

Packet Capture @ Cisco Nexus and Catalyst Switch

By Yame Kim Sense 야매 김선생

Catalyst Embedded Packet Capture

- Catalyst 9000 series, 3850/3650, 4500
- Physical ports only - not VLAN or logical
- One live session
- 1,000 PPS limit while no duration, size limit
- no Egress control plane
- Saved to Memory or flash



Catalyst Configuration from cisco live

```
Switch#monitor capture CLUS interface GigabitEthernet 1/0/2 both
Switch#monitor capture CLUS match ipv4 any any
Switch#monitor capture CLUS limit duration 60
Switch#monitor capture CLUS file location flash:clus_cap
Switch#monitor capture CLUS start display brief

Starting the packet display ..... Press Ctrl + Shift + 6 to exit
```

Where and what
capture

```
  1  0.000000 10.254.111.100 -> 10.254.254.1 TCP 74 734 b^F^R 2049 [SYN]
Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=445826583 TSecr=0 WS=128
  2  0.000501 10.254.254.1 -> 10.254.111.100 TCP 60 2049 b^F^R
Seq=1 Ack=1 Win=0 Len=0
  3  1.001299 10.254.111.100 -> 10.254.254.1 TCP 74 711 b^F^R :
Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=445826833 TSecr=0 WS=128
  4  1.001582 10.254.254.1 -> 10.254.111.100 TCP 60 2049 b^F^R 711 [RST, ACK]
Seq=1 Ack=1 Win=0 Len=0
```

Storage location and
duration

Capture CLUS stopped - Capture duration limit reached

Catalyst Display from cisco live

```
Switch#show monitor capture file flash:cl.cap brief
```

```
Starting the packet display ..... Press Ctrl + Shift + 6 to exit
```

```
1 0.000000 10.200.10.100 -> 10.200.10.200 TCP 66 59498 b^F^R 80 [ACK] Seq=1 Ack=1
```

```
Switch#show moni capture file flash:cl.cap packet-number 1 detailed | be Transmission
```

```
Transmission Control Protocol, Src Port: 59498 (59498), Dst Port: 80 (80), Seq: 1, Ack:
```

```
1, Source Port: 59498
```

```
Destination Port: 80
```

```
Sequence number: 1 (relative sequence number)
```

```
Acknowledgment number: 1 (relative ack number)
```

```
Header Length: 32 bytes
```

```
Flags: 0x010 (ACK)
```

```
000. .... = Reserved: Not set
```

```
...0 .... = Nonce: Not set
```

```
.... 0... = Congestion Window Reduced (CWR): Not set
```

```
.... .0.. = ECN-Echo: Not set
```

```
.... ..0. = Urgent: Not set
```

```
.... ...1 = Acknowledgment: Set
```

```
.... .... 0... = Push: Not set
```

```
.... .... .0.. = Reset: Not set
```

```
.... .... ..0. = Syn: Not set
```

```
.... .... ...0 = Fin: Not set
```

```
[TCP Flags: *****A*****]
```

```
Window size value: 24464
```

saved captures

Details packet
decodes

Off Box Analysis
using Wireshark also
possible