CCIE Routing and Switching v4.0 Quick Reference

Brad Ellis
Jacob Uecker

Cisco Press

CCIE Routing and Switching v4.0

Quick Reference

Brad Ellis
Jacob Uecker
Steven Means

ciscopress.com

Table of Contents

Chapter 6

Network Optimization

IP Service Level Agreement (SLA)

One of the most important aspects in maintaining a network is providing a guarantee of a specific level of service to customers. To ensure that such an agreement is met at all times, IOS provides a mechanism to actively test specific metrics, called IP SLA. When configured, the IP SLA service actively monitors a specific aspect of the network, such as UDP VOIP jitter, DNS response time, ping latency, and so on. If the IP SLA thresholds are not met, IOS sends a notification, such as an SNMP trap or syslog message.

To create a basic IP SLA monitor, the type, options, and frequency must be specified. After the monitor has been created, a schedule is build that kicks off the monitor. To monitor the round-trip response time between a router and an IP, you can use the ICMP Echo Operation:

```
Router(config)# ip sla monitor <OPERATION #>
Router(config-sla-monitor)# type echo protocol ipIcmpEcho <DESTINATION>
Router(config-sla-monitor)# frequency <SECONDS>
Router(config-sla-monitor)# exit
Router(config)# ip sla monitor schedule <OPERATION #> [life {forever | seconds}] [start-time {hh:mm[:ss]
[month day | day month] | pending | now | after hh:mm:ss] [ageout seconds] [recurring]
```

Some monitors require that a responder be configured (UDP Jitter, UDP Echo, and TCP Connect) on one router:

```
Router(config)# ip sla monitor responder
```

 Please see page 245 for more details.

Following are other IP SLA monitor operations:

UDP Jitter: **`type jitter`**
VOIP Jitter: **`type`**
VOIP Gatekeeper Delay: **`type voip delay gatekeeper registration`**
UDP Echo: **`type udp echo`**
HTTP Connect: **`type http operation`**
TCP Connect: **`type tcpConnect`**
ICMP Echo: **`type echo protocol ipIcmpEcho`**
ICMP Path Echo: **`type pathEcho protocol ipIcmpEcho`**
ICMP Path Jitter: **`type pathJitter`**
FTP Operations: **`type ftp`**
DNS Operations: **`type dns`**
DHCP Operations: **`type dhcp`**

NetFlow

As packets are sent through router interfaces, they can be classified into flows. This information can be sent from the router to a monitoring server that can provide valuable information about the traffic traversing the network. A flow can be described by a number of fields:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol type
- Type of Service
- Interface

 Please see page 245 for more details.

To determine if a packet belongs in a particular flow, the seven packet fields are inspected. If any one of the fields is different, the packet in question can be considered a new flow. NetFlow statistics can be collected on the following types of networks: IP, Frame Relay, MPLS, and ATM.

To enable NetFlow on an interface, the **ip flow** command set is used. To configure NetFlow on an interface:

```
Router(config-if)# ip flow ingress
Egress support can also be added:
Router(config-if)# ip flow egress
```

To configure the router to export the NetFlow data to a NetFlow server

```
Router(config)# ip flow-export {destination {ip-address | hostname} udp-port | source {interface-name}
| version {1 | [{5 | 9} [origin-as | peer-as] [bgp-nexthop]]} | template {refresh-rate packets | time-
out-rate minutes} [options {export-stats | refresh-rate packets | sampler | timeout-rate minutes}]}
```

To be exported to the NetFlow collection server, the flow must have been exported from the flow cache. Active flows (when there is an ongoing conversation) live for 30 minutes by default before they are exported. Inactive flows, those that have been terminated, are sent after 15 seconds. These values are configurable:

```
Router(config)# ip flow-cache timeout [active minutes | inactive seconds]
```

The number of flows that can be collected can be modified with:

```
Router(config)# ip flow-cache entries <#>
```

SPAN, RSPAN, and Router IP Traffic Export (RITE)

Viewing the packets between two devices is often the best way to troubleshoot a networking issue. Many organizations deploy network monitoring servers for both network functionality and security purposes. To provide these servers a stream of data from all segments of the network, the Switched Port Analyzer (SPAN) mechanism built into Cisco switches can be used. A SPAN port is a physical port that is configured to send data received on other ports or VLANs. When the data is sent out the SPAN port, it is simply a copy of all the data that has been sent through the configured source ports.

To configure the source of the data to be sent out the SPAN port

 Please see page 245 for more details.

```
Router(config)# monitor source <#> source {interface interface-id | vlan vlan-id} [, | -] [both | rx | tx]
```

Either a source interface or entire VLAN can be specified. You can use the command multiple times with the same session number if multiple sources are used.

To configure the destination of the data to be sent:

```
Router(config)# monitor destination <#> destination interface <INT>
```

The data received in the source interface is sent to the specified destination interface.

The SPAN functionality assumes that the destination of the traffic is directly connected to the switch. If the network is large, it might not be possible to wire a single monitoring station to multiple switches with SPAN ports. Fortunately a special remote SPAN (RSPAN) VLAN can be created that transports the SPAN port information to another switch. This enables an aggregation of monitoring data into a single VLAN that can be sent to the monitoring station.

To configure the RSPAN VLAN, the **remote-span** command must be specified within the VLAN configuration mode:

```
Router(config-vlan)# remote-span
Specify the destination of the SPAN port as the remote-span VLAN:
Router(config)# monitor session <#> destination remote vlan <VLAN>
```

This is great for switches, but is there a similar technology for a router? Yes! The Router IP Traffic Export (RITE) mechanism can export traffic to specific devices defined by the MAC address. To configure, a RITE profile is created and then it's applied to an interface. The traffic that RITE applies to can be limited by ACLs.

To configure the profile

```
Router(config)# ip traffic-export profile <PROFILE NAME>
Specify the outgoing interface:
Router(config-rite)# interface <INT>
Specify the MAC address to send the traffic to:
Router(config-rite)# mac-address <MAC>
```

 Please see page 245 for more details.

Specify whether bidirectional traffic is necessary. Without this command, only packets incoming to the router are sent:

```
Router(config-rite)# bidirectional
```

Optionally, ACLs can limit the traffic sent:

```
Router(config)# incoming {access-list {standard | extended | named} | sample one-in-every packet-number}
Router(config)# outgoing {access-list {standard | extended | named} | sample one-in-every packet-number}
```

Apply the RITE policy to an interface:

```
Router(config-if)# ip traffic-export apply <POLICY NAME>
```

Cisco IOS Embedded Event Manager (EEM)

In the normal operations of the switch or router, events such as a CLI command, a syslog message, or an SNMP trap, for example, are constantly occurring. These events are detected by the EEM Event Detectors that send their information to the EEM server. The EEM server can then be programmed to implement an EEM policy. The two different types of EEM policies are applets and TCL scripts, which can be programmed to perform a variety of tasks, such as send syslog messages and SNMP traps, fire off emails, and even open raw sockets.

An applet can be configured directly within the IOS CLI by first creating a policy and registering it:

```
Router(config)# event manager applet <APPLET NAME>
```

The applet must be configured to detect a specific event. There are a number of different event detectors, each with their own syntax:

```
Router(config-applet)#  event <EVENT DETECTOR>
```

- **application**: Application-specific event
- **cli:** CLI event
- **counter:** Counter event
- **interface:** Interface event
- **ioswdsysmon:** IOS WDSysMon event

 Please see page 245 for more details.

CCIE Routing and Switching v4.0 Quick Reference

Brad Ellis
Jacob Uecker
Steven Means

Technical Editor: **Scott Morris**

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

First Printing September 2011

ISBN-10: 1-58714-163-9

ISBN-13: 978-1-58714-163-8

Warning and Disclaimer

This book is designed to provide information about the CCIE Routing and Switching written exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc

Trademark Acknowledgments

All terms mentioned in this ebook that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this ebook should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical ebooks of the highest quality and value. Each ebook is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments on how we could improve the quality of this ebook, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please be sure to include the ebook title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this ebook when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com.

For sales outside the United States please contact: **International Sales** international@pearsoned.com

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.**