Cisco IOS Embedded Packet Capture (EPC)

Cisco IOS Embedded Packet Capture (EPC)

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.

EPC 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 and, optionally, further defined by specifying a maximum packet capture rate or by specifying a sampling interval.

Note: You need to be running IOS version 12.4(20)T or later to use EPC.

Cisco IOS Embedded Packet Capture (EPC)

Cisco IOS Embedded Packet Capture provides enhanced capabilities beyond those previously enabled in the Router IP Traffic Export feature. EPC includes:

- 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
- Filter captured packets.
- Methods to decode data packets captured with varying degree of detail.
- Extensible infrastructure for enabling packet capture points.
- Facility to export the packet capture in PCAP format suitable for analysis using an external tool such as Wireshark

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.

Prerequisites and Restrictions

The EPC software subsystem consumes CPU and memory resources in its operation. You must have adequate system resources for different types of operations. Some guidelines for arranging the system resources are provided below:

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.**

Restrictions for Embedded Packet Capture:

- **In Cisco IOS Release 12.2(33)SRE, EPC is supported only on 7200 platform.**
- **EPC only captures multicast packets on ingress and does not capture the replicated packets on egress.**
- **Currently, the capture file can only be exported off the device; for example, TFTP or FTP servers and local disk.**

Capture Buffer

The capture buffer is an area in memory for holding the packet data. You can specify unique names, size and type of the buffer, and configure the buffer to handle incoming data as required. The following types of data are stored in a capture buffer:

Packet data - The packet data starts from datagramstart and copies a minimum of the per-packet-capture size or datagramsize to the capture buffer.

Metadata - The metadata contains descriptive information about a set of packet data. It contains:

- A timestamp of when it is added to a buffer.
- The direction in which the packet data is transmitted—egress or ingress.
- The switch path captured.
- Encapsulation type corresponding to input or output interface to allow the decoding of L2 decoders.

The following actions can be performed on capture buffers:

- Define a capture buffer and associate it with a capture point.
- Clear capture buffers.
- Export capture buffers for offline analysis. Export writes off the file using one of the supported file transfer options: FTP, HTTP, HTTPS, PRAM, RCP, SCP, and TFTP.
- Display content of the capture buffers.

Capture Point

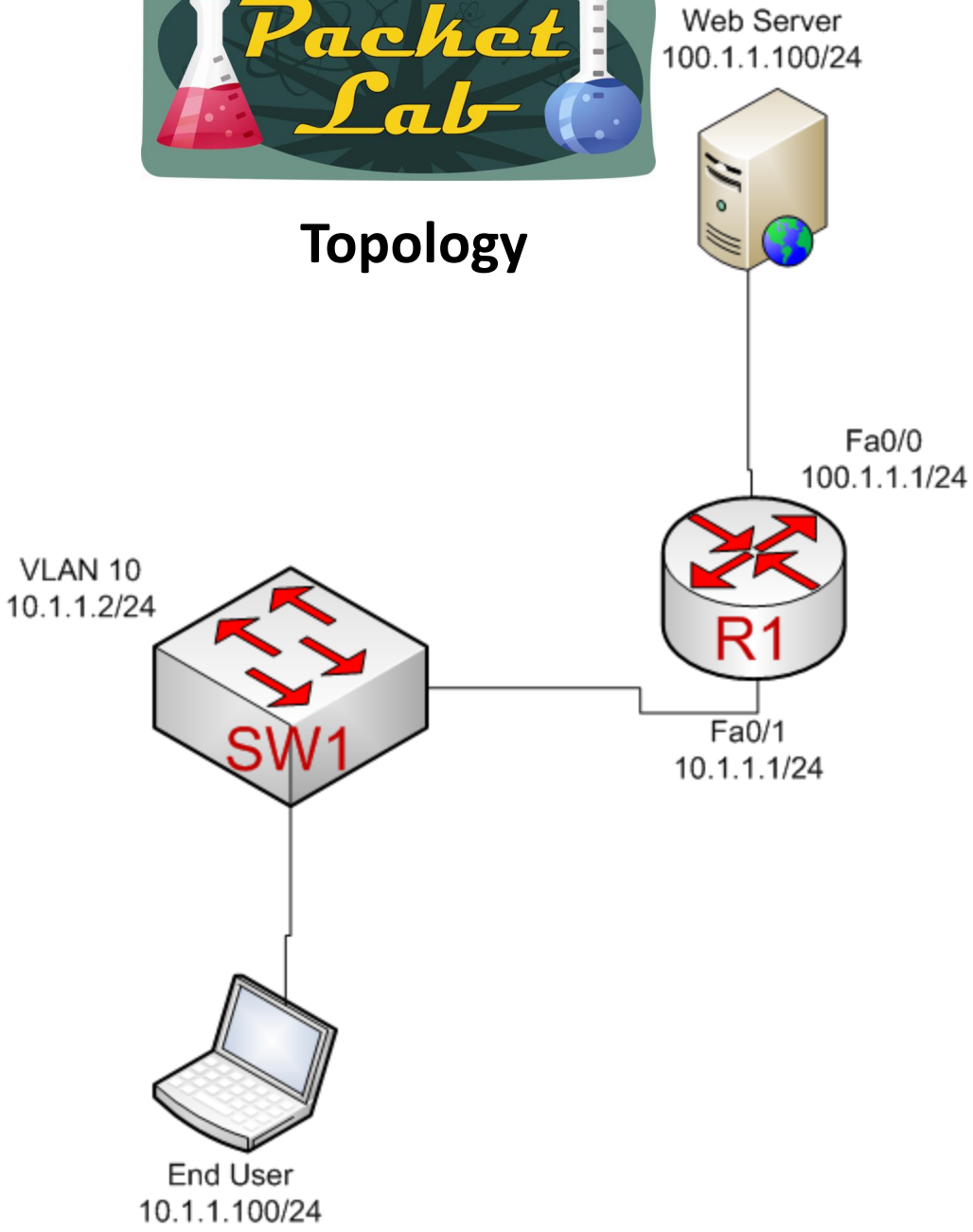
The capture point is a **traffic transit point where a packet is captured** and associated with a buffer. You can define capture points by providing unique names and different parameters.

The following capture points are available:
•IPv4 CEF/interrupt switching path with interface input and output
•IPv6 CEF/interrupt switching path with interface input and output

You can perform the following actions on the capture point:
•Associate or disassociate capture points with capture buffers. **Each capture point can be associated with only one capture buffer.**
•**Destroy** capture points. ☺
•Activate packet capture points on a given interface. Multiple packet capture points can be made active on a given interface. For example, Border Gateway Protocol (BGP) packets can be captured into one capture buffer and Open Shortest Path First (OSPF) packets can captured into another capture buffer.
•Access Control Lists (ACLs) can be applied to capture points.

Multiple packet capture points can be activated on a given interface. For example, Border Gateway Protocol (BGP) packets can be captured into one capture buffer and Open Shortest Path First (OSPF) packets into another.

Topology


Web Server
100.1.1.100/24
Fa0/0
100.1.1.1/24
R1
VLAN 10
10.1.1.2/24
SW1
Fa0/1
10.1.1.1/24
End User
10.1.1.100/24

Configuring EPC

1) Define Capture Buffer
2) Define Capture Point
3) Associate Capture Point with Capture Buffer
4) Start packet capture
5) Stop packet capture
6) Transport capture from Capture Buffer to another device
7) Analyze packet capture.

Starting Packet Data Capture

To capture packet data, a capture buffer and a capture point need to be defined. The capture point should then be associated with the capture buffer. Enabling the capture point will start the process of capturing packet data.

First we need to define a a capture buffer with a name and parameters:

```
r1#monitor capture buffer MYCAPTUREBUFFER ?
 circular  Circular Buffer
 clear     Clear contents of capture buffer
 export    Export in Pcap format
 filter    Configure filters
 limit     Limit the packets dumped to the buffer
 linear    Linear Buffer(Default)
 max-size  Maximum size of element in the buffer (in bytes)
 size      Packet Dump buffer size (in Kbytes)
 <cr>
```

```
r1#monitor capture buffer MYCAPTUREBUFFER size 512 max-size 256 linear
```

Capture Buffer Options

circular (Optional) - Specifies that the buffer is of circular type.
clear (Optional) - Clears contents of capture buffer.
filter access-list (Optional) - Configures filters to filter the packets stored in the capture buffer using access **control lists** (ACLs). Name or type of access lists can be specified as criteria for configuring the filters.
limit (Optional) - Limits the packets captured based on the parameters specified.
allow-nth-pak nth-packet (Optional) - Allows every nth packet in the captured data through the buffer.
duration seconds (Optional) - Specifies the duration of capture measured, in seconds. Range is from 1 to 2147483647.
packet-count total-packets (Optional) - Specifies the total number of packets captured. Range is from 1 to 2147483647.
packets-per-sec packets (Optional) - Specifies the number of packets copied per second. Range is from 1 to 2147483647.
linear (Optional) - Specifies that the buffer is of linear type. **By default, the capture buffer is of linear type**.
max-size element-size (Optional) - Maximum size of element in the buffer, in bytes. Range is from 68 to 9500.
size buffer-size (Optional) - Size of the buffer. Range is from 256 kilo bytes (KB) to 100 mega bytes (MB). The default value is 1 MB.

Starting Packet Data Capture

Once we've configured our capture buffer, we need to configure our capture point. In this example we want to capture IPv4 traffic in both directions on FastEthernet port 0/1 (connected to the Internal LAN):

```
r1#monitor capture point ip cef INTERNALLAN fastEthernet 0/1 both

*Jun 20 20:45:34.487: %BUFCAP-6-CREATE: Capture Point INTERNALLAN created.
```

Now that we have a capture buffer and a capture point defined, we need to associate the capture point with a capture buffer [remember: Each capture point can be associated with only one capture buffer]:

```
r1#monitor capture point associate ?
  WORD  Name of the Capture Point

r1#monitor capture point associate INTERNALLAN ?
  WORD  Name of the Capture Buffer

r1#monitor capture point associate INTERNALLAN MYCAPTUREBUFFER
```

Capture Point Options

ip - Configures an IPv4 capture point.
ipv6 - Configures an IPv6 capture point.
cef - Specifies that the capture point contains Cisco Express Forwarding (CEF) packets.
process-switched - Specifies that the capture point contains process switched packets.
in - Specifies that the packets are captured in ingress direction.
out - Specifies that the packets are captured in egress direction.
both - Specifies that the packets are captured in ingress and egress directions.
from-us - Specifies that the packets are originating locally.

Starting Packet Data Capture

After the capture buffer and capture point have been created and associated, all that remains is to start the capture:

```
r1#monitor capture point start ?
  WORD  Name of the Capture Point
  all   All Capture Points

r1#monitor capture point start INTERNALLAN

*Jun 20 21:05:23.919: %BUFCAP-6-ENABLE: Capture Point INTERNALLAN enabled.
```

Stopping Packet Data Capture

Once you've captured enough packets, you can stop the packet capture:

```
r1#monitor capture point stop ?
  WORD  Name of the Capture Point
  all   All Capture Points

r1#monitor capture point stop INTERNALLAN

*Jun 20 21:05:58.831: %BUFCAP-6-DISABLE: Capture Point INTERNALLAN
disabled.
```

Exporting Packet Data For Analysis

You can export a packet capture to another device via multiple methods:

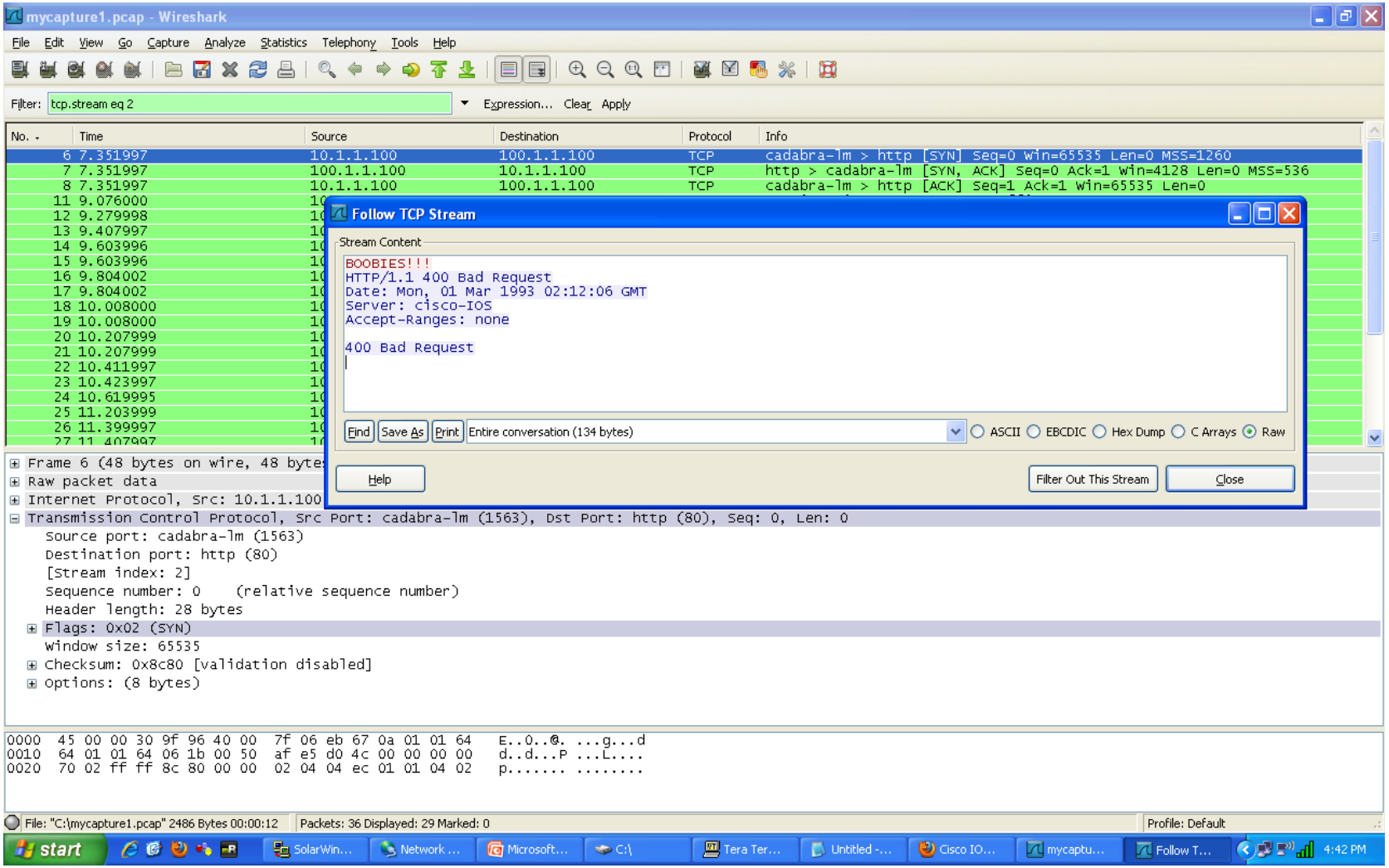
```
r1#monitor capture buffer MYCAPTUREBUFFER export ?
  ftp:    Location to dump buffer
  http:   Location to dump buffer
  https:  Location to dump buffer
  pram:   Location to dump buffer
  rcp:    Location to dump buffer
  scp:    Location to dump buffer
  tftp:   Location to dump buffer

r1#monitor capture buffer MYCAPTUREBUFFER export tftp://10.1.1.100/mycapture1.pcap
!
```

Make sure you name your file when exporting or you'll get an error:

```
r1#monitor capture buffer MYCAPTUREBUFFER export tftp://10.1.1.100
% Export of Capture Buffer failed
*Jun 20 21:25:30.031: %BUFCAP-3-EXPORT_BUFFER: Error exporting buffer
MYCAPTUREBUFFER to location tftp://10.1.1.100
```

Open With Packet Analysis Software



Clearing Packet Capture Buffer

```
r1#show monitor capture buffer MYCAPTUREBUFFER parameters
Capture buffer MYCAPTUREBUFFER (linear buffer)
Buffer Size : 524288 bytes, Max Element Size : 256 bytes, Packets : 36
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Name : INTERNALLAN, Status : Inactive
Configuration:
monitor capture buffer MYCAPTUREBUFFER size 512 max-size 256 linear
monitor capture point associate INTERNALLAN MYCAPTUREBUFFER

r1#monitor capture buffer MYCAPTUREBUFFER clear

r1#show monitor capture buffer MYCAPTUREBUFFER parameters
Capture buffer MYCAPTUREBUFFER (linear buffer)
Buffer Size : 524288 bytes, Max Element Size : 256 bytes, Packets : 0
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Name : INTERNALLAN, Status : Inactive
Configuration:
monitor capture buffer MYCAPTUREBUFFER size 512 max-size 256 linear
monitor capture point associate INTERNALLAN MYCAPTUREBUFFER
```

Disassociating Capture Point from Capture Buffer

```
r1#monitor capture point disassociate INTERNALLAN

r1#show monitor capture point all
Status Information for Capture Point INTERNALLAN
IPv4 CEF
Switch Path: IPv4 CEF             , Capture Buffer: None
Status : Inactive

Configuration:
monitor capture point ip cef INTERNALLAN FastEthernet0/1 both

r1#show monitor capture buffer MYCAPTUREBUFFER parameters
Capture buffer MYCAPTUREBUFFER (linear buffer)
Buffer Size : 524288 bytes, Max Element Size : 256 bytes, Packets : 0
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Configuration:
monitor capture buffer MYCAPTUREBUFFER size 512 max-size 256 linear
```

Deleting Packet Capture Buffer and Capture Points

```
r1#no monitor capture buffer MYCAPTUREBUFFER
Capture Buffer deleted

r1#show monitor capture buffer MYCAPTUREBUFFER parameters
Capture Buffer MYCAPTUREBUFFER does not exist

r1#no monitor capture point ip cef INTERNALLAN fa0/1
*Jun 21 00:07:25.471: %BUFCAP-6-DELETE: Capture Point INTERNALLAN deleted.

r1#show monitor capture point INTERNALLAN
Capture point INTERNALLAN does not exist
```

Viewing Packet Capture Data On The Router

While it's highly recommended that you export the packet capture data to another device and analyze the data with a program like Wireshark, you do have the option to view the packets on the router in ASCII format:

```
r1#show monitor capture buffer MYCAPTUREBUFFER dump
21:05:34.235 UTC Jun 20 2010 : IPv4 LES CEF    : Fa0/1 None

48063CC0:                   001E7ADF AA39001D          ..z_*9..
48063CD0: 09DEFFF5 08004500 003E9F8B 00007F11  .^.u..E..>......
48063CE0: 1BEE0A01 0164C6CB AE05C0DD 0035002A  .n...dFK..@].5.*
48063CF0: 91D6367B 01000001 00000000 00000377  .V6{...........w
48063D00: 77770866 61636562 6F6F6B03 636F6D00  ww.facebook.com.
48063D10: 00010001 00                          .....

21:05:35.235 UTC Jun 20 2010 : IPv4 LES CEF    : Fa0/1 None

48063CC0:                   001E7ADF AA39001D          ..z_*9..
48063CD0: 09DEFFF5 08004500 003E9F8D 00007F11  .^.u..E..>......
48063CE0: 1BEA0A01 0164C6CB AE07C0DD 0035002A  .j...dFK..@].5.*
48063CF0: 91D4367B 01000001 00000000 00000377  .T6{...........w
48063D00: 77770866 61636562 6F6F6B03 636F6D00  ww.facebook.com.
48063D10: 00010001 00
```

Viewing Packet Capture Data On The Router

You also have some simple filtering options when viewing data on the router:

```
r1#show monitor capture buffer MYCAPTUREBUFFER dump filter ?
  direction          Filter output based on direction
  input-interface    Filters packet on an input interface
  l3protocol         Filter packets with specific L3 protocol
  output-interface   Filters packet on an output interface
  pak-size           Filter output based on packet size
  time               Filter packets from a specific clock time/date
```

Verification Commands

There are two very good verification commands associated with EPC:

```
r1#show monitor capture buffer ?
  WORD    Name of the Capture Buffer
  all     All capture buffers
  merged  Merged View of Capture Buffers

r1#show monitor capture buffer all ?
  parameters  Parameters of capture buffer

r1#show monitor capture buffer all parameters
Capture buffer MYCAPTUREBUFFER (linear buffer)
Buffer Size : 524288 bytes, Max Element Size : 256 bytes, Packets : 36
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Name : INTERNALLAN, Status : Inactive
Configuration:
monitor capture buffer MYCAPTUREBUFFER size 512 max-size 256 linear
monitor capture point associate INTERNALLAN MYCAPTUREBUFFER
```

Verification Commands

```
r1#show monitor capture point ?
  WORD  Name of the Capture Point
  all   All capture points

r1#show monitor capture point all
Status Information for Capture Point INTERNALLAN
IPv4 CEF
Switch Path: IPv4 CEF             , Capture Buffer: MYCAPTUREBUFFER
Status : Inactive

Configuration:
monitor capture point ip cef INTERNALLAN FastEthernet0/1 both
```

Summary

With the addition of the Embedded Packet Capture (EPC) feature, Cisco IOS gives you ability to capture data packets flowing through, to, and from, a Cisco router. You'll need to be running IOS version 12.4(20)T or later and you'll need a beefy router with plenty of DRAM and CPU like the ISR series. You do have the ability to view captured data on the router in ASCII format with some limited filters, but in most cases you'll want to transfer the captured data to another device to do the packet analysis (FTP, HTTP, HTTPS, PRAM, RCP, SCP, and TFTP are all supported transfer methods).

While EPC does not take the place of a dedicated sniffer, NAM, or even a laptop with packet analysis software installed; it does give you a nice packet capture option in situations when you don't have another method to capture packets.