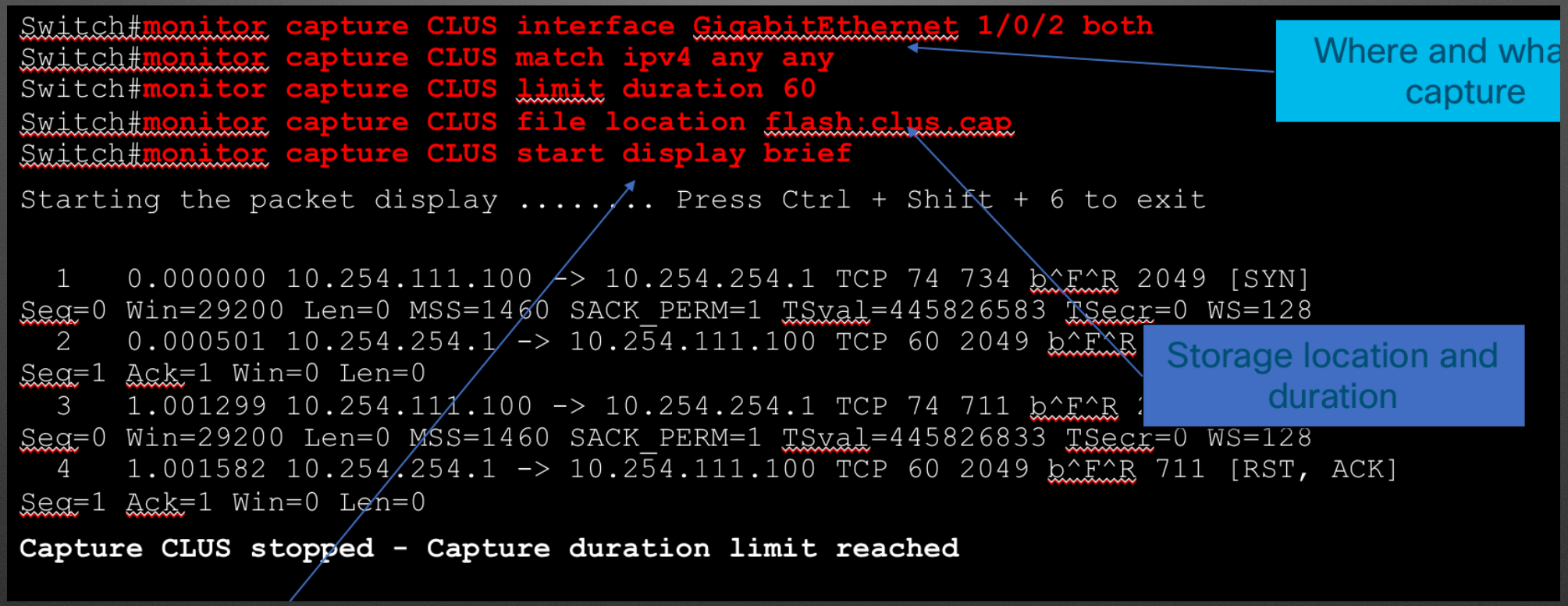
Packet Capture @ Cisco Nexus and Catalyst Switch

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



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