The bridge to possible

Troubleshoot Control Plane Issues on C9500X and C9600X Switches

Tips and Tricks

Mario Aquino Lopez - TCE
Miguel Perez - TCE

TACENT-2017

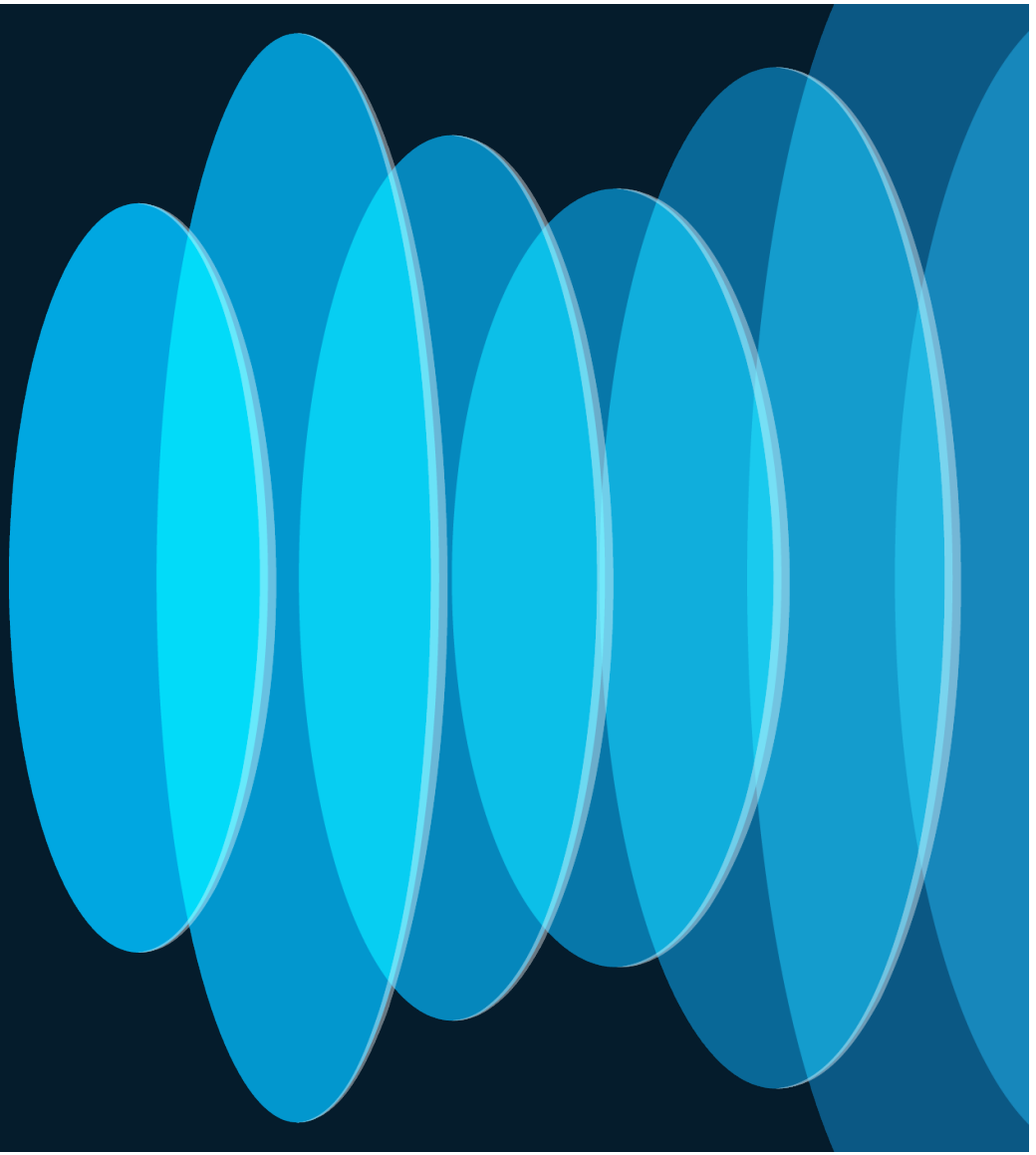
cisco Live!

Agenda

- Introduction
- Problem Description
- Troubleshooting Tools
- Packet Capture Analysis
- Root Cause and Resolution
- Conclusion
- Q&A

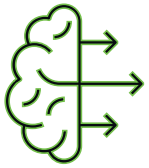
cisco Live!

Introduction

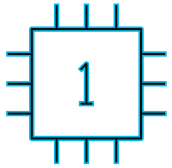


cisco Live!

Control Plane Overview



Control plane is responsible for maintaining the switch's forwarding tables updated.



Data plane simply transmits user traffic from one interface to the other.

There is a system default policy that groups control-plane traffic into 53 class maps, which are rate limited to protect the CPU.

View the rate limit for each class-map with the following command:

```
C9500X#show policy-map control-plane
```

If the rate limit is exceeded, traffic on the same class map is dropped

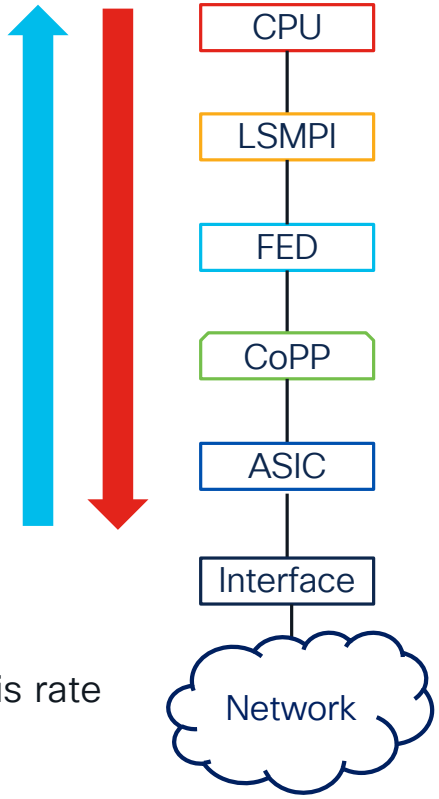
Note: Above command is comparable to Doppler based Cat9k Switches:

```
Cat9k#show platform hardware fed switch active qos queue internal cpu policer
```

Terminology

Punt: Network traffic travels from hardware to software for CPU processing.

Inject: Local CPU generated network traffic travels from software to hardware into the network.



ASIC

Instances mapped to different interfaces that derive from code translated by FED based on CLI configurations.

Forwarding Engine Driver

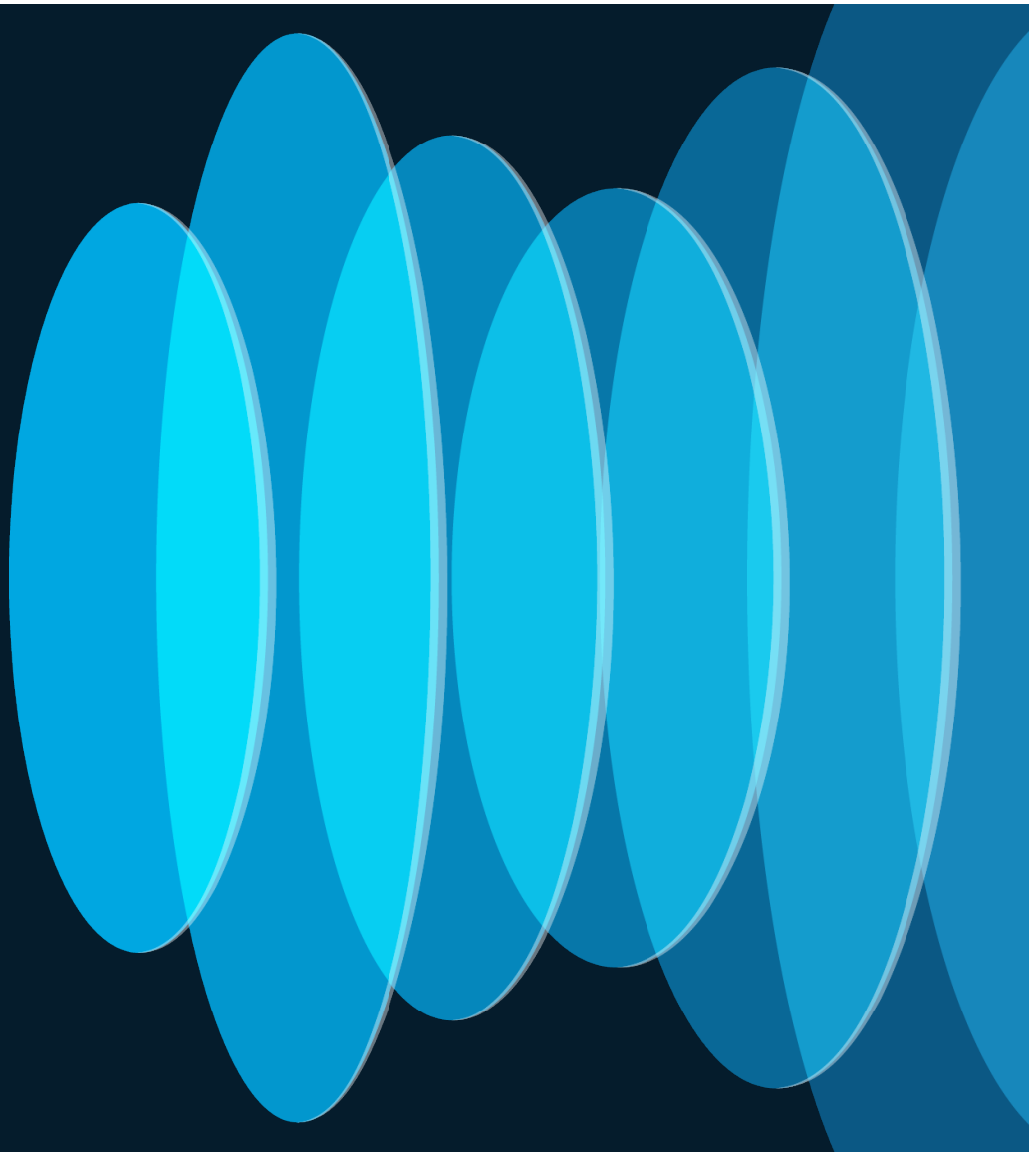
Process responsible for programming the ASIC derived from CLI commands.

Linux Shared Memory Punt Interface

Process responsible from moving packets in and out of the Linux kernel.

Note: Only punt direction is rate limited by CoPP.

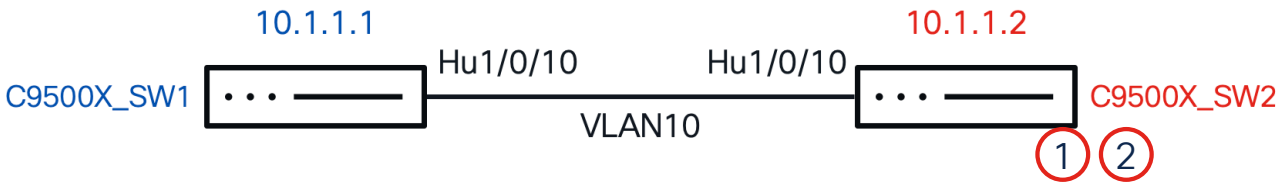
Problem Description



cisco Live!

Connectivity Issue

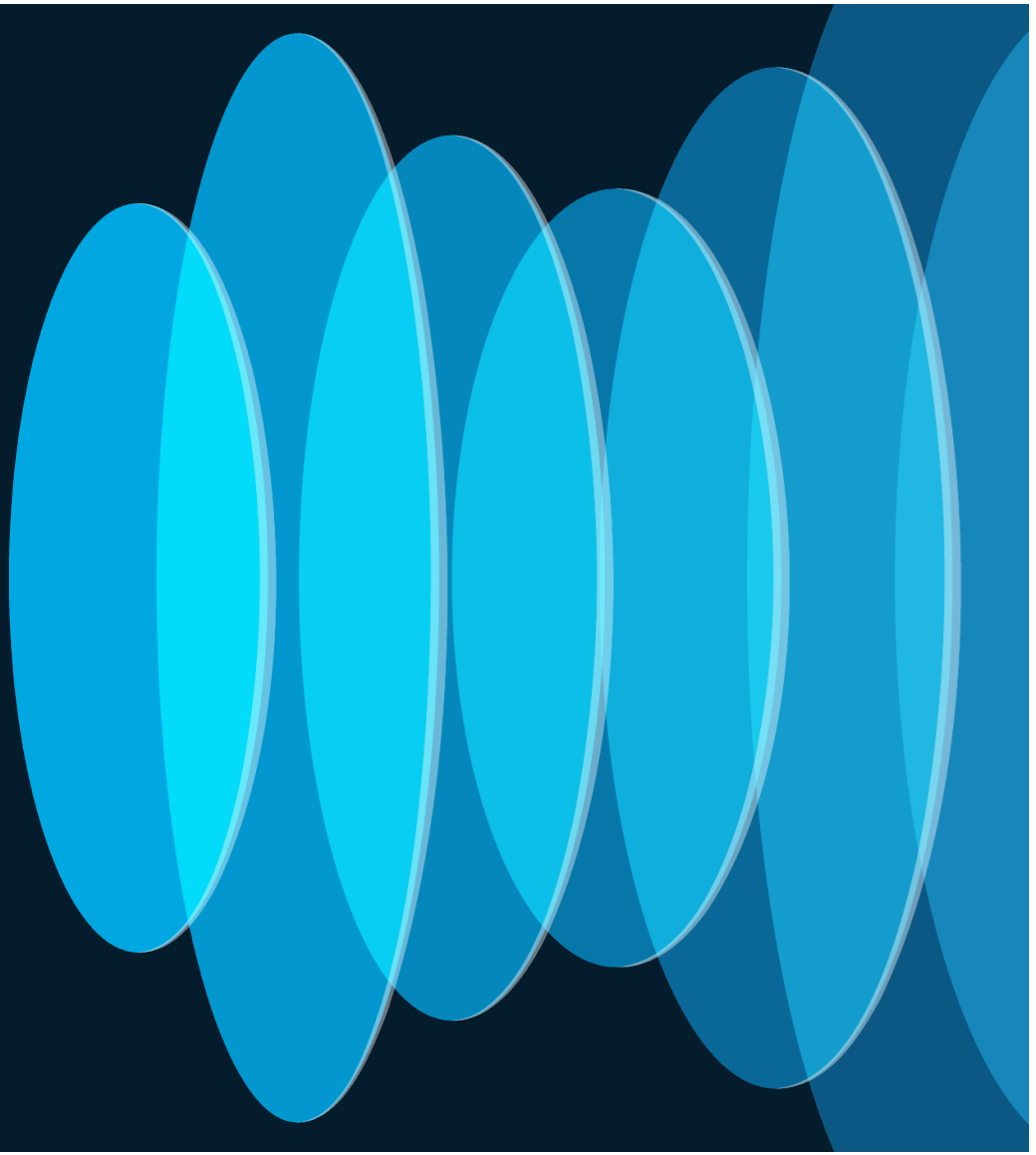
Two directly connected switches on the same subnet cannot communicate over vlan 10.



1
```
C9500X_SW2#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

2
```
C9500X_SW2#show ip arp vlan 10
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.1               0   Incomplete      ARPA
```

Troubleshooting Tools



cisco Live!

Inject Packet Capture

Start a packet capture from CPU to hardware.

1
```
C9500X_SW2#debug platform software fed active inject packet-capture start
Inject packet capturing started.
```

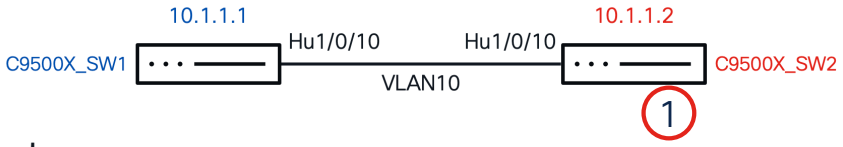
Test connectivity to switch one.

2
```
C9500X_SW2#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Stop the packet capture.

3
```
C9500X_SW2#debug platform software fed active inject packet-capture stop
Inject packet capturing stopped. Captured 40 packet(s)
```

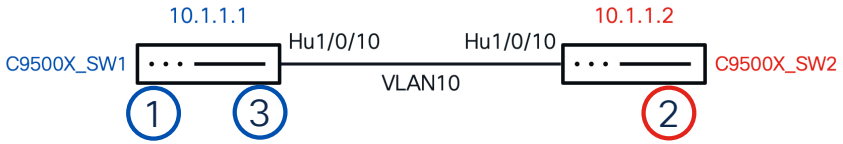
Inject Packet Capture



Look for ARP request on VLAN 10 in the packet capture.

1
```
C9500X_SW2#show platform software fed active inject packet-capture display-filter "arp"
brief
<snip>
------ Inject Packet Number: 7, Timestamp: 2024/05/03 00:42:26.717 ------
 interface : phy: Vlan10 [if-id: 0x000004a8], pal: Vlan10 [if-id: 0x000004a8]
 misc info : cause: 12 [ARP request or response], sub-cause: 0, linktype: LAYER2 [10]
 CE    hdr : dest mac: 4e41.5000.0111, src mac: 4e41.5000.0010, ethertype: 0X8100
 CE    hdr : vlan: 0x406, ethertype: 0x7103
 meta  hdr : Type: 0 (Inject Down), Encap: 0, Dest. Type: 0xc0
 meta  hdr : Dest. Value: 0xc, L3 DLP: 0, Down NH: 0, ethertype: 0x7103
 meta  hdr : Type: 0x22 (Inject Up(ETH)), SSP: 0xc
 ether hdr : dest mac: ffff.ffff.ffff, src mac: 748f.c21f.4d02
 ether hdr : q-in-q, out-vlan 4095, in-vlan: 11, ethertype: 0x9100
 arp   hdr : opcode: 1 (ARP Request), src mac: 748f.c21f.4d02 dest mac: 0000.0000.0000
 arp   hdr : src ip: 10.1.1.2, dest ip: 10.1.1.1
```

Punt Packet Capture



Start a packet capture from hardware to CPU.

1
```
C9500X_SW1#debug platform software fed active punt packet-capture start
Punt packet capturing started.
```

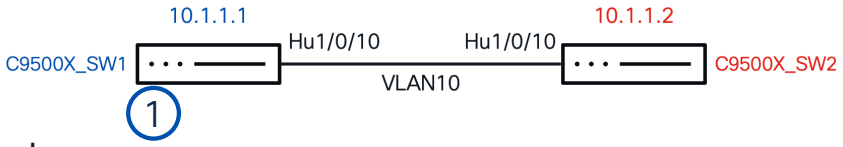
Test connectivity to switch one.

2
```
C9500X_SW2#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Stop the packet capture.

3
```
C9500X_SW1#debug platform software fed active punt packet-capture stop
Punt packet capturing stopped. Captured 4096 packet(s)
```

Punt Packet Capture



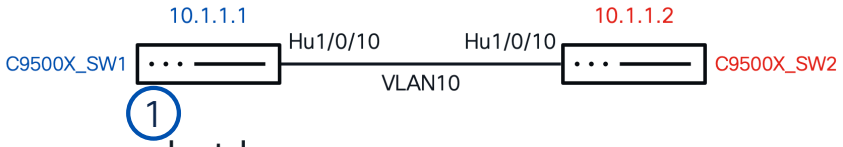
Look for ARP request on VLAN 10 in the packet capture.

1
```
C9500X_SW1#show platform software fed active punt packet-capture display-filter
"eth.src==748f.c21f.4d02" brief
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far :  4096 packet(s)
Capture capacity      :  4096 packet(s)
Max. Meta header size :    88 byte(s)
Max. Packet data size :   128 byte(s)

No packets matching display filter
```

Note: If packet is not captured in the FED PUNT debug, then that does not mean the expected traffic did not ingress the interface.

Rule out Interface Drops

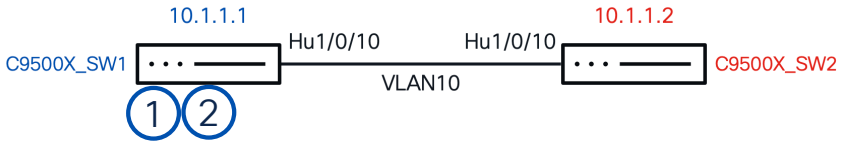


Input queue drops, Output drops, or Input errors cause packet loss.

1
```
C9500X_SW1#show interface Hu1/0/10 human-readable
<snip>
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  <snip>
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    <snip>
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Note: If no drops on interface level, then keep moving up the stack.

Punt ASIC Cause



Clear drop counters from the ASIC perspective.

1
```
C9500X_SW1#show platform software fed active punt asic-cause clear
```

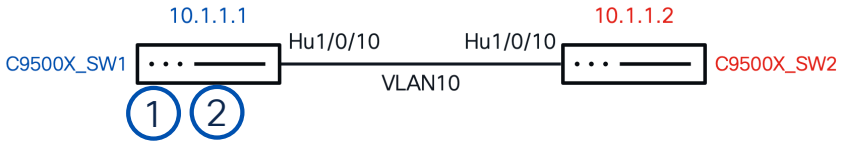
Display drop counters from the ASIC perspective.

2
```
C9500X_SW1#show platform software fed active punt asic-cause brief
<snip>

ASIC Cause Statistics Brief

+-------------------------------------------------------------------------------+
| Source |          Cause          |            Rx             |          Drop          |
|        |                         |     cur     |    delta    |     cur     |    delta    |
+-------------------------------------------------------------------------------+
   INMIR   ARP MIRROR                      1975        398138             0             0
   ITRAP   CISCO Protocols                    6          1408             0             0
```

Punt IOS Cause



Clear drop counters from the IOS perspective.

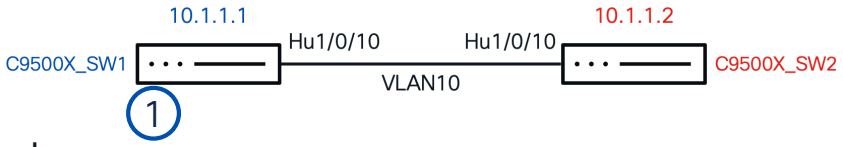
1
```
C9500X_SW1#show platform software fed active punt ios-cause clear
```

Display drop counters from the IOS perspective.

2
```
C9500X_SW1#show platform software fed active punt ios-cause brief
Statistics for all causes

Cause  Cause Info                          Rcvd                 Dropped
-------------------------------------------------------------------------
7      ARP request or response             3549                 0
96     Layer2 control protocols            12                   0
-------------------------------------------------------------------------
```

Punt Entries



Display drop counters in control plane policing per class map.

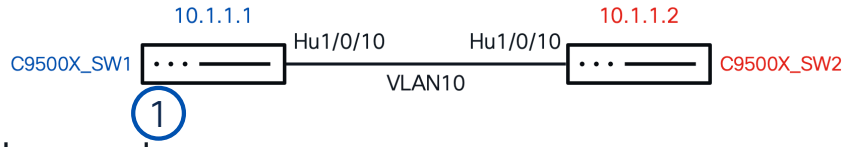
1

```
C9500X_SW1#show platform software fed active punt entries
<snip>
```

Source	Name	Pri	TC	Policy	CIR-SW	CIR-HW	Pkts(A)	Bytes(A)	Pkts(D)	Bytes(D)
MIRROR	ARP	4	4	system-cpp-police-arp	1000	965	7345	807950	33862	3724820
TRAP	CISCO Protocols	3	5	system-cpp-police-l2-control	16000	15449	25	3346	0	0
TRAP	DHCP Client(v4)	3	4	system-cpp-police-dhcp-v4	6000	5793	0	0	0	0
TRAP	DHCP Server(v4)	3	4	system-cpp-police-dhcp-v4	6000	5793	0	0	0	0
TRAP	DHCP Client(v6)	3	4	system-cpp-police-dhcp-v6	6000	5793	0	0	0	0
TRAP	DHCP Server(v6)	3	4	system-cpp-police-dhcp-v6	6000	5793	0	0	0	0
TRAP	ETH HOP-OPT	88	3	system-cpp-police-sw-forward	2000	1931	0	0	0	0
MIRROR	ISIS(L2)	3	5	system-cpp-police-isis	1000	965	0	0	0	0

Note: It is helpful to re-run the same command consecutively to check for incrementing drops.

Control Plane Policing

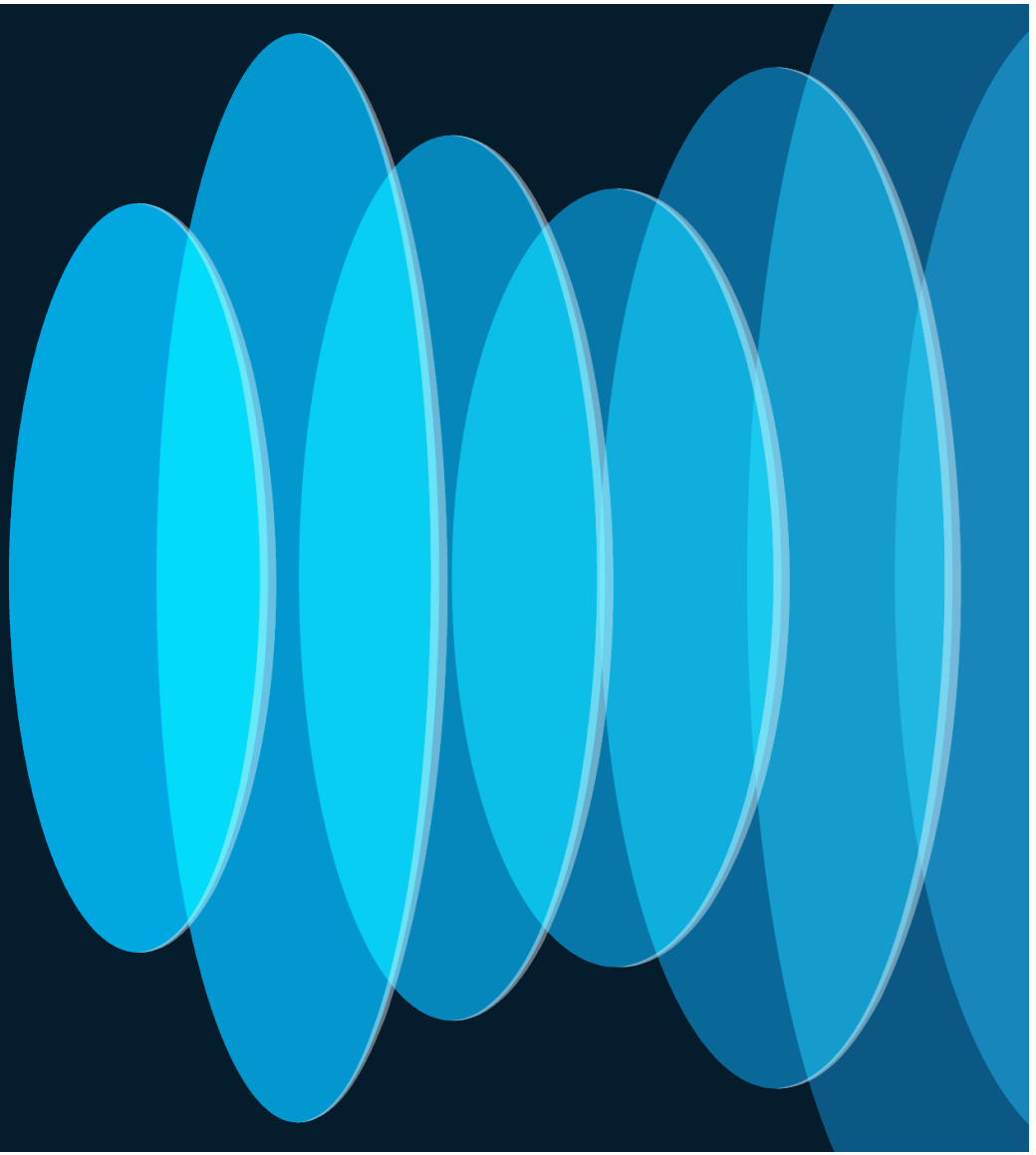


Display control plane policing rate limit and bytes dropped.

1
```
C9500X_SW1#show policy-map control-plane | section arp
    Class-map: system-cpp-police-arp (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: none
      police:
          rate 1000 pps, burst 11264 packets
        conformed 195214182 bytes; actions:
          transmit
        exceeded 855478258 bytes; actions:
          drop
```

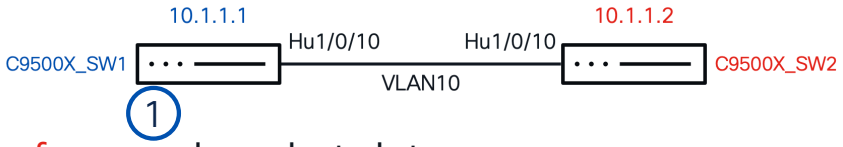
Note: It is helpful to re-run the same command consecutively to check for incrementing drops.

Packet Capture Analysis



cisco Live!

Punt packet capture brief

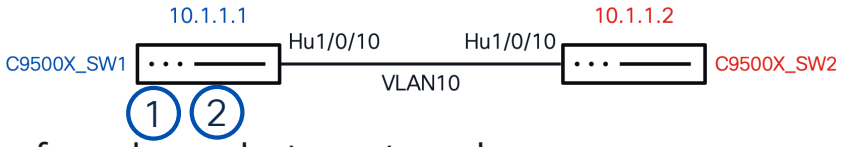


Use this command to get punt cause, incoming interface and packet data.

1
```
C9500X_SW1#show platform software fed active punt packet-capture brief
<snip>

------ Punt Packet Number: 1, Timestamp: 2024/05/04 22:16:19.614 ------
 interface : phy: Port11Vlan669 [if-id: 0x500000001029d], pal: Vlan669 [if-id:
0x000004a9]
 misc info : cause: 7 [ARP request or response], sub-cause: 1, linktype: IP [1]
 CE    hdr : dest mac: 4e41.5000.0010, src mac: 4e41.5000.0111, ethertype: 0x7102
 meta  hdr : Nxt. Hdr: 0x1, Fwd. Hdr: 0, SSP: 0x1b
 meta  hdr : DSP: 0xffff, SLP: 0x8002d, DLP: 0, ethertype: 0x773d
 ether hdr : dest mac: ffff.ffff.ffff, src mac: 0000.0300.0500
 ether hdr : vlan: 669, ethertype: 0x8100
 arp   hdr : opcode: 1 (ARP Request), src mac: 0000.0300.0500 dest mac: 0000.0000.0000
 arp   hdr : src ip: 172.16.20.20, dest ip: 172.16.20.254
```

Punt packet capture detail



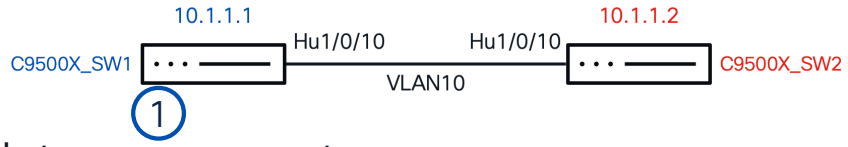
This command adds a hexadecimal representation of each packet captured.

1
```
C9500X_SW1#show platform software fed active punt packet-capture detailed
------ Punt Packet Number: 1, Timestamp: 2024/05/04 22:16:19.614 ------
<snip>
 Packet Data Hex-Dump (captured packet length: 64 bytes) :
 FFFFFFFFFFFF0000  030005008100029D  0806000108000604  0001000003000500
 AC10141400000000  0000AC1014FE0001  0203040506070809  0A0B0C0D0E0F1011
```

Use this command to store the packet capture in a text file.

2
```
C9500X_SW1#show platform software fed active punt packet-capture detailed | redirect
flash:punt.txt
```

Wireshark conversion



1. Export the packet capture from the switch's flash to your computer.

```
1 C9500X_SW1#copy flash:punt.txt tftp://192.168.1.1 vrf example
Address or name of remote host [192.168.1.1]?
Destination filename [punt.txt]?
!!!
7017109 bytes copied in 44.396 secs (158057 bytes/sec)
```

2. Edit the packet capture to match this format.

```
Traffic direction + Timestamp + Hexdump

< 2024/05/04 22:16:19.614 FFFFFFFFFFFF000003000500810002 9D080600010800060400010000030...
```

Blank space is used as field delimiter.
Packets are separated by new line character.
< represents punt.
> represents inject.

Simplified packet capture

The packet capture must look like this after editing.

```
< 2024/05/04 22:16:19.614 FFFFFFFFFFFF000003000500810002 9D080600010800060400010000030005
< 2024/05/04 22:16:19.615 FFFFFFFFFFFF000003000500810002 9D080600010800060400010000030005
< 2024/05/04 22:16:19.615 FFFFFFFFFFFF000003000500810002 9D080600010800060400010000030005
< 2024/05/04 22:16:19.615 FFFFFFFFFFFF000003000500810002 9D080600010800060400010000030005
< 2024/05/04 22:16:19.615 FFFFFFFFFFFF000003000500810002 9D080600010800060400010000030005
```

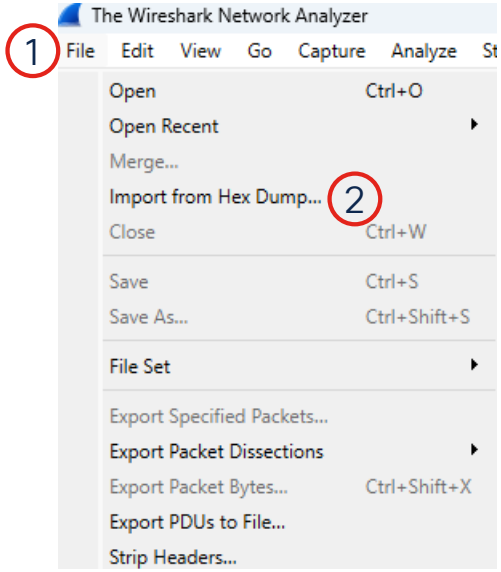
Note: output has been cropped horizontally to fit the slide.

This regular expression matches the packet capture format.

```
^(?<dir>[<>])\s(?<time>\d{4}\/\d{2}\/\d{2}\s\d{2}:\d{2}:\d{2}.\d{3})\s(?<data>[0-9A-F]+)$
```

Import to Wireshark

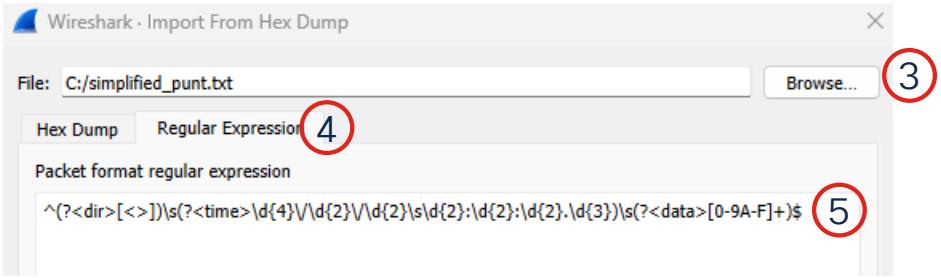
0. **Open** Wireshark.
1. **Click** file.
2. **Select** Import from Hex Dump.



3. **Click** browse to select the packet capture.
4. **Select** Regular Expression.
5. **Copy and paste** this regular expression.

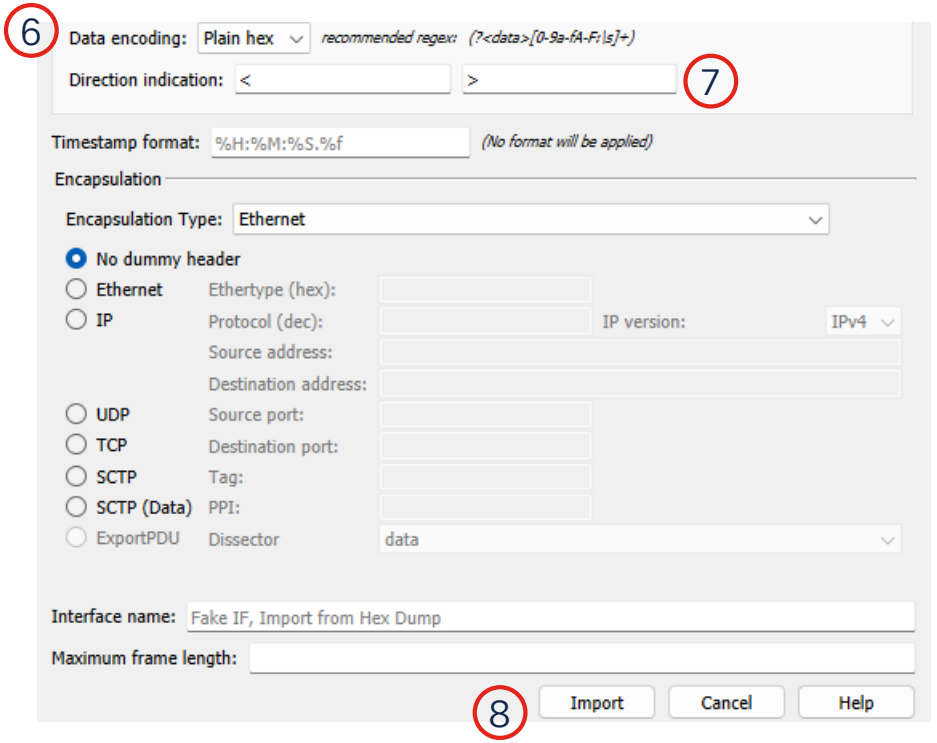
```
^(?<dir>[<>])\s(?<time>\d{4}\/\d{2}\/\d{2}\s\d{2}:\d{2}:\d{2}.\d{3})\s(?<data>[0-9A-F]+)$
```

Ensure there are not any blank spaces at the end of the line.



Import to Wireshark

6. **Select** Plain hex.
7. **Configure** traffic direction symbols.
8. **Click** Import.



Results

- There is a top talker in VLAN669 overwhelming the control plane.
- Hundreds of ARP packets are received in less than one second.

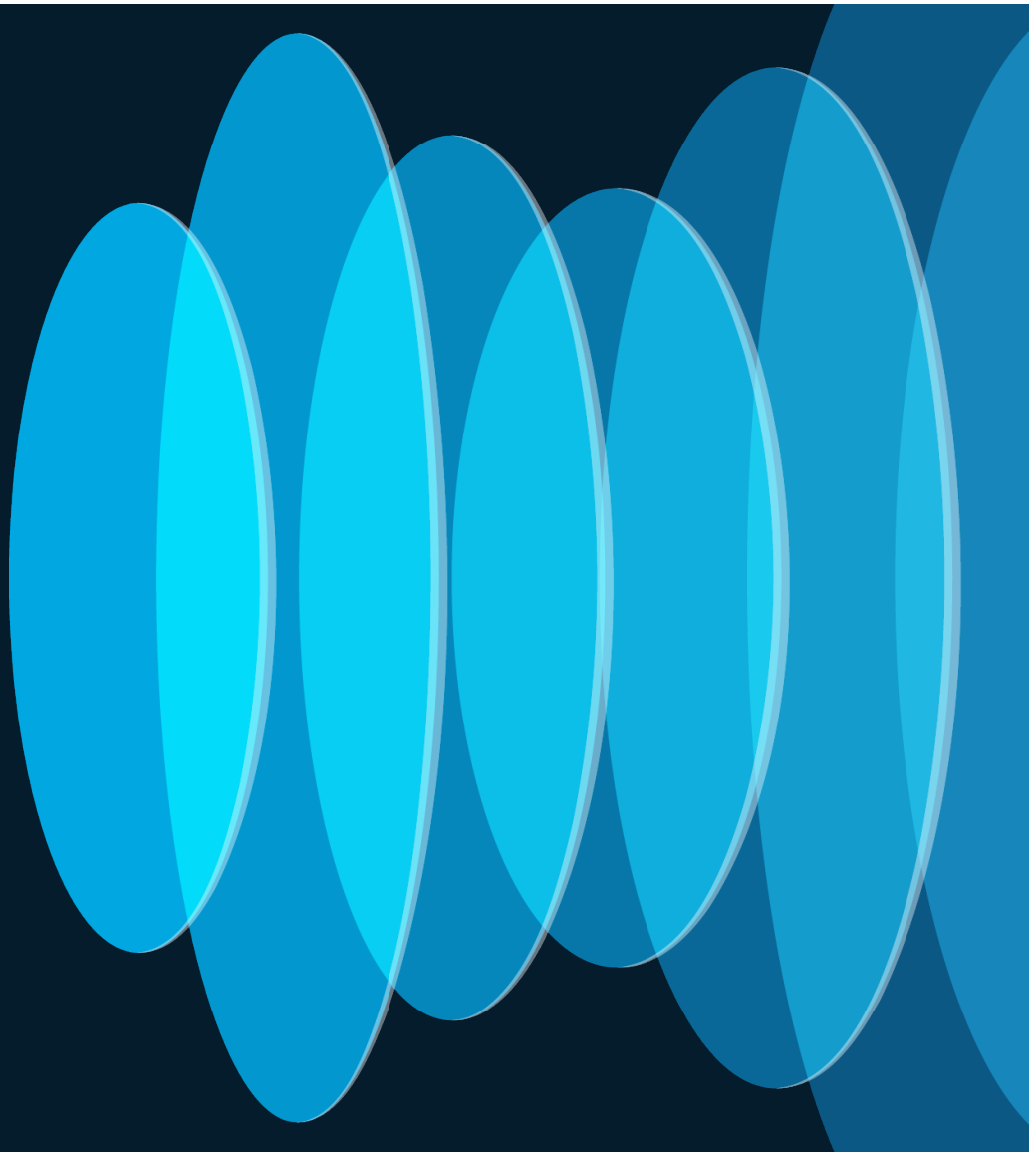
Apply a display filter ... <Ctrl-/>

No.	Time	Source Address	Destination	Info
1	2024-05-16 02:29:29.000001000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20
2	2024-05-16 02:29:29.000002000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20
3	2024-05-16 02:29:29.000003000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20
4	2024-05-16 02:29:29.000004000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20
5	2024-05-16 02:29:29.000005000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20
6	2024-05-16 02:29:29.000006000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20
7	2024-05-16 02:29:29.000007000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20
8	2024-05-16 02:29:29.000008000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20
9	2024-05-16 02:29:29.000009000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20
10	2024-05-16 02:29:29.000010000	00:00:03:00:05:00	ff:ff:ff:ff:ff:ff	Who has 172.16.20.254? Tell 172.16.20.20

```
> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on
> Ethernet II, Src: 00:00:03:00:05:00, Dst: ff:ff:ff:ff:ff:ff
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 669
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 00  03 00 05 00 81 00 02 9d
0010  08 06 00 01 08 00 06 04  00 01 00 00 03 00 05 00
0020  ac 10 14 14 00 00 00 00  00 00 ac 10 14 fe 00 01
0030  02 03 04 05 06 07 08 09  0a 0b 0c 0d 0e 0f 10 11
```

Root Cause & Resolution

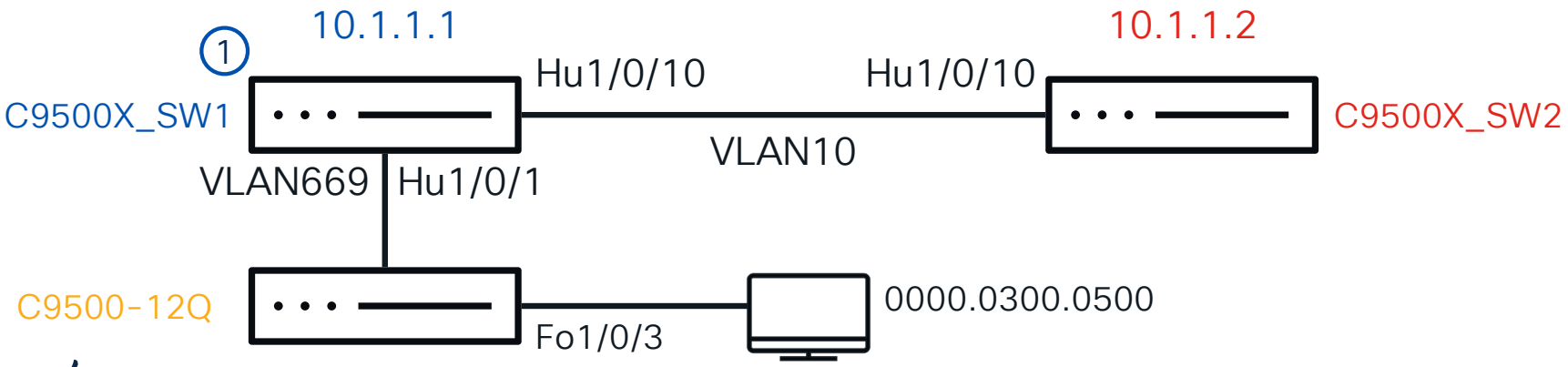


cisco Live!

Locate top offender device

You can look up the source MAC address to determine what interface connects to that host.

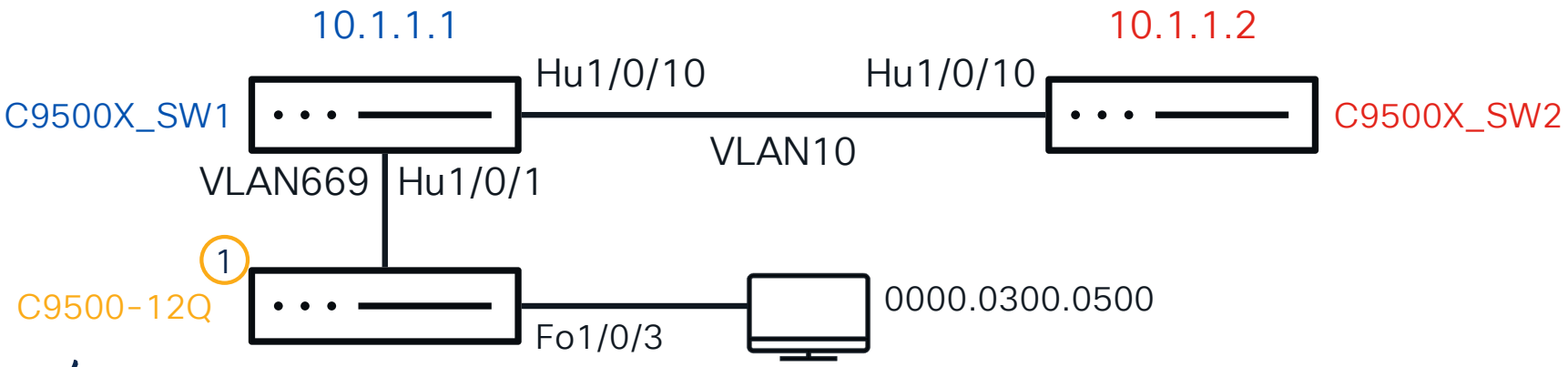
```
1 C9500X_SW1#show mac address-table address 00:00:03:00:05:00
<snip>
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 669    0000.0300.0500    DYNAMIC     Hu1/0/1
Total Mac Addresses for this criterion: 1
```



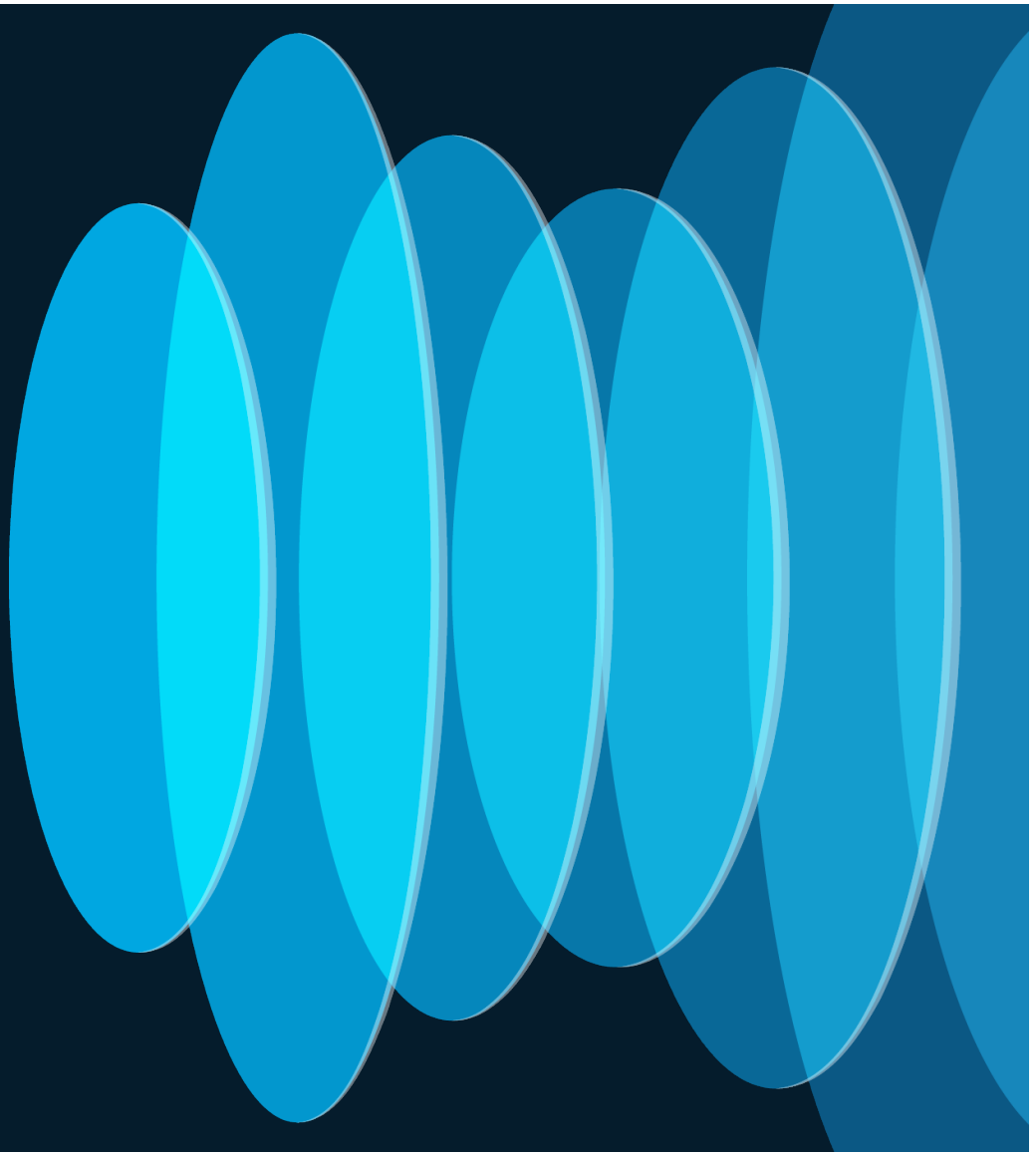
Storm control

You can configure storm control at the access layer ports to prevent similar issues.

```
1 C9500-12Q(config)#int fo1/0/3
  C9500-12Q(config-if)#storm-control broadcast level pps 100
  C9500-12Q(config-if)#storm-control action shutdown
  C9500-12Q(config-if)#end
  *May 16 03:14:50.931: %PM-4-ERR_DISABLE: storm-control error detected on Fo1/0/3,
  putting Fo1/0/3 in err-disable state
```

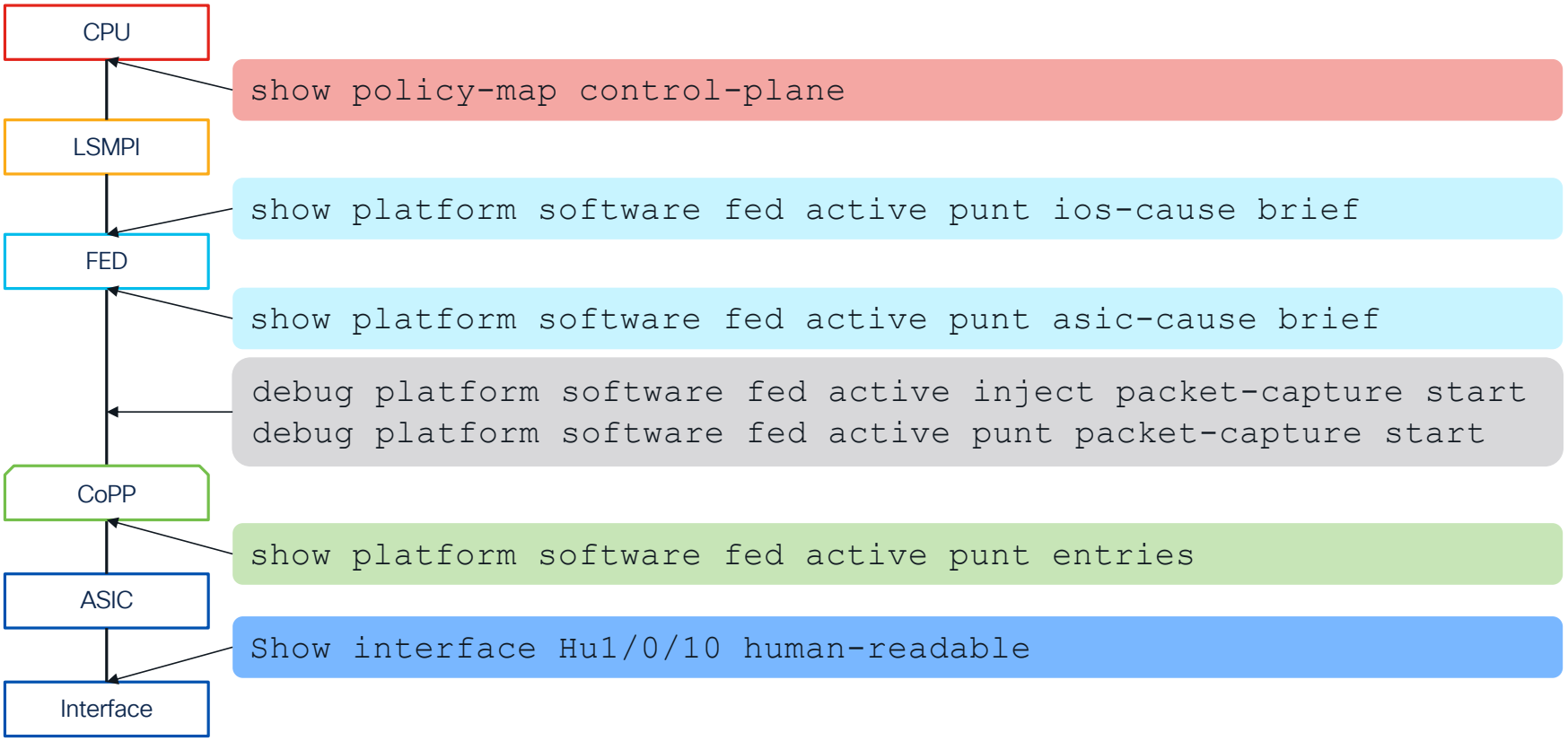


Conclusion



cisco Live!

Troubleshooting Layers



Additional Resources

Troubleshoot Control Plane Operations on Catalyst 9000 Switches
https://www.cisco.com/c/en/us/support/docs/switches/catalyst-9300-switch/221841-troubleshoot-control-plane-operations-on.html

Configure FED CPU Packet Capture on Catalyst 9000 Switches
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-gibraltar-16121/216746-configure-punt-inject-fed-packet-capture.html

Security Configuration Guide, Cisco IOS XE 17.14.X (Catalyst 9500 Switches)
Configure CoPP
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-14/configuration_guide/sec/b_1714_sec_9500_cg/configuring_control_plane_policing.html

Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9500 Switches)
Configure Storm Control
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-9/configuration_guide/sec/b_179_sec_9500_cg/configuring_port_based_traffic_control.html

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

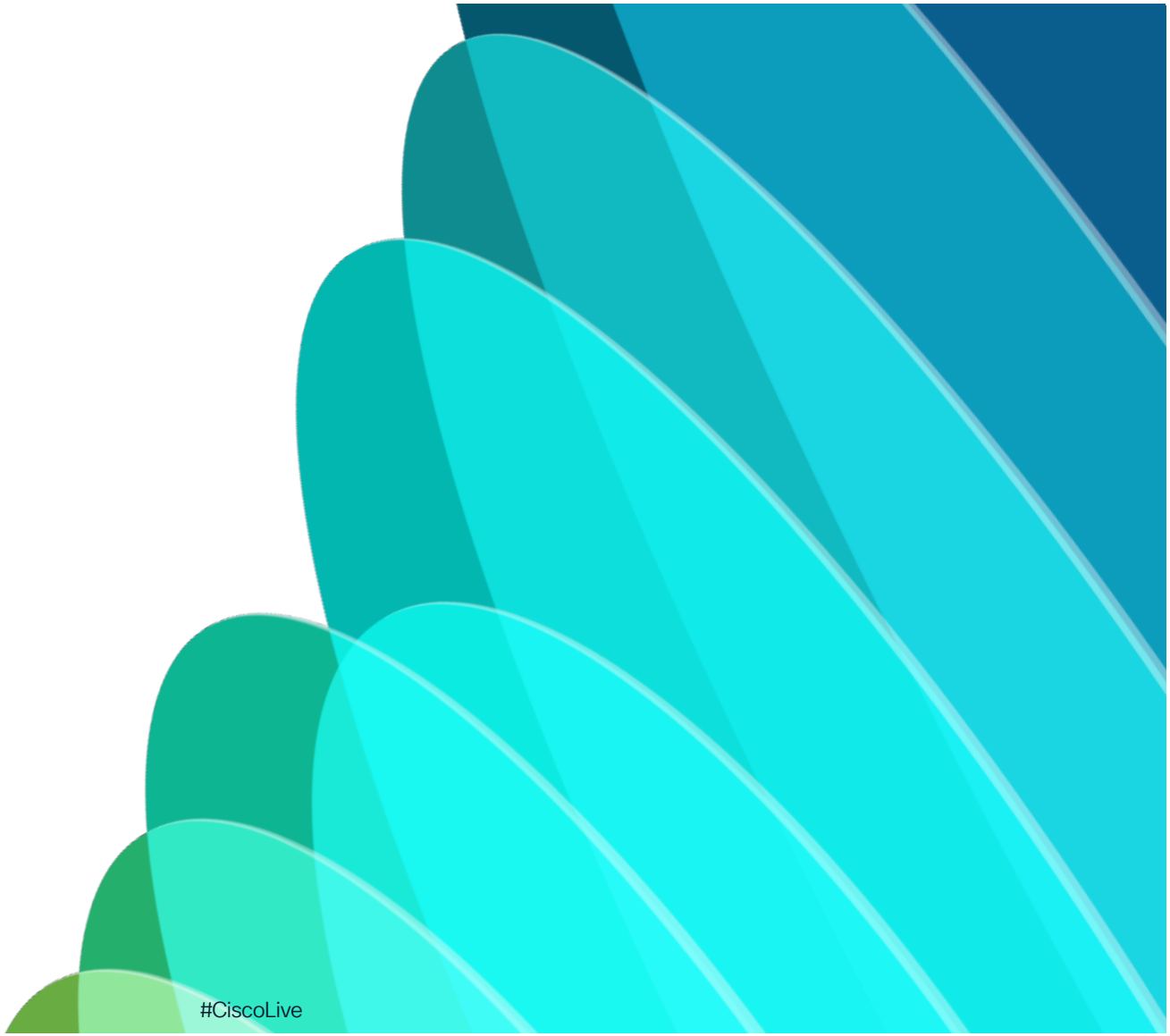
Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand
- Capturing Tools for Cat9k Troubleshooting: Case Studies TACENT-2016 Monday, Jun 3 2:30 pm - 3:00 pm PDT

The bridge to possible

Thank you



#CiscoLive