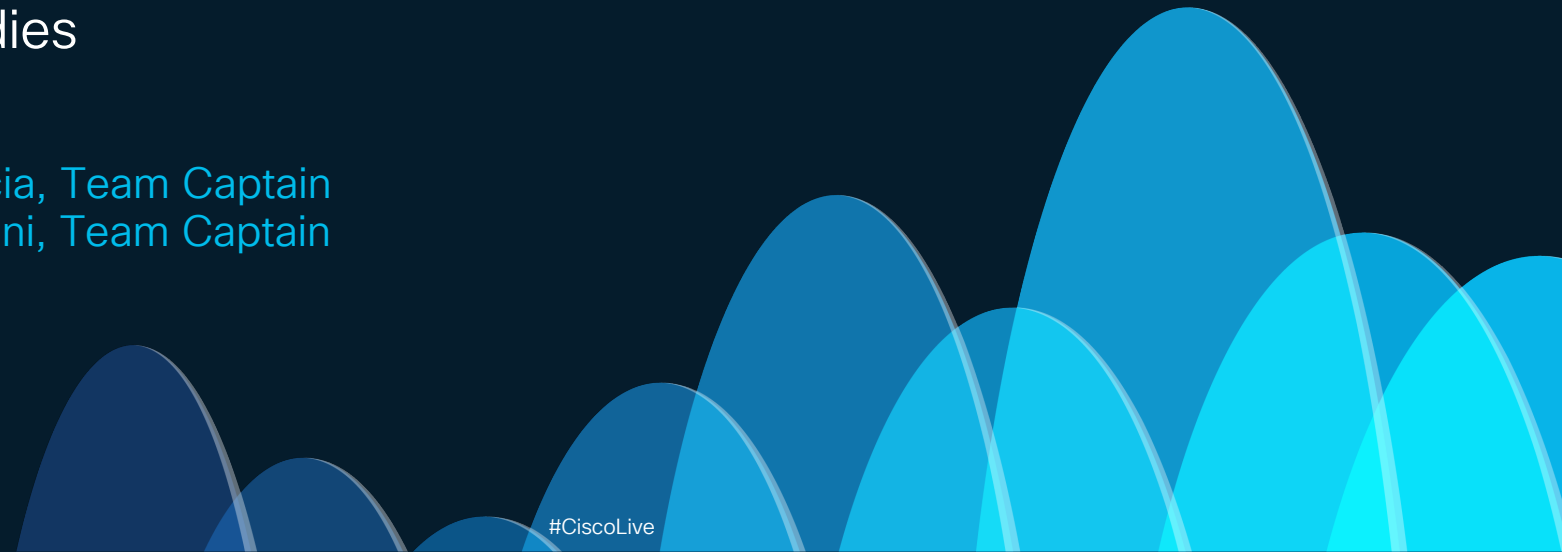
The bridge to possible

Capturing Tools for Cat9k Troubleshooting

Case Studies

Patricia Garcia, Team Captain
Carlos Bustani, Team Captain

TACENT-2016



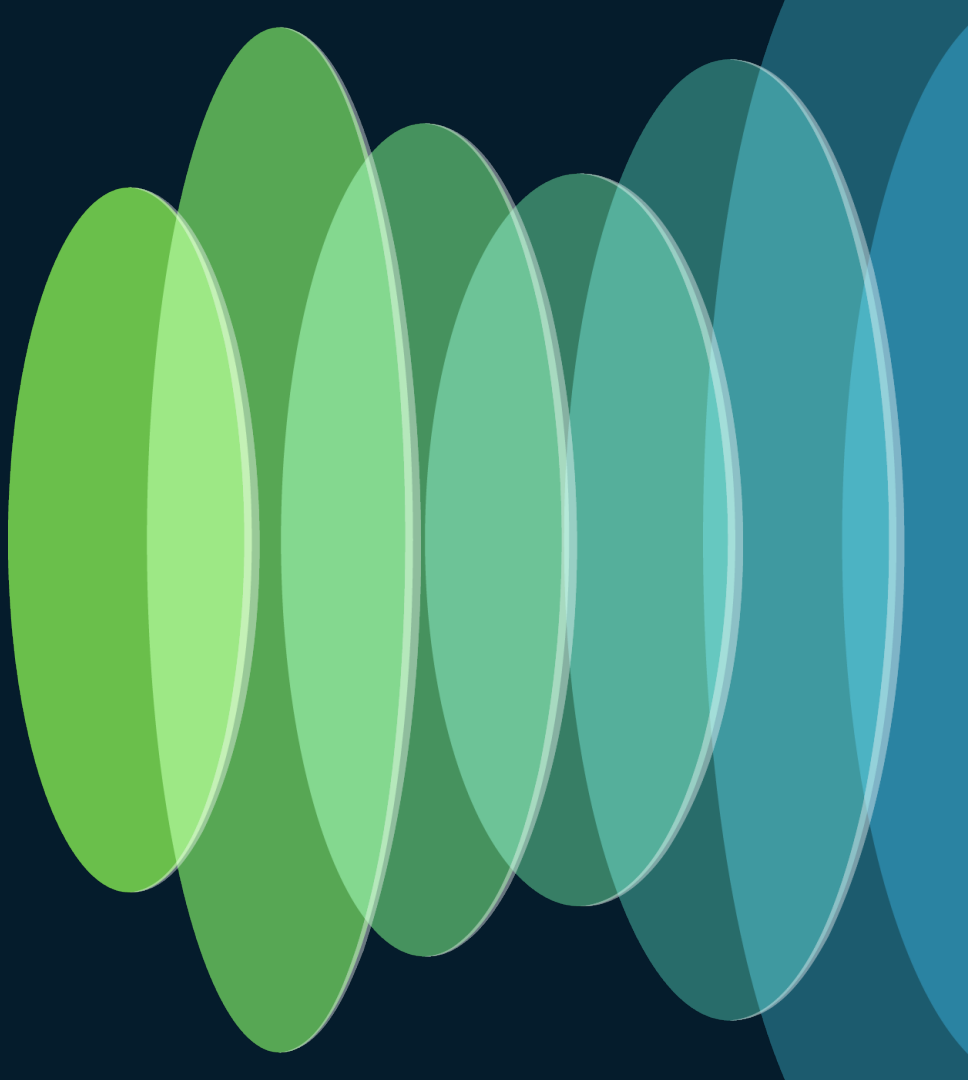
cisco Live!

#CiscoLive

Agenda

- Capturing Tools
  - SPAN
  - EPC
- Case Studies
  - Slowness
  - DHCP issues
- Conclusion

Capturing Tools

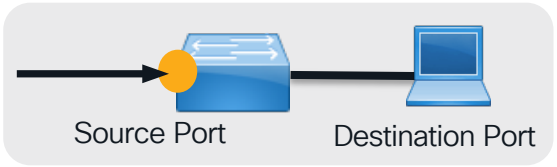


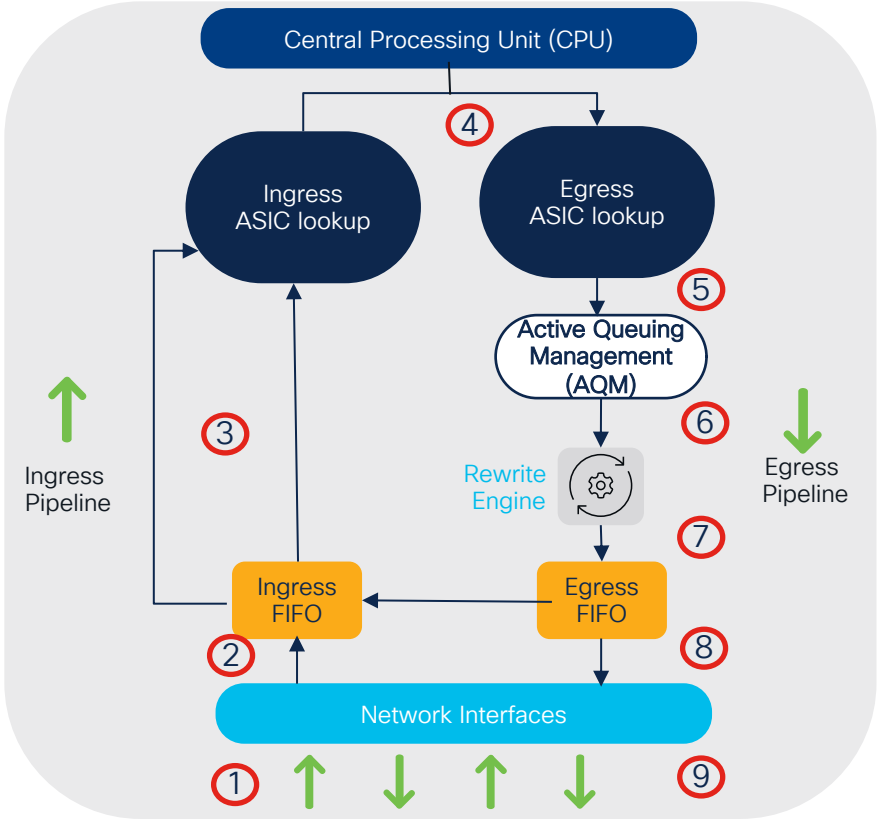
Switched Port Analyzer (SPAN)

What is it?	· Is a monitoring tool that mirrors traffic from a source port or VLAN to a destination port.
How does it work?	· SPAN configures a destination index port to direct the traffic towards the mirrored port.
What restrictions does it have?	· SPAN sessions capture only DHCP ingress packets when DHCP snooping is enabled on the device. · EPC does not capture egress packets when egress span is active. · SPAN doesn't disrupt device function, but oversubscribed destination can lose packets. · A maximum of 8 source sessions can be configured.
What platforms support it?	· Cisco IOS-XE.

Switched Port Analyzer (SPAN)

How does it work?





Switched Port Analyzer (SPAN)

Configuration

1

```
Switch(config)# monitor session 1 source interface {interface-id | vlan}[rx|tx|both]
Switch(config)# monitor session 1 destination interface {interface-id}
                [encapsulation replicate]
Switch(config)# monitor session 1 filter {ip|ipv6|mac|vlan}
```

Verification

2

```
Switch#show monitor session 1
Session 1
---------
Type                          : Local Session
Source Ports                  :
    Both                      : Te1/0/48
Destination Ports             : Te1/0/47
    Encapsulation             : Native
          Ingress             : Disabled
IP Access-group               : test
```

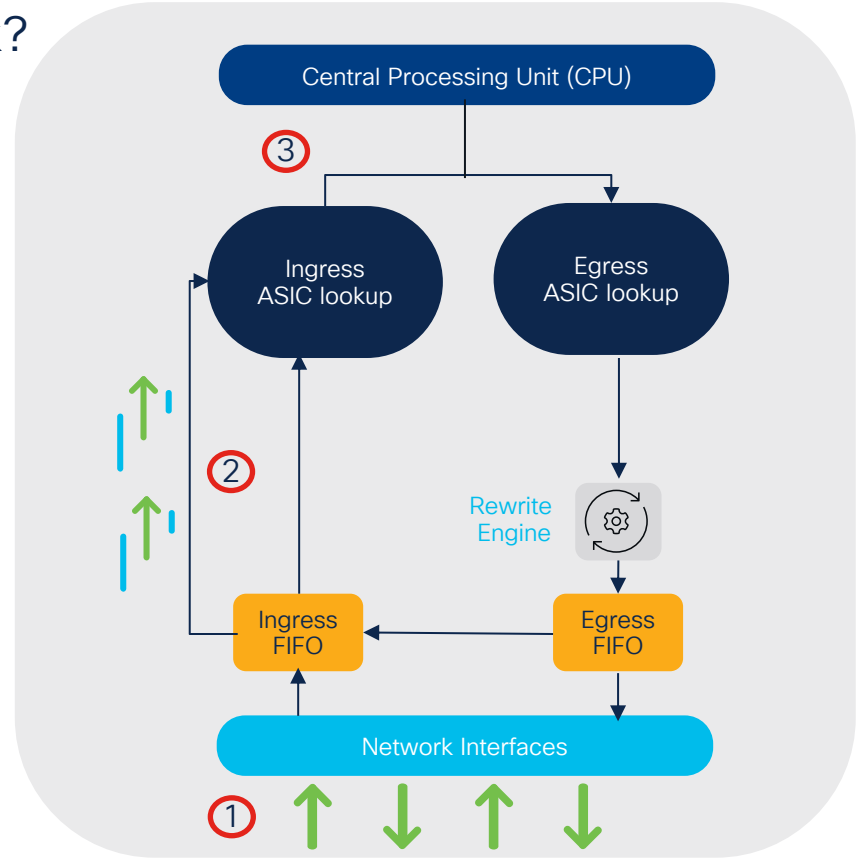
```
Switch#show platform software monitor session 1
Span Session 1 (FED Session 0):
  Type:       Local SPAN
  Prev type: Local SPAN
  Ingress Src Ports: Te1/0/48
  Egress Src Ports:  Te1/0/48
  Destination Ports:  Te1/0/47
  Ingress Src Vlans:
  Egress Src Vlans:
  IP FSPAN ACL: test
<snip>
```

Embedded Packet Capture (EPC)

What is it?	· Built-in feature for data or control plane packets. · Facilitates troubleshooting.
How does it work?	· Traffic is copied and punted to CPU. · On box analysis. · Export to PCAP.
What restrictions does it have?	· No EtherChannels · TX does not reflect rewrite changes. · Some CPU-injected packets not seen. · 8 captures supported, only 1 active. · Limit to 1000 packets per second.
What platforms support it?	· Cisco IOS-XE.

Embedded Packet Capture (EPC)

How does it work?



Embedded Packet Capture (EPC)

Configuration

1

switch# **monitor capture** {*name*} **interface** {*interface-id* } {in | out | both} | **control-plane** {in | out | both}
switch# **monitor capture** {*name*} **buffer** [circular] **size** {size}

Privileged exec mode

Filters

2

switch# **monitor capture** {*name*} **match** {any}
or
switch# **monitor capture** {name} **access-list** {acl-name}

IPv4
IPv6
MAC

ip access-list extended
ACL1
10 permit icmp any any
20 permit udp any any

3

switch# **monitor capture** {*name*} **start**
switch# **monitor capture** {*name*} **stop**

Embedded Packet Capture (EPC)

Verification

show monitor capture {name}
show monitor capture {name} **parameter**

```
switch# show monitor capture CAP parameter
      monitor capture CAP interface GigE1/0/1 BOTH
      monitor capture CAP match any
      monitor capture CAP buffer size 100
```

Display

show monitor capture {name} **buffer brief**
show monitor capture {name} **buffer detail**
show monitor capture {name} **buffer display-filter** {"wireshark-filter"} **brief**

monitor capture {name} **export file location** flash:cap.pcap

show monitor capture file flash:cap.pcap **brief**
show monitor capture file flash:cap.pcap **detail**
show monitor capture file flash:cap.pcap **display-filter** {"wireshark-filter"} **brief**

Embedded Packet Capture (EPC)

Display examples

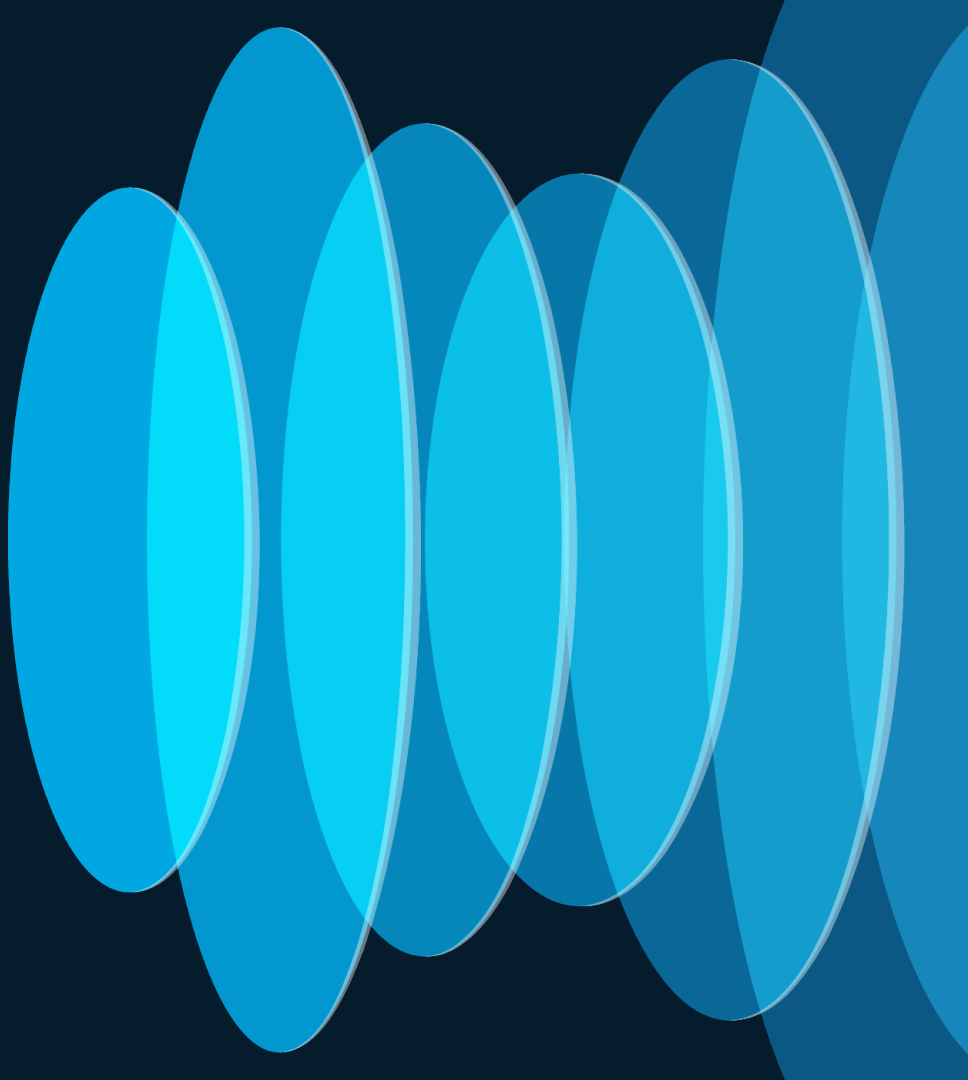
```
switch# show monitor capture CAP buffer brief

    1   0.000000 78:02:b1:07:bf:05 -> 01:00:0c:cc:cc:cc DTP 60 Dynamic Trunk Protocol
    2   0.636135  192.168.0.1 -> 255.255.255.255 DHCP 368 DHCP Discover
    3   7.658671 4c:5d:3c:bf:03:25 -> 4c:5d:3c:bf:03:25 LOOP 60 Reply
```

```
switch# show monitor capture cap buffer detail

    Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
<snippet>
    Arrival Time: May 14, 2024 18:19:08.087844000 UTC
<snippet>
     Frame Length: 60 bytes (480 bits)
    [Protocols in frame: eth:llc:dtp]
IEEE 802.3 Ethernet
    Destination: 01:00:0c:cc:cc:cc (01:00:0c:cc:cc:cc)
    Source: 4c:5d:3c:bf:03:25 (4c:5d:3c:bf:03:25)
<snippet>
```

Case Study 1: Slowness



Problem Statement

Isolate the problem

Site 1:

User A at site 1 experience slow file transfers over Ethernet.
Downloading a 10 GB file required 15 minutes, compared to 7 minutes at other sites.

Troubleshooting

Resources

Network

- ✓ Application
- ✓ Presentation
- ✓ Session
- ✓ Transport
- ✓ Network
- ✓ Data Link
- ✓ Physical

What capture do I select?

Embedded Packet Capture (EPC) **vs** Switched port Analyzer (SPAN)

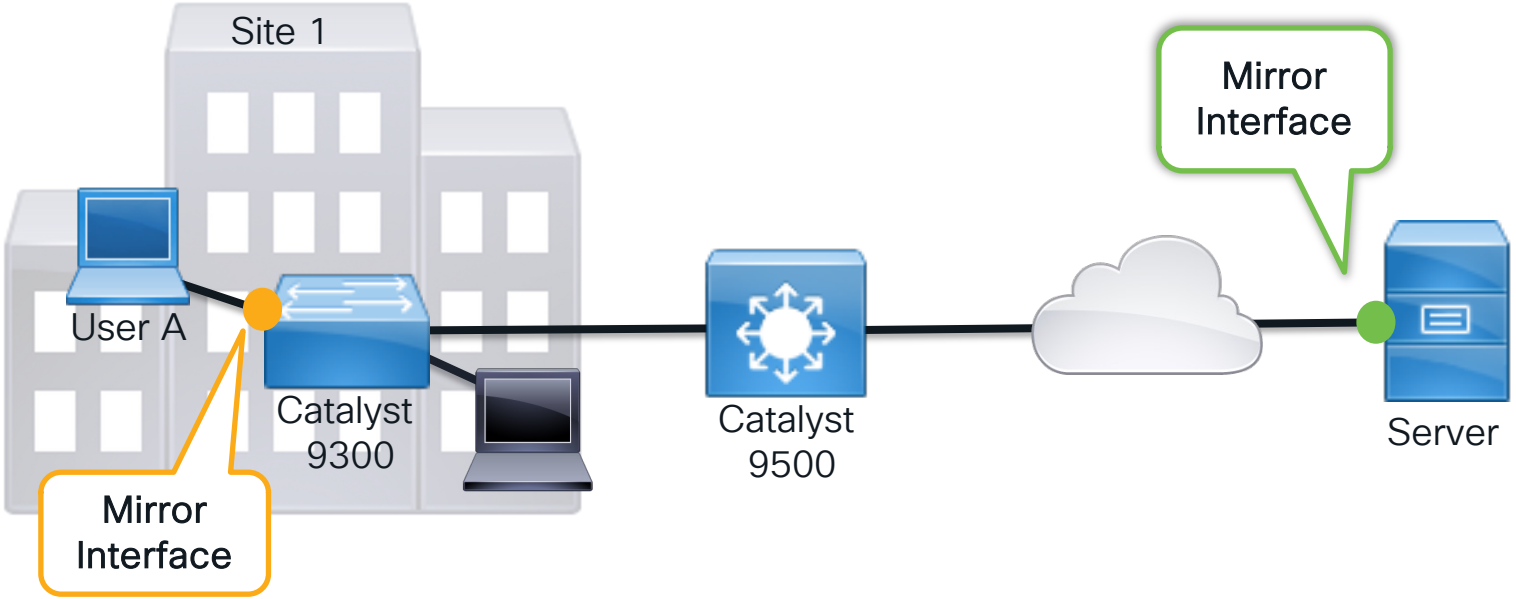
Rate limit

Restrictions

Benefits

Capture Configuration: Where and How?

Symptoms observed → Define the Problem → Possible causes → Data gathering → Analysis → Identify cause → Verify and fix



Common Issues

What is next?

- ✓ Connection Establishment Three-Way Handshake
- Congestion Control
- Flow Control

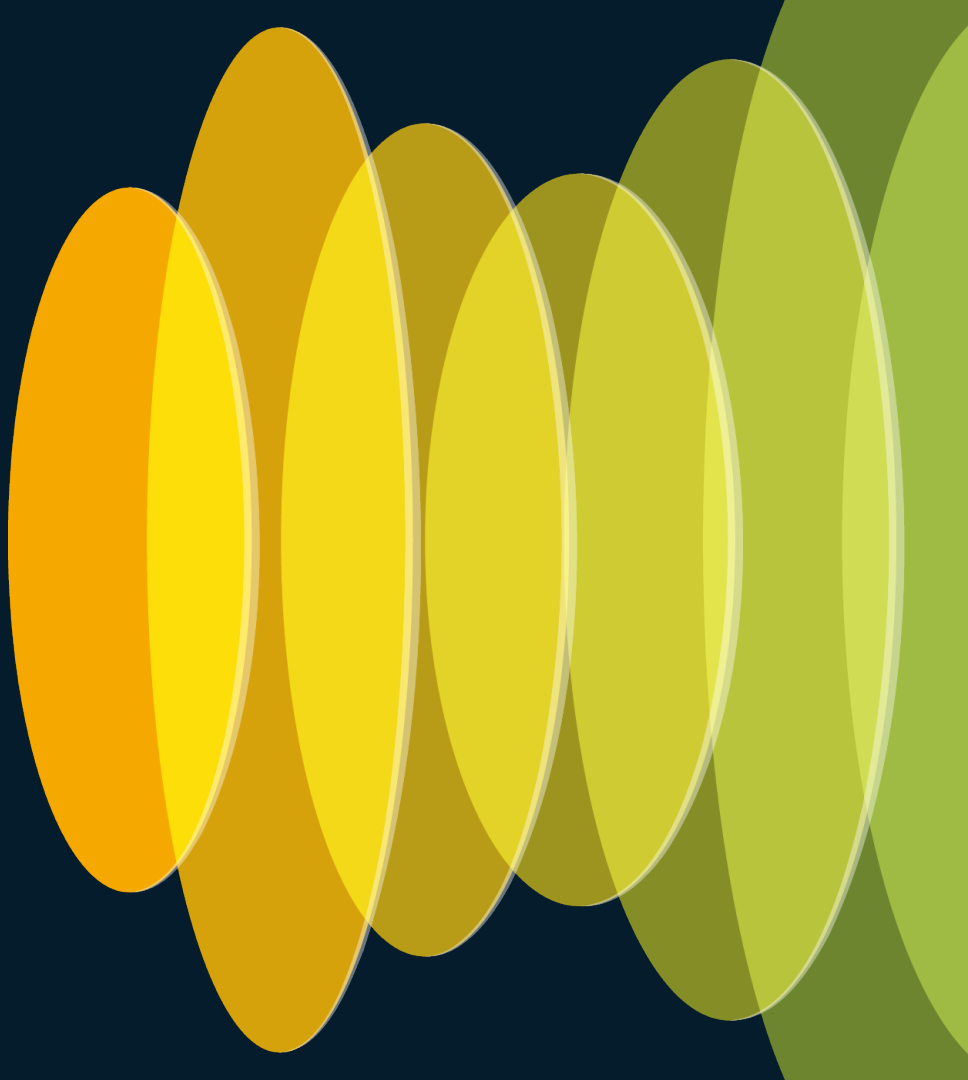
Non-Working

```
[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM
[ACK] Seq=1 Ack=1 Win=262656 Len=0
```

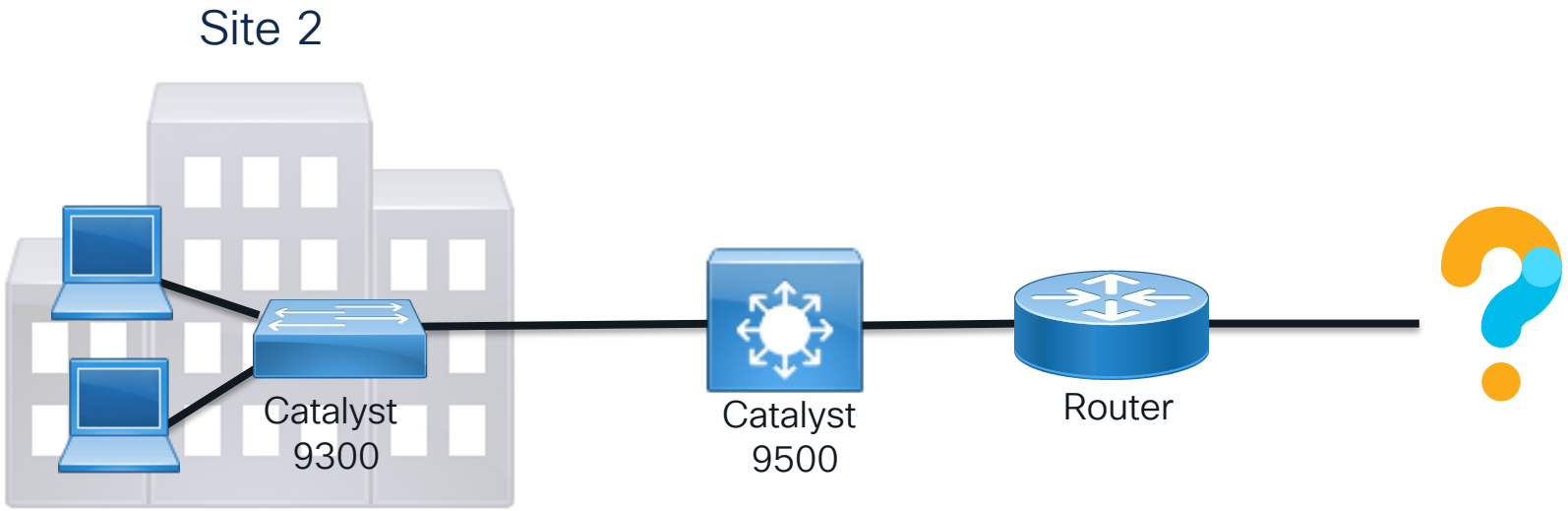
Working

```
[SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1781208375 TSecr=0
[SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM TSval
[ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=1781208423 TSecr=512401
```

Case Study 2: DHCP issues

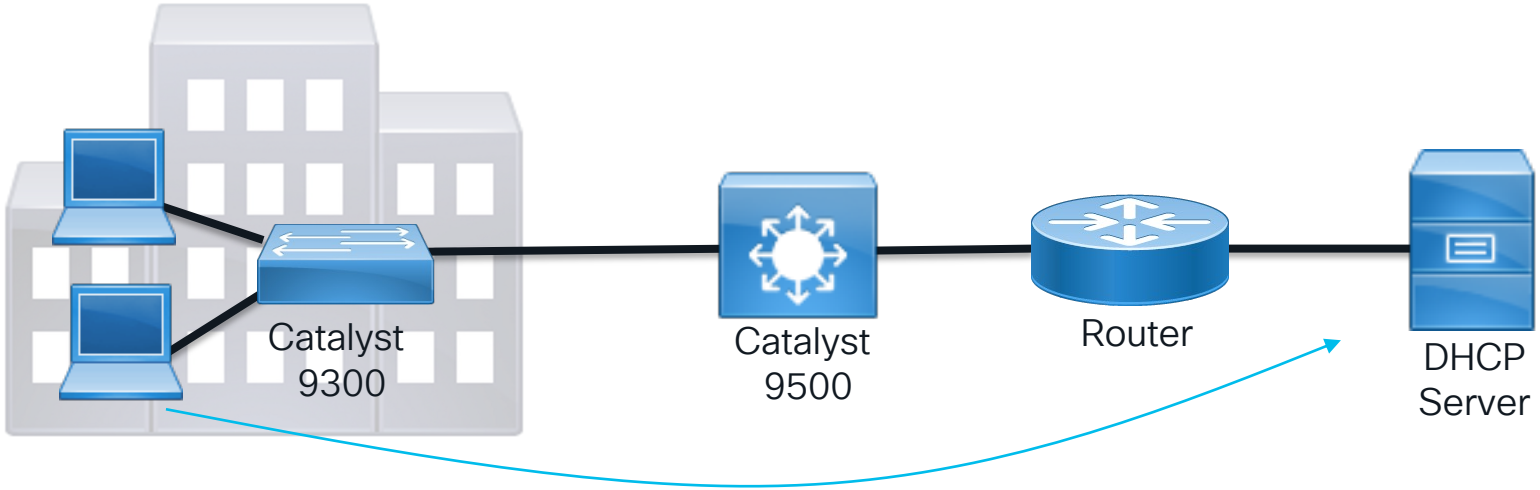


Problem statement



Problem statement

Users at the office are taking around 10 minutes to get an ip address. (it has been working fine for years).



Network Health Check

- ✓ DHCP Server Overload or Malfunction
- ✓ Physical connectivity
- ✓ End user issues

What capture do I select?

Embedded Packet Capture (EPC) **vs** Switched Port Analyzer (SPAN)

Benefits

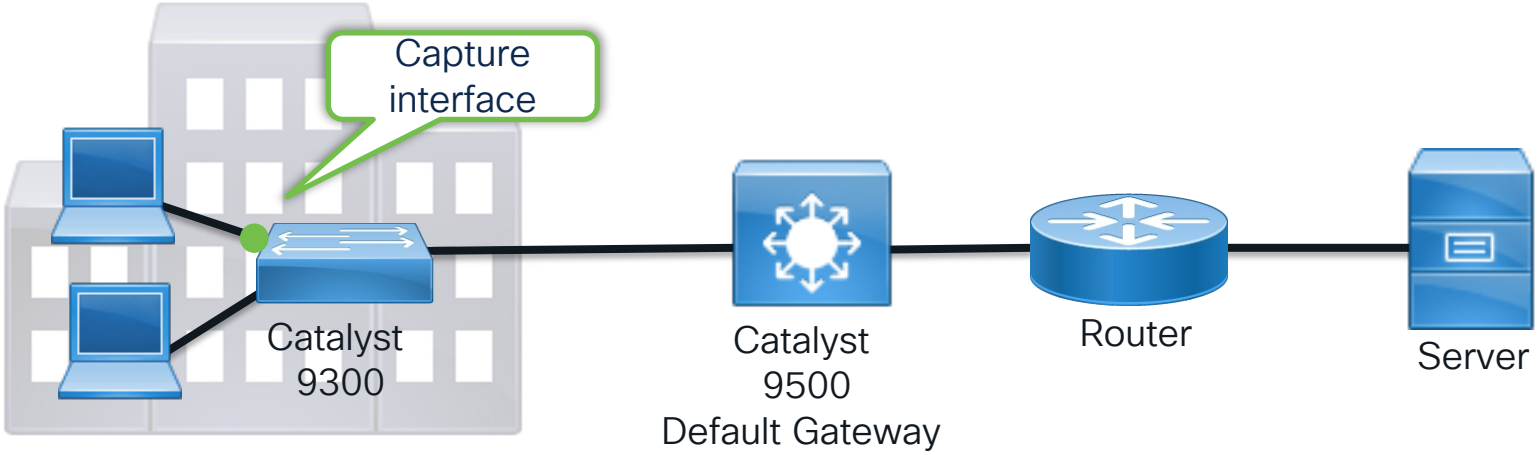
CPU captures

No need to have physical access

Restrictions

1000 packets per second

Configuring Embedded Packet Capture




```
9300_access#monitor capture Port1 interface g1/0/1 both
9300_access#monitor capture Port1 access-list ACL1
9300_access#monitor capture Port1 buffer size 100
9300_access#monitor capture Port1 start
```

ACL for filtering DHCP packets

Displaying Embedded Packet Capture

```
9300_access#show monitor capture Port1 buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

    1   0.000000      0.0.0.0 -> 255.255.255.255 DHCP 362 DHCP Discover - Transaction ID 0x11d9
    2   3.284655      0.0.0.0 -> 255.255.255.255 DHCP 362 DHCP Discover - Transaction ID 0x11d9
    3  15.368499      0.0.0.0 -> 255.255.255.255 DHCP 362 DHCP Discover - Transaction ID 0xb9c
    4  19.285600      0.0.0.0 -> 255.255.255.255 DHCP 362 DHCP Discover - Transaction ID 0xb9c
```

```
9300_access#show monitor capture Port1 buffer detail
      Ethernet II, Src: 9c:54:16:b7:ff:46 (9c:54:16:b7:ff:46), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
      802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
          000. .... .... .... = Priority: Best Effort (default) (0)
          ...0 .... .... .... = DEI: Ineligible
          .... 0000 0000 1010 = ID: 10
      Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
      Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      User Datagram Protocol, Src Port: 68, Dst Port: 67
      Dynamic Host Configuration Protocol (Discover)
      Bootp flags: 0x8000, Broadcast flag (Broadcast)
      Client IP address: 0.0.0.0
          Your (client) IP address: 0.0.0.0
      Client MAC address: 9c:54:16:b7:ff:46 (9c:54:16:b7:ff:46)
```

Displaying Embedded Packet Capture

```
9300_access#monitor capture Port1 export location flash:9500Port1.pcap
Export Started Successfully

9300_access#copy flash:9500Port1.pcap tftp:
Address or name of remote host []? 192.168.0.1
Destination filename [9500Port1.pcap]?
!!
2648 bytes copied in 1.009 secs (2624 bytes/sec)
```

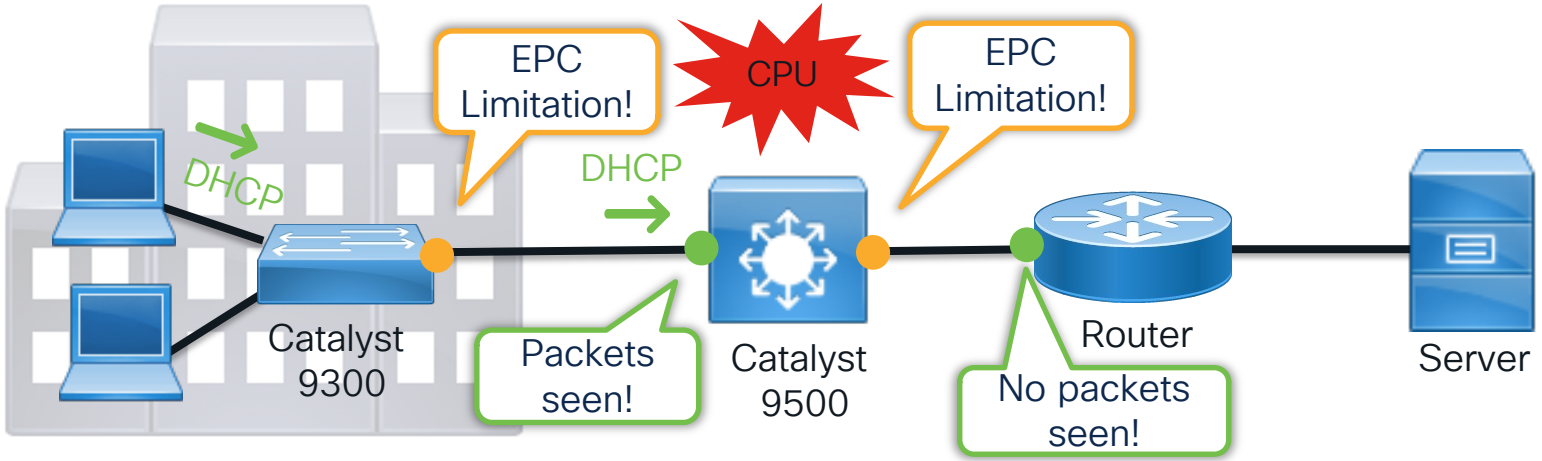
Capture in buffer not available anymore!

```
9300_access# show monitor capture file flash:9500Port1.pcap brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

    1   0.000000      0.0.0.0 -> 255.255.255.255 DHCP 366 DHCP Discover - Transaction ID 0x125b
    2   3.849494      0.0.0.0 -> 255.255.255.255 DHCP 366 DHCP Discover - Transaction ID 0x125b
    3   7.850675      0.0.0.0 -> 255.255.255.255 DHCP 366 DHCP Discover - Transaction ID 0x125b
```

```
9300_access# show monitor capture file flash:9500Port1.pcap display-filter "eth.addr==9c54.16b7.ff46" brief
    1    0.000000      0.0.0.0 -> 255.255.255.255 DHCP 366 DHCP Discover - Transaction ID 0x125b
    2   3.849494      0.0.0.0 -> 255.255.255.255 DHCP 366 DHCP Discover - Transaction ID 0x125b
    3   7.850675      0.0.0.0 -> 255.255.255.255 DHCP 366 DHCP Discover - Transaction ID 0x125b
```

Configuring Embedded Packet Capture




```
9500_Gateway#monitor capture CPU control-plane in
9500_Gateway#monitor capture CPU match any
9500_Gateway#monitor capture CPU buffer size 100
9500_Gateway#monitor capture CPU start
```

Displaying Embedded Packet Capture

```
9500_Gateway#monitor capture CPU stop
Capture statistics collected at software:
       Capture duration - 2 seconds
       Packets received - 9715
       Packets dropped - 0
       Packets oversized - 0

Bytes dropped in asic - 672640
```

Thousands of packets to the CPU per second

Drops seen after +1000 pps

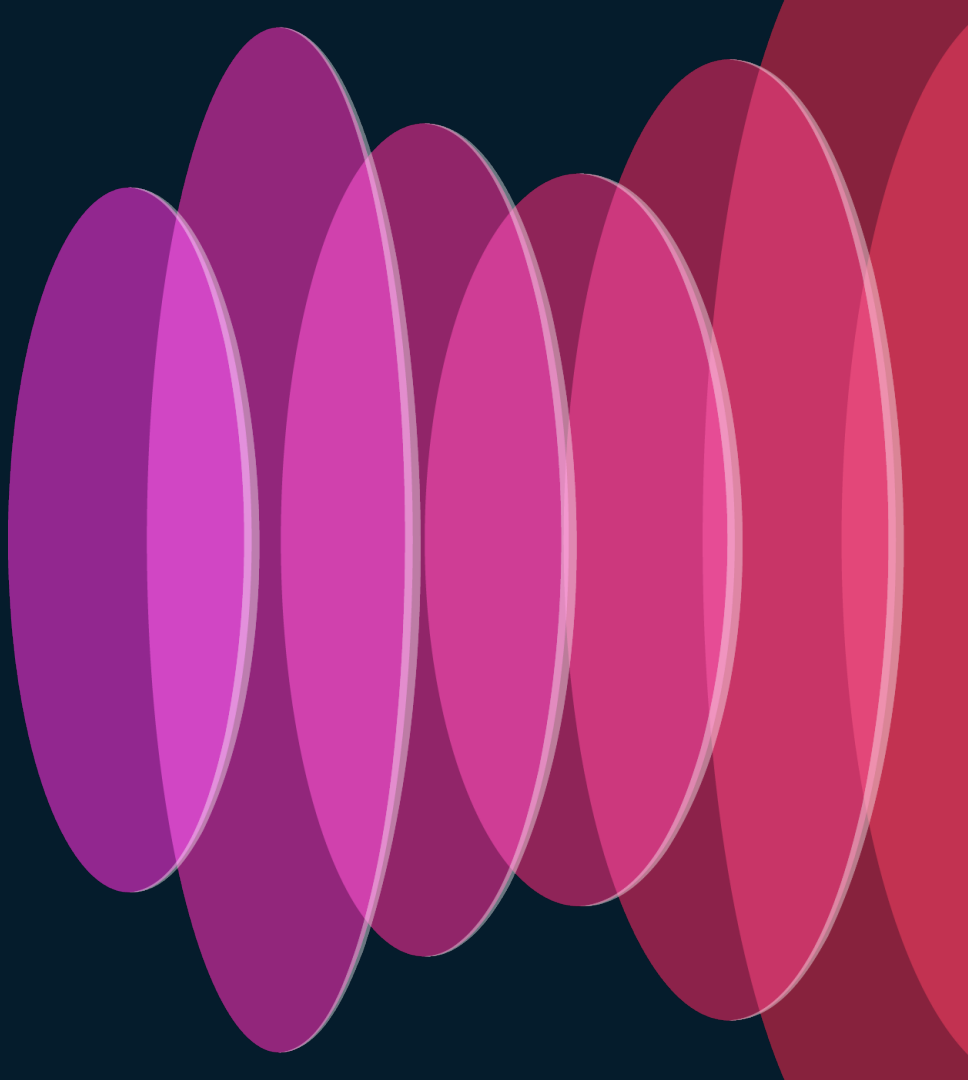
TAC Tip

show mac address-table address xxxx.xxxx.xxxx

```
9500_Gateway#show monitor capture CPU buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

    1   0.000000 70:7d:b9:be:11:d9 -> ff:ff:ff:ff:ff:ff ARP 60 Who has 10.10.10.2? Tell 10.10.10.1
    2   0.000007 70:7d:b9:be:11:d9 -> ff:ff:ff:ff:ff:ff ARP 60 Who has 10.10.10.2? Tell 10.10.10.1
    3   0.000009 70:7d:b9:be:11:d9 -> ff:ff:ff:ff:ff:ff ARP 60 Who has 10.10.10.2? Tell 10.10.10.1
    4   0.000011 70:7d:b9:be:11:d9 -> ff:ff:ff:ff:ff:ff ARP 60 Who has 10.10.10.2? Tell 10.10.10.1
    5   0.000014 70:7d:b9:be:11:d9 -> ff:ff:ff:ff:ff:ff ARP 60 Who has 10.10.10.2? Tell 10.10.10.1
    6   0.000016 70:7d:b9:be:11:d9 -> ff:ff:ff:ff:ff:ff ARP 60 Who has 10.10.10.2? Tell 10.10.10.1
    7   0.000096 70:7d:b9:be:11:d9 -> ff:ff:ff:ff:ff:ff ARP 60 Who has 10.10.10.2? Tell 10.10.10.1
    8   0.000129 70:7d:b9:be:11:d9 -> ff:ff:ff:ff:ff:ff ARP 60 Who has 10.10.10.2? Tell 10.10.10.1
```

Conclusion



Key Session Takeaways

1. Know the benefits and restrictions of each capturing tool to use it according to the nature of the issue.
2. Understand how to analyze information in a capture.
3. If you are lost... Take a packet capture.

References

SPAN configuration guide 17.9.x for 9300 switches:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/nmgmt/b_179_nmgmt_9300_cg/configuring_span_and_rspan.html

EPC configuration guide 17.9.x for 9300 switches:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/nmgmt/b_179_nmgmt_9300_cg/configuring_packet_capture.html

9300 Architecture White Paper:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-architecture-cte-en.html

Continue your education

- 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

Contact us at:

cbustani@cisco.com

patrgarc@cisco.com

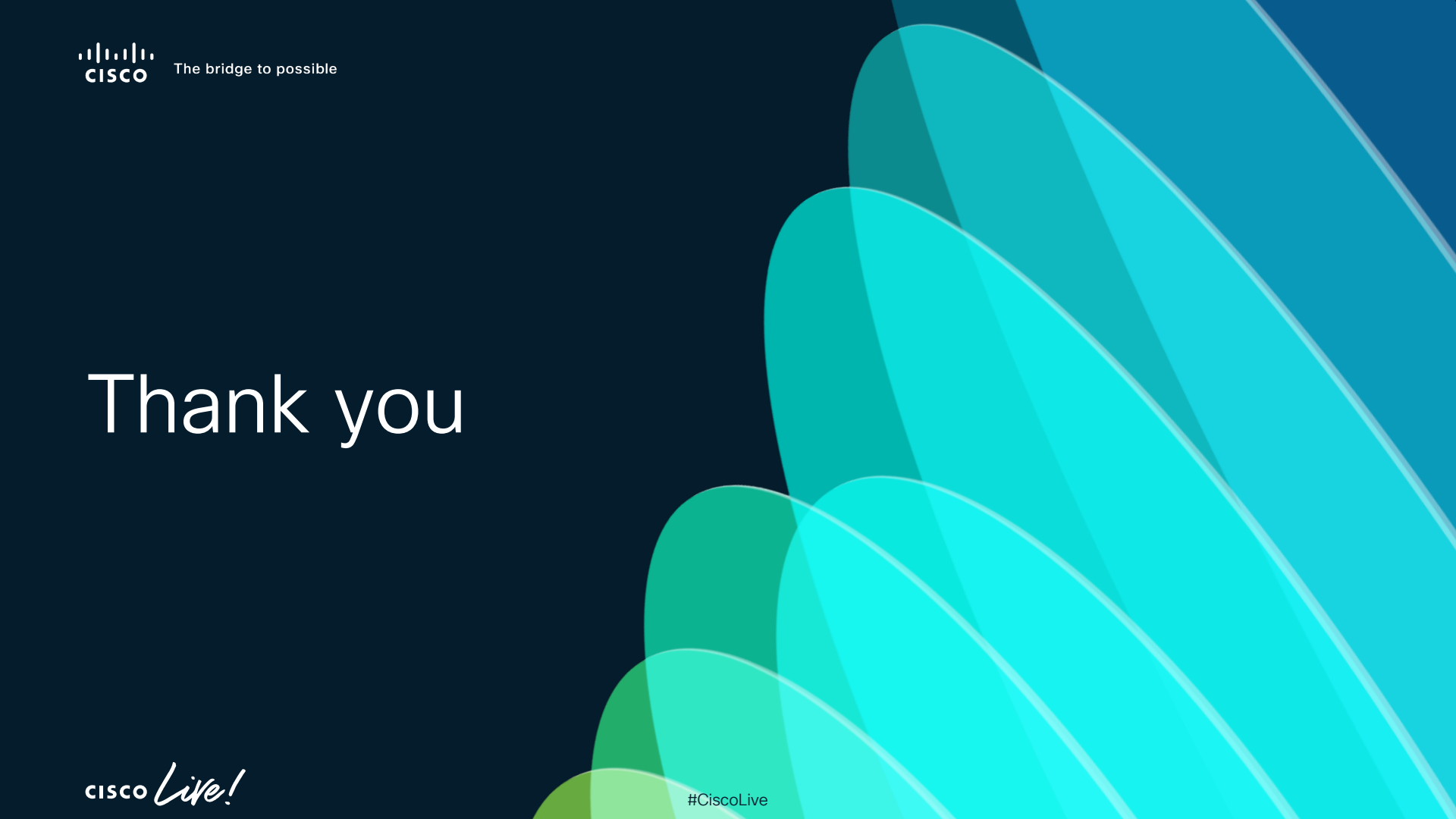
Complete Your Session Evaluations

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.**


The bridge to possible
Thank you
cisco Live!
#CiscoLive