Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

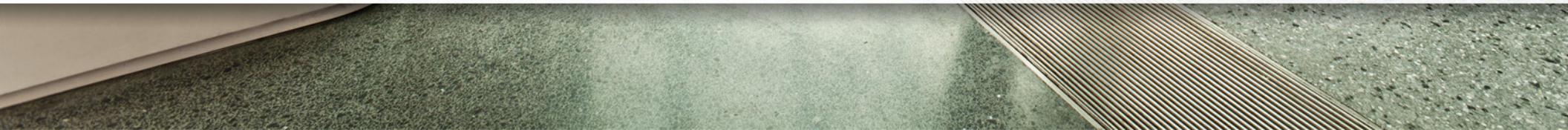
BORDERLESS NETWORKS

DEPLOYMENT GUIDE

Network Monitoring Using IP SLA and Cisco Prime LMS Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series



Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

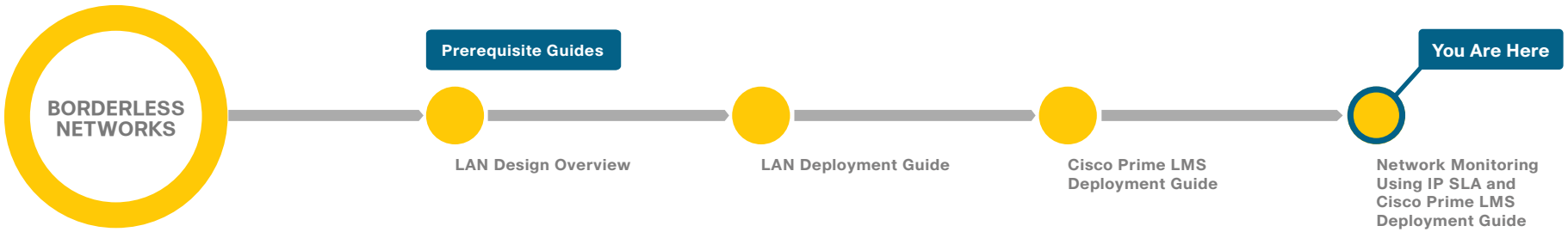
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



Introduction

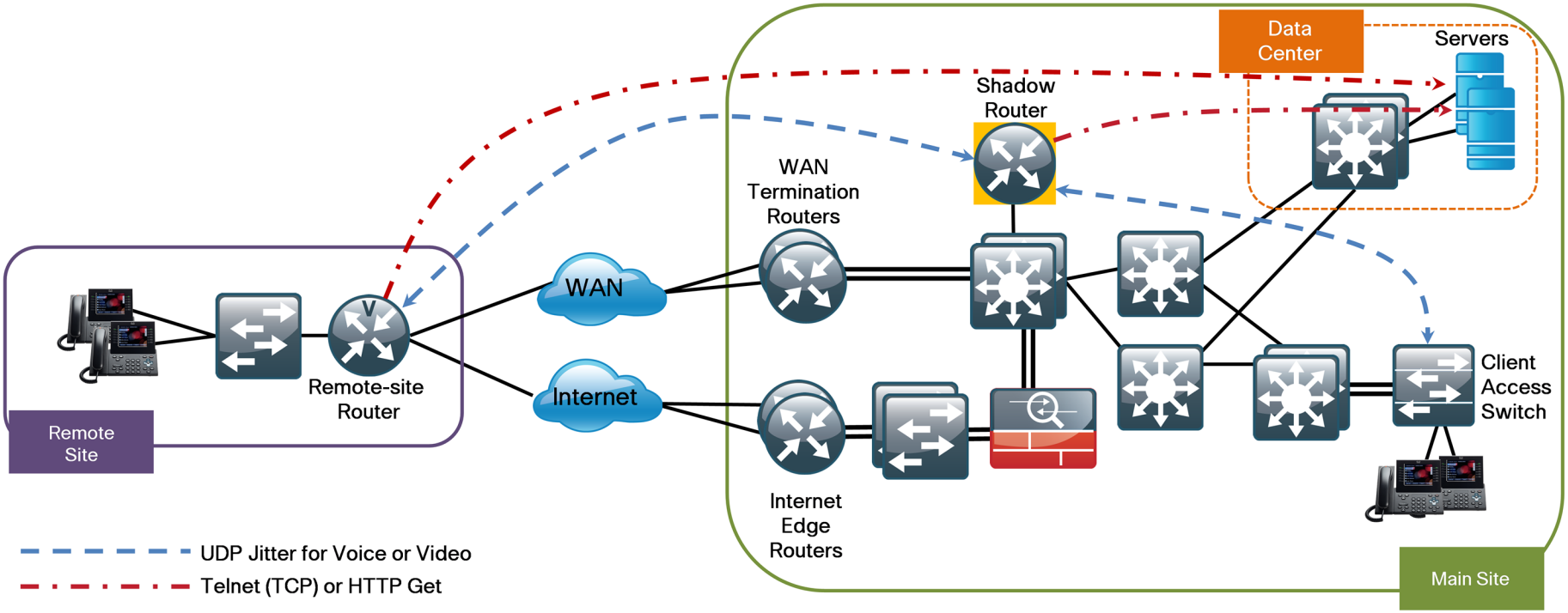
Business Overview

The services that networks provide have changed dramatically in recent years with the addition of voice and video on networks already transporting mission-critical and delay-sensitive applications. As users rely more on the network to connect them to the applications and resources they need to perform their jobs, the performance of the network becomes even more key to their productivity. IT organizations have service levels that they must support for their user applications. In order to grow a cost-effective network, many organizations use outsourced and service provider–based network offerings that have defined service-level agreements (SLAs) for the traffic that transits their network offerings. The challenge for IT organizations is monitoring the various parts of their networks—those internally built and managed as well as those contracted for—to guarantee the service level for their end users.

IP services like quality of service (QoS) guarantee reliable delivery of multiple data types such as mission-critical enterprise resource applications, web-based resources, and IP-based multimedia applications including voice and video. The performance of the network must be measurable at multiple points to allow IT to baseline their network when it is performing well and detect hotspots when performance is degraded. Deploying standalone network probes at all endpoints can be expensive, and spotty coverage of network analysis causes blind spots. The key to cost-effectively monitoring and managing network performance is to embed intelligence into the network to reduce blind spots and provide end-to-end visibility with a reduced number of management systems to integrate the information.

Notes

Figure 1 - IP SLA streams monitoring the Cisco SBA network



Technology Overview

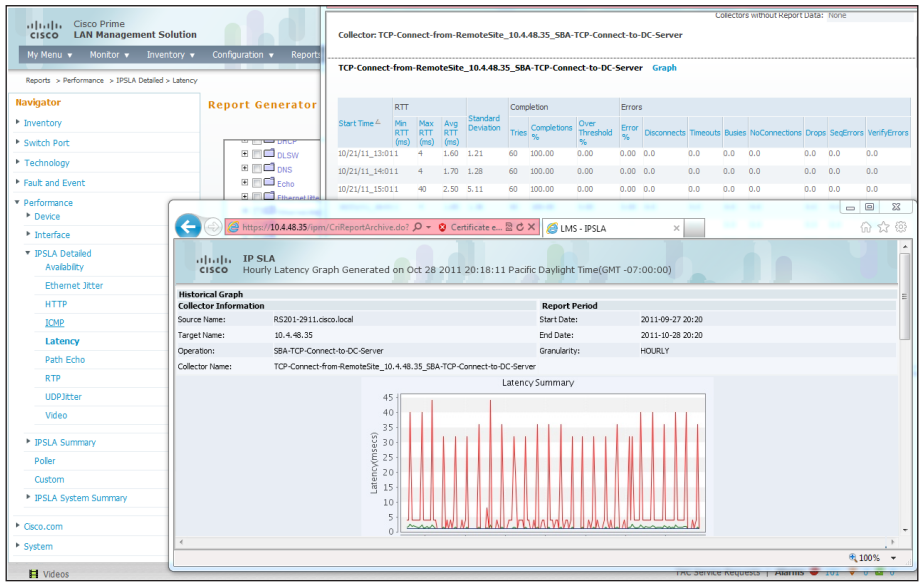
Cisco® Small Business Architecture (SBA)—Borderless Networks is based on building a sound foundation network that allows IT organizations to add network services that provide end users with effective access to their applications. Cisco SBA uses Cisco routers and LAN switches that provide the intelligence and capabilities to enhance network operation. One key network service that the Cisco infrastructure can provide is embedded IP SLA performance-management tools. Every Cisco router and switch in Cisco SBA—Borderless Networks has the ability to generate, measure, and monitor various IP packet streams to emulate an organization's multimedia and data applications. Using Cisco IOS IP SLAs in the network, organizations can cost-effectively deploy network analysis intelligence without the need to deploy standalone probes.

Key Cisco IOS Software IP SLA Benefits

- Embedded service in Cisco IOS Software in Cisco routers and Cisco Catalyst LAN switches
- Automated, real-time, and accurate network performance and network health monitoring
- Verification and measurement of IP service levels and parameters defined by network service providers
- Per-class QoS traffic monitoring
- Flexible test operation scheduling
- Proactive notifications with Simple Network Management Protocol (SNMP) traps
- Hop-by-hop and end-to-end performance measurement
- Centralized control through SNMP-based management applications or Cisco IOS Software command-line interface (CLI)
- Voice over IP (VoIP) codec simulation and VoIP quality measurements: mean opinion score (MOS) and calculated planning impairment factor (ICPIF)

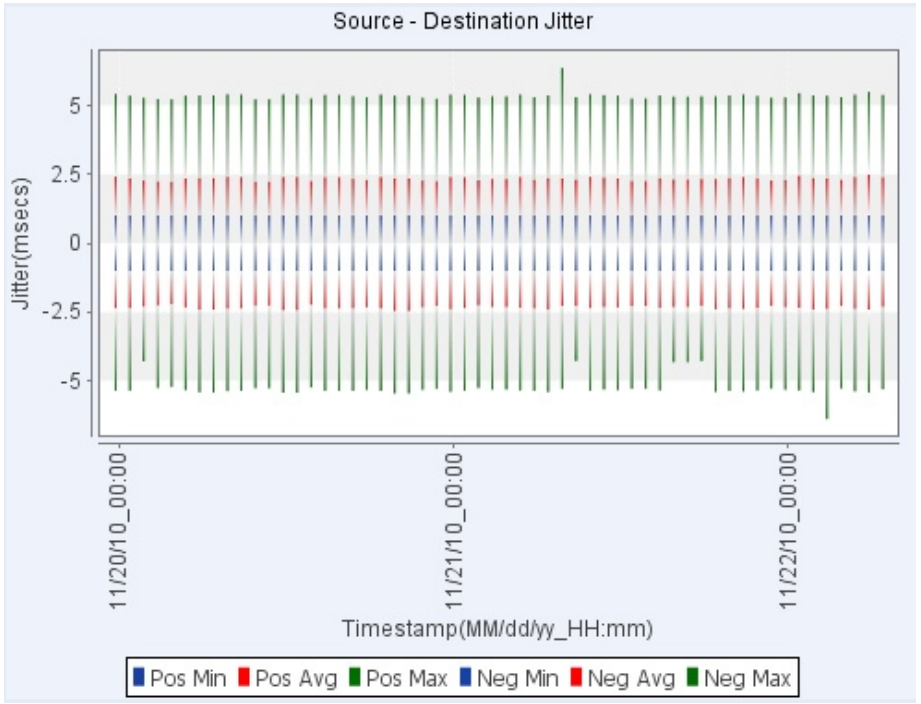
Deploying and managing multiple IP SLA endpoints can be challenging if done on a device-by-device basis using CLIs. Cisco Prime LAN Management Solution (Cisco Prime LMS) offers an integrated suite of management functions that simplify the configuration, administration, monitoring, and troubleshooting of Cisco solutions. Built on top of the latest Web 2.0 standards, Cisco Prime LMS allows network administrators to deploy and manage Cisco IP SLA through a browser-based interface that can be accessed from anywhere within the network, at any time.

Figure 2 - Cisco Prime LMS browser-based configuration and monitoring



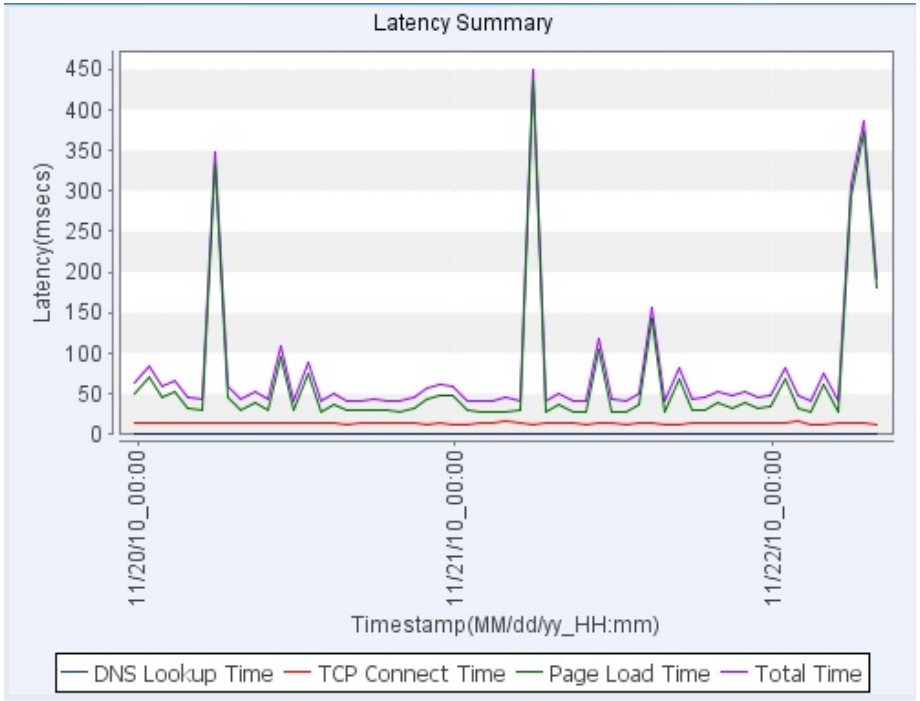
Cisco Prime LMS and Cisco IP SLA use User Datagram Protocol (UDP) streams from routers and switches in the network to test for jitter, latency, and loss that could affect delivery of voice and video. This allows IT to analyze delay and loss across WAN and Internet links as well as in the larger campus LAN. Using end-to-end, immediate, and historical measurements, as well as SNMP alerts when performance thresholds are exceeded, IT staff can spot problems before they affect user applications.

Figure 3 - Sample Cisco Prime LMS IP SLA UDP jitter measurement



Cisco Prime LMS and Cisco IP SLA offer the ability to monitor the network beyond multimedia application support. Probes for HTTP and TCP response times can help identify trends in connection times for critical enterprise resource planning applications or other mission-critical web-based applications. Cisco IP SLA also offers data operations profiles for email applications with Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) 3 support, Systems Network Architecture (SNA)–based networks with data-link switching (DLSw) profiles, and network services like Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS).

Figure 4 - Sample Cisco Prime LMS IP SLA HTTP Get measurement



Network administrators can also use Cisco IP SLA as a troubleshooting tool. They can obtain hop-by-hop performance statistics between two Cisco routers, LAN switches, or between a router and a server. If the network performance level drops during the operation (for example, due to congestion), the network administrator can promptly identify the location of the bottleneck and resolve the problem. Cisco IP SLA can also perform a network assessment for a new IP service and verify QoS levels. For example, Cisco IP SLA can determine whether the network is ready for VoIP by simulating VoIP codecs and measuring network performance and VoIP quality across the IP network.

How Cisco IP SLA Works

To measure performance, a source router sends one or more packets to a destination IP device or to a Cisco router or LAN switch. Cisco IP SLA uses the time-stamp information to calculate performance metrics such as jitter, latency, network and server response times, packet loss, and MOS voice quality scores.

A destination router that is running Cisco IOS Software can be configured as a responder, which processes measurement packets and provides detailed time-stamp information. A Cisco IP SLA responder can send information about the destination router's processing delay back to the source Cisco router. This delay is removed during calculation to further improve accuracy. One-direction measurements are also possible with Cisco IP SLA. Users can schedule a Cisco IP SLA operation at any point in time or continuously over any time interval.

Cisco IP SLA can be configured to monitor QoS or per-class traffic over the same link by setting the differentiated services code point (DSCP) bits. It can also be used for troubleshooting Multiprotocol Label Switching (MPLS) network operations; the performance measurements are essential for MPLS VPN SLA monitoring.

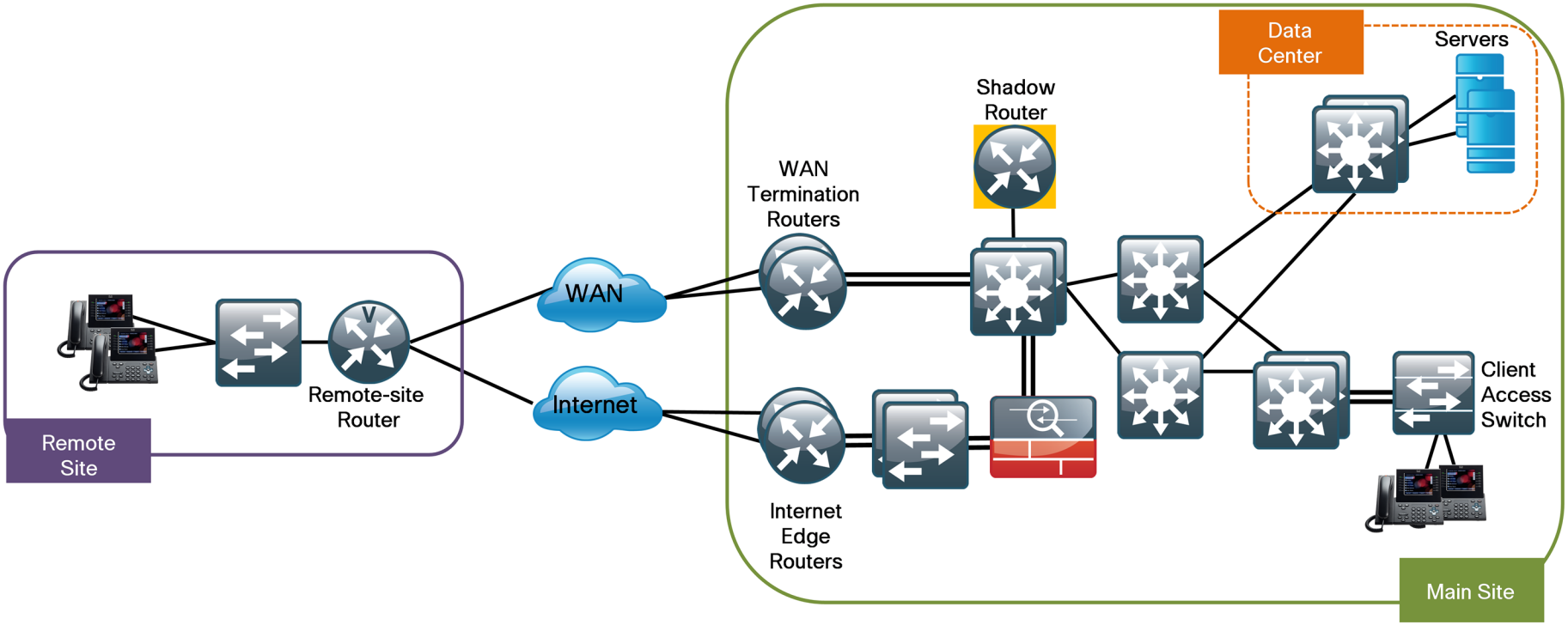
Cisco IP SLA provides a proactive notification feature with an SNMP trap. Each measurement operation can monitor performance against a preset threshold. Cisco IP SLA generates an SNMP trap to alert management applications when this threshold is crossed. An alert occurs if jitter exceeds a specified value between any two points in the network, and a trap sent to a network management system (NMS) can alert the network administrator. Administrators can also configure Cisco IP SLA to run a new operation automatically when the threshold is crossed. This feature, combined with hop-by-hop measurement capability, enables immediate real-time problem analysis.

In larger networks with hundreds of remote-site routers that need monitoring, many customers use a shadow router strategically placed in the core of the network to provide a central testing point. Shadow routers:

- Offload head-end WAN termination routers of the IP SLA task for hundreds of remote routers and switches.
- Simplify deployment by providing a single location or reduced number of locations to define two-way traffic probes.
- Run the version of Cisco IOS Software best suited for Cisco IP SLA, regardless of what the head-end WAN termination routers require.

Cisco IP SLA builds on the Cisco SBA model by providing integrated network services, which allow your organization to monitor the health of your network and to support user applications. Cisco Prime LMS provides a simplified and scalable method to deploy, test, and manage IP SLA monitoring for your IT organization.

Figure 5 - Cisco IP SLA shadow router



Deployment Details

This section describes the configuration and deployment of Cisco IP SLA for a typical organization. The first process contains procedures that walk you through how to enable Cisco IP SLA on your routers and switches to respond to end-to-end packet tests. The second process explains how to create operations that define the characteristics of a packet test, such as payload types, and IP and QoS parameters. The third process explains how to deploy a shadow router. The procedures in the fourth process help you define the endpoints you will test and tie those endpoints to the operation testing that you need. The final process describes ways to report on the IP SLA tests that you run in the network.

This guide does not cover all operations and test types available in the Cisco IP SLA portfolio. However, it does provide a basis for creating additional tests that meet the specific needs of your organization. Note the following prerequisites and recommendations:

- **Cisco Prime LMS 4.2**—If you have not already deployed Cisco Prime LMS 4.2 in your organization's network, refer to the *Prime LMS Deployment Guide*.
- **Cisco IOS IP Base**—Cisco IP SLA responder is included in the IP Base image. Cisco IP SLA sender, for operations beyond basic Internet Control Message Protocol (ICMP) operations, requires an image beyond IP Base (for example, Unified Communications, Security, etc.).
- **Network Time Protocol (NTP)**—Cisco IP SLA responder does not require NTP, however, the use of NTP network-wide is recommended in the Cisco SBA baseline.

Process

Grouping Devices and Enabling Cisco IP SLA Responder

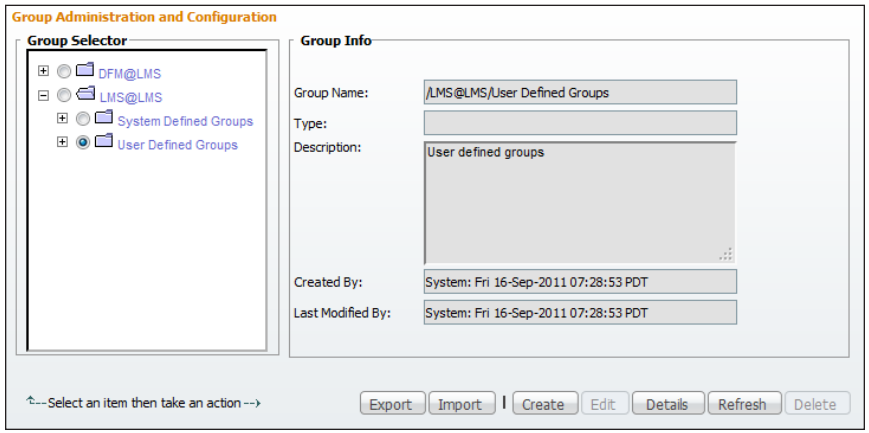
1. Configure device groups
2. Enable Cisco IP SLA responder

Procedure 1 Configure device groups

Device groups in Cisco Prime LMS allow you to create a custom list of devices for use in operations. Configuring device groups is optional but will prove an important time saver. In this example, you create a device group that contains all remote-site routers so that you can perform an operation on all of them at once.

Step 1: From the main Cisco Prime LMS window, navigate to **Admin > System > Group Management > Device**.

Step 2: Select **User Defined Groups**, and then click **Create**.

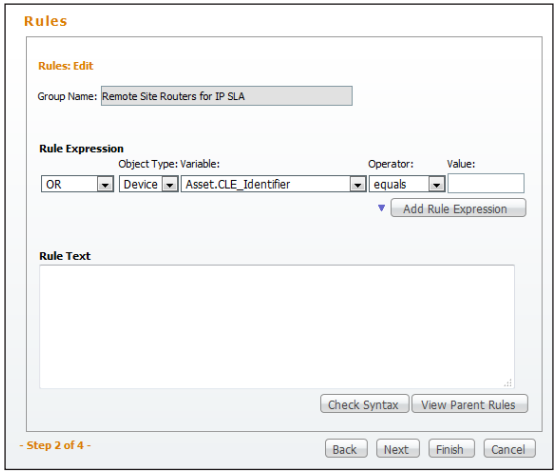


Step 3: Type a name and a description for the group, and then click **Next**.

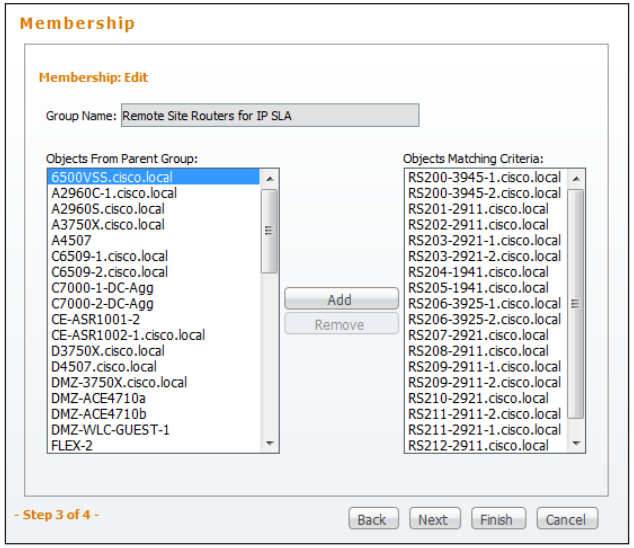
Step 4: Click **Next** to add devices from an existing Parent Group. Rules will be created for you later in Step 6.

Tech Tip

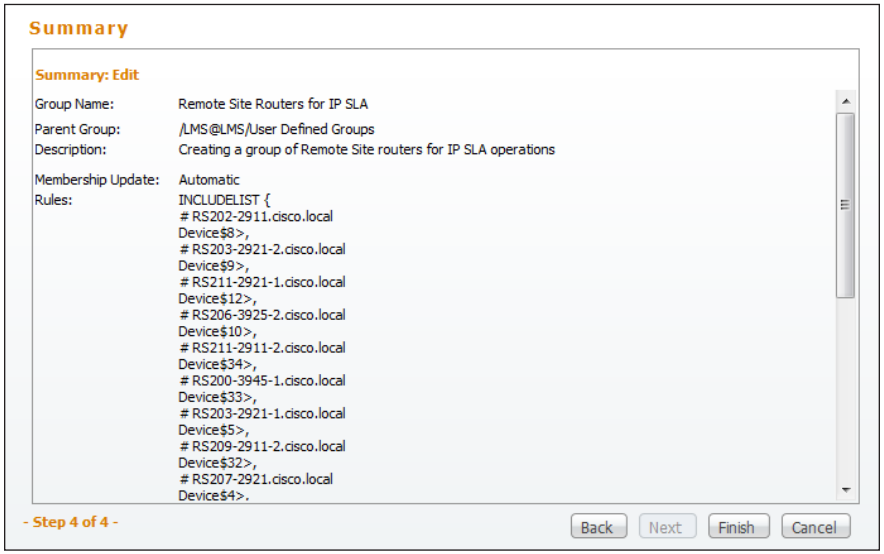
If you prefer, you can create rules in this screen to classify the devices to include in this group.



Step 5: In the **Objects from Parent Group** list on the left, choose the devices that you want included in the operation (to select multiple devices, press and hold the Ctrl key), and then click **Add**. The devices appear in the **Objects Matching Criteria** list on the right. Click **Next**.



Step 6: Ensure that the Summary list is correct for your devices, and then click **Finish**.

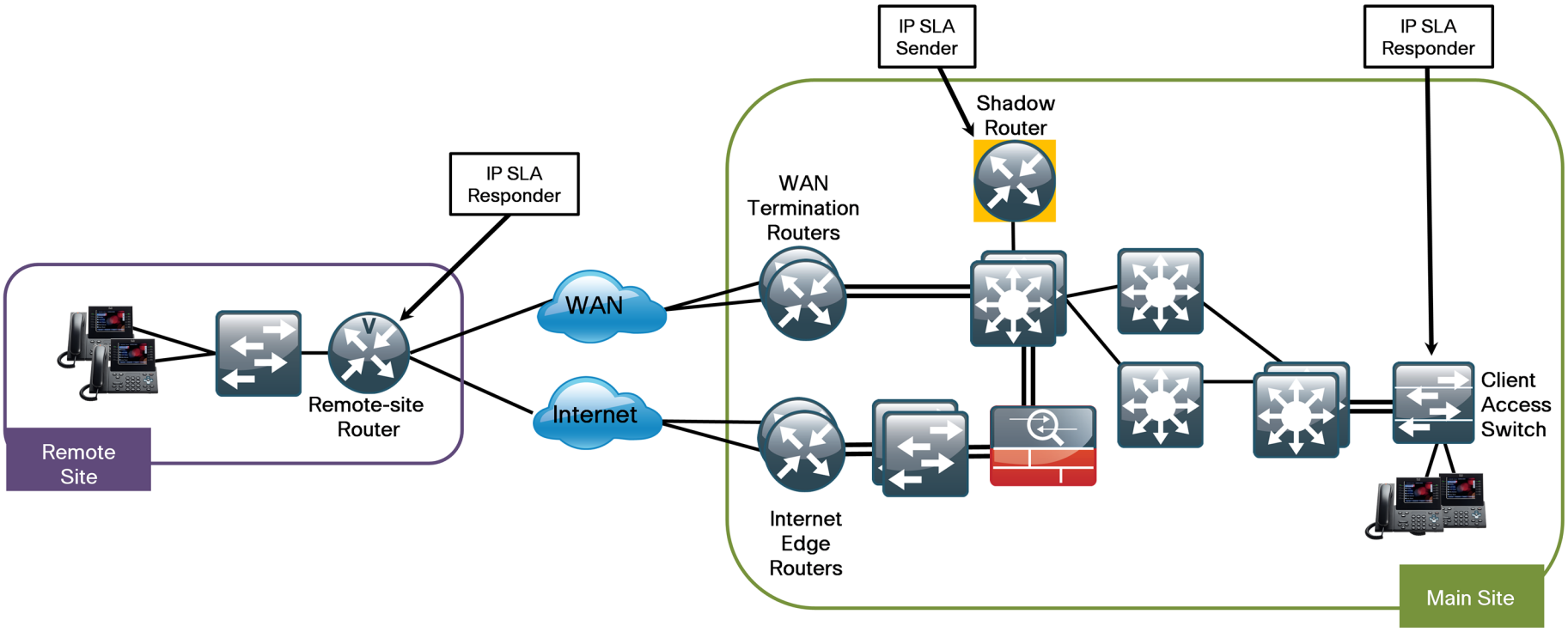


Procedure 2 Enable Cisco IP SLA responder

Cisco IP SLA can consist of two parts of an operation. IP SLA measurements that require only a target use only Cisco IP SLA sender on the source router. Examples of measurements that require only a target include ICMP Echo and TCP Connect to an IP host that has a TCP stack but no Cisco IOS software. For end-to-end two-way tests, such as UDP jitter, the remote device needs to run Cisco IP SLA responder as well.

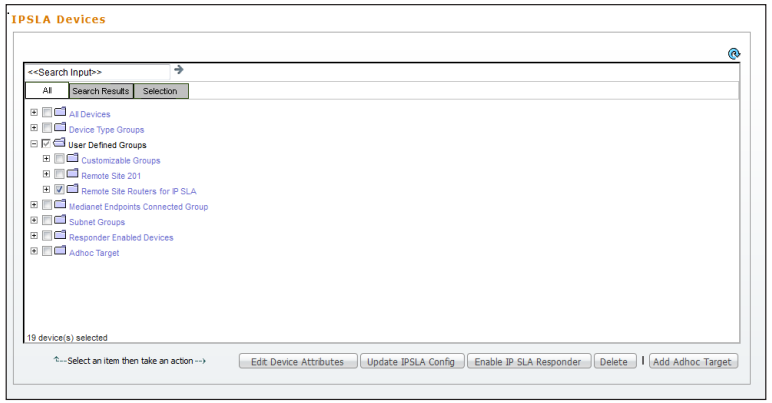
After you have mapped out the measurements you want to perform on your network, you should enable Cisco IP SLA responder on the remote routers and switches that you will include in your end-to-end measurements. A device programmed as a responder can also be programmed as a sender for other collection operations.

Figure 6 - IP SLA responder device location



Step 1: From the main Cisco Prime LMS window, navigate to **Inventory** > **Device Administration** > **IP SLA Devices**.

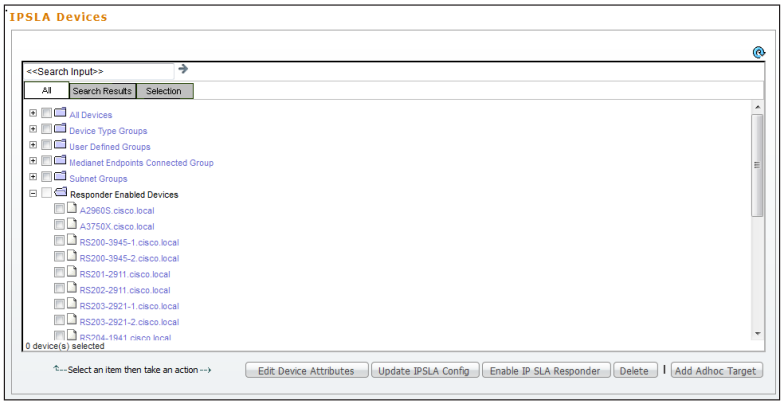
Step 2: Expand **User Defined Groups**, and then select the check box next to the group you created in Procedure 1.



Step 3: Expand **All Devices**, determine which additional devices need Cisco IP SLA responder enabled, and then select the check boxes next to those devices.

Step 4: Click **Enable IP SLA Responder**, and in the window that alerts you that Cisco IP SLA responder will be enabled only if SNMP RO and RW credentials are correct, click **OK**.

Step 5: Expand **Responder Enabled Devices**, and ensure that the correct devices appear in the list.



Process

Creating Cisco IP SLA Operations

1. Create a UDP jitter operation for IP voice
2. Create a UDP jitter operation for IP video
3. Create a Telnet (TCP) Connect operation
4. Create an HTTP Get operation

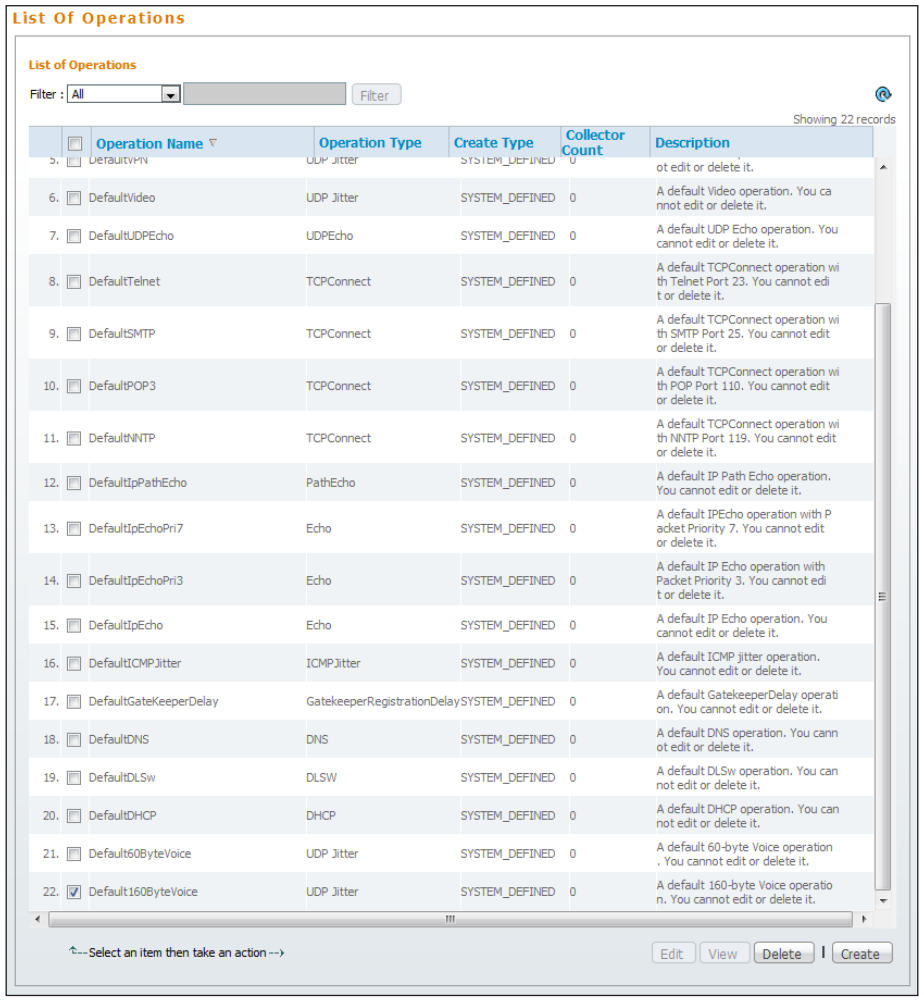
Cisco IP SLA operations are the IP packet–generation test types that measure performance on your network. The following four sample operations show you ways you can monitor your organization's network. If your organization's needs vary from these examples, you can create additional operations to meet your requirements.

In the "Creating IP SLA Collectors" process later in this guide, you create the endpoints that define the locations where you will use these operations to test performance.

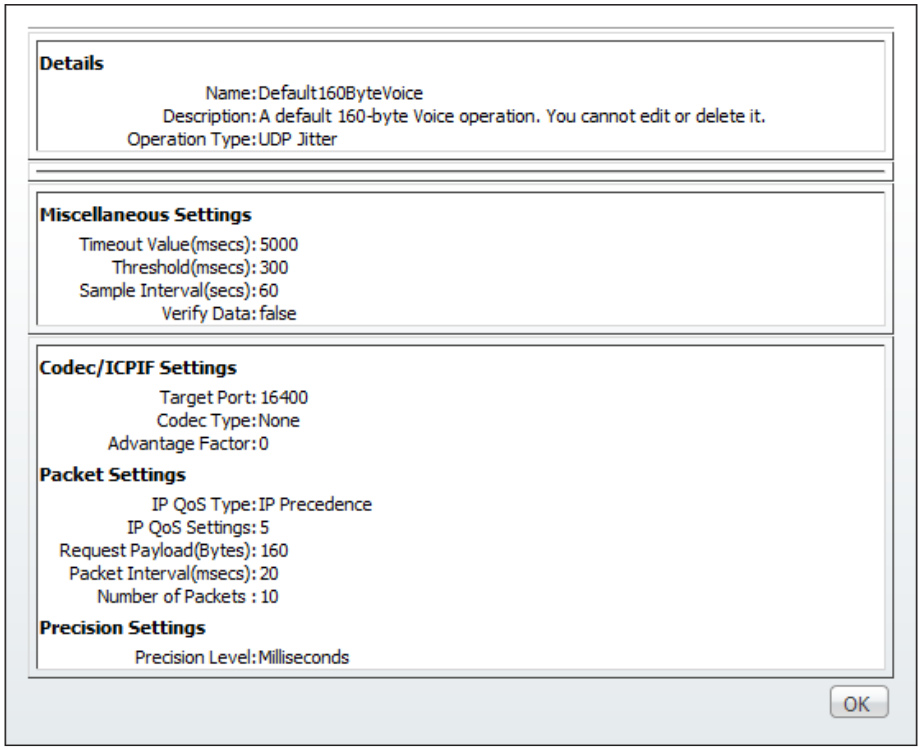
Procedure 1 Create a UDP jitter operation for IP voice

In this example, you create a voice packet test operation. The purpose of this operation type is to check for delay, jitter, and loss, all of which can affect IP-based voice in the network.

Step 1: From the main Cisco Prime LMS window, navigate to **Monitor > Performance Settings > IP SLA > Operations**.



Step 2: Select **Default160ByteVoice or Default60ByteVoice**, and then click **View**. A window appears that lists the settings in the system default operation.



Step 3: At the bottom of the **List of Operations** window, click **Create**.

Step 4: In the **Name** field, type a name for your operation. For this example, you can use SBA-UDP-Jitter-Voice-DSCP-46.

Step 5: In the **Type** list, choose **UDP Jitter**.

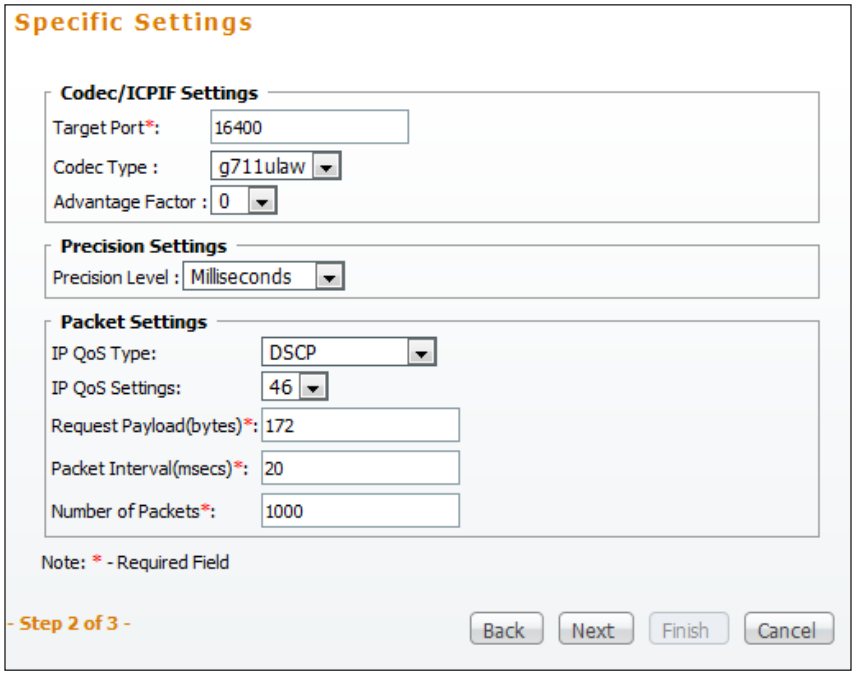
Step 6: If you want to generate SNMP traps for events that exceed your desired thresholds, configure **Reaction Settings**.

Step 7: Enter values for timeout, threshold, and sample interval, and then click **Next**.

Reader Tip

For more information about filling in fields, click **Help** in the upper-right corner of any window.

Step 8: In the **Target Port** field, type a port number for the UDP jitter operation; this example uses port 16400.



Step 9: In the **Codec Type** list, choose the type you are using in your network to generate MOS and IPCIF voice scores. If you are not using a codec, choose **None**.

Step 10: In the **Precision Level** list, choose **Milliseconds**.

Step 11: In the **IP QoS Type** list, choose **DSCP**. In this example, **DSCP 46** matches QoS settings for voice in the Cisco SBA network.

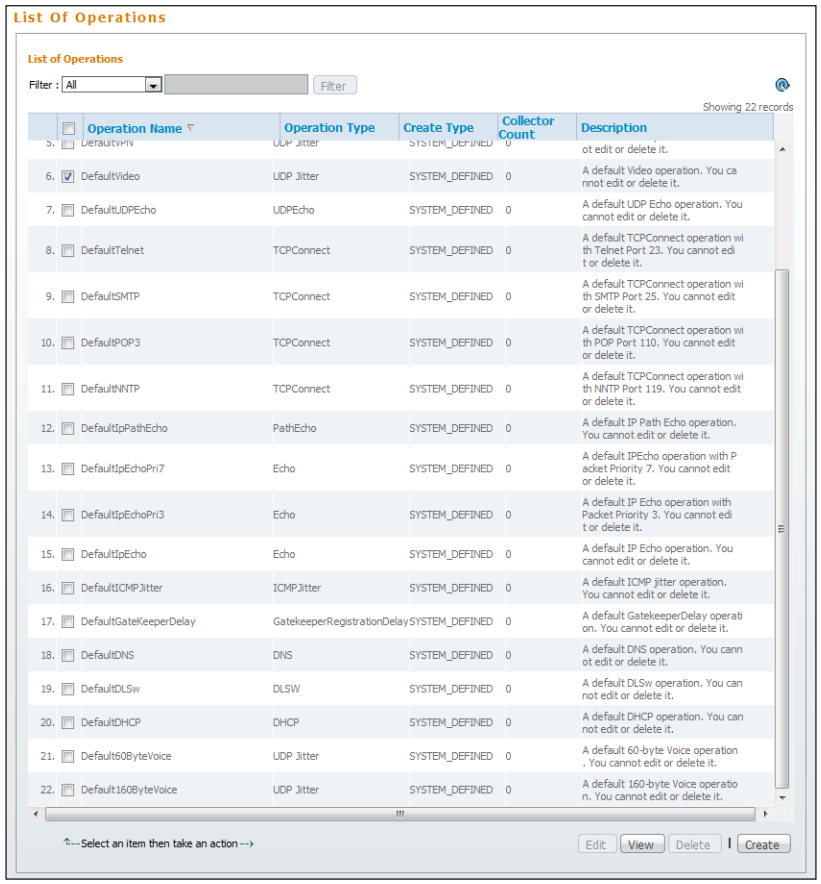
Step 12: Type values for the request payload size, packet interval and the number of packets, and then click **Next**.

Step 13: Ensure that your new operation is listed in the table of available operations, and then click **Finish**.

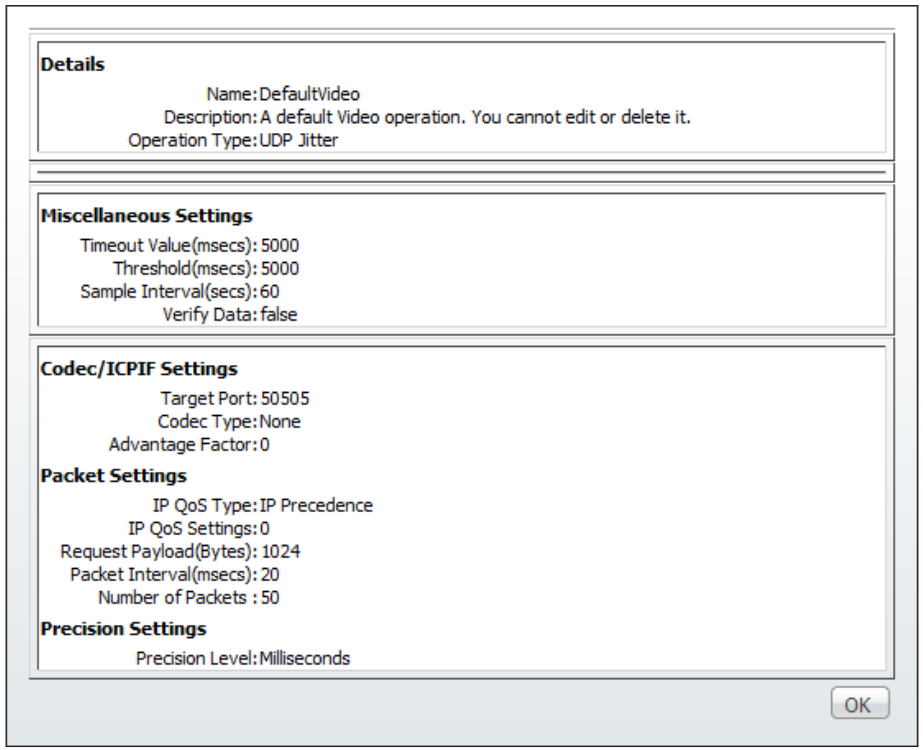
Procedure 2 Create a UDP jitter operation for IP video

In this example, you create a simulated video packet test operation. The purpose of this operation type is to check for delay, jitter, and loss, all of which can affect IP-based video in the network. Note that this test is not actually sending video streams but is emulating a video stream of IP packets.

Step 1: From the main Cisco Prime LMS window, navigate to **Monitor** > **Performance Settings** > **IP SLA** > **Operations**.

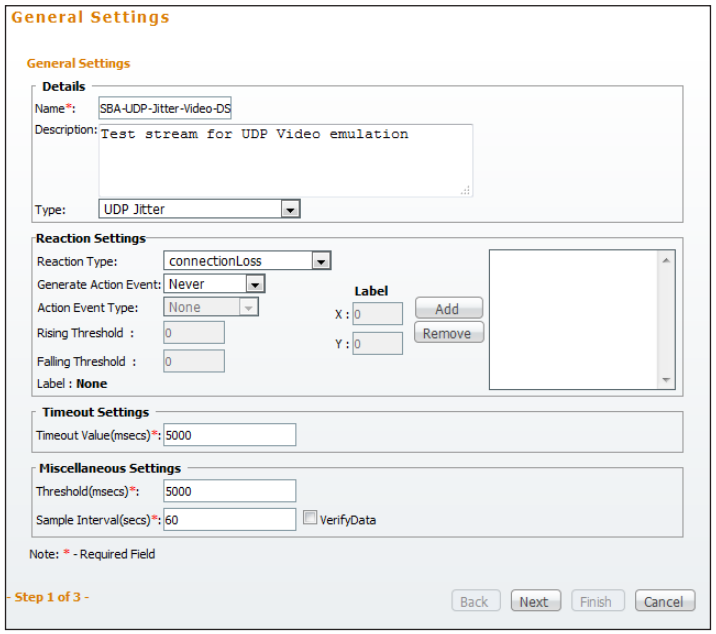


Step 2: Select **DefaultVideo**, and then click **View**. A window appears that lists the settings in the system default operation.



Step 3: At the bottom of the **List of Operations** window, click **Create**.

Step 4: In the **Name** field, type a name for your operation. For this example, you can use SBA-UDP-Jitter-Video-DSCP-46.

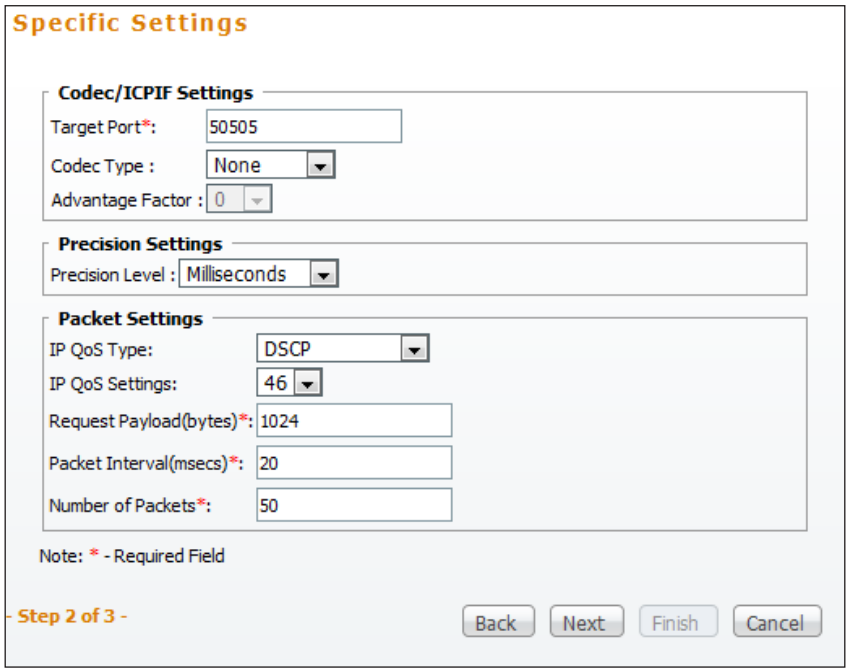


Step 5: In the **Type** list, choose **UDP Jitter**.

Step 6: If you want to generate SNMP traps for events that exceed your desired thresholds, configure **Reaction Settings**.

Step 7: Type values for timeout, threshold, and sample interval, and then click **Next**.

Step 8: In the **Target Port** field, type a port number for the UDP jitter operation.



Step 9: In the **Codec Type** list, leave the default selection of **None**.

Step 10: In the **Precision Level** list, choose **Milliseconds**.

Step 11: In the **IP QoS Type** list, choose **DSCP**. In this example, **DSCP 46** matches QoS settings for interactive video in the Cisco SBA network.

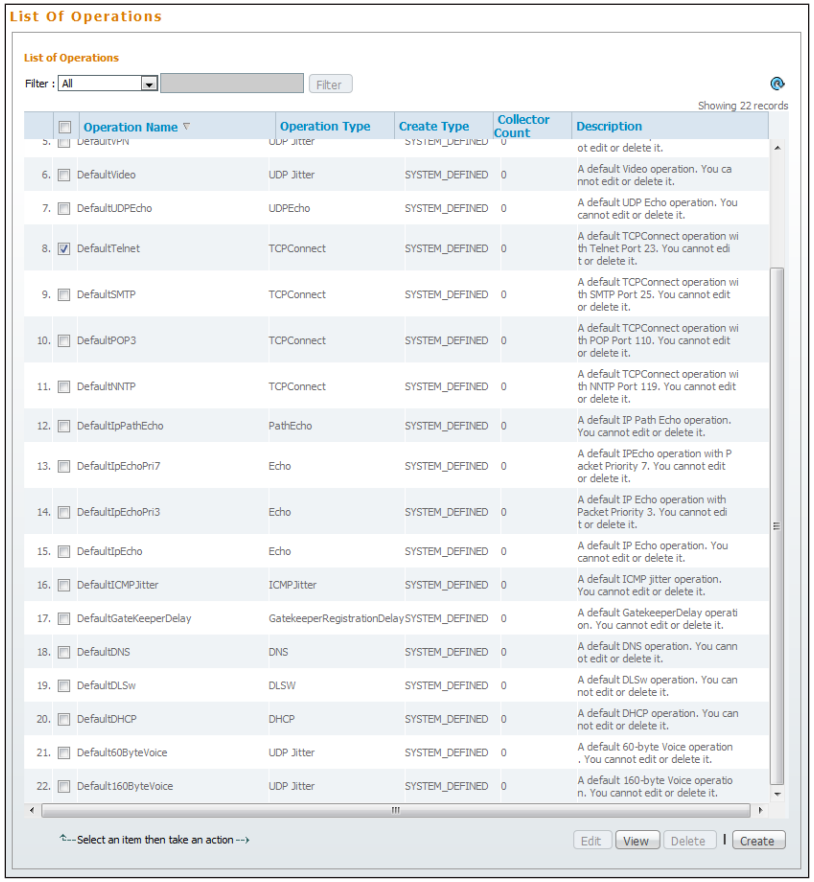
Step 12: Type a value for request payload size; this example uses 1024 from the template for default video. Type values for packet interval and number of packets, and then click **Next**.

Step 13: Review the Operation Summary, and then click **Finish**. Ensure that your new operation is listed in the table of available operations.

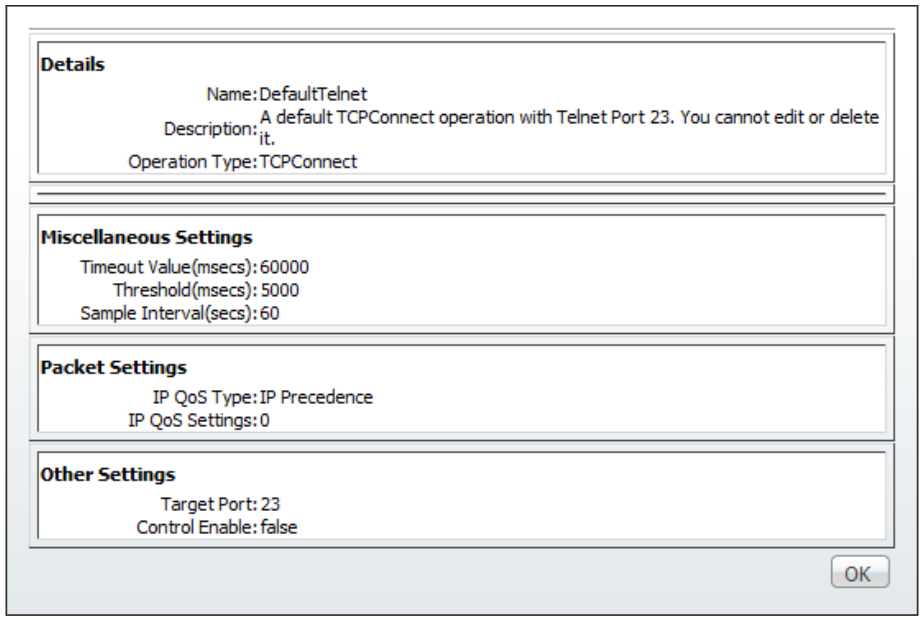
Procedure 3 Create a Telnet (TCP) Connect operation

In this example, you create a TCP Connect operation that runs from a remote-site router, or the shadow router, to a server in the data center. This operation measures connect times from the far remote site all the way to the server.

Step 1: From the main Cisco Prime LMS window, navigate to **Monitor > Performance Settings > IP SLA > Operations**.

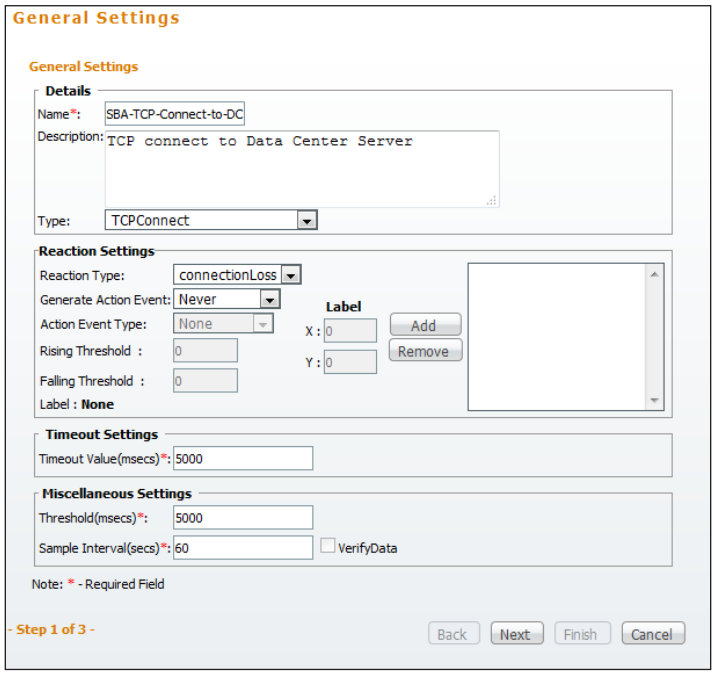


Step 2: Select **DefaultTelnet**, and then click **View**. A window appears that lists the settings in the system default operation.



Step 3: At the bottom of the **List of Operations** window, click **Create**.

Step 4: In the **Name** field, type a name for your operation. For this example, you can use SBA-TCP-Connect-to-DC-Server.

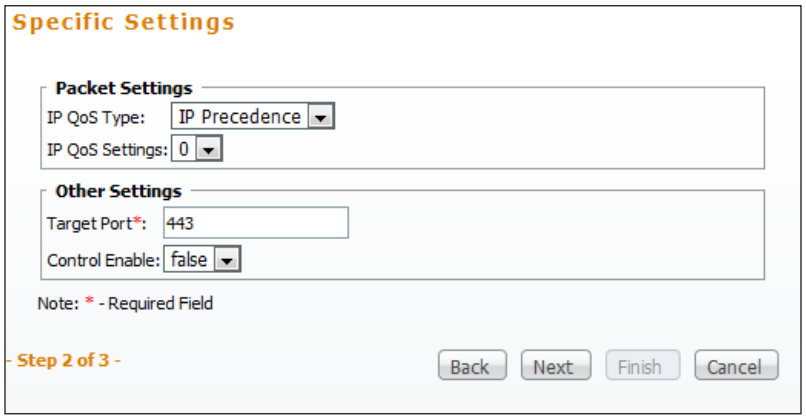


Step 5: In the **Type** list, choose **TCPConnect**.

Step 6: If you want to generate SNMP traps for events that exceed your desired thresholds, configure **Reaction Settings**.

Step 7: Type values for timeout, threshold, and sample interval, and then click **Next**.

Step 8: In the **IP QoS Settings** list, choose an appropriate value. If you have not defined any QoS settings, leave the default value of **0**.



Step 9: In the **Target Port** field, type a port number for the active application on the server, and then click **Next**.

Step 10: Ensure that your new operation is listed in the table of available operations, and then click **Finish**.

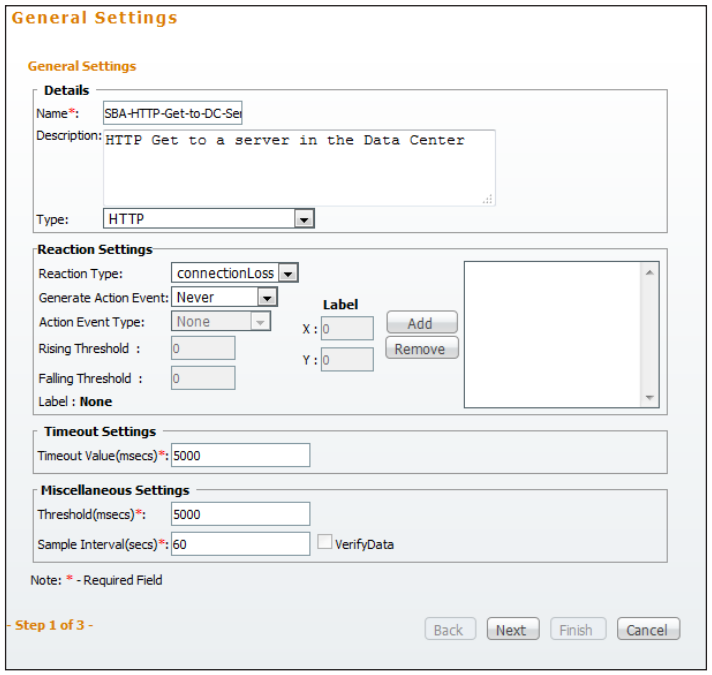
Procedure 4 Create an HTTP Get operation

In this example, you create an HTTP Get operation that runs from a remote-site router, or the shadow router, to a server in the data center. This operation measures connect times from the far remote site all the way to the server.

Step 1: From the main Cisco Prime LMS window, navigate to **Monitor** > **Performance Settings** > **IP SLA** > **Operations**.

Step 2: Click **Create** at the bottom of the window.

Step 3: In the **Name** field, type a name for your operation. For this example, you can use SBA-HTTP-Get-to-DC-Server.

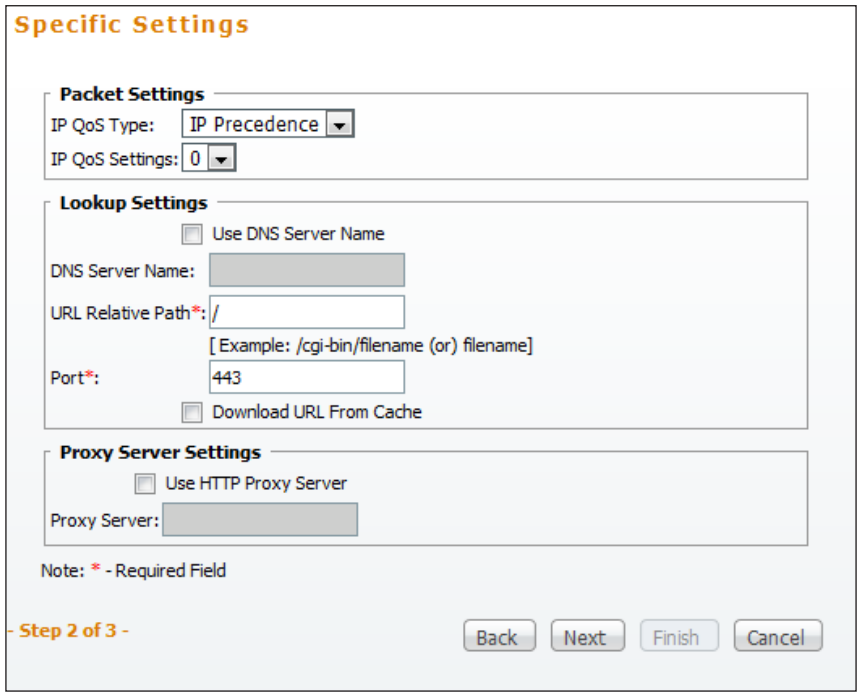


Step 4: In the **Type** list, choose **HTTP**.

Step 5: If you want to generate SNMP traps for events that exceed your desired thresholds, configure **Reaction Settings**.

Step 6: Type values for timeout, threshold, and sample interval, and then click **Next**.

Step 7: In the **IP QoS Settings** list, choose an appropriate value. If you have not defined any QoS settings, leave the default value of **0**.



Step 8: If you are using DNS, select **Use DNS Name**, and then type the DNS server name. This allows you to measure DNS lookup times.

Step 9: In the **URL Relative Path** field, type the relative path for the HTTP operation.

Step 10: In the **Port** field, type the port number for the application destination, and then click **Next**.

Step 11: Ensure that your new operation is listed in the table of available operations, and then click **Finish**.

Process

Deploying a Shadow Router

1. Apply router universal configuration
2. Connect to the LAN distribution switch
3. Configure the switch for the shadow router

A shadow router needs to be deployed to be a source device for IP SLA operations. You will use this device later when you create IP SLA collectors.

Procedure 1 Apply router universal configuration

You first need to apply the universal configuration to the shadow router.

Step 1: Configure the device host name.

```
hostname IP-SLA-2951
```

Step 2: Configure local login and password.

The local login account and password provide basic access authentication to a router and provide only limited operational privileges. The enable password secures access to the device configuration mode. By enabling password encryption, you prevent the disclosure of plain-text passwords when viewing configuration files. By default, HTTPS access to the router uses the enable password for authentication.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

Step 3: If you do not want to configure centralized user authentication, then skip to step 4.

As the number of devices to maintain on a network increases, there is an increasing operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (Secure Shell (SSH) Protocol and HTTPS) is controlled by AAA.

Reader Tip

The AAA server used in this architecture is the Cisco Authentication Control System. For details about ACS configuration, see the *Device Management Using ACS Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined in Step 2 on each network infrastructure device to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 4: Configure device management protocols.

HTTPS and SSH are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Secure management of the network device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy, and the nonsecure protocols, Telnet and HTTP, are turned off.

Specify "transport preferred none" on vty lines to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
 transport input ssh
 transport preferred none
```

When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. With this command, you can continue typing at the device console when debugging is enabled.

```
line con 0
 logging synchronous
```

Enable SNMP to allow the network infrastructure devices to be managed by an NMS. SNMPv2c is configured for both a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 5: If you do not want to create an access list, then skip to step 6.

In networks where network operational support is centralized, you can increase network security by using an access list to limit the networks that can access your device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
 access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

Tech Tip

If you configure an access list on the vty interface, you may lose the ability to use SSH to log in from one router to the next for hop-by-hop troubleshooting.

Step 6: Configure a synchronized clock.

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

You should program network devices to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source. By configuring console messages, logs, and debug output to provide time stamps on output, you can cross-reference events in a network.

```
ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Procedure 2 Connect to the LAN distribution switch

The following procedure creates a link from the shadow router to the rest of the network.

Step 1: Configure the interface and assign an IP address.

As a best practice, use the same channel numbering on both sides of the link where possible.

```
interface GigabitEthernet 0/0
 description Link to WAN-D3750X
 ip address 10.4.32.190 255.255.255.192
```

Step 2: Configure the default route.

Provide reachability information for the shadow router to reach the rest of the network using the default route.

```
ip route 0.0.0.0 0.0.0.0 10.4.32.129
```

Procedure 3 Configure the switch for the shadow router

The WAN distribution switch is the appropriate location to physically connect devices—such as the shadow router—at the WAN-aggregation site.

This guide assumes that the distribution layer switch has already been configured and only includes the procedures required to complete the connection of the switch to the shadow router. For more information about distribution layer switch configuration, see the *Borderless Networks LAN Deployment Guide*.

You must create a VLAN and switch virtual interface (SVI) for the shadow router and other devices that have similar connectivity requirements. This VLAN is referred to as the WAN service network.

Step 1: Configure Layer 2.

With the hub-and-spoke design, there are no spanning-tree loops or blocked links; however, Rapid Per VLAN Spanning Tree (PVST) is still enabled to protect against unintentional loops.

Create the VLAN and set the distribution layer switch to be the spanning-tree root for the VLAN (if necessary).

```
vlan 350
  name WAN_Service_Net
```

Step 2: Configure the access port connection to the shadow router and apply the egress QoS macro that was defined in the platform configuration procedure.

```
interface GigabitEthernet 2/0/5
  description IP-SLA-2951 Gig0/0
  switchport
  switchport access vlan 350
  switchport host
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  logging event bundle-status
```

Step 3: Configure Layer 3 (if necessary).

Configure an SVI so devices in the VLAN can communicate with the rest of the network.

```
interface Vlan350
  ip address 10.4.32.129 255.255.255.192
  ip pim sparse-mode
  no shutdown
```

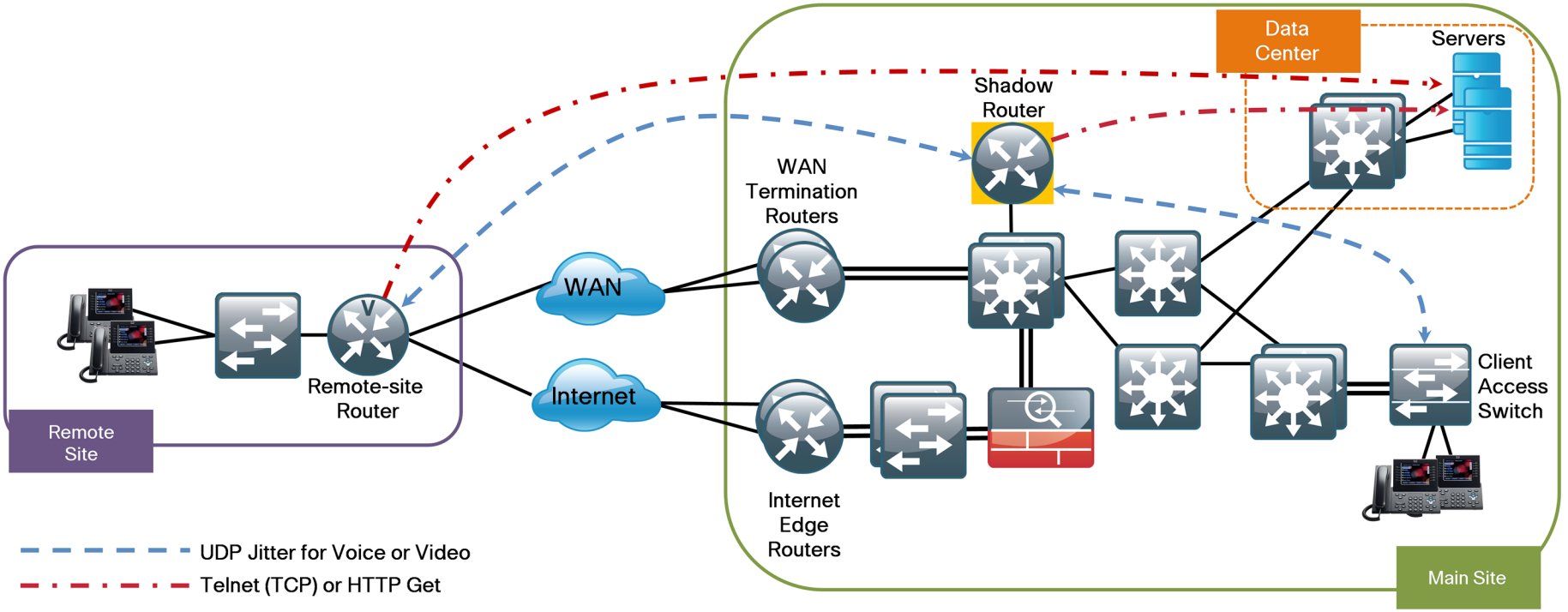
Process

Creating IP SLA Collectors

1. Create collectors for UDP jitter
2. Create collectors for TCP or HTTP Get

IP SLA collectors define the test source and destination endpoints you want to measure with the operations you create. In these procedures, you create sample collectors to support the operations you created in "Creating Cisco IP SLA Operations," earlier in this guide.

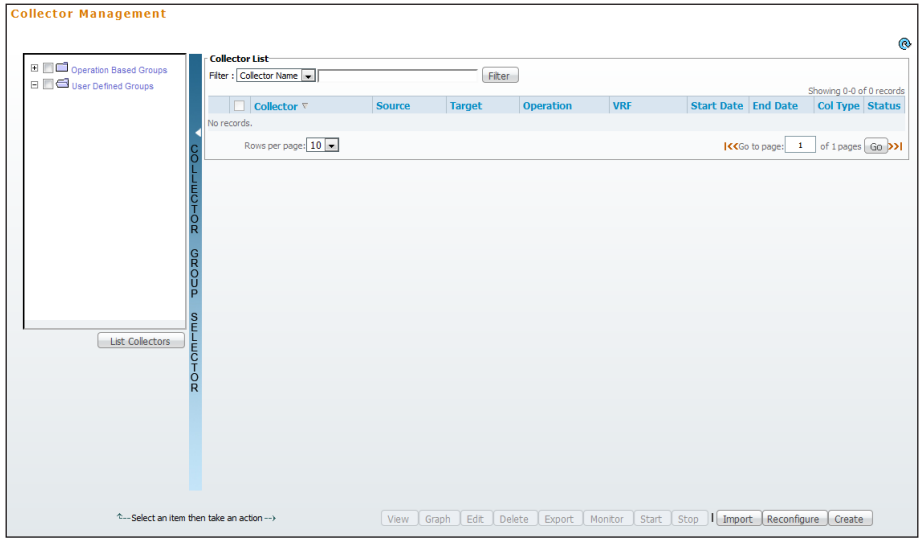
Figure 7 - IP SLA packet test streams



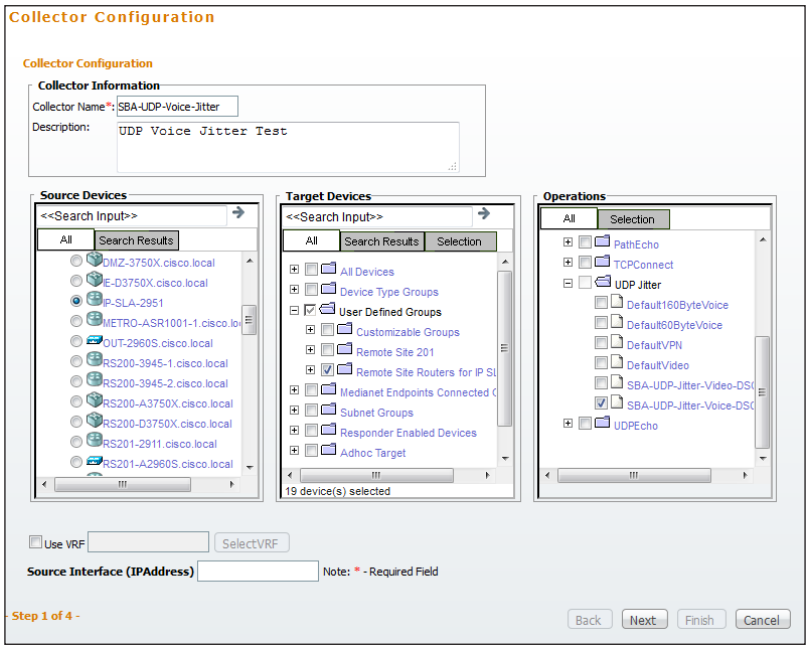
Procedure 1 Create collectors for UDP jitter

In this procedure, you define test endpoints and create a UDP jitter packet test that runs between the shadow router in the core of the network and the Cisco IP SLA responder in the remote-site routers. This test checks the WAN for delay, jitter, and loss. You then run another test between the shadow router and LAN switches in the campus to check for delay without the WAN component.

Step 1: From the main Cisco Prime LMS window, navigate to **Monitor** > **Performance Settings** > **IP SLA** > **Collectors**, and then click **Create**.



Step 2: In the **Name** field, type a name for the collector.



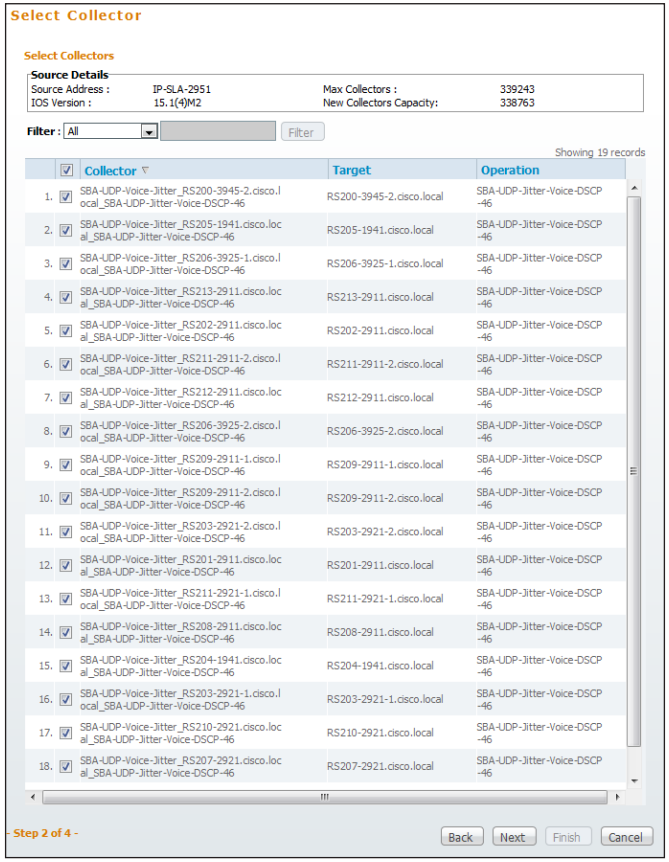
Step 3: In the **Source Devices** list, select the option button next to the source device for the operation. This example uses the shadow router 10.4.32.190. If your source router has multiple interfaces and multiple IP addresses, you can specify the source interface (IP address) to use.

Step 4: In the **Target Devices** list, select the check boxes next to the target devices for the operation. This example uses the user-defined group named Remote Site Routers for IP SLA and two LAN switches in the HQ Campus. This tests connections between the shadow router and each WAN router, as well as connections between the shadow router and the local LAN switches.

Step 5: In the **Operations** list, expand **UDP Jitter**.

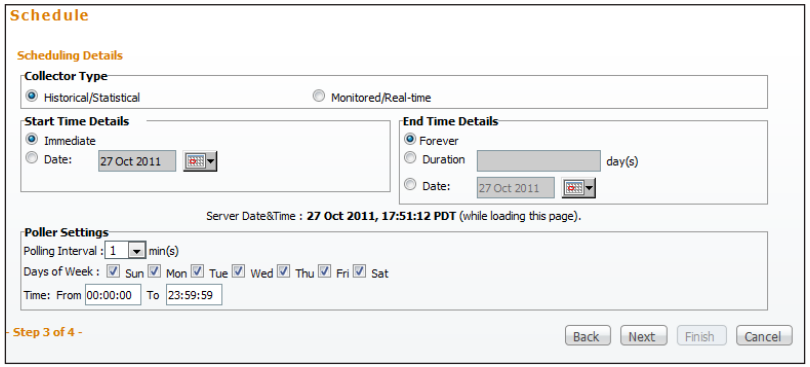
- For voice, select **SBA-UDP-Jitter-Voice-DSCP-46**. This is the operation you created in Procedure 1, "Create a UDP jitter operation for IP voice."
- For video, select **SBA-UDP-Jitter-Video-DSCP-46**. This is the operation you created in Procedure 2, "Create a UDP jitter operation for IP video."

Step 6: Click **Next**. The system creates a list of the collectors to be generated. At the top of the window, you see the details for the IP SLA source operation, maximum collectors supported, and collector capacity for new collectors.



Step 7: Ensure that the list is correct, and then click **Next**.

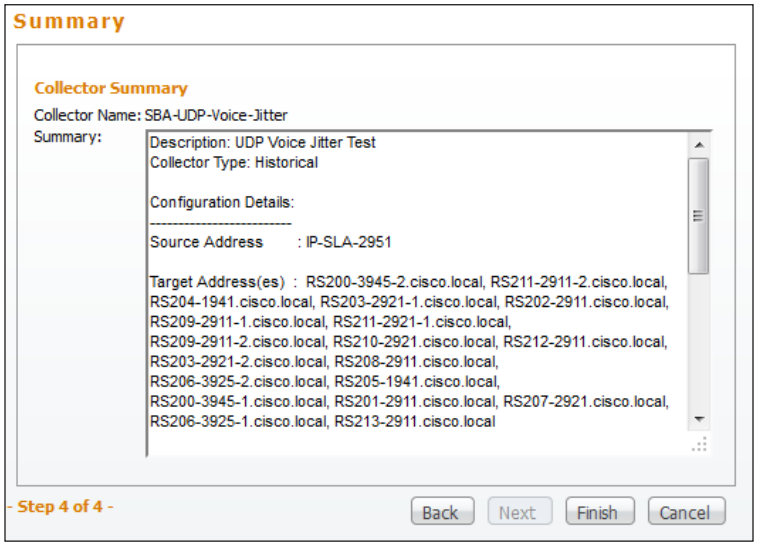
Step 8: In the **Collector Type** area, select a schedule type for running your collectors. In this example, you select **Historical/Statistical** to provide a database of collections over time.



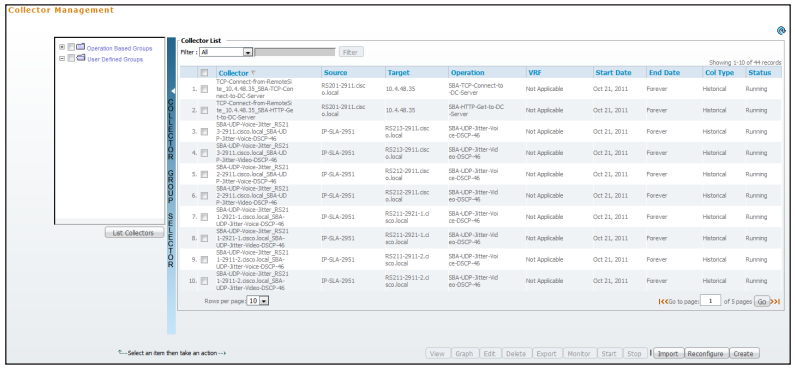
Step 9: Enter a start and end time. If you select **Forever**, the operation will run until you stop it.

Step 10: In the **Polling Interval** list, choose the amount of time that should elapse between the polling of routers for reports, and then click **Next**. To generate reports based on minute granularity, you must choose a polling interval of 1, 5, 15, or 30 minutes. You can generate historical reports and graphs for any polling interval.

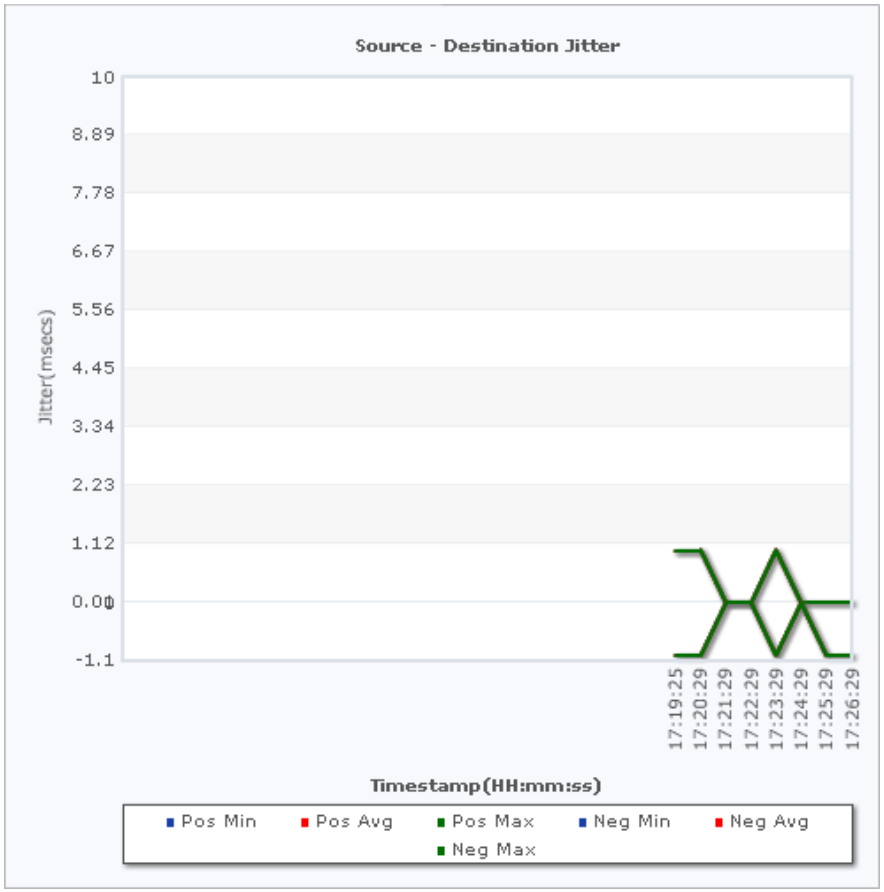
Step 11: Ensure that the Collector Summary is correct, and then click **Finish**. The system creates collectors and deploys them to the IP SLA devices. In this example, the schedule is set to begin immediately.



Step 12: To ensure that the operation is running, select one of the collectors you created, and then click **Monitor**.



Another browser window opens displaying the collector operations. In this example, you selected a polling interval of 1 minute, so you quickly see that the collector operation is proceeding as programmed.

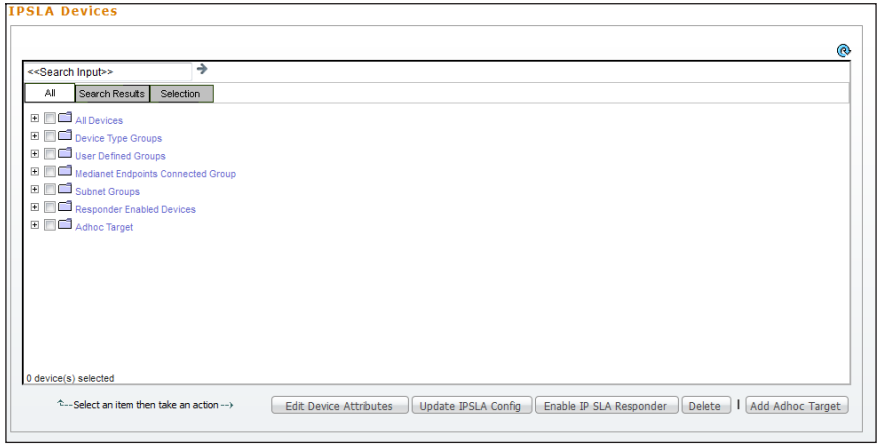


Procedure 2 Create collectors for TCP or HTTP Get

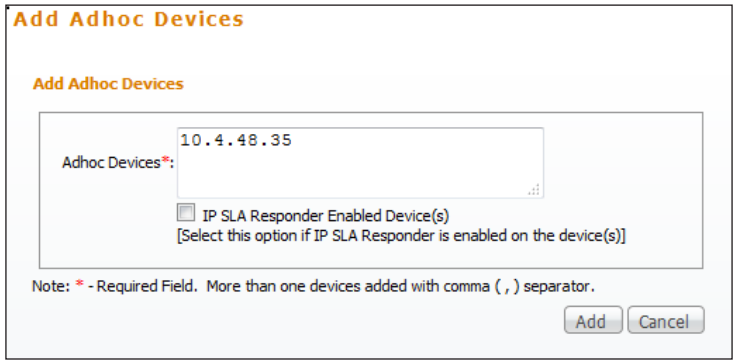
In this example, you define test endpoints and create a host access test that you can use for either a Telnet (TCP) Connect or HTTP Get operation. You set up the collector to run from a remote-site router to a server in the data center. This measures connect times from the far remote site all the way to the server. Because you can only select a single source, you can replicate

this operation for additional remote-site router tests. To measure connect times without the WAN component, set up an additional collector to sample from the shadow router to the server.

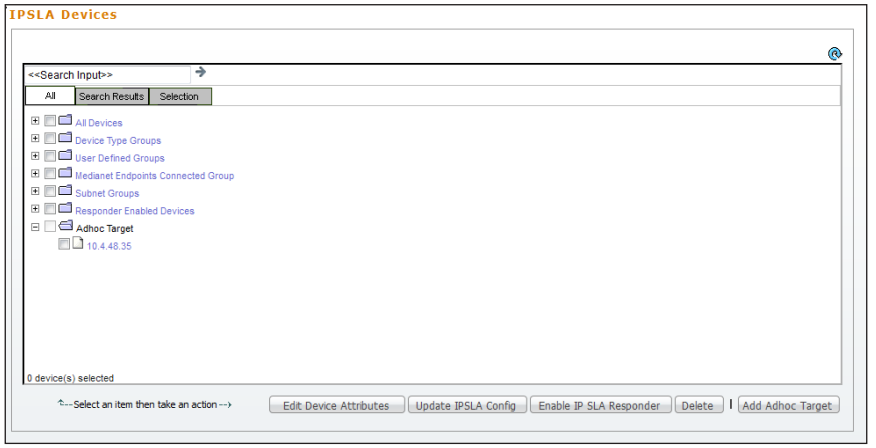
Step 1: Because Cisco Prime LMS does not learn all of the hosts on your network, you must define each host target separately for this test. To create a host machine, from the main Cisco Prime LMS window, navigate to **Inventory > Device Administration > IPSLA Devices**, and then click **Add Adhoc Target**.



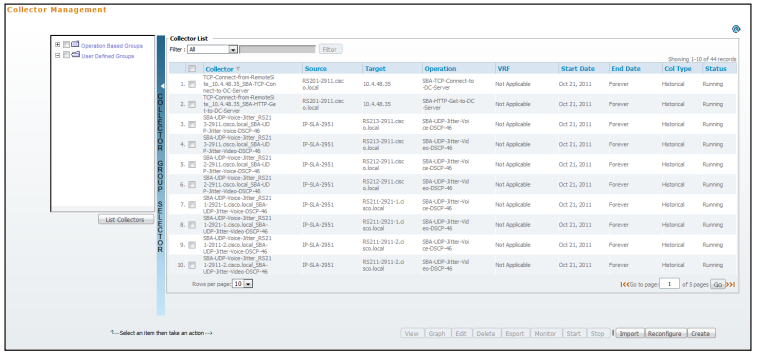
Step 2: In the **Adhoc Devices** field, type the IP address of the servers you wish to add as targets for the TCP Connect operation, and then click **Add**. This example uses 10.4.48.35.



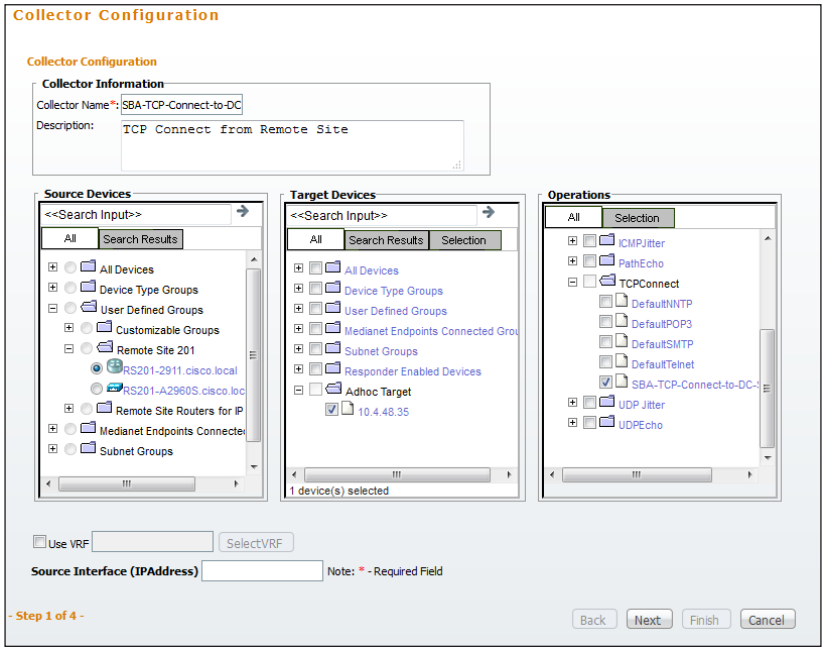
Step 3: After the devices are successfully added, expand **Adhoc Target**.



Step 4: Navigate to **Monitor > Performance Settings > IP SLA > Collectors**, and then click **Create**.



Step 5: In the **Name** field, type a name for the collector.



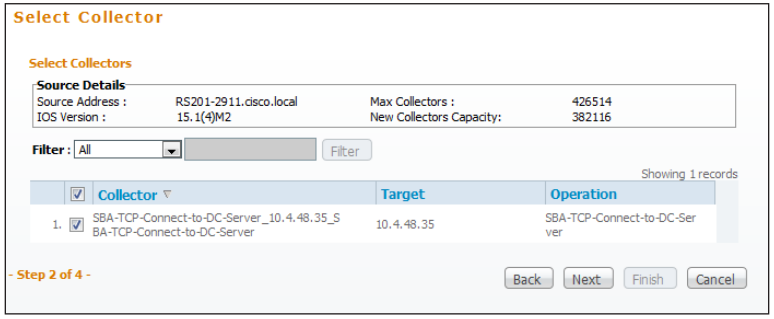
Step 6: In the **Source Devices** list, select the option button next to the source device for the operation. This example uses **Remote Site br201**. Because the source router has multiple interfaces and multiple IP addresses, you specify the source interface (IP address) to use.

Step 7: In the **Target Devices** list, select the check boxes next to the target devices for the operation. In this example, you use the ad-hoc target **10.4.48.35** that you added in Step 2.

Step 8: In the **Operations** list, do the following:

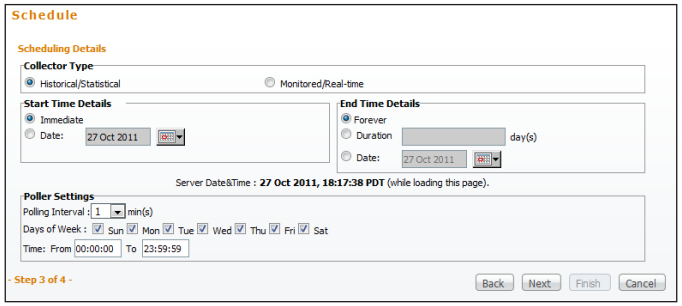
- For Telnet Connect, expand **TCPConnect**, and then select **SBA-TCP-Connect-to-DC-Server**.
- For HTTP Get, expand **HTTP**, and then select **SBA-HTTP-Get-to-DC-Server**.

Step 9: Click **Next**. The system creates a list of the collectors to be generated. At the top of the window, you see the details for the IP SLA source operation, maximum collectors supported, and collector capacity for new collectors.



Step 10: Ensure that the list is correct, and then click **Next**.

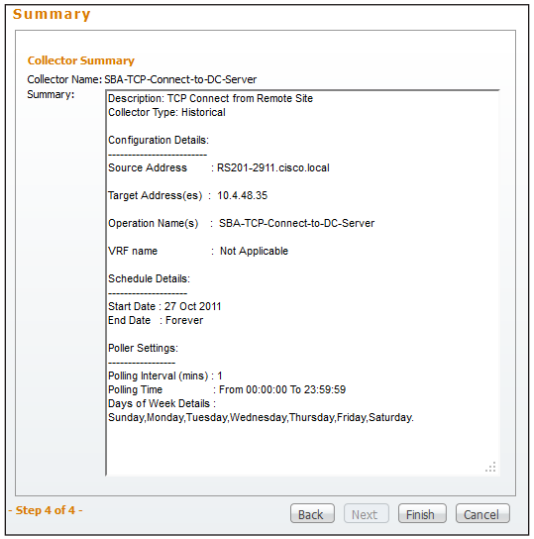
Step 11: In the **Collector Type** area, select a schedule type for running your collectors. In this example, you select **Historical/Statistical** to provide a database of collections over time.



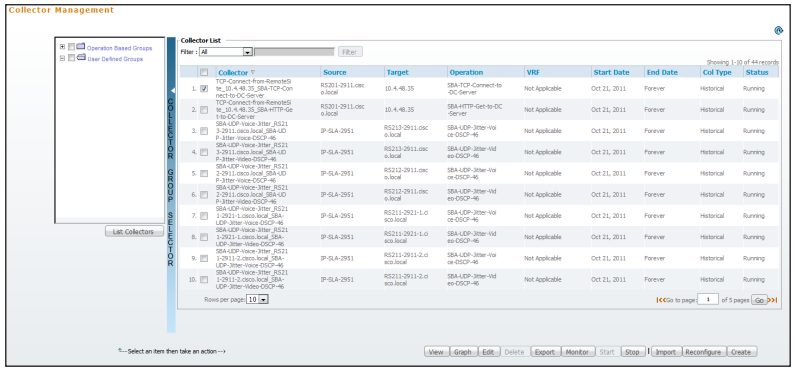
Step 12: Enter a start and end time. If you select **Forever**, the operation will run until you stop it.

Step 13: In the **Polling Interval** list, choose the amount of time that should elapse between the polling of routers for reports, and then click **Next**. To generate reports based on minute granularity, you must choose a polling interval of 1, 5, 15, or 30 minutes. You can generate historical reports and graphs for any polling interval.

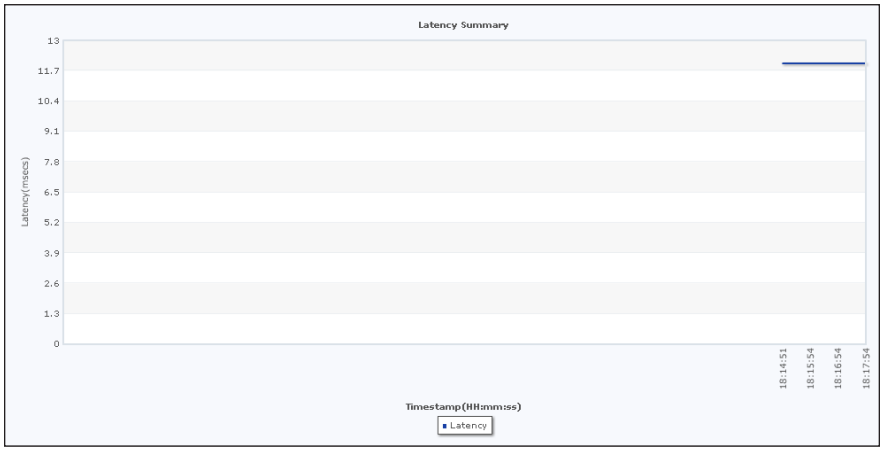
Step 14: Review the **Collector Summary**, and then click **Finish**. The system creates collectors and deploys them to the IP SLA devices. In this example, you set the schedule to begin immediately.



Step 15: To ensure that the operation is running, select one of the collectors you created, and then click **Monitor**.



Another browser window opens displaying the collector operations. In this example, you selected a polling interval of 1 minute, so you quickly see that the collector operation is proceeding as programmed.



Process

Generating IP SLA Reports

1. Generate an immediate report
2. Generate scheduled reports

Cisco IP SLA performance reporting can generate both immediate and scheduled reports. *Immediate* reports and graphs are generated instantly and are not stored in the report archives. *Scheduled* reports and graphs are set to run at a specific time. Using the publish option, you can store the scheduled reports for future reference.

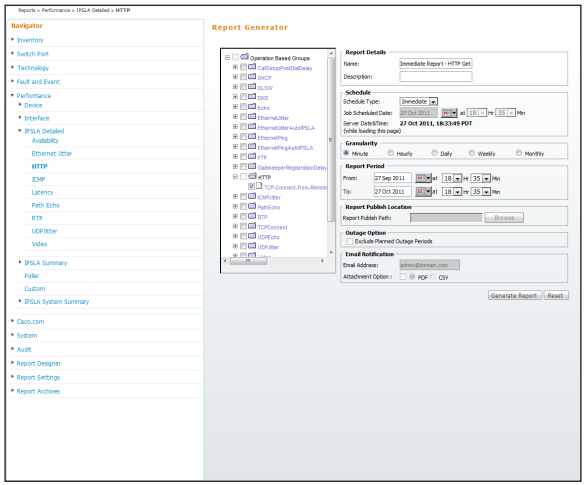
The following reports are available:

- **HTTP**—Reports DNS lookup times, TCP Connect times, page load times, and completion summary statistics for HTTP test operations.
- **UDP Jitter**—Reports two-way jitter and latency times, round-trip latency, and MOS and CPIF scores if they are enabled.
- **Latency**—Reports latency, errors, and completion information for TCP test operations.

Procedure 1 Generate an immediate report

In this example, you configure the system to generate an HTTP report on demand.

Step 1: From the main Cisco Prime LMS window, navigate to **Reports > Performance > IP SLA Detailed.**



Step 2: In the **Navigator** pane, expand **IP SLA Detailed**, and then select **HTTP**.

Step 3: In the **Operation Based Groups** list, expand **HTTP** to view a list of the defined collectors for that operation, and then select **SBA-HTTP-Get-Test**.

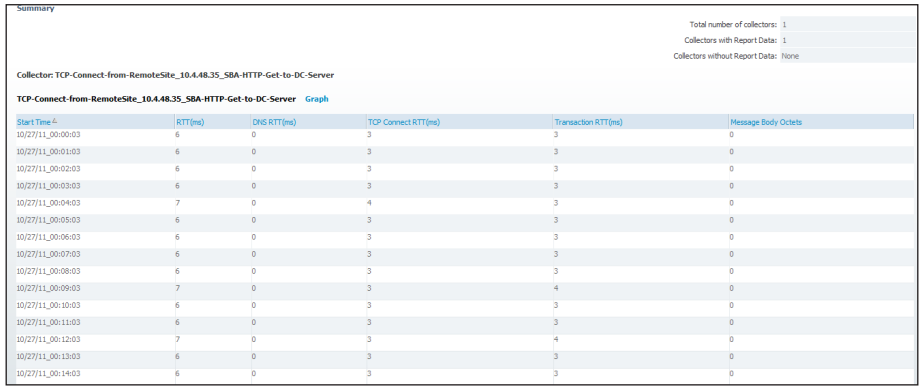
Step 4: In the **Name** field, type a name for the report or leave the field blank.

Step 5: In the **Schedule Type** list, choose **Immediate**.

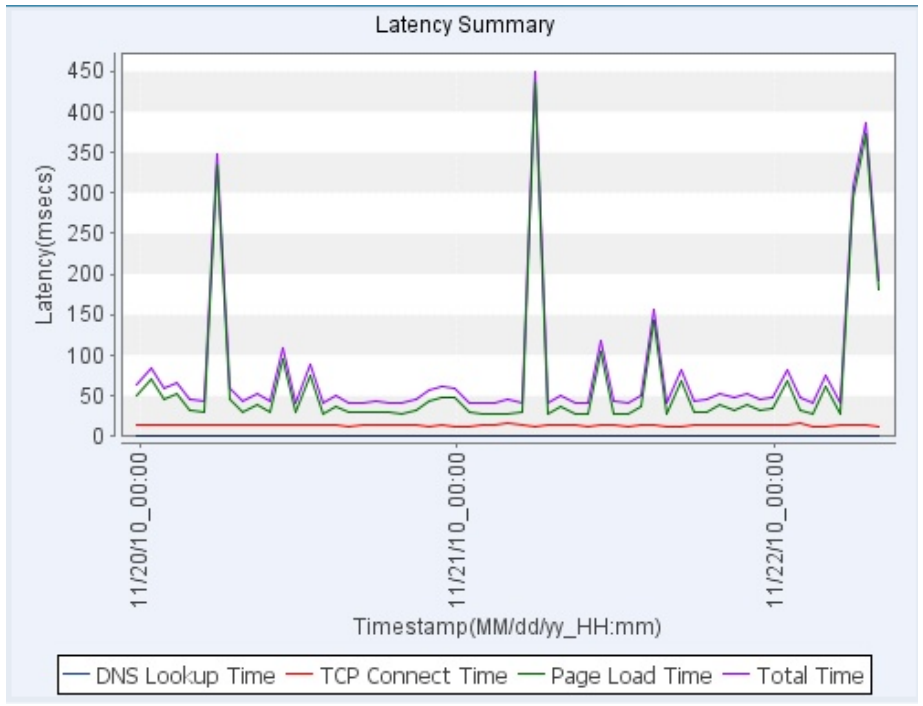
Step 6: To generate a report that covers a period of multiple days, select **Hourly**. Selecting **Minute** will only allow you to generate a report of one day or less.

Step 7: Enter **From** and **To** dates for the report period, and then click **Generate Report**.

A browser window opens displaying the table- and text-based results.



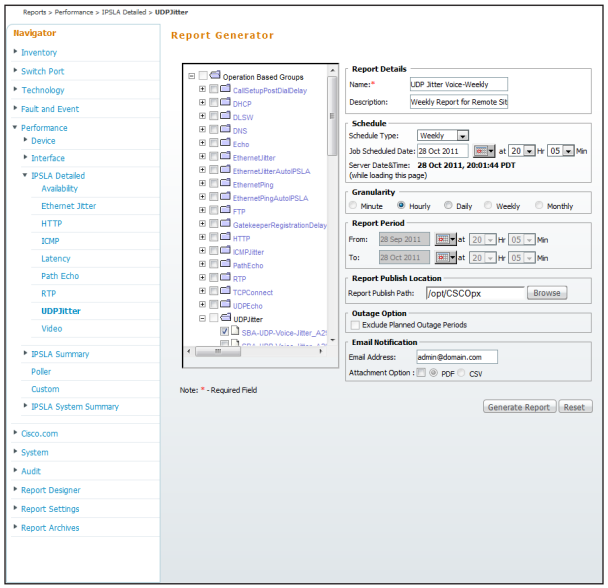
Step 8: To see the results in a graphic format, click **Graph** next to the operation type heading. A new browser window opens displaying the results.



Procedure 2 Generate scheduled reports

In this example, you configure a scheduled report for the UDP jitter for IP voice test.

Step 1: From the main Cisco Prime LMS window, navigate to **Reports > Performance > IP SLA Detailed**.



Step 2: In the **Navigator** pane, expand the **IPSLA Detailed**, and then select **UDP Jitter**.

Step 3: In the **Operation Defined Groups** list, expand **UDP Jitter**, and then select **SBA-UDP-Jitter-Voice**.

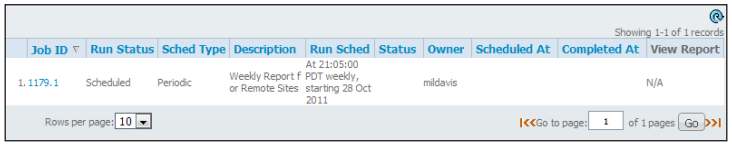
Step 4: In the **Name** field, type a name for the report.

Step 5: In the **Schedule Type** list, choose an interval for the scheduled report. In this example, you choose **Weekly**.

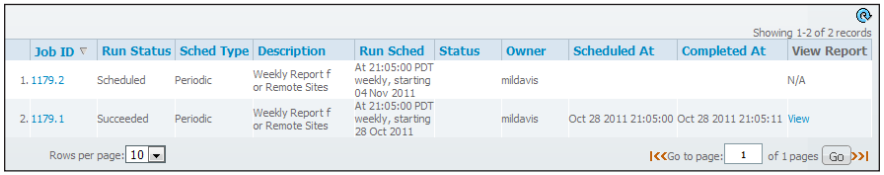
Step 6: To generate a report that covers a multi-day period, select **Hourly**. Selecting **Minute** only allows you to generate a report of one day or less.

Step 7: Click **Generate Report**.

The browser window updates and displays the new scheduled report job in a table at the bottom of the window.



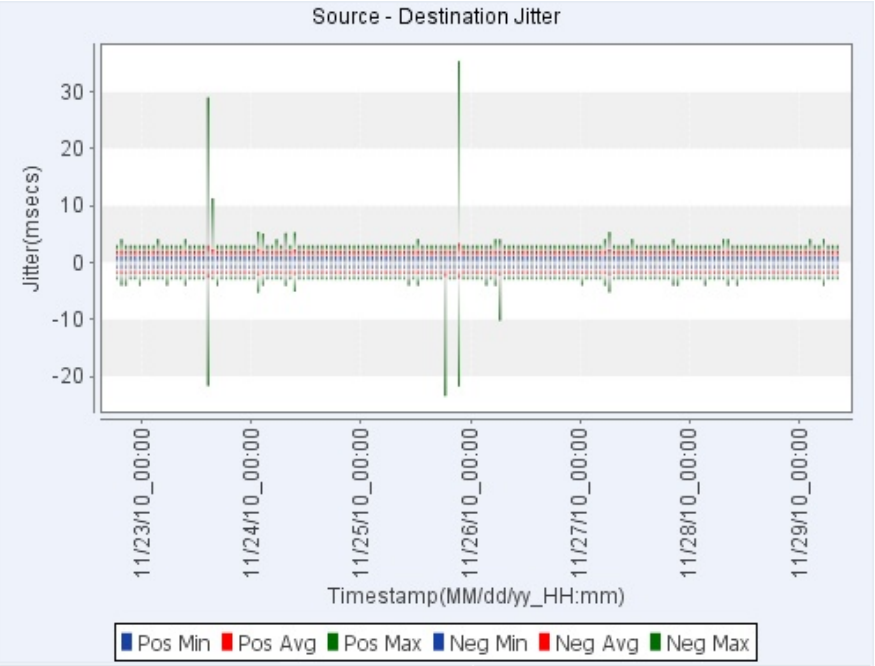
After the report runs, its status changes to Succeeded.



Step 8: In the right-hand column of the scheduled reports table, click **View** to see the report data. A new browser window opens displaying the table- and text-based results.

The **View** command is only available after the report has been run at its scheduled time.

Step 9: To see the results in a graphic format, click **Graph** next to the operation type heading. A new browser window opens displaying the results.



Source - Destination Jitter	msecs
Positive Maximum:	32
Pos. Average Maximum:	1.55
Pos. Average:	1.03
Pos. Average Minimum:	1.00
Negative Maximum:	-21
Neg. Average Maximum:	1.56
Neg. Average:	1.02
Neg. Average Minimum:	1.00

Notes

Appendix A: Product List

Network Management

Functional Area	Product Description	Part Numbers	Software
Network Management	Cisco Prime Infrastructure 1.1	R-PI-1.1-K9	4.2
	Prime Infrastructure 1.1 Software – 5K Device Base License	R-PI-1.1-5K-K9	
	Prime Infrastructure 1.1 Software – 2.5K Device Base License	R-PI-1.1-2.5K-K9	
	Prime Infrastructure 1.1 Software – 1K Device Base License	R-PI-1.1-1K-K9	
	Prime Infrastructure 1.1 Software – 500 Device Base License	R-PI-1.1-500-K9	
	Prime Infrastructure 1.1 Software – 100 Device Base License	R-PI-1.1-100-K9	
	Prime Infrastructure 1.1 Software – 50 Device Base License	R-PI-1.1-50-K9	

WAN Aggregation

Functional Area	Product Description	Part Numbers	Software
WAN-aggregation Router	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	IOS-XE 15.2(2)S
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	Advanced Enterprise
WAN-aggregation Router	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.1(4)M4
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	securityk9, datak9
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
Modular WAN Remote-site Router	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
Modular WAN Remote-site Router	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	15.1(4)M4 securityk9, datak9
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.1(4)M4 securityk9, datak9

Appendix B: Configuration Files

IP-SLA-2951

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname IP-SLA-2951
!
boot-start-marker
boot system flash0:c2951-universalk9-mz.SPA.151-4.M4.bin
boot-end-marker
!
!
logging buffered 51200 warnings
enable secret 5 $1$E5HW$DV.rY5AKCzW/Hw0CkZvJL/
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
!
ip domain name cisco.local
ip name-server 10.4.48.10
multilink bundle-name authenticated
!
!
!
!
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-4084286964
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4084286964
 revocation-check none
!
!
crypto pki certificate chain TP-self-signed-4084286964
 certificate self-signed 01
  3082024F 308201B8 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 34303834 32383639 3634301E 170D3132 30373137
30373236
```

```
  31355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34
30383432
  38363936 3430819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100B40C 68F38B82 02A5D128 018C3222 6709C6E9 8350EDFF 09BC7886
69EA2C89
  DD1E0BD6 977C6C9D 622FEF7D 3F0BB4D2 7D346EB7 E4342163 EDF78F12
95F86148
  7165DD82 66604A28 3D2D1881 13317C9F 80FE5806 02B4EF5F 18184D0B
B6F1C037
  355723C0 95941881 CCB0248A E4AD3E9B 1720CC52 2A462E70 05BDF6E6
EB425272
  32B30203 010001A3 77307530 0F060355 1D130101 FF040530 030101FF
30220603
  551D1104 1B301982 1749502D 534C412D 32393531 2E636973 636F2E6C
6F63616C
  301F0603 551D2304 18301680 147B49DF 30C8E3B9 8F7057C8 5B7680A8
713F4CF5
  D3301D06 03551D0E 04160414 7B49DF30 C8E3B98F 7057C85B 7680A871
3F4CF5D3
  300D0609 2A864886 F70D0101 04050003 8181002A 62F4B20C 2F93E16B
B4036074
  18FC1F12 CB270EE6 54437A6A DC0B9704 0CAF11F3 53C23E37 F702627A
102D6674
  131816A1 4AD674FB C8390C3E BB4DDBB5 39D5BF17 D1AFCB4E F819C5F3
09D6DB4F
  C83A0BF3 71B2A836 2A7053E4 F85D0013 675916B1 9DFE4CB3 2E11CD69
B679001B
  DFFAEB98 89D1ADE7 B99802F8 9191F01D FD434D
       quit
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2951/K9 sn FTX1452AH3K
hw-module pvdm 0/0
!
!
!
username admin password 7 06055E324F41584B56
!
redundancy
!
!
ip ssh version 2
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description Links to WAN-D3750X (Gig 1/0/15)
 ip address 10.4.32.190 255.255.255.192
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
```

```
 duplex auto
 speed auto
!
ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.4.32.129
!
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 55 permit 10.4.48.0 0.0.0.255
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
tacacs-server host 10.4.48.15 key 7 142417081E013E002131
tacacs server TACACS-SERVER-1
 key 7 15210E0F162F3F0F2D2A
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class 55 in
 privilege level 15
 transport preferred none
 transport input ssh
line vty 5 15
 access-class 55 in
 privilege level 15
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp server 10.4.48.17
end
```

Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We upgraded the Cisco Prime LMS software to 4.2.
- We made minor changes to improve the readability of this guide.

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

B-0000255-1 8/12