Cisco IOS® Embedded Packet Capture Datasheet

Product Overview

The Cisco IOS Embedded Packet Capture (EPC) delivers a powerful troubleshooting and tracing tool. The feature allows for network administrators to capture data packets flowing through, to, and from, a Cisco router.

Applications

The Cisco IOS Embedded Packet Capture function will mainly be used in troubleshooting scenarios where it is helpful to see the actual data being sent through, from, or to the network device.

Suppose, for example, helpdesk personnel need to determine why a particular device cannot access the network or some application. It might be necessary to capture IP data packets and examine the data to determine the problem.

Another case might be, when trying to determine an attack signature for a network threat or server system security breach. Cisco IOS Embedded Packet Capture can help capture packets flowing into the network at the origin or perimeter.

Cisco IOS Embedded Packet Capture is useful whenever a network protocol analyzer might be useful in debugging a problem, but when it's not practical to install such a device.

Features and Benefits

Cisco IOS Embedded Packet Capture provides an additional level of embedded systems management not previously seen in Cisco IOS Software. The feature provides enhanced capabilities beyond those previously enabled in the Router IP Traffic Export feature.

EPC includes:

- The ability to capture IPv4 and IPv6 packets in the Cisco Express Forwarding path
- A flexible method for specifying the capture buffer size and type
- EXEC-level commands to start and stop the capture
- Show commands to display packet contents on the device
- Facility to export the packet capture in PCAP format, suitable for analysis using an external tool such as Wireshark
- Extensible infrastructure for enabling packet capture points

Product Architecture

The Cisco IOS Embedded Packet Capture is a software feature consisting of infrastructure to allow for packet data to be captured at various points in the packet-processing path. The network administrator may define the capture buffer size and type (circular, or linear) and the maximum number of bytes of each packet to capture. The packet capture rate can be throttled using further administrative controls. For example, options allow for filtering the packets to be captured using an

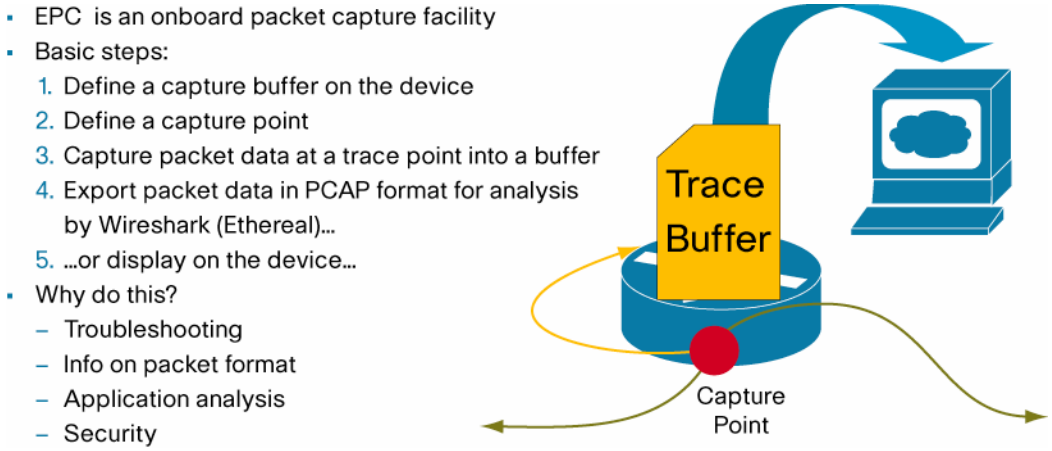
Access Control List (ACL) and, optionally, further defined by specifying a maximum packet capture rate or by specifying a sampling interval.

CLI commands are available for controlling the packet capture buffer (defining, clearing, destroying, and displaying). EXEC-level commands initiate and terminate captures at defined capture points.

The feature currently allows for capture points at the ingress and egress interfaces for Cisco Express Forwarding path and the process-switching path. Both IPv4 and IPv6 packets may be captured.

Packet data may be displayed in hex and ASCII on the CLI, or may be exported using typical file transfer methods such as a PCAP-formatted file that may be further analyzed using the open-source tool Wireshark.

Figure 1. Embedded Packet Capture



Cisco IOS Embedded Packet Capture extends the embedded management capabilities of Cisco IOS and provides another powerful tool to help resolve application and network problems. It can be particularly useful in situations where it is not practical or desirable to tap into the network using a stand-alone packet-sniffing tool, or when the need arises to remotely debug or troubleshoot issues.

Feature Specifications

Please use the Cisco IOS Feature Navigator application on Cisco.com to check the latest information on software and product availability. Go to http://cisco.com/go/fn.

The following table includes the EPC feature availability information.

Table 1. Feature Specifications

Feature	Description
Product Compatibility	EPC is available for the Cisco Integrated Services Routers, and the Cisco 7200 Series Routers
Software Compatibility	EPC is available in Cisco IOS Software Release 12.4(20)T and future versions
Software Packaging	Please refer to the Cisco IOS Feature Navigator for the latest packaging information

System Requirements

The EPC software subsystem will consume CPU and memory resources in its operation. Customers should examine the operation in their environment to ensure resources exist for their specific scenarios. Some basic guidelines are included in Table 2.

Table 2. System Requirements

Feature	Description
Hardware	CPU utilization requirements are platform dependent
Memory	The packet buffer is stored in DRAM; The size of the packet buffer is user specified
Disk Space	Packets can be exported to external systems; No intermediate storage on flash disk is required

Service and Support

Using the Cisco Lifecycle Services approach, Cisco and its partners provide a broad portfolio of end-to-end services and support that can help increase your network's business value and return on investment. This approach defines the minimum set of activities needed, by technology and by network complexity, to help you successfully deploy and operate Cisco technologies and optimize their performance throughout the lifecycle of your network.

Customers authorized for service and support may contact the Cisco Technical Assistance Center (TAC) for issues related to EPC. The TAC will resolve problems related to the operation of the EPC infrastructure.

For More Information

For more information about the Cisco IOS Embedded Packet Capture, visit http://www.cisco.com/go/epc or contact your local account representative or send email to askaboutiosinfra@cisco.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.

Printed in USA C78-502727-00 10/08