

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, triangular rays in various shades of blue and cyan, creating a sunburst effect that spreads across the right half of the image.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Automation and In-Depth Troubleshooting of Cat8k, ASR1k, ISR and SD-WAN Edge

Mark Fisher, Technical Leader
BRKTRS-3475

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

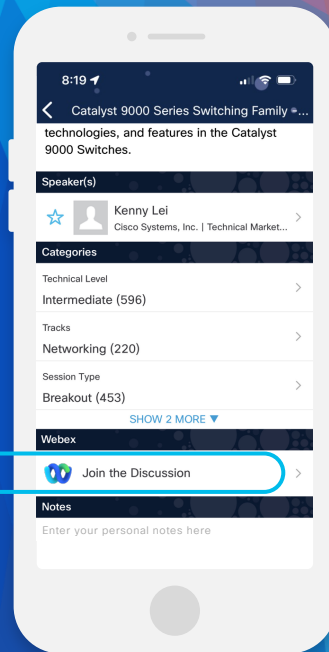
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKTRS-3475>

Troubleshooting

Can be like bad Sci-Fi..

Top Down



Stuck?



Bottom Up!



You need

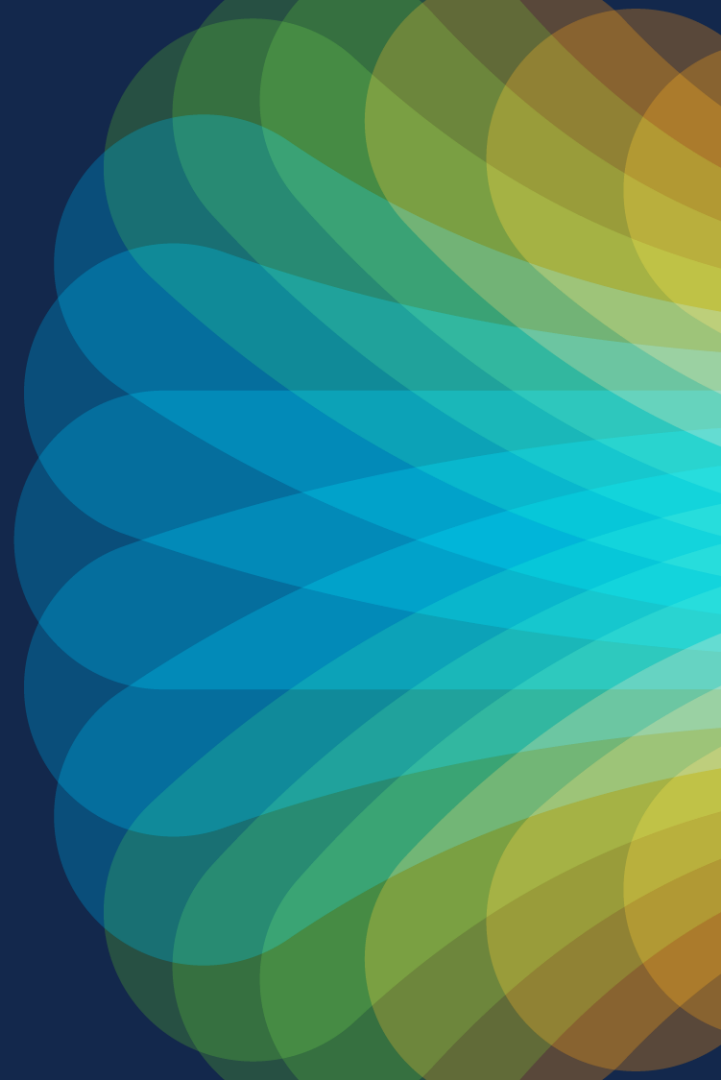


Adobe Stock | #226753553

Agenda

- How are packet forwarded (architecture)
- IOS-XE Dataplane Troubleshooting
- Tools and Applications for Network-level troubleshooting
- IOS-XE Resource Monitoring
- Wrapping up...

Background



Troubleshooting Overview

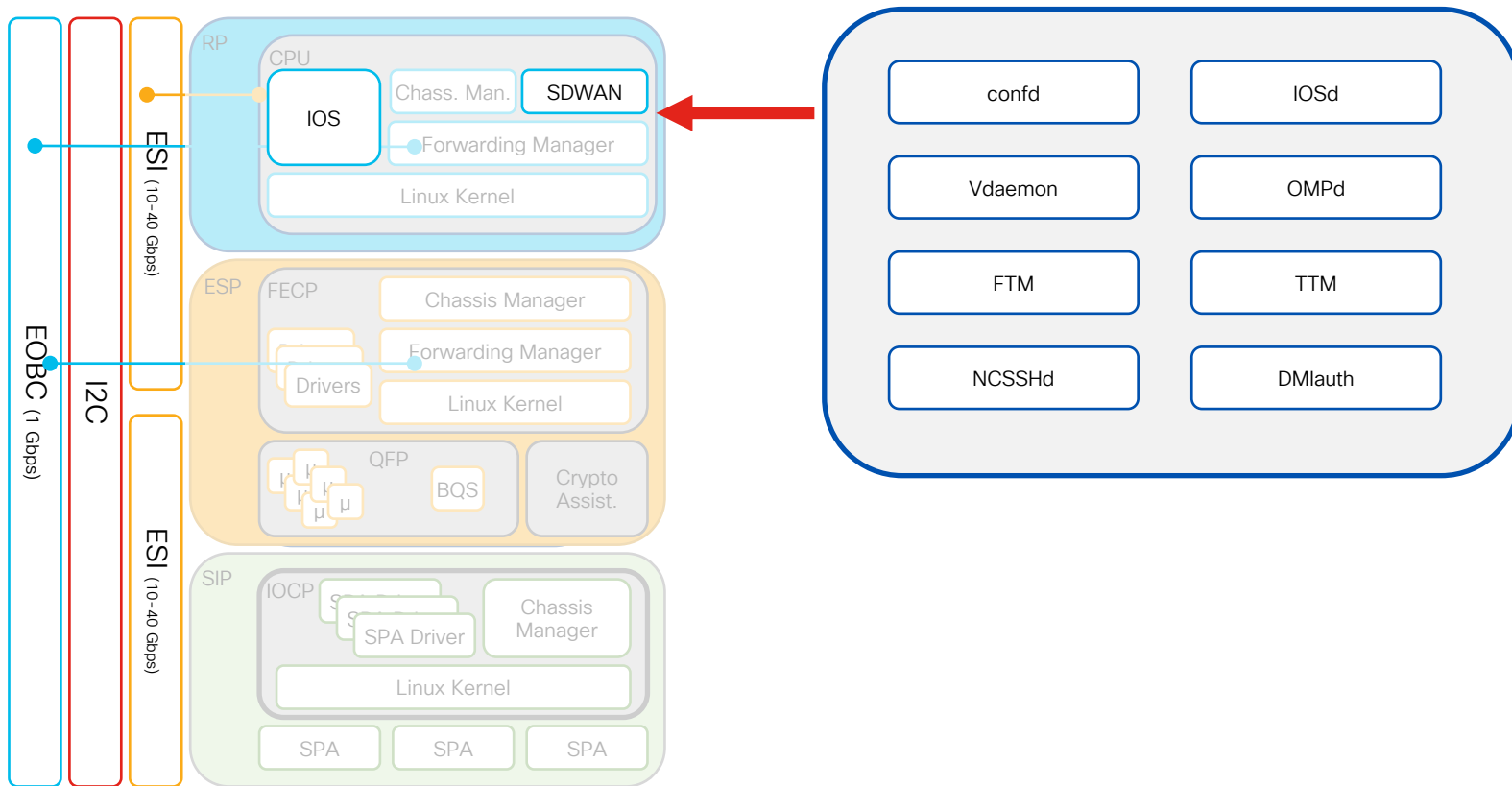
- Top down – topology, configuration etc.
- Working vs Non-Working
- Bottom up – drops etc.
- Starting point depends on issue e.g. broken vs intermittent
- Use architecture to inform direction, can really be easier to start from bottom
- Commands, scripting, features to help automate

Key Acronyms used in diagrams

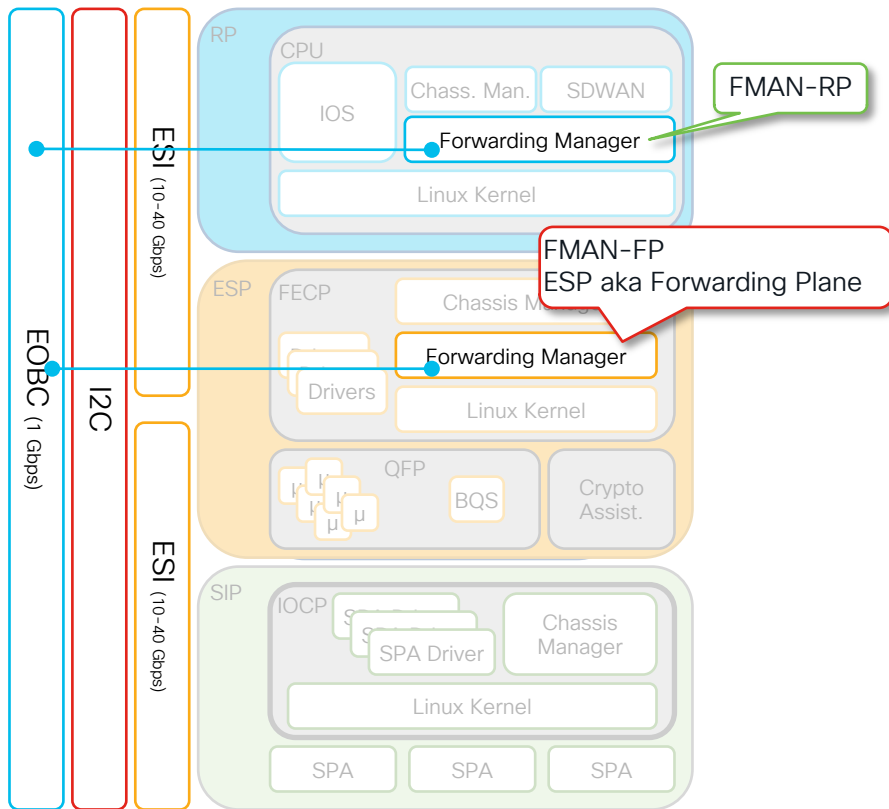
- RP – Route Processor
- FP – Forwarding Processor = ESP (Embedded Service Processor)
- CPP – Cisco Packet Processor Complex = QFP (Quantum Flow Processor)
- PPE – Packet Processing Engine
- IOCP – I/O Control Processor
- FECF – Forwarding Engine Control Processor
- SPA – Shared Port Adapter
- SIP – SPA Interface Processor
- IOS(d) – IOS image that runs as a process on the RP, as a daemon.
- FMAN – Forwarding manager (FMAN-RP, FMAN-FP)
- IOS-XE (BinOS) = Linux Based Software Infrastructure that runs on device

Software architecture

The Route Processor (General view)

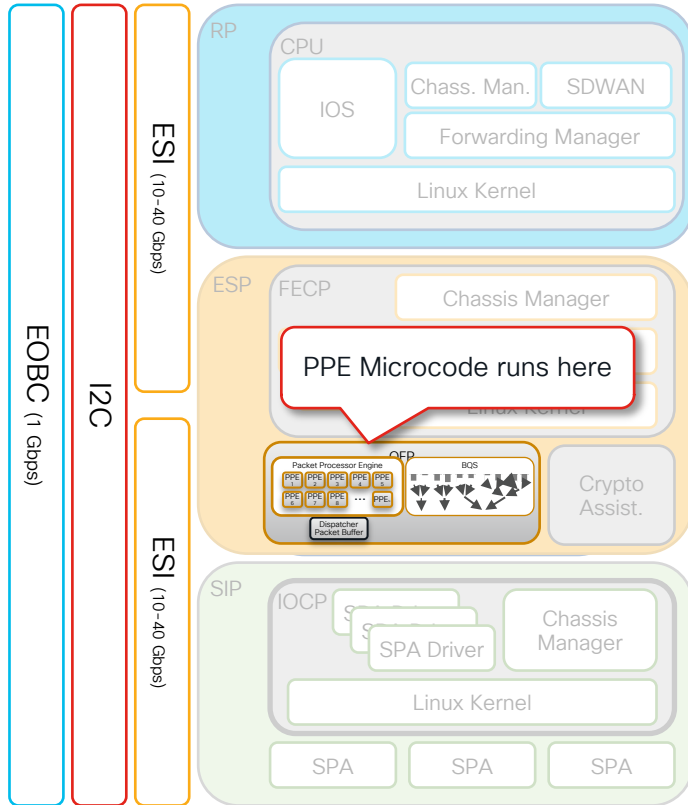


Forwarding Manager (FMAN)



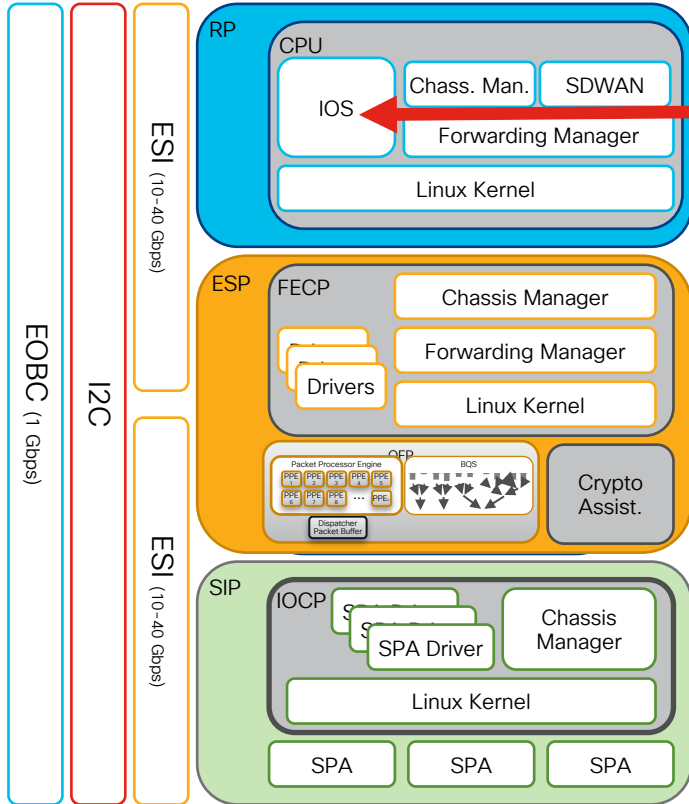
- FMAN on RP communicates with FMAN process on ESP
 - Distributed function
- Propagates control plane ops. to ESP
 - CEF tables, ACL's, NAT, SA's,...
- FMAN-FP communicates information back to FMAN-RP
 - e.g. statistics
 - FMAN-RP pushes info back to IOS
- FMAN on active RP maintains state for both active & standby ESP's
 - Facilitates NSF after re-start with bulk download of state information

PPE microcode



- Written in C
 - proper features, no hack
- Runs on each thread of the PPE
- Processes packets
 - run to completion
 - assisted by various memories
 - TCAM, DRAM,... various speeds
- Features applied via FIA
 - Feature Invocation Array
- FIA per interface
 - input FIA, output FIA
 - drop FIA (Null interface)
- on Cat8500 / ASR1k /ISR4400– running on bare metal
- Other platforms: running as Linux process

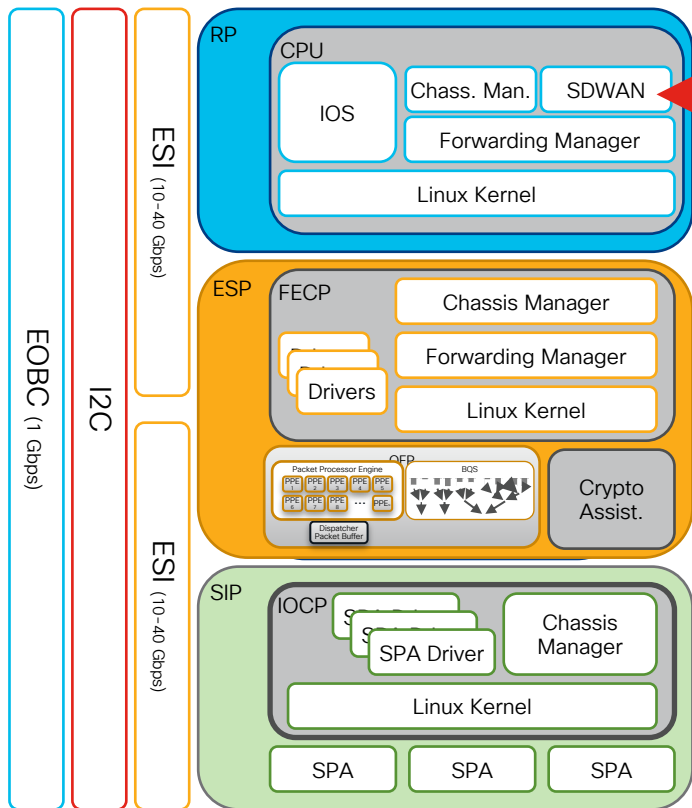
From Architecture to CLI



```
cedge1#show ip route
<removed>
Gateway of last resort is 192.168.4.1 to network 0.0.0.0

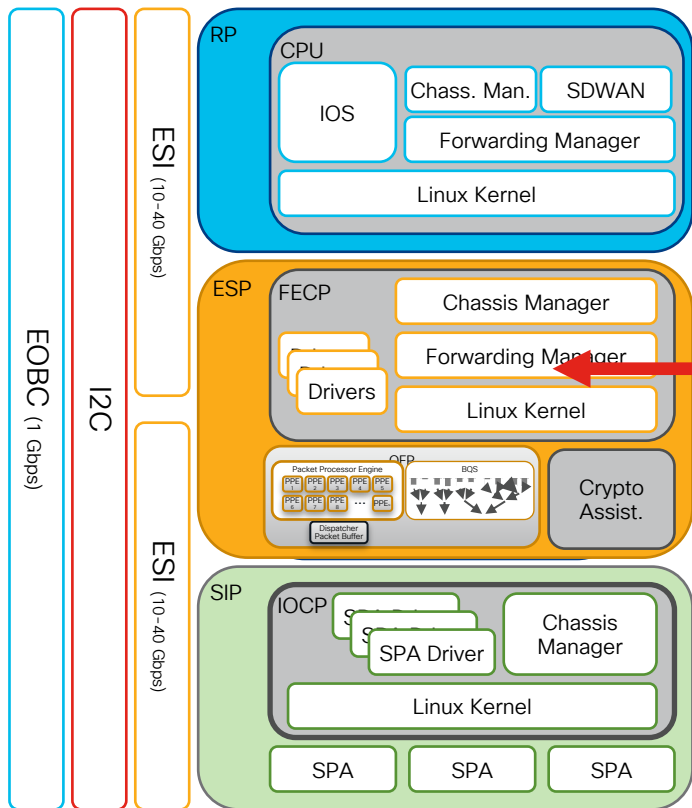
S*    0.0.0.0/0 [1/0] via 192.168.4.1
      [1/0] via 172.16.11.1
      172.16.0.0/16 is variably subnetted, 12 subnets, 2 masks
C      172.16.11.0/24 is directly connected, GigabitEthernet3
L      172.16.11.254/32 is directly connected, GigabitEthernet3
O      172.16.12.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
O      172.16.13.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
O      172.16.14.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
O      172.16.15.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
O      172.16.16.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
O      172.16.17.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
O      172.16.18.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
O      172.16.41.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
O      172.16.119.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
O      172.16.120.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.4.0/24 is directly connected, GigabitEthernet1
L      192.168.4.31/32 is directly connected, GigabitEthernet1
O      192.168.8.0/24 [110/2] via 172.16.11.1, 2w0d, GigabitEthernet3
cedge1#
```

From Architecture to CLI



```
cedgel#show sdwan omp summary
oper-state          UP
admin-state         UP
personality          vedge
device-role          Edge-Router
omp-uptime           7:20:50:13
routes-received      316
routes-installed     91
routes-sent          8
tlocs-received       42
tlocs-installed      20
tlocs-sent           4
services-received    2
services-installed   0
services-sent        4
mcast-routes-received 18
mcast-routes-installed 2
mcast-routes-sent    4
hello-sent           67989
hello-received       67980
handshake-sent       2
handshake-received   2
alert-sent           0
alert-received       0
inform-sent          26
[...]
```

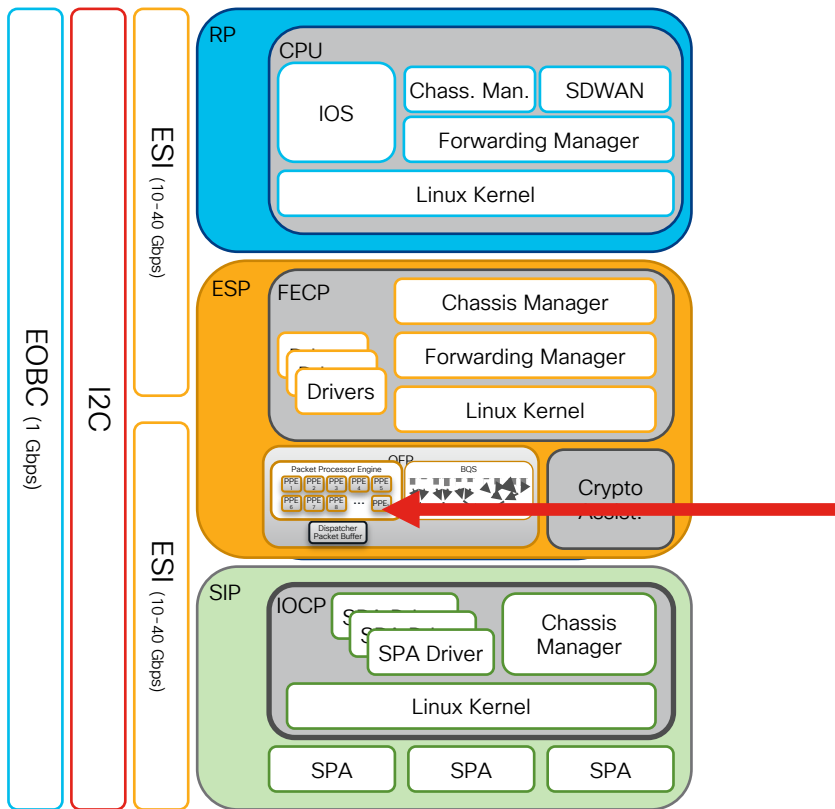
From Architecture to CLI



```

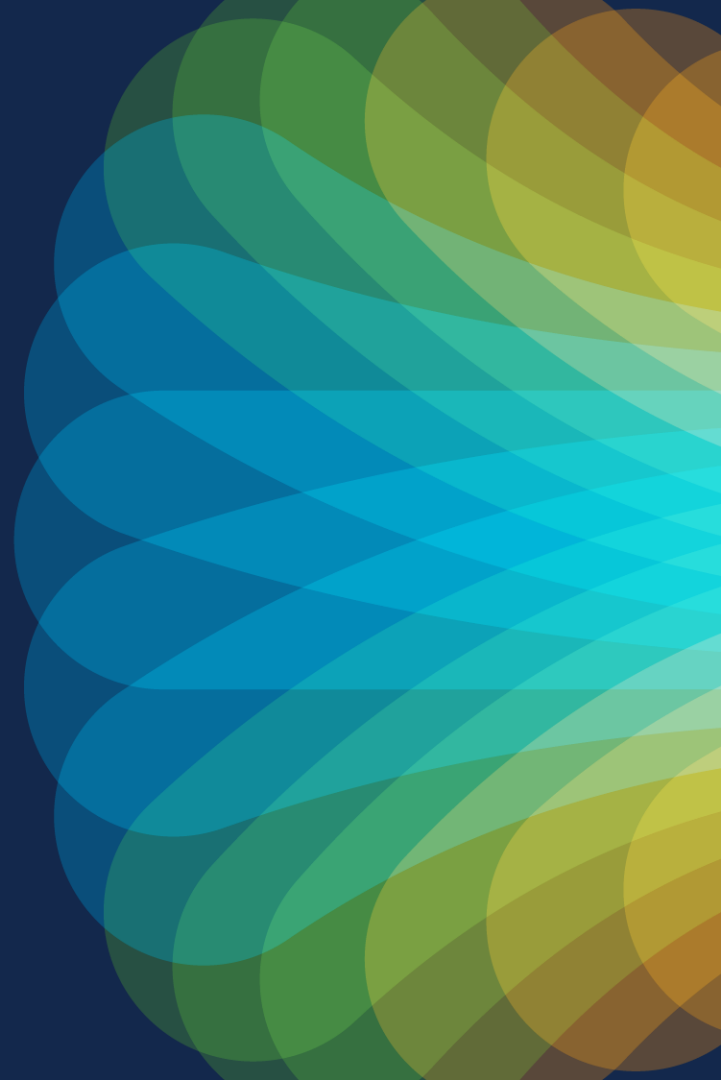
edge7#show platform software ipsec fp active flow all
===== Flow id: 1
        mode: transport
        direction: inbound
        protocol: esp
        SPI: 0x0001bd
        local IP addr: 172.16.17.254
        remote IP addr: 172.16.12.254
        crypto map id: 1
        SPD id: 1
        cpp SPD id: 1
        ACE line number: 1
        QFP SA handle: 14
        crypto device id: 0
        IOS XE interface id: 17
        interface name: Tunnel3
        object state: active
===== Flow id: 2
        mode: transport
        direction: outbound
        protocol: esp
        SPI: 0x000109
        local IP addr: 172.16.17.254
        remote IP addr: 172.16.12.254
        crypto map id: 1
        SPD id: 1
        cpp SPD id: 1
        ACE line number: 1
        QFP SA handle: 33
        crypto device id: 0
        IOS XE interface id: 17
        interface name: Tunnel3
        use path MTU: 1480
        object state: active
        object bind state: active
    
```

From Architecture to CLI

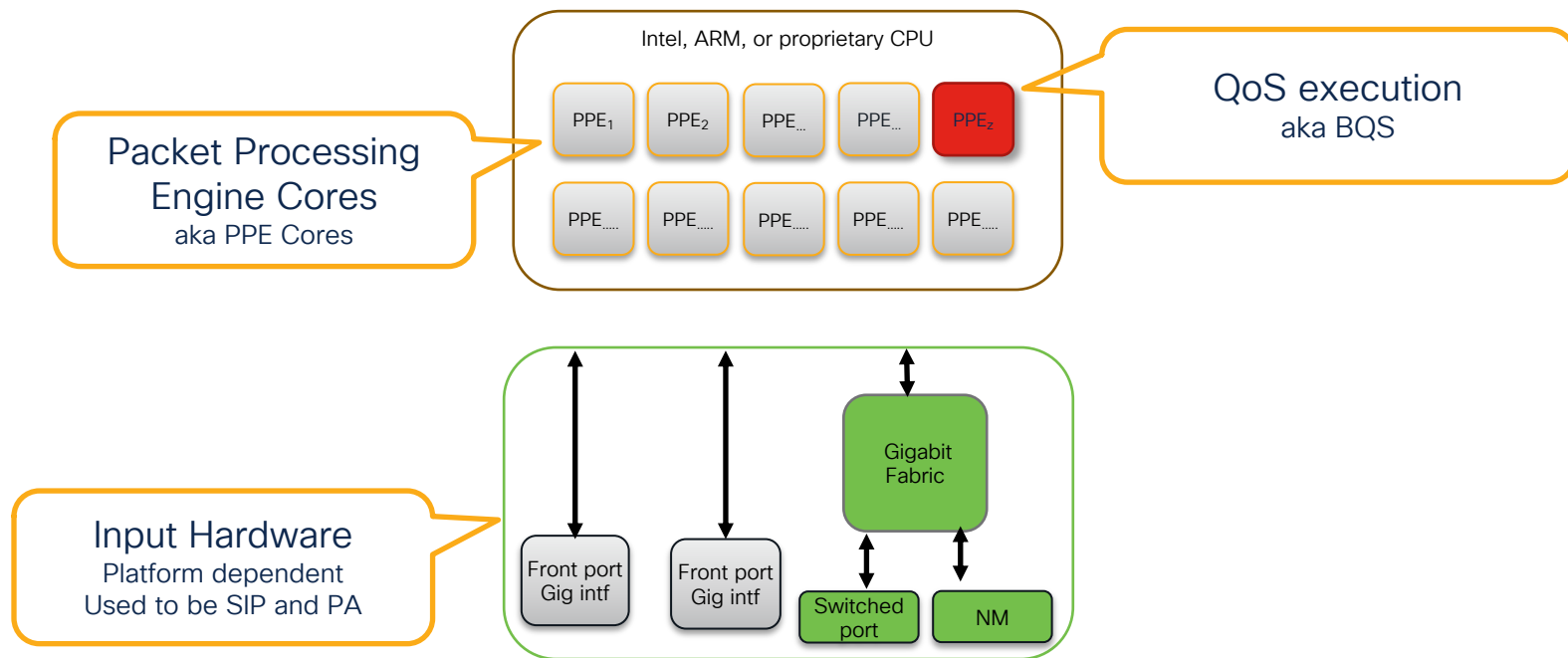


```
cedge6#show platform hardware qfp active feature acl control
Stats Poll Period: 0
Stats Entry Size: 16
Ha Init: 1
Fm Ready: 0
IPv4 Logging Threshold: 2147483647
IPv4 Logging Interval: 0
IPv6 Logging Threshold: 350000
IPv6 Logging Interval: 0
Maximum Aces Per Acl: 256000
Stats Update size: 180
Maximum Entries: 0
Maximum Entries per Classifier: 0
Result Bit Size: 0
Result Start Bit Pos: 0
Maximum Profiles: 0
Maximum Blocks per Profile: 0
Device Select: 0
Maximum Tree Depth: 0
Dimention: 0
Number Cuts: 0
```

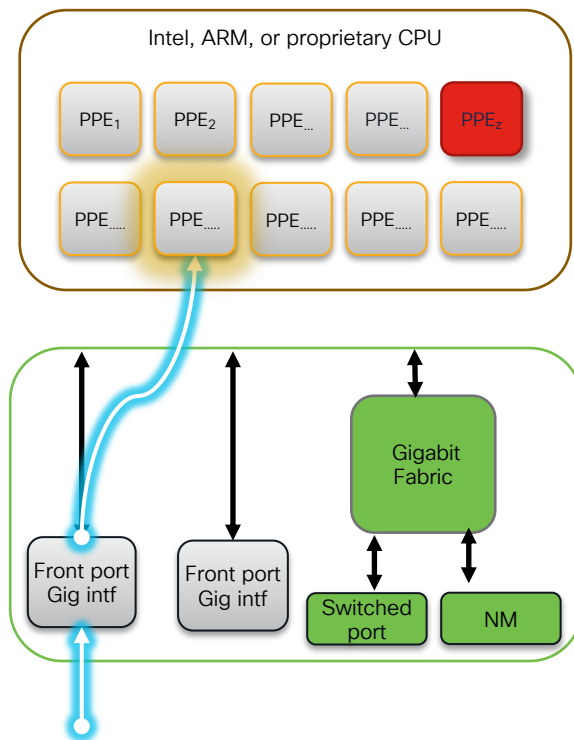
The forwarding plane



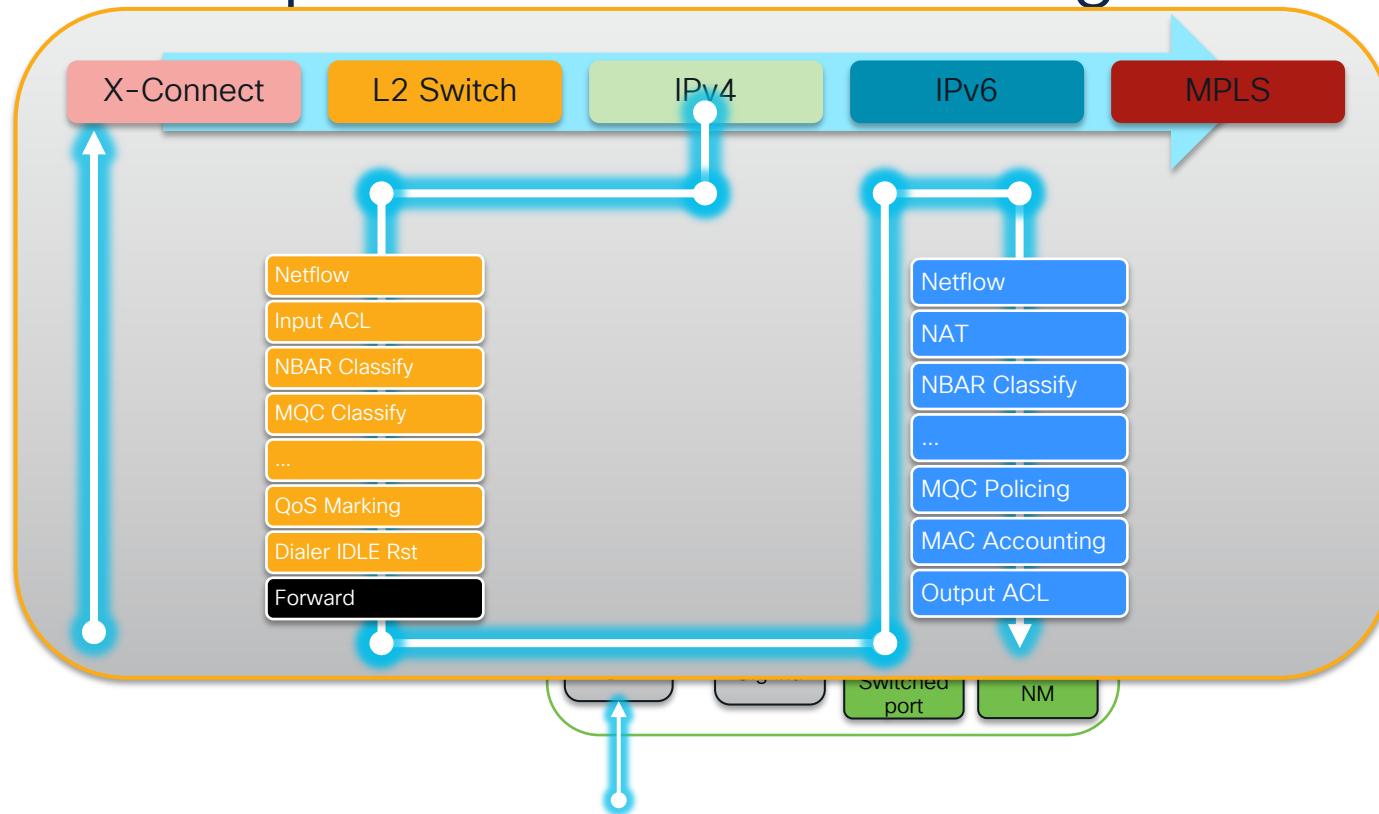
Life of a packet – Abstract Hardware



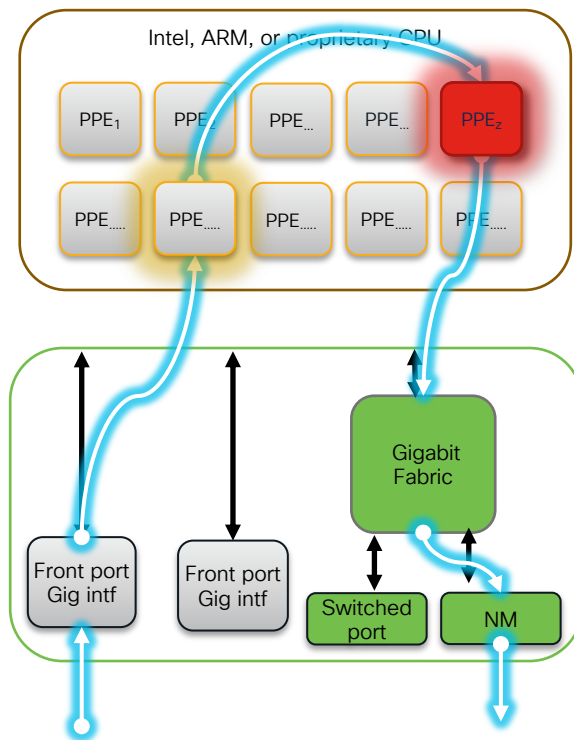
Life of a packet – Traffic entering interface



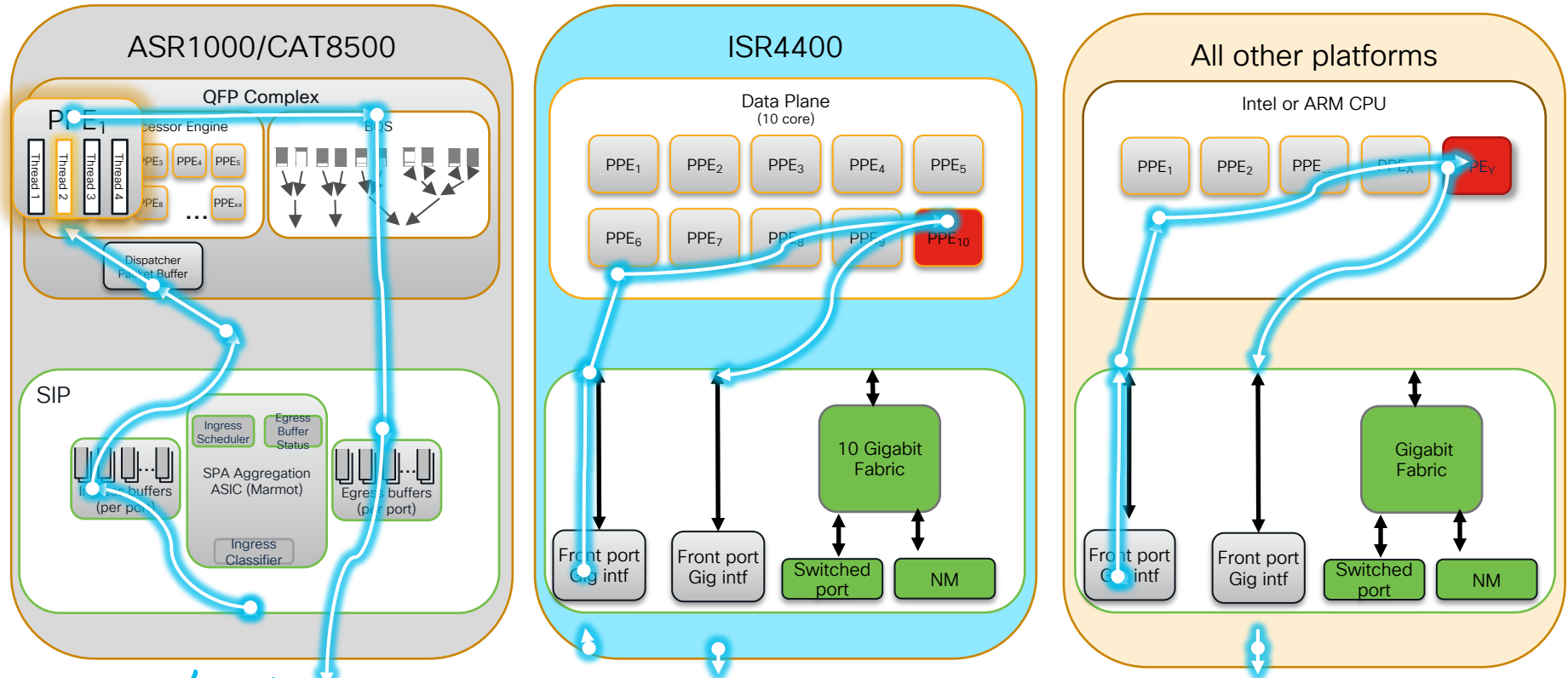
Life of a packet – Traffic entering interface



Life of a packet – BQS and Exit



Life of a packet – Various Platforms; Same Story

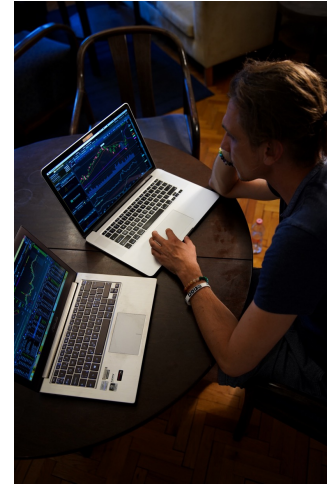


Features

- Step One – What feature went wrong?



- Step Two – What went wrong in the feature?



Interface FIA and Feature Order

show platform hardware qfp active interface if-name GigabitEthernet1

General interface information

Interface Name: GigabitEthernet1
Interface state: VALID
Platform interface handle: 7
QFP interface handle: 6
Rx uidb: 1023
Tx uidb: 65530
Channel: 30
Interface Relationships

BGPPA/QPPB interface configuration information

Ingress: BGPPA/QPPB not configured. flags: 0000
Egress: BGPPA not configured. flags: 0000

ipv4_input enabled.
ipv4_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.

Features Bound to Interface:

2 GIC FIA state
57 PUNT INJECT DB
46 ethernet
44 VNIC Path
1 IFM
[...]

Protocol 0 - ipv4_input

FIA handle - CP:0x2fccfe0 DP:0xe73998c0
IPV4_INPUT_DST_LOOKUP_ISSUE (M)
IPV4_INPUT_ARL_SANITY (M)
CBUG_INPUT_FIA
DEBUG_COND_INPUT_PKT
IPV4_INPUT_DST_LOOKUP_CONSUME (M)
IPV4_INPUT_ACL
IPV4_INPUT_FOR_US_MARTIAN (M)
IPV4_INPUT_STILE_LEGACY
IPV4_INPUT_QOS
IPV4_INPUT_VFR
IPV4_NAT_INPUT_FIA
IPV4_INPUT_LOOKUP_PROCESS (M)
IPV4_INPUT_IPOPTIONS_PROCESS (M)
IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)

Protocol 1 - ipv4_output

FIA handle - CP:0x2fcd4a8 DP:0xe7390840
IPV4_OUTPUT_VFR
IPV4_OUTPUT_INSPECT
IPV4_NAT_OUTPUT_FIA
IPV4_OUTPUT_THREAT_DEFENSE
IPV4_VFR_REFRAQ (M)
IPV4_OUTPUT_L2_REWRITE (M)
IPV4_OUTPUT_STILE_LEGACY
IPV4_OUTPUT_QOS
IPV4_OUTPUT_FRAG (M)
IPV4_OUTPUT_DROP_POLICY (M)
MARMOT_SPA_D_TRANSMIT_PKT
DEF_IF_DROP_FIA (M)

Protocol 8 - layer2_input

FIA handle - CP:0x2fcd100 DP:0xe73976c0
LAYER2_INPUT_SIA (M)
CBUG_INPUT_FIA
DEBUG_COND_INPUT_PKT
LAYER2_INPUT_ARL (D)
LAYER2_INPUT_QOS
LAYER2_INPUT_LOOKUP_PROCESS (M)
LAYER2_INPUT_GOTO_OUTPUT_FEATURE (M)

Protocol 9 - layer2_output

FIA handle - CP:0x2fcd460 DP:0xe73910c0
LAYER2_OUTPUT_ARL (D)
LAYER2_OUTPUT_QOS
LAYER2_OUTPUT_DROP_POLICY (M)
MARMOT_SPA_D_TRANSMIT_PKT
DEF_IF_DROP_FIA (M)

Protocol 14 - ess_ac_input

FIA handle - CP:0x2fcd190 DP:0xe73965c0
CBUG_INPUT_FIA
PPPOE_GET_SESSION
ESS_ENTER_SWITCHING
PPPOE_HANDLE_UNCLASSIFIED_SESSION
DEF_IF_DROP_FIA (M)

QfpEth Physical Information

DPS Addr: 0x00000000038b7e48
Submap Table Addr: 0x00000000
VLAN Ethertype: 0x8100
QOS Mode: Per Link
VLAN AutoSense: No

Per-Feature Drop Counters - show drop

```
cedge6#show drop
```

```
----- show platform hardware qfp active statistics drop detail -----
```

```
Last clearing of QFP drops statistics : never
```

-----			-----		
ID	Global Drop Stats		Packets		Octets

139	Disabled		1376		207022
62	IpTtlExceeded		13401		2410871
56	IpsecInput		54		8379
134	IpsecOutput		1		91
94	Ipv4NoAdj		33635		20883939
19	Ipv4NoRoute		937		119941
33	Ipv6NoRoute		3		168
98	MplsFragReq		7177		10862378
246	Nat64v6tov4		6		480
20	QosPolicing		166		183128
216	UnconfiguredIpv6Fia		279862		30355630

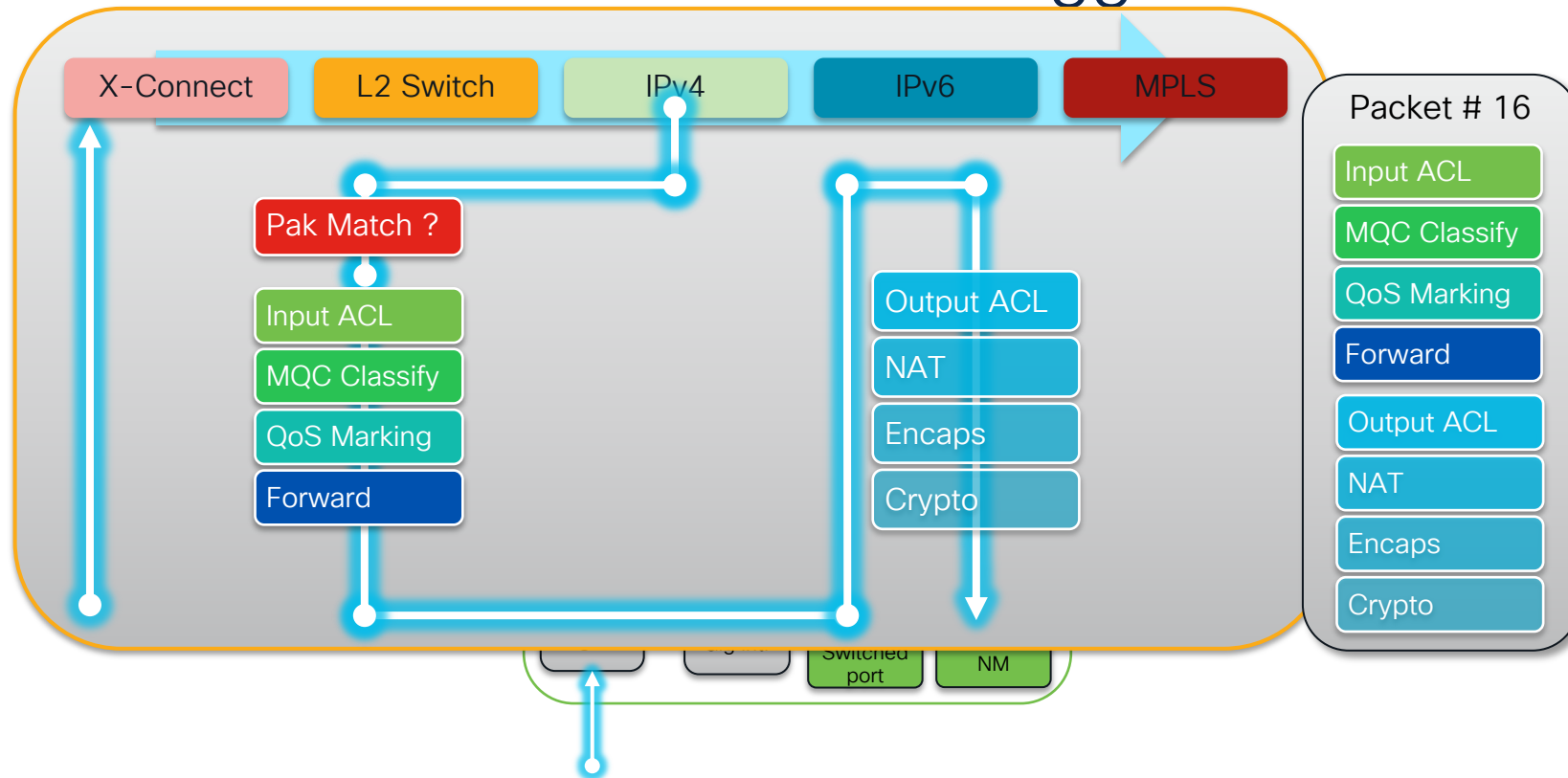
```
----- show platform hardware qfp active interface all statistics drop_summary -----
```

```
[...]
```

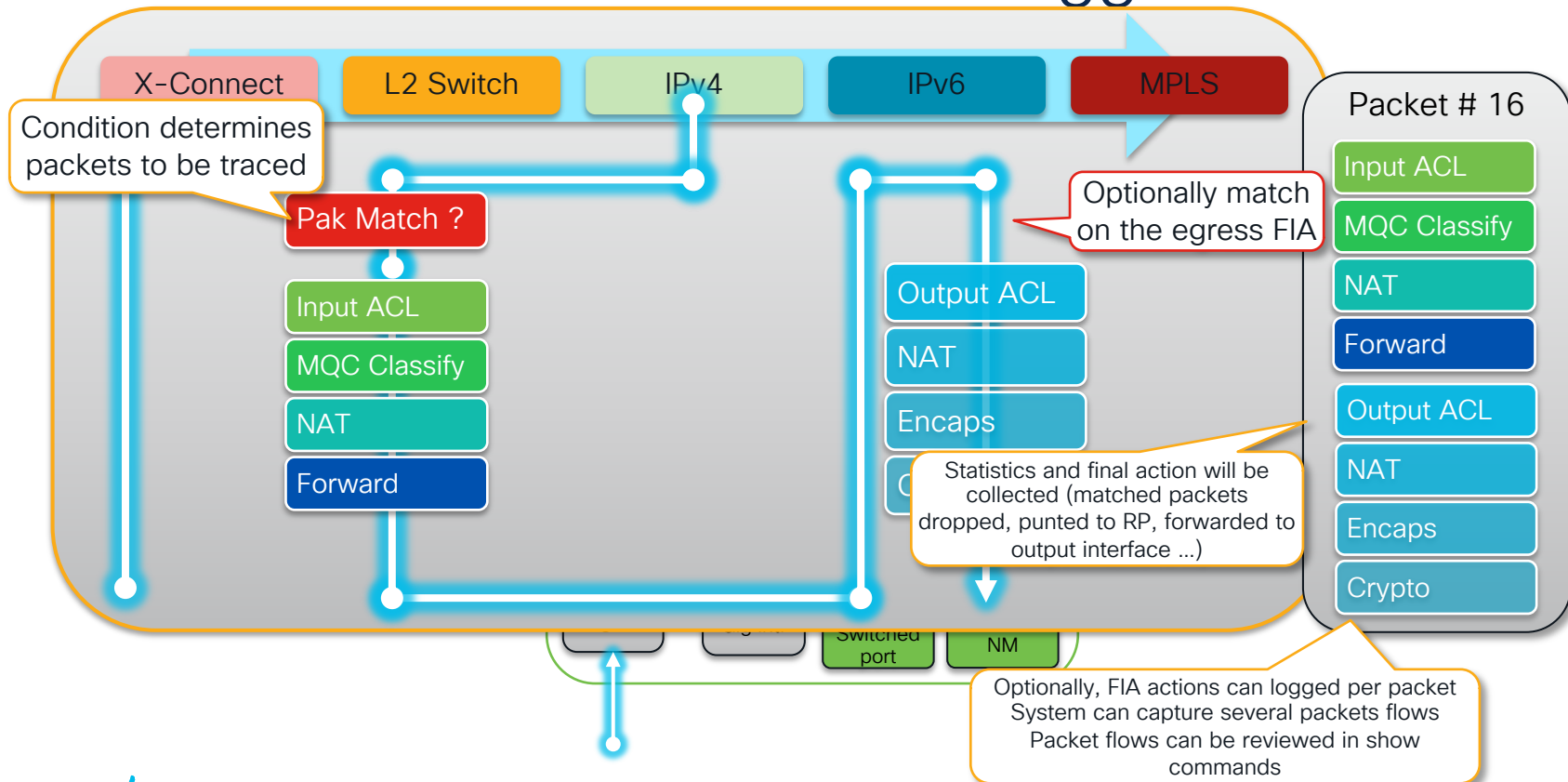
Interface	Rx Pkts	Tx Pkts

GigabitEthernet1	94074	166
GigabitEthernet2	18437	0
[...]		
Tunnel1	2458	0
Tunnel3	34564	0
NVI0	0	6

The Packet Tracer and FIA Debugger



The Packet Tracer and FIA Debugger



Back of mind – packet patterns

- Multicast Replication
- Fragmentation
- ICMP Echo Request/Reply
- Reassembly of packet for us
- Virtual Reassembly of Pass Thru packets
- Reassembly of Overlay VPN

Packet Tracer – General Flow

1. Check clock/NTP (sync=True in Python radkit) and *always* run show clock
2. Define platform condition/match (be specific)
3. Define packet trace limits/counts and traces (we want FIA trace!)
4. Define packet trace data to copy
5. Start packet trace
6. Traffic passes (or not)
7. Stop trace (if limit/count not already hit)
8. Check results
9. Clear buffer/statistics (if desired)

Conditionally Matching Packets

Identifying Interesting Packets

```
asr-1k# debug platform condition ?
debug platform condition ?
  both      Simultaneous ingress and egress debug
  egress    Egress only debug
...
  ingress   Ingress only debug
  interface Set interface for conditional debug
  ipv4      Debug IPv4 conditions
  ipv6      Debug IPv6 conditions
  mpls      Debug MPLS conditions
...
```

Match all ingress packets

```
asr-1k#debug platform condition ingress
asr-1k#debug platform condition interface gig0/0/3 ingress
asr-1k#debug platform condition ipv4 10.0.0.1/32 both
asr-1k#debug platform condition ipv4 access-list 100 egress
asr-1k#debug platform condition mpls 10 1 ingress
```

Match all ingress packets on interface gig0/0/3

Match in & out packets with source or destination 10.0.0.1

Match egress packets passing access-list 100

Match MPLS packets with top ingress label 10

Conditionally Matching Packets

Stopping

```
asr-1k# debug platform condition stop  
asr-1k# clear platform condition all
```

Manually stop packet-trace

Also clears results

Plan your debugs, have an inbuilt stop condition where possible (limit or circular buffer)

Activating the Packet Tracer

Following packets through IOS-XE – Basic Statistics

```
asr-1k# debug platform packet-trace ?
copy      Copy packet data
drop      Trace drops only
enable    Enable packet trace
packet    Packet count
```

The packet tracer follows a set of packets in details through the FIA

```
asr-1k# debug platform condition interface gig0/0/0 ingress
asr-1k# debug platform condition start
asr-1k# debug platform packet-trace enable
asr-1k# ... !send traffic
asr-1k# show platform packet-trace statistics
```

Avoid egress, use ingress or both

Extraneous command - was suppressed in 16.3

Packets Summary

```
Matched 102
Traced 0
```

102 packets were matched by the condition

Packets Received

```
Ingress 12
Inject 90
```

Count	Code	Cause
90	9	QFP ICMP generated packet

Packets Processed

```
Forward 12
Punt 0
Drop 90
```

12 packets were forwarded

90 packets were dropped

Count	Code	Cause
13	92	Ipv4Null0
17	47	FirewallInvalidZone
60	184	FirewallL4
Consume	0	

13 packets were dropped due to no route

60 packets dropped by L4 inspection (e.g. receiving window)

17 packets were dropped due to absence of zone pair

Packet Tracer – Tracing Packets...

The fate of 16 packets

```
asr-1k# debug platform condition interface gig0/0/0 ingress
```

```
asr-1k# debug platform condition start
```

```
asr-1k# debug platform packet-trace packet 16
```

Automatically stops tracing
after 16 packets

```
asr-1k# debug platform packet-trace packet 16 circular
```

16 around and around
instead?

```
asr-1k# debug platform packet-trace enable
```

```
asr-1k# ... !send traffic
```

Extraneous command -
was suppressed in 16.3

```
asr-1k# show platform packet-trace summary
```

Pkt	Input	Output	State	Reason
0	Gi0/0/2	internal0/0/rp:0	PUNT	55 (For-us control)
1	Gi0/0/2	internal0/0/rp:0	PUNT	55 (For-us control)
2	Gi0/0/2	internal0/0/rp:0	PUNT	55 (For-us control)
3	Gi0/0/2	internal0/0/rp:0	PUNT	55 (For-us control)
4	INJ.7	Gi0/0/2	FWD	
5	INJ.7	Gi0/0/2	FWD	
6	Gi0/0/2	internal0/0/rp:0	PUNT	55 (For-us control)
7	INJ.7	Gi0/0/2	FWD	
8	...			

16 packets were traced; we
can zoom in

INJ.7: Packet injected by the RP
internal0/0/rp:0: Packet punted to the RP

Packet Tracer – Tracing Packets...

The fate of an individual packet

```
asr-1k# show platform packet-trace packet 1
```

```
Packet: 1          CBUG ID: 109056985
```

Summary

```
Input      : GigabitEthernet0/0/2
```

```
Output     : internal0/0/rp:0
```

```
State      : PUNT 55  (For-us control)
```

Timestamp

```
Start      : 334771580191282 ns (04/29/2014 08:01:38.017738 UTC)
```

```
Stop       : 334771580487612 ns (04/29/2014 08:01:38.018035 UTC)
```

Path Trace

Feature: IPV4

```
Source      : 17.0.0.196
```

```
Destination : 172.18.0.1
```

```
Protocol    : 50 (ESP)
```

Feature: IPSec

```
Action      : DECRYPT
```

```
SA Handle   : 753
```

```
SPI         : 0x30ba5940
```

```
Peer Addr   : 17.0.0.196
```

```
Local Addr  : 172.18.0.1
```

Zooming on packet 1

Feature specific details are displayed

Only major features are shown

Packet Tracer – Tracing Packets

... even keeping a copy of the packet if necessary

```
asr-1k# debug platform condition interface gig0/0/0 ingress
asr-1k# debug platform condition start
asr-1k# debug platform packet-trace packet 16
asr-1k# debug platform packet-trace copy packet both [12 | 13 | 14]
```

Keep a copy of the packet in
ingress and egress of the ESP
(before and after the FIA)

```
asr-1k# debug platform packet-trace enable
```

Can store L2, L3 or L4...
pick-a-choose

```
asr-1k# ... !send traffic
```

```
asr-1k# show platform packet-trace packet 1
```

```
Packet: 1          CBUG ID: 109056985
```

Summary

```
Input      : GigabitEthernet0/0/2
Output     : internal0/0/rp:0
State      : PUNT 55  (For-us control)
```

Display the stored packet copy

Path Trace

```
Feature: IPV4
Feature: IPSec
```

Packet Copy In

```
45c00088 c5ee0000 ff32346f 11000313 ac120001 d4b46317 0000017c 68a60265
0ef58135 650e2341 15cf6e81 dd434455 b42efef8 c6cf5ab1 44ad3f98 b165c3d5
```

Packet Copy Out

```
45c0003c 00000000 015804f4 c0ab1301 e000000a 0205efc8 00000000 00000000
00000000 0000000a 0001000c 01000100 0000000f 00040008 0a000200
```

Packet Tracer – Tracing Packets...

The fate of a single packet... even more more more details

```
asr-1k# show platform packet-trace packet 1 decode
Packet: 1          CBUG ID: 109056985
Summary
  Input       : GigabitEthernet0/0/2
  Output      : internal0/0/rp:0
  State       : PUNT 55  (For-us control)
Path Trace
  Feature: IPV4
  Feature: IPSec
Packet Copy In
  45c00088 c5ee0000 ff32346f 11000313 ac120001 d4b46317 0000017c 68a60265
  0ef58135 650e2341 15cf6e81 dd434455 b42efef8 c6cf5ab1 44ad3f98 b165c3d5
IPV4
  Version      : 4
  Header Length : 5
  ToS          : 0xc0
  Total Length : 136
  Identifier   : 0xc5ee
  IP Flags     : 0x0
  Frag Offset  : 0
  TTL          : 255
  Protocol     : 50 (ESP)
  Header Checksum : 0x346f
  Source Address : 17.0.3.19
  Destination Address : 172.18.0.1
ESP
  SPI          : 0xd4b46317
  Sequence Number : 0x0000017c
...
```

Decode the stored packet copy

Here showing the input copy
(output copy follows)

Packet Tracer – Focus on Drops

Dropped packets – nothing else

```
asr-1k# debug platform condition interface gig0/0/0 ingress
asr-1k# debug platform condition start
asr-1k# debug platform packet-trace packet 16
asr-1k# debug platform packet-trace drop [code <dropcode>]
asr-1k# debug platform packet-trace enable
asr-1k# ... !send traffic
asr-1k# debug platform condition stop
asr-1k# show platform packet-trace summary
```

For drops, condition is optional...

Only save dropped packets

Focus on specific drop codes
(find codes in packet-trace statistics)

Stop tracing before dumping the
summary (code limitation)

Admire dropped packets... real close

Pkt	Input	Output	State	Reason
0	Gi0/0/2	Gi0/0/2	DROP	53 (IpssecInput)
1	Gi0/0/2	Gi0/0/2	DROP	53 (IpssecInput)
2	Gi0/0/2	Gi0/0/2	DROP	53 (IpssecInput)
3	Gi0/0/2	Gi0/0/2	DROP	53 (IpssecInput)
4	Gi0/0/2	Gi0/0/2	DROP	53 (IpssecInput)
5	Gi0/0/2	Gi0/0/2	DROP	53 (IpssecInput)
6	Gi0/0/2	Gi0/0/2	DROP	53 (IpssecInput)
7	Gi0/0/2	Gi0/0/2	DROP	53 (IpssecInput)
8	...			

```
asr-1k#show platform packet-trace packet 1
Packet: 1          CBUG ID: 148787639
Summary
  Input   : GigabitEthernet0/0/2
  Output  : GigabitEthernet0/0/2
  State   : DROP 53 (IpssecInput)
  Timestamp
    Start  : 361426338620013 ns (04/29/2014 15:25:52.785406 UTC)
    Stop   : 361426338684993 ns (04/29/2014 15:25:52.785471 UTC)
  Path Trace
  Feature: IPV4
    Source   : 17.0.1.34
    Destination : 172.18.0.1
    Protocol  : 50 (ESP)
  Packet Copy Out
002304bb 72020007 7dfbe301 080045c0 0088d135 0000fe32 2c191100 0122ac12
0001085e 1d620000 00c8172c e8010c3e 44726e6f 3eb231d5 166298c1 f519313c
```

Packet Tracing – FIA Trace (I)

asr1000#show platform packet-trace packet 0

Packet: 0 CBUG ID: 655

Summary

Input : GigabitEthernet1

Output : GigabitEthernet2

State : FWD

Timestamp

Start : 5456699323393 ns (07/11/2016 23:30:28.244810 UTC)

Stop : 5456699556099 ns (07/11/2016 23:30:28.245043 UTC)

Path Trace

Feature: **IPV4**

Input : GigabitEthernet1

Output : <unknown>

Source : 192.168.3.1

Destination : 192.168.255.167

Protocol : 50 (ESP)

Feature: FIA_TRACE

Input : GigabitEthernet1

Output : <unknown>

Entry : 0x8139f260 – DEBUG_COND_INPUT_PKT

Lapsed time : 9680 ns

Feature: **IPV4_INPUT_DST_LOOKUP_CONSUME**

Entry : Input – 0x816999a8

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : **9320 ns**

Feature: **IPV4_INPUT_ACL**

Entry : Input – 0x816999a4

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : **60613 ns**

Feature: **IPV4_INPUT_FOR_US_MARTIAN**

Entry : Input – 0x816999a5

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : **303133 ns**

Feature: **CFT**

API : cft_handle_pkt

packet capabilities : 0x0000008c

input vrf_idx : 0

calling feature : STILE

direction : Input

triplet.vrf_idx : 0

triplet.network_start : 0x00000000

triplet.triplet_flags : 0x00000000

triplet.counter : 0

cft_bucket_number : 2120447

cft_l3_payload_size : 100

cft_pkt_ind_flags : 0x00000000

cft_pkt_ind_valid : 0x000000935

tuple.src_ip : 192.168.3.1

tuple.dst_ip : 192.168.255.167

[...]

Feature: **NBAR**

Packet number in flow: N/A

Classification state: Final

Classification name: ipsec

Classification ID: [CANAL7:9]

Number of matched sub-classifications: 0

Number of extracted fields: 0

Is PA (split) packet: False

TPH-MQC bitmask value: 0x0

Feature: **IPV4_INPUT_STILE_LEGACY**

Entry : Input – 0x80fa0f88

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : **396533 ns**

Packet Tracing – FIA Trace (II)

Feature: **QOS**
Direction : Ingress
Action : SET
Fields : DSCP
Feature: **IPV4_INPUT_QOS**
Entry : Input - 0x814699a8
Input : GigabitEthernet1
Output : <unknown>
Lapsed time : **64586 ns**

Feature: **IPV4_INPUT_VFR**
Entry : Input - 0x814699a8
Input : GigabitEthernet1
Output : <unknown>
Lapsed time : **3653 ns**

Feature: **IPV4_NAT_INPUT_FIA**
Entry : Input - 0x816999r
Input : GigabitEthernet1
Output : <unknown>
Lapsed time : **303560 ns**

Feature: **IPV4_INPUT_LOOKUP_PROCESS**
Entry : Input - 0x816999a8
Input : GigabitEthernet1
Output : GigabitEthernet2
Lapsed time : **29306 ns**

Route lookup and output interface selection

Feature: **IPV4_INPUT_IPOPTIONS_PROCESS**
Entry : Input - 0x816999a8
Input : GigabitEthernet1
Output : GigabitEthernet2
Lapsed time : **2813 ns**

Feature: **IPV4_INPUT_GOTO_OUTPUT_FEATURE**
Entry : **Input** - 0x8166b2ed
Input : GigabitEthernet2
Output : GigabitEthernet3
Lapsed time : 453 ns

Here, we switch from the input FIA of GigabitEthernet1 to the output FIA of GigabitEthernet2

Feature: **CBUF_OUTPUT_FIA**
Entry : **Output** - 0x8166b1e8
Input : GigabitEthernet2
Output : GigabitEthernet3
Lapsed time : **533 ns**

And now the packet proceeds along the output FIA.

Feature: **IPV4_VFR_REFRAG**
Entry : Output - 0x8166b354
Input : GigabitEthernet2
Output : GigabitEthernet3
Lapsed time : **320 ns**

Feature: **IPV4_OUTPUT_L2_REWRITE**
Entry : Output - 0x8166ad94
Input : GigabitEthernet2
Output : GigabitEthernet3
Lapsed time : **586 ns**

Feature: **IPV4_OUTPUT_QOS**
Entry : Output - 0x8166b2cc
Input : GigabitEthernet2
Output : GigabitEthernet3
Lapsed time : **1866 ns**

Feature: **IPV4_OUTPUT_FRAG**
Entry : Output - 0x8166b33c
Input : GigabitEthernet2
Output : GigabitEthernet3
Lapsed time : **320 ns**

Feature: **IPV4_OUTPUT_DROP_POLICY**
Entry : Output - 0x8166b2d0
Input : GigabitEthernet2
Output : GigabitEthernet3
Lapsed time : **3173 ns**

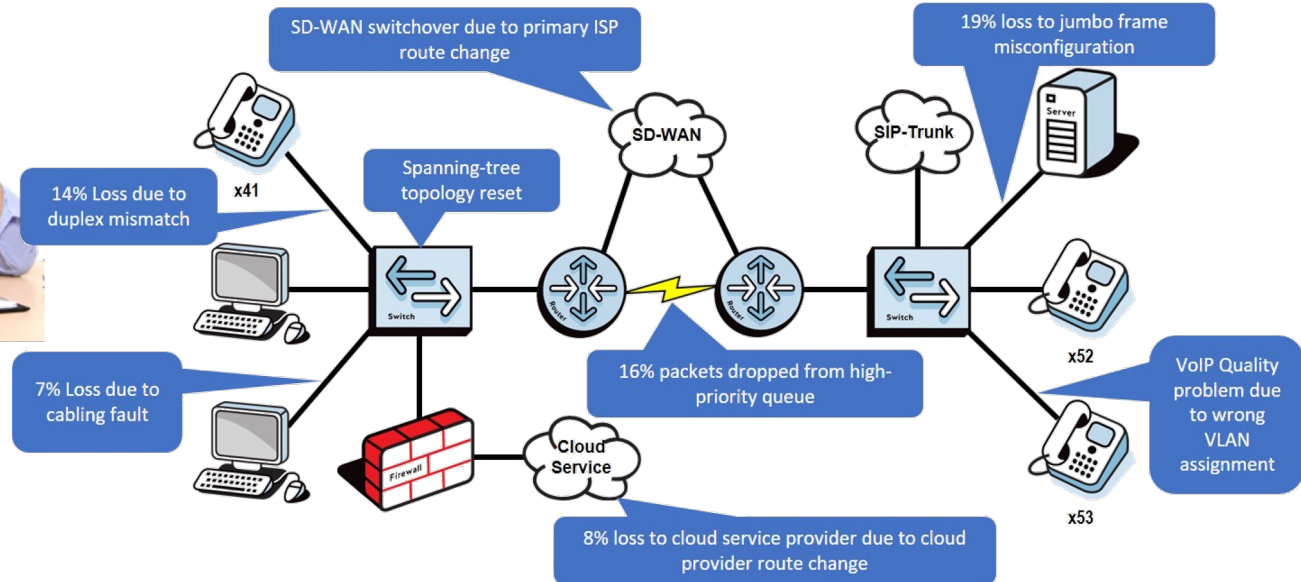
Feature: **DEBUG_COND_OUTPUT_PKT**
Entry : Output - 0x8166b1dc
Input : GigabitEthernet2
Output : GigabitEthernet3
Lapsed time : **346 ns**

Feature: **MARMOT_SPA_D_TRANSMIT_PKT**
Entry : Output - 0x8166b38c
Input : GigabitEthernet2
Output : GigabitEthernet3
Lapsed time : **5280 ns**

Packet Tracing Resources

- Tech Note Article (with examples)
 - <https://www.cisco.com/c/en/us/support/docs/content-networking/adaptive-session-redundancy-asr/117858-technote-asr-00.html>
- Cisco.com (CCO) Documentation
 - https://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/Packet_Trace.html

What is the real issue?

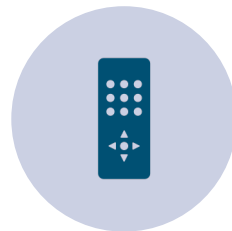


What is RADKit ?

(Remote Automation Development Kit)



RADKit is a Software Development Kit. It frees you from CVE monitoring of dozens of opensource packages.



The included tools allow your NetOps staff to interactively connect to remote terminals, WebUI's or desktops.



Use our powerful and easy to use our efficient and scalable APIs for remote and local automation.

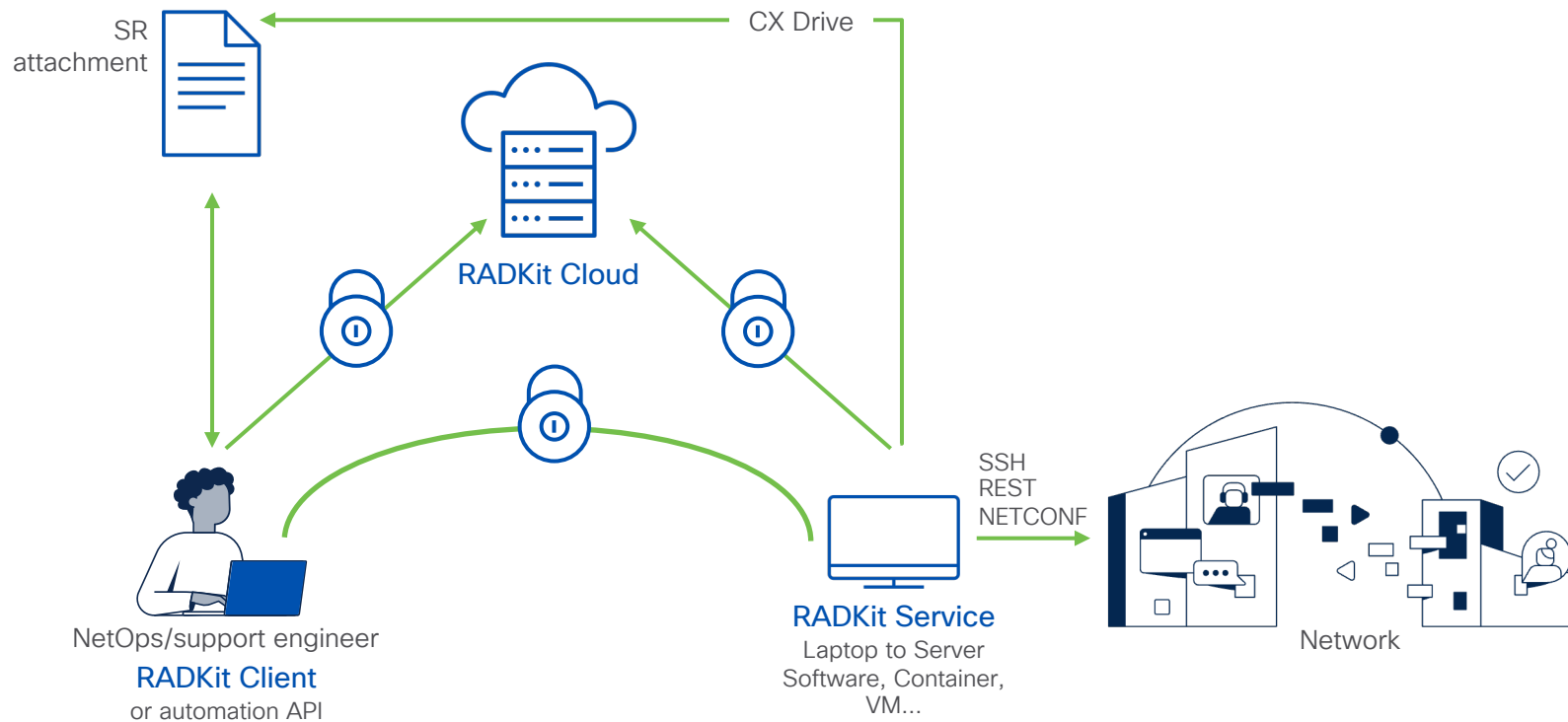


Full-on security with SSO, Certificates, data encryption at rest and in transit, exhaustive audit-logs,...

RADKit enhances all NetOps activities, streamlines incident escalation processes, and more!

RADKit General Architecture

Visit
<https://radkit.cisco.com>



Benefits from start to finish

Automate



Automate frequent or complex tasks

with network-wide API's and tap into SSH, REST, Open API, Netconf/YANG, etc.

Empower



Empower your staff

RADKit API's feature a smooth learning curve purpose-built for scripters and developers.

Secure



More Security, Less Effort

Cisco's Secure Development Lifecycle frees you from CVE monitoring of opensource software.

Simplify



Experience a 10x reduction in process complexity

Focus on your workflows and eliminate busywork.

Features

Human



Reduce barriers to automation

REST/Netconf/YANG
Or tried and true CLI
Easy API for Ops or
Developers

Secure



Simply secure

Secure connections
Authentication, Authorization,
Access Control
Encryption
Audit Trail

Scalable

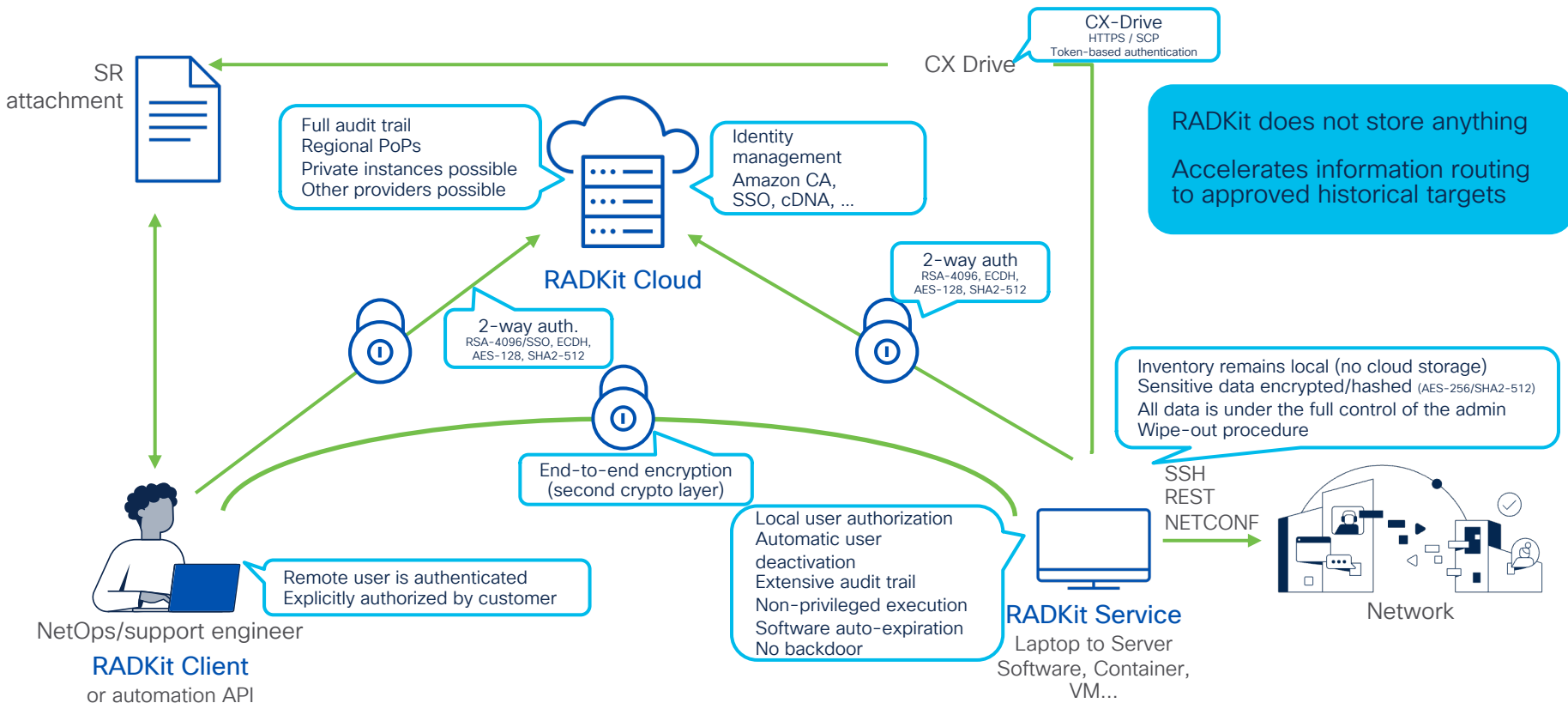


Address networks at scale

Collect data, monitor,
troubleshoot.
Just in time orchestration

Share the data you decide. Not your computer.

RADKit Architecture – Security & Data Privacy

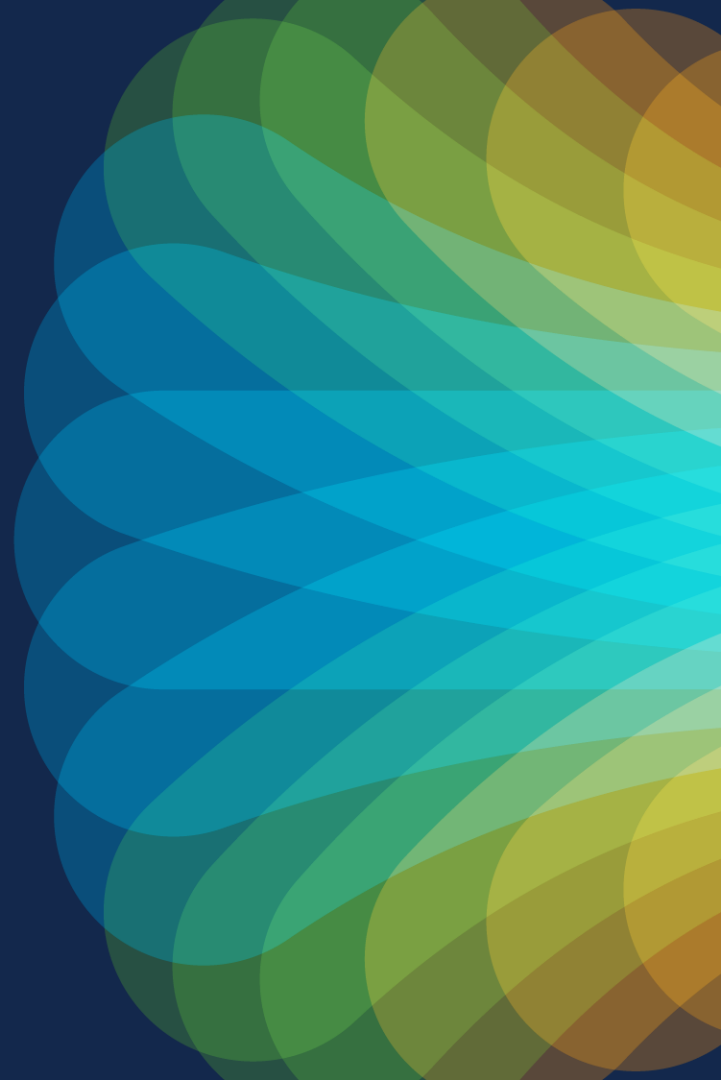


Demo 1 – Radkit and Packet Tracer

RADKit Network Console (EXPERIMENTAL)
Type 'help' to list commands

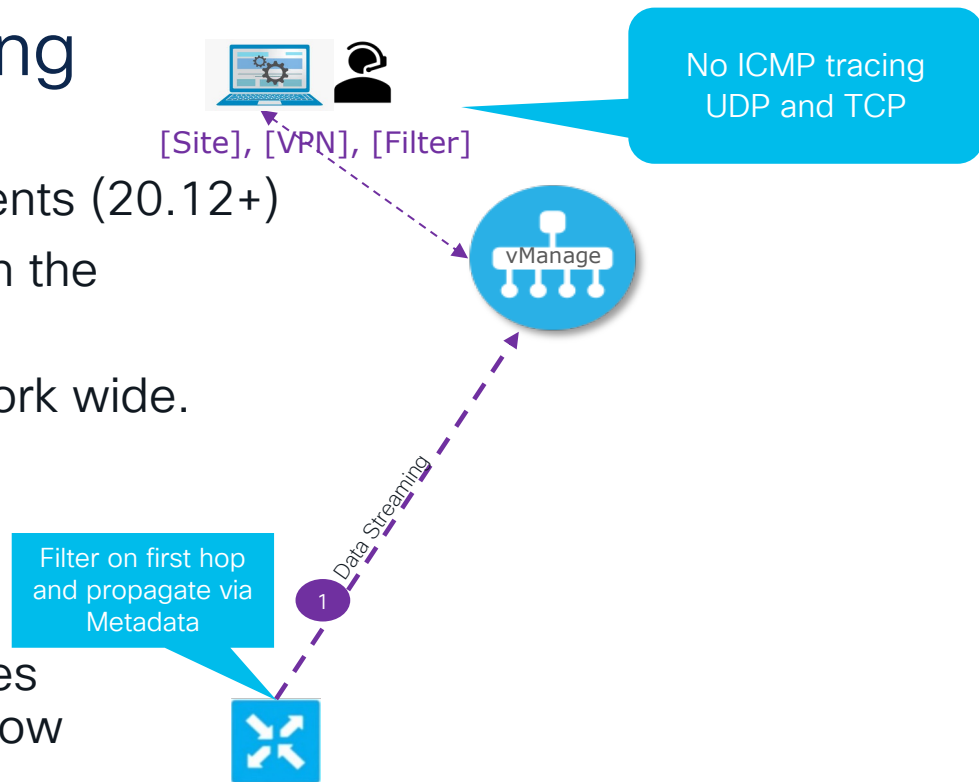
>

Cisco Catalyst SDWAN's Network Wide Path Insight (NWPI)



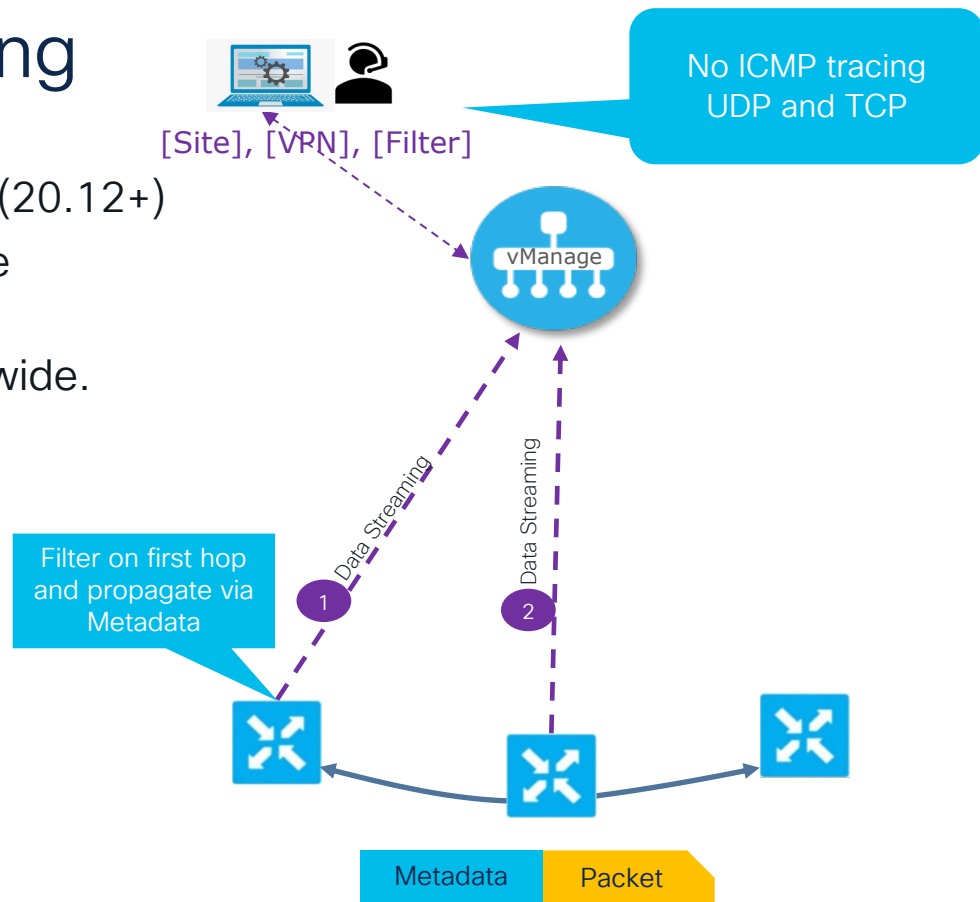
NWPI – Transitive Marking

- Currently works on demand, or events (20.12+)
 - On demand enable filter **ONLY** on the **1st hop router**.
 - No persistent configuration network wide.
- Metadata triggered flow metrics and trace streaming to vManage.
- vManage correlates multiple devices and data sources to visualize per flow **End to End** insight views in UI.



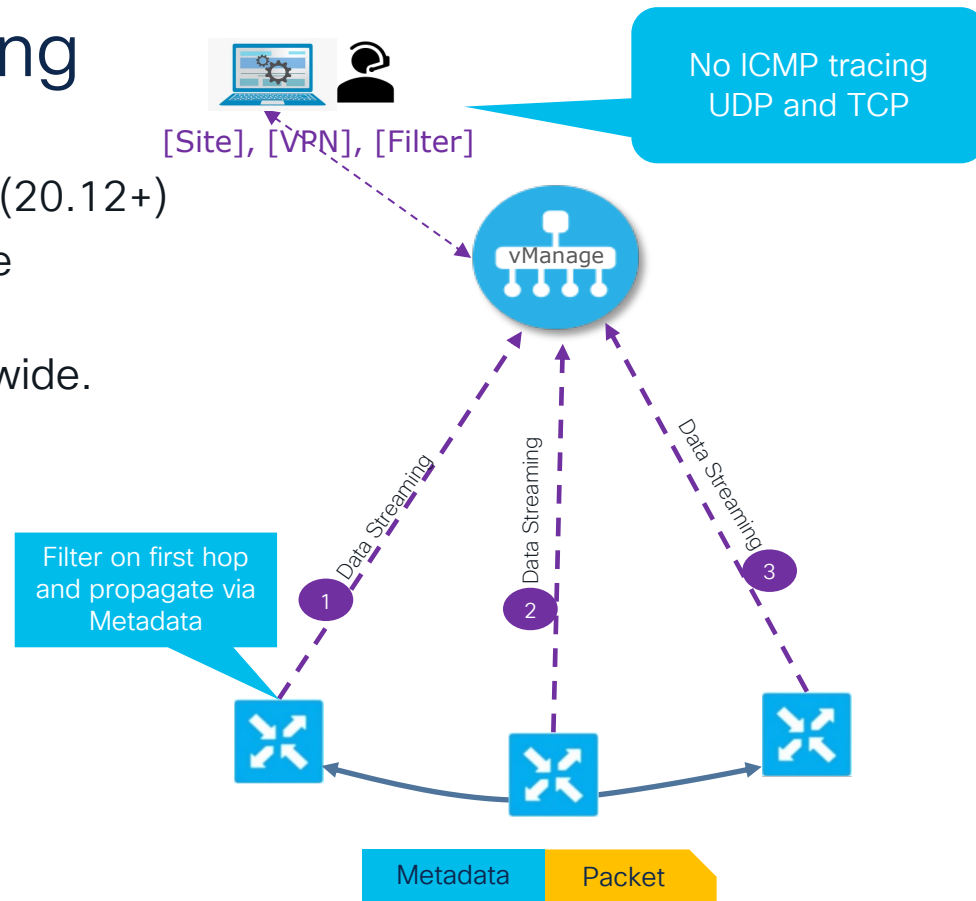
NWPI – Transitive Marking

- Currently works on demand, or events (20.12+)
 - On demand enable filter **ONLY** on the **1st hop router**.
 - No persistent configuration network wide.
- Metadata triggered flow metrics and trace streaming to vManage.
- vManage correlates multiple devices and data sources to visualize per flow **End to End** insight views in UI.

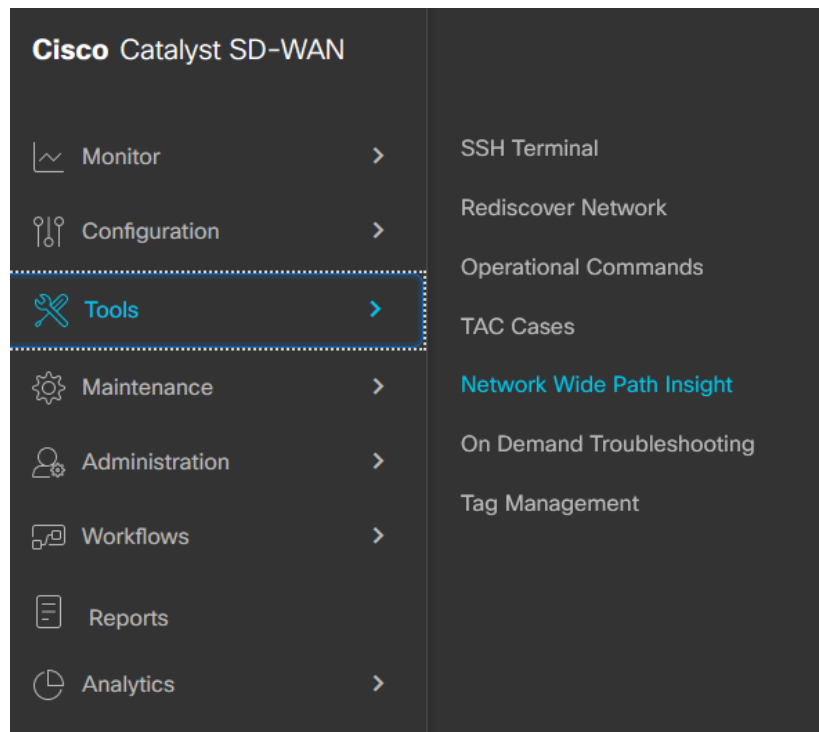


NWPI – Transitive Marking

- Currently works on demand, or events (20.12+)
 - On demand enable filter **ONLY** on the **1st hop router**.
 - No persistent configuration network wide.
- Metadata triggered flow metrics and trace streaming to vManage.
- vManage correlates multiple devices and data sources to visualize per flow **End to End** insight views in UI.



Navigating to NWPI



Navigating to NWPI

The screenshot displays the Cisco Catalyst SD-WAN Network Wide Path Insight (NWPI) interface. The top navigation bar includes the Cisco Catalyst SD-WAN logo, a 'Select Resource Group' dropdown, and the title 'Tools · Network Wide Path Insight'. The breadcrumb trail shows 'Overview > Troubleshooting > Network Wide Path Insight'. The main section is titled 'TRACE' and contains two buttons: 'New Trace' and 'New Auto-on Task'. Below these buttons are tabs for 'All Trace' (selected) and 'Auto-On Task'. A search bar labeled 'Search Table' is present. The table header includes columns: Trace Name, Trace ID, Start Time, Stop Time, Src. Site, VPN ID, Application/App Group, Domain, Trace State, and Action. The table body is currently empty, displaying 'No data available'. The footer of the table section shows '0 Record' and pagination controls. The bottom section is titled 'INSIGHT' and contains tabs for 'DNS Domains' (selected), 'Applications', 'Active Flows', and 'Completed Flows'. A 'Filter' dropdown is located below the tabs. At the bottom, there are two buttons: 'Discovered Domains' and 'Monitored Domains'. A vertical 'Feedback' button is located on the right side of the interface.

Tools · Network Wide Path Insight

Overview > Troubleshooting > Network Wide Path Insight

TRACE

New Trace New Auto-on Task

How to Get Started | FAQ | Administration Setting

Please click "View Insight" to load data for "INSIGHT".

All Trace Auto-On Task

Search Table

0 selected Insight Summary As of: Oct 16, 2023 02:29 PM

Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain	Trace State	Action
No data available									

0 Record Items per page: 5 0 of 0

INSIGHT

DNS Domains Applications Active Flows Completed Flows

Filter

Discovered Domains Monitored Domains

Setting a
condition –
activate tracing
[without DNS
discovery]

Create new trace

The screenshot displays the Cisco Catalyst SD-WAN Network Wide Path Insight interface. The top navigation bar includes the Cisco Catalyst SD-WAN logo, a 'Select Resource Group' dropdown, and the title 'Tools · Network Wide Path Insight'. Below the navigation bar, the breadcrumb trail shows 'Overview > Troubleshooting > Network Wide Path Insight'. The main content area is divided into two sections: 'TRACE' and 'INSIGHT'. The 'TRACE' section is currently active and contains two buttons: 'New Trace' and 'New Auto-on Task'. An arrow points from the text 'DNS discovery is covered later in the presentation' to the 'New Trace' button. Below the buttons, there are tabs for 'All Trace' and 'Auto-On Task'. A search bar labeled 'Search Table' is present. Below the search bar, there is a table with columns: Trace Name, Trace ID, Start Time, Stop Time, Src. Site, VPN ID, Application/App Group, Domain, Trace State, and Action. The table currently shows 'No data available'. At the bottom of the table, it indicates '0 Record' and 'Items per page: 5'. The 'INSIGHT' section is partially visible below the 'TRACE' section, showing tabs for 'DNS Domains', 'Applications', 'Active Flows', and 'Completed Flows'. The 'DNS Domains' tab is selected, and there is a 'Filter' dropdown. At the bottom of the 'INSIGHT' section, there are two buttons: 'Discovered Domains' and 'Monitored Domains'.

Tools · Network Wide Path Insight

Overview > Troubleshooting > Network Wide Path Insight

TRACE

New Trace New Auto-on Task

DNS discovery is covered later in the presentation

How to Get Started | FAQ | Administration Setting

Please click "View Insight" to load data for "INSIGHT".

All Trace Auto-On Task

Search Table

0 selected Insight Summary As of: Oct 17, 2023 03:11 PM

Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain	Trace State	Action
No data available									

0 Record Items per page: 5 0 of 0

INSIGHT

DNS Domains Applications Active Flows Completed Flows

Filter

Discovered Domains Monitored Domains

Create new trace

Cisco Catalyst SD-WAN Select Resource Group Tools · Network Wide Path Insight

Overview > Troubleshooting > Network Wide Path Insight

TRACE

TRACE

Mandatory

Optional

Optional

[New Trace](#) ☐ Enable DNS Domain Discovery ⓘ

Trace Name: Trace Duration (minutes): Default: 60

Filters:

Site ID(*) VPN(*) Source Address/Prefix: ⓘ Destination Address/Prefix: ⓘ Application ⓘ Application Group ⓘ

e.g v4: 10.0.0.0/8 or v6: 2001:0:0:1::/64 e.g v4: 10.0.0.0/8 or v6: 2001:0:0:1::/64 Select one or more applications

Advanced Filters: >

Monitor Settings: >

Start Cancel

Search

Discovered Domains Monitored Domains

Create new trace (Optional aspects)

The screenshot shows the 'New Trace' configuration page in the Cisco Catalyst SD-WAN Network Wide Path Insight interface. The page is titled 'TRACE' and has two tabs: 'New Trace' (active) and 'New Auto-on Task'. It includes a 'Feedback' button on the right side.

Configuration Fields:

- ☐ Enable DNS Domain Discovery ⓘ
- Trace Name:
- Trace Duration (minutes):
- Filters:**
 - Site ID(*), branch site only:
 - VPN(*):
 - Source Address/Prefix: ⓘ
 - Destination Address/Prefix: ⓘ
 - ☒ Application ⓘ ☐ Application Group
 - Select one or more applications:
- Advanced Filters:** ⌵
 - Device:
 - Source Interface:
 - Source Port:
 - Destination Port:
 - Protocol:
 - DSCP:
- Monitor Settings:** ⌵
 - ☒ QoS Insight ⓘ
 - ☒ ART Visibility ⓘ
 - ☒ APP Visibility ⓘ
 - ☐ DIA Visibility ⓘ
 - ☐ WAN Visibility ⓘ
 - ☐ Sampling ⓘ
 - Local Drop Rate Threshold(%):
 - Wan Loss Rate Threshold(%):
- Synthetic Traffic:** ⌵
 - URL(*):
 - VPN(*):
 - DNS Server:
 - DSCP(*):
 - Interval(minute):

Buttons: 'New Trace', 'New Auto-on Task', and a 'Save' button at the bottom right.

- DIA
- Synthetic Traffic (more later)

Activate tracing

Cisco SD-WAN Select Resource Group Tools · Network Wide Path Insight

TRACE

New Trace ☐ Enable DNS Domain Discovery [How to Get Started](#) | [FAQ](#)
Please click 'View Insight' to load data for 'INSIGHT'.

Trace Name: Trace Duration (minutes):
Default: 60

Filters:
Site ID(*): VPN(*): Source Address/Prefix: Destination Address/Prefix: ☒ Application ☐ Application Group
12 VPN - 1 192.168.12.220/32 e.g v4: 10.0.0.0/8 or v6: 2001:0:0:1::/64 Select one or more applications

Advanced Filters: >
Monitor Settings: >

Start **Cancel**

Discovered Domains Monitored Domains

Search

0 Rows Selected

Total Rows: 0

>	☐ Domain	Update Time	Application	App Group	DNS Server	DNS Redirect	Resolved IP	DNS Transport	DNS Egress	TTL(sec)	Request	Monitor State
---	---------------------------------	-------------	-------------	-----------	------------	--------------	-------------	---------------	------------	----------	---------	---------------

Activate tracing

Tracing and metadata marking
enabled only on 1 device

Start Trace

Trace id: 880
Start Time: Wed Aug 24 2022 11:28:28 GMT+0200 (Central European Summer Time)
Source Site: 12
***** Device List *****
Device IP: 172.16.255.12
Status: success
Message: Trace Starting

Close

Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group
No data available							

First look at the tracing results

Active flows

INSIGHT Selected trace: trace_880 (Trace Id: 880)

Applications **Active Flows** Completed Flows

Please expand a flow/domain to load data for 'INSIGHT - ADVANCED VIEWS'.

Search by Domain, Application, Readout, etc. ⓘ

* Readout Legend: ❌ - Error, ⚠️ - Warning, ✅ - Information.

Search

Total Rows: 2

>	Start - Update Time	Flow Id	Readout *	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	ART CND(ms)/SND(ms)
>	11:28:51 AM-11:28:51 AM	1	⚠️	192.168.12.220	40564	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	N/A
>	11:28:51 AM-11:28:51 AM	2	⚠️	192.168.12.220	45044	52.97.144.178	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	Unknown	N/A

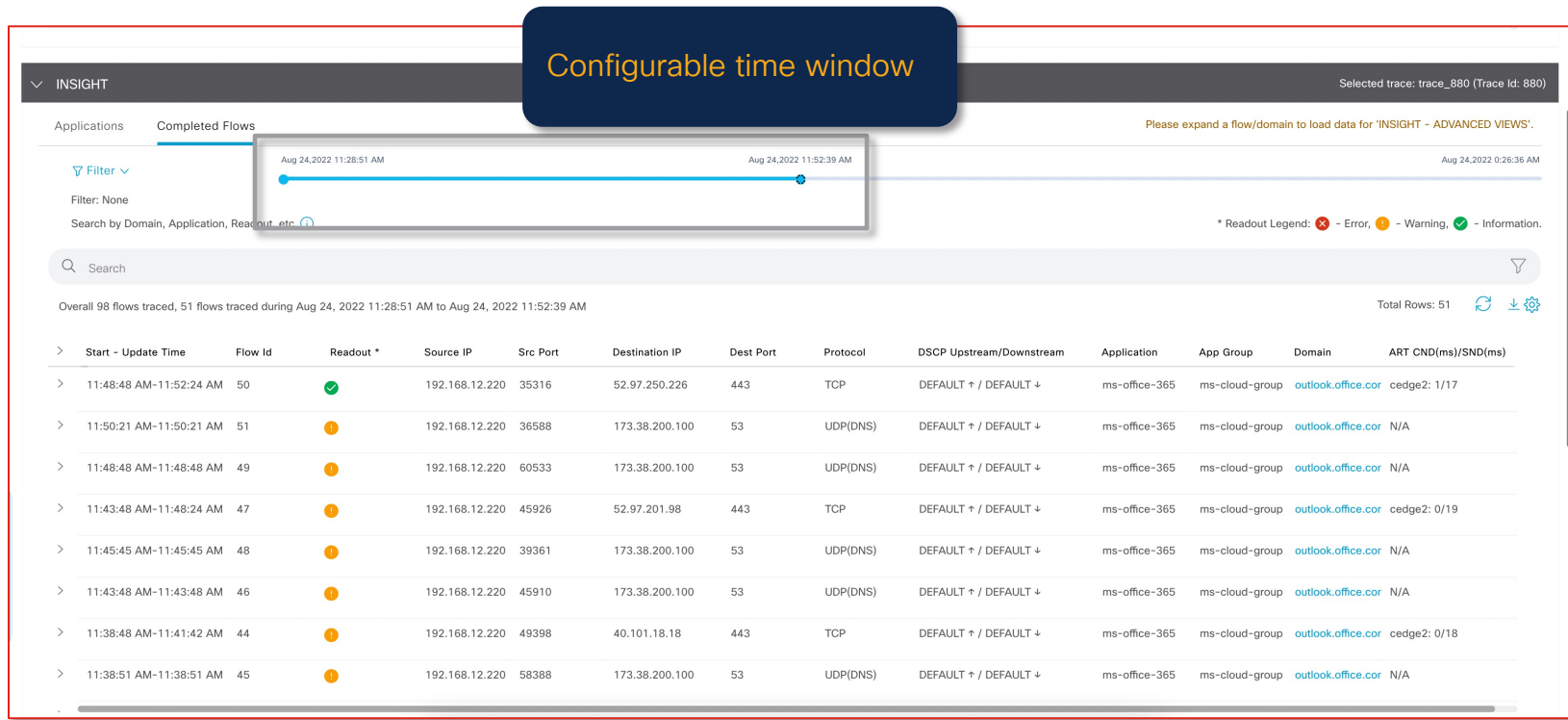
Flow readout

Green: Undamaged symmetric flow

Yellow: Deviation from green (eg flow asymmetry / color mismatch / ...)

Red: Damaged flow

Completed flows



Applications

INSIGHT

Selected trace: trace_880 (Trace Id: 880)

Applications

Active Flows

Completed Flows

Please expand a flow/domain to load data for 'INSIGHT - ADVANCED VIEWS'.

Search by Domain, Application, Readout, etc.

Search

Total Rows: 3

>	Last Update Time	App Name	App Group	Upstream Flow Count	Downstream Flow Count	Upstream Bytes(K)	Downstream Bytes(K)
>	24 Aug 2022 11:32:42 AM CEST	ms-office-365	ms-cloud-group	2	2	8.11	9.29
>	24 Aug 2022 11:32:42 AM CEST	ssl	other	6	6	12.55	7.17
>	24 Aug 2022 11:32:42 AM CEST	ms-office-web-apps	ms-cloud-group	1	1	0	0

Classification by app name or groups
Downstream / upstream bandwidth

Deeper in NWPI tracing: Flow analysis



Flow analysis

Expand by clicking on arrow

>	Start - Update Time	Flow Id	Readout *	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	ART CND(ms)/SND(ms)			
▼	0:54:44 AM-0:54:59 AM	24	🟡	192.168.12.220	51714	10.48.66.216	80	TCP	DEFAULT ↑ / DEFAULT ↓	http	other	Unknown	cedge2: 0/2			
	Direction	HopIndex	Local Edge	Remote Edge	Local Color	Remote Color	Local Drop(%)	Wan Loss(%)	Remote Drop(%)	Jitter(ms)	Latency(ms)	ART CND(ms)/SND(ms)	Total Packets	Total Bytes	Queue Id	QDepth Limit/Max /Min/Avg
	Upstream	0	(Gi2) cedge2	cedge7	BIZ_INTERNET	BIZ_INTERNET	0.67	N/A	0.00	< 1	1	cedge2: 0/2	25544	1687884	2	64/0/0/0
	Upstream	1	cedge7 (Gi3)	Internet	BIZ_INTERNET (NAT_DIA)	N/A	0.00	N/A	N/A	N/A	N/A	cedge7: 1/0	25373	2793010	N/A	N/A
	Downstream	0	Internet	(Gi3)cedge7	N/A	BIZ_INTERNET (NAT_DIA)	N/A	N/A	0.00	N/A	N/A	N/A	157904	217016502	N/A	N/A
>	0:53:23 AM-0:54:32 AM	22	🟢	192.168.12.220	60140	52.97.179.194	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	cedge2: 0/19			

DROPS!

Traffic volume
QOS information

Flow analysis

Expand by clicking on arrow

Drop Details

Drop Cause Details:

=====

FirewallL7: 2 packets

Start - Upstream

Direction

Upstream

Upstream

Downstream

0:54:44 AM

0:53:23 AM

Total Rows: 2

ND(ms)

/Max

Flow analysis – readout

Expand by clicking on arrow

>	Start - Update Time	Flow Id	Readout *	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream		Application	App Group	Domain	ART CND(ms)/SND(ms)		
√	0:54:44 AM-0:54:59 AM	24		192.168.12.220	51714	10.48.66.216	80	TCP	DEFAULT ↑ / DEFAULT ↓		http	other	Unknown	cedge2: 0/2		
	Direction	HopIndex	Local Edge	Remote Edge	Local Color	Remote Color	Local Drop(%)	Wan Loss(%)	Remote Drop(%)	Jitter(ms)	Latency(ms)	ART CND(ms)/SND(ms)	Total Packets	Total Bytes	Queue Id	QDepth Limit/Max /Min/Avg
	Upstream	0	(Gi2) cedge2	cedge7	BIZ_INTERNET	BIZ_INTERNET	0.67	N/A	0.00	< 1	1	cedge2: 0/2	25544	1687884	2	64/0/0/0
	Upstream	1	cedge7 (Gi3)	Internet	BIZ_INTERNET (NAT_DIA)	N/A	0.00	N/A	N/A	N/A	N/A	cedge7: 1/0	25373	2793010	N/A	N/A
	Downstream	0	Internet	(Gi3)cedge7	N/A	BIZ_INTERNET (NAT_DIA)	N/A	N/A	0.00	N/A	N/A	N/A	157904	217016502	N/A	N/A
>	0:53:23 AM-0:54:32 AM	22		192.168.12.220	60140	52.97.179.194	443	TCP	DEFAULT ↑ / DEFAULT ↓		ms-office-365	ms-cloud-group	outlook.office.cor	cedge2: 0/19		

Traffic volume
QOS information

Flow analysis – readout

Expand by clicking on an

Flow Readout

Overview

Path Insight

Trace: trace_896 (ID: 896), Flow ID: 124 (Application:ms-office-365)

Upstream From 192.168.12.220:59746 to 40.101.18.18:443

Downstream From 40.101.18.18:443 to 192.168.12.220:59746

Overall Status

✓ Flow TCP RESET: Yes
24/8/2022, 13:52:08, downstream TCP RESET on cedge7

✓ NAT Translation: Yes
* Upstream hop(cege7 (Gi3) -> NAT_DIA:GigabitEthernet3)
Translate Source:
pre-nat: 192.168.12.220, port: 59746
post-nat: 172.16.17.254, port: 5063
* Downstream hop(NAT_DIA -> (Gi3)cege7)
Translate Destination:
pre-nat: 172.16.17.254, port: 5063
post-nat: 192.168.12.220, port: 59746

● WAN Color Inconsistency: Yes
* Downstream hop(cege7:BIZ_INTERNET -> cedge2(Gi2) :BIZ_INTERNET)
cege7:
Egress Color: BIZ_INTERNET,
Ingress Color: MPLS

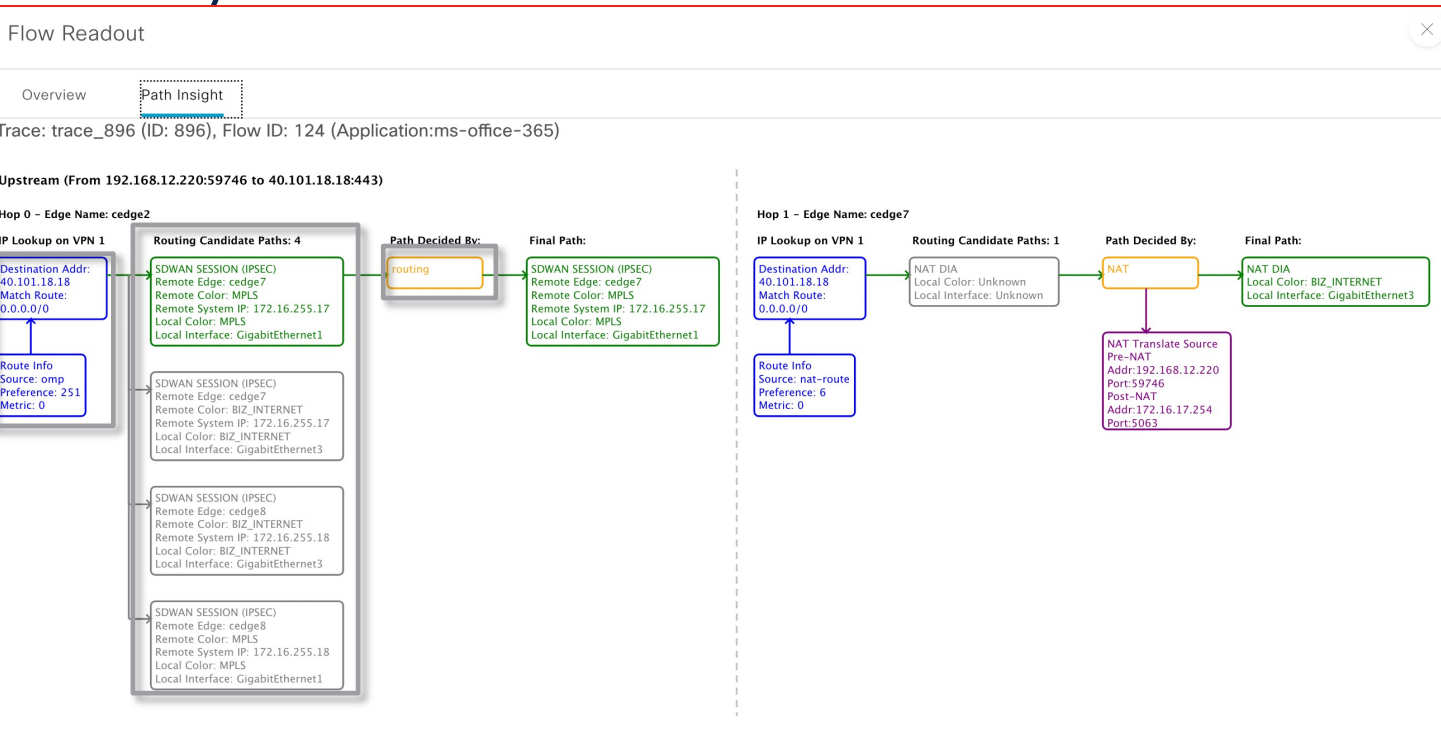
Total Rows: 2

Application	App Group	Domain	ART CND(ms)/SND(ms)	
	other	Unknown	cege2: 0/2	
D(ms)	Total Packets	Total Bytes	Queue Id	QDepth Limit/Max /Min/Avg
	25544	1687884	2	64/0/0/0
	25373	2793010	N/A	N/A
	157904	217016502	N/A	N/A
office-365	ms-cloud-group	outlook.office.cor	cege2: 0/19	

Traffic volume
QOS information

Flow analysis - readout

Expand by c



Total Rows: 2

ART CND(ms)/SND(ms)

cedge2: 0/2

QDepth Limit/Max /Min/Avg

64/0/0/0

N/A

N/A

cedge2: 0/19

me
nation

Flow analysis – Going deeper in router processing

The screenshot displays the Cisco INSIGHT flow analysis interface. The top section shows a list of flows with columns for Start - Update Time, Flow Id, Readout, Source IP, Src Port, Destination IP, Dest Port, Protocol, DSCP Upstream/Downstream, Application, App Group, Domain, and ART CND(ms)/SND(ms). A blue callout box with the text "Expand by clicking on arrow" points to the expand icon in the first row of the flow list.

Below the flow list, a detailed view of a specific flow is shown. This view is divided into two main sections: "Upstream Feature" and "Downstream Feature". The "Upstream Feature" section includes a table with columns for Direction, HopIndex, Local Edge, Remote Edge, Local Color, Remote Color, Local Drop(%), Wan Loss(%), Remote Drop(%), Jitter(ms), Latency(ms), ART CND(ms)/SND(ms), Total Packets, Total Bytes, Queue Id, and QDepth Limit/Max/Min/Avrg. The "Downstream Feature" section includes a table with columns for Ingress Feature and Egress Feature. A blue callout box with the text "Advanced view analysis" points to the "Upstream Feature" section.

The interface also includes a search bar, a filter dropdown, and a legend for Readout status (Error, Warning, Information). The bottom section shows the "INSIGHT - ADVANCED VIEWS" tab, which includes a "Flow Trend" section and a "Geography" section.

Flow analysis – Upstream router(s) processing

Flow Trend **Upstream Feature** Downstream Feature Geography

Hostname: cedge2 Event List: FIRST_PACKET/DPL_DONE Expand All Features

Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3

Ingress Feature	Egress Feature
<ul style="list-style-type: none">> Ingress Report> CEF Forwarding> SDWAN ACL IN >> View Policy <<> NBAR> SDWAN App Route Policy >> View Policy <<> SDWAN Forwarding	<ul style="list-style-type: none">> NBAR> IPSec> SDWAN QoS Output> QOS >> View Policy <<> Transmit Report

Ingress feature processing on first upstream router

Egress feature processing on first upstream router



Hostname: cedge7 Event List: FIRST_PACKET/DPL_DONE Expand All Features

Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet3

Ingress Feature	Egress Feature
<ul style="list-style-type: none">> SDWAN Forwarding> CEF Forwarding> NBAR> SDWAN Data Policy OUT >> View Policy <<> NBAR	<ul style="list-style-type: none">> UTD Policy (First FIA)> ZBFW >> View Policy <<> ZBFW >> View Policy <<> CFT> NAT> Transmit Report

Ingress feature processing on last upstream router

Egress feature processing on last upstream router

Flow analysis – Upstream router(s) processing

The screenshot displays the Cisco Flow Analysis tool interface, showing the 'Upstream Feature' tab selected. The interface is divided into two main panels, one for Hostname: cedge2 and one for Hostname: cedge7. Each panel has a top navigation bar with 'Flow Trend', 'Upstream Feature', 'Downstream Feature', and 'Geography'. Below the navigation bar, there's a header section with 'Hostname: cedge2' and 'Event List: FIRST_PACKET/DPL_DONE' for the left panel, and 'Hostname: cedge7' and 'Event List: FIRST_PACKET/DPL_DONE' for the right panel. Both panels have a version string: 'Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3'. The main content area is split into two columns: 'Ingress Feature' (blue background) and 'Egress Feature' (green background). An arrow points from the 'Ingress Feature' column of cedge2 to the 'Ingress Feature' column of cedge7. Below each panel, there are two dark blue rounded rectangles with yellow text. For cedge2, the text reads 'Ingress feature processing on first upstream router' and 'Egress feature processing on first upstream router'. For cedge7, the text reads 'Ingress feature processing on last upstream router' and 'Egress feature processing on last upstream router'. The 'Ingress Feature' list for cedge2 includes: Ingress Report, CEF Forwarding, SDWAN ACL IN, NBAR, SDWAN App Route Policy, and SDWAN Forwarding. The 'Egress Feature' list for cedge2 includes: NBAR, IPSec, SDWAN QoS Output, QOS, and Transmit Report. The 'Ingress Feature' list for cedge7 includes: SDWAN Forwarding, CEF Forwarding, NBAR, SDWAN Data Policy OUT, and NBAR. The 'Egress Feature' list for cedge7 includes: UTD Policy (First FIA), ZBFW, CFT, NAT, and Transmit Report.

Flow Trend **Upstream Feature** Downstream Feature Geography

Hostname: cedge2 Event List: FIRST_PACKET/DPL_DONE Expand All Features
Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3

Ingress Feature

- > Ingress Report
- > CEF Forwarding
- > SDWAN ACL IN >> View Policy <<
- > NBAR
- > SDWAN App Route Policy >> View Policy <<
- > SDWAN Forwarding

Egress Feature

- > NBAR
- > IPSec
- > SDWAN QoS Output
- > QOS >> View Policy <<
- > Transmit Report

Hostname: cedge7 Event List: FIRST_PACKET/DPL_DONE Expand All Features
Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet3

Ingress Feature

- > SDWAN Forwarding
- > CEF Forwarding
- > NBAR
- > SDWAN Data Policy OUT >> View Policy <<
- > NBAR

Egress Feature

- > UTD Policy (First FIA)
- > ZBFW >> View Policy <<
- > ZBFW >> View Policy <<
- > CFT
- > NAT
- > Transmit Report

Ingress feature processing on first upstream router

Egress feature processing on first upstream router

Ingress feature processing on last upstream router

Egress feature processing on last upstream router

Flow analysis – Upstream router(s) processing – Checking policy sequence

Flow Trend **Upstream Feature** Downstream Feature Geography

Hostname: cedge2 Event List: FIRST_PACKET/DPL_DONE Expand All Features

Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3

Ingress Feature	Egress Feature
<ul style="list-style-type: none">> Ingress Report> CEF Forwarding> SDWAN ACL IN >> View Policy <<> NBAR> SDWAN App Route Policy >> View Policy <<> SDWAN Forwarding	<ul style="list-style-type: none">> NBAR> IPSec> SDWAN QoS Output> QOS >> View Policy <<> Transmit Report

Ingress feature processing on first upstream router

Egress feature processing on first upstream router



Hostname: cedge7 Event List: FIRST_PACKET/DPL_DONE Expand All Features

Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet3

Ingress Feature	Egress Feature
<ul style="list-style-type: none">> SDWAN Forwarding> CEF Forwarding> NBAR> SDWAN Data Policy OUT >> View Policy <<> NBAR	<ul style="list-style-type: none">> UTD Policy (First FIA)> ZBFW >> View Policy <<> ZBFW >> View Policy <<> CFT> NAT> Transmit Report

Ingress feature processing on last upstream router

Egress feature processing on last upstream router

Flow analysis – Upstream router(s) processing – Checking policy sequence

Flow Trend **Upstream Feature** Downstream Feature Geography

Hostname: cedge2 Event List: FIRST_PACKET/DPL_DONE Expand All Features

Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3

Ingress Feature	Egress Feature
<ul style="list-style-type: none">> Ingress Report> CEF Forwarding> SDWAN ACL IN >> View Policy <<> NBAR> SDWAN App Route Policy >> View Policy <<> SDWAN Forwarding	<ul style="list-style-type: none">> NBAR> IPSec> SDWAN QoS Output> QOS >> View Policy <<> Transmit Report

Ingress feature processing on first upstream router

Egress feature processing on first upstream router



Hostname: cedge7 Event List: FIRST_PACKET/DPL_DONE Expand All Features

Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet3

Ingress Feature	Egress Feature
<ul style="list-style-type: none">> SDWAN Forwarding> CEF Forwarding> NBAR> SDWAN Data Policy OUT >> View Policy <<> NBAR	<ul style="list-style-type: none">> UTD Policy (First FIA)> ZBFW >> View Policy <<> ZBFW >> View Policy <<> CFT> NAT> Transmit Report

Ingress feature processing on last upstream router

Egress feature processing on last upstream router

Flow analysis – Upstream router(s) processing – Checking policy sequence

The screenshot displays the Cisco Flow Analyzer interface for two upstream routers, cedge2 and cedge7. The 'Upstream Feature' tab is selected, showing the flow processing sequence. The interface is divided into Ingress and Egress feature sections. A callout box highlights the 'SDWAN Data Policy OUT' policy, showing its configuration details. Blue arrows indicate the flow from the Ingress Report to the Policy Name and then to the Seq field. Below the interface, four dark blue callout boxes describe the processing stages: Ingress feature processing on first upstream router, Egress feature processing on first upstream router, processing on last upstream router, and Egress feature processing on last upstream router.

Flow Trend **Upstream Feature** Downstream Feature Geography

Hostname: cedge2 Event List: FIRST_PACKET/DPL_DONE Expand All Features
Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3

Hostname: cedge7 Event List: FIRST_PACKET/DPL_DONE Expand All Features
Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet3

Ingress Feature **Egress Feature**

Ingress Report

- > CEF Forwarding
- > SDWAN ACL IN >> View Policy <<
- > NBAR
- > SDWAN App Route Policy >> View Policy <<
- > SDWAN Forwarding

Egress Feature

- > NBAR
- > IPSec
- > SDWAN QoS Output
- > QOS >> View Policy <<
- > Transmit Report

SDWAN Data Policy OUT >> View Policy <<

VPN ID : 1
VRF : 1
Policy Name : _VPN_1_protect-site7-8-VPN_1 (CG:2)
Seq : Default
DNS Flags : (0x8) NONE
Policy Flags : 8x10000
Nat Map ID : 148
SNG ID : 129

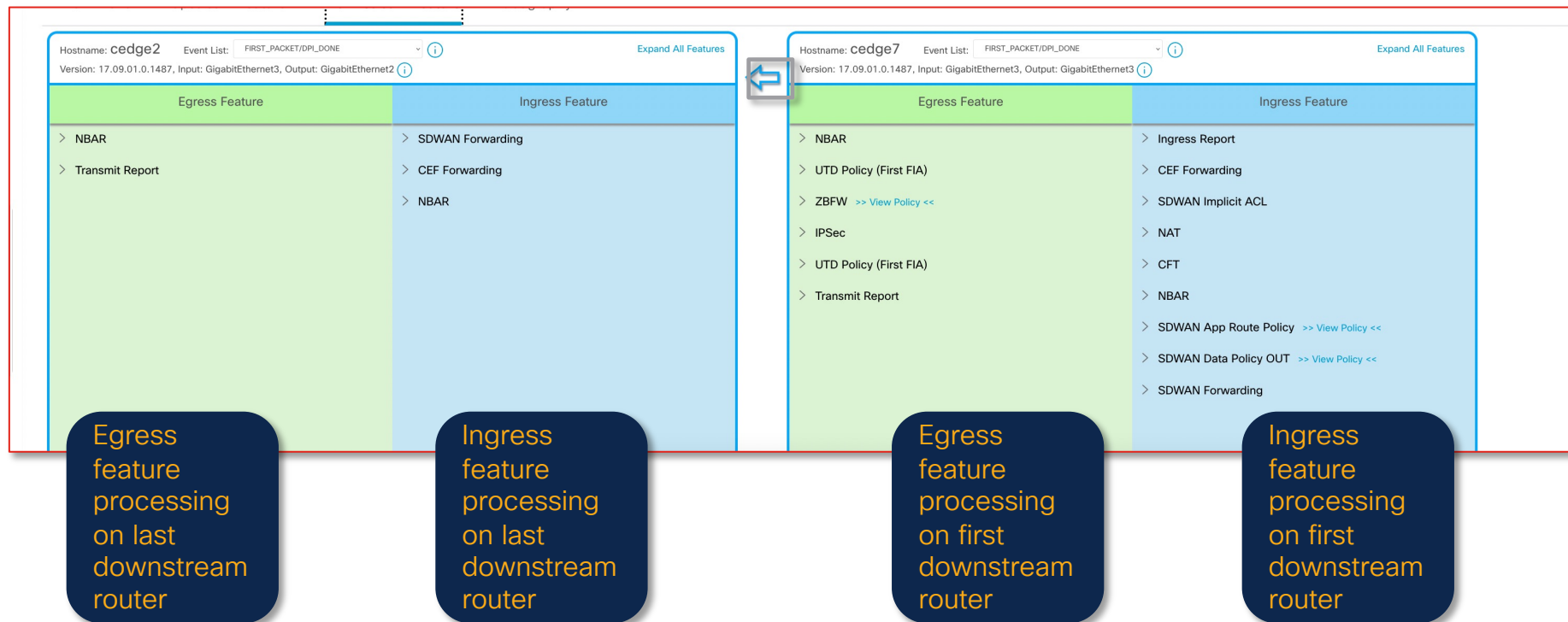
Ingress feature processing on first upstream router

Egress feature processing on first upstream router

processing on last upstream router

Egress feature processing on last upstream router

Flow analysis – Downstream router(s) processing



Flow analysis – Policy analysis

The image displays two side-by-side screenshots of the Cisco Flow Analysis tool interface, showing policy analysis for two different hosts: cedge2 and cedge7. Both panels show a top header with the hostname, event list (FIRST_PACKET/DPL_DONE), and version information (17.09.01.0.1487). The left panel (cedge2) shows Egress features (NBAR, Transmit Report) and Ingress features (SDWAN Forwarding, CEF Forwarding, NBAR). The right panel (cedge7) shows Egress features (NBAR, UTD Policy (First FIA), ZBFW, IPSec, UTD Policy (First FIA), Transmit Report) and Ingress features (Ingress Report, CEF Forwarding, SDWAN Implicit ACL, NAT, CFT, NBAR, SDWAN App Route Policy, SDWAN Data Policy OUT, SDWAN Forwarding). A blue arrow points from the right panel to the left panel. In the right panel, the ZBFW feature has a link '>> View Policy <<' and the SDWAN App Route Policy and SDWAN Data Policy OUT features also have links '>> View Policy <<'.

Flow analysis – Policy analysis

ZBFW

```
name:To_Internet_copy_2
type:zoneBasedFW
description:Description
isActiveedByVsmart:false
zones:
  sourceZone:1      vpn: 1
  destinationZone:Internet      vpn: 0

sequences:
  sequenceId: 1
  sequenceType: zoneBasedFW
  baseAction: inspect
  sequenceType N/A
  match sourceDataPrefixList LAN
    prefixes: 192.168.0.0/16
  match appList Internet-apps
    app: N/A
    app: gtalk
    app: gtalk-chat
    app: google-services
    app: google-plus
    app: google-earth
    app: google-docs
  sequenceId: 11
  sequenceType: zoneBasedFW
  baseAction: drop
  sequenceType N/A
  match sourceDataPrefixList LAN
    prefixes: 192.168.0.0/16
  match destinationPort 22
  match protocol 6
  sequenceId: 21
```

Close

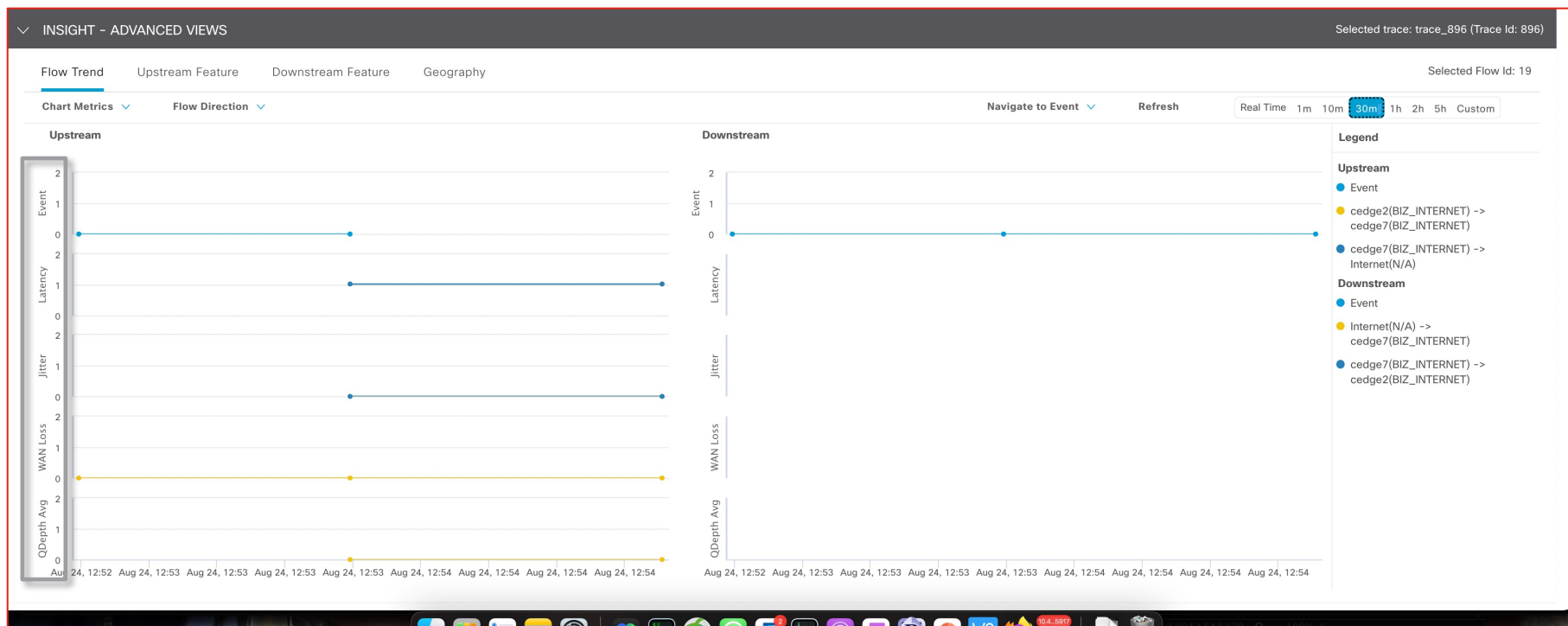
SDWAN App Route Policy

```
name:web-ssh-AAR
type:appRoute
description:web-ssh-AAR
isActiveedByVsmart:true
sequences:
  sequenceId: 1
  sequenceType: appRoute
  sequenceType ipv4
  match appList SSH_policy
  apps: sshell
  action
    slaClass:TEST1
    latency:100
    loss:10
    jitter:10
    preferredColor biz-internet
  sequenceId: 11
  sequenceType: appRoute
  sequenceType ipv4
  match appList web_services
  appFamily: instant-messaging
  action
    slaClass:TEST1
    latency:100
    loss:10
    jitter:10
    preferredColor biz-internet
```

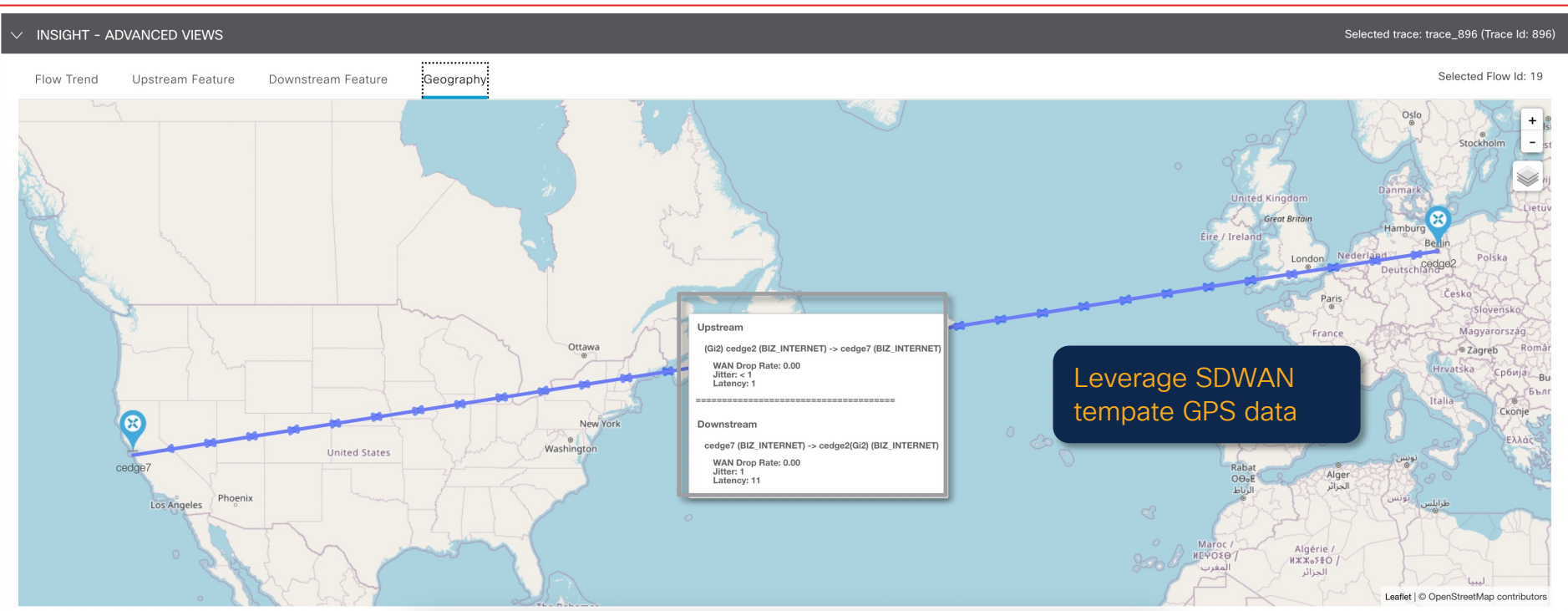
* The latency Configured in the App-Route policy is RTT Round-Trip-Delay and the latency of each hop in the flow table is One-Way-Delay.

Close

Flow analysis – Flow trends



Flow analysis – Geography



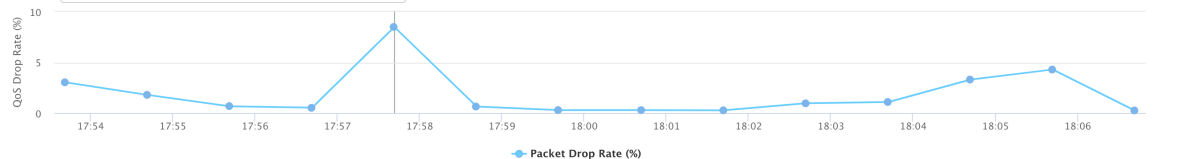
Insight summary – integrated view

Insight Summary – QoS Insight

Overview App Performance Insight Event Insight QoS Insight

Trace: alanwan-0810 (ID: 688)

Devices: SJC-Branch



Applications: webex-meeting x ms-office-web-apps x unknown x rtp-audio x

VPNs: VPN 0 x

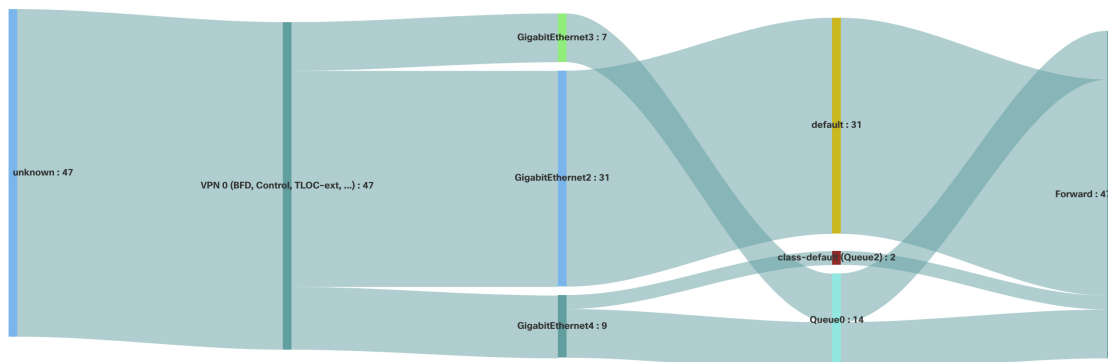
Interfaces: GigabitEthernet3 x GigabitEthernet2 x GigabitEthernet4 x

Queues: Queue1 x default x Queue3 x class-default x Queue0 x

Forward/Drop: Drop x Forward x

QoS - Applications Distribution (pps)

Snapshot of 8/10/2022, 5:57:41 PM



Tips

Traffic in VPN0 may compete bandwidth with user traffic.

- Control messages, DPI/FNF records within TLS/DTLS to vManage
- BFD over SDWAN
- TLOC extension, Routing protocols over WAN underlay

Gap: Can't classify these VPN0 traffic:

- Gig3(MPLS), Gig4(INET): QoS configured queue0(priority) for BFD etc.
queue2(class-default) for what VPN0 traffic?

Gig2(WAN w/o color, QoS)
no class queues, all into interface default

DNS discovery tracing

Troubleshooting web applications

Sort by size

Automatic replies

Automatic replies are currently turned on. [Turn off](#)

Junk Email

Nothing in Junk

Looks empty over here.

Inspector Console Debugger Network Style Editor Performance Memory Storage 16

Filter URLs

HTML CSS JS XHR Fonts Images Media WS Other

Status	Method	Domain	File	In	Tra...	Size	Latency
200	GET	res-h3.public.cdn.office.net	owa.229613.m.js	ow	j ser...	467.45 kB	0 ms
200	GET	res-h3.public.cdn.office.net	owa.383693.m.js	ow	j ser...	761.06 kB	0 ms
200	GET	res-h3.public.cdn.office.net	owa.797158.m.js	ow	j ser...	1.32 MB	0 ms
	GET	outlook.office.com	connect?transport=serverSentEvents&clientProtocol=1.5&UA=0	xhr			0 min
300	GET	res-h3.public.cdn.office.net	owa.worker.ven.fluent.js	42	j ser...	20.57 kB	0 ms
300	GET	res-h3.public.cdn.office.net	owa.122842.m.js	ow	j ser...	23.15 kB	0 ms
200	POST	outlook.office.com	service.svc?action=GetRegionalConfiguration&app=Mail&n=33	fet	j 11...	48.95 kB	343 ms
200	GET	outlook.office.com	account?settingname=Plain Text&n=31&cv=pRmaNx1TDL6ynpi	fet	j 98...	97.18 kB	446 ms
200	GET	res-h3.public.cdn.office.net	owa.worker.AppBarControlQueryWeb.js	42	j ser...	111.16 kB	0 ms
200	GET	res-h3.public.cdn.office.net	owa.162007.m.js	ow	j ser...	1.39 MB	0 ms

779 requests 42.16 MB / 34.79 MB transferred Finish: 2.48 min DOMContentLoaded: 562 ms load: 2.71 s

Starting NWPI (with DNS Domain Discovery)

TRACE

New Trace

☒ Enable DNS Domain Discovery ⓘ

Trace Name:

Trace Duration (minutes):

Default: 60

Filters:

Site ID(*):

VPN(*):

Client Address/Prefix:

Application Group: ⓘ

12

VPN - 1

192.168.12.220/32

Select one or more App Groups

Monitor Settings: >

Start

Cancel

[How to Get Started](#) | [FAQ](#)
Please click 'View Insight' to load data for 'INSIGHT'.

Monitoring dns traffic

DNS Domains Applications Active Flows Completed Flows

Please expand a flow/domain to load data for 'INSIGHT - ADVANCED VIEWS'.

Discovered Domains Monitored Domains

Search

0 Rows Selected

Total Rows: 21

Domain	Update Time	Application	App Group	DNS Server	DNS Redirect	Resolved IP	DNS Transport	DNS Egress	TTL(sec)	Request	Monitor State
☐ res.cdn.office.net	02 Sep 2022 10:02:04 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-	2a02:26f0:1e00:4b7::1e0f:2a02	UDP	GigabitEthernet1 [IPSEC - SD-1	0	4	never started
☐ safebrowsing.googleapis.co...	02 Sep 2022 10:00:04 AM C...	google-services	google-group	173.38.200.100,144.254.71.18	-	-	UDP	GigabitEthernet1 [IPSEC - SD-1	0	18	never started
☐ safebrowsing.googleapis.com	02 Sep 2022 9:59:34 AM CEST	google-services	google-group	173.38.200.100,144.254.71.18	-	-	UDP	GigabitEthernet1 [IPSEC - SD-1	0	18	never started
☐ contile.services.mozilla.com	02 Sep 2022 9:56:04 AM CEST	dns	other	173.38.200.100	-	34.117.237.239	UDP	GigabitEthernet1 [IPSEC - SD-1	0	3	never started
☐ outlook.office.com	02 Sep 2022 10:02:01 AM C...	ms-office-365	ms-cloud-group	173.38.200.100	-	40.99.204.66,52.97.179.194,40	UDP	GigabitEthernet1 [IPSEC - SD-1	0	19	never started
☐ login.microsoftonline.com	02 Sep 2022 10:01:49 AM C...	ms-services	ms-cloud-group	173.38.200.100	-	-	UDP	GigabitEthernet1 [IPSEC - SD-1	0	2	never started
☐ r4.res.office365.com	02 Sep 2022 10:01:49 AM C...	ms-office-365	ms-cloud-group	173.38.200.100	-	-	UDP	GigabitEthernet1 [IPSEC - SD-1	0	2	never started

Select interested application domains to start/stop monitoring related flows.

Start Flow Monitor

Focusing on O365

Start monitoring to effectively trace TCP or UDP flows to those fully qualified domain names [FQDN]

Drill down and enable flow tracing

The screenshot displays the Cisco FlowTracer interface. At the top, a navigation bar includes 'DNS Domains', 'Applications', 'Active Flows', and 'Completed Flows'. Below this, a search bar contains 'cdn' and shows '3 Rows Selected'. A table lists discovered domains with columns for Update Time, Application, App Group, DNS Server, DNS Redirect, Resolved IP, DNS Transport, DNS Egress, TTL(sec), Request, and Monitor State. Three domains are listed: res-1.cdn.office.net, res.cdn.office.net, and amcdn.msftauth.net. A callout box on the right shows a detailed view of network traffic, including status (200), method (GET), domain (res.cdn.office.net), and file paths (ova.ReadingPane.js, ova.MailBoot.js, ova.Addins.js, ova.11877.js, ova.42170.js, ova.MailRibbon.js). A 'Start Flow Monitor' button is visible in the bottom right corner.

Select flows to be traced

Switch to monitored domains

INSIGHT

Selected trace: trace_1000 (Trace ID: 1000)

DNS Domains Applications Active Flows Completed Flows

Selected Domain: res.cdn.office.net

Discovered Domains **Monitored Domains**

Search

0 Rows Selected

Total Rows: 3

Domain	Update Time	Application	App Group	DNS Server	DNS Redirect	Resolved IP	DNS Transport	DNS Egress	TTL(sec)	Request	Monitor State																											
☐ res.cdn.office.net	02 Sep 2022 10:23:04 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-	2a02:2600:fe00:4b7::1e0f:2a02	UDP	GigabitEthernet1 [IPSEC - SD-1	0	6	running																											
<div><div><div>Egress Interface ⓘ</div><table><thead><tr><th>Local Edge</th><th>Remote Edge</th><th>Local Color</th><th>Remote Color</th><th>App CND(ms)</th></tr></thead><tbody><tr><td>(C) GigabitEthernet3</td><td>cedge2</td><td>Internet</td><td>BIZ_INTERNET</td><td>N/A</td></tr><tr><td>(C) GigabitEthernet1</td><td>cedge2</td><td>Internet</td><td>MPLS</td><td>N/A</td></tr></tbody></table></div><div><table><thead><tr><th>App SND(ms)</th><th>HTTP Probe Response Time(ms)</th><th>HTTP Probe Loss(%)</th><th>Path Score</th></tr></thead><tbody><tr><td>N/A</td><td>83</td><td>0</td><td>10</td></tr><tr><td>N/A</td><td>82</td><td>0</td><td>10</td></tr></tbody></table></div></div>												Local Edge	Remote Edge	Local Color	Remote Color	App CND(ms)	(C) GigabitEthernet3	cedge2	Internet	BIZ_INTERNET	N/A	(C) GigabitEthernet1	cedge2	Internet	MPLS	N/A	App SND(ms)	HTTP Probe Response Time(ms)	HTTP Probe Loss(%)	Path Score	N/A	83	0	10	N/A	82	0	10
Local Edge	Remote Edge	Local Color	Remote Color	App CND(ms)																																		
(C) GigabitEthernet3	cedge2	Internet	BIZ_INTERNET	N/A																																		
(C) GigabitEthernet1	cedge2	Internet	MPLS	N/A																																		
App SND(ms)	HTTP Probe Response Time(ms)	HTTP Probe Loss(%)	Path Score																																			
N/A	83	0	10																																			
N/A	82	0	10																																			
☐ res-1.cdn.office.net	02 Sep 2022 10:23:04 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-																																	

Router is sending HTTP probes to destination in order to evaluate:

- Loss score %
- Path score

Switch to active flows or completed flow for further analysis

Start - Update Time	Flow Id	Readout *	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain
10:26:52 AM-10:27:22 AM	3	✓	192.168.12.220	40590	152.199.21.175	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-web-apps	ms-cloud-group	res.cdn.office
10:27:10 AM-10:27:10 AM	7	✗	192.168.12.220	33790	104.85.0.113	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	rd.res.office365
10:27:10 AM-10:27:10 AM	8	●	192.168.12.220	57174	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-web-apps	ms-cloud-group	res-1.cdn.office
10:27:10 AM-10:27:10 AM	9	●	192.168.12.220	34494	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-web-apps	ms-cloud-group	res-1.cdn.office
10:27:07 AM-10:27:07 AM	10	●	192.168.12.220	33806	104.85.0.113	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	res-1.cdn.office
10:27:10 AM-10:27:10 AM	11	●	192.168.12.220	51269	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-web-apps	ms-cloud-group	res-1.cdn.office

INSIGHT - ADVANCED VIEWS

Domain Trend Flow Trend Upstream Feature Downstream Feature Geography

Same functionality as "non dns based" tracing
Check readout per application / fqdn / destination IP
Check advanced view for further drill down

Switch to active flows or completed flow for further analysis

[illegible]

In case of congestion – qdepth will be reported
Tool useful to monitor QOS performance

Workflows – validating a AAR policy

AAR policy

```
cedge2#show sdwan policy from-vsmart
from-vsmart sla-class TEST1
  loss      10
  latency 100
  jitter   10
from-vsmart app-route-policy _VPN_1_web-ssh-AAR
vpn-list VPN_1
sequence 1
  match
    source-ip 0.0.0.0/0
    app-list  SSH_policy
  action
    sla-class      TEST1
    no sla-class strict
    sla-class preferred-color biz-internet
sequence 11
  match
    source-ip 0.0.0.0/0
    app-list  Microsoft_Apps
  action
    sla-class      TEST1
    no sla-class strict
    sla-class preferred-color mpls
sequence 21
  match
    source-ip 0.0.0.0/0
    app-list  web_services
  action
    sla-class      TEST1
    no sla-class strict
    sla-class preferred-color biz-internet
```

0365 apps should flow through MPLS until:

- drop is greater than 10 %
- Jitter greater than 10msec
- Latency greater than 100msec

Realistic network problems -netem

<https://wiki.linuxfoundation.org/networking/netem>

netem

netem provides [Network Emulation](#) functionality for testing protocols by emulating the properties of wide area networks. The current version emulates variable delay, loss, duplication and re-ordering.

If you run a current 2.6 distribution, ([Fedora](#), [OpenSuse](#), [Gentoo](#), [Debian](#), [Mandriva](#), [Ubuntu](#)), then netem is already enabled in the kernel and a current version of [iproute2](#) is included. The netem kernel component is enabled under:

```
Networking -->
Networking Options -->
  QoS and/or fair queuing -->
    Network emulator
```

Netem is controlled by the command line tool 'tc' which is part of the [iproute2](#) package of tools. The tc command uses shared libraries and data files in the /usr/lib/tc directory.

Contents

- 1 Examples
 - 1.1 Emulating wide area network delays
 - 1.2 Delay distribution
 - 1.3 Packet loss
 - 1.3.1 Caveats
 - 1.4 Packet duplication
 - 1.5 Packet corruption
 - 1.6 Packet re-ordering
 - 1.6.1 Caveats
 - 1.7 Rate control
 - 1.8 Non FIFO queuing
 - 1.9 Delaying only some traffic

Table of Contents

- * netem
 - * Contents
 - * Examples
 - * Emulating wide area network delays
 - * Delay distribution
 - * Packet loss
 - * Packet duplication
 - * Packet corruption
 - * Packet re-ordering
 - * Rate control
 - * Combining netem with other qdiscs
 - * Non FIFO queuing
 - * Delaying only some traffic
 - * FAQ
 - * How come first ping takes longer?
 - * How come TCP is so slow over netem?
 - * How can I use netem on incoming traffic?
 - * How to reorder packets based on jitter?
 - * How does the value of HZ impact Netem?
 - * Links
 - * Contact Info

High level steps for using netem with SDWAN

- Deploy Linux VM, set Hub IP as Gateway
- Install iproute2/iproute-tc and netem (if needed)
- Enable IPv4 forwarding into sysctl
- Allow IPTables to accept FORWARD
- Use Service Chain to send/receive traffic from cEdge to VM
- Create Custom Control Policy to direct traffic from Site to Hub via VM
- Apply shenanigans

Looking at NWPI

Search

Total Rows: 1

Start - Update Time	Flow Id	Readout *	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	ART CND(ms)/SND(ms)
1:59:31 PM-2:19:58 PM	15		192.168.12.220	42972	52.97.250.226	443	TCP	DEFAULT + / DEFAULT +	ms-office-365	ms-cloud-group	outlook.office.com(ts)	cedge2: 0/168

Direction	HopIndex	Local Edge	Remote Edge	Local Color	Remote Color	Local Drop(%)	Wan Loss(%)	Remote Drop(%)	Jitter(ms)	Latency(ms)	ART CND(ms)/SND(ms)	Total Packets	Total Bytes	Queue Id	QDepth Limit/Max/Min/Avg
Upstream	0	(Gi2) cedge2	cedge7	BIZ_INTERNET	BIZ_INTERNET	0.00	N/A	0.00	< 1	34	cedge2: 0/168	356	80129	2	64/0/0/0
Upstream	1	cedge7 (Gi3)	Internet	BIZ_INTERNET (NAT_DIA)	N/A	0.00	N/A	N/A	N/A	N/A	cedge7: 134/46	158	56181	N/A	N/A
Downstream	0	Internet	(Gi3)cedge7	N/A	BIZ_INTERNET (NAT_DIA)	N/A	N/A	0.00	N/A	N/A	N/A	160	45519	N/A	N/A
Downstream	1	cedge7	cedge2(Gi2)	BIZ_INTERNET	BIZ_INTERNET	0.00	N/A	0.00	< 1	26	N/A	460	323351	N/A	N/A

INSIGHT - ADVANCED VIEWS

Selected trace: trace_1040 (Trace Id: 1040)

Domain Trend | Flow Trend | **Upstream Feature** | Downstream Feature | Geography

Hostname: cedge2 | Event List | PATH_CHANGE | Expand All Features

Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet1

Ingress Feature

- > Ingress Report
- > CEF Forwarding
- > SDWAN ACL IN => View Policy <<
- > SDWAN App Route Policy => View Policy <<
- > SDWAN Forwarding

Egress Feature

- > NBAR
- > IPSec
- > SDWAN QoS Output
- > QoS => View Policy <<
- > Transit Report

SDWAN App Route Policy

```

VRF ID      : 1
VRF         : 1
Policy Name : 1_VRF_LW_HISTOGRAM_POLICY (5612)
Seq         : 11
Req SLA     : TEST1 (1)
Act SLA     : TEST1 (1)
Policy Flags : B2D
Failback to best Path : no
SLA Strict   : No
Actual Color : biz-internet (4)
Preferred Color : alpha (164)
Tunnel Match Reason : MATCHES_SLA_AND_COLOR_ANY_INCAP
    
```

Matching seq 11 from AAR policy

Policy in red – We failback [loadbalance because the SLA is not met].

NWPI feature evolution

17.4.1/20.4 (Phase I)

- Network wide bidirectional application
 - flow visibility, incl. network path,
 - network metrics (loss, latency, jitter), and SD-WAN policy
 - enforcement details in an on-demand manner

17.6.1/20.6 (Phase II)

Local & WAN drop
TCP Reset
NAT Translated
Network Path Changed
DPI First Packet Classification failed
SLA Violated
QoS Congestion
DNS domain discovery for APP / SAAS troubleshooting

NWPI feature evolution

17.9.1/20.9 (Phase III)

Multi-dimensional Insight Summary of aggregation dashboard and readout

“Overview” , “QoS insight” “App Performance Insight”, “Event Insight”.

Application flow’s domain visibility (w/o DNS Discovery)

Flow level readout of “Path Insight”

17.12.1/20.12 (Phase IV)

Automatic trigger based on QoS Congestion or SLA Violation

Synthetic traffic for design validation

Flexible aggregation

Application traffic pattern insights

Traces across multiple VPN’s

Enhancement to “Summary”, “Application” and “Path Insight” views

NWPI triggered on events (20.12+)

[Overview](#) > [Troubleshooting](#) > [Network Wide Path Insight](#)

TRACE

New Trace

New Auto-on Task

[How to Get Started](#) | [FAQ](#)

Please click 'View Insight' to load data for 'INSIGHT'.

Task Name * Select Event * Select Site Select Duration

Start

Cancel

All Trace

Auto-On Task

Search Table

As of: Jun 05, 2023 08:40 PM

Task Name	Task ID	Event(s)	Site(s)	State	Start Time	Duration	Stop Time	Actions
TOI_Demo	2	QoS Congestion,SLA Violation	100 500 600	Active	05 Jun, 2023 08:36:34 PM	168 hour(s)	12 Jun, 2023 08:36:34 PM	...
auto-on	1	QoS Congestion,SLA Violation	100 500 600	Finished	05 Jun, 2023 08:11:08 PM	9 hour(s)	05 Jun, 2023 08:17:27 PM	...

Trigger traces on QOS Congestion and/or SLA Violations

NWPI triggered on events

[Overview](#) > [Troubleshooting](#) > [Network Wide Path Insight](#)

TRACE

[New Trace](#) [New Auto-on Task](#)

[How to Get Started](#) | [FAQ](#)

Please click 'View Insight' to load data for 'INSIGHT'.

All Trace Auto-On Task

Q Search Table

As of: Jun 05, 2023 08:53 PM 

Task Name	Task ID	Event(s)	Site(s)	State	Start Time	Duration	Stop Time	Actions
▼ Insight Summary TOL_Demo	2	QoS Congestion,SLA Violation	100 500 600	 Active	05 Jun, 2023 08:36:34 PM	168 hour(s)	12 Jun, 2023 08:36:34 PM	...
Insight Summary TOL_Demo_sla_violation_240	240	SLA Violation	500	 Running	05 Jun, 2023 08:49:19 PM	5 min(s)	N/A	...

If two consecutive events occur, 5 minute NWPI trace triggered
Note: 30 minute cooldown period applies once a trace starts per site

Challenges in validation and troubleshooting

- User not available? Can't deploy VM?
- What about initial validation of site or policy change?
- NWPI Synthetic Traffic can provide traffic which is application aware, realistic etc.
- Traffic traverses LAN side FIA's
- We can then use NWPI features to validate flow as needed



Generating synthetic traffic

TRACE

New Trace

New Auto-on Task

How to Get Started | FAQ

Selected trace: auto-on-rhixiao-6_sia_violation_20592 (Trace Id: 20592)

☐ Enable DNS Domain Discovery ⓘ

Trace Name:
alanwan-domain-0504

Trace Duration (minutes):
Default: 60

Filters:

Site ID(*, branch site only):
3

VPN(*):
All X VPN - 10 X

Source Address/Prefix: ⓘ
e.g v4: 10.0.0.0/8 or v6: 2001:0:0:1::/64

Destination Address/Prefix: ⓘ
e.g v4: 10.0.0.0/8 or v6: 2001:0:0:1::/64

☒ Application ⓘ ☐ Application Group
Select one or more applications

Advanced Filters: >

Monitor Settings

Synthetic Traffic: ▾

	URL(*)	VPN(*)	DNS Server	DSCP(*)	Interval(minute)	
1	chat.openai.com	VPN-10	64.104.76.247	AF22	1 ⓘ	
2	concur.cisco.com	VPN-10	64.104.76.247	AF41	1 ⓘ	
3	www.clarity.com	VPN-10	64.104.76.247	DEFAULT	1 ⓘ +	

Save

Grouping Fields: ▾

☒ Client Prefix ⓘ ☒ Server Prefix ⓘ ☒ Source SGT ⓘ

Start

Cancel

Synthetic traffic via CLI (17.12+)

CLI command to trigger one off probe. Use **show logging** to see result

```
request platform software sdwan synthetic-traffic probe vpn-id 1 url www.cisco.com [dscp  
<code> [dns <address of nameserver>]
```

NOTE: vpn-id and url is mandatory and dscp/dns are optional

Example:

```
cEdge1#request sdwan synthetic-traffic probe vpn-id 1 url www.cisco.com
```

```
*Apr 11 02:05:34.302: %Cisco-SDWAN-Site25-cEdge-1-DBGD-6-INFO-1500002: Synthetic test probe  
result for app: Def-Test, url: www.cisco.com, src_intf: GigabitEthernet7, latency: 253, loss:  
0%, score: 6, count 1
```

Use cases

Poor application
performance

Cloud-on Ramp
SAAS validation

Provider performance
problems

[any] Policy validation

Cloud on-Ramp
SAAS troubleshooting

DIA troubleshooting

Learning SDWAN
forwarding

Problem isolation

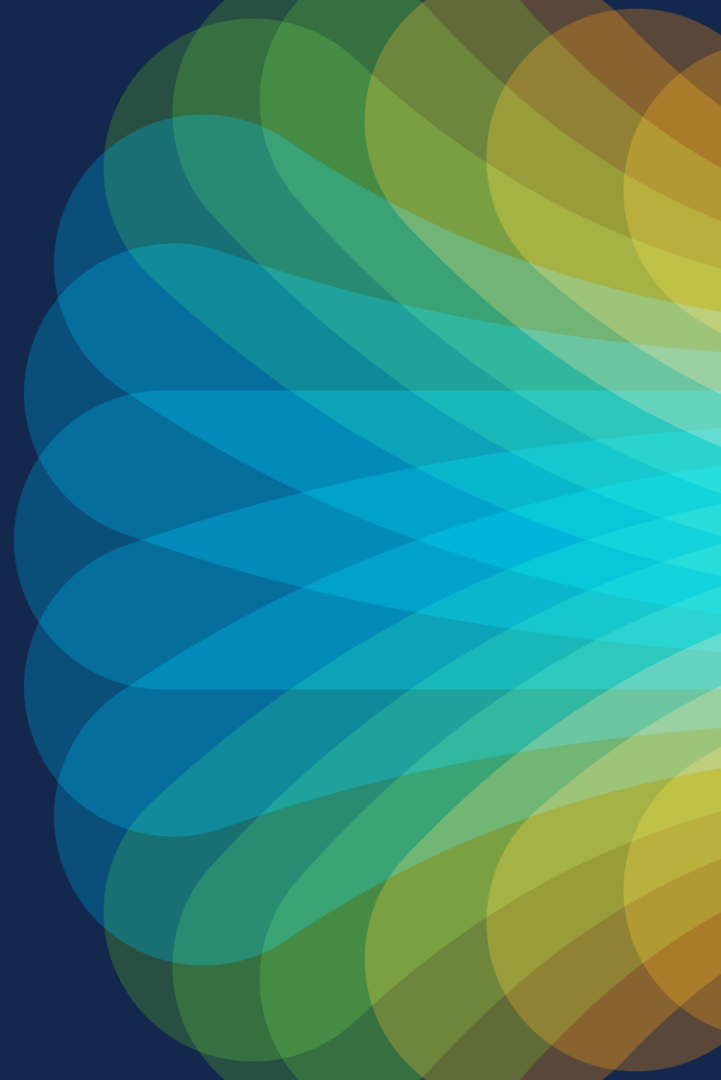
[any] overlay/underlay
dataplane

Thousand Eyes versus NWPI

<u>Thousand Eyes</u>	<u>NWPI</u>
Probe based	Real™ traffic traced (+ synthetic)
Network wide visibility based on agents /tests distributed on each sides	Network transitive condition applied initially on a single site ID
No packet processing visibility	Packet processing visibility

Thousand Eyes and NWPI are complementary:
Thousand eyes gives a network-wide overview
NWPI is the magnifying glass that explains drops for a particular set of flows

Platform Resource Monitoring and Troubleshooting



Why monitor resources?

- Can be key reason why performance is not as expected
- Always worth a quick sanity check for any complex issues
- Can be indicative of unexpected configuration, scale issues or potential software defects
- Key data point for most complex issues, or at least ruling it out.

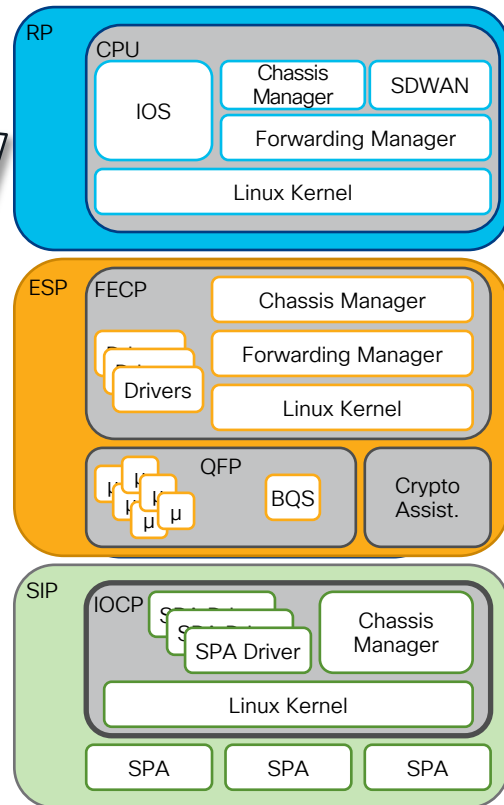


Resources: simplified view

cat8000v#show platform resources

****State Acronym: H - Healthy, W - Warning, C - Critical**

Resource	Usage	Max	Warning	Critical	State
<hr/>					
RP0 (ok, active)					H
Control Processor	27.44%	100%	80%	90%	H
DRAM	4122MB (52%)	7897MB	88%	93%	H
ESP0 (ok, active)					H
QFP					H
DRAM	188960KB (36%)	524288KB	85%	95%	H
IRAM	207KB (10%)	2048KB	85%	95%	H
CPU Utilization	1.00%	100%	90%	95%	H
B4Q Pool 124	5KB (0%)	1587KB	75%	85%	H
B4Q Pool 128	2KB (0%)	1966KB	75%	85%	H
B4Q Pool 256	8KB (0%)	3932KB	75%	85%	H
B4Q Pool 512	15KB (0%)	5767KB	75%	85%	H
B4Q Pool 1024	43KB (0%)	8155KB	75%	85%	H
B4Q Pool 1536	54KB (0%)	9678KB	75%	85%	H
B4Q Pool 2048	58KB (0%)	8634KB	75%	85%	H
B4Q Pool 4096	128KB (1%)	8260KB	75%	85%	H
B4Q Pool 10240	230KB (3%)	6470KB	75%	85%	H
B4Q Pool 16384	0KB (0%)	1296KB	75%	85%	H
B4Q PMD	8553KB (3%)	236544KB	75%	85%	H



Monitoring beyond CLI

SNMP

- What is OLD monitoring? IOSd or IOS-XE platform
- Only monitoring IOSd can be misleading
- Samples of point in time, can be spiky
- Does show overall trends
- Not available for all platform resources
- Can use Radkit, as well as NMS



Monitoring beyond CLI

Syslog

- Present for many common resource issues
- Can contain key context on possible area of issue (QOS, ACL's etc.)
- More accurate timestamps, map to changes/policy deployments
- Easily available locally as well as to central location



Wrong logging?

Monitoring beyond CLI – Resources

- SNMP OID for CPU, Memory and COPP
 - <https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/118901-technote-snmp-00.html>
- SNMP OID for QFP
 - ceqfpUtilizationTable (especially ceqfpUtilInputTotalBitRate, ceqfpUtilOutputTotalBitRate, ceqfpUtilProcessingLoad) – <https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.4.1.9.9.715.1.1.6.1>
 - ceqfpMemoryResourceTable (especially ceqfpMemoryResFree) – <https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.4.1.9.9.715.1.1.7.1>

Interpret QFP Usage with QFP profiling (new in 17.11)

```
cedge2#debug platform condition both
cedge2#debug platform packet-trace packet 8192 data-size 4096 fia-trace
cedge2#debug platform condition start
```

Sorted by average utilization

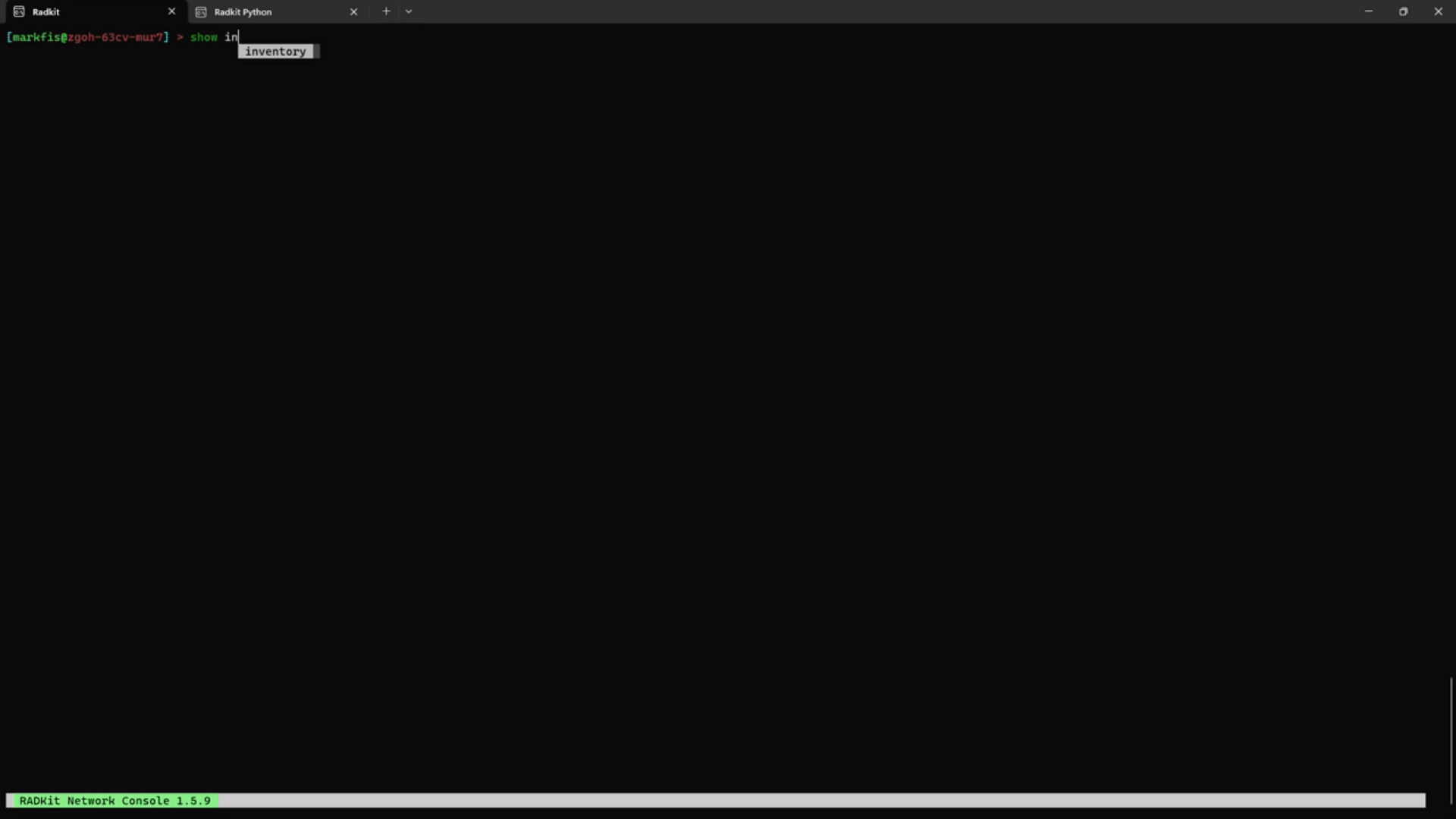
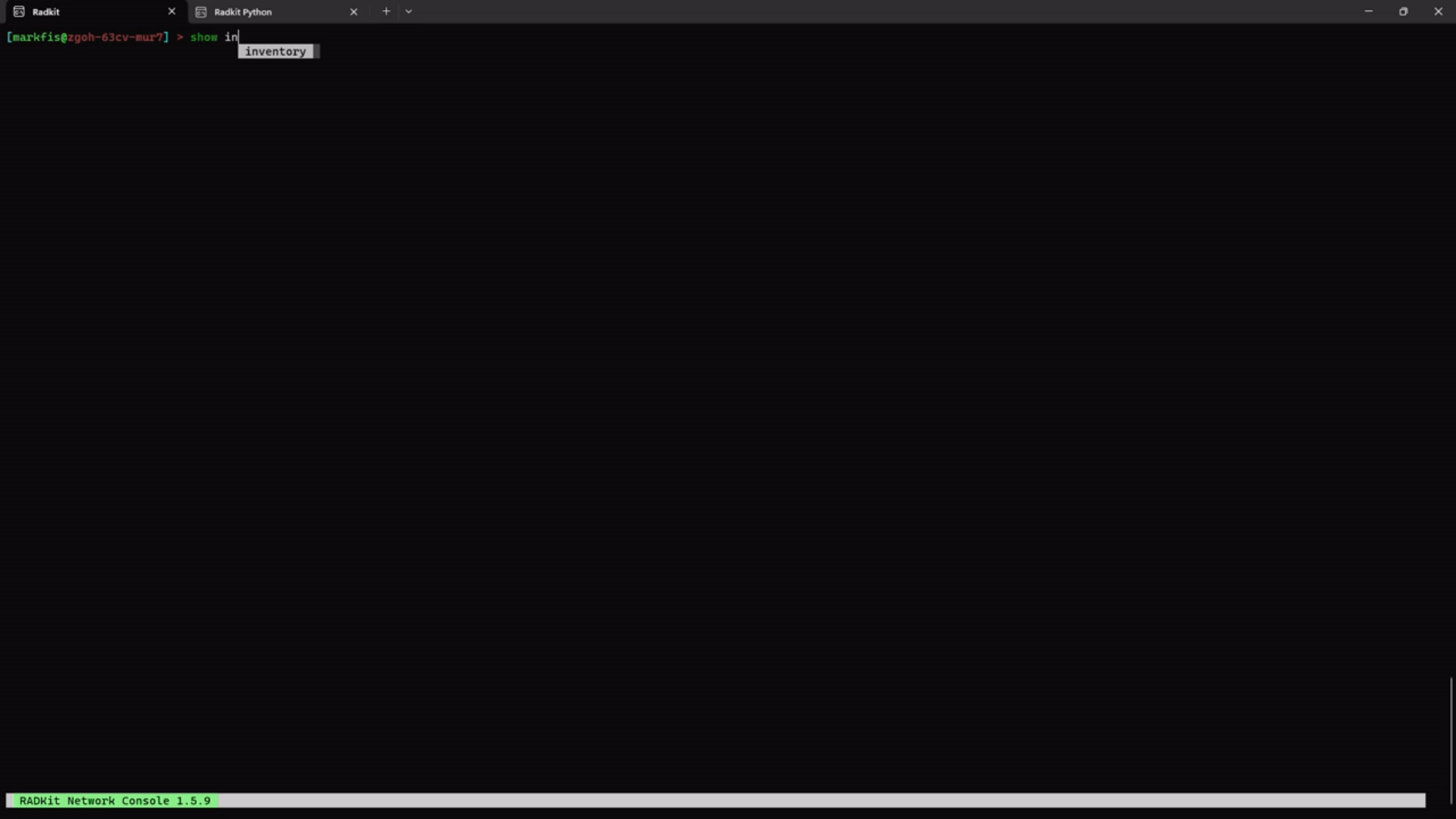
```
cedge2#show platform packet-trace fia-statistics
```

Feature	Count	Min (ns)	Max (ns)	Avg (ns)
IPV4_OUTPUT_STILE_SDWAN_LAN_EXT	1	11828	11828	11828
IPV4_INPUT_IPSEC_INLINE_PROCESS	4546	1407	89575	4480
MARMOT_SPA_D_TRANSMIT_PKT_EXT	8	1232	9387	4028
SDWAN_POLICY_FIA	8123	70	45532	3949
SDWAN_BFD_TX_FEATURE	7	2671	5993	3673
INTERNAL_TRANSMIT_PKT_EXT	41	900	17700	3484
IPV4_INPUT_STILE_LEGACY	8123	841	187112	3073
IPV4_OUTPUT_QOS_EXT	7	755	4928	2923
IPV4_OUTPUT_IPSEC_INLINE_PROCESS	3595	862	35475	2170
BFD_SDWAN_CALL_QOS_TX_FIA	7	61	13914	2120
SDWAN_ACL_IN	3590	513	27001	1966
INPUT_FNF_DROP	8	356	7261	1803
LAYER2_INPUT_LOOKUP_PROCESS_EXT	1	1569	1569	1569
...				

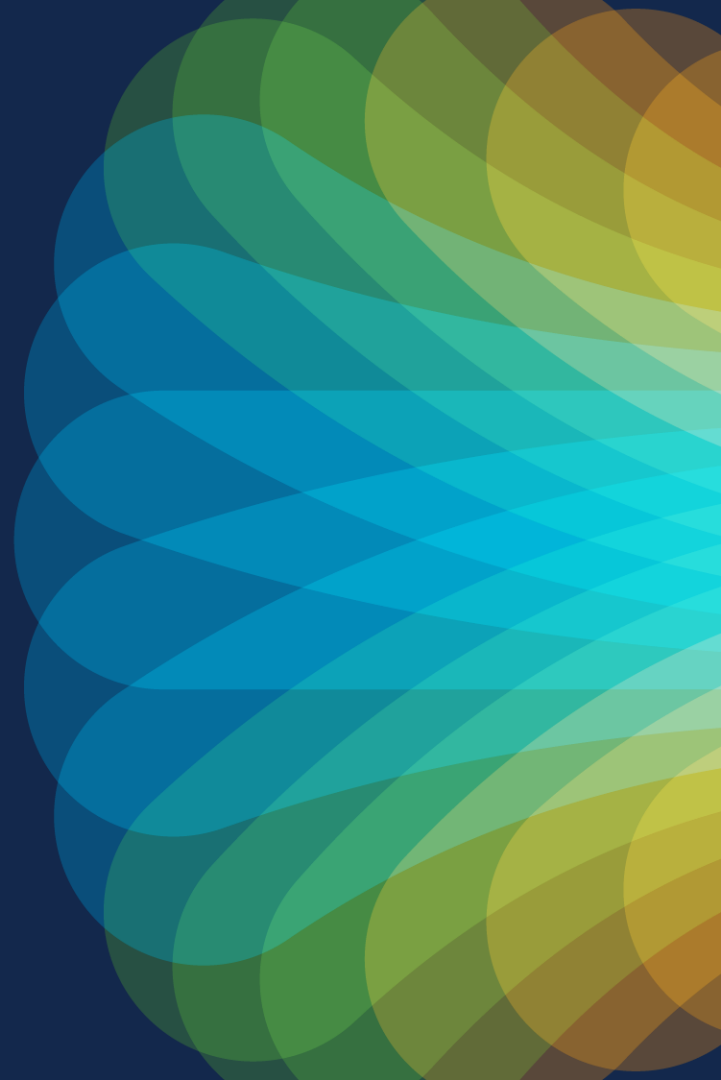
Relative QFP consumption by individual features

Demo 2 – Resource Usage and QFP Profiling





Wrapping up...



New Debugging Strategy



IOS Control Plane

- show interface, show ip route, show bgp ...
- Feature debugging

Platform Control Plane

- Unified show commands
- Platform show commands
- Future: control plane conditional debugging

Data Plane

- Packet Tracer
- Forwarding plane conditional debugging
- Embedded Packet Capture



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

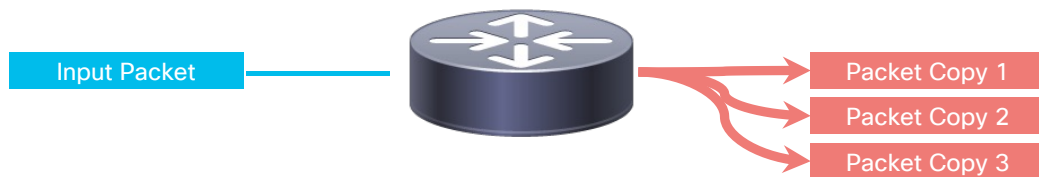
Appendix

Breaking, Multiplying and Gluing Packets

Patterns of Interest



Multicast Replication



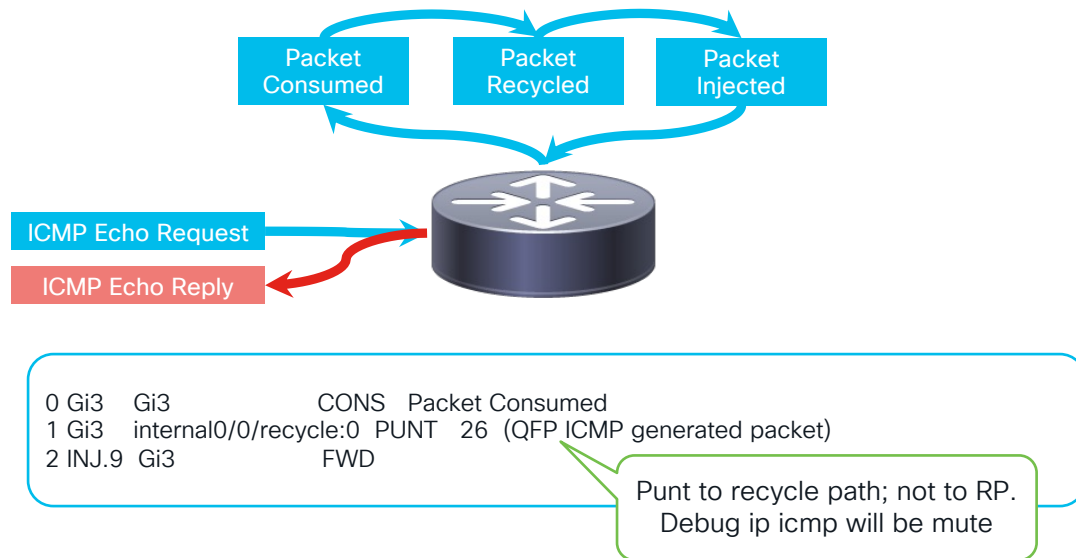
0	Gi1	<none>	CONS	Packet Consumed Silently
1	Gi1	Gi2	FWD	
2	Gi1	Gi3	FWD	
3	Gi1	Gi4	FWD	

Fragmentation



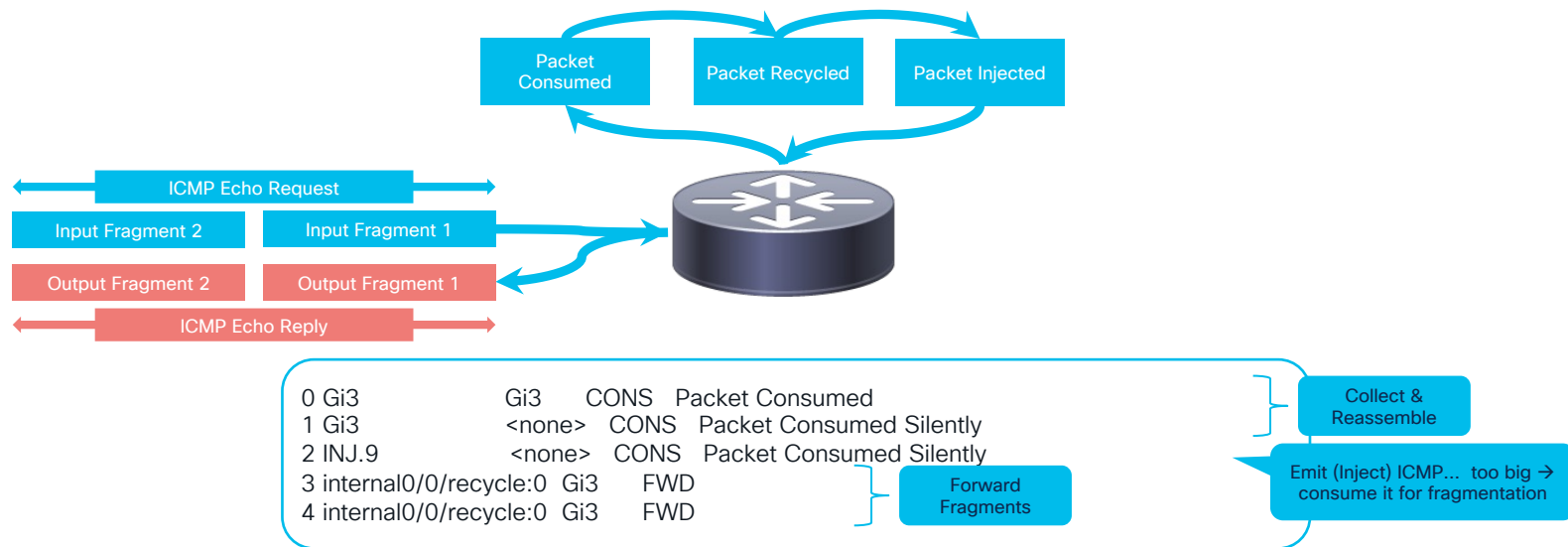
```
0 Gi1 <none> CONS Packet Consumed Silently
1 Gi1      Gi2 FWD
2 Gi1      Gi2 FWD
```

ICMP Echo Request & Reply



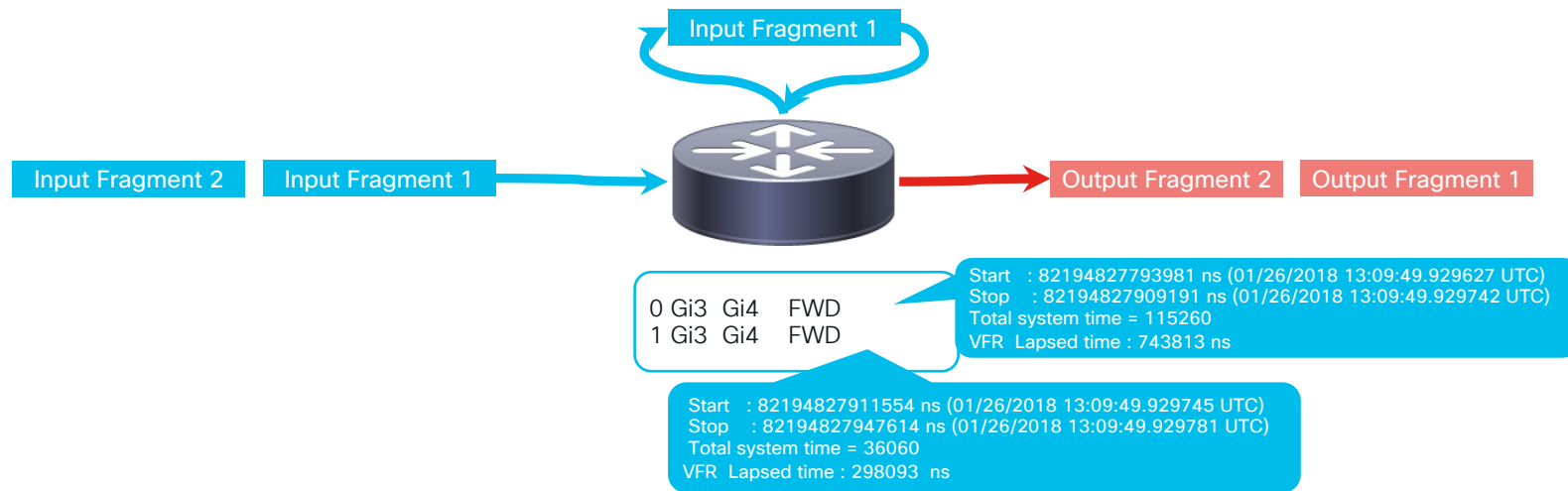
Reassembly of For-Us Packets

- (e.g. large ICMP Echo Request-Reply)



Virtual Reassembly of Pass-Thru Packets

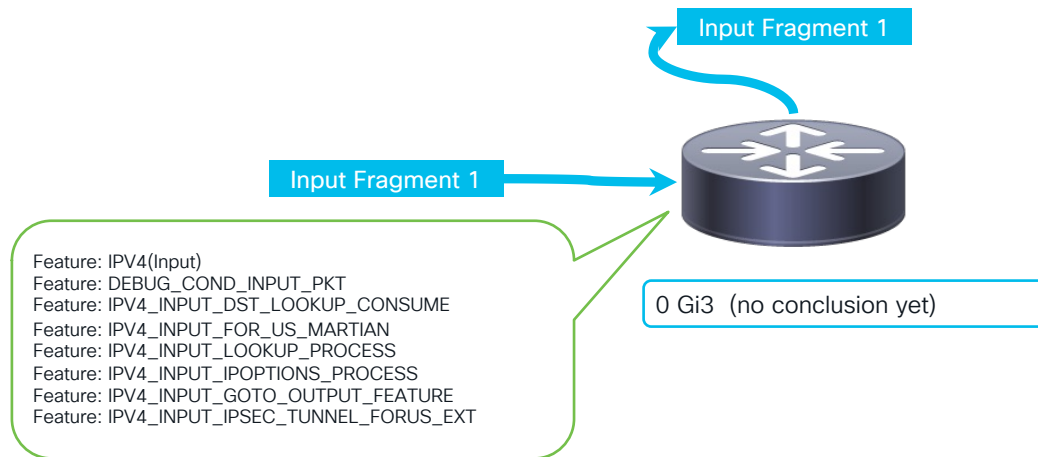
- (e.g. with NAT)



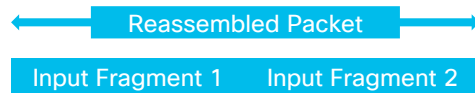
Fragment 1 enters and is processed until VFR. Then the packet freezes.

Fragment 2 enters until VFR at which point Fragment 1 is released and processing continues.

Reassembly of Overlay VPN Packets (I) – e.g. FlexVPN



Reassembly of Overlay VPN Packets (II)



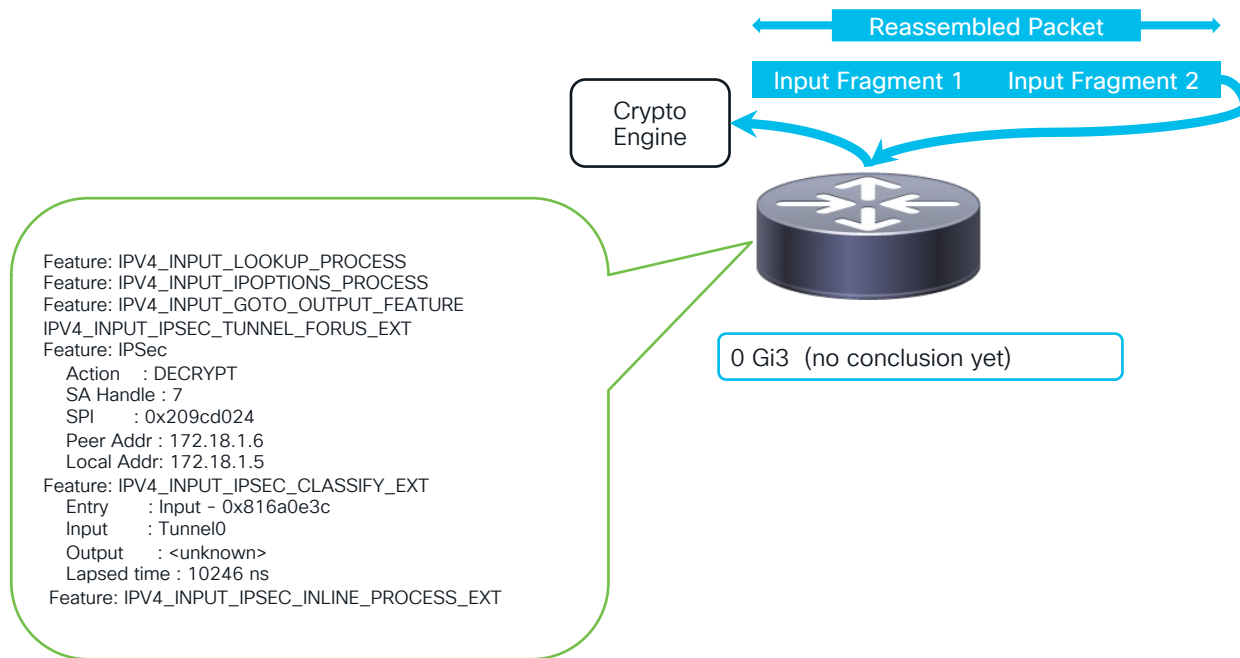
Input Fragment 2



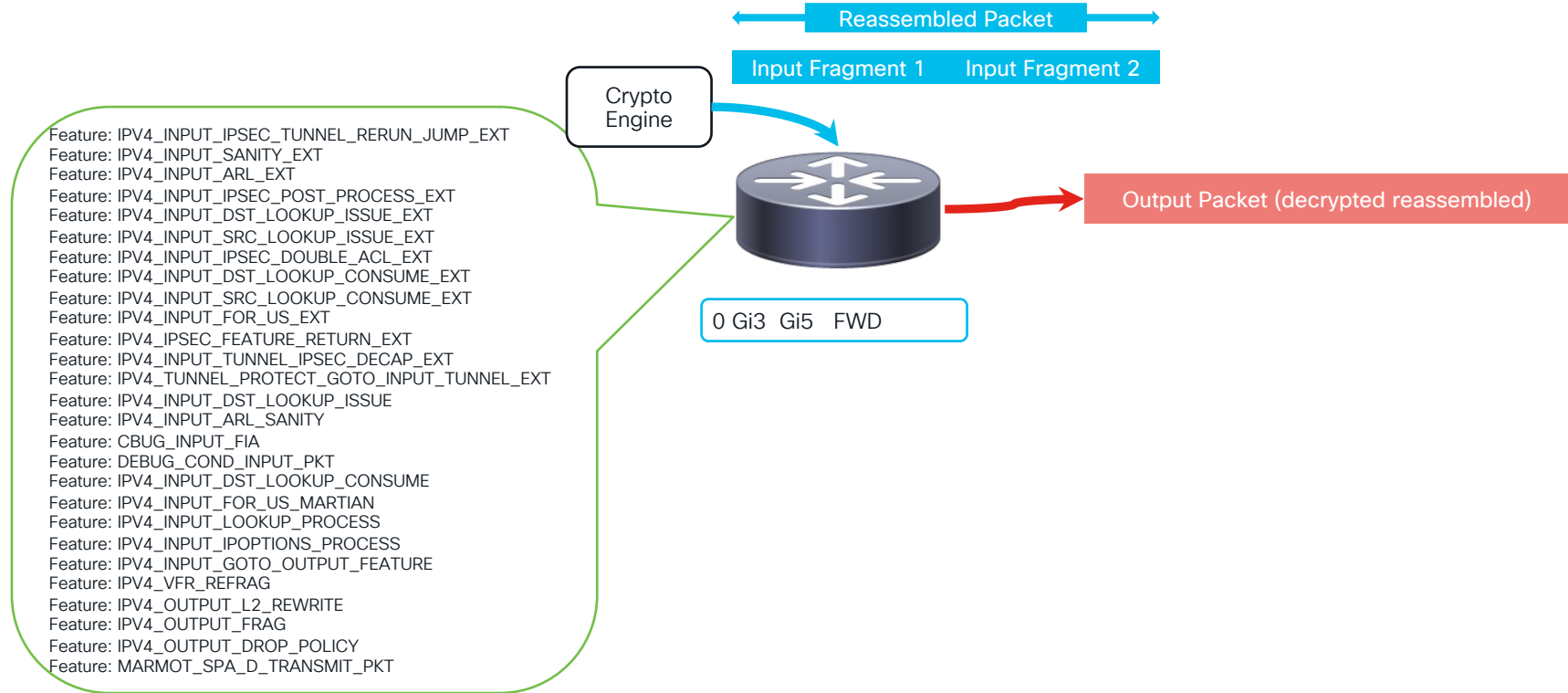
Feature: IPV4(Input)
Feature: DEBUG_COND_INPUT_PKT
Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
Feature: IPV4_INPUT_FOR_US_MARTIAN
Lapsed time : 258953 ns

1 Gi3 <none> CONS Packet Consumed Silently

Reassembly of Overlay VPN Packets (III)



Reassembly of Overlay VPN Packets (IV)



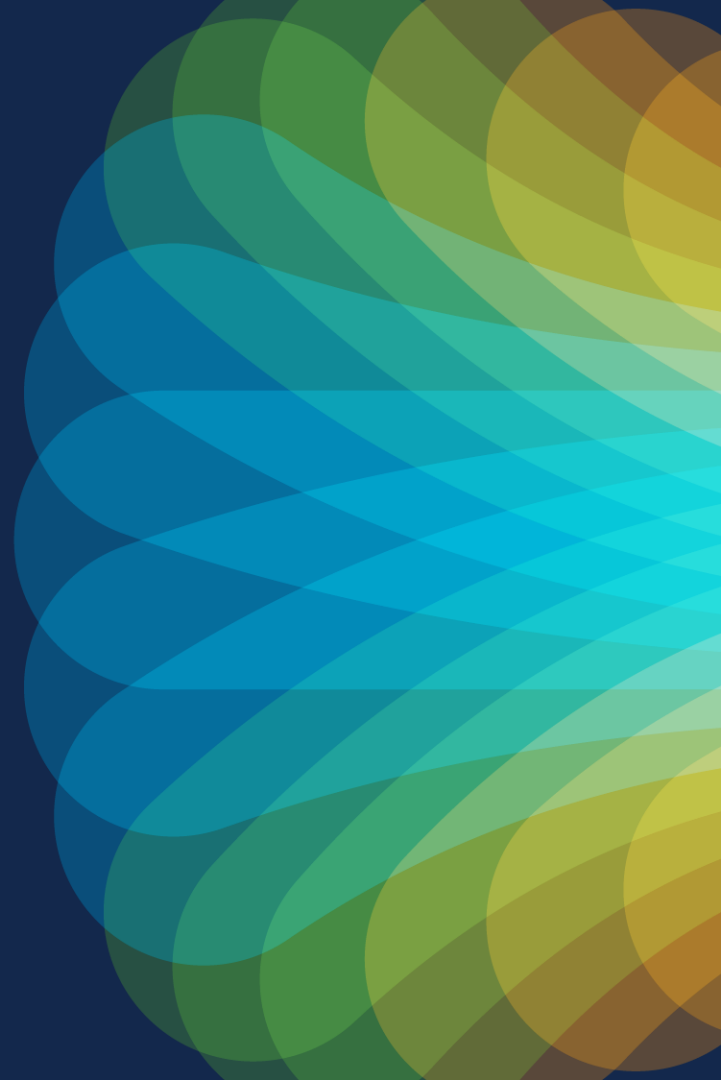


The bridge to possible

Thank you



#CiscoLiveAPJC



The background is a vibrant, abstract graphic featuring a rainbow color palette. On the left, there are horizontal, wavy bands of color transitioning from red at the top to blue at the bottom. On the right, a bright white light source emits a series of sharp, triangular rays of color in a radial pattern, also following the rainbow spectrum. The overall effect is energetic and celebratory.

cisco *Live!*

Let's go

#CiscoLiveAPJC