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA JITTER Performance ***(Continued)***		Average latency, destination to source		
		Sum of RTTs of all positive jitter values, destination to source		
		Average latency, source to destination		
		Sum of RTTs of all positive jitter values, source to destination		
		Maximum one-way latency, destination to source		
		Number of complete RTT operations out of sync with NTP		
Cisco IPSLA Jitter Test Completion Stats	CISCO-RTTMON-MIB	RTT operation type	5 minutes	Yes
		Number of jitter operations successfully completed		
		RTT target label		
		Number of RTT operations initiated		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA MPLS Configuration	CISCO-RTTMON-MIB	LPD group identifier	1 hour	Yes
		Time of last LSP Path discovery attempt		
		"lspGroup" probe identifier		
		Target PE path identifier		
		LPD group status identifier		
		Latest operation return code for LPD Group single probes		
		IPSLA MPLS configuration		
		Time when statistics row was last reset		
		Cause of failure for last-attempted LSP Path discovery		
		Time of row creation		
		LSP Path discovery failure status		
		LPD group target PE address		
		Completion time for last successful LSP Path discovery		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA MPLS Performance	CISCO-RTTMON-MIB	VPN name used for the Auto SAA L3 MPLS VPN RTT operation	1 minute	Yes
		String used to identify the RTT target		
		Average RTT across all probes in the LPD group		
		Completion time of last successful LSP path discovery to target PE		
		Maximum number of active paths discovered to the rttMonLpdGrpStatsTargetPE target		
		Maximum number of successfully measured RTTs for all probes in the LPD group		
		Minimum number of active paths discovered to the rttMonLpdGrpStatsTargetPE target		
		Minimum number of successfully measured RTTs for all probes in the LPD group		
		Number of failed single-probe operations for all paths in the LPD group		
		Number of successful single-probe completions for all paths in the LPD group		
		Number of timed-out single-probe operations for all paths in the LPD group		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA Packet Loss Performance	CISCO-RTTMON-MIB	RTT operation type	1 minute	Yes
		Number of packets that arrived after timeout		
		RTT target label		
		Number of packets lost from source to destination		
		Number of RTTs successfully measured		
		Number of packets lost, unable to determine direction		
Cisco IPSLA Transaction OK Performance	CISCO-RTTMON-MIB	Number of RTT operations successfully completed	1 minute	Yes
		RTT target label		
		Maximum completion time of successful RTT operations		
		Cumulative completion time of successful RTT operations		
		Minimum completion time of successful RTT operations		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA VOIP RTP Performance	CISCO-RTTMON-MIB	RTT target label	1 minute	Yes
		Estimated mean opinion score for listening quality at source for latest operation		
		Latest RTP operation completion status sense description		
		Number of early packets at source for latest operation		
		Average one-way latency, destination to source		
		Number of late packets at source for latest operation		
		Average one-way latency, source to destination		
		Packet loss for latest operation, destination to source		
		Codec frame loss events at source for latest operation		
		Packet loss for latest operation, source to destination		
		Inter-arrival jitter at source for the latest operation		
		Number of out-of-sequence packets at source for latest operation		
		Inter-arrival jitter at destination for the latest operation		
		Number of packets missing in action while measuring statistics, source to destination		
		Maximum one-way latency, destination to source		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Cisco IPSLA VOIP RTP Performance ***(Continued)***		Minimum one-way latency, destination to source		
		Computed value of R-factor at source for latest operation		
		Maximum one-way latency, source to destination		
		Estimated value of R-factor at destination for latest operation		
		RTP packet round-trip time		
		Minimum one-way latency, source to destination		
		Latest RTP operation completion status sense code		
		Estimated mean opinion score for conversational quality at source for latest operation		
		Total packets sent, destination to source		
		Estimated mean opinion score for conversational quality at destination for latest operation		
		Total packets sent, source to destination		

PowerPack: Force 10 Base Pack

If your network includes Force 10 devices, you can use the following Dynamic Applications to collect additional data from your routers and switches.

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Force 10: Asset	SNMPv2-SMI	Version of the code	24 hours	Yes
		description of device		
		number of 1G Ethernet interfaces		
		serial number		
		status		
		system uptime		
		status of current boot image		
		version of current boot image		
		release date of current boot image		
		model number		
Force 10: CPU Utilization	SNMPv2-SMI	CPU utilization, in percent, for last 5 minutes	5 minutes	Yes
Force 10: Power Supply/Fan	SNMPv2-SMI	index for the power supply	15 minutes	Yes
		index for the fan		
		operational status of the power supply		
		operational status of the fan		
		type of power supply		
Force 10: Temp	SNMPv2-SMI	Temperature of the unit	5 minutes	Yes

PowerPack: Juniper Base Pack

If your network includes Juniper devices, you can use the following Dynamic Applications to collect additional data from your routers and switches.

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Juniper: Chassis MIB Configuration	JUNIPER-MIB	FRU name	5 minutes	Yes
		FRU current state		
		FRU type		
		Box name, model, or description		
		Box revision		
		Box serial number		
		Chassis description		
		Chassis identifier		
		CLEI code		
		Contents description		
		sysUptime during last installation		
		Container's level 1 index		
		Container's level 2 index		
		Container's level 3 index		
		Contents part number		
		Content revision		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Juniper: Chassis MIB Configuration ***(continued)***		Content serial number		
		Content type		
		FRU sysUptime when last powered off		
		FRU sysUptime when last powered on		
		FRU offline reason		
		FRU slot number		
		FRU uptime		
		Operating description		
		Operating level 1 index		
		Operating level 2 index		
		Operating level 3 index		
		Operating state		
Juniper: Chassis MIB Performance	JUNIPER-MIB	CPU load average	5 minutes	Yes
		CPU utilization, in percent		
		FRU power voltage		
		Heap utilization, in percent		
		CPU utilization in interrupt service routine		
		Chassis description		
		Object temperature, in degrees Celsius		
Juniper: CPU	JUNIPER-MIB	CPU usage, in percent	5 minutes	Yes

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Juniper: DOM Performance	JUNIPER-SMI	Module temperature	5 minute	Yes
		Receiver laser power		
		Transmitter laser bias current		
		Transmitter laser output power		
Juniper: FRU MIB Configuration	JUNIPER-SMI	FRU administrative state	5 minutes	Yes
		FRU level 1 index		
		FRU level 2 index		
		FRU level 3 index		
		FRU operational state		
		FRU object ID		
Juniper: Memory	JUNIPER-MIB	Buffer pool utilization, in percent	5 minutes	Yes
Juniper: Process Count	JUNIPER-MIB	Number of processes running	5 minutes	Yes
Juniper: Temperature Stats	JUNIPER-MIB	Object name	5 minutes	Yes
		Object temperature, in degrees Celsius		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Juniper: VPN MIB Configuration	JUNIPER-VPN-MIB	Interface VPN name	15 minutes	Yes
		Route Target VPN name		
		Interface VPN type		
		Pseudo-Wire VPN name		
		Route Target VPN type		
		VPN description string		
		Interface status		
		Pseudo-Wire VPN index		
		Pseudo-Wire VPN type		
		Route Target index		
		Route Target type		
		VPN name		
		VPN type		
		Remote PE address		
		Remote PE address type		
		Associated Pseudo-Wire index		
		Maximum bandwidth in, in kilobytes		
		Maximum bandwidth out, in kilobytes		
		VPN interface index		
		VPN interface protocol		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Juniper: VPN MIB Configuration ***(continued)***		Interface row status		
		Interface storage type		
		Next VPN interface index		
		Next Pseudo-Wire index		
		Next Route Target index		
		Number of active sites		
		Number of active VPNs		
		Number of configured sites		
		Number of configured VPNs		
		Number of local addresses		
		Pseudo-Wire associated interface VPN index		
		Pseudo-Wire local site identifier		
		Pseudo-Wire LR octets received		
		Pseudo-Wire LR octets sent		
		Pseudo-Wire LR packets received		
		Pseudo-Wire LR packets sent		
		Pseudo-Wire octets received		
		Pseudo-Wire octets sent		
		Pseudo-Wire packets received		
		Pseudo-Wire packets sent		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Juniper: VPN MIB Configuration ***(continued)***		Pseudo-Wire received packets demultiplexor		
		Pseudo-Wire remote site identifier		
		Pseudo-Wire remote site status		
		Pseudo-Wire row status		
		Pseudo-Wire status		
		Pseudo-Wire storage type		
		Pseudo-Wire uptime		
		Pseudo-Wire state transitions		
		Pseudo-Wire sent packets demultiplexor		
		Pseudo-Wire tunnel name		
		Pseudo-Wire tunnel status		
		Pseudo-Wire tunnel type		
		Route Target		
		Route Target export distribution type		
		Route Target row status		
		Route Target storage type		
		VPN RIB total addresses		
		VPN age		
		VPN identifier		
		VPN row status		
		VPN type identifier		

PowerPack: Netscreen Base Pack

If your network includes Netscreen devices, you can use the following Dynamic Applications to collect additional data from your firewalls:

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Netscreen: Configuration	NETSCREEN-SET-DNS-MIB NETSCREEN-RESOURCE-MIB NETSCREEN-VPN-PHASEONE-MIB NETSCREEN-SCHEDULE-MIB	Active Session number	1 hour	Yes
		MIP address		
		Block Java/ActiveX/ZIP/EXE Component		
		Failed session allocation counters		
		Detect Address Sweep attack		
		Host name of the device		
		Detect Filter IP Source Route Option attack		
		Alarm threshold for ICMP attack		
		Alarm threshold for UDP attack		
		Detect Land attack		
		Alarm thresholds for ICMP port scans		
		Detect Ping of Death		

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Netscreen: Configuration ***(continued)***		Detect IP Spoofing attack		
		Unique interface ID		
		Detect Port Scan Death attack		
		Age time of SYN flood		
		Detect SYN attack		
		Alarm threshold for SYN attack		
		Detect Tear Drop attack		
		Queue size for SYN attack		
		Detect UDP Flood attack		
		Threshold for SYN attack		
		Detect Win Nuke attack		
		Timeout for SYN attack		
		Domain name of device		
		Alarm threshold for UDP attak		
		Interface netmask that is linked to a MIP		
		OS license information		
		Host IP address to which MIP is mapped		
		OS version		
		IP address		
		Session number		
		Maximum number of session device can afford		
		Unique interface ID		
Netscreen: CPU	NETSCREEN-RESOURCE-MIB	Average CPU use, in percent	5 minutes	Yes

Dynamic Application	Required MIB	Collected Data Points	Frequency	Applied Automatically During Discovery?
Netscreen: Memory Collection	NETSCREEN-RESOURCE-MIB	Unused memory	5 minutes	Yes
		Used memory		
Netscreen: Policy	NETSCREEN-POLICY-MIB	ID associated with a policy	1 hour	Yes
		Policy status		
		Destination address		
		Destination zone		
		Firewall action (permit, deny, tunnel)		
		Layer-4 services allowed		
		Layer-4 services allowed, by name		
		Source address		
		Source zone		
		VPN tunnel associated with the policy		
Netscreen: Session Graph	NETSCREEN-RESOURCE-MIB	Session number	5 minutes	Yes
Netscreen: VPN Tunnels	NETSCREEN-VPN-MON-MIB	Timestamp for start of session	15 minutes	Yes
		IKE Phase 2 status		
		IP address of peer gateway		
		VPN entity associated with the tunnel		

Appendix C

Dashboards

Overview

The following sections describe the dashboards that are included in vendor-specific PowerPacks that enable you to discover and monitor routers, switches, and firewalls:

PowerPack: Juniper Base Pack *106*

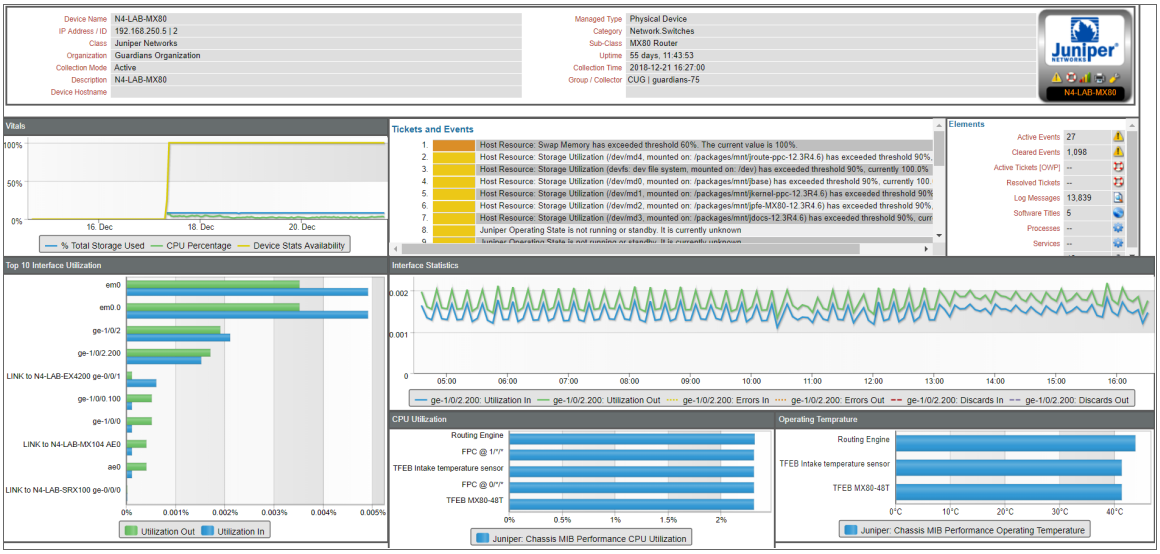
Juniper Network *107*

PowerPack: Juniper Base Pack

If your network includes Juniper devices, the *Juniper Base Pack* PowerPack includes the following device dashboard that provides summary information for Juniper component devices.

Juniper Network

The "Juniper Network" device dashboard is set as the default device dashboard for all Juniper component devices. It displays the following information:



- The basic information about the device
- A graph that shows the device's availability, CPU utilization, and storage utilization
- A list of tickets and events for the device
- A count of, and links to, the elements associated with the device
- A list of the top 10 device interfaces based on utilization in and out
- A graph that shows the utilization in and out statistics over time for the interface selected in the Top 10 Interface Utilization widget
- The CPU utilization of the device components
- The operating temperatures of the device components

© 2003 - 2021, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010