Packet Capture Capabilities of Cisco Routers and Switches

Hitesh Kumar
CCIE SP (#38757)
High Touch Technical Support

Rahul Rammanohar
CCIE R&S, SP (#13015)
High Touch Technical Support
Case 1 – 7600/6500
Sup720/Sup32/Sup2T/RSP720

**Mini Protocol Analyzer**

- It captures traffic from a SPAN session and stores it into a local buffer.
- Supported in releases 12.2(33)SRD and 12.2(33)SXI onwards.
- Can be used to capture both transit and traffic destined to the device.
- Can capture both ingress and egress traffic.
- Choosing the right filter is important, else it can cause a lot of traffic getting punted to the RP CPU.

**Reference**

Case 1 – 7600/6500 Sup720/Sup32/Sup2T/RSP720

**Mini Protocol Analyzer**

R2(config)#monitor session <session number> type capture

R2(config-mon-capture)#source interface <interface> <direction>  \(\leftarrow\) Choose the source interface of the traffic

R2(config-mon-capture)#filter access-group <Access List>  \(\leftarrow\) Choose the filter (either HW or SW based)

R2#monitor capture start  \(\leftarrow\) Start the capture

R2#monitor capture stop  \(\leftarrow\) Stop the capture

R2#show monitor capture status captured  \(\leftarrow\) To determine the status of the capture and the number of packets captured

R2#show monitor capture buffer …  \(\leftarrow\) To display the packets

R2#monitor capture export buffer <location>  \(\leftarrow\) To store the packets in a libpcap file that can be read by an external tool like Wireshark.

© 2010 Cisco and/or its affiliates. All rights reserved.
Case 1 – 7600/6500
Sup720/Sup32/Sup2T/RSP720

Loop0 – 9.0.0.3
Traffic Generator

Loop0 – 9.0.0.2
Gig1/9 7600 Gig5/2

Loop0 – 10.105.98.65
Transit Traffic Destination

Transit Traffic for the DUT
Traffic Destined to the DUT
Case 1 – 7600/6500
Sup720/Sup32/Sup2T/RSP720

Mini Protocol Analyzer

DEMO
ELAM

- It provides information on the forwarding decision taken by the forwarding ASICs.
- Can be used to capture both transit and traffic destined to the device as it captures the packet before the forwarding decision is made.
- It can capture only one packet at a time.
- If the ingress line card has a DFC then perform the ELAM on the ingress line card else preform the ELAM on the active Supervisor.
- Requires ‘service internal’, a hidden command, to be configured.
ELAM

R2#show platform capture elam asic  ← List the forwarding ASICs where an ELAM can be performed

R2#show platform capture elam asic <forwarding ASIC> slot <slot number>  ← Select the forwarding ASIC and slot number, where ELAM will be performed

R2#show platform capture elam trigger dbus ipv4 help  ← List out the triggers

R2#show platform capture elam trigger dbus ipv4 if <triggers>  ← Select the packet capture triggers

R2#show platform capture elam start  ← Start the capture

R2#show platform capture elam status been captured  ← To verify the trigger and to check whether the packet has been captured

R2#show platform capture elam data  ← To display the packet
Case 1 – 7600/6500
Sup720/Sup32/Sup2T/RSP720

ELAM

DEMO
Case 1 – 7600/6500
Sup720/Sup32/Sup2T/RSP720

**NETDR**

- The tool allows packets to be captured just before they reach the processor, either Switch Processor or Route Processor.

- A single command to capture the packets.

- Can capture only 4096 packets at a time.

- Though the command starts with a debug, it is not an IOS related debug. Hence, the command can be run even when the CPU is 99%.

- Very useful to troubleshoot high CPU utilization issues due to traffic.
Case 1 – 7600/6500 Sup720/Sup32/Sup2T/RSP720

**NETDR**

**Route Processor**

R2#debug netdr capture …

(can specify the direction of traffic, the source/destination IP addresses, ethertype, interface …)

**Switch Processor**

R2-sp#debug netdr capture … ← run the command from the Switch Processor prompt

R2#show netdr captured-packets ← view the captured packets
Case 1 – 7600/6500
Sup720/Sup32/Sup2T/RSP720

NETDR

DEMO
Network Processor Capture

- Packets can be captured on the network processor of the 2\textsuperscript{nd} generation line cards based on counters. 2\textsuperscript{nd} generation line cards use the Typhoon network processor.
- Most useful to capture packets based on the dropped counters.
- Can be used to capture both transit and traffic destined to the device.
- Each packet that is captured will be dropped.
- Network Processor will reset after the capture, resulting in up to 50ms of traffic loss.

Reference (also lists the limitations)
https://supportforums.cisco.com/docs/DOC-29010
https://supportforums.cisco.com/docs/DOC-15552
Case 2 – ASR9K – 2nd Generation LCs Only

**Network Processor Capture**

R2#show controller np ports all location 0/X/cpu0 ← Line cards have multiple NPs, firstly need to
determine the NP for the incoming interface.

R2#show controllers np counters <network processor> location 0/X/CPU0 ← This command would list
the various counters for the particular NP

R2#monitor np counter <counter> <network processor> location 0/X/CPU0 ← Command to capture the
packets

R2#debug netio drivers… ← Can be used to capture the packets getting punted to Line Card or Route
processor CPU. Not advisable to run in a live network, hence we will not talk about it here.
Case 2 – ASR9K – 2nd Generation LCs Only

Traffic Generator 192.168.1.2 Ten0/1/0/3 ASR9k Ten0/0/0/3 Transit Traffic Destination 172.20.60.1

Transit Traffic for the DUT
Traffic Destined to the DUT
Case 2 – ASR9K – 2nd Generation LCs Only

Network Processor Capture

DEMO
Case 3 – 7200/ISRs

Embedded Packet Capture

- It’s an IOS feature that can capture transit packets, packets destined to the router and packets generated from the router.
- Implemented from 12.4(20)T onwards.
- In 12.2(33)SRE, supported only on the 7200.

Reference

https://supportforums.cisco.com/docs/DOC-5799
Case 3 – 7200/ISR

Embedded Packet Capture

**Step 1** - Define the buffer where the frames would be stored.

R2#monitor capture buffer <buffer name> size <buffer size> filter <ACL>…  ← Can specify the size, the type of buffer, an ACL to allow only certain packets and where to export the buffer to.

**Step 2** - Define the capture point where the frames need to be captured.

R2#monitor capture point <capture point name> ip <cef | processed-switching> interface <interface name> <both | in | out>  ← Specify the switching path, the interface and the direction of the traffic to the captured.

**Step 3** - Associate the capture point to the capture buffer.

R2#monitor capture point associate <capture point name> <buffer name>

R2#monitor capture point start < capture point name>  ← Start the capture

R2#monitor capture point stop < capture point name>  ← Stop the capture

R2#monitor capture < capture point name> export <path>  ← To store the packets captured into a file

R2#show monitor capture <buffer name> dump  ← To display the packets.

R2#show monitor capture <buffer name> dump
Case 3 – 7200/ISR

- Loop0 – 9.0.0.3
  - Traffic Generator
- Loop0 – 9.0.0.221
  - Gig0/1
  - 7200
  - Gig0/2
- Loop0 – 10.105.98.65
  - Transit Traffic Destination

Transit Traffic for the DUT
Traffic Destined to the DUT
Case 3 – 7200/ISR

Embedded Packet Capture

DEMO
Case 4 – Nexus 7K, 5K and 3K

Ethalyzer

- A very advanced sniffer that is built in to the router that is based on the Wireshark open source code.
- It stores packets in a libpcap format on the router.
- Best suited to capture packets that are destined to the router. On the N7K, can also be used to capture transit traffic by configuring an ACL with log.
- Packets can be captured based on wireshark filter syntax or tcpdump filter syntax.
- A single command is required to enable the capture and can be stopped by pressing Ctrl C.

Reference

http://wiki.wireshark.org/DisplayFilters
Case 4 – Nexus 7K, 5K and 3K

Ethanalyzer

Nexus 7K

R2#ethanalyzer local interface inband capture-filter “<filter in TCP Dump syntax>”  ➙ Traffic being sent to the CPU are captured

OR

R2#ethanalyzer local interface inband display-filter “<filter in Wireshark syntax>”  ➙ Traffic being sent to the CPU are captured

R2#ethanalyzer local read <libpcap file stored on the router> ➙ An earlier captured file can be read.

Nexus 3K or 5K

R2#ethanalyzer local interface inbound-low/inbound-hi display-filter “<filter in Wireshark syntax>”  ➙ Traffic being sent to the CPU are captured

OR

R2#ethanalyzer local interface inbound-low/inbound-hi capture-filter “<filter in TCP Dump syntax>”  ➙ Traffic being sent to the CPU are captured
Case 4 – Nexus 7K, 5K and 3K

Traffic Generator

2.2.2.2

Vlan200

2.2.2.3

Nexus 7K

Vlan20

20.20.20.3

Transit Traffic Destination

Transit Traffic for the DUT

Traffic Destined to the DUT
Case 4 – Nexus 7K, 5K and 3K

Ethanalyzer

DEMO
Case 4 – Nexus 7K

ELAM

- It provides detailed information on the forwarding decision taken by the forwarding ASICs.
- Similar to the ELAM on the 7600/6500.
- Can be used to capture transit traffic, traffic destined to the device and traffic generated from the device.
- It can capture only one packet at a time.
Case 4 – Nexus 7K

**ELAM**

Nexus 7K

attach module <x> ➔ connect to the line card

show hardware internal dev-port-map ➔ to determine to which ASIC we need to perform the capture

elam slot <x> asic eureka instance <x> ➔ to specify the forwarding ASIC and instance

trigger dbus dbi ingress ipv4 if? ➔ lists the various trigger options available for the selected ASIC

trigger dbus dbi ingress ipv4 if <triggers> rbi-corelate ➔ setup the dbus trigger

trigger rbus rbi <packet buffer> ip if cap2 1 ➔ setup the rbus trigger

show elam slot <x> asic status ➔ verify elam config and status of capture

start ➔ start the elam capture

show elam slot <x> asic eureka instance <y> dbus ➔ to view the dbus information for the captured pkt

show elam slot <x> asic eureka instance <y> rbus ➔ to view the rbus information for the captured pkt
Case 4 – Nexus 7K

Traffic Generator 3.3.100.2 Vlan300 Eth1/31 Nexus 7K

Vlan20 3.3.100.1

Transit Traffic for the DUT

Traffic Destined to the DUT

Transit Traffic Destination 20.20.20.3
Case 4 – Nexus 7K

ELAM

DEMO
Show Captured Packets

- Displays packets that are destined to the device and switched in software. Also, captures hardware switched dropped packets by default.
- Works in both ingress and egress direction.
- The buffer holds about 200 packets and is circular.
- For software switched packets, need to configure “capture software packets” under the interface.

Reference

http://www.cisco.com/en/US/docs/routers/crs/software/crs_r4.0/adv_system/command/reference/b_ar_crs1_chapter_01.html#wp2306296788
Case 5 – CRS

Show Captured Packets

For software switched

R2(config-if)#capture software packets ➦ under the interface config

R2#show captured packets ingress/egress interface <interface name> location <CPU of the interface> ➦ To display the packets.
Case 5 – CRS

Traffic Generator

3.3.3.1

Ten0/6/0/0

CRS

3.3.3.2

Ten0/0/0/4

Transit Traffic for the DUT

Transit Traffic Destination

96.34.0.145

Traffic Destined to the DUT
Case 5 – CRS

Show Captured Packets

DEMO
Embedded Packet Capture

- Similar to EPC on 7200/ISR routers but the syntax is slightly different.
- Supported from 3.7 release onwards. Need to use ERSPAN for previous releases.
- Packets can be captured through, to and from the router.

Reference

Embedded Packet Capture

R2#monitor capture <name> access-list <ACL name>  ↩ Specify the filter.
R2#monitor capture <name> limit … ↩ Specifies the capture limits either duration, number of packets …
R2#monitor capture <name> interface <interface name>  ↩ To capture transit packets.

OR

R2#monitor capture <name> control-plane <interface name>  ↩ To capture packets to and from the router.
R2#monitor capture <name> buffer …  ↩ Specify the buffer size and type
R2#monitor capture <name> start  ↩ Start the capture
R2#monitor capture <name> stop  ↩ Stop the capture
R2#monitor capture <name> export <path>  ↩ To store the packets captured into a file

R2#show monitor capture <name> parameter  ↩ To display the capture configuration.
R2#show monitor capture <name> buffer dump  ↩ To display the packets.
Case 6 – ASR1K

Loop0 – 9.0.0.3
Traffic Generator

Gig1/0/1
ASR1K
Gig1/0/3

 Transit Traffic for the DUT

 loop0 – 9.0.0.6

 Loop0 – 10.105.98.65

 Transit Traffic Destination

 loop0 – 9.0.0.3
Case 6 – ASR1K

Embedded Packet Capture

DEMO
Thank you for Watching 😊
Common Topology

Loop0 – 9.0.0.3
Traffic Generator

Loop0 – 9.0.0.X
DUT

Loop0 – 10.105.98.65
Transit Traffic Destination

Transit Traffic for the DUT
Traffic Destined to the DUT
Case 2 – ASR9K – 2\textsuperscript{nd} Generation LCs Only

Traffic Generator

192.168.1.2

ASR9k

192.168.1.1

Transit Traffic for the DUT

Transit Traffic for the DUT

Traffic Destined to the DUT

Traffic Destined to the DUT

Ten0/1/0/3

Ten0/0/0/3

172.20.60.1

Transit Traffic Destination