



Configuring IP SLAs Video Operations

Last Updated: November 21, 2012

This document describes how to configure the Cisco IOS IP Service Level Agreements (SLAs) Video Operation feature to analyze one-way delay, one-way packet loss, one-way jitter, and connectivity in networks that carry video traffic.

- [Finding Feature Information, page 1](#)
- [Prerequisites for IP SLAs Video Operations, page 1](#)
- [Restrictions for IP SLAs Video Operations, page 2](#)
- [Information About IP SLAs Video Operations, page 2](#)
- [How to Configure IP SLAs Video Operations, page 3](#)
- [Configuration Examples for IP SLAs Video Operations, page 14](#)
- [Additional References, page 16](#)
- [Feature Information for IP SLAs Video Operations, page 16](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IP SLAs Video Operations

- Both the source and responder devices for the IP SLAs video operation must be capable of providing platform-assisted video traffic generation and reflection.
- Time synchronization, such as that provided by Network Time Protocol (NTP), is required between the source and the responder device in order to provide accurate one-way delay (latency) measurements. To configure NTP on the source and target devices, perform the tasks in the “Performing Basic System Management” module in the Cisco IOS Network Management Configuration Guide.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for IP SLAs Video Operations

- This feature is supported only on Cisco devices that are capable of generating platform-assisted video traffic and reflection, such as the Cisco Catalyst 3560, 3560-E, 3560-X, 3750, 3750-E, and 3750-X Series switches.

**Note**

The preceding list is not all inclusive. See your product documentation for more information.

- IP SLAs video operations do not support Round Trip Time (RTT) traffic.
- Because IP SLAs video operations support only one-way traffic, an operation and a responder must be configured on both the source and responder and both devices must support SNMP access.
- IP SLAs video operations are supported in IPv4 networks only.

Information About IP SLAs Video Operations

The platform-independent IP Service Level Agreements (SLAs) is a feature embedded in Cisco software. It allows you to understand IP service levels, increase productivity, lower operational costs, and reduce the frequency of network outages. IP SLAs performs the active monitoring of the network performance and can be used for network troubleshooting, network readiness assessment, and health monitoring.

IP SLAs in Cisco software is incapable of generating the high data rates, 4 to 16 Mbps, which are typical of video applications. To eliminate the protocol overhead and the process scheduling delays that contribute to the limitations of the earlier IP SLAs software to generate video traffic, the Cisco IP SLAs Video Operation feature makes the traffic generation and transmission routines platform dependent. The Application programming interface (API) calls in the IP SLAs video operation software to enable a more precise timer interrupt than the general system timer, which is insufficient for the packet generation requirements for a true video stream. Devices that can act as a source or a responder for an IP SLAs video operation are limited to Cisco devices that are capable of providing platform-assisted video traffic generation and reflection.

An IP SLAs video operation differs from other IP SLA operations in that all traffic is one way only, with a responder required to process the sequence numbers and time stamps locally and to wait for a request from the source before sending the calculated data back.

The source sends a request to the responder when the current video operation is done. This request signals the responder that no more packets will arrive, and that the video sink function in the video operation can be turned off. When the response from the responder arrives at the source, the statistics are read from the message, and the relevant fields in the operation are updated.

Because all video operation traffic is one way, the responder is responsible for actually collecting and verifying the packets. The software that does packet count verification and time stamp jitter calculations is shared by both the source and responder. The responder stores this information until such time that the source requests the data, or a timer expires and the data is released.

Because the responder cannot directly read the video packets, the responder creates two queues and a block of reallocated memory for use by both video sink and the responder itself.

When a packet arrives at video sink, it is processed to extract the sequence numbers and time stamps, and that information is put into one of the pre-allocated memory blocks. A pointer to this block is put into the used queue for later processing by the main responder task.

At periodic timer intervals, the responder processes a number of the packet information blocks from the used queue and updates the statistics appropriately. When the data is processed, the blocks are returned to the free-memory list to be used again.

This procedure continues until the video operation is complete.

How to Configure IP SLAs Video Operations

- [Configuring an IP SLAs Responder, page 3](#)
- [Configuring an IP SLAs Video Profile, page 4](#)
- [Configuring Proactive Threshold Monitoring, page 7](#)
- [Scheduling IP SLAs Operations, page 10](#)
- [Displaying Statistics for IP SLAs, page 13](#)
- [Troubleshooting Tips, page 14](#)

Configuring an IP SLAs Responder

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla responder**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla responder Example: Device(config-term)# ip sla responder	Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source.

Command or Action	Purpose
Step 4 <code>exit</code> Example: Device(config-term)# <code>exit</code>	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an IP SLAs Video Profile

To configure a source IP address for the operation and identify the prepackaged video profile to be used for the video traffic type to be analyzed, perform the following steps.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip sla operation-number`
4. `video destination-ip-address | destination-hostname destination-port source-ip source-address | source-hostname source-port port-number profile traffic-type`
5. `duration seconds`
6. `frequency seconds`
7. `history distribution-of-statistics-kept size`
8. `history enhanced [interval seconds] [ buckets number-of-buckets]`
9. `history hours-of-statistics-kept hours`
10. `history statistics-distribution-interval milliseconds`
11. `owner owner`
12. `tag text`
13. `timeout milliseconds`
14. `threshold milliseconds`
15. `vrf vrf-name`
16. `end`
17. `show ip sla configuration [operation-number]`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Device> <code>enable</code>	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config-term)# ip sla 10	Begins configuration of an IP SLAs operation and enters IP SLA configuration mode.
Step 4	video destination-ip-address destination-hostname destination-port source-ip source-address source-hostname source-port port-number profile traffic-type Example: Device(config-ip-sla)# video 192.168.2.17 997 source-ip 192.168.2.16 source-port 555 profile telepresence	Configures a source address and a prepackaged video profile for the IP SLAs operation being configured and enters IP SLA video configuration mode.
Step 5	duration seconds Example: Device(config-ip-sla-video)# duration 20	(Optional) Sets the amount of time during which synthetic traffic is generated for the IP SLAs video operation.
Step 6	frequency seconds Example: Device(config-ip-sla-video)# frequency 60	(Optional) Sets the amount of time during which synthetic traffic is generated for the IP SLAs video operation.
Step 7	history distribution-of-statistics-kept size Example: Device(config-ip-sla-video)# history distribution-of-statistics-kept 1	(Optional) Sets the number of statistics distributions kept during the IP SLAs video operation.

	Command or Action	Purpose
Step 8	history enhanced [<i>interval seconds</i>] [<i>buckets number-of-buckets</i>] Example: <pre>Device(config-ip-sla-video)# history enhanced interval 900 buckets 100</pre>	(Optional) Enables enhanced history gathering for the IP SLAs video operation.
Step 9	history hours-of-statistics-kept <i>hours</i> Example: <pre>Device(config-ip-sla-video)# history hours-of-statistics-kept 2</pre>	(Optional) Sets the number of hours for which statistics are maintained for the IP SLAs video operation.
Step 10	history statistics-distribution-interval <i>milliseconds</i> Example: <pre>Device(config-ip-sla-video)# history statistics-distribution-interval 10</pre>	(Optional) Sets the time interval for each statistics distribution kept for the IP SLAs video operation.
Step 11	owner <i>owner</i> Example: <pre>Device(config-ip-sla-video)# 192.168.2.189 cwb.cisco.com User1 RTP 555-0100</pre>	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of the IP SLAs video operation.
Step 12	tag <i>text</i> Example: <pre>Device(config-ip-sla-video)# tag TelnetPollServer1</pre>	(Optional) Creates a user-specified identifier for the IP SLAs video operation.
Step 13	timeout <i>milliseconds</i> Example: <pre>Device(config-ip-sla-video)# timeout 5000</pre>	(Optional) Sets the amount of time the IP SLAs video operation waits for a response from its request packet.

	Command or Action	Purpose
Step 14	threshold <i>milliseconds</i> Example: <pre>Device(config-ip-sla-video)# threshold 5000</pre>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by the IP SLAs video operation.
Step 15	vrf <i>vrf-name</i> Example: <pre>Device(config-ip-sla-video)# vrf vpn-1</pre>	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) VPNs using IP SLAs operations.
Step 16	end Example: <pre>Device(config-ip-sla-video)# end</pre>	Returns to global configuration mode.
Step 17	show ip sla configuration [<i>operation-number</i>] Example: <pre>Device# show ip sla configuration 600</pre>	(Optional) Displays configuration information, including defaults, for all IP SLAs operations or a specified operation.

Configuring Proactive Threshold Monitoring

Perform this task to configure thresholds and reactive triggering for generating traps or starting another operation.

- IP SLAs operations to be started when violation conditions are met must be configured.

**Note**

- RTT reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT).
- SNMP traps for RTT for jitter operations are based on the average value for the return-trip time (RTTAvg) for the whole operation only and do not include return-trip time values for individual packets sent during the operation. Only syslog messages are supported for RTTAvg threshold violations.
- Only syslog messages are supported for RTT violations during Jitter operations.
- Only SNMP traps are supported for RTT violations during non-Jitter operations.
- Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.
- Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]
4. **ip sla reaction-trigger** *operation-number* *target-operation*
5. **ip sla logging traps**
6. Do one of the following:
 - **snmp-server enable traps rtr**
 - **snmp-server enable traps syslog**
7. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
8. **exit**
9. **show ip sla reaction configuration** [*operation-number*]
10. **show ip sla reaction trigger** [*operation-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Device> enable	• Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla reaction-configuration operation-number react monitored-element [action-type option] [threshold-type {average [number-of-measurements] consecutive [occurrences] immediate never xofy [x-value y-value]}] [threshold-value upper-threshold lower-threshold] Example: Device(config)# ip sla reaction-configuration 10 react jitterAvg threshold-type immediate threshold-value 5000 3000 action-type trapAndTrigger	Configures the action (SNMP trap or IP SLAs trigger) that is to occur based on violations of specified thresholds.
Step 4	ip sla reaction-trigger operation-number target-operation Example: Device(config)# ip sla reaction-trigger 10 2	(Optional) Starts another IP SLAs operation when the violation conditions are met. Required only if the ip sla reaction-configuration command is configured with either the trapAndTrigger or triggerOnly keyword.
Step 5	ip sla logging traps Example: Device(config)# ip sla logging traps	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.
Step 6	Do one of the following: snmp-server enable traps rtr snmp-server enable traps syslog Example: Device(config)# snmp-server enable traps rtr Example: Device(config)# snmp-server enable traps syslog	(Optional) The first example shows how to enable the system to generate CISCO-RTTMON-MIB traps. (Optional) The second example shows how to enable the system to generate CISCO-SYSLOG-MIB traps.

	Command or Action	Purpose
Step 7	snmp-server host {hostname ip-address} [vrf vrf-name] [traps informs] [version {1 2c 3 [auth noauth priv]]] community-string [udp-port port] [notification-type] Example: Device(config)# snmp-server host 10.1.1.1 public syslog	(Optional) Sends traps to a remote host. Required if the snmp-server enable traps command is configured.
Step 8	exit Example: Device(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 9	show ip sla reaction configuration [operation-number] Example: Device# show ip sla reaction configuration 10	(Optional) Displays the configuration of proactive threshold monitoring.
Step 10	show ip sla reaction trigger [operation-number] Example: Device# show ip sla reaction trigger 2	(Optional) Displays the configuration status and operational state of target operations to be triggered.

Scheduling IP SLAs Operations



Note

- All IP SLAs operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group is limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
 - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh:mm:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}] [**ageout** *seconds*] [**recurring**]
 - **ip sla group schedule** *group-operation-number* *operation-id-numbers* **schedule-period** *schedule-period-range* [**ageout** *seconds*] [**frequency** *group-operation-frequency*] [**life** {**forever** | *seconds*}] [**start-time**{*hh:mm[:ss]* [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm[:ss]*}]
4. **exit**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 Do one of the following: • ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {<i>hh:mm:ss</i> <i>month day day month</i>} pending now after <i>hh:mm:ss</i>] [ageout <i>seconds</i>] [recurring] • ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life {forever <i>seconds</i>}] [start-time {<i>hh:mm:ss</i> <i>month day day month</i>} pending now after <i>hh:mm:ss</i>}] Example: <pre>Device(config)# ip sla schedule 10 life forever start-time now</pre> Example: <pre>Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now</pre>	• Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.
Step 4 exit Example: <pre>Device(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5 show ip sla group schedule Example: <pre>Device# show ip sla group schedule</pre>	(Optional) Displays IP SLAs group schedule details.
Step 6 show ip sla configuration Example: <pre>Device# show ip sla configuration</pre>	(Optional) Displays IP SLAs configuration details.

Displaying Statistics for IP SLAs

SUMMARY STEPS

1. enable
2. show ip sla configuration [operation]
3. show ip sla statistics [operation-number] [details]
4. show ip sla statistics aggregated [operation-number] [details]
5. exit

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2 show ip sla configuration [operation] Example: Device# show ip sla configuration 10	(Optional) Displays configuration values, including all defaults, for all IP SLAs operations or the specified operation.
Step 3 show ip sla statistics [operation-number] [details] Example: Device# show ip sla statistics 10 details	(Optional) Displays display the current operational status and statistics of all IP SLAs operations or the specified operation.
Step 4 show ip sla statistics aggregated [operation-number] [details] Example: Device# show ip sla statistics aggregated 10 deatils	(Optional) Displays the aggregated statistical errors and distribution information for all IP SLAs operations or the specified operation.
Step 5 exit Example: Device# exit	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

- If the IP SLAs operation is not running and not generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

Configuration Examples for IP SLAs Video Operations

- [Example: Basic IP SLAs Video Profile for Cisco TelePresence 1080P Traffic, page 14](#)
- [Example: Basic IP SLAs Video Profile for IP Television Traffic, page 14](#)
- [Example: Basic IP SLAs Video Profile for IP Surveillance Camera Traffic, page 15](#)
- [Example: SNMP Commands for Configuring a Video Operation, page 15](#)

Example: Basic IP SLAs Video Profile for Cisco TelePresence 1080P Traffic

```

      IP SLAs Infrastructure Engine-III
Entry number: 600
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: video
Video profile name: TELEPRESENCE
Target address/Source address: 10.10.10.1/10.10.10.2
Target port/Source port: 1/1
Vrf Name:
Control Packets: enabled
Schedule:
  Operation frequency (seconds): 60 (not considered if randomly scheduled)
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:

```

Example: Basic IP SLAs Video Profile for IP Television Traffic

```

      IP SLAs Infrastructure Engine-III
Entry number: 700
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: video
Video profile name: IPTV

```

```

Target address/Source address: 10.10.10.3/10.10.10.4
Target port/Source port: 1/1
Vrf Name:
Control Packets: enabled
Schedule:
  Operation frequency (seconds): 60 (not considered if randomly scheduled)
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:

```

Example: Basic IP SLAs Video Profile for IP Surveillance Camera Traffic

```

IP SLAs Infrastructure Engine-III
Entry number: 800
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: video
Video profile name: IPVSC
Target address/Source address: 10.10.10.5/10.10.10.6
Target port/Source port: 1/1
Vrf Name:
Control Packets: enabled
Schedule:
  Operation frequency (seconds): 60 (not considered if randomly scheduled)
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:

```

Example: SNMP Commands for Configuring a Video Operation

The following SNMP commands can be used to configure an IP SLAs video operation.

```

setany -v2c x.x.x.x public rttMonCtrlAdminStatus.1 -i 5 \ >
rttMonCtrlAdminRttType.1 -i 22 \ >
rttMonEchoAdminProtocol.1 -i 37 \ >
rttMonEchoAdminTargetPort.1 -i 7810 \ >
rttMonEchoAdminSourcePort.1 -i 7011 \ >
rttMonEchoAdminSourceAddress.1 -o "65 65 65 02" \ >
rttMonEchoAdminVideoTrafficProfile.1 -o "IPTV" \ >
rttMonCtrlAdminNvgen.1 -i true \ >
rttMonEchoAdminTargetAddress.1 -o "65 65 65 01"

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP SLAs commands	Cisco IOS IP SLAs Command Reference

Standards and RFCs

Standard/RFC	Title
No new or modified standards or RFCs are supported by this feature, and support for existing standards has not been modified by features in this document.	--

MIBs

MIB	MIBs Link
- CISCO-IPSLA-VIDEO-MIB - CISCO-RTTMON-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs Video Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software

release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 **Feature Information for IP SLAs Video Operations**

Feature Name	Releases	Feature Information
IP SLAs Video Operations	12.2(58)SE	Analyzes one-way delay, one-way packet loss, one-way jitter, and connectivity in IPv4 networks that carry video traffic.
	15.2(2)T	
	15.1(1)SG	
	Cisco IOS XE Release 3.3SG	The following commands were introduced or modified: bitrate , codec (VO profile) , description (VO profile) , dscp (IP SLA video) , endpoint , frame (VO profile) , ip sla profile video , reserve dsp , resolution , rtp (VO profile) , show ip sla video , video (IP SLA) , video content .

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)

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

© 2012 Cisco Systems, Inc. All rights reserved.