



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.....	1	Appendix A: Product List	31
Cisco SBA Borderless Networks.....	1	Appendix B: Configuration Files.....	33
Route to Success	1	IP-SLA-2951	33
About This Guide	1	Appendix C: Changes	36
Introduction.....	2		
Business Overview.....	2		
Technology Overview	3		
Deployment Details.....	7		
Grouping Devices and Enabling Cisco IP SLA Responder	7		
Creating Cisco IP SLA Operations	10		
Deploying a Shadow Router	18		
Creating IP SLA Collectors.....	21		
Generating IP SLA Reports	27		

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

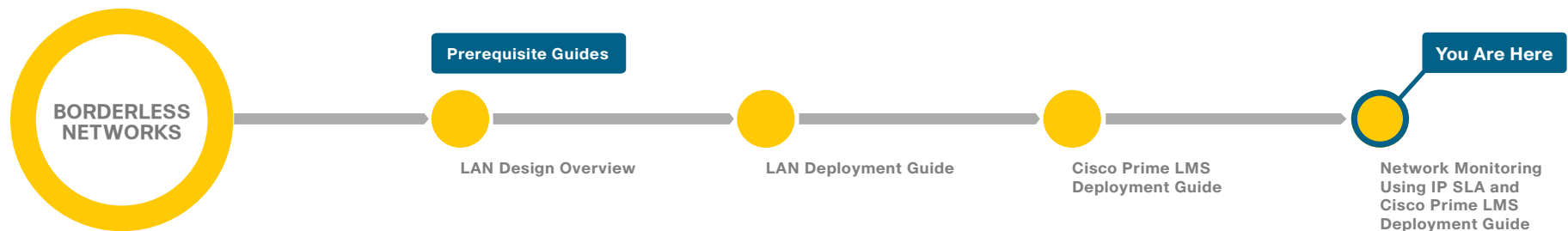
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **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

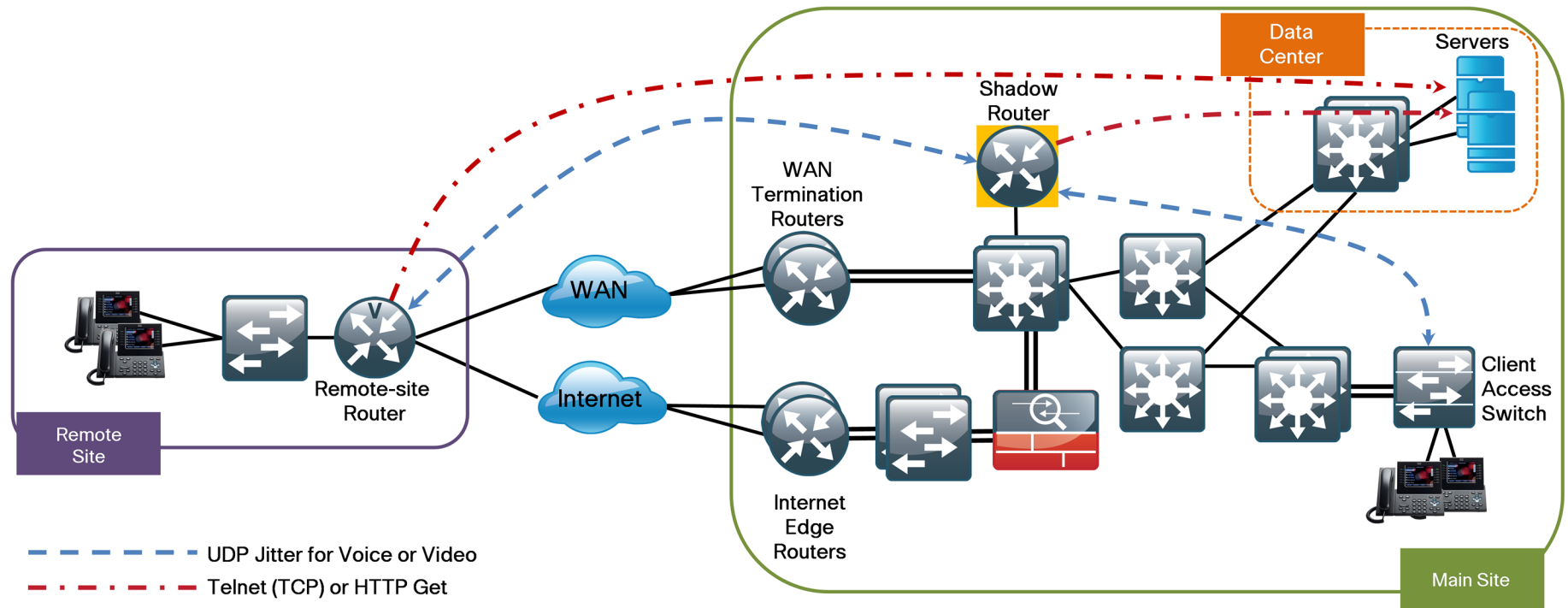
Business Overview

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

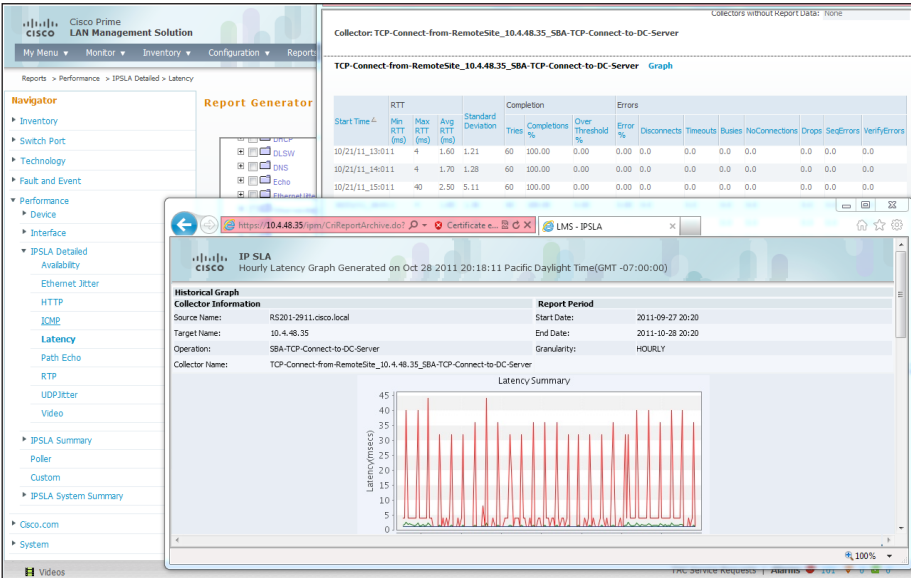
Cisco® Small Business Architecture (SBA)—Borderless Networks is based on building a sound foundation network that allows IT organizations to add network services that provide end users with effective access to their applications. Cisco SBA uses Cisco routers and LAN switches that provide the intelligence 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)

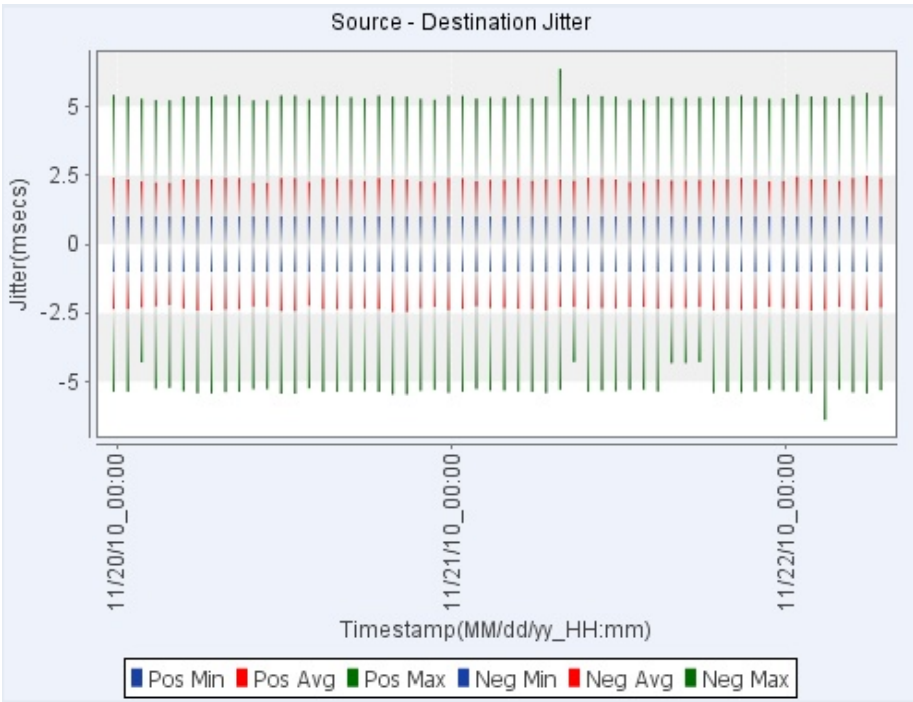
Deploying and managing multiple IP SLA endpoints can be challenging if done on a device-by-device basis using CLIs. Cisco Prime LAN Management Solution (Cisco Prime LMS) offers an integrated suite of management functions that simplify the configuration, administration, monitoring, and troubleshooting 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



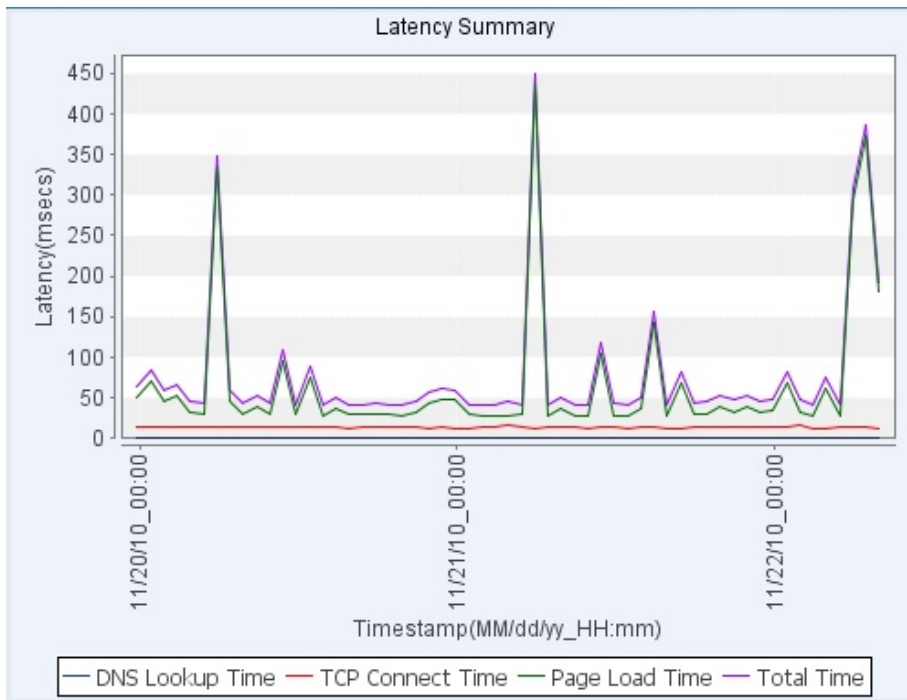
Cisco Prime LMS and Cisco IP SLA use User Datagram Protocol (UDP) streams from routers and switches in the network to test for jitter, latency, and loss that could affect delivery of voice and video. This allows IT to analyze delay and loss across WAN and Internet links as well as in the larger campus 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.

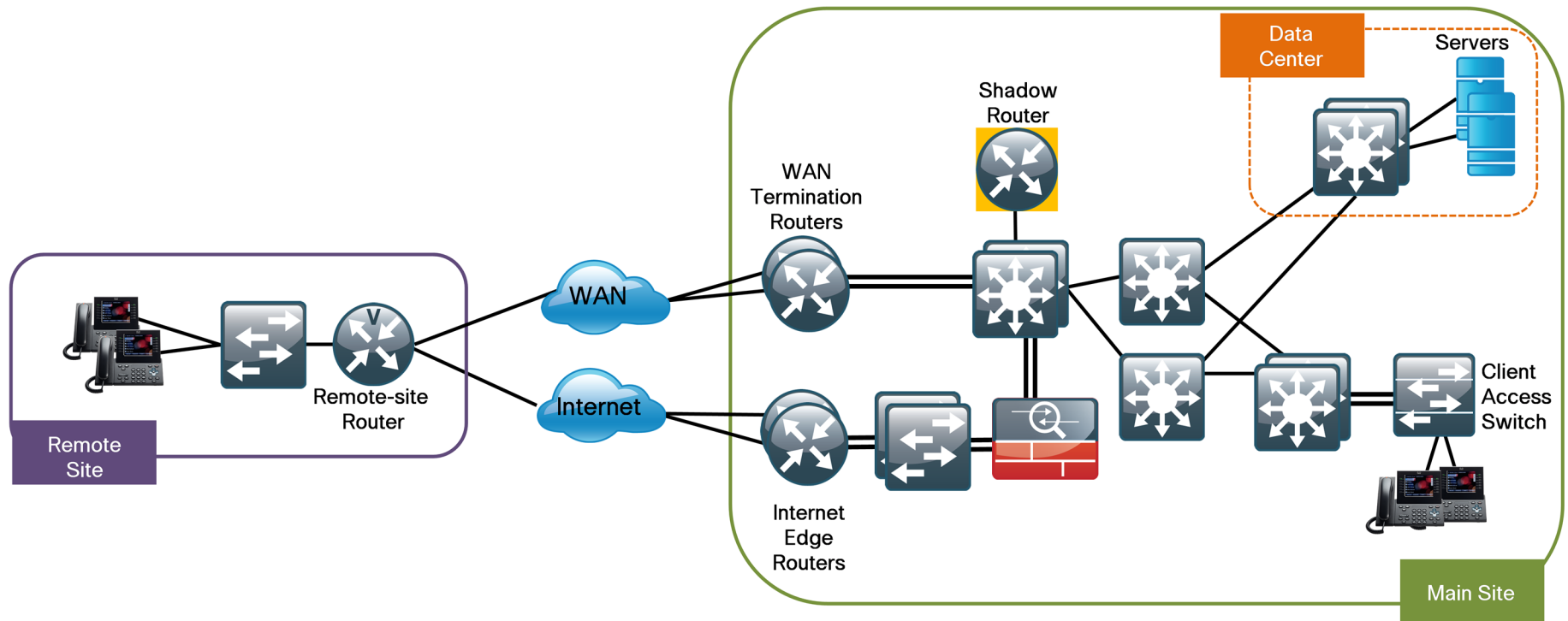
Cisco IP SLA provides a proactive notification feature with an SNMP trap. Each measurement operation can monitor performance against a preset threshold. Cisco IP SLA generates an SNMP trap to alert management applications when this threshold is crossed. An alert occurs if jitter exceeds a specified value 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**.

Group Administration and Configuration

Group Selector

- DFM@LMS
- LMS@LMS
- System Defined Groups
- User Defined Groups

Group Info

Group Name: LMS@LMS/User Defined Groups

Type:

Description: User defined groups

Created By: System: Fri 16-Sep-2011 07:28:53 PDT

Last Modified By: System: Fri 16-Sep-2011 07:28:53 PDT

Select an item then take an action -->

Export Import Create Edit Details Refresh Delete

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

The Properties dialog box shows the 'Properties: Edit' section. The 'Group Name' field contains 'Remote Site Routers for IP SLA'. The 'Parent Group' dropdown is set to '/LMS@LMS/User Defined Groups'. The 'Description' field contains 'Creating a group of Remote Site routers for IP SLA operations'. The 'Membership Update' section has 'Automatic' selected. The 'Visibility Scope' section has 'Public' selected. At the bottom, there are 'Back', 'Next', and 'Finish' buttons, and a status bar indicating '- Step 1 of 4 -'.

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.

The Rules dialog box shows the 'Rules: Edit' section. The 'Group Name' field contains 'Remote Site Routers for IP SLA'. The 'Rule Expression' section shows 'Object Type: Variable', 'Operator: equals', and 'Value:'. Below this, there are dropdowns for 'OR', 'Device', and 'Asset.CLE_Identifier', followed by an 'Add Rule Expression' button. The 'Rule Text' section is a large text area. At the bottom, there are 'Check Syntax' and 'View Parent Rules' buttons, and a status bar indicating '- Step 2 of 4 -'.

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**.

The Membership dialog box shows the 'Membership: Edit' section. The 'Group Name' field contains 'Remote Site Routers for IP SLA'. The 'Objects From Parent Group' list on the left contains a long list of devices, with '6500VSS.cisco.local' selected. The 'Objects Matching Criteria' list on the right contains a list of criteria. Between the lists are 'Add' and 'Remove' buttons. At the bottom, there are 'Back', 'Next', 'Finish', and 'Cancel' buttons, and a status bar indicating '- Step 3 of 4 -'.

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

The Summary dialog box shows the 'Summary: Edit' section. The 'Group Name' field contains 'Remote Site Routers for IP SLA'. The 'Parent Group' dropdown is set to '/LMS@LMS/User Defined Groups'. The 'Description' field contains 'Creating a group of Remote Site routers for IP SLA operations'. The 'Membership Update' section has 'Automatic' selected. The 'Rules' section contains a list of rules, including 'INCLUDELIST {', '# RS202-2911.cisco.local', 'Device\$8>', '# RS203-2921-2.cisco.local', 'Device\$9>', '# RS211-2921-1.cisco.local', 'Device\$12>', '# RS206-3925-2.cisco.local', 'Device\$10>', '# RS211-2911-2.cisco.local', 'Device\$34>', '# RS200-3945-1.cisco.local', 'Device\$33>', '# RS203-2921-1.cisco.local', 'Device\$5>', '# RS209-2911-2.cisco.local', 'Device\$32>', and '# RS207-2921.cisco.local', 'Device\$4>'. At the bottom, there are 'Back', 'Next', 'Finish', and 'Cancel' buttons, and a status bar indicating '- Step 4 of 4 -'.

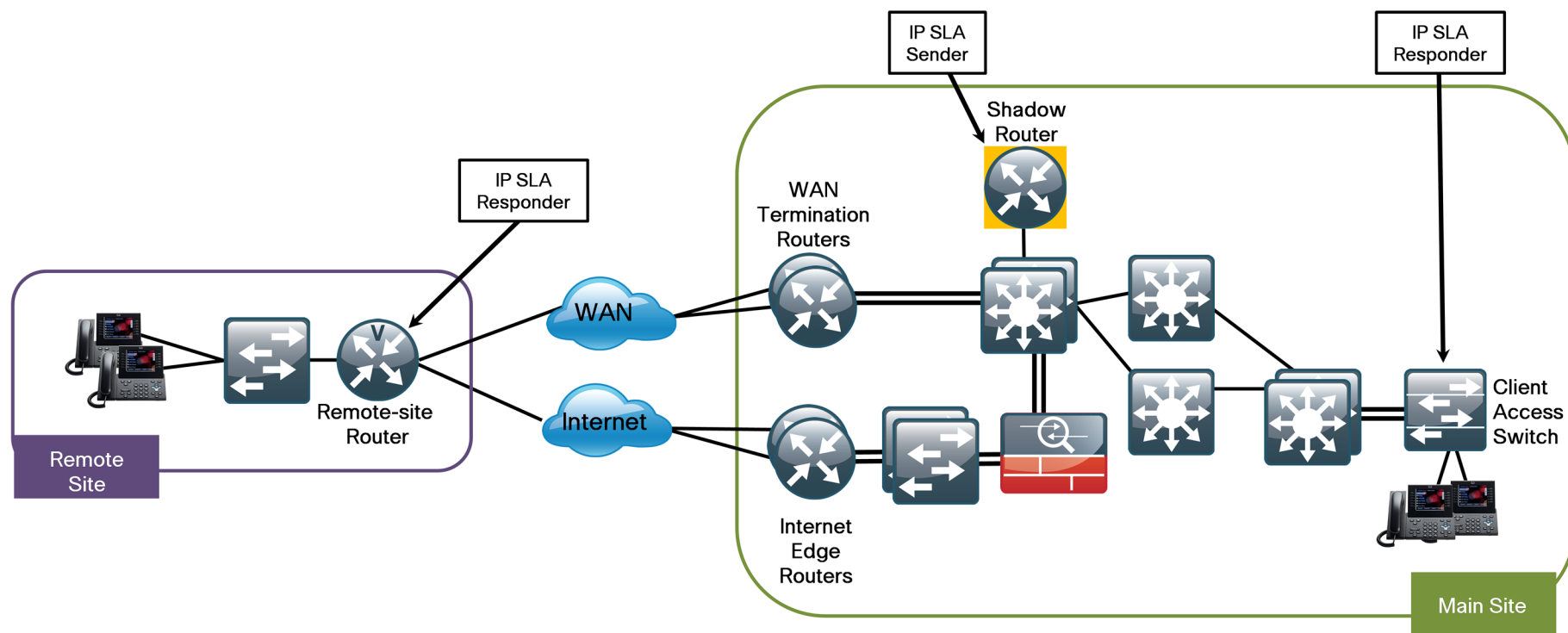
Procedure 2

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**.

List Of Operations

Filter : Showing 22 records

<input type="checkbox"/>	Operation Name	Operation Type	Create Type	Collector Count	Description
<input type="checkbox"/>	DefaultViv	UDP Jitter	SYSTEM_DEFINED	0	ot edit or delete it.
<input type="checkbox"/>	DefaultVideo	UDP Jitter	SYSTEM_DEFINED	0	A default Video operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultUDPEcho	UDPEcho	SYSTEM_DEFINED	0	A default UDP Echo operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultTelnet	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with Telnet Port 23. You cannot edit or delete it.
<input type="checkbox"/>	DefaultSMTP	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with SMTP Port 25. You cannot edit or delete it.
<input type="checkbox"/>	DefaultPOP3	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with POP Port 110. You cannot edit or delete it.
<input type="checkbox"/>	DefaultNNTP	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with NNTP Port 119. You cannot edit or delete it.
<input type="checkbox"/>	DefaultIpPathEcho	PathEcho	SYSTEM_DEFINED	0	A default IP Path Echo operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultIpEchoPri7	Echo	SYSTEM_DEFINED	0	A default IPEcho operation with Packet Priority 7. You cannot edit or delete it.
<input type="checkbox"/>	DefaultIpEchoPri3	Echo	SYSTEM_DEFINED	0	A default IP Echo operation with Packet Priority 3. You cannot edit or delete it.
<input type="checkbox"/>	DefaultIpEcho	Echo	SYSTEM_DEFINED	0	A default IP Echo operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultICMPJitter	ICMPJitter	SYSTEM_DEFINED	0	A default ICMP jitter operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultGatekeeperDelay	GatekeeperRegistrationDelay	SYSTEM_DEFINED	0	A default GatekeeperDelay operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultDNS	DNS	SYSTEM_DEFINED	0	A default DNS operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultDLSw	DLSW	SYSTEM_DEFINED	0	A default DLSw operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultDHCP	DHCP	SYSTEM_DEFINED	0	A default DHCP operation. You cannot edit or delete it.
<input type="checkbox"/>	Default60ByteVoice	UDP Jitter	SYSTEM_DEFINED	0	A default 60-byte Voice operation. You cannot edit or delete it.
<input checked="" type="checkbox"/>	Default160ByteVoice	UDP Jitter	SYSTEM_DEFINED	0	A default 160-byte Voice operation. You cannot edit or delete it.

←---Select an item then take an action--->

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

Details

Name: Default160ByteVoice
Description: A default 160-byte Voice operation. You cannot edit or delete it.
Operation Type: UDP Jitter

Miscellaneous Settings

Timeout Value(msecs): 5000
Threshold(msecs): 300
Sample Interval(secs): 60
Verify Data: false

Codec/ICPIF Settings

Target Port: 16400
Codec Type: None
Advantage Factor: 0

Packet Settings

IP QoS Type: IP Precedence
IP QoS Settings: 5
Request Payload(Bytes): 160
Packet Interval(msecs): 20
Number of Packets: 10

Precision Settings

Precision Level: Milliseconds

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**.

Specific Settings

Codec/ICPIF Settings

Target Port*: 16400

Codec Type : g711ulaw ▼

Advantage Factor : 0 ▼

Precision Settings

Precision Level : Milliseconds ▼

Packet Settings

IP QoS Type: DSCP ▼

IP QoS Settings: 46 ▼

Request Payload(bytes)*: 172

Packet Interval(msecs)*: 20

Number of Packets*: 1000

Note: * - Required Field

- Step 2 of 3 -

Back Next Finish Cancel

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**.

List of Operations

Filter: All Filter

Showing 22 records

<input type="checkbox"/>	Operation Name	Operation Type	Create Type	Collector Count	Description
<input type="checkbox"/>	DefaultJitter	UDP Jitter	SYSTEM_DEFINED	0	not edit or delete it.
<input checked="" type="checkbox"/>	DefaultVideo	UDP Jitter	SYSTEM_DEFINED	0	A default Video operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultUDPEcho	UDPEcho	SYSTEM_DEFINED	0	A default UDP Echo operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultTelnet	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with Telnet Port 23. You cannot edit or delete it.
<input type="checkbox"/>	DefaultSMTP	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with SMTP Port 25. You cannot edit or delete it.
<input type="checkbox"/>	DefaultPOP3	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with POP Port 110. You cannot edit or delete it.
<input type="checkbox"/>	DefaultNNTP	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with NNTP Port 119. You cannot edit or delete it.
<input type="checkbox"/>	DefaultPathEcho	PathEcho	SYSTEM_DEFINED	0	A default IP Path Echo operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultIPEchoPri7	Echo	SYSTEM_DEFINED	0	A default IP Echo operation with Packet Priority 7. You cannot edit or delete it.
<input type="checkbox"/>	DefaultIPEchoPri3	Echo	SYSTEM_DEFINED	0	A default IP Echo operation with Packet Priority 3. You cannot edit or delete it.
<input type="checkbox"/>	DefaultIPEcho	Echo	SYSTEM_DEFINED	0	A default IP Echo operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultICMPJitter	ICMPJitter	SYSTEM_DEFINED	0	A default ICMP jitter operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultGateKeeperDelay	GatekeeperRegistrationDelay	SYSTEM_DEFINED	0	A default GatekeeperRegistrationDelay operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultDNS	DNS	SYSTEM_DEFINED	0	A default DNS operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultDLSw	DLSw	SYSTEM_DEFINED	0	A default DLSw operation. You cannot edit or delete it.
<input type="checkbox"/>	DefaultDHCP	DHCP	SYSTEM_DEFINED	0	A default DHCP operation. You cannot edit or delete it.
<input type="checkbox"/>	Default60ByteVoice	UDP Jitter	SYSTEM_DEFINED	0	A default 60-byte Voice operation. You cannot edit or delete it.
<input type="checkbox"/>	Default160ByteVoice	UDP Jitter	SYSTEM_DEFINED	0	A default 160-byte Voice operation. You cannot edit or delete it.

← Select an item then take an action →

Edit View Delete Create

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

Details

Name: DefaultVideo
Description: A default Video operation. You cannot edit or delete it.
Operation Type: UDP Jitter

Miscellaneous Settings

Timeout Value(msecs): 5000
Threshold(msecs): 5000
Sample Interval(secs): 60
Verify Data: false

Codec/ICPIF Settings

Target Port: 50505
Codec Type: None
Advantage Factor: 0

Packet Settings

IP QoS Type: IP Precedence
IP QoS Settings: 0
Request Payload(Bytes): 1024
Packet Interval(msecs): 20
Number of Packets: 50

Precision Settings

Precision Level: Milliseconds

OK

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**.

The screenshot shows the 'General Settings' window. The 'Name' field is filled with 'SBA-UDP-Jitter-Video-DSCP-46' and the 'Description' is 'Test stream for UDP Video emulation'. The 'Type' is set to 'UDP Jitter'. Under 'Reaction Settings', 'Reaction Type' is 'connectionLoss', 'Generate Action Event' is 'Never', and 'Action Event Type' is 'None'. The 'Timeout Settings' section shows 'Timeout Value(msecs)*' as 5000. The 'Miscellaneous Settings' section shows 'Threshold(msecs)*' as 5000 and 'Sample Interval(secs)*' as 60. The 'VerifyData' checkbox is checked. At the bottom, it says '- Step 1 of 3 -' and has 'Back', 'Next', 'Finish', and 'Cancel' buttons.

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.

The screenshot shows the 'Specific Settings' window. Under 'Codec/ICPIF Settings', 'Target Port*' is 50505, 'Codec Type' is 'None', and 'Advantage Factor' is 0. Under 'Precision Settings', 'Precision Level' is 'Milliseconds'. Under 'Packet Settings', 'IP QoS Type' is 'DSCP', 'IP QoS Settings' is 46, 'Request Payload(bytes)*' is 1024, 'Packet Interval(msecs)*' is 20, and 'Number of Packets*' is 50. At the bottom, it says '- Step 2 of 3 -' and has 'Back', 'Next', 'Finish', and 'Cancel' buttons.

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**.

List Of Operations

Filter: All Filter Showing 22 records

	Operation Name	Operation Type	Create Type	Collector Count	Description
5.	DefaultVRRP	UDP Jitter	SYSTEM_DEFINED	0	not edit or delete it.
6.	DefaultVideo	UDP Jitter	SYSTEM_DEFINED	0	A default Video operation. You cannot edit or delete it.
7.	DefaultUDPEcho	UDPEcho	SYSTEM_DEFINED	0	A default UDP Echo operation. You cannot edit or delete it.
8.	<input checked="" type="checkbox"/> DefaultTelnet	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with Telnet Port 23. You cannot edit or delete it.
9.	DefaultSMTP	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with SMTP Port 25. You cannot edit or delete it.
10.	DefaultPOP3	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with POP Port 110. You cannot edit or delete it.
11.	DefaultNNTP	TCPConnect	SYSTEM_DEFINED	0	A default TCPConnect operation with NNTP Port 119. You cannot edit or delete it.
12.	DefaultPathEcho	PathEcho	SYSTEM_DEFINED	0	A default IP Path Echo operation. You cannot edit or delete it.
13.	DefaultIpEchoPri7	Echo	SYSTEM_DEFINED	0	A default IP Echo operation with Packet Priority 7. You cannot edit or delete it.
14.	DefaultIpEchoPri3	Echo	SYSTEM_DEFINED	0	A default IP Echo operation with Packet Priority 3. You cannot edit or delete it.
15.	DefaultIpEcho	Echo	SYSTEM_DEFINED	0	A default IP Echo operation. You cannot edit or delete it.
16.	DefaultICMPJitter	ICMPJitter	SYSTEM_DEFINED	0	A default ICMP jitter operation. You cannot edit or delete it.
17.	DefaultGateKeeperDelay	GatekeeperRegistrationDelay	SYSTEM_DEFINED	0	A default GatekeeperDelay operation. You cannot edit or delete it.
18.	DefaultDNS	DNS	SYSTEM_DEFINED	0	A default DNS operation. You cannot edit or delete it.
19.	DefaultDLSw	DLSw	SYSTEM_DEFINED	0	A default DLSw operation. You cannot edit or delete it.
20.	DefaultDHCP	DHCP	SYSTEM_DEFINED	0	A default DHCP operation. You cannot edit or delete it.
21.	Default60ByteVoice	UDP Jitter	SYSTEM_DEFINED	0	A default 60-byte Voice operation. You cannot edit or delete it.
22.	Default160ByteVoice	UDP Jitter	SYSTEM_DEFINED	0	A default 160-byte Voice operation. You cannot edit or delete it.

← Select an item then take an action → Edit View Delete Create

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

Details

Name: DefaultTelnet
Description: A default TCPConnect operation with Telnet Port 23. You cannot edit or delete it.
Operation Type: TCPConnect

Miscellaneous Settings

Timeout Value(msecs): 60000
Threshold(msecs): 5000
Sample Interval(secs): 60

Packet Settings

IP QoS Type: IP Precedence
IP QoS Settings: 0

Other Settings

Target Port: 23
Control Enable: false

OK

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**.

The screenshot shows the 'General Settings' window. The 'Details' section has 'Name' set to 'SBA-TCP-Connect-to-DC' and 'Description' set to 'TCP connect to Data Center Server'. The 'Type' is set to 'TCPConnect'. The 'Reaction Settings' section shows 'Reaction Type' as 'connectionLoss', 'Generate Action Event' as 'Never', and 'Action Event Type' as 'None'. There are input fields for 'Rising Threshold' and 'Falling Threshold', both set to '0'. A 'Label' section has 'X' and 'Y' fields set to '0' and 'Add'/'Remove' buttons. The 'Timeout Settings' section has 'Timeout Value(msecs)' set to '5000'. The 'Miscellaneous Settings' section has 'Threshold(msecs)' set to '5000' and 'Sample Interval(secs)' set to '60'. A 'VerifyData' checkbox is present. At the bottom, there is a 'Note: * - Required Field' and a progress indicator '- Step 1 of 3 -' with 'Back', 'Next', 'Finish', and 'Cancel' buttons.

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**.

The screenshot shows the 'Specific Settings' window. The 'Packet Settings' section has 'IP QoS Type' set to 'IP Precedence' and 'IP QoS Settings' set to '0'. The 'Other Settings' section has 'Target Port*' set to '443' and 'Control Enable' set to 'false'. A 'Note: * - Required Field' is present. At the bottom, there is a progress indicator '- Step 2 of 3 -' and 'Back', 'Next', 'Finish', and 'Cancel' buttons.

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

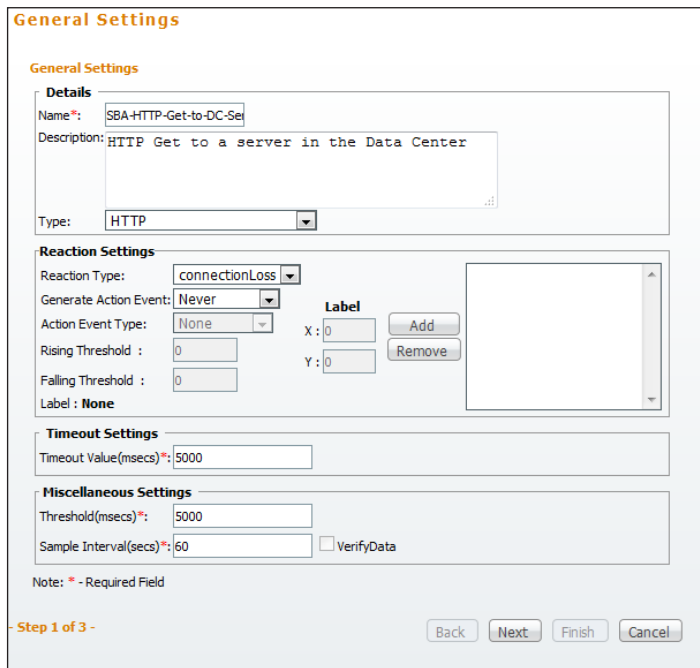
Create an HTTP Get operation

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**.



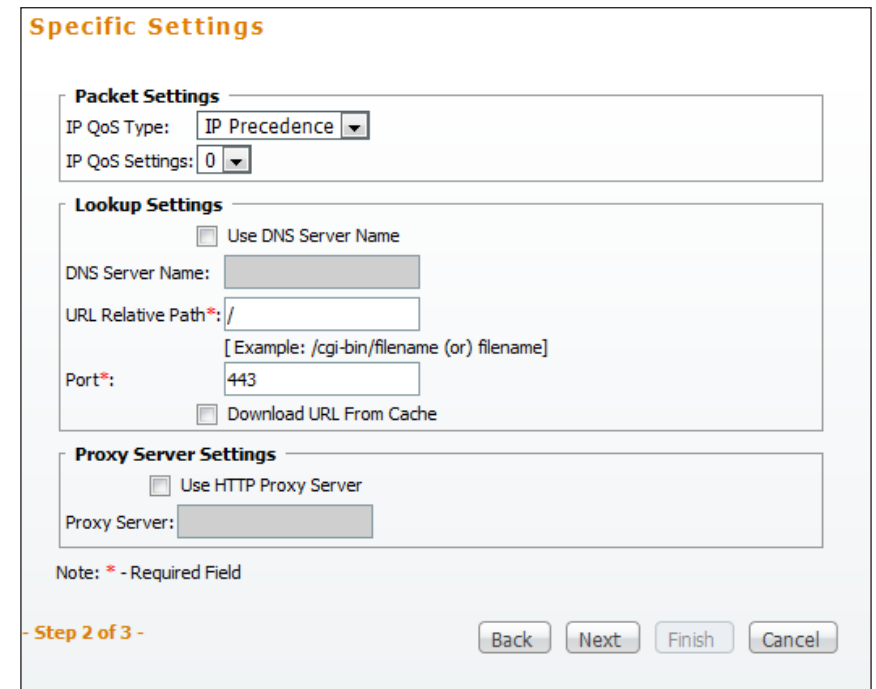
The **General Settings** dialog box is shown. It has a title bar and a close button. The content is organized into sections: **General Settings** (containing **Details** with Name and Description fields, and **Type** dropdown set to HTTP), **Reaction Settings** (containing Reaction Type dropdown set to connectionLoss, Generate Action Event dropdown set to Never, Action Event Type dropdown set to None, Rising and Falling Threshold input fields set to 0, and a Label section with X and Y input fields set to 0 and Add/Remove buttons), **Timeout Settings** (containing Timeout Value(msecs)* input field set to 5000), and **Miscellaneous Settings** (containing Threshold(msecs)* input field set to 5000, Sample Interval(secs)* input field set to 60, and a VerifyData checkbox). A note at the bottom states '* - Required Field'. Navigation buttons at the bottom are Back, Next, Finish, and Cancel. The status bar at the bottom left indicates '- Step 1 of 3 -'.

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**.



The **Specific Settings** dialog box is shown. It has a title bar and a close button. The content is organized into sections: **Packet Settings** (containing IP QoS Type dropdown set to IP Precedence and IP QoS Settings dropdown set to 0), **Lookup Settings** (containing Use DNS Server Name checkbox, DNS Server Name input field, URL Relative Path* input field set to /, a note '[Example: /cgi-bin/filename (or) filename]', Port* input field set to 443, and Download URL From Cache checkbox), and **Proxy Server Settings** (containing Use HTTP Proxy Server checkbox and Proxy Server input field). A note at the bottom states '* - Required Field'. Navigation buttons at the bottom are Back, Next, Finish, and Cancel. The status bar at the bottom left indicates '- Step 2 of 3 -'.

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
```

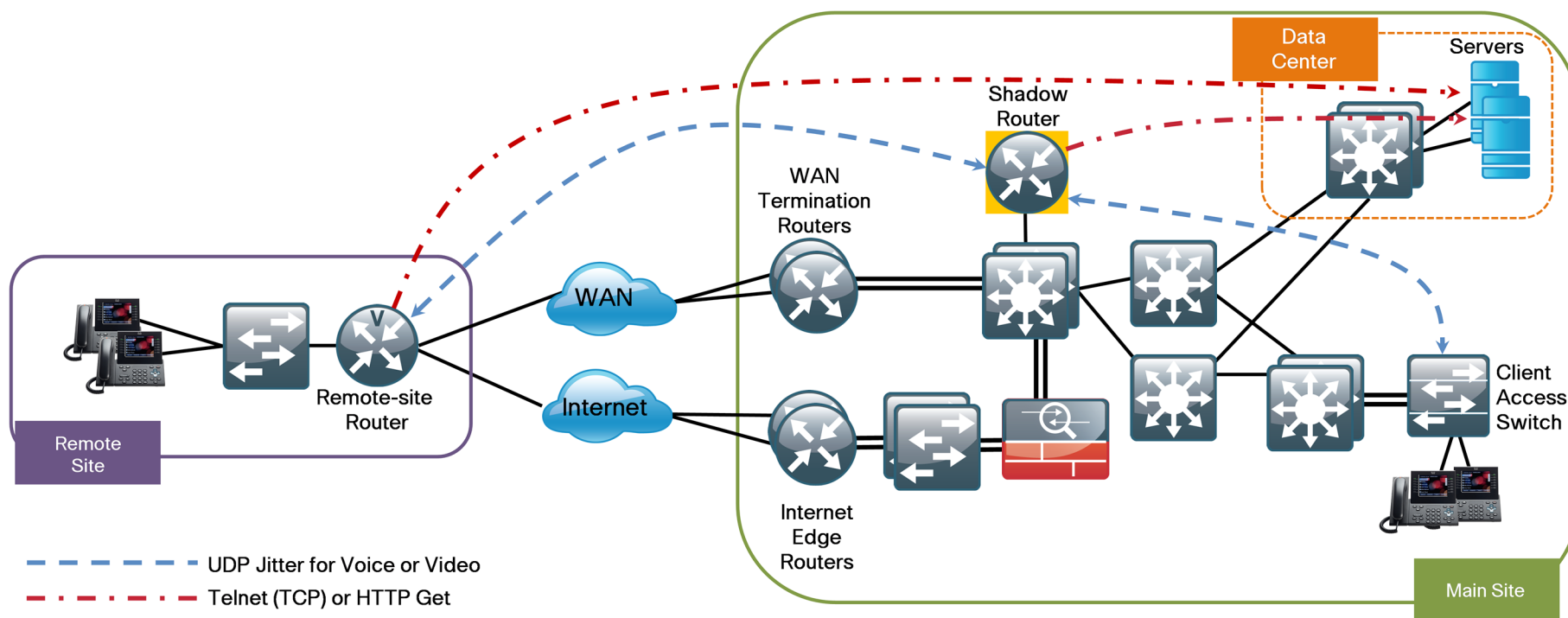
Process

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.

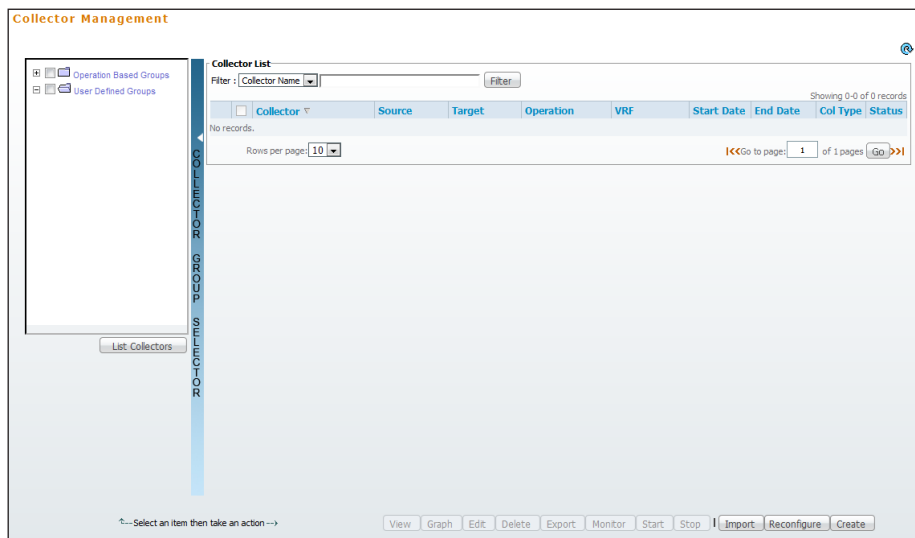
Figure 7 - IP SLA packet test streams



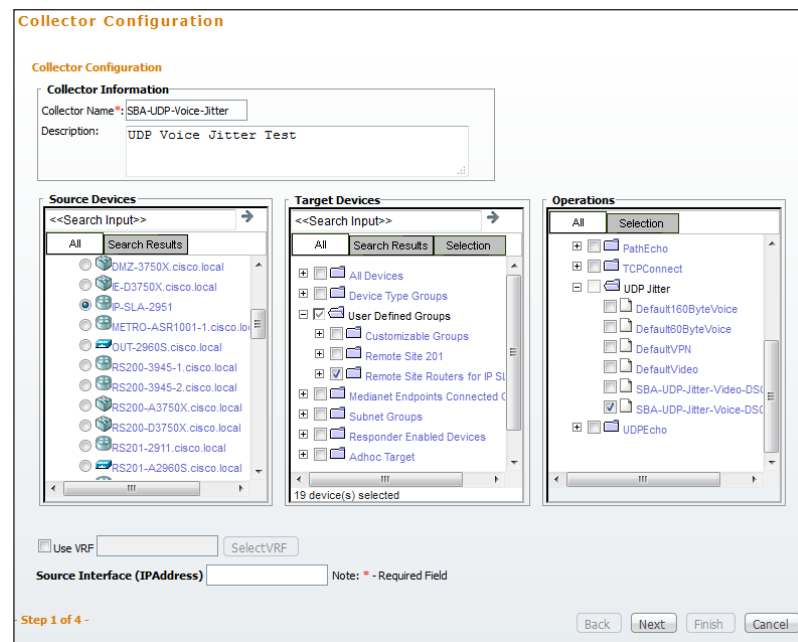
Procedure 1 Create collectors for UDP jitter

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.

Select Collector

Source Details

Source Address : IP-SLA-2951
IOS Version : 15.1(4)M2

Max Collectors : 339243
New Collectors Capacity: 338763

Filter: All [Filter]

Showing 19 records

Collector	Target	Operation
1. SBA-UDP-Voice-Jitter_RS200-3945-2.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS200-3945-2.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
2. SBA-UDP-Voice-Jitter_RS205-1941.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS205-1941.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
3. SBA-UDP-Voice-Jitter_RS206-3925-1.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS206-3925-1.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
4. SBA-UDP-Voice-Jitter_RS213-2911.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS213-2911.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
5. SBA-UDP-Voice-Jitter_RS202-2911.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS202-2911.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
6. SBA-UDP-Voice-Jitter_RS211-2911-2.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS211-2911-2.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
7. SBA-UDP-Voice-Jitter_RS212-2911.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS212-2911.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
8. SBA-UDP-Voice-Jitter_RS206-3925-2.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS206-3925-2.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
9. SBA-UDP-Voice-Jitter_RS209-2911-1.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS209-2911-1.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
10. SBA-UDP-Voice-Jitter_RS209-2911-2.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS209-2911-2.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
11. SBA-UDP-Voice-Jitter_RS203-2921-2.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS203-2921-2.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
12. SBA-UDP-Voice-Jitter_RS201-2911.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS201-2911.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
13. SBA-UDP-Voice-Jitter_RS211-2921-1.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS211-2921-1.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
14. SBA-UDP-Voice-Jitter_RS208-2911.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS208-2911.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
15. SBA-UDP-Voice-Jitter_RS204-1941.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS204-1941.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
16. SBA-UDP-Voice-Jitter_RS203-2921-1.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS203-2921-1.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
17. SBA-UDP-Voice-Jitter_RS210-2921.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS210-2921.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46
18. SBA-UDP-Voice-Jitter_RS207-2921.cisco.local_SBA-UDP-Jitter-Voice-DSCP-46	RS207-2921.cisco.local	SBA-UDP-Jitter-Voice-DSCP-46

Step 2 of 4 - [Back] [Next] [Finish] [Cancel]

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.

Schedule

Scheduling Details

Collector Type

☒ Historical/Statistical ☐ Monitored/Real-time

Start Time Details

☒ Immediate ☐ Date: 27 Oct 2011 [Calendar]

End Time Details

☒ Forever ☐ Duration: [] day(s) ☐ Date: 27 Oct 2011 [Calendar]

Server Date&Time : 27 Oct 2011, 17:51:12 PDT (while loading this page).

Poller Settings

Polling Interval : 1 min(s)

Days of Week : ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Time: From 00:00:00 To 23:59:59

Step 3 of 4 - [Back] [Next] [Finish] [Cancel]

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.

Summary

Collector Summary

Collector Name: SBA-UDP-Voice-Jitter

Summary:

Description: UDP Voice Jitter Test

Collector Type: Historical

Configuration Details:

Source Address : IP-SLA-2951

Target Address(es) : RS200-3945-2.cisco.local, RS211-2911-2.cisco.local, RS204-1941.cisco.local, RS203-2921-1.cisco.local, RS202-2911.cisco.local, RS209-2911-1.cisco.local, RS211-2921-1.cisco.local, RS209-2911-2.cisco.local, RS210-2921.cisco.local, RS212-2911.cisco.local, RS203-2921-2.cisco.local, RS208-2911.cisco.local, RS206-3925-2.cisco.local, RS205-1941.cisco.local, RS200-3945-1.cisco.local, RS201-2911.cisco.local, RS207-2921.cisco.local, RS206-3925-1.cisco.local, RS213-2911.cisco.local

- Step 4 of 4 -

Back Next Finish Cancel

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

Collector Management

Filter (All) Filter

Collector List

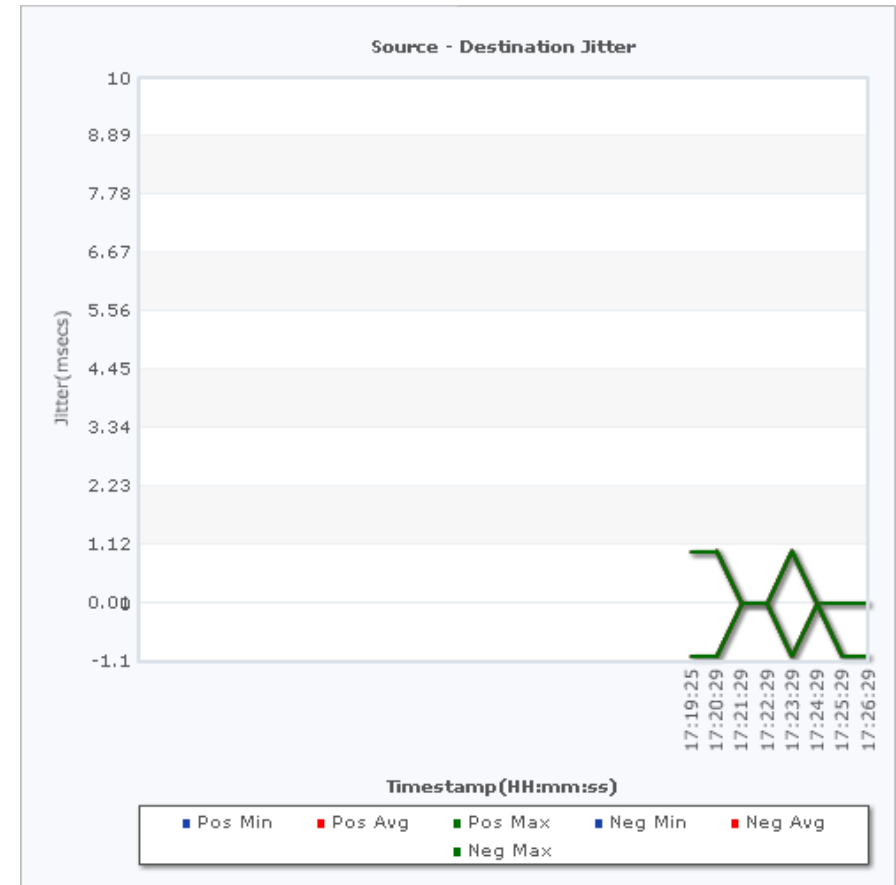
Collector #	Source	Target	Operation	VNF	Start Date	End Date	Col Type	Status
1	TCP Connect from Remote to 10.4.48.35, SBA-TCP-Conn	RS201-2911.cisco.local	SBA-TCP-Connect-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running
2	TCP Connect from Remote to 10.4.48.35, SBA-HTTP-Get	RS201-2911.cisco.local	SBA-HTTP-Get-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running
3	SBA-UDP-Voice-Jitter, RS211-2911-2.cisco.local	IP-SLA-2951	SBA-UDP-Voice-Jitter-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running
4	SBA-UDP-Voice-Jitter, RS211-2911-2.cisco.local	IP-SLA-2951	SBA-UDP-Voice-Jitter-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running
5	SBA-UDP-Voice-Jitter, RS211-2911-2.cisco.local	IP-SLA-2951	SBA-UDP-Voice-Jitter-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running
6	SBA-UDP-Voice-Jitter, RS211-2911-2.cisco.local	IP-SLA-2951	SBA-UDP-Voice-Jitter-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running
7	SBA-UDP-Voice-Jitter, RS211-2911-2.cisco.local	IP-SLA-2951	SBA-UDP-Voice-Jitter-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running
8	SBA-UDP-Voice-Jitter, RS211-2911-2.cisco.local	IP-SLA-2951	SBA-UDP-Voice-Jitter-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running
9	SBA-UDP-Voice-Jitter, RS211-2911-2.cisco.local	IP-SLA-2951	SBA-UDP-Voice-Jitter-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running
10	SBA-UDP-Voice-Jitter, RS211-2911-2.cisco.local	IP-SLA-2951	SBA-UDP-Voice-Jitter-to-CC-Server	Not Applicable	Oct 21, 2011	Forever	Historical	Running

Rows per page (10) 1 of 5 pages (Go)

Select an item then take an action

View Graph Edit Delete Export Monitor Stop Import Reconfigure Create

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

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.

The **Collector Configuration** window is divided into three main sections: **Collector Information**, **Source Devices**, and **Target Devices**.

- Collector Information:** Contains fields for **Collector Name** (SBA-TCP-Connect-to-DC) and **Description** (TCP Connect from Remote Site).
- Source Devices:** A tree view showing various device groups. The **Remote Site 201** group is expanded, showing **RS201-2911.cisco.local** and **RS201-A2960S.cisco.local**.
- Target Devices:** A tree view showing various device groups. The **Adhoc Target** group is expanded, showing **10.4.48.35**.
- Operations:** A tree view showing various operations. The **TCPConnect** group is expanded, showing **SBA-TCP-Connect-to-DC-Server**.

At the bottom, there are buttons for **Back**, **Next**, **Finish**, and **Cancel**. A status bar at the bottom left indicates **- Step 1 of 4 -**.

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.

The **Select Collector** window displays **Source Details** at the top:

- Source Address:** RS201-2911.cisco.local
- IOS Version:** 15.1(4)M2
- Max Collectors:** 426514
- New Collectors Capacity:** 382116

Below this is a **Filter** dropdown set to **All** and a **Filter** button. A table shows the selected collector:

Collector	Target	Operation
1. SBA-TCP-Connect-to-DC-Server_10.4.48.35_SBA-TCP-Connect-to-DC-Server	10.4.48.35	SBA-TCP-Connect-to-DC-Server

At the bottom, there are buttons for **Back**, **Next**, **Finish**, and **Cancel**. A status bar at the bottom left indicates **- Step 2 of 4 -**.

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.

The **Schedule** window displays **Scheduling Details** at the top:

- Collector Type:** **Historical/Statistical** (selected), **Monitored/Real-time** (unselected).
- Start Time Details:** **Immediate** (selected), **Date:** 27 Oct 2011.
- End Time Details:** **Forever** (selected), **Duration:** day(s), **Date:** 27 Oct 2011.
- Server Date&Time:** 27 Oct 2011, 18:17:38 PDT (while loading this page).
- Poller Settings:** **Polling Interval:** 1 min(s), **Days of Week:** Sun, Mon, Tue, Wed, Thu, Fri, Sat (all checked), **Time:** From 00:00:00 To 23:59:59.

At the bottom, there are buttons for **Back**, **Next**, **Finish**, and **Cancel**. A status bar at the bottom left indicates **- Step 3 of 4 -**.

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.

Collector Summary

Collector Name: SBA-TCP-Connect-to-DC-Server

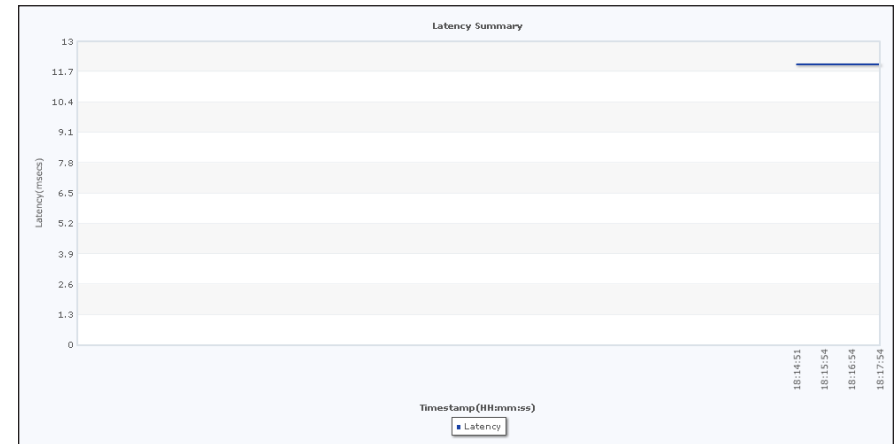
Summary:

Description: TCP Connect from Remote Site	
Collector Type: Historical	
Configuration Details:	
Source Address	: RS201-2911.cisco.local
Target Address(es)	: 10.4.48.35
Operation Name(s)	: SBA-TCP-Connect-to-DC-Server
VRF name	: Not Applicable
Schedule Details:	
Start Date	: 27 Oct 2011
End Date	: Forever
Poller Settings:	
Polling Interval (mins)	: 1
Polling Time	: From 00:00:00 To 23:59:59
Days of Week Details	: Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday.

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

[illegible]

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:

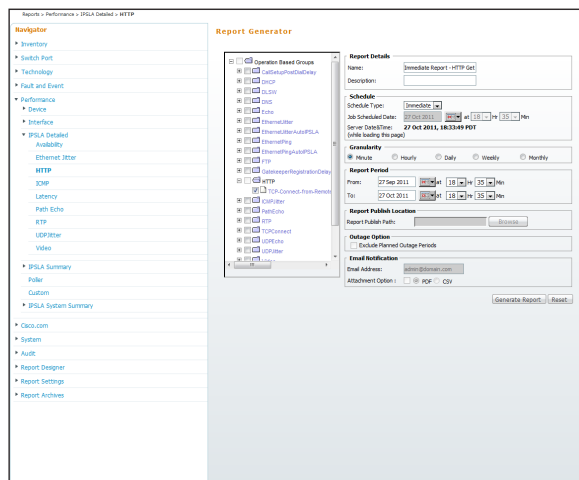
- **HTTP**—Reports DNS lookup times, TCP Connect times, page load times, and completion summary statistics for HTTP test operations.
- **UDP Jitter**—Reports two-way jitter and latency times, round-trip latency, and MOS and CPIF scores if they are enabled.
- **Latency**—Reports latency, errors, and completion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

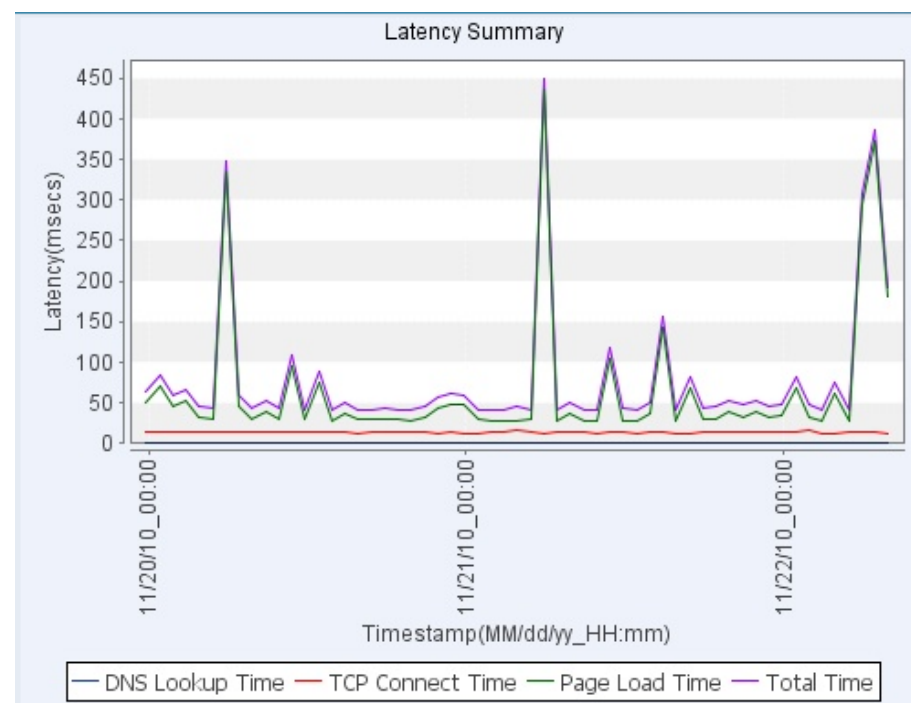
Step 6: To generate a report that covers a period of multiple days, select **Hourly**. Selecting **Minute** will only allow you to generate a report of one day or less.

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.

Summary					
Collector: TCP-Connect-from-RemoteSite_10.4.48.35_SBA-HTTP-Get-to-DC-Server					
TCP-Connect-from-RemoteSite_10.4.48.35_SBA-HTTP-Get-to-DC-Server					
Start Time	RTT(ms)	DNS RTT(ms)	TCP Connect RTT(ms)	Transaction RTT(ms)	Message Body Octets
10/27/11_00:00:03	6	0	3	3	0
10/27/11_00:01:03	6	0	3	3	0
10/27/11_00:02:03	6	0	3	3	0
10/27/11_00:03:03	6	0	3	3	0
10/27/11_00:04:03	7	0	4	3	0
10/27/11_00:05:03	6	0	3	3	0
10/27/11_00:06:03	6	0	3	3	0
10/27/11_00:07:03	6	0	3	3	0
10/27/11_00:08:03	6	0	3	3	0
10/27/11_00:09:03	7	0	3	4	0
10/27/11_00:10:03	6	0	3	3	0
10/27/11_00:11:03	6	0	3	3	0
10/27/11_00:12:03	7	0	3	4	0
10/27/11_00:13:03	6	0	3	3	0
10/27/11_00:14:03	6	0	3	3	0

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.

Job ID	Run Status	Sched Type	Description	Run Sched	Status	Owner	Scheduled At	Completed At	View Report
1. 1179.1	Scheduled	Periodic	Weekly Report f or Remote Sites	At 21:05:00 starting 28 Oct 2011		mldavis		N/A	

After the report runs, its status changes to **Succeeded**.

Job ID	Run Status	Sched Type	Description	Run Sched	Status	Owner	Scheduled At	Completed At	View Report
1. 1179.2	Scheduled	Periodic	Weekly Report f or Remote Sites	At 21:05:00 PDT weekly, starting 04 Nov 2011		mldavis			
2. 1179.1	Succeeded	Periodic	Weekly Report f or Remote Sites	At 21:05:00 PDT weekly, starting 28 Oct 2011		mldavis	Oct 28 2011 21:05:00	Oct 28 2011 21:05:11	View

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.

Summary

Total number of collectors: 1

Collectors with Report Data: 1

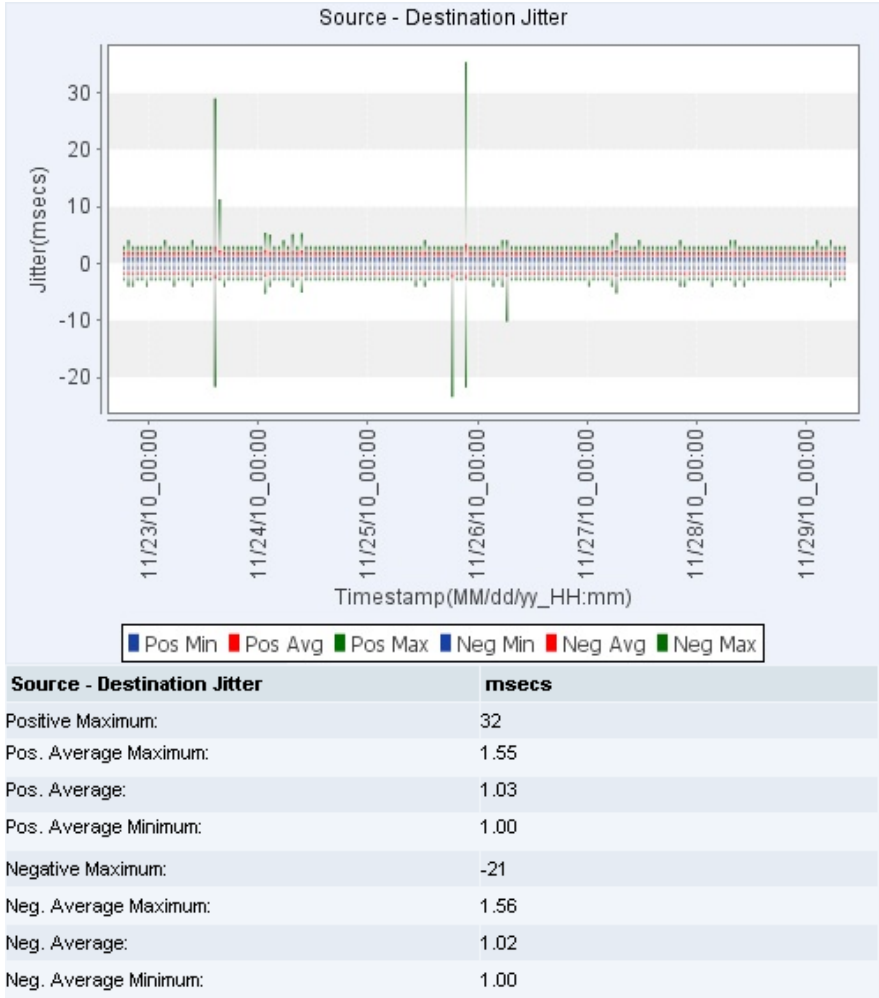
Collectors without Report Data: None

Collector: SBA-UDP-Voice-Jitter_A2960S.cisco.local_SBA-UDP-Jitter-Video-DSCP-46

SBA-UDP-Voice-Jitter_A2960S.cisco.local_SBA-UDP-Jitter-Video-DSCP-46 [Graph](#)

Start Time	Round Trip Latency			Positive Source -> Dest Jitter			Negative Source->Dest Jitter			Positive Dest -> Source Jitter			Negative Dest->Source Jitter			MOS		ICPIF		
	Min(ms)	Avg(ms)	Max(ms)	Std Dev	Min(ms)	Avg(ms)	Max(ms)	Std Dev	Min(ms)	Avg(ms)	Max(ms)	Std Dev	Min(ms)	Avg(ms)	Max(ms)	Std Dev	MinMOS	MaxMOS	MinICPIF	MaxICPIF
10/21/11_21:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/21/11_22:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/21/11_23:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_00:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_01:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_02:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_03:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_04:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_05:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_06:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_07:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_08:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_09:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A
10/22/11_10:46:0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	N/A	N/A	N/A

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.



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 Advanced Enterprise
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
WAN-aggregation Router	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	
	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
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	securityk9, datak9
	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
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	securityk9, datak9
	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
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	securityk9, datak9
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

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)