The bridge to possible

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

Frederic Detienne, Distinguished Engineer
Olivier Pelerin, Principal Engineer

BRKTRS-3475

Agenda

- How are packet forwarded (architecture)
- Dataplane Troubleshooting
- Network-level troubleshooting (SDWAN)
- Resource Monitoring
- Wrapping up...

Cisco Webex App

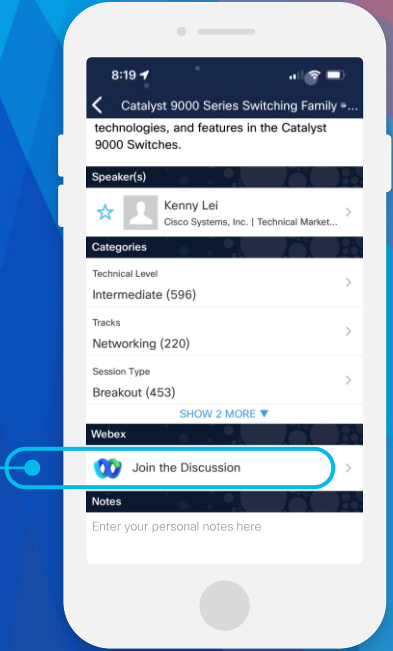
Questions?

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 June 9, 2023.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

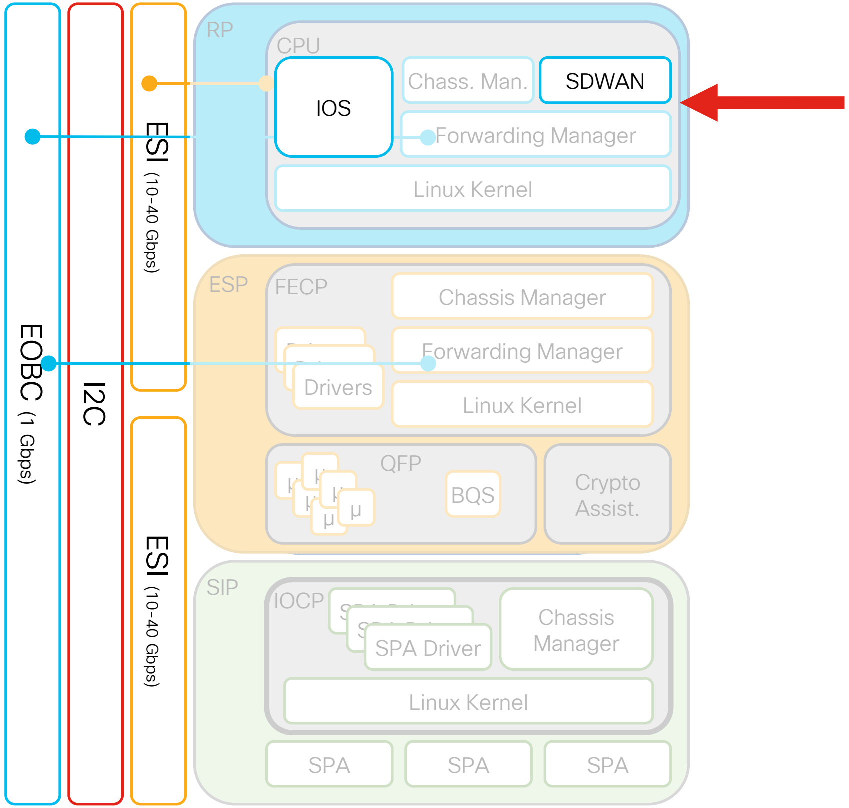
Enter your personal notes here

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

cisco Live!

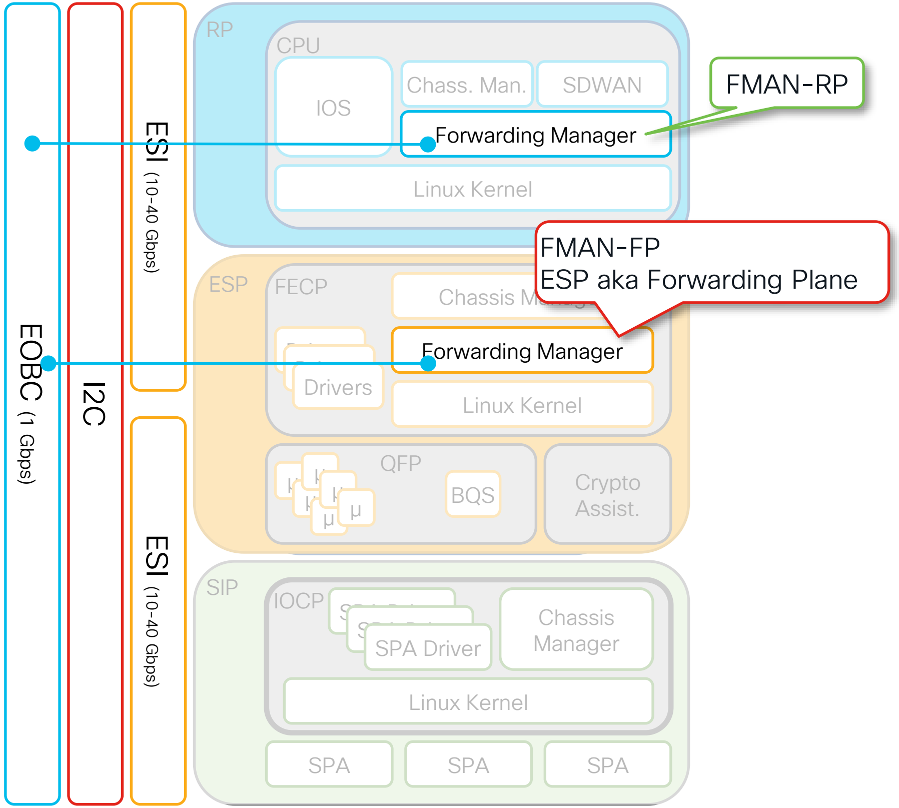
Software architecture

The Route Processor (General view)



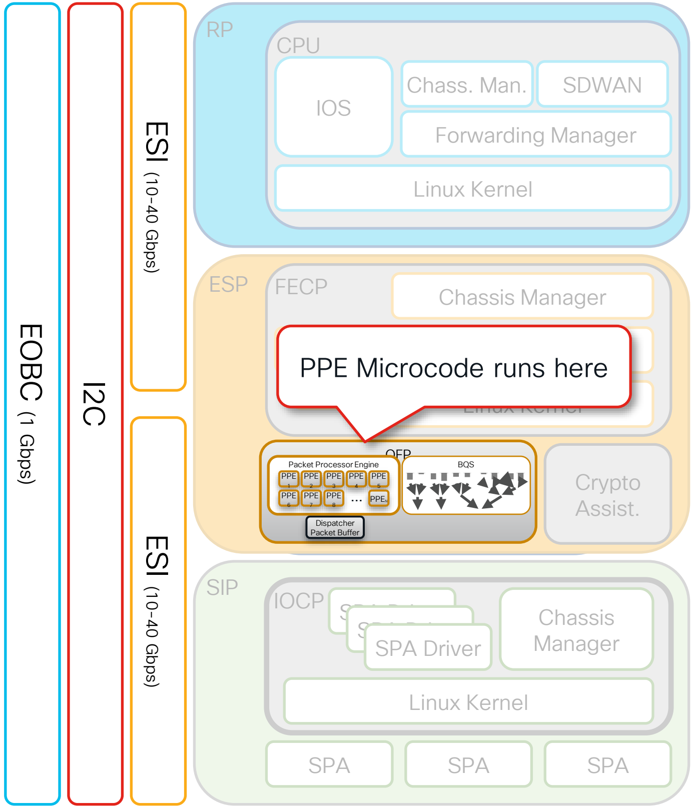
confd	IOSd
Vdaemon	OMPd
FTM	TTM
NCSSHd	DMIauth

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

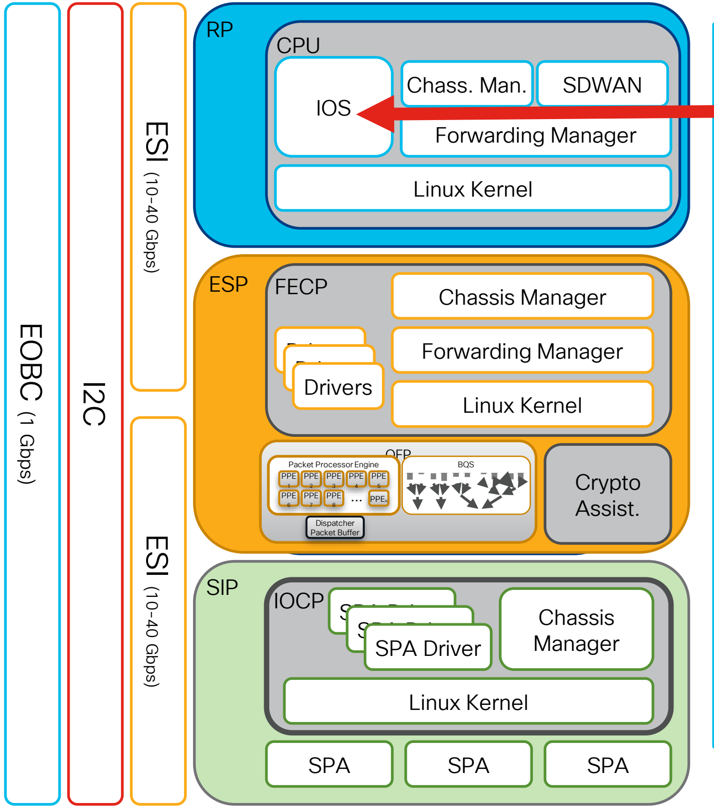
PPE microcode

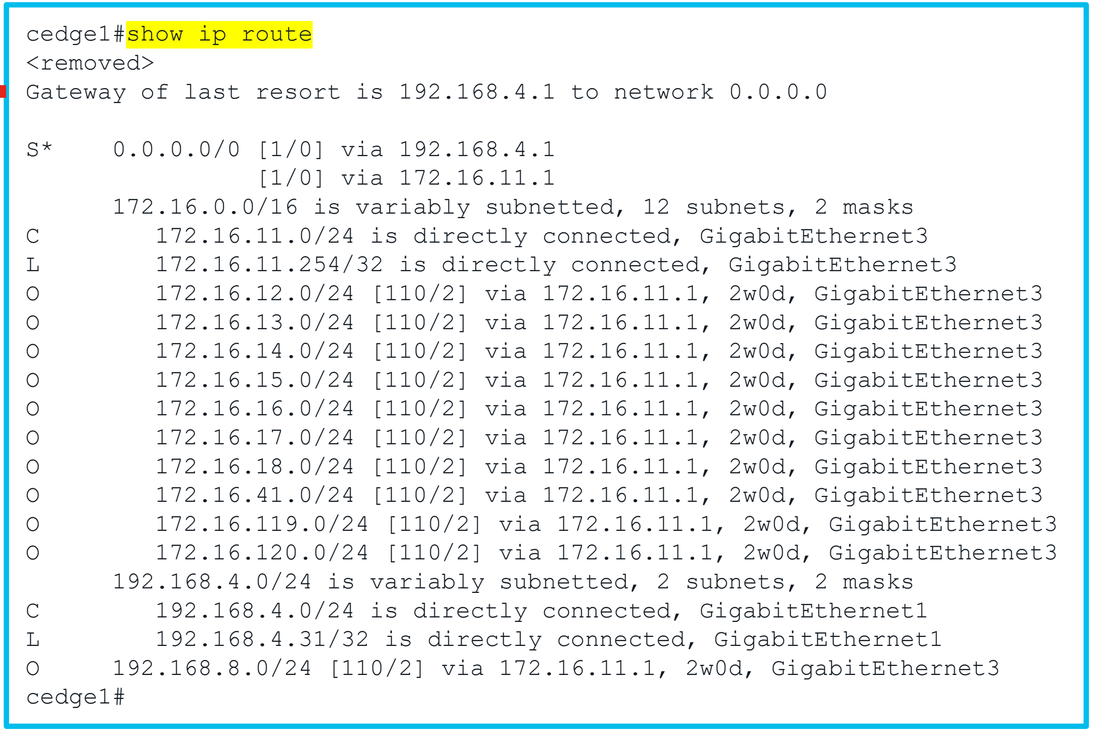


PPE Microcode runs here

- 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

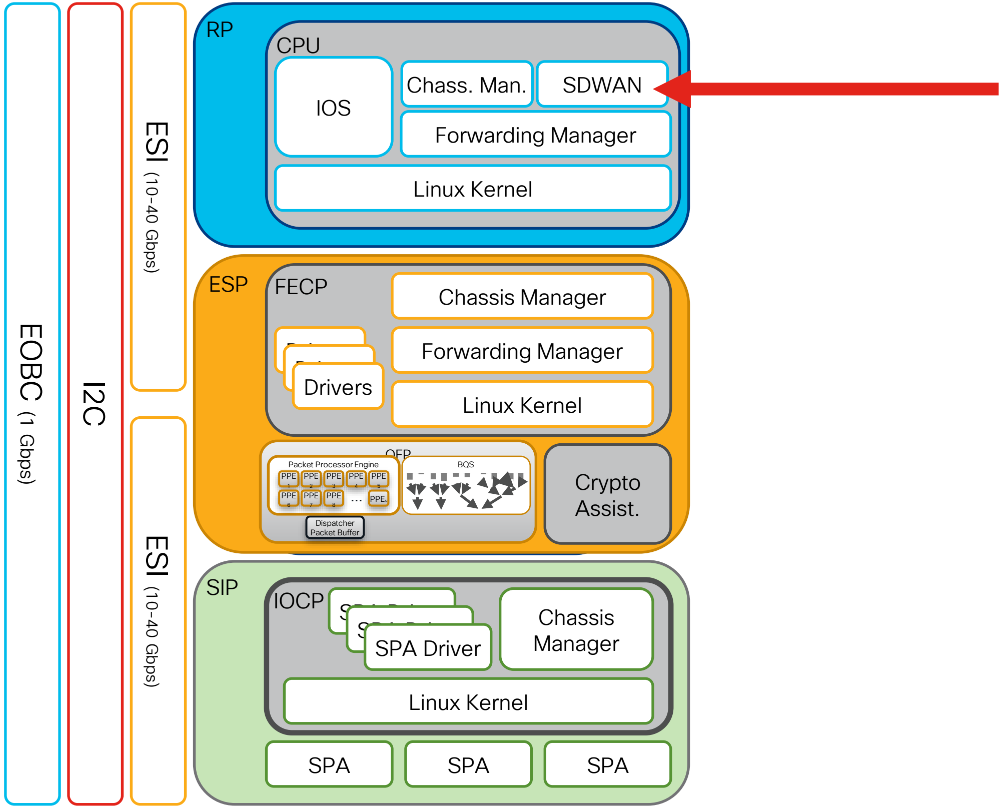
From Architecture to CLI





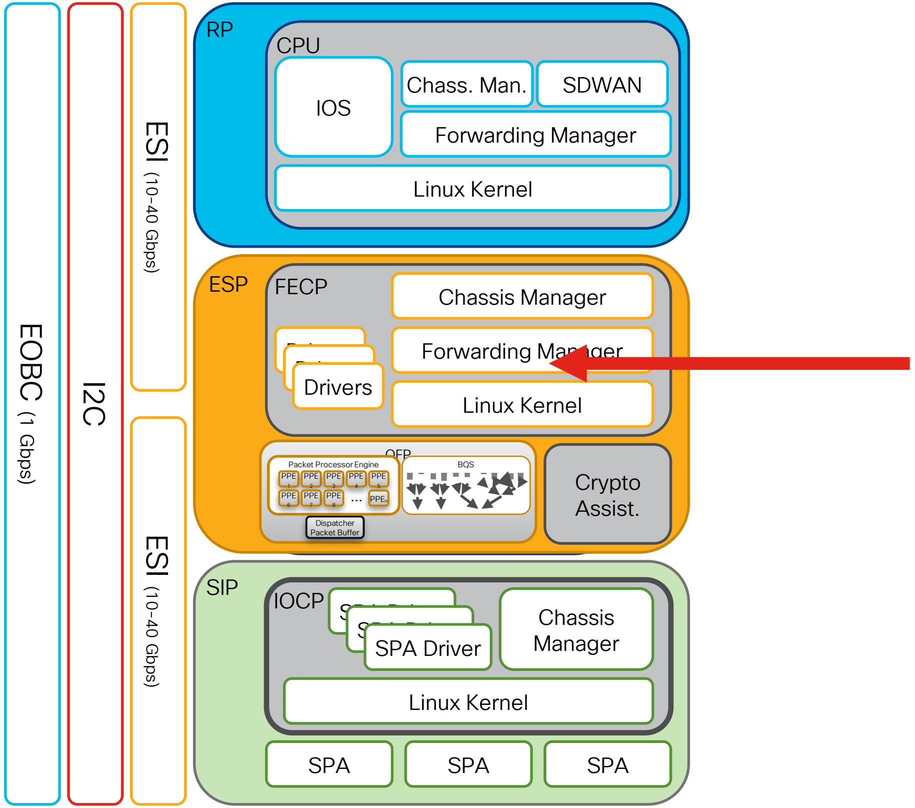
```
cedge1#show ip route
<removed>
Gateway of last resort is 192.168.4.1 to network 0.0.0.0

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



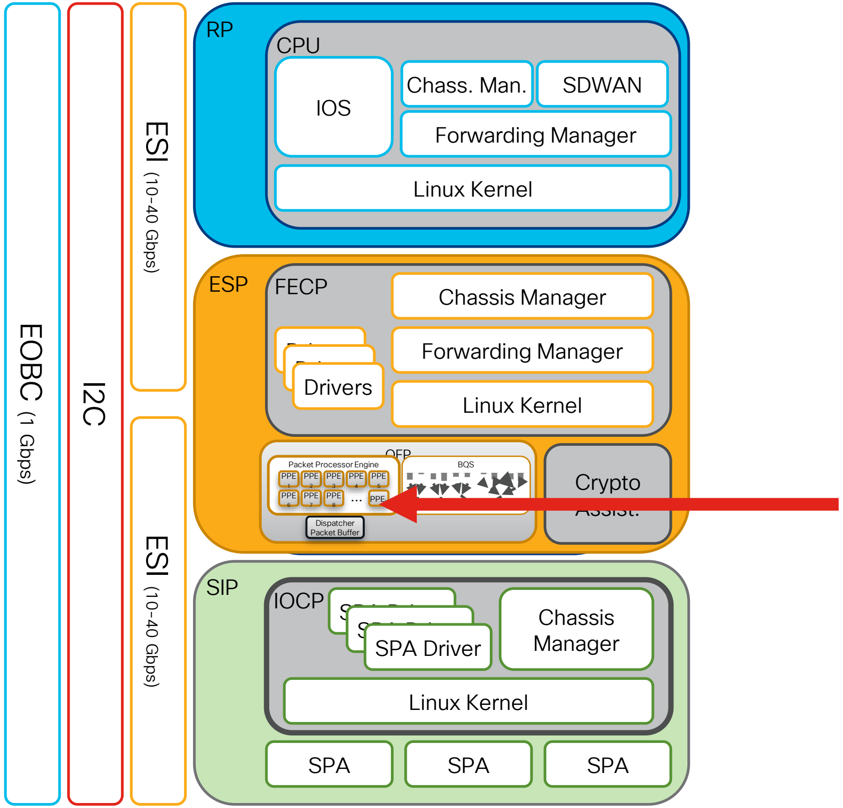
```
cedge6#show sdwan omp summary
oper-state                UP
admin-state               UP
personality               vedge
device-role               Edge-Router
omp-uptime                7:20:50:13
routes-received           316
routes-installed          91
routes-sent               8
tlocs-received            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



```
cedge7#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
```

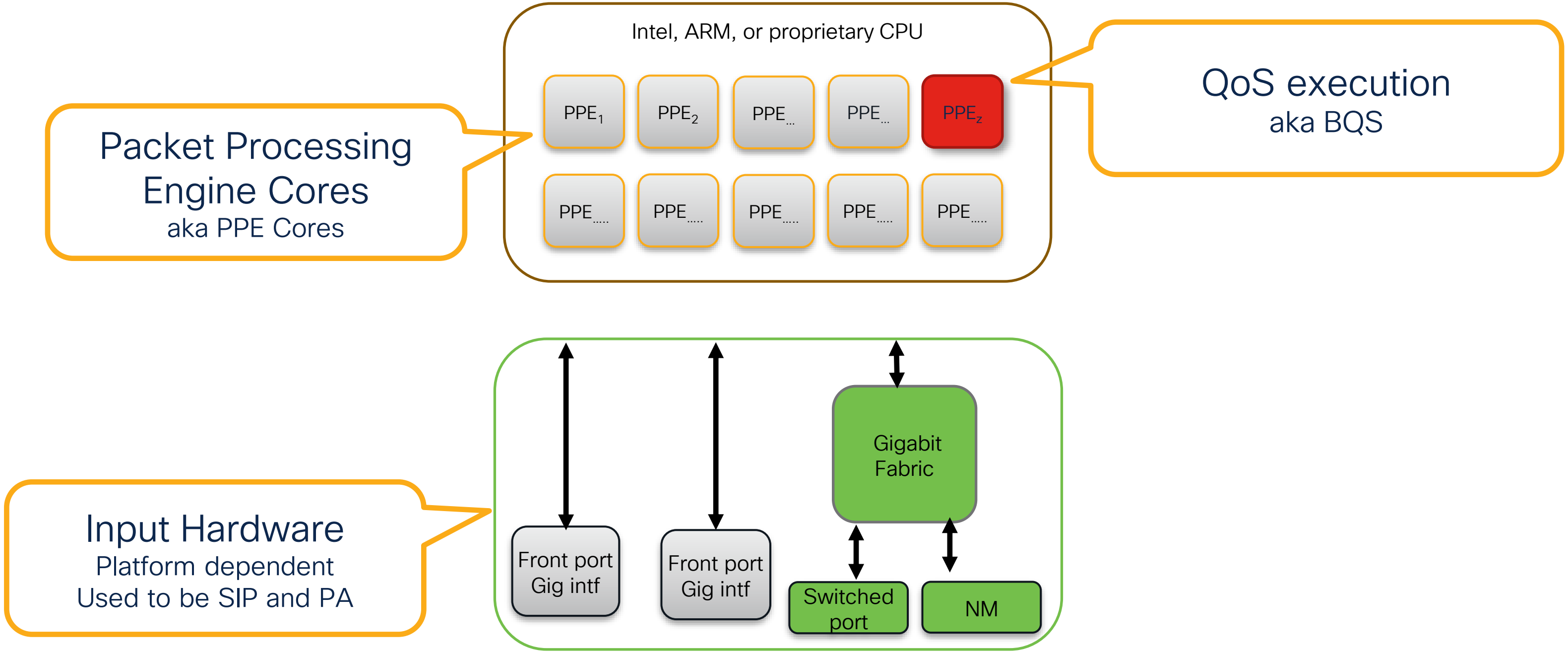
From Architecture to CLI



```
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

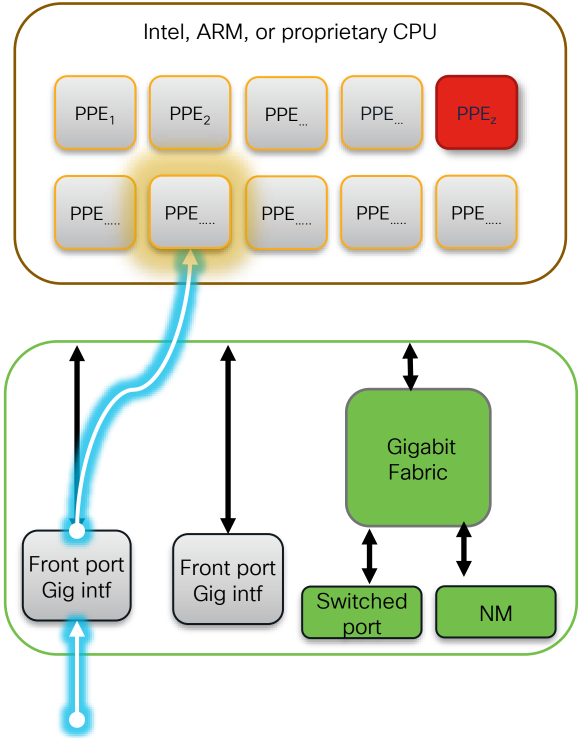


Packet Processing Engine Cores
aka PPE Cores

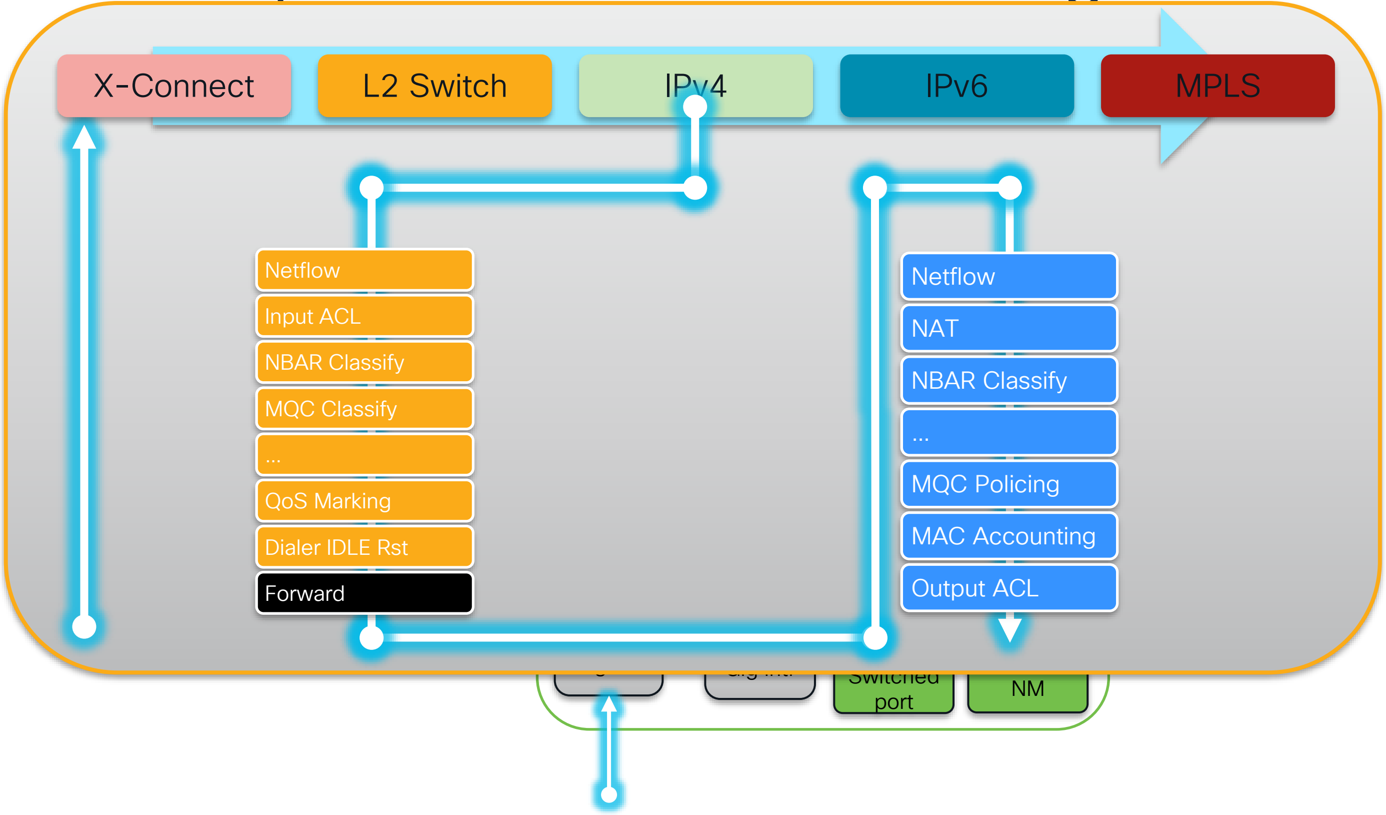
QoS execution
aka BQS

Input Hardware
Platform dependent
Used to be SIP and PA

Life of a packet – Traffic entering interface



Life of a packet – Traffic entering interface



X-Connect

L2 Switch

IPv4

IPv6

MPLS

Netflow

Input ACL

NBAR Classify

MQC Classify

…

QoS Marking

Dialer IDLE Rst

Forward

Netflow

NAT

NBAR Classify

…

MQC Policing

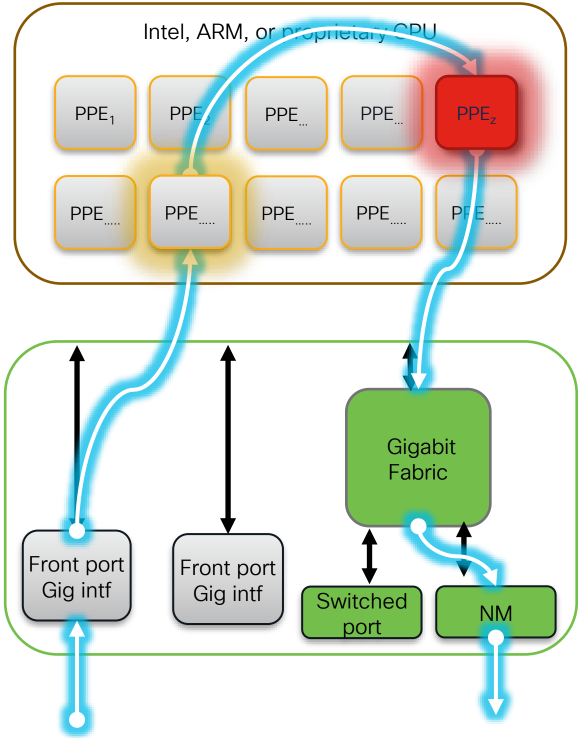
MAC Accounting

Output ACL

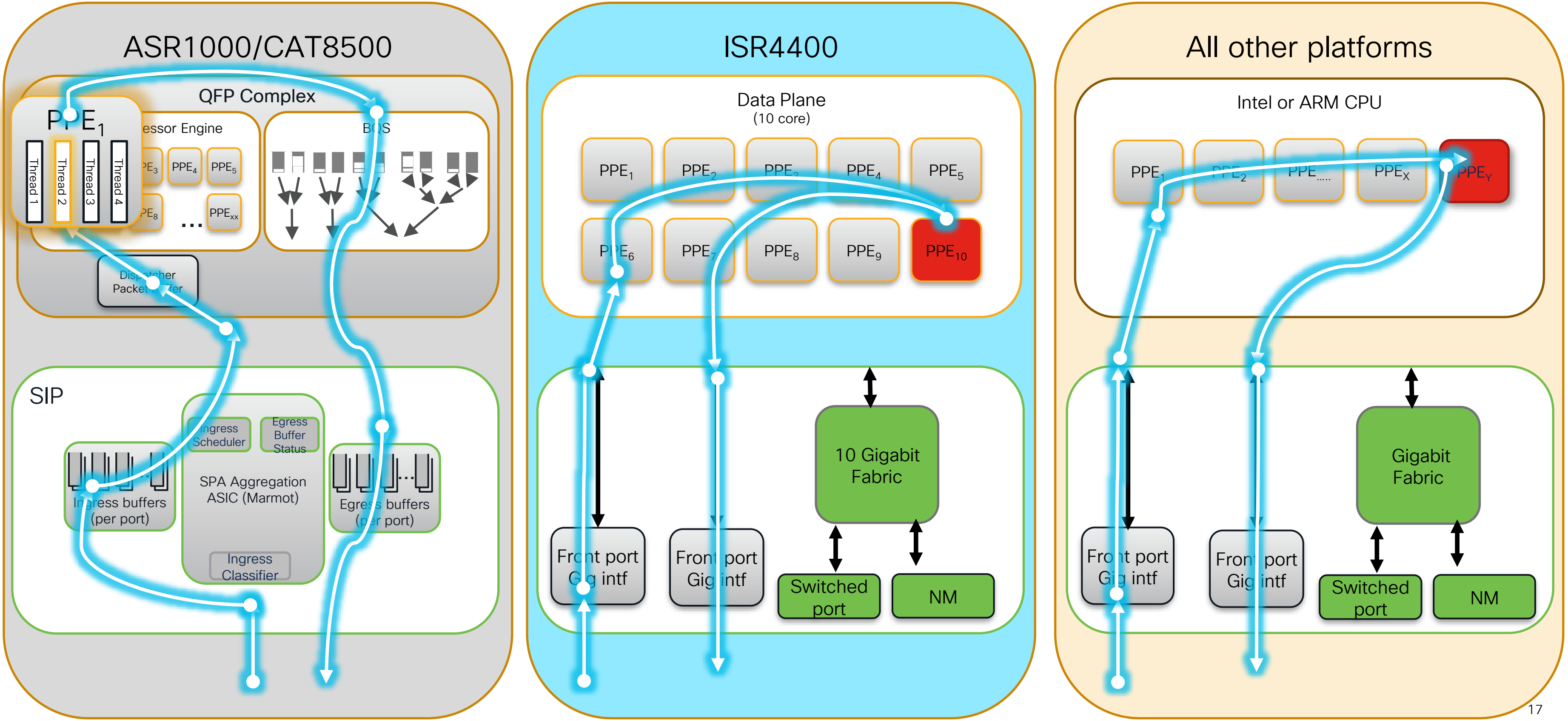
Switched port

NM

Life of a packet – BQS and Exit



Life of a packet – Various Platforms; Same Story



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
[…]
```

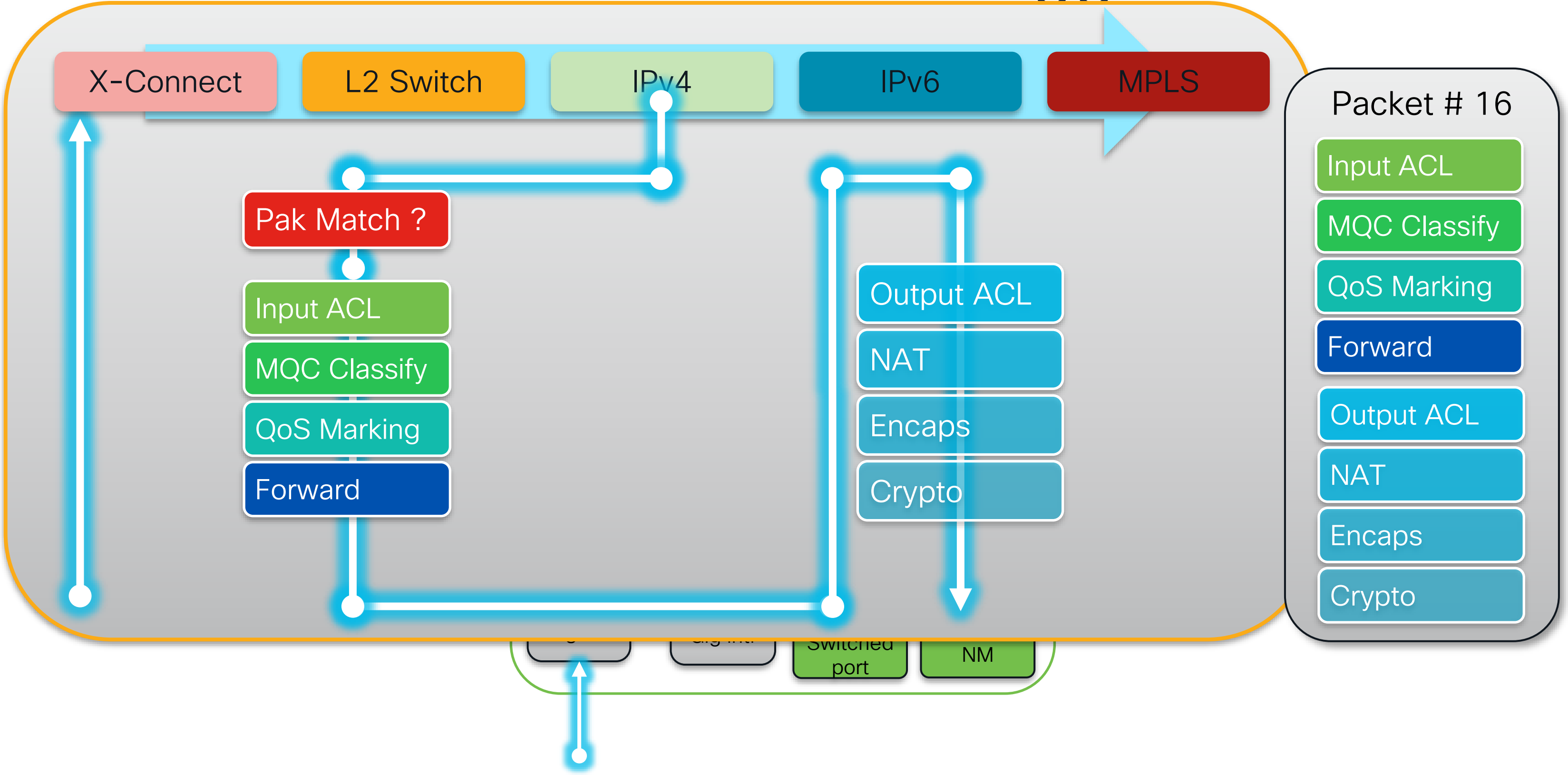
```
Protocol 0 - ipv4_input
FIA handle - CP:0x2fccfe0  DP:0xe73998c0
  IPV4_INPUT_DST_LOOKUP_ISSUE (M)
  IPV4_INPUT_ARL_SANITY (M)
  CBUG_INPUT_FIA
  DEBUG_COND_INPUT_PKT
  IPV4_INPUT_DST_LOOKUP_CONSUME (M)
  IPV4_INPUT_ACL
  IPV4_INPUT_FOR_US_MARTIAN (M)
  IPV4_INPUT_STILE_LEGACY
  IPV4_INPUT_QOS
  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_REFRAG (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



X-Connect

L2 Switch

IPv4

IPv6

MPLS

Pak Match ?

Input ACL

MQC Classify

QoS Marking

Forward

Output ACL

NAT

Encaps

Crypto

Switched port

NM

Packet # 16

Input ACL

MQC Classify

QoS Marking

Forward

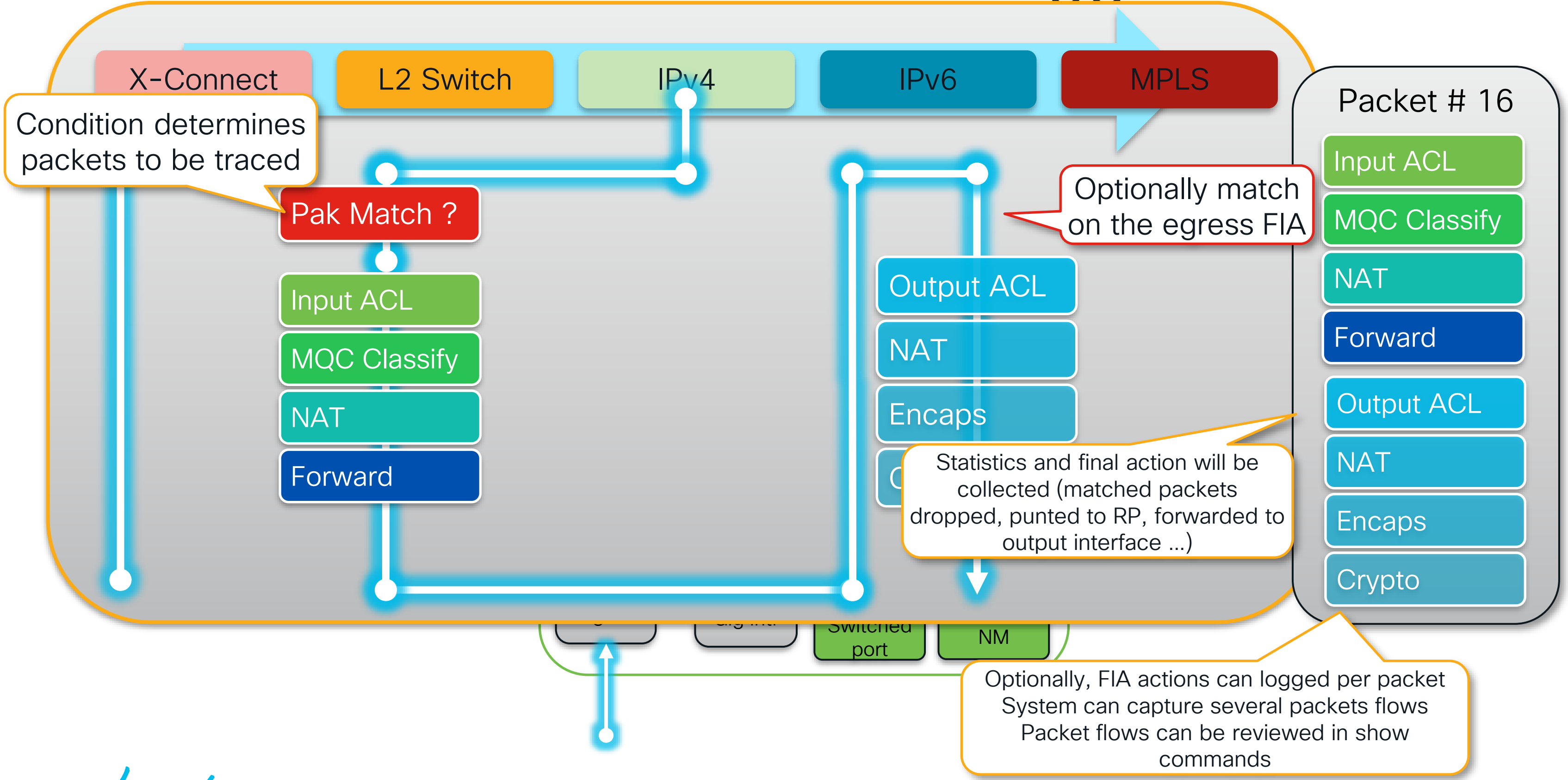
Output ACL

NAT

Encaps

Crypto

The Packet Tracer and FIA Debugger



Condition determines packets to be traced

Optionally match on the egress FIA

Statistics and final action will be collected (matched packets dropped, punted to RP, forwarded to output interface …)

Optionally, FIA actions can logged per packet
System can capture several packets flows
Packet flows can be reviewed in show commands

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
…
```

```
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

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

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
Packets Summary
  Matched  102
  Traced   0
Packets Received
  Ingress  12
  Inject   90
    Count        Code  Cause
    90           9     QFP ICMP generated packet
Packets Processed
  Forward  12
  Punt     0
  Drop     90
    Count        Code  Cause
    13           92    Ipv4Null0
    17           47    FirewallInvalidZone
    60           184   FirewallL4
  Consume  0
```

Extraneous command – was suppressed in 16.3

102 packets were matched by the condition

12 packets were forwarded

90 packets were dropped

13 packets were dropped due to no route

17 packets were dropped due to absence of zone pair

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

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
asr-1k# debug platform packet-trace enable
asr-1k# … !send traffic
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       …
```

Automatically stops tracing after 16 packets

Extraneous command - was suppressed in 16.3

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
asr-1k# debug platform condition start
asr-1k# debug platform packet-trace packet 16
asr-1k# debug platform packet-trace copy packet both [l2 | l3 | l4]
asr-1k# debug platform packet-trace enable
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)
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
```

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

Can store L2, L3 or L4… pick-a-choose

Display the stored packet copy

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

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

```
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  (IpsecInput)
  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       : 0x00000935
  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: [CANA-L7:9]
  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 - 0x841699a8
  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      : GigabtEthernet2
  Lapsed time : 2813 ns

Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE
  Entry       : Input - 0x8166b2ec
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 453 ns
```

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

```
Feature: CBUG_OUTPUT_FIA
  Entry       : Output - 0x8166b1e8
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 533 ns
```

And **now** the packet proceeds along the output FIA.

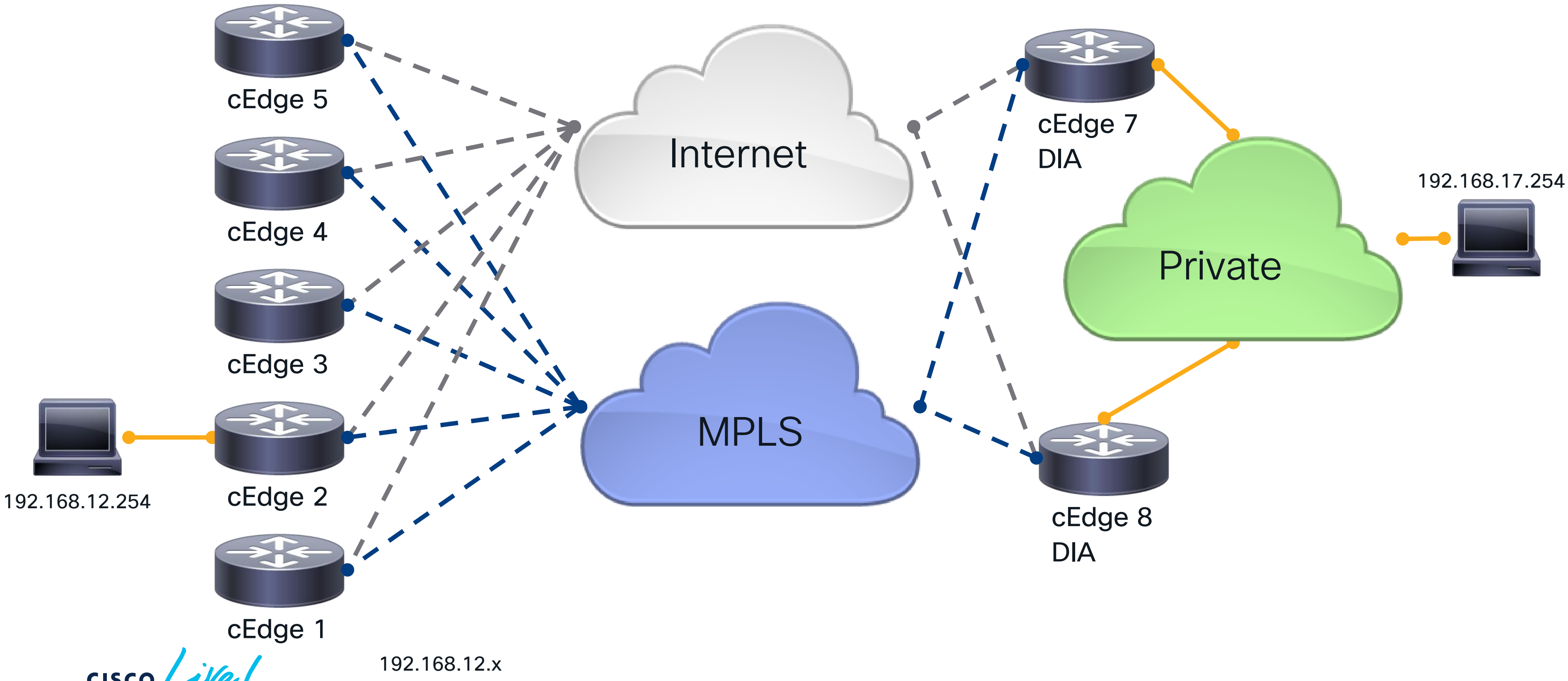
```
Feature: IPV4_VFR_REFRAG
  Entry       : Output - 0x8166b354
  Input       : GigabitEthernet2
  Output      : GigabitEthernet3
  Lapsed time : 320 ns

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
```

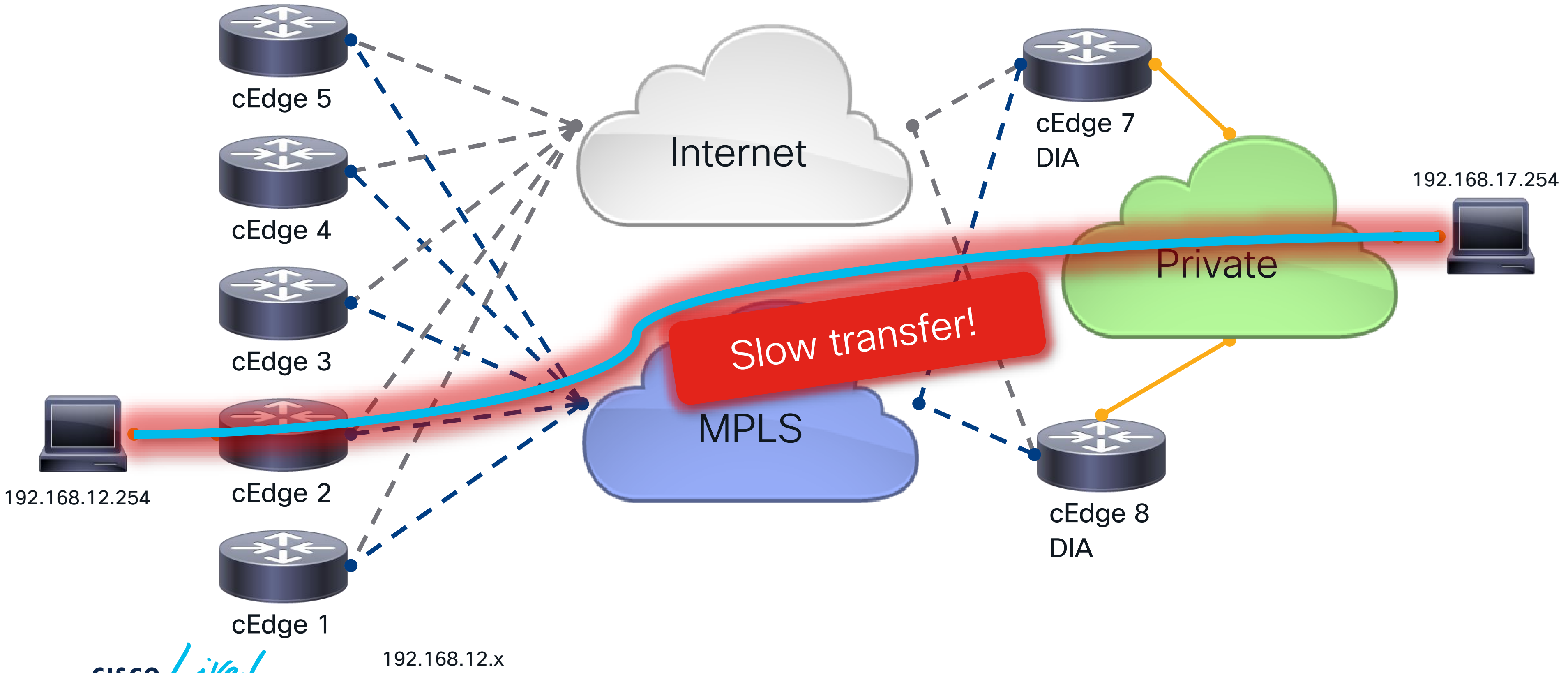
Packet Tracing Ressources

- 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
- CCO Documentation
  - https://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/Packet_Trace.html

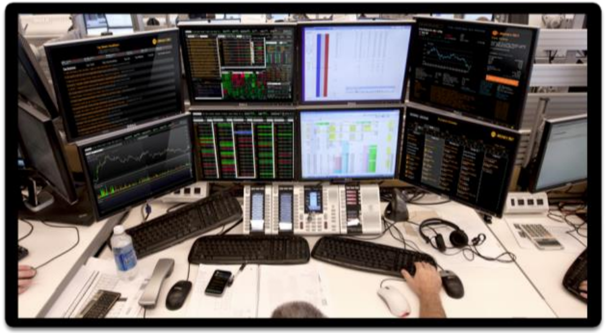
Network Topology

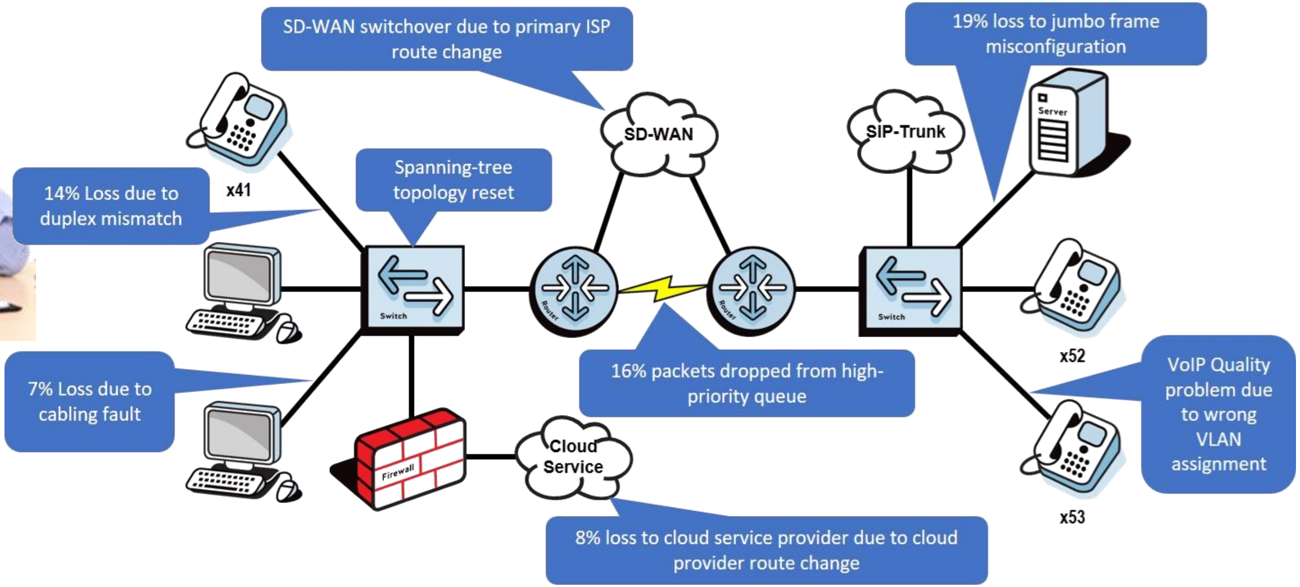


Network Topology



How painful is this ?





SD-WAN switchover due to primary ISP route change

19% loss to jumbo frame misconfiguration

14% Loss due to duplex mismatch

Spanning-tree topology reset

7% Loss due to cabling fault

16% packets dropped from high-priority queue

VoIP Quality problem due to wrong VLAN assignment

8% loss to cloud service provider due to cloud provider route change

Demo

What is RADKit ?

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 automations.

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!

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.

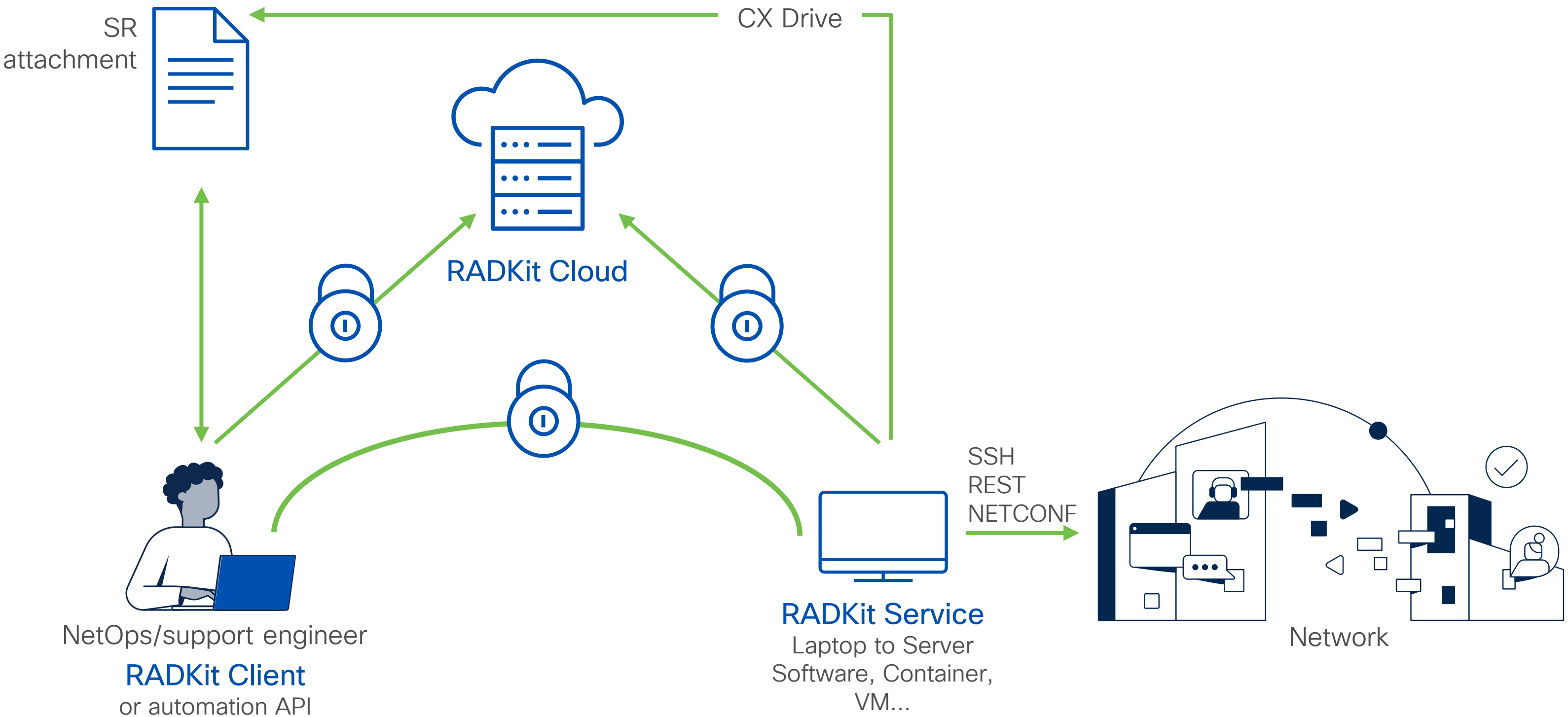
Simplify

Experience a 10x reduction in process complexity

Focus on your workflows and eliminate busywork.

RADKit General Architecture

Visit https://radkit.cisco.com



SR attachment

CX Drive

RADKit Cloud

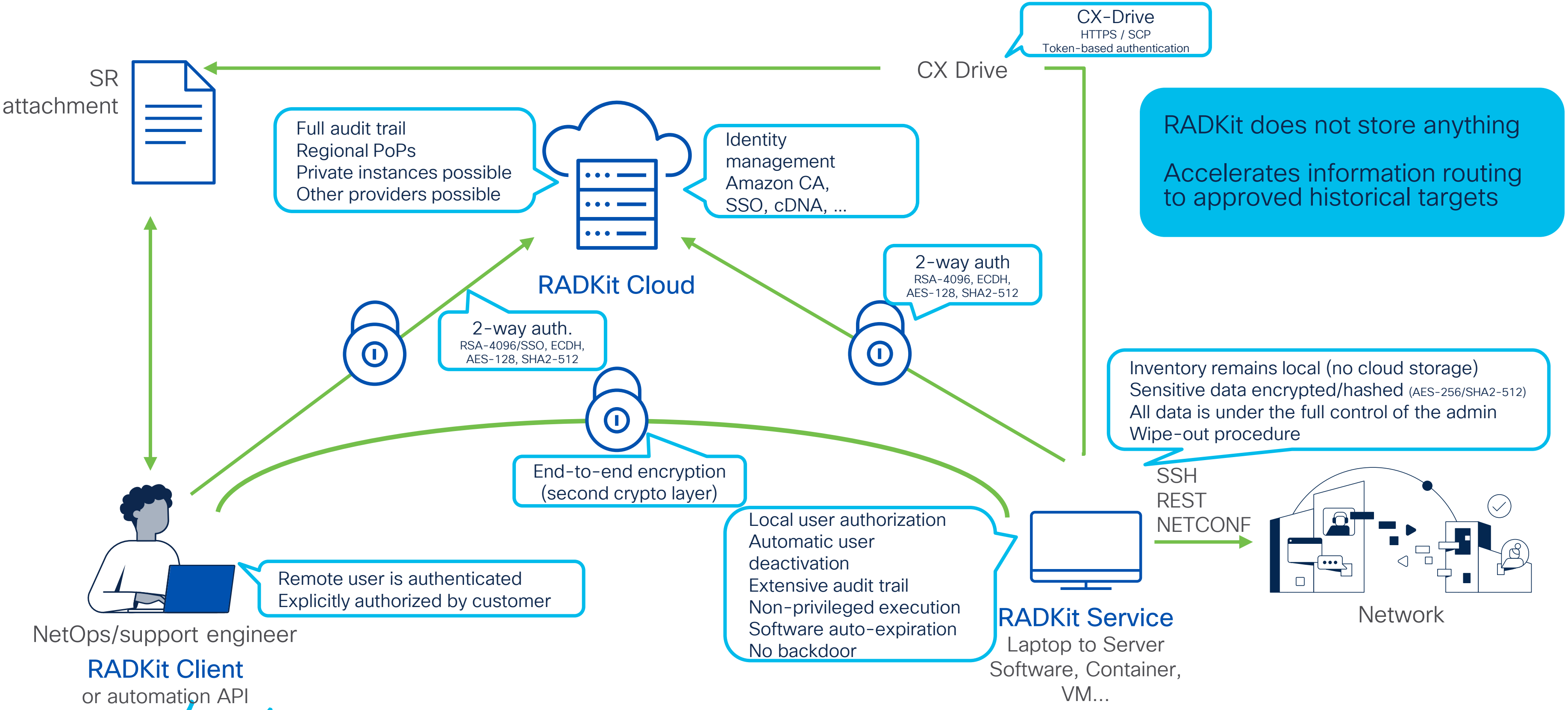
SSH
REST
NETCONF

NetOps/support engineer
RADKit Client
or automation API

RADKit Service
Laptop to Server
Software, Container,
VM...

Network

RADKit Architecture – Security & Data Privacy



CX-Drive
HTTPS / SCP
Token-based authentication

CX Drive

SR attachment

RADKit does not store anything

Accelerates information routing to approved historical targets

Full audit trail
Regional PoPs
Private instances possible
Other providers possible

Identity management
Amazon CA,
SSO, cDNA, ...

RADKit Cloud

2-way auth.
RSA-4096/SSO, ECDH,
AES-128, SHA2-512

2-way auth
RSA-4096, ECDH,
AES-128, SHA2-512

Inventory remains local (no cloud storage)
Sensitive data encrypted/hashed (AES-256/SHA2-512)
All data is under the full control of the admin
Wipe-out procedure

End-to-end encryption
(second crypto layer)

SSH
REST
NETCONF

Network

Local user authorization
Automatic user deactivation
Extensive audit trail
Non-privileged execution
Software auto-expiration
No backdoor

Remote user is authenticated
Explicitly authorized by customer

NetOps/support engineer

RADKit Client
or automation API

RADKit Service
Laptop to Server
Software, Container,
VM...

See more, learn more at the World of Solutions

- ✓ **Visit** https://radkit.cisco.com
- ✓ **Attend** the dedicated RADKit session TACEN-2001
- ✓ **Try** RADKit yourself at the walk-in lab LABARC-2543
- ✓ **Talk** to one of our engineers and ask for a 1:1 RADKit demo at the CX booth

Demo 2

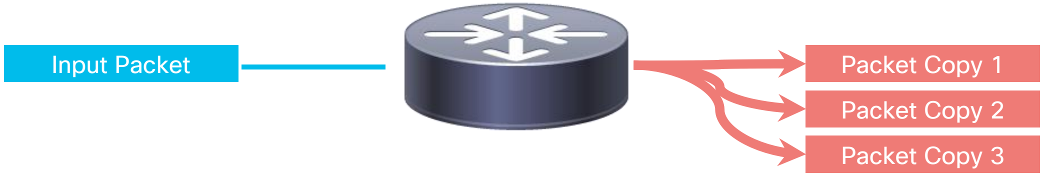
Optional
RADKit + drops on large lab

For reference

Breaking, Multiplying and Gluing Packets

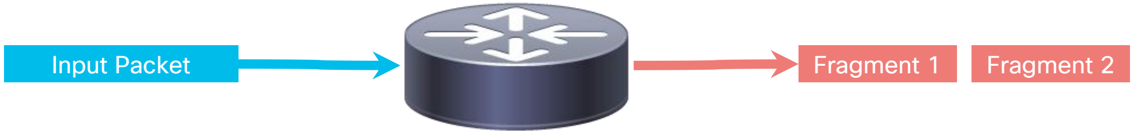
Patterns of Interest

Multicast Replication



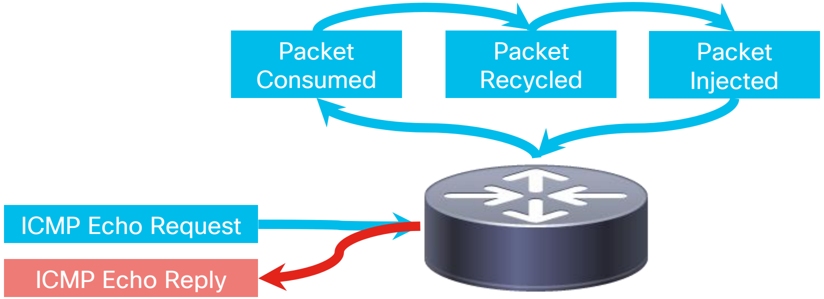
```
0 Gi1    <none>    CONS   Packet Consumed Silently
1 Gi1             Gi2    FWD
2 Gi1             Gi3    FWD
3 Gi1             Gi4    FWD
```

Fragmentation



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

ICMP Echo Request & Reply

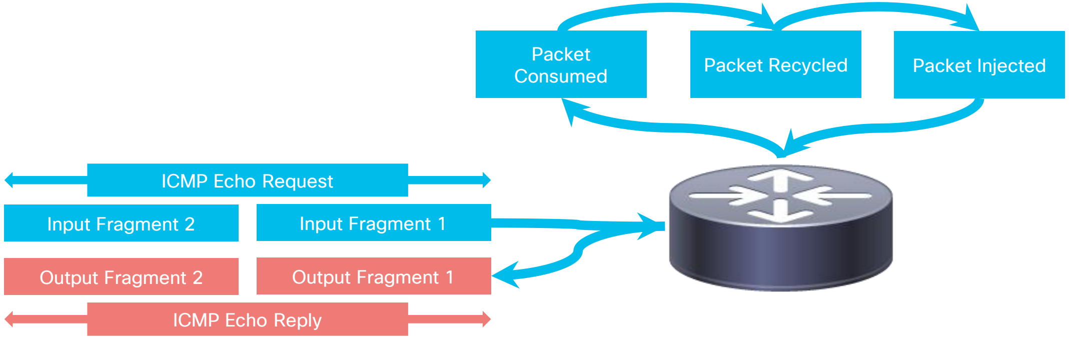


```
0 Gi3    Gi3                    CONS   Packet Consumed
1 Gi3    internal0/0/recycle:0  PUNT   26  (QFP ICMP generated packet)
2 INJ.9  Gi3                    FWD
```

Punt to recycle path; not to RP.
Debug ip icmp will be mute

Reassembly of For-Us Packets

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



```
0 Gi3                   Gi3      CONS   Packet Consumed
1 Gi3                   <none>   CONS   Packet Consumed Silently
2 INJ.9                 <none>   CONS   Packet Consumed Silently
3 internal0/0/recycle:0  Gi3      FWD
4 internal0/0/recycle:0  Gi3      FWD
```

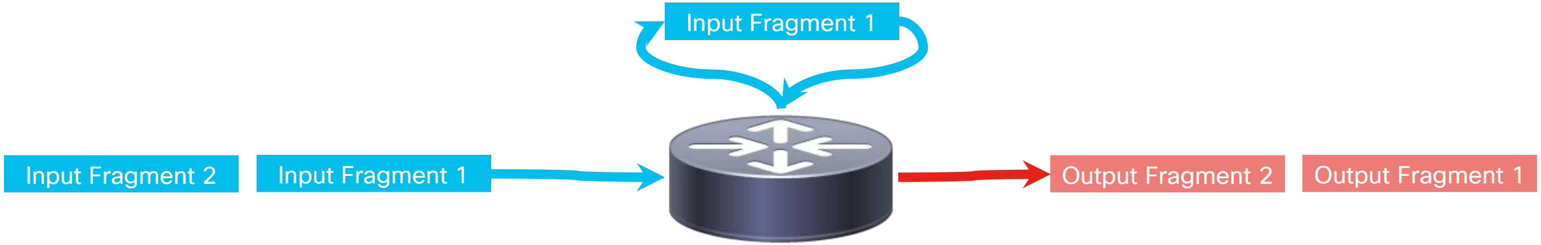
Collect & Reassemble

Emit (Inject) ICMP... too big → consume it for fragmentation

Forward Fragments

Virtual Reassembly of Pass-Thru Packets

- (e.g. with NAT)



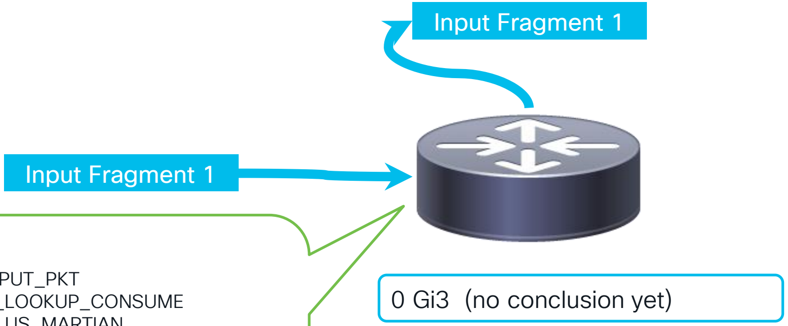
```
0 Gi3  Gi4    FWD
1 Gi3  Gi4    FWD
```

```
Start   : 82194827793981 ns (01/26/2018 13:09:49.929627 UTC)
Stop    : 82194827909191 ns (01/26/2018 13:09:49.929742 UTC)
Total system time = 115260
VFR  Lapsed time : 743813 ns
```

```
Start   : 82194827911554 ns (01/26/2018 13:09:49.929745 UTC)
Stop    : 82194827947614 ns (01/26/2018 13:09:49.929781 UTC)
Total system time = 36060
VFR  Lapsed time : 298093  ns
```

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.

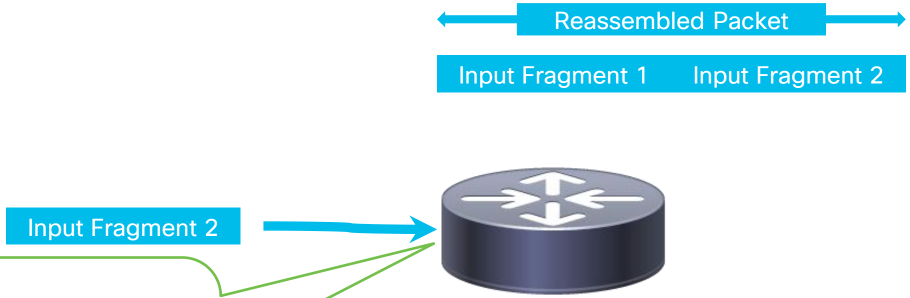
Reassembly of Overlay VPN Packets (I) – e.g. FlexVPN



Feature: IPV4(Input)
Feature: DEBUG_COND_INPUT_PKT
Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
Feature: IPV4_INPUT_FOR_US_MARTIAN
Feature: IPV4_INPUT_LOOKUP_PROCESS
Feature: IPV4_INPUT_IPOPTIONS_PROCESS
Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE
Feature: IPV4_INPUT_IPSEC_TUNNEL_FORUS_EXT

0 Gi3 (no conclusion yet)

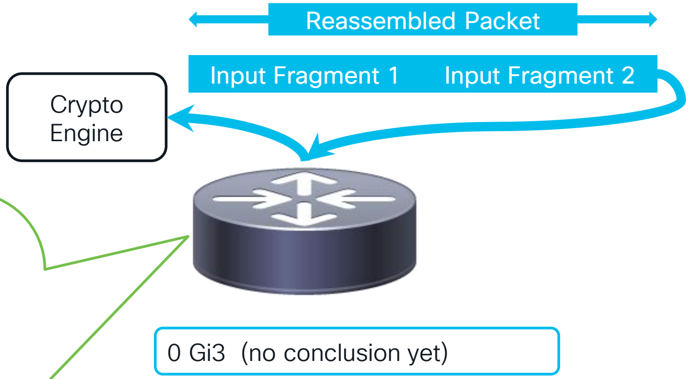
Reassembly of Overlay VPN Packets (II)



```
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
```

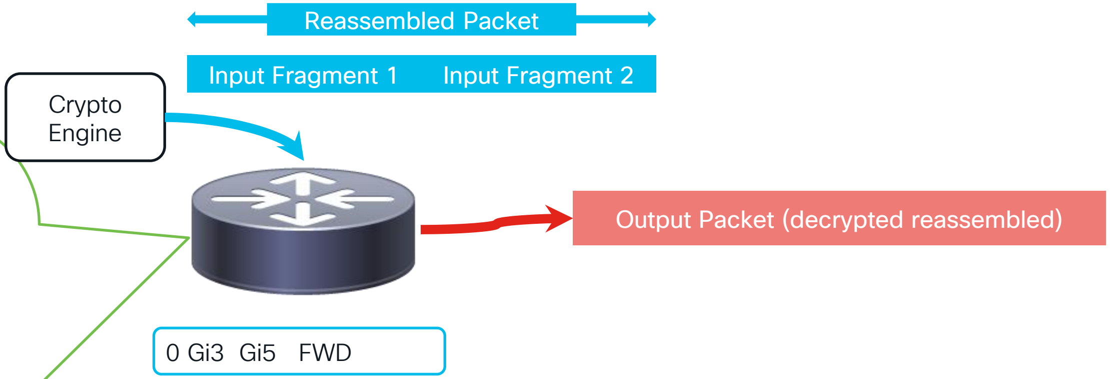
Reassembly of Overlay VPN Packets (III)



```
Feature: IPV4_INPUT_LOOKUP_PROCESS
Feature: IPV4_INPUT_IPOPTIONS_PROCESS
Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE
IPV4_INPUT_IPSEC_TUNNEL_FORUS_EXT
Feature: IPSec
    Action    : DECRYPT
    SA Handle : 7
    SPI       : 0x209cd024
    Peer Addr : 172.18.1.6
    Local Addr: 172.18.1.5
Feature: IPV4_INPUT_IPSEC_CLASSIFY_EXT
    Entry      : Input - 0x816a0e3c
    Input      : Tunnel0
    Output      : <unknown>
    Lapsed time : 10246 ns
 Feature: IPV4_INPUT_IPSEC_INLINE_PROCESS_EXT
```

Reassembly of Overlay VPN Packets (IV)

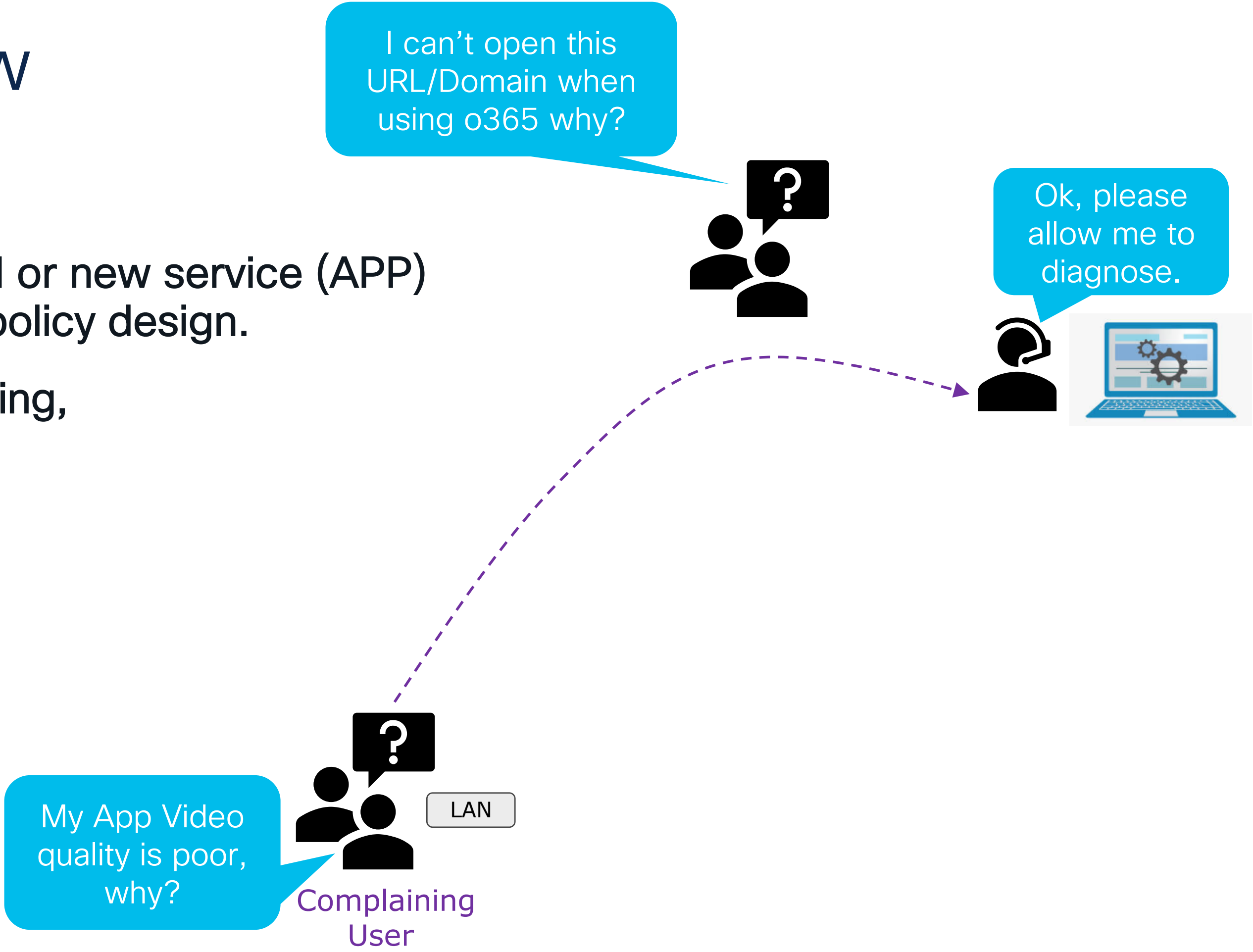
```
Feature: IPV4_INPUT_IPSEC_TUNNEL_RERUN_JUMP_EXT
Feature: IPV4_INPUT_SANITY_EXT
Feature: IPV4_INPUT_ARL_EXT
Feature: IPV4_INPUT_IPSEC_POST_PROCESS_EXT
Feature: IPV4_INPUT_DST_LOOKUP_ISSUE_EXT
Feature: IPV4_INPUT_SRC_LOOKUP_ISSUE_EXT
Feature: IPV4_INPUT_IPSEC_DOUBLE_ACL_EXT
Feature: IPV4_INPUT_DST_LOOKUP_CONSUME_EXT
Feature: IPV4_INPUT_SRC_LOOKUP_CONSUME_EXT
Feature: IPV4_INPUT_FOR_US_EXT
Feature: IPV4_IPSEC_FEATURE_RETURN_EXT
Feature: IPV4_INPUT_TUNNEL_IPSEC_DECAP_EXT
Feature: IPV4_TUNNEL_PROTECT_GOTO_INPUT_TUNNEL_EXT
Feature: IPV4_INPUT_DST_LOOKUP_ISSUE
Feature: IPV4_INPUT_ARL_SANITY
Feature: CBUG_INPUT_FIA
Feature: DEBUG_COND_INPUT_PKT
Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
Feature: IPV4_INPUT_FOR_US_MARTIAN
Feature: IPV4_INPUT_LOOKUP_PROCESS
Feature: IPV4_INPUT_IPOPTIONS_PROCESS
Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE
Feature: IPV4_VFR_REFRAG
Feature: IPV4_OUTPUT_L2_REWRITE
Feature: IPV4_OUTPUT_FRAG
Feature: IPV4_OUTPUT_DROP_POLICY
Feature: MARMOT_SPA_D_TRANSMIT_PKT
```



SDWAN’s Network wide Path Insight

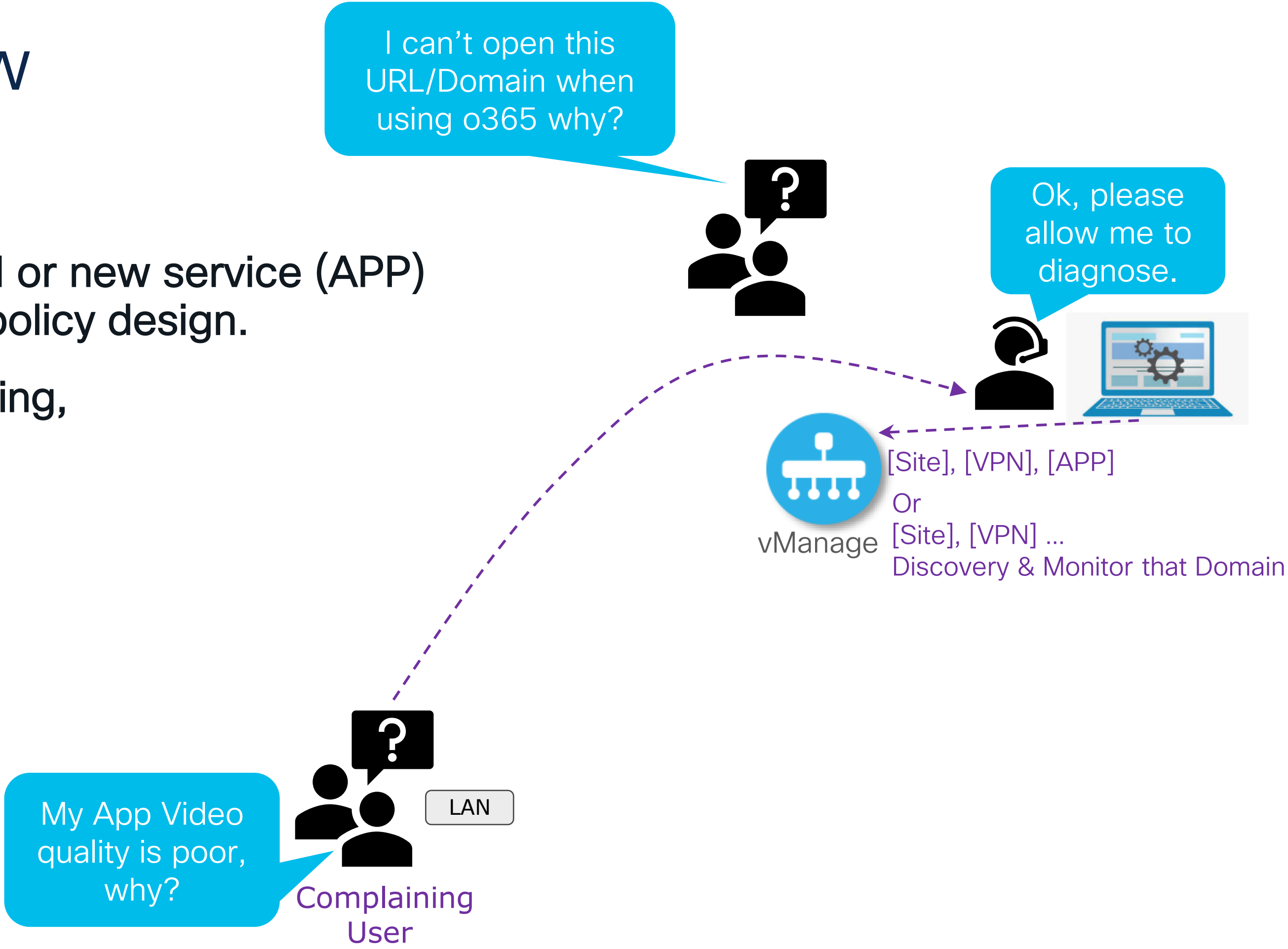
NWPI Workflow

- IT deploy new site, new VPN or new service (APP) and need to verify network/policy design.
- Daily network/policy monitoring, reaction to Events/Alarms.
- Customer Support, e.g.
  User from this [Site], [VPN], complaining about
  this [APP] or [Domain/URL].


I can't open this URL/Domain when using o365 why?
Ok, please allow me to diagnose.
My App Video quality is poor, why?
LAN
Complaining User

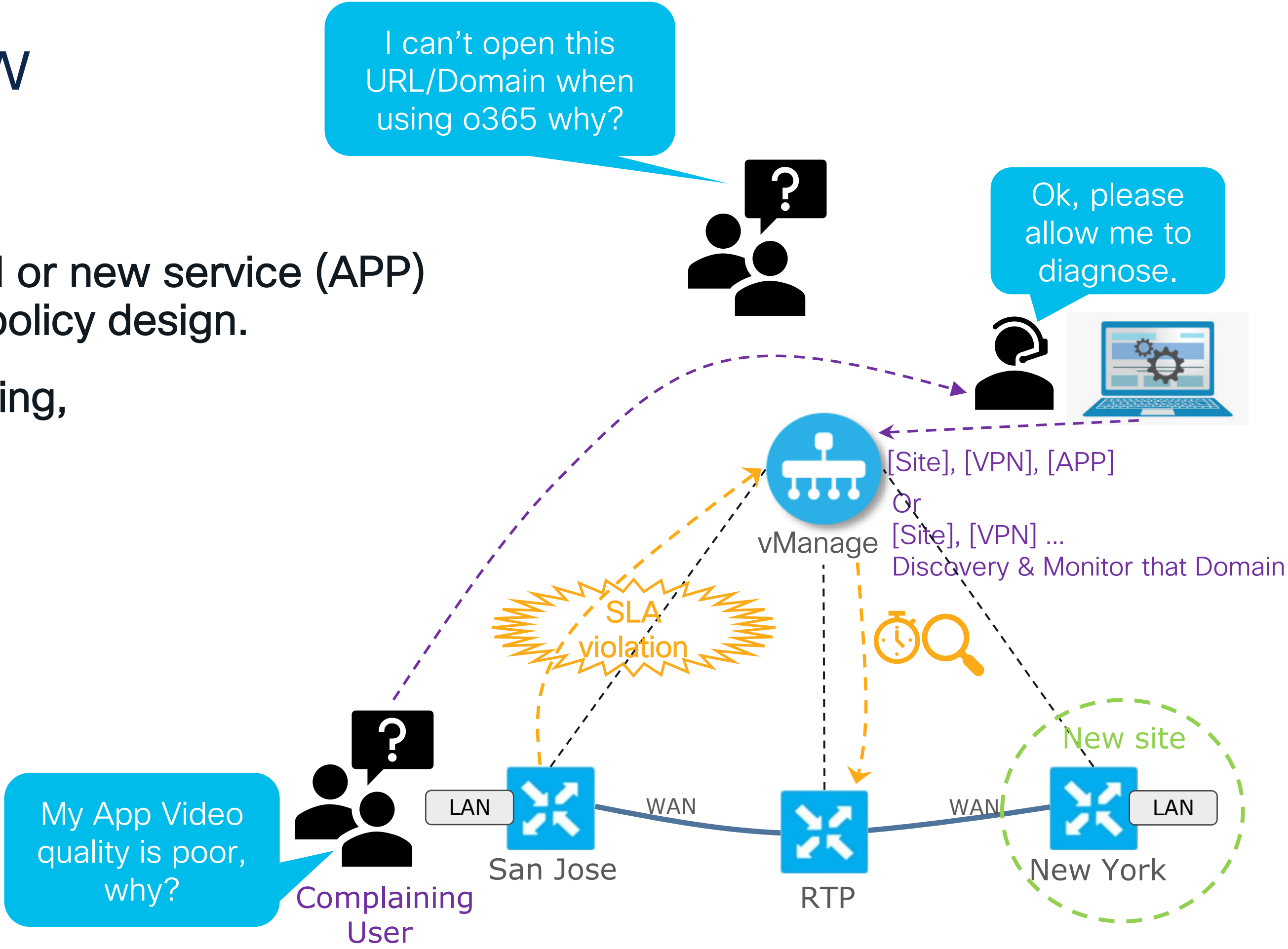
NWPI Workflow

- IT deploy new site, new VPN or new service (APP) and need to verify network/policy design.
- Daily network/policy monitoring, reaction to Events/Alarms.
- Customer Support, e.g. User from this [Site], [VPN], complaining about this [APP] or [Domain/URL].


I can't open this URL/Domain when using o365 why?
Ok, please allow me to diagnose.
vManage
[Site], [VPN], [APP]
Or
[Site], [VPN] ...
Discovery & Monitor that Domain
My App Video quality is poor, why?
LAN
Complaining User

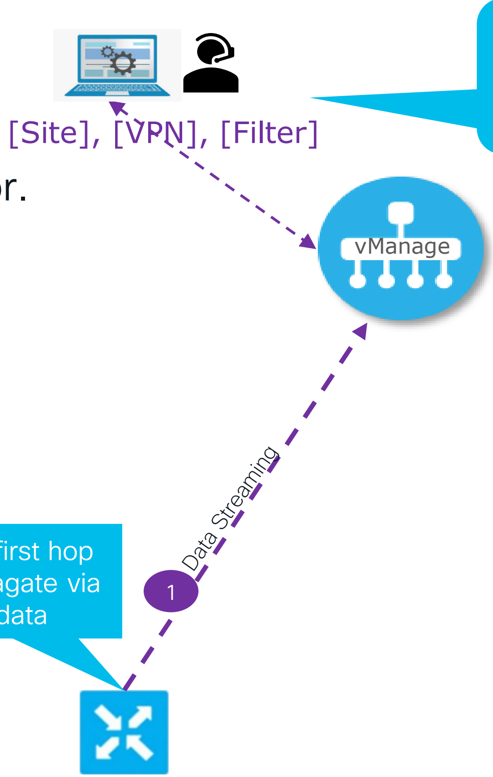
NWPI Workflow

- IT deploy new site, new VPN or new service (APP) and need to verify network/policy design.
- Daily network/policy monitoring, reaction to Events/Alarms.
- Customer Support, e.g. User from this [Site], [VPN], complaining about this [APP] or [Domain/URL].


I can't open this URL/Domain when using o365 why?
Ok, please allow me to diagnose.
vManage
[Site], [VPN], [APP]
Or
[Site], [VPN] ...
Discovery & Monitor that Domain
SLA violation
New site
LAN
WAN
WAN
LAN
San Jose
RTP
New York
My App Video quality is poor, why?
Complaining User

NWPI – Transitive Marking

- Currently works on demand: Trace and Monitor.
  - 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.

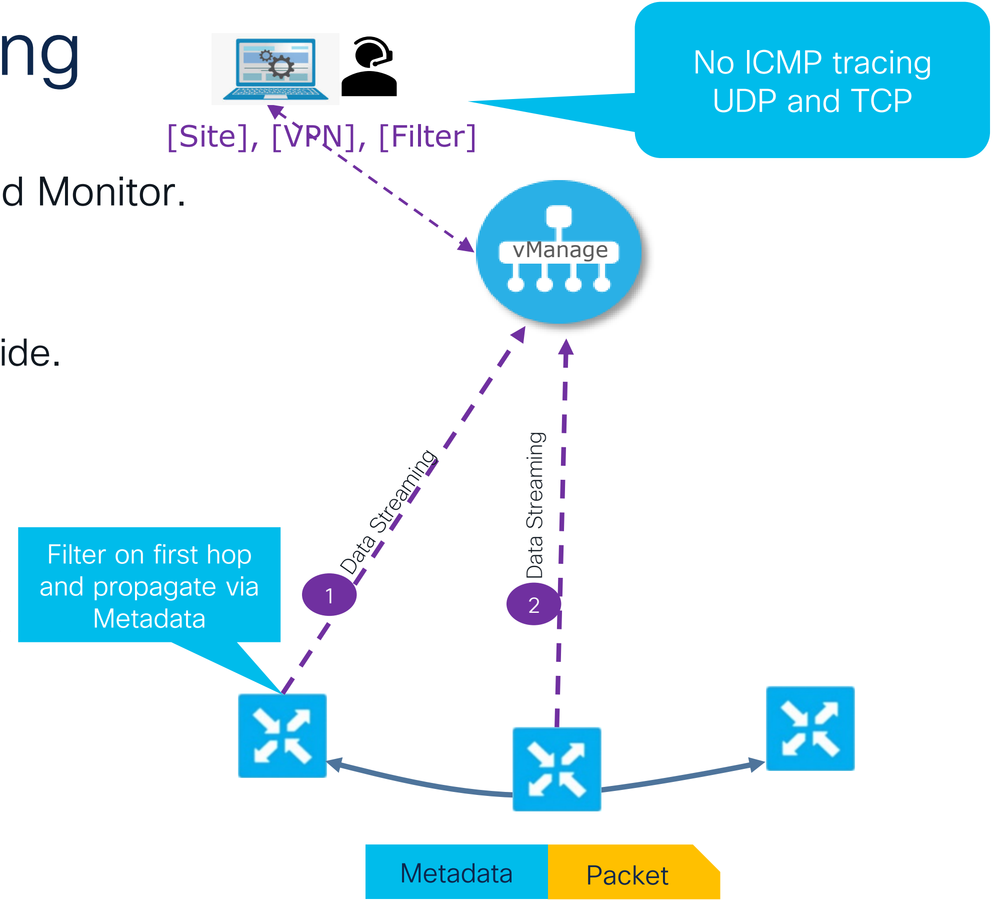


No ICMP tracing
UDP and TCP

Filter on first hop and propagate via Metadata

NWPI – Transitive Marking

- Currently works on demand: Trace and Monitor.
  - 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.

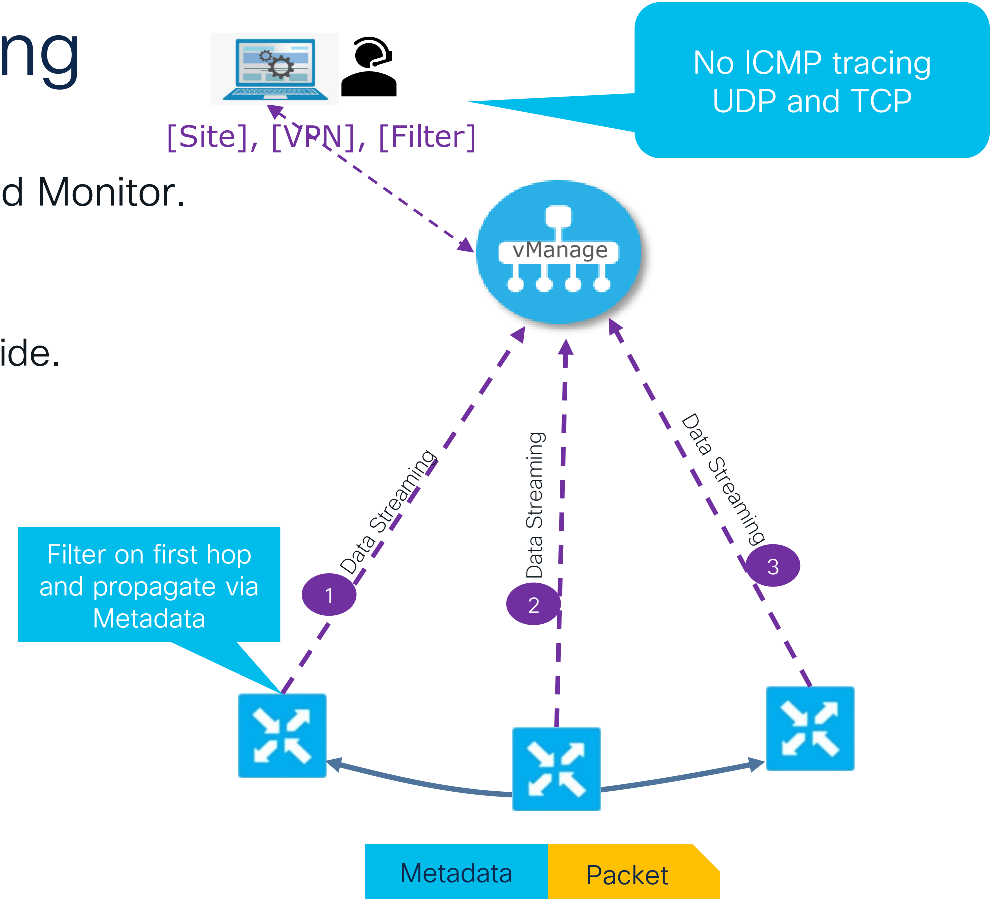


No ICMP tracing UDP and TCP

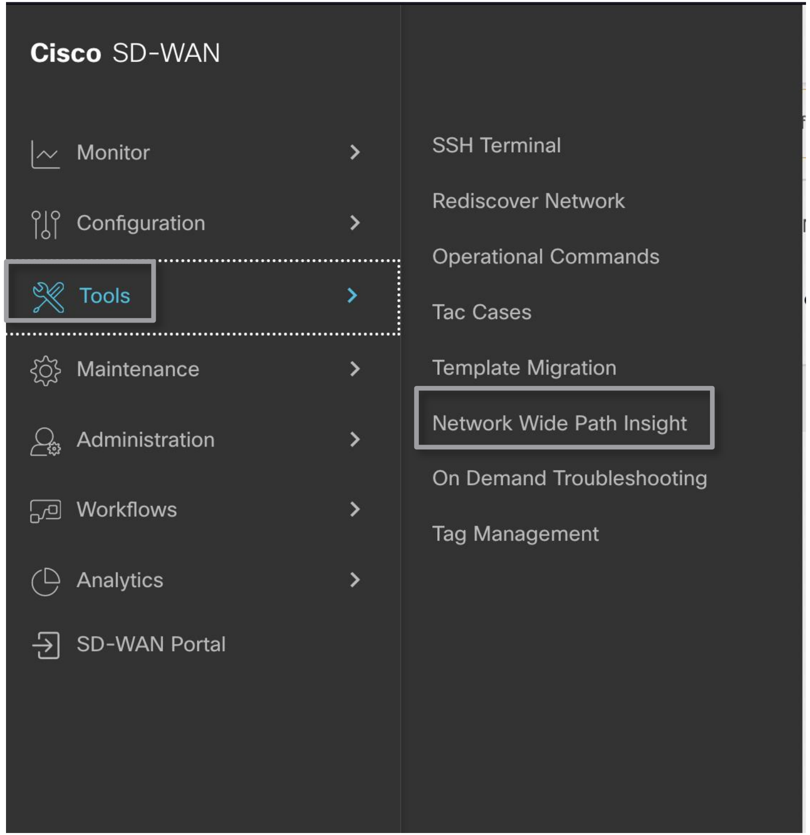
Filter on first hop and propagate via Metadata

NWPI – Transitive Marking

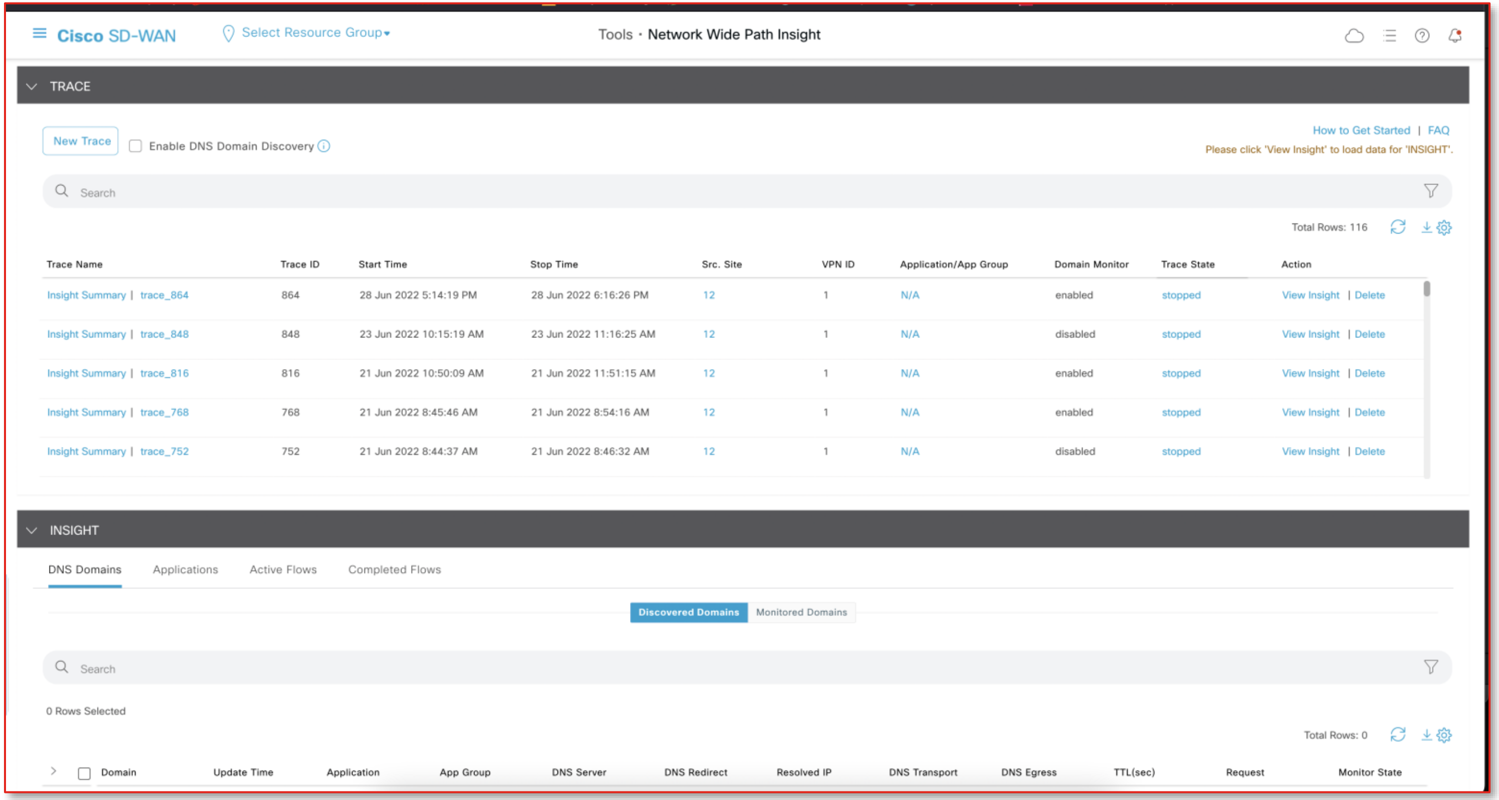
- Currently works on demand: Trace and Monitor.
  - On demand enable filter ONLY on the 1st hop router.
  - No persistent configuration network wide.
- Metadata triggered flow metrics and trace streaming to vWanage.
- vManage correlates multiple devices and data sources to visualize per flow End to End insight views in UI.



Navigating to NWPI



Navigating to NWPI



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'.

Search

Total Rows: 116

Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain Monitor	Trace State	Action
Insight Summary | trace_864	864	28 Jun 2022 5:14:19 PM	28 Jun 2022 6:16:26 PM	12	1	N/A	enabled	stopped	View Insight | Delete
Insight Summary | trace_848	848	23 Jun 2022 10:15:19 AM	23 Jun 2022 11:16:25 AM	12	1	N/A	disabled	stopped	View Insight | Delete
Insight Summary | trace_816	816	21 Jun 2022 10:50:09 AM	21 Jun 2022 11:51:15 AM	12	1	N/A	enabled	stopped	View Insight | Delete
Insight Summary | trace_768	768	21 Jun 2022 8:45:46 AM	21 Jun 2022 8:54:16 AM	12	1	N/A	enabled	stopped	View Insight | Delete
Insight Summary | trace_752	752	21 Jun 2022 8:44:37 AM	21 Jun 2022 8:46:32 AM	12	1	N/A	disabled	stopped	View Insight | Delete

INSIGHT

DNS Domains | Applications | Active Flows | Completed Flows

Discovered Domains | Monitored Domains

Search

0 Rows Selected

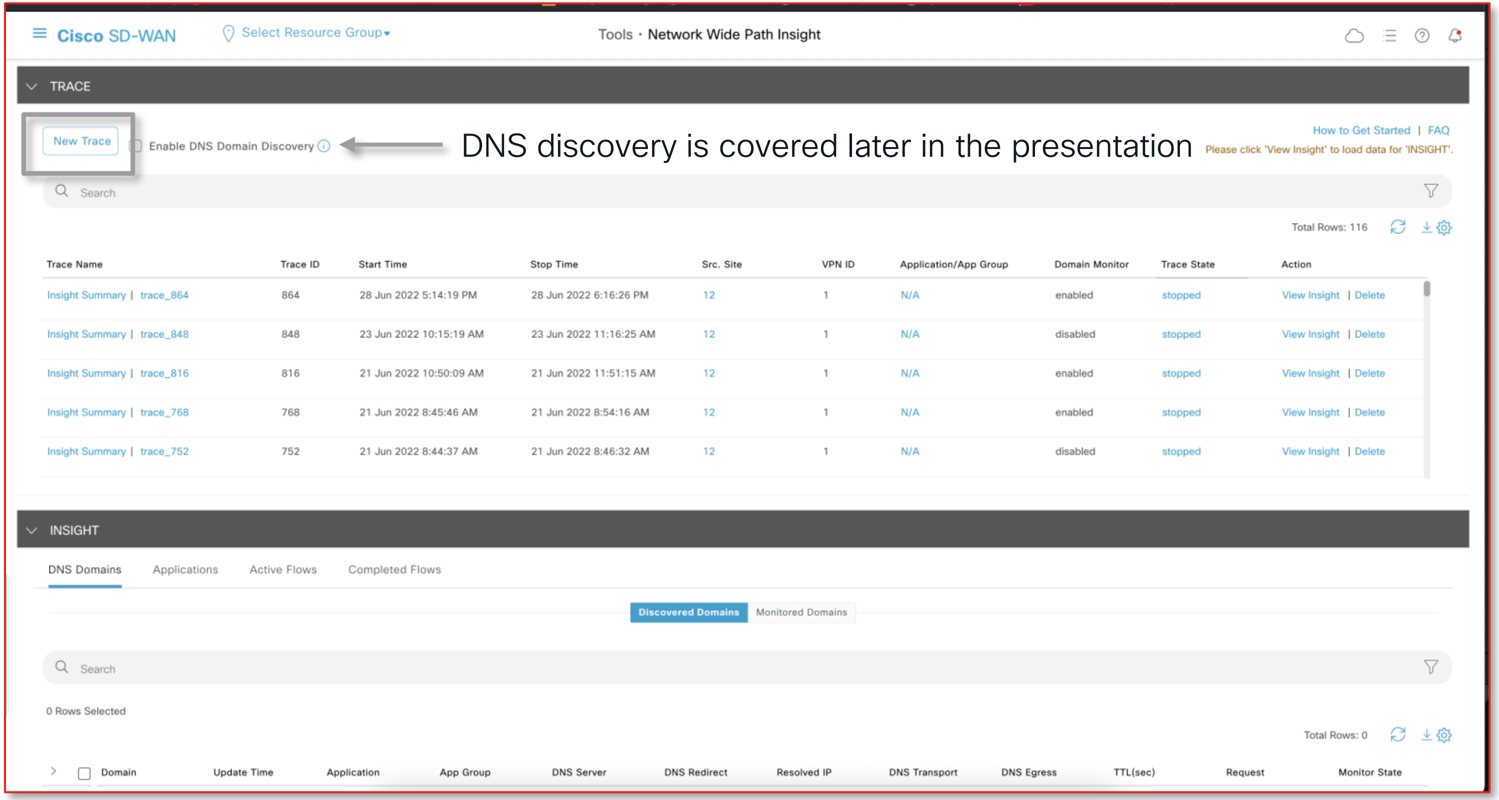
Total Rows: 0

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

Demo

Setting a condition – activate tracing [without DNS discovery]

Create new trace



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

TRACE

New Trace | □ Enable DNS Domain Discovery ⓘ

DNS discovery is covered later in the presentation

How to Get Started | FAQ

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

Search

Total Rows: 116

Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain Monitor	Trace State	Action
Insight Summary | trace_864	864	28 Jun 2022 5:14:19 PM	28 Jun 2022 6:16:26 PM	12	1	N/A	enabled	stopped	View Insight | Delete
Insight Summary | trace_848	848	23 Jun 2022 10:15:19 AM	23 Jun 2022 11:16:25 AM	12	1	N/A	disabled	stopped	View Insight | Delete
Insight Summary | trace_816	816	21 Jun 2022 10:50:09 AM	21 Jun 2022 11:51:15 AM	12	1	N/A	enabled	stopped	View Insight | Delete
Insight Summary | trace_768	768	21 Jun 2022 8:45:46 AM	21 Jun 2022 8:54:16 AM	12	1	N/A	enabled	stopped	View Insight | Delete
Insight Summary | trace_752	752	21 Jun 2022 8:44:37 AM	21 Jun 2022 8:46:32 AM	12	1	N/A	disabled	stopped	View Insight | Delete

INSIGHT

DNS Domains | Applications | Active Flows | Completed Flows

Discovered Domains | Monitored Domains

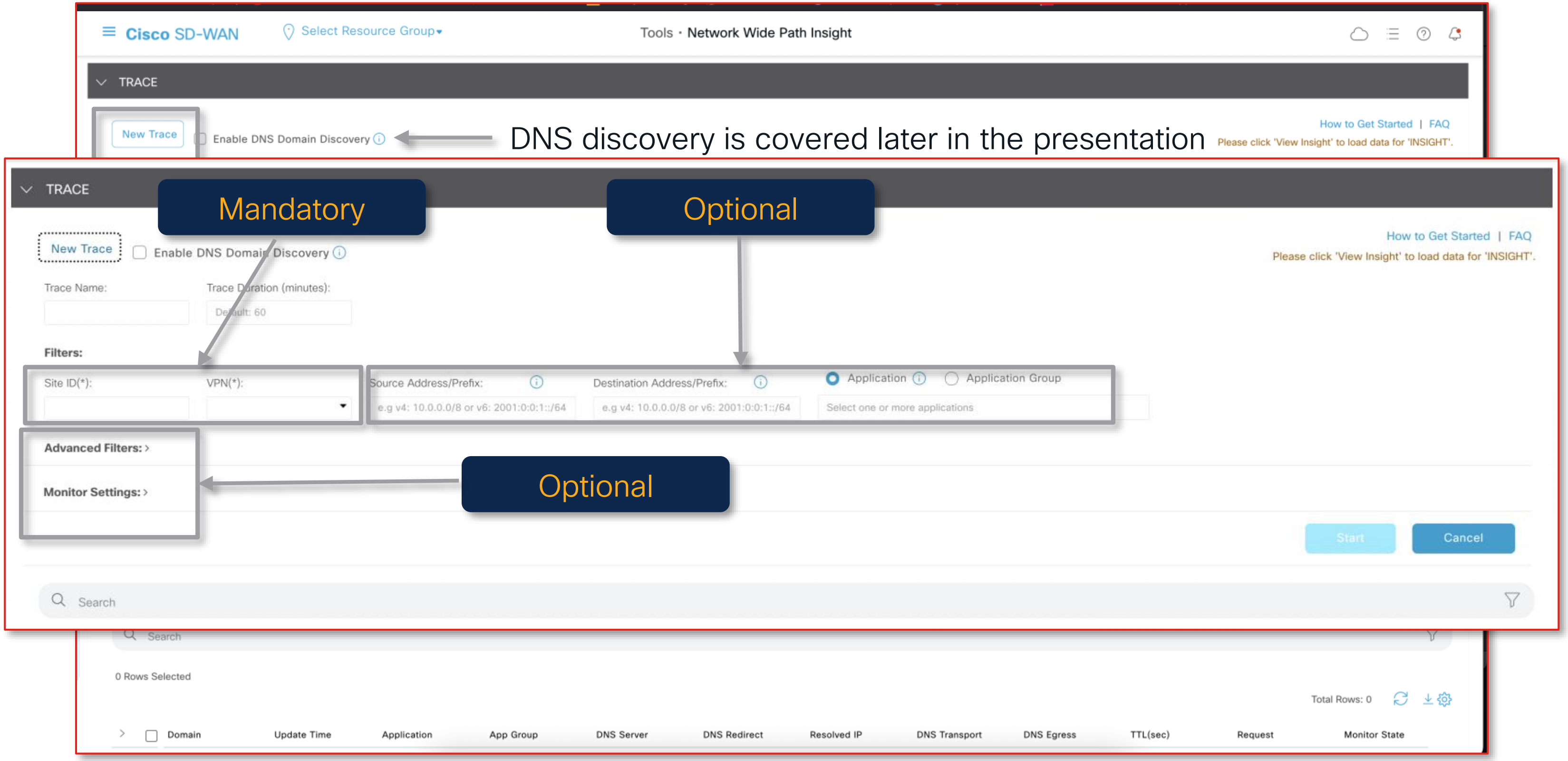
Search

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

Create new trace



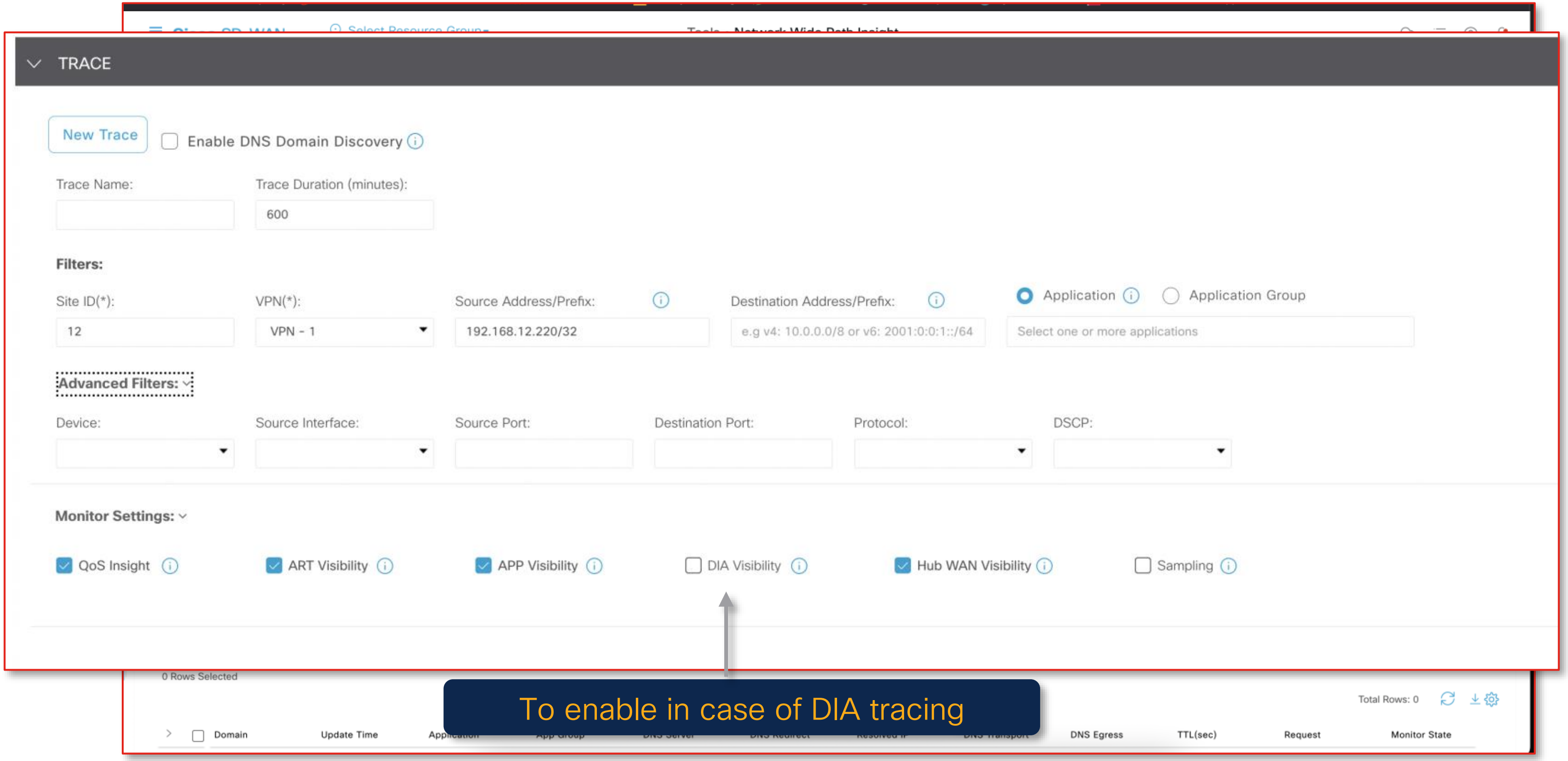
DNS discovery is covered later in the presentation

Mandatory

Optional

Optional

Create new trace (Optional filters)



TRACE

New Trace □ Enable DNS Domain Discovery

Trace Name:

Trace Duration (minutes): 600

Filters:

Site ID(*): 12

VPN(*): VPN - 1

Source Address/Prefix: 192.168.12.220/32

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:

Device:

Source Interface:

Source Port:

Destination Port:

Protocol:

DSCP:

Monitor Settings:

☑ QoS Insight ☑ ART Visibility ☑ APP Visibility □ DIA Visibility ☑ Hub WAN Visibility □ Sampling

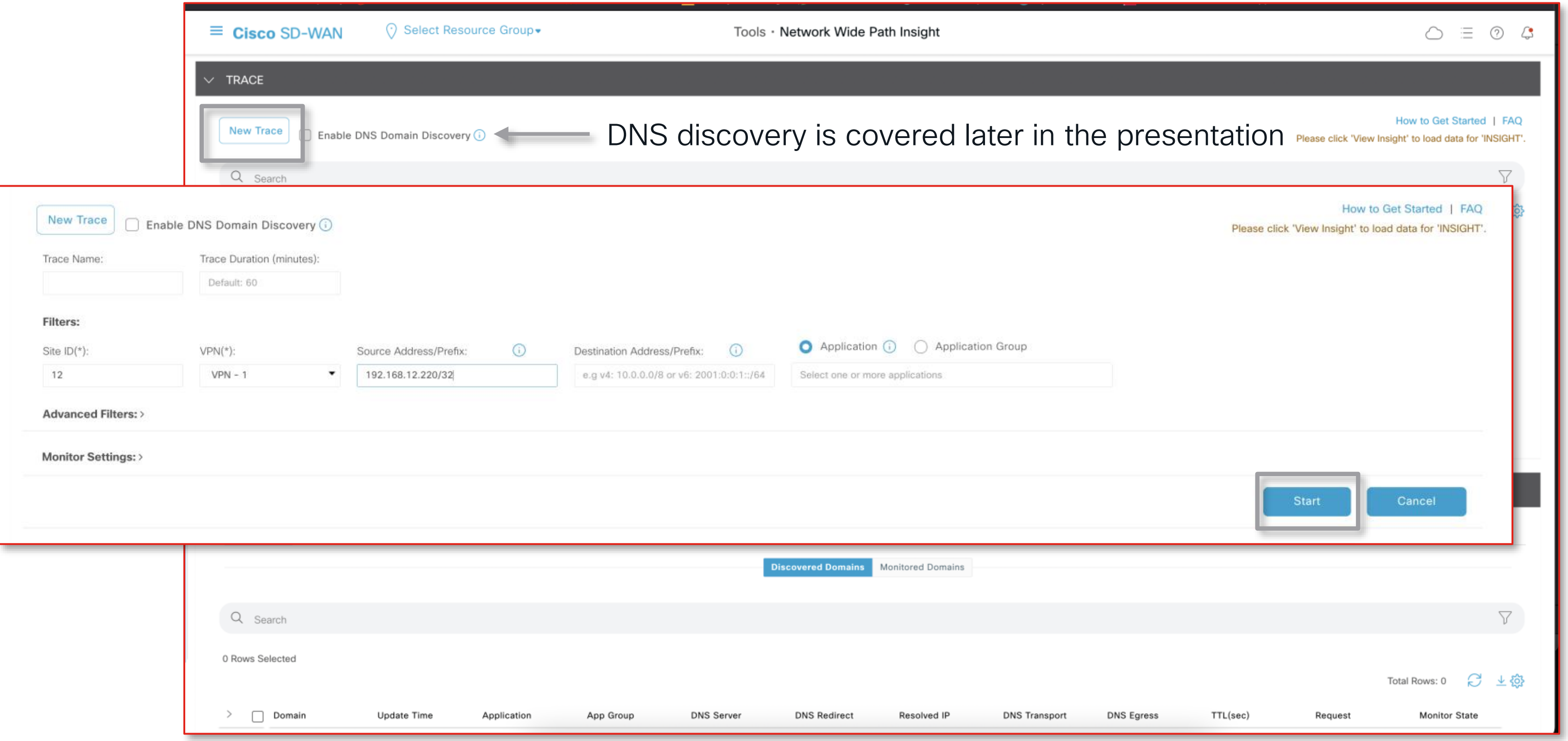
0 Rows Selected

Total Rows: 0

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

To enable in case of DIA tracing

Activate tracing



☐ Enable DNS Domain Discovery

DNS discovery is covered later in the presentation

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

New Trace ☐ Enable DNS Domain Discovery

Trace Name:

Trace Duration (minutes): Default: 60

Filters:

Site ID(*): 12

VPN(*): VPN - 1

Source Address/Prefix: 192.168.12.220/32

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: >

Start Cancel

Discovered Domains | Monitored Domains

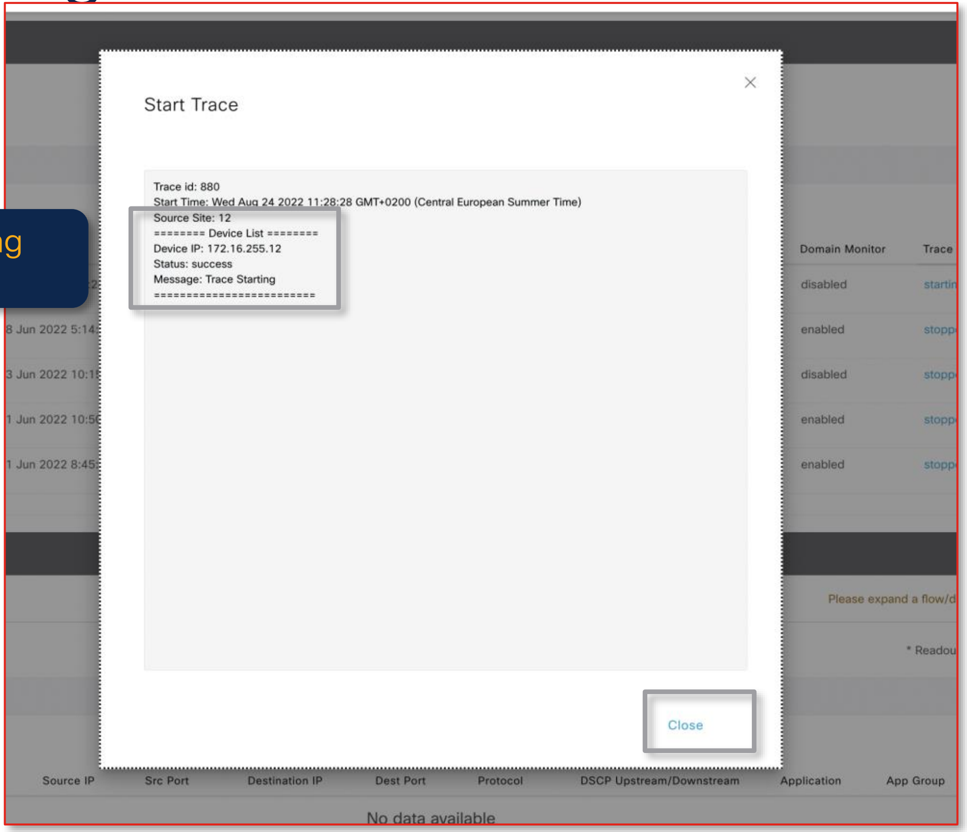
0 Rows Selected

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

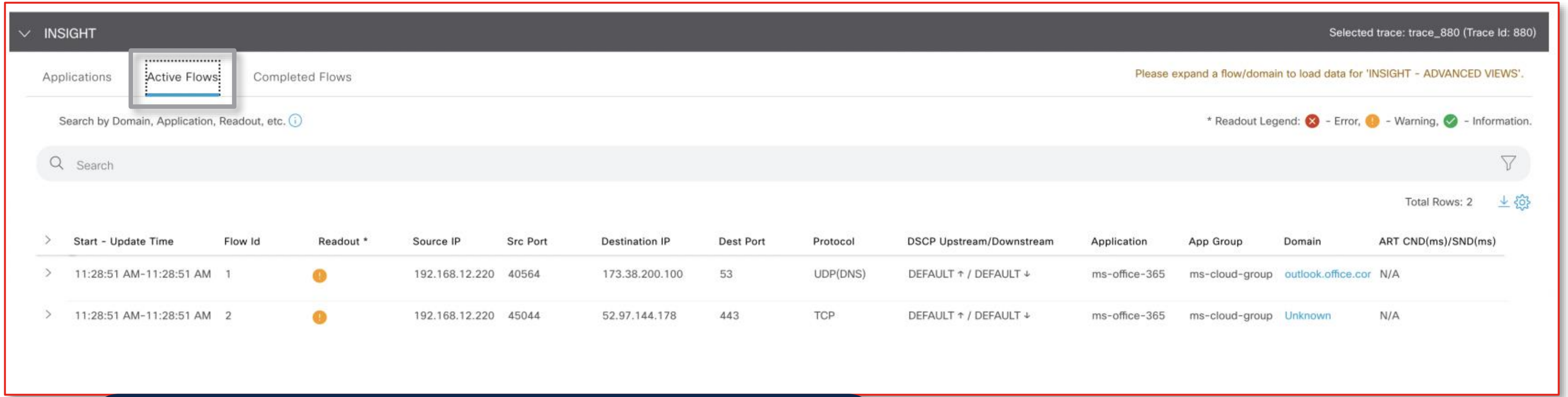


Start Trace

```
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
==========================
```

First look at the tracing results

Active flows



INSIGHT

Selected trace: trace_880 (Trace Id: 880)

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

Search by Domain, Application, Readout, etc.

* Readout Legend: ⊗ - Error, ● - Warning, ✓ - Information.

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

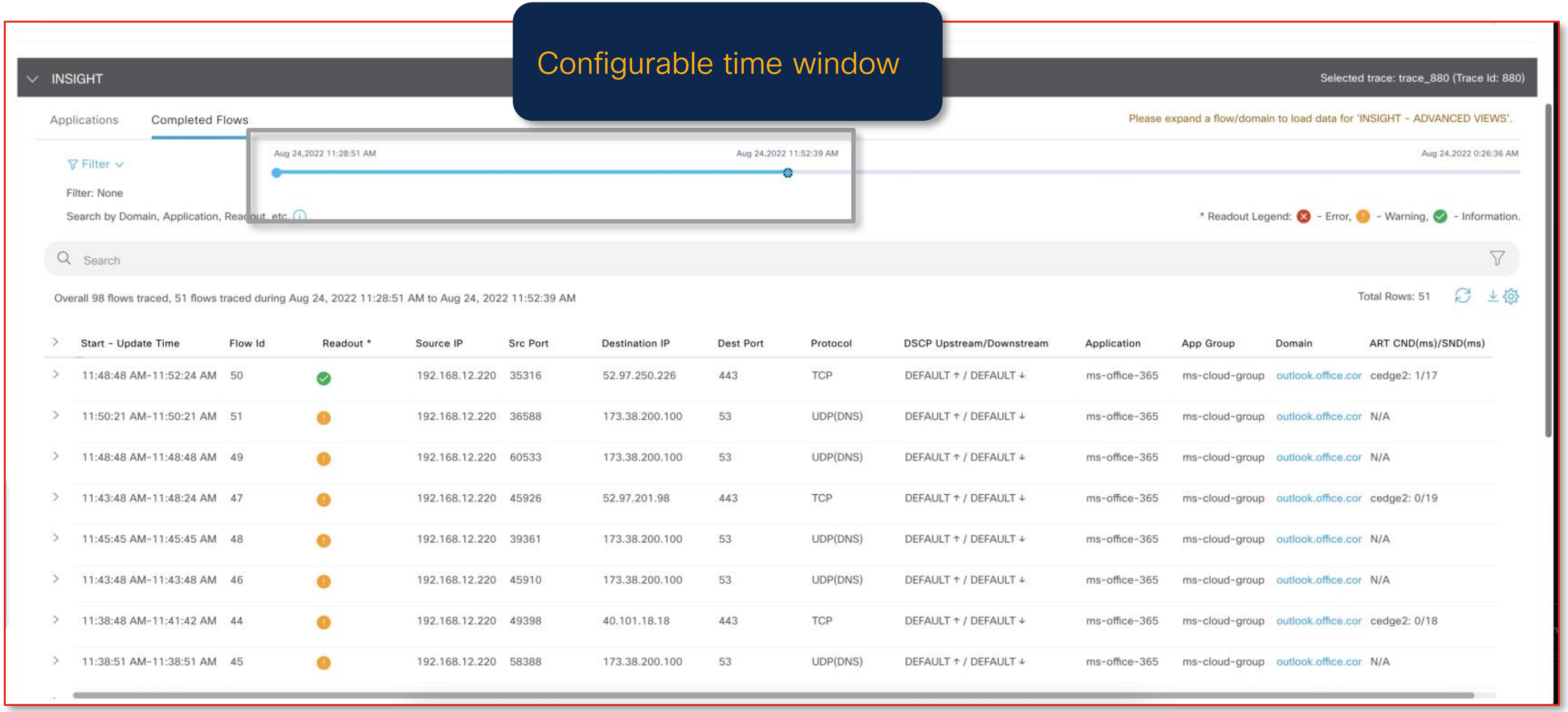
Flow readout

Green: Undamaged symetric flow

Yelow: Deviation from green (eg flow asymmetry / color mismatch / …)

Red: Damaged flow

Completed flows



Configurable time window

INSIGHT

Selected trace: trace_880 (Trace Id: 880)

Applications | Completed Flows

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

Aug 24,2022 11:28:51 AM — Aug 24,2022 11:52:39 AM — Aug 24,2022 0:26:36 AM

Filter

Filter: None

Search by Domain, Application, Readout, etc.

* Readout Legend: ✕ - Error, ! - Warning, ✓ - Information.

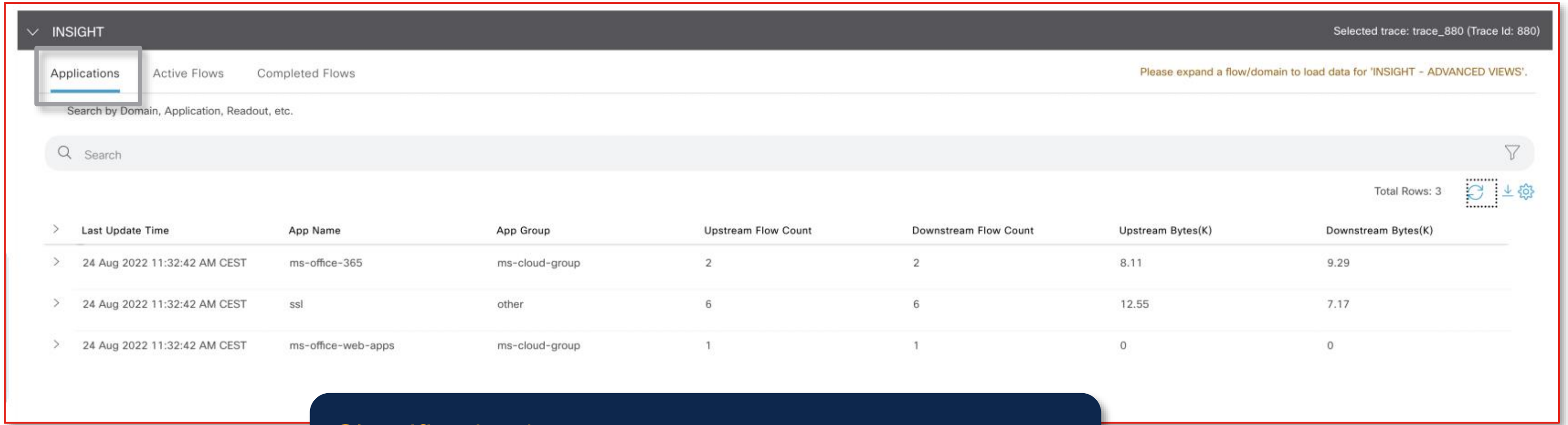
Search

Overall 98 flows traced, 51 flows traced during Aug 24, 2022 11:28:51 AM to Aug 24, 2022 11:52:39 AM

Total Rows: 51

>	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)
>	11:48:48 AM-11:52:24 AM	50	✓	192.168.12.220	35316	52.97.250.226	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	cedge2: 1/17
>	11:50:21 AM-11:50:21 AM	51	!	192.168.12.220	36588	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	N/A
>	11:48:48 AM-11:48:48 AM	49	!	192.168.12.220	60533	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	N/A
>	11:43:48 AM-11:48:24 AM	47	!	192.168.12.220	45926	52.97.201.98	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	cedge2: 0/19
>	11:45:45 AM-11:45:45 AM	48	!	192.168.12.220	39361	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	N/A
>	11:43:48 AM-11:43:48 AM	46	!	192.168.12.220	45910	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	N/A
>	11:38:48 AM-11:41:42 AM	44	!	192.168.12.220	49398	40.101.18.18	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	cedge2: 0/18
>	11:38:51 AM-11:38:51 AM	45	!	192.168.12.220	58388	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	outlook.office.cor	N/A

Applications



Selected trace: trace_880 (Trace Id: 880)

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

Search by Domain, Application, Readout, etc.

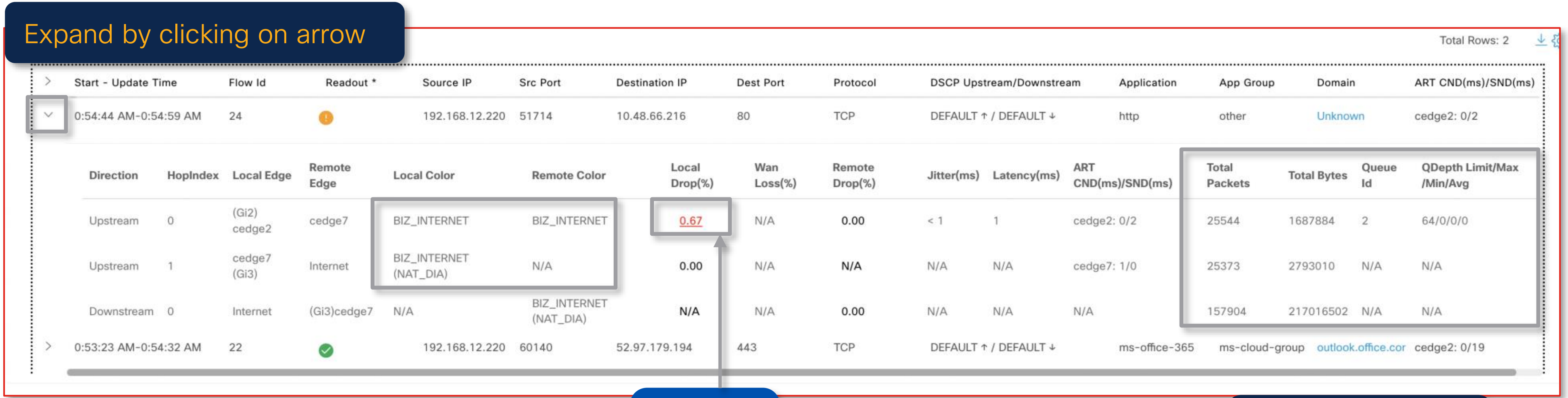
Total Rows: 3

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 bandwith

Deeper in NWPI tracing: Flow analysis

Flow analysis



Expand by clicking on arrow

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)
⌄	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
>	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

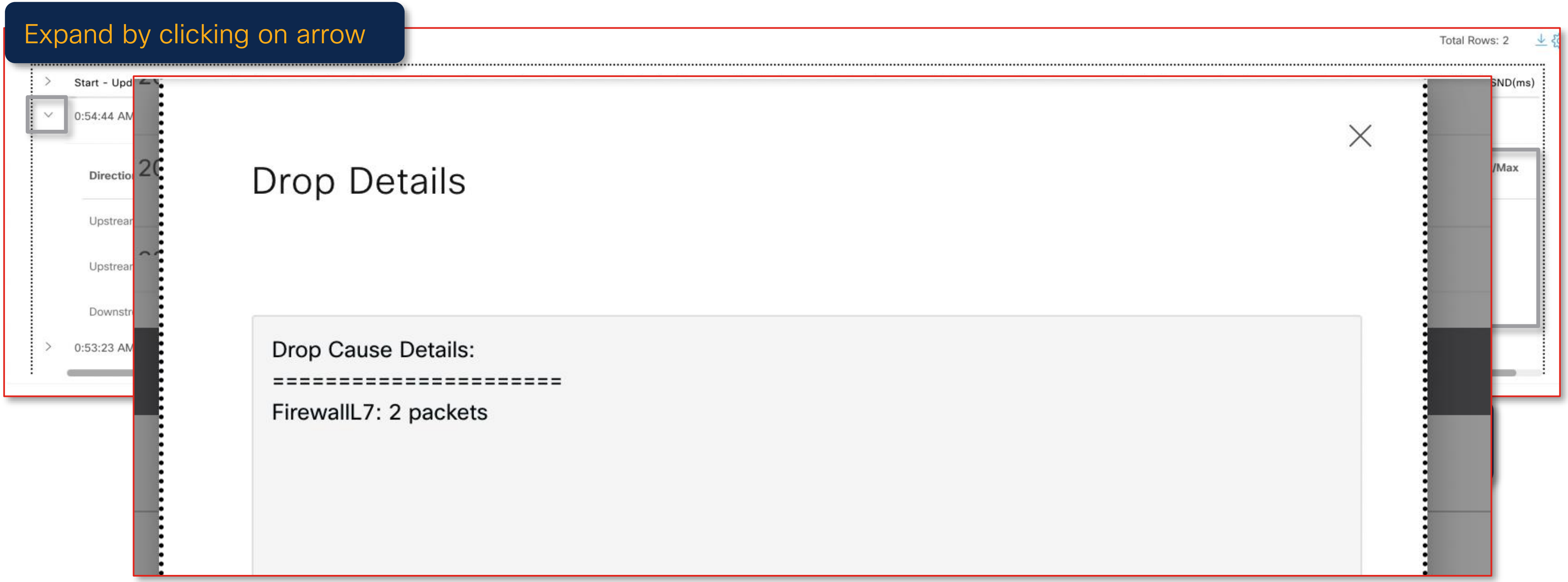
Direction	HopIndex	Local Edge	Remote Edge	Local Color	Remote Color	Local Drop(%)	Wan Loss(%)	Remote Drop(%)	Jitter(ms)	Latency(ms)	ART CND(ms)/SND(ms)	Total Packets	Total Bytes	Queue Id	QDepth Limit/Max /Min/Avg
Upstream	0	(Gi2) cedge2	cedge7	BIZ_INTERNET	BIZ_INTERNET	0.67	N/A	0.00	< 1	1	cedge2: 0/2	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

DROPS!

Traffic volume
QOS information

Flow analysis

Expand by clicking on arrow

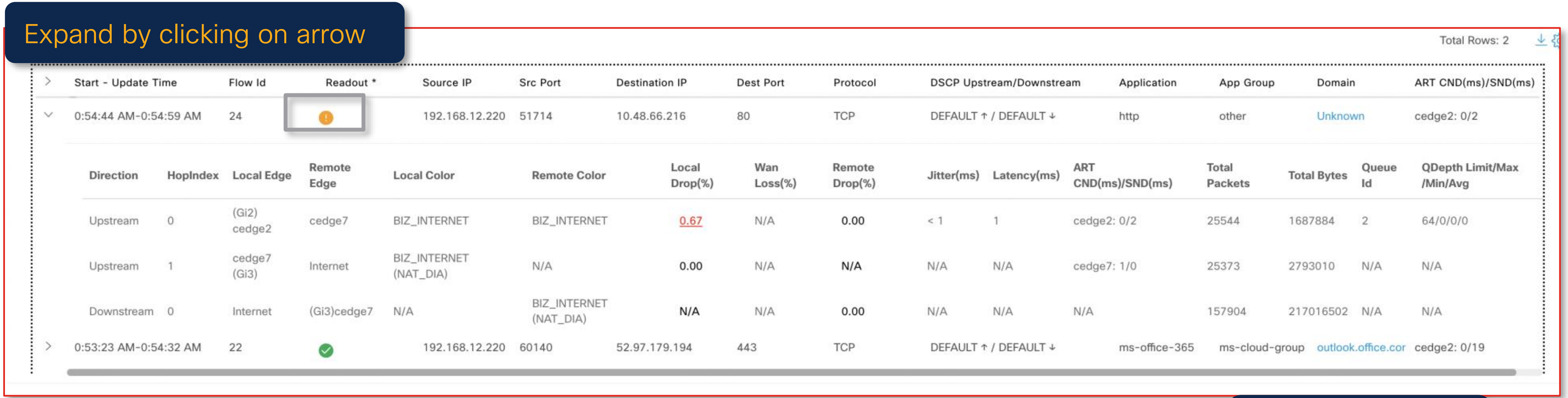


Drop Details

Drop Cause Details:

```
=======================
FirewallL7: 2 packets
```

Flow analysis - readout



Expand by clicking on arrow

Total Rows: 2

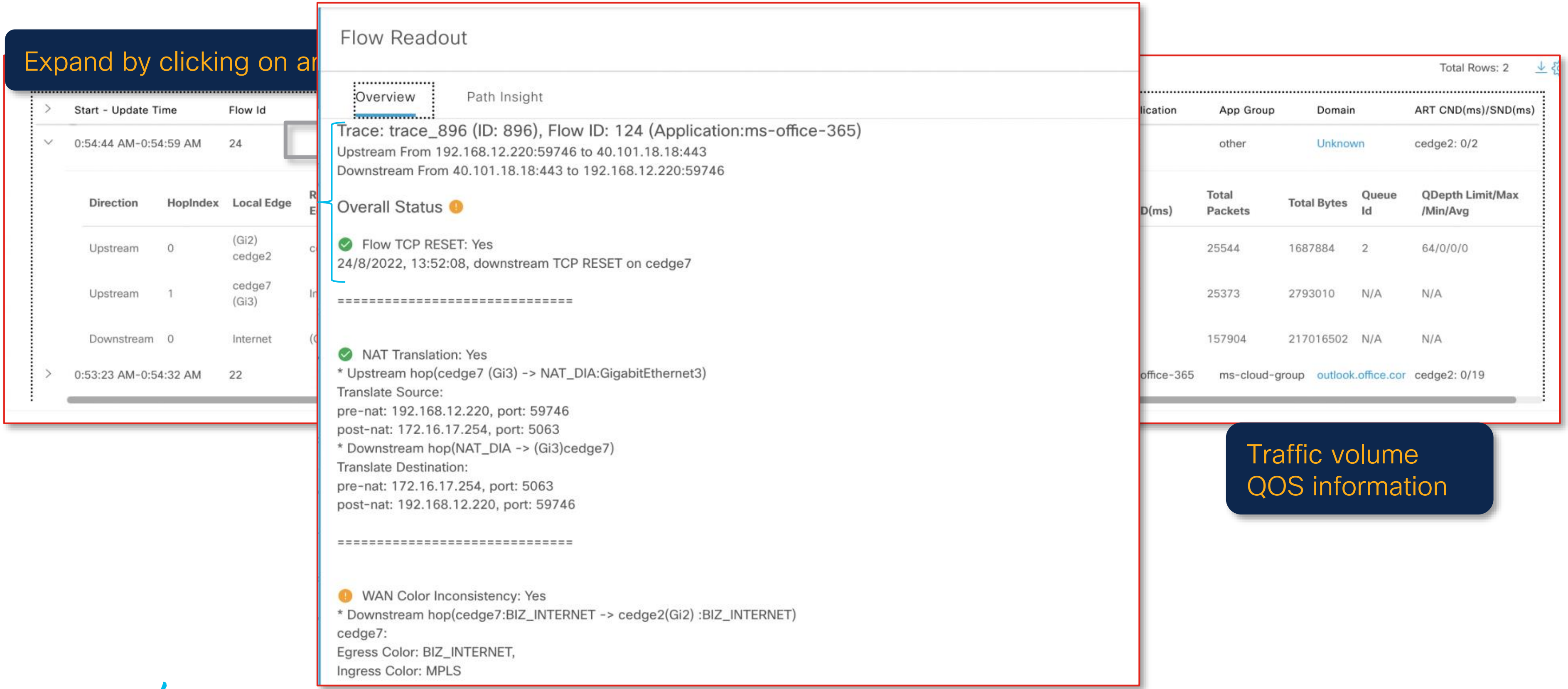
	Start - Update Time	Flow Id	Readout *	Source IP	Src Port	Destination IP	Dest Port	Protocol	DSCP Upstream/Downstream	Application	App Group	Domain	ART CND(ms)/SND(ms)
⌄	0:54:44 AM-0:54:59 AM	24	!	192.168.12.220	51714	10.48.66.216	80	TCP	DEFAULT ↑ / DEFAULT ↓	http	other	Unknown	cedge2: 0/2
>	0:53:23 AM-0:54:32 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

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

Traffic volume
QOS information

Flow analysis - readout

Expand by clicking on ar



Total Rows: 2

	Start - Update Time	Flow Id	lication	App Group	Domain	ART CND(ms)/SND(ms)
⌄	0:54:44 AM-0:54:59 AM	24		other	Unknown	cedge2: 0/2
>	0:53:23 AM-0:54:32 AM	22	office-365	ms-cloud-group	outlook.office.cor	cedge2: 0/19

Direction	HopIndex	Local Edge	R E	D(ms)	Total Packets	Total Bytes	Queue Id	QDepth Limit/Max /Min/Avg
Upstream	0	(Gi2) cedge2	c		25544	1687884	2	64/0/0/0
Upstream	1	cedge7 (Gi3)	Ir		25373	2793010	N/A	N/A
Downstream	0	Internet	((		157904	217016502	N/A	N/A

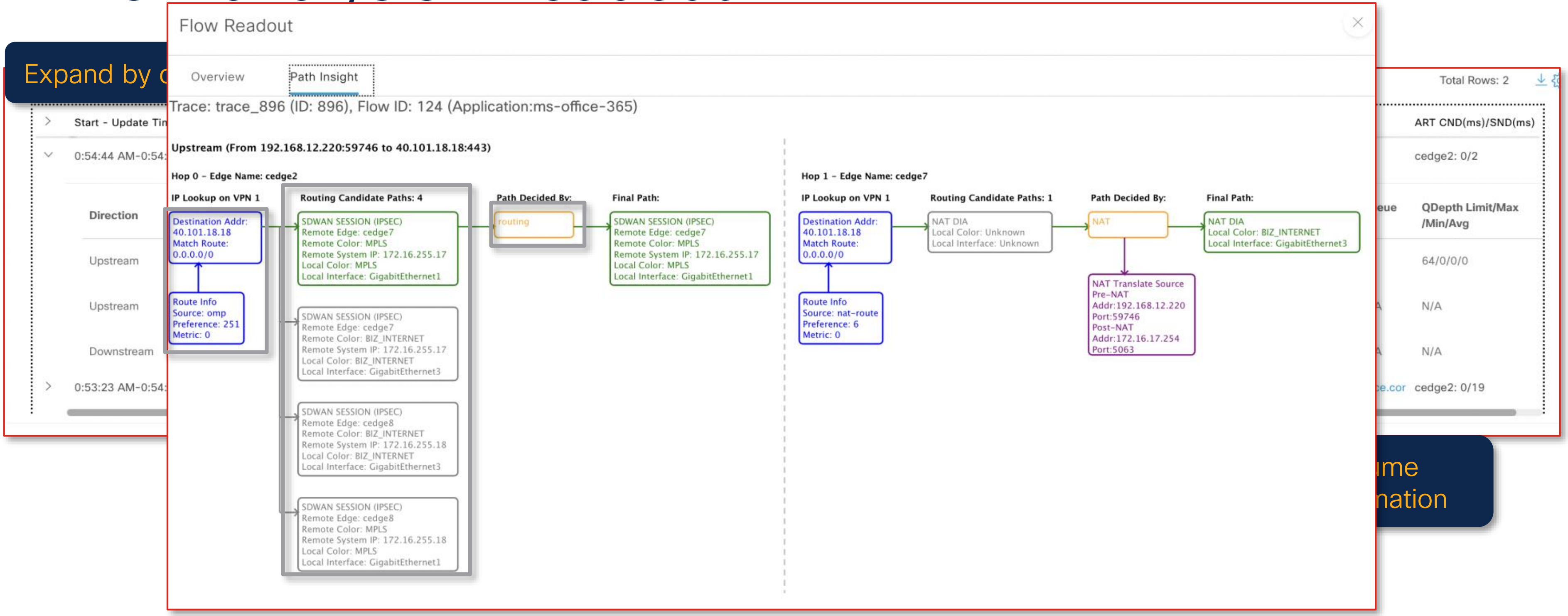
Flow Readout

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(cedge7 (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)cedge7)
Translate Destination:
pre-nat: 172.16.17.254, port: 5063
post-nat: 192.168.12.220, port: 59746

==============================

! WAN Color Inconsistency: Yes
* Downstream hop(cedge7:BIZ_INTERNET -> cedge2(Gi2) :BIZ_INTERNET)
cedge7:
Egress Color: BIZ_INTERNET,
Ingress Color: MPLS
```

Traffic volume
QOS information

Flow analysis - readout



Flow Readout

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)

Hop 0 – Edge Name: cedge2

IP Lookup on VPN 1

Destination Addr: 40.101.18.18
Match Route: 0.0.0.0/0

Route Info
Source: omp
Preference: 251
Metric: 0

Routing Candidate Paths: 4

SDWAN SESSION (IPSEC)
Remote Edge: cedge7
Remote Color: MPLS
Remote System IP: 172.16.255.17
Local Color: MPLS
Local Interface: GigabitEthernet1

SDWAN SESSION (IPSEC)
Remote Edge: cedge7
Remote Color: BIZ_INTERNET
Remote System IP: 172.16.255.17
Local Color: BIZ_INTERNET
Local Interface: GigabitEthernet3

SDWAN SESSION (IPSEC)
Remote Edge: cedge8
Remote Color: BIZ_INTERNET
Remote System IP: 172.16.255.18
Local Color: BIZ_INTERNET
Local Interface: GigabitEthernet3

SDWAN SESSION (IPSEC)
Remote Edge: cedge8
Remote Color: MPLS
Remote System IP: 172.16.255.18
Local Color: MPLS
Local Interface: GigabitEthernet1

Path Decided By:

routing

Final Path:

SDWAN SESSION (IPSEC)
Remote Edge: cedge7
Remote Color: MPLS
Remote System IP: 172.16.255.17
Local Color: MPLS
Local Interface: GigabitEthernet1

Hop 1 – Edge Name: cedge7

IP Lookup on VPN 1

Destination Addr: 40.101.18.18
Match Route: 0.0.0.0/0

Route Info
Source: nat-route
Preference: 6
Metric: 0

Routing Candidate Paths: 1

NAT DIA
Local Color: Unknown
Local Interface: Unknown

Path Decided By:

NAT

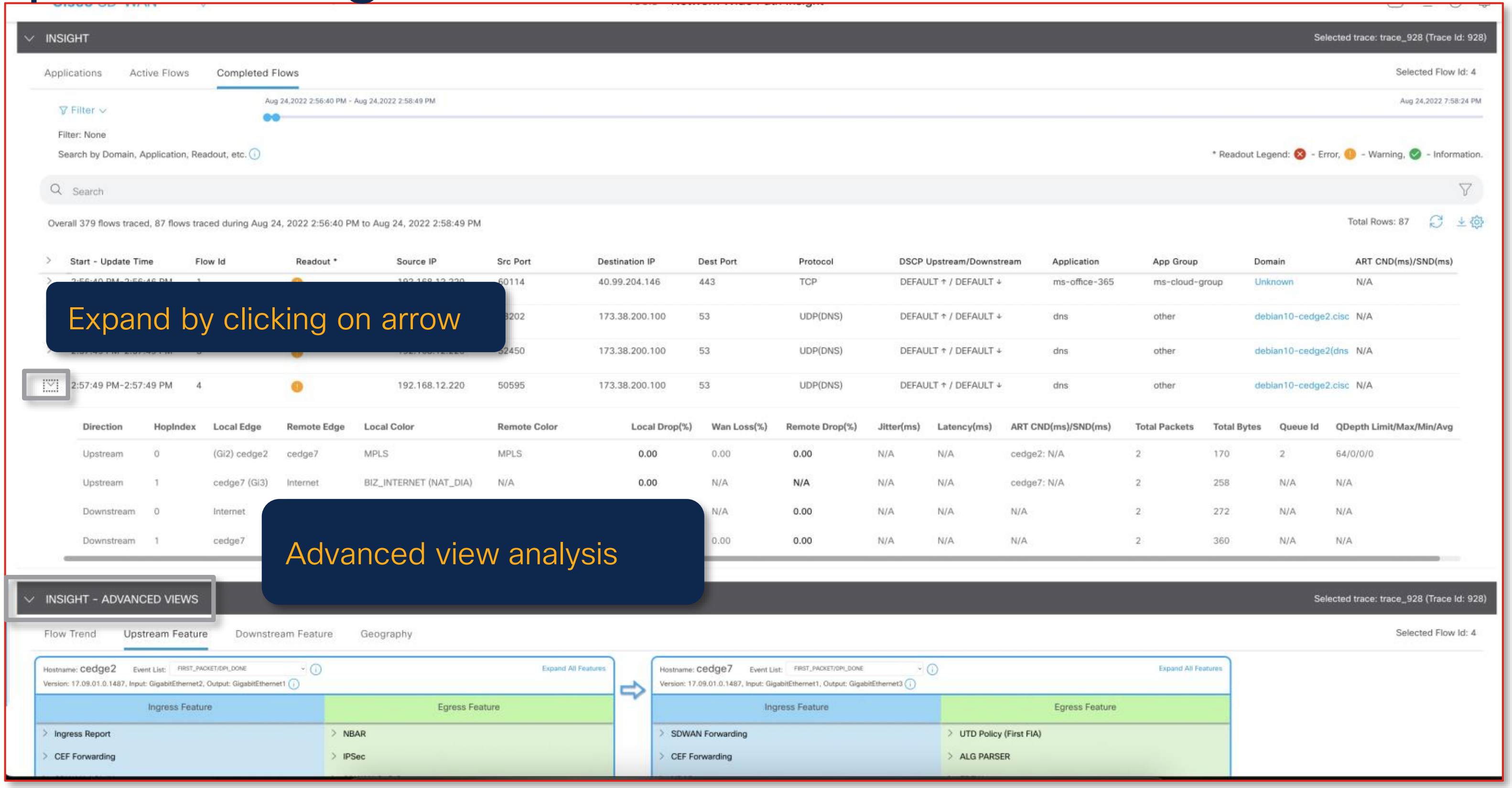
NAT Translate Source
Pre-NAT
Addr:192.168.12.220
Port:59746
Post-NAT
Addr:172.16.17.254
Port:5063

Final Path:

NAT DIA
Local Color: BIZ_INTERNET
Local Interface: GigabitEthernet3

cisco Live!

Flow analysis – Going deeper in router processing



Selected trace: trace_928 (Trace Id: 928)

Selected Flow Id: 4

Aug 24,2022 2:56:40 PM - Aug 24,2022 2:58:49 PM

Aug 24,2022 7:58:24 PM

Filter: None

Search by Domain, Application, Readout, etc.

* Readout Legend: ✗ - Error, ● - Warning, ✓ - Information.

Overall 379 flows traced, 87 flows traced during Aug 24, 2022 2:56:40 PM to Aug 24, 2022 2:58:49 PM

Total Rows: 87

>	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)
>	2:56:40 PM-2:56:46 PM	1	●	192.168.12.220	60114	40.99.204.146	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-365	ms-cloud-group	Unknown	N/A
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]3202	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	dns	other	debian10-cedge2.cisc	N/A
>	2:57:49 PM-2:57:49 PM	3	●	192.168.12.220	[illegible]2450	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	dns	other	debian10-cedge2(dns	N/A
⌄	2:57:49 PM-2:57:49 PM	4	●	192.168.12.220	50595	173.38.200.100	53	UDP(DNS)	DEFAULT ↑ / DEFAULT ↓	dns	other	debian10-cedge2.cisc	N/A

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	MPLS	MPLS	0.00	0.00	0.00	N/A	N/A	cedge2: N/A	2	170	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: N/A	2	258	N/A	N/A
Downstream	0	Internet	[illegible]	[illegible]	[illegible]	[illegible]	N/A	0.00	N/A	N/A	N/A	2	272	N/A	N/A
Downstream	1	cedge7	[illegible]	[illegible]	[illegible]	[illegible]	0.00	0.00	N/A	N/A	N/A	2	360	N/A	N/A

Selected trace: trace_928 (Trace Id: 928)

Selected Flow Id: 4

Hostname: cedge2 Event List: FIRST_PACKET/DPI_DONE
Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet1

Ingress Feature	Egress Feature
> Ingress Report	> NBAR
> CEF Forwarding	> IPSec

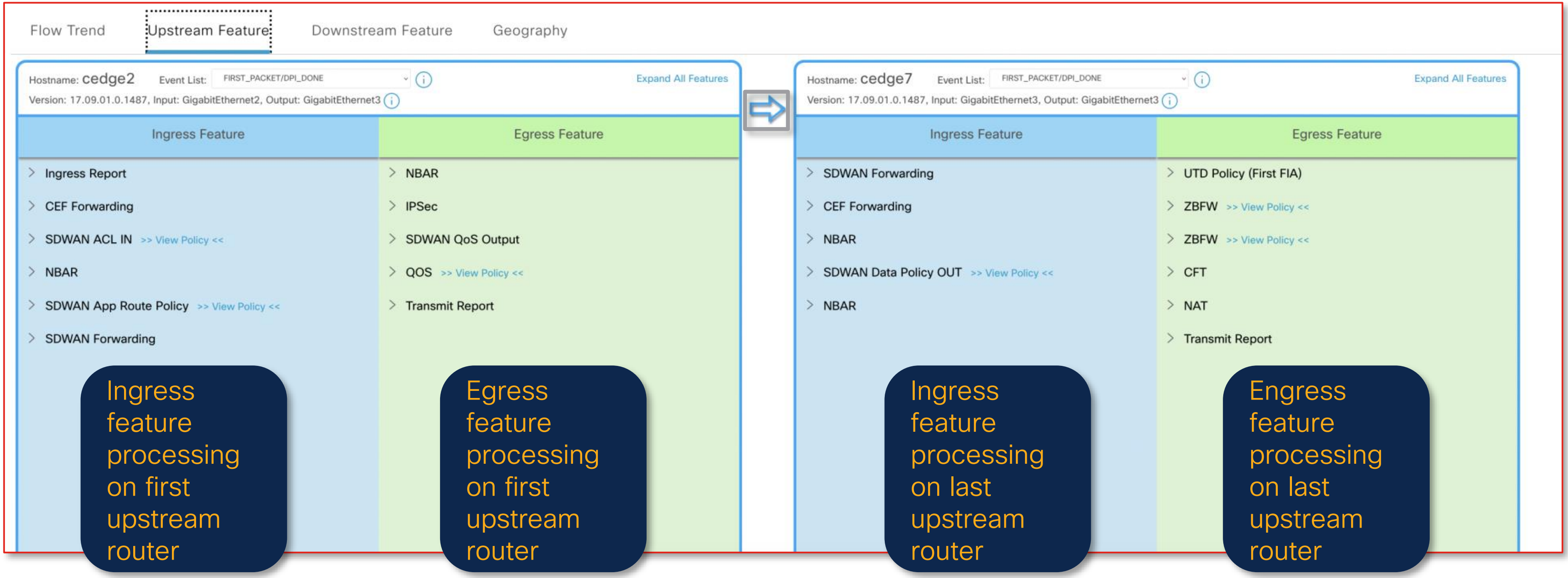
Hostname: cedge7 Event List: FIRST_PACKET/DPI_DONE
Version: 17.09.01.0.1487, Input: GigabitEthernet1, Output: GigabitEthernet3

Ingress Feature	Egress Feature
> SDWAN Forwarding	> UTD Policy (First FIA)
> CEF Forwarding	> ALG PARSER

Expand by clicking on arrow

Advanced view analysis

Flow analysis – Upstream router(s) processing



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

Ingress Feature	Egress Feature
Ingress Report	NBAR
CEF Forwarding	IPSec
SDWAN ACL IN >> View Policy <<	SDWAN QoS Output
NBAR	QOS >> View Policy <<
SDWAN App Route Policy >> View Policy <<	Transmit Report
SDWAN Forwarding	

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

Ingress Feature	Egress Feature
SDWAN Forwarding	UTD Policy (First FIA)
CEF Forwarding	ZBFW >> View Policy <<
NBAR	ZBFW >> View Policy <<
SDWAN Data Policy OUT >> View Policy <<	CFT
NBAR	NAT
	Transmit Report

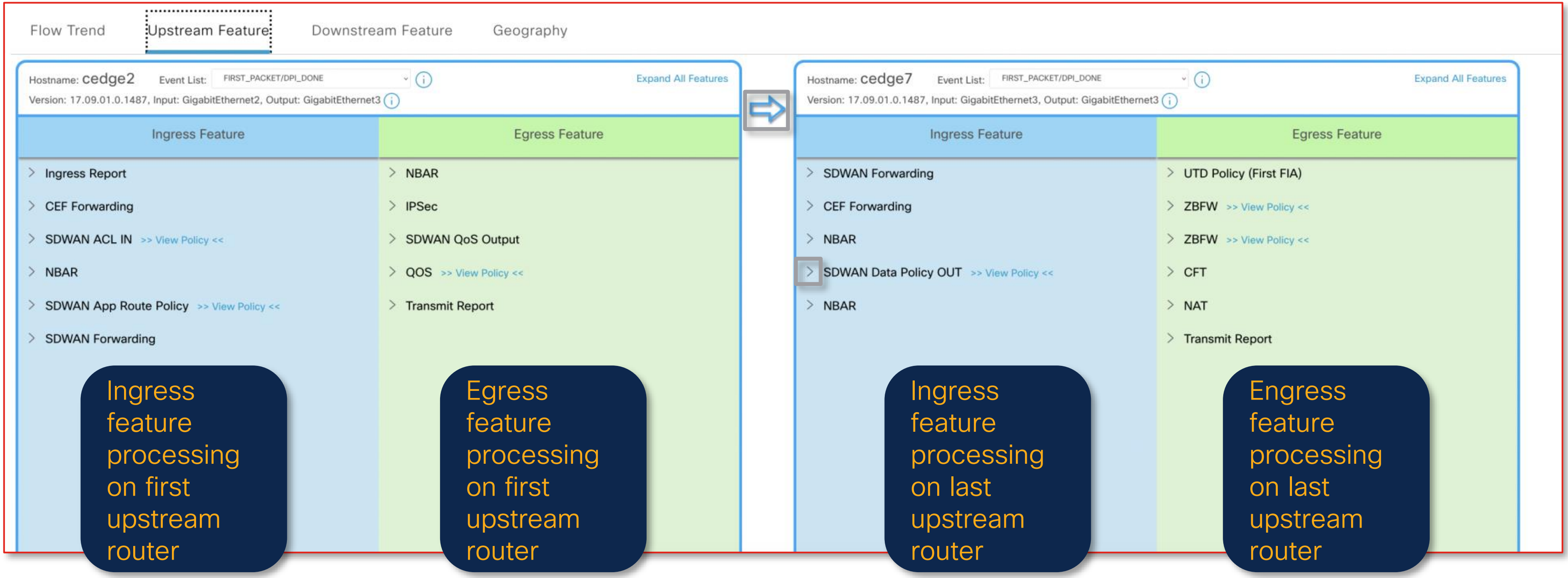
Ingress feature processing on first upstream router

Egress feature processing on first upstream router

Ingress feature processing on last upstream router

Engress feature processing on last upstream router

Flow analysis – Upstream router(s) processing



Flow Trend | Upstream Feature | Downstream Feature | Geography

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

Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3

Ingress Feature	Egress Feature
Ingress Report	NBAR
CEF Forwarding	IPSec
SDWAN ACL IN >> View Policy <<	SDWAN QoS Output
NBAR	QOS >> View Policy <<
SDWAN App Route Policy >> View Policy <<	Transmit Report
SDWAN Forwarding	

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

Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet3

Ingress Feature	Egress Feature
SDWAN Forwarding	UTD Policy (First FIA)
CEF Forwarding	ZBFW >> View Policy <<
NBAR	ZBFW >> View Policy <<
SDWAN Data Policy OUT >> View Policy <<	CFT
NBAR	NAT
	Transmit Report

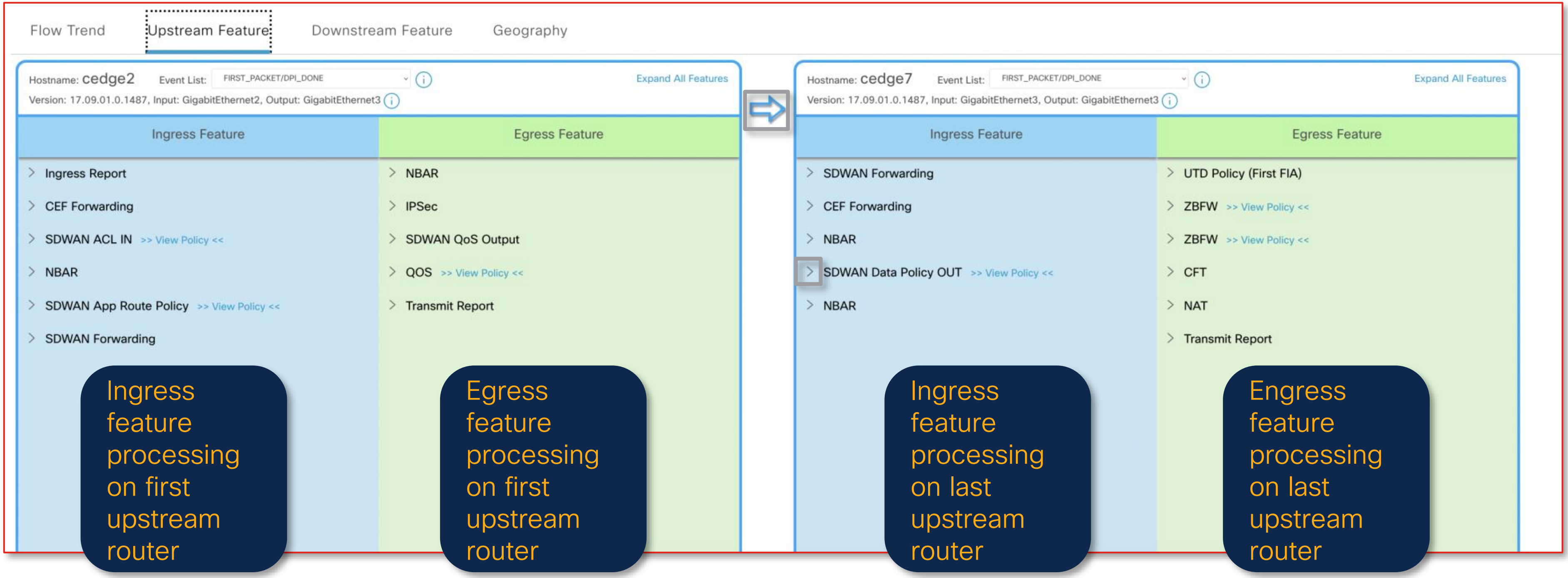
Ingress feature processing on first upstream router

Egress feature processing on first upstream router

Ingress feature processing on last upstream router

Engress 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/DPI_DONE ⓘ Expand All Features
Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3 ⓘ

Ingress Feature	Egress Feature
> Ingress Report	> NBAR
> CEF Forwarding	> IPSec
> SDWAN ACL IN >> View Policy <<	> SDWAN QoS Output
> NBAR	> QOS >> View Policy <<
> SDWAN App Route Policy >> View Policy <<	> Transmit Report
> SDWAN Forwarding	

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

Ingress Feature	Egress Feature
> SDWAN Forwarding	> UTD Policy (First FIA)
> CEF Forwarding	> ZBFW >> View Policy <<
> NBAR	> ZBFW >> View Policy <<
> SDWAN Data Policy OUT >> View Policy <<	> CFT
> NBAR	> NAT
	> Transmit Report

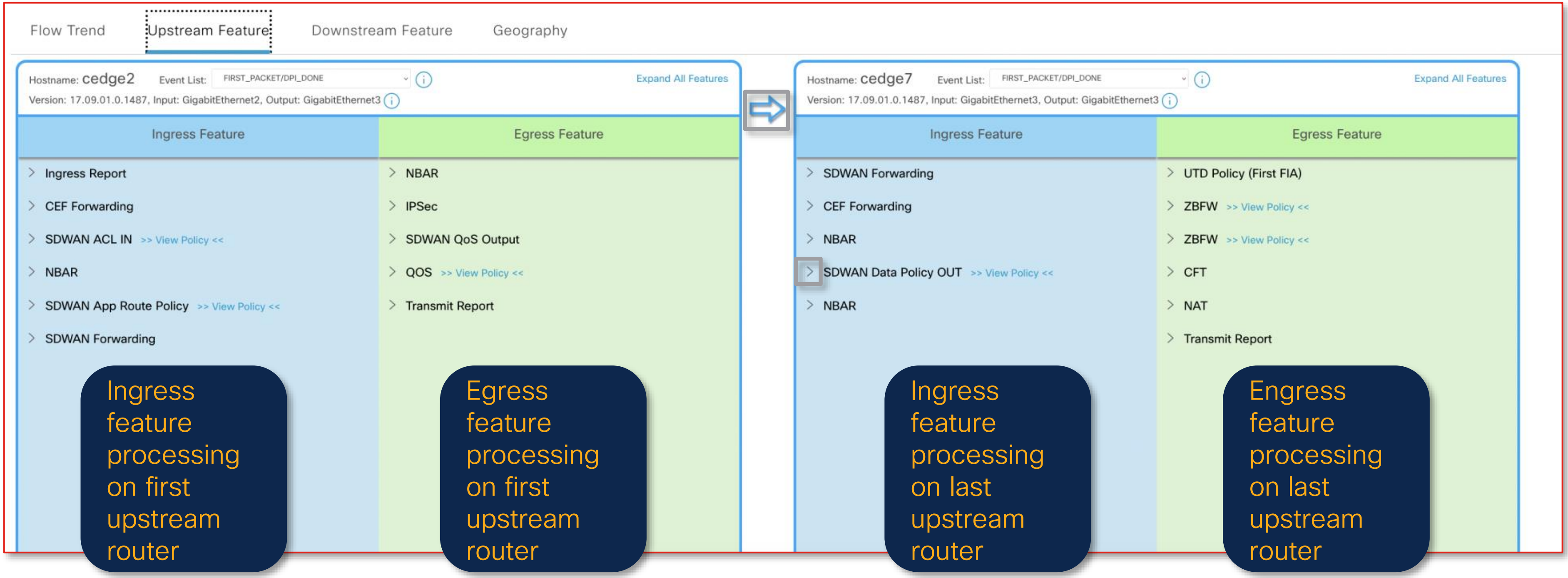
Ingress feature processing on first upstream router

Egress feature processing on first upstream router

Ingress feature processing on last upstream router

Engress 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/DPI_DONE Expand All Features
Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3

Ingress Feature	Egress Feature
Ingress Report	NBAR
CEF Forwarding	IPSec
SDWAN ACL IN >> View Policy <<	SDWAN QoS Output
NBAR	QOS >> View Policy <<
SDWAN App Route Policy >> View Policy <<	Transmit Report
SDWAN Forwarding	

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

Ingress Feature	Egress Feature
SDWAN Forwarding	UTD Policy (First FIA)
CEF Forwarding	ZBFW >> View Policy <<
NBAR	ZBFW >> View Policy <<
SDWAN Data Policy OUT >> View Policy <<	CFT
NBAR	NAT
	Transmit Report

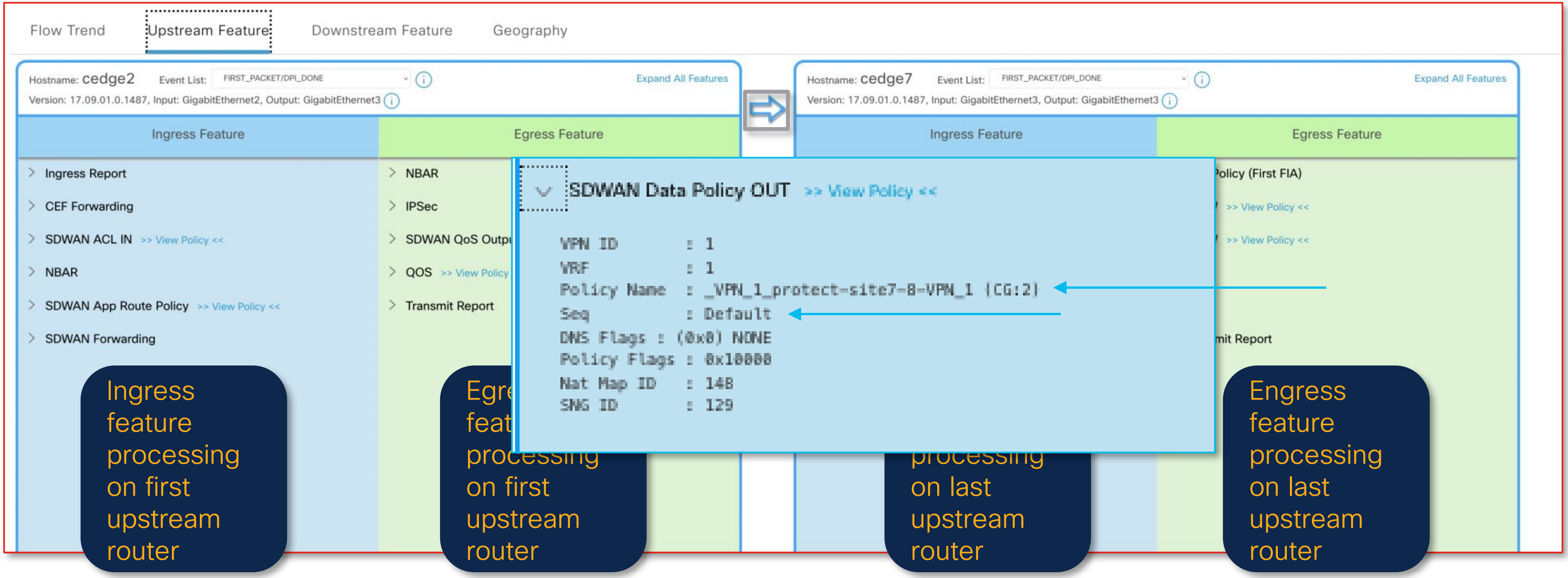
Ingress feature processing on first upstream router

Egress feature processing on first upstream router

Ingress feature processing on last upstream router

Engress feature processing on last upstream router

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



Hostname: cedge2 Event List: FIRST_PACKET/DPI_DONE

Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3

Hostname: cedge7 Event List: FIRST_PACKET/DPI_DONE

Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet3

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 : (0x0) NONE
Policy Flags  : 0x10000
Nat Map ID    : 148
SNG ID        : 129
```

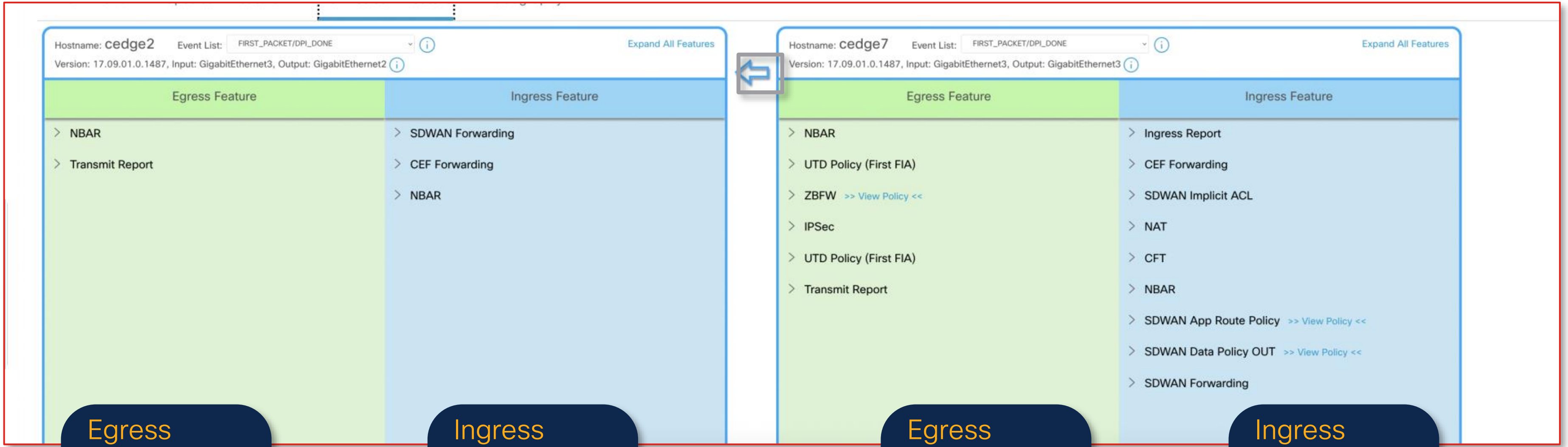
Ingress feature processing on first upstream router

Egre feat processing on first upstream router

processing on last upstream router

Engress feature processing on last upstream router

Flow analysis – Downstream router(s) processing



Hostname: cedge2 Event List: FIRST_PACKET/DPI_DONE

Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet2

Egress Feature	Ingress Feature
NBAR	SDWAN Forwarding
Transmit Report	CEF Forwarding
	NBAR

Hostname: cedge7 Event List: FIRST_PACKET/DPI_DONE

Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet3

Egress Feature	Ingress Feature
NBAR	Ingress Report
UTD Policy (First FIA)	CEF Forwarding
ZBFW >> View Policy <<	SDWAN Implicit ACL
IPSec	NAT
UTD Policy (First FIA)	CFT
Transmit Report	NBAR
	SDWAN App Route Policy >> View Policy <<
	SDWAN Data Policy OUT >> View Policy <<
	SDWAN Forwarding

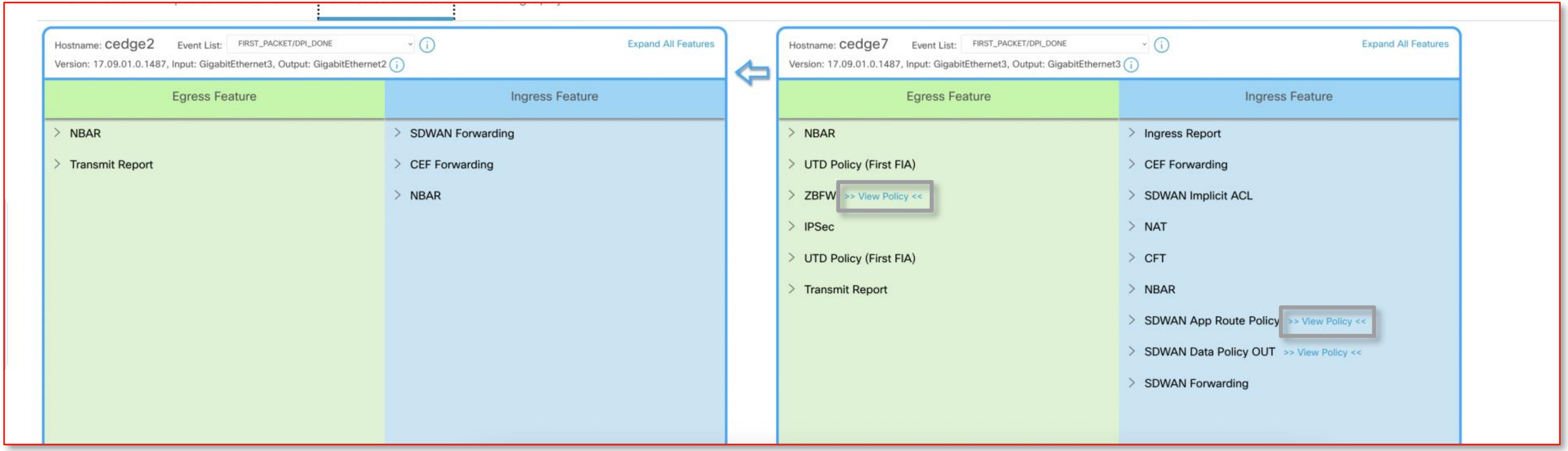
Egress feature processing on last downstream router

Ingress feature processing on last downstream router

Egress feature processing on first downstream router

Ingress feature processing on first downstream router

Flow analysis – Policy analysis



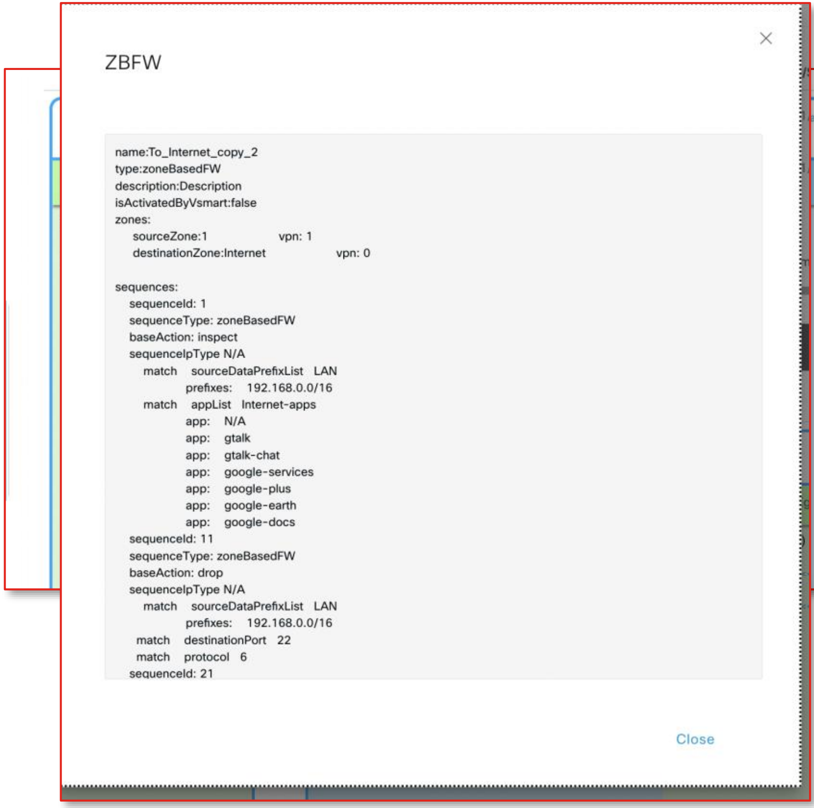
Hostname: cedge2 Event List: FIRST_PACKET/DPI_DONE
Version: 17.09.01.0.1487, Input: GigabitEthernet3, Output: GigabitEthernet2
Expand All Features

Egress Feature	Ingress Feature
NBAR	SDWAN Forwarding
Transmit Report	CEF Forwarding
	NBAR

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

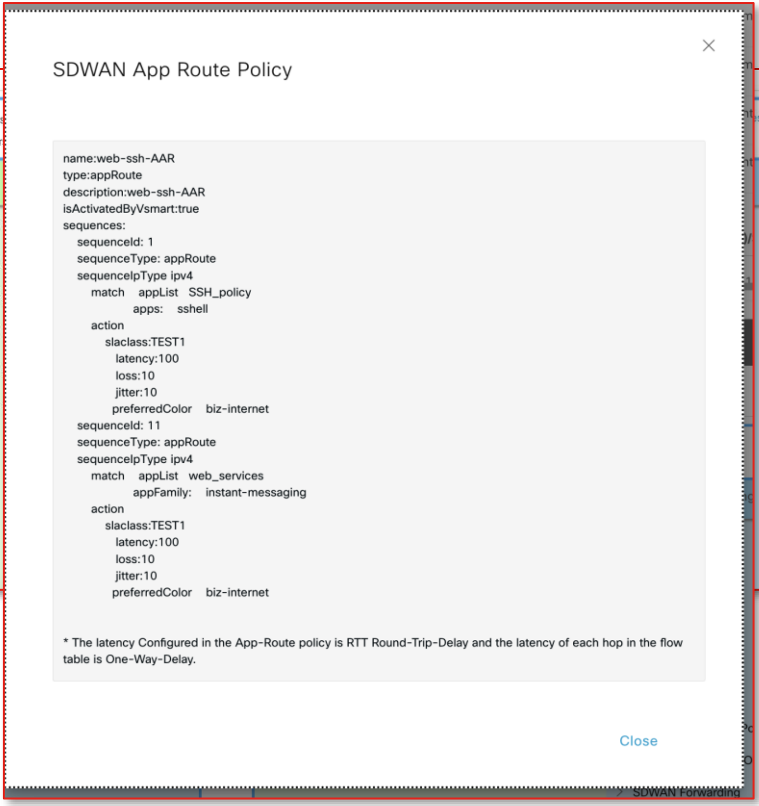
Egress Feature	Ingress Feature
NBAR	Ingress Report
UTD Policy (First FIA)	CEF Forwarding
ZBFW >> View Policy <<	SDWAN Implicit ACL
IPSec	NAT
UTD Policy (First FIA)	CFT
Transmit Report	NBAR
	SDWAN App Route Policy >> View Policy <<
	SDWAN Data Policy OUT >> View Policy <<
	SDWAN Forwarding

Flow analysis – Policy analysis



ZBFW

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

sequences:
   sequenceId: 1
   sequenceType: zoneBasedFW
   baseAction: inspect
   sequenceIpType 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
   sequenceIpType N/A
      match   sourceDataPrefixList   LAN
               prefixes:   192.168.0.0/16
     match   destinationPort   22
     match   protocol   6
   sequenceId: 21
```

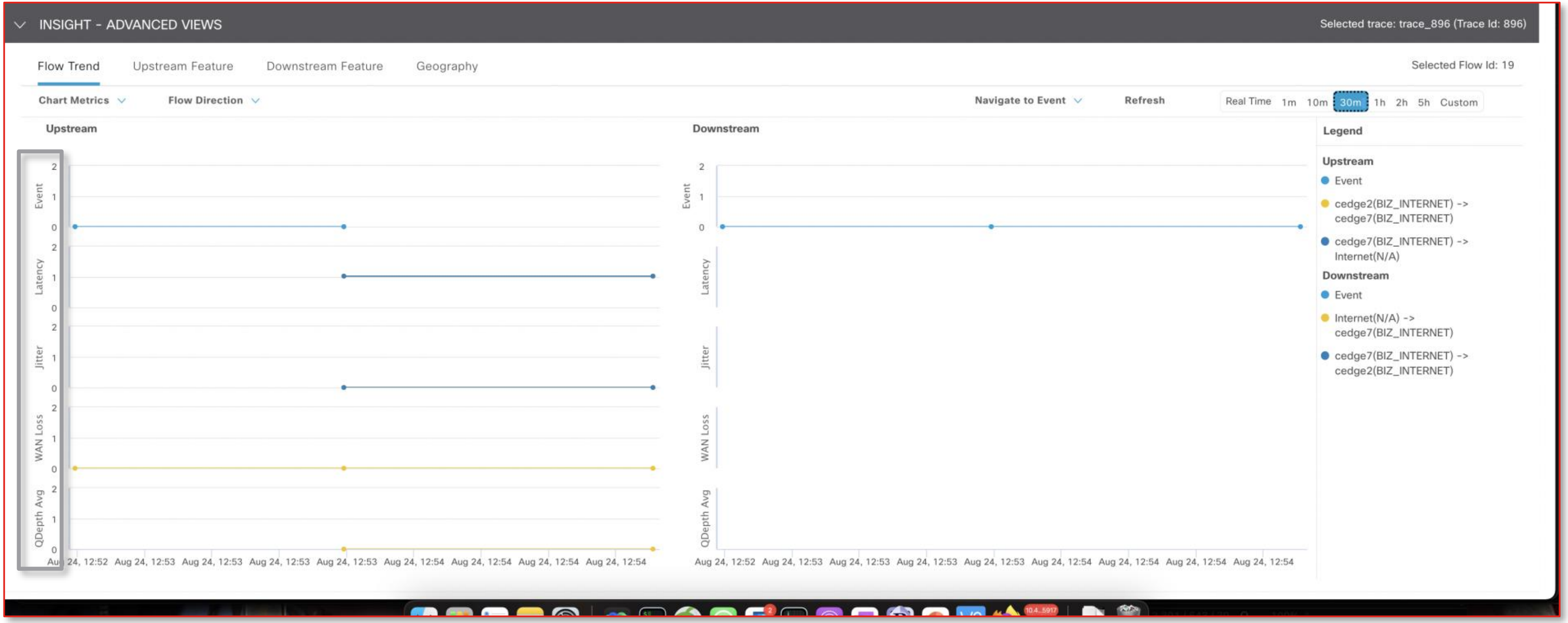


SDWAN App Route Policy

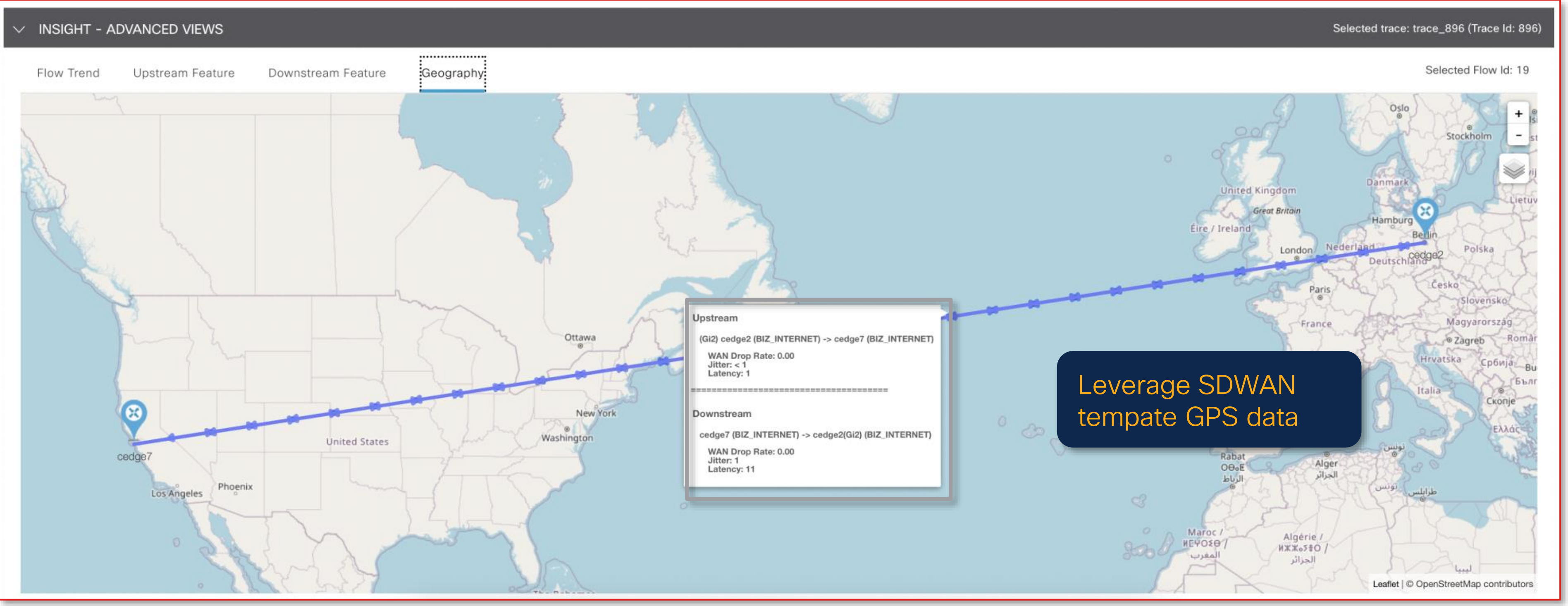
```
name:web-ssh-AAR
type:appRoute
description:web-ssh-AAR
isActivatedByVsmart:true
sequences:
   sequenceId: 1
   sequenceType: appRoute
   sequenceIpType ipv4
      match   appList   SSH_policy
               apps:   sshell
      action
         slaclass:TEST1
            latency:100
            loss:10
            jitter:10
           preferredColor   biz-internet
   sequenceId: 11
   sequenceType: appRoute
   sequenceIpType 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.

Flow analysis – Flow trends



Flow analysis – Geography



INSIGHT - ADVANCED VIEWS

Selected trace: trace_896 (Trace Id: 896)

Flow Trend | Upstream Feature | Downstream Feature | Geography

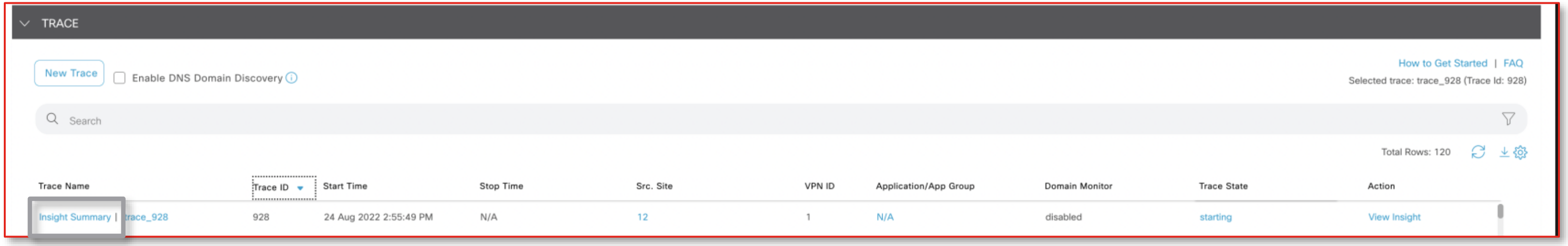
Selected Flow Id: 19

```
Upstream

  (Gi2) cedge2 (BIZ_INTERNET) -> cedge7 (BIZ_INTERNET)

    WAN Drop Rate: 0.00
    Jitter: < 1
    Latency: 1

========================================

Downstream

  cedge7 (BIZ_INTERNET) -> cedge2(Gi2) (BIZ_INTERNET)

    WAN Drop Rate: 0.00
    Jitter: 1
    Latency: 11
```

Leverage SDWAN tempate GPS data

Insight summary – integrated view

Insight summary

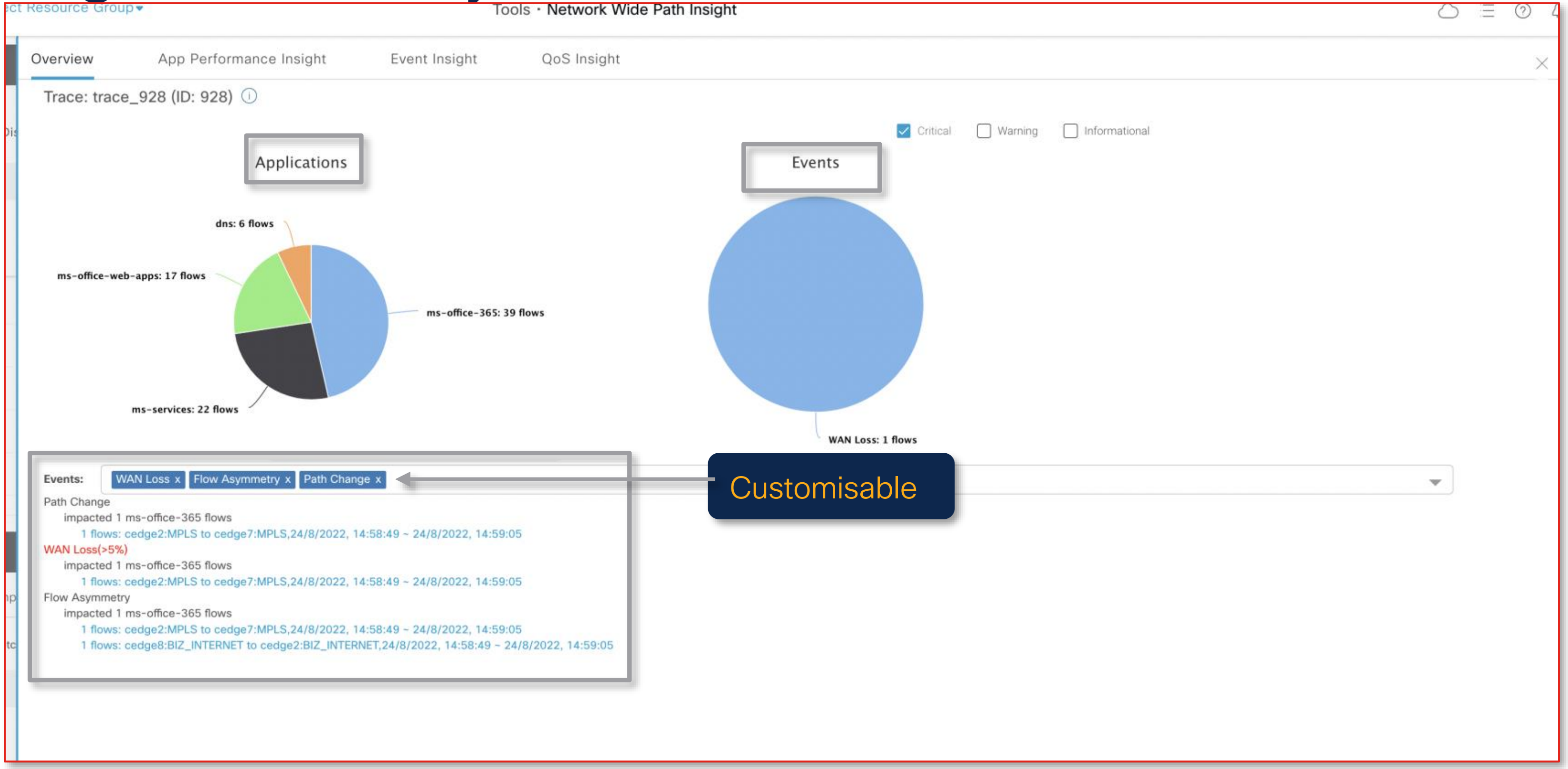


Selected trace: trace_928 (Trace Id: 928)

Total Rows: 120

Trace Name	Trace ID	Start Time	Stop Time	Src. Site	VPN ID	Application/App Group	Domain Monitor	Trace State	Action
Insight Summary | trace_928	928	24 Aug 2022 2:55:49 PM	N/A	12	1	N/A	disabled	starting	View Insight

Insight summary: Overview



Trace: trace_928 (ID: 928)

Events: WAN Loss x Flow Asymmetry x Path Change x

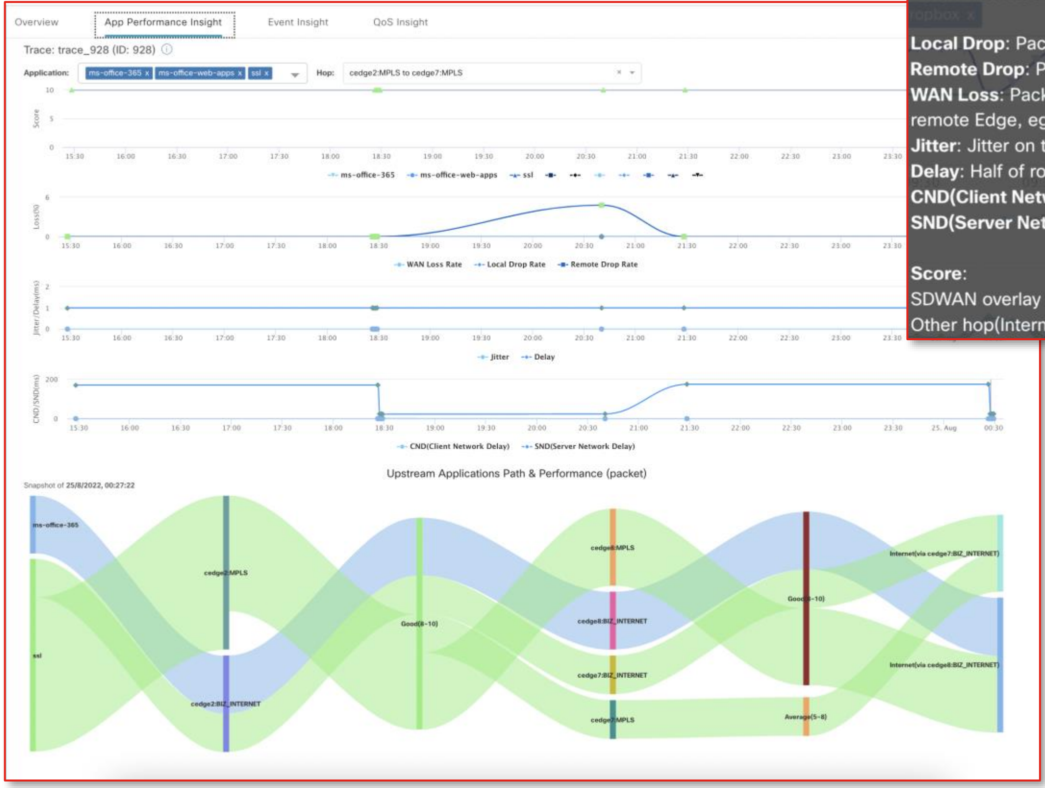
Path Change
impacted 1 ms-office-365 flows
1 flows: cedge2:MPLS to cedge7:MPLS,24/8/2022, 14:58:49 ~ 24/8/2022, 14:59:05

WAN Loss(>5%)
impacted 1 ms-office-365 flows
1 flows: cedge2:MPLS to cedge7:MPLS,24/8/2022, 14:58:49 ~ 24/8/2022, 14:59:05

Flow Asymmetry
impacted 1 ms-office-365 flows
1 flows: cedge2:MPLS to cedge7:MPLS,24/8/2022, 14:58:49 ~ 24/8/2022, 14:59:05
1 flows: cedge8:BIZ_INTERNET to cedge2:BIZ_INTERNET,24/8/2022, 14:58:49 ~ 24/8/2022, 14:59:05

Customisable

Insight Summary: App Performance insight



Overview | App Performance Insight | Event Insight | QoS Insight

Trace: trace_928 (ID: 928)

Application: ms-office-365 x ms-office-web-apps x ssl x Hop: cedge2:MPLS to cedge7:MPLS

Upstream Applications Path & Performance (packet)

Snapshot of 25/8/2022, 00:27:22

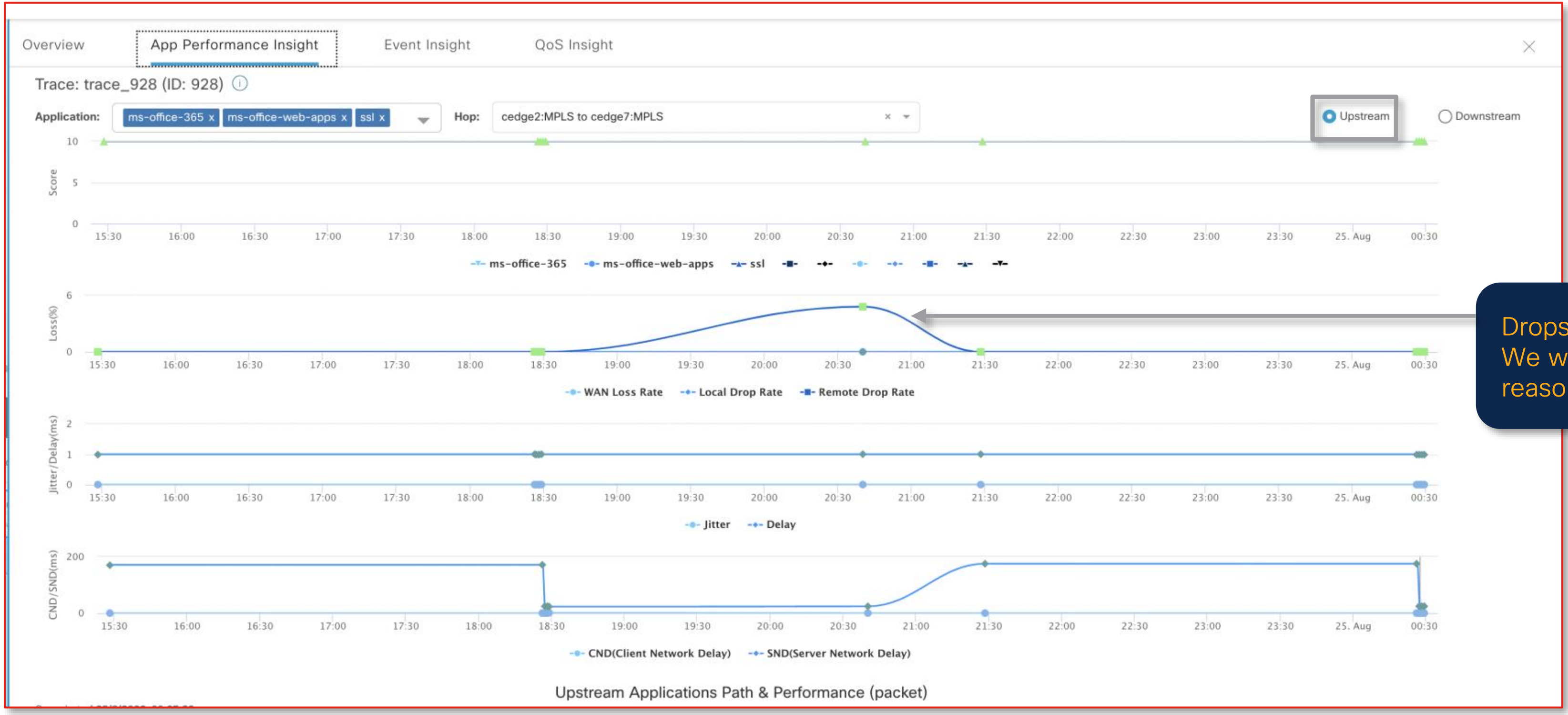
Below metrics all based on sampled application flows:

Local Drop: Packet drop on hop's local Edge
Remote Drop: Packet drop on hop's remote Edge (WAN underlay drop on remote Edge excluded)
WAN Loss: Packet loss on WAN from hop's local Edge to remote Edge (includes WAN underlay drop on remote Edge, eg. IPSec Anti-Replay drop)
Jitter: Jitter on the hop
Delay: Half of round trip delay on the hop
CND(Client Network Delay): TCP round trip delay between hop's local Edge and the client
SND(Server Network Delay): TCP round trip delay between hop's local Edge and the server

Score:
SDWAN overlay hop: Calculated based on Loss/Jitter/Latency
Other hop(Internet/SaaS/SIG/LAN etc.): Calculated based on SND

Let's deep dive into it….

Insight Summary: App Performance insight



Overview | App Performance Insight | Event Insight | QoS Insight

Trace: trace_928 (ID: 928)

Application: ms-office-365 x ms-office-web-apps x ssl x

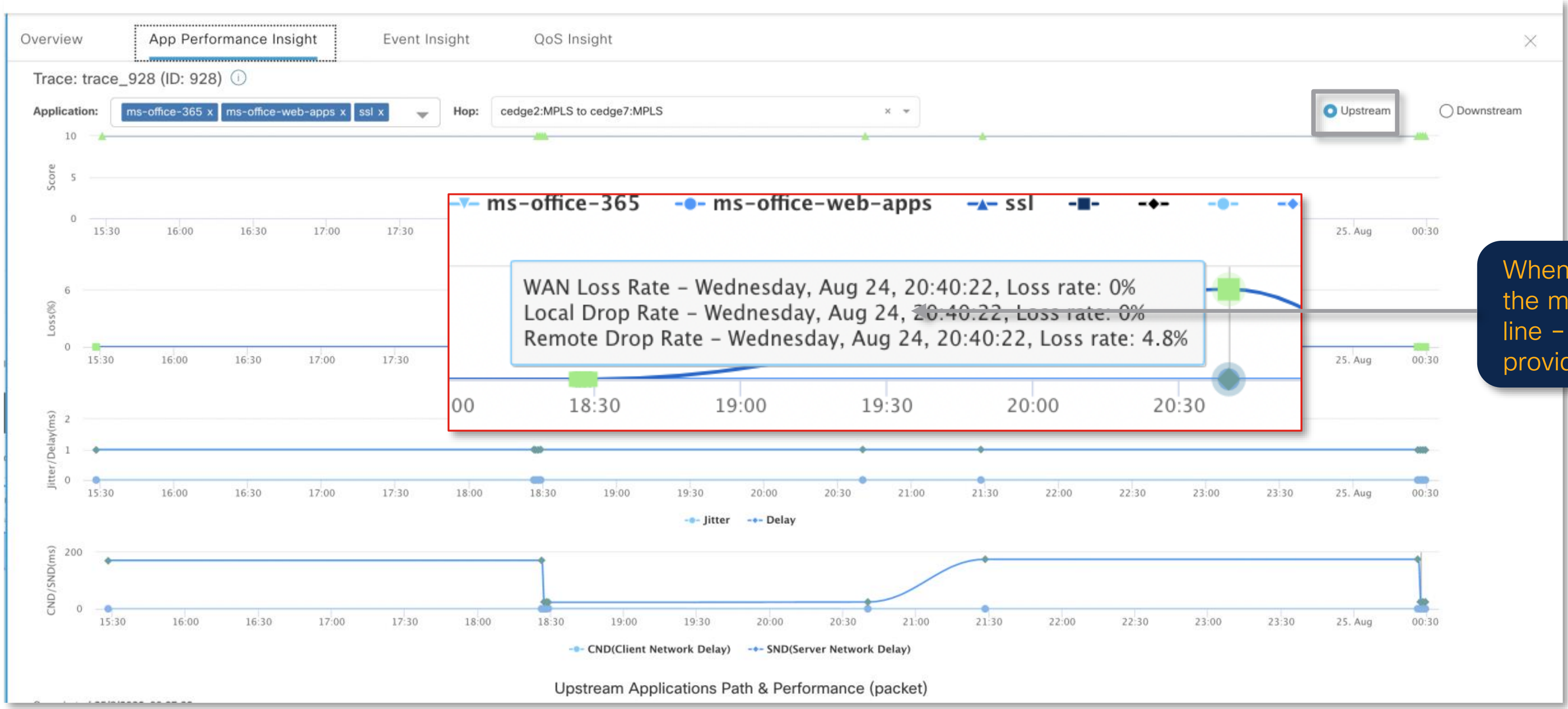
Hop: cedge2:MPLS to cedge7:MPLS

● Upstream ○ Downstream

Upstream Applications Path & Performance (packet)

Drops!
We will find out the reason later

Insight Summary: App Performance insight



Trace: trace_928 (ID: 928)

Application: ms-office-365 x ms-office-web-apps x ssl x

Hop: cedge2:MPLS to cedge7:MPLS

● Upstream ○ Downstream

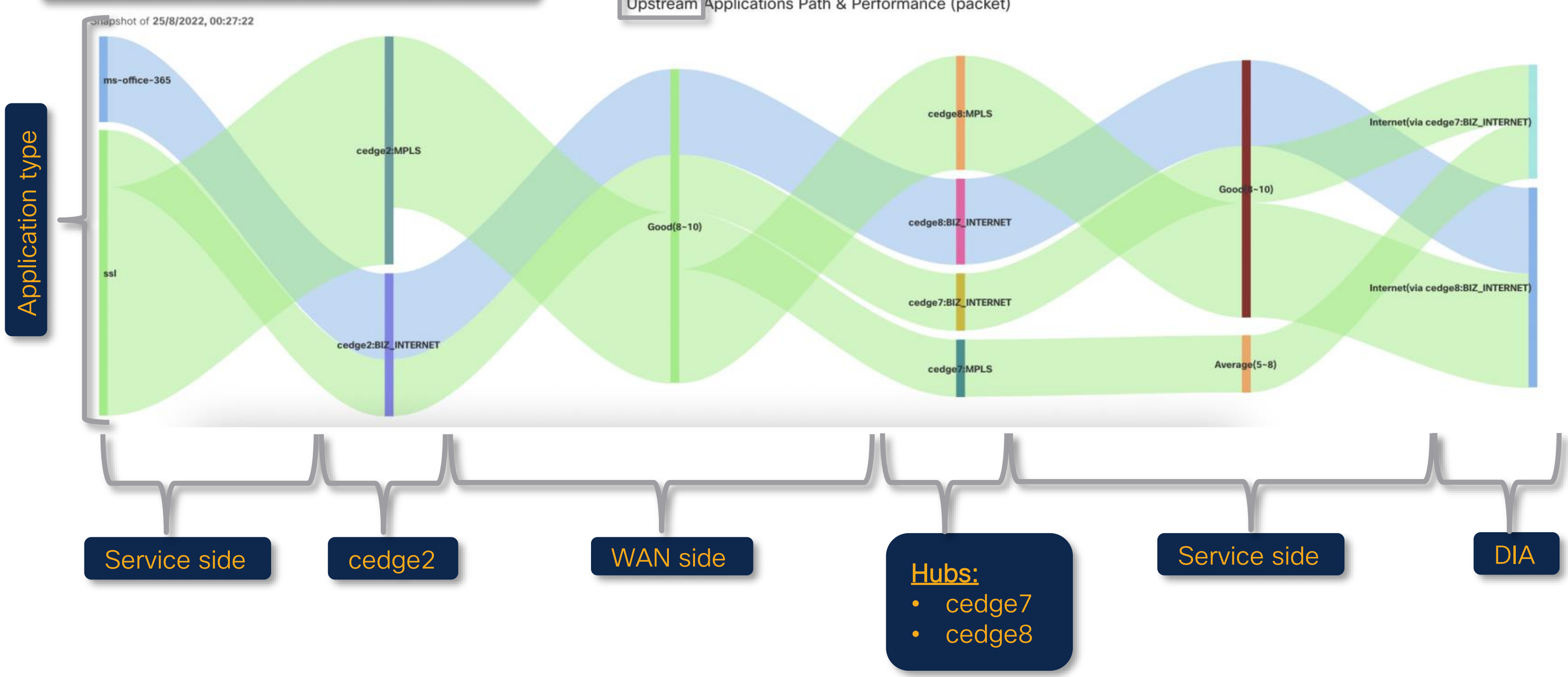
WAN Loss Rate – Wednesday, Aug 24, 20:40:22, Loss rate: 0%
Local Drop Rate – Wednesday, Aug 24, 20:40:22, Loss rate: 0%
Remote Drop Rate – Wednesday, Aug 24, 20:40:22, Loss rate: 4.8%

Upstream Applications Path & Performance (packet)

When hovering with the mouse over the line – drop rate is provided

Insight Summary: Applications path and performance

Downstream can be selected as well



Application type

Service side

cedge2

WAN side

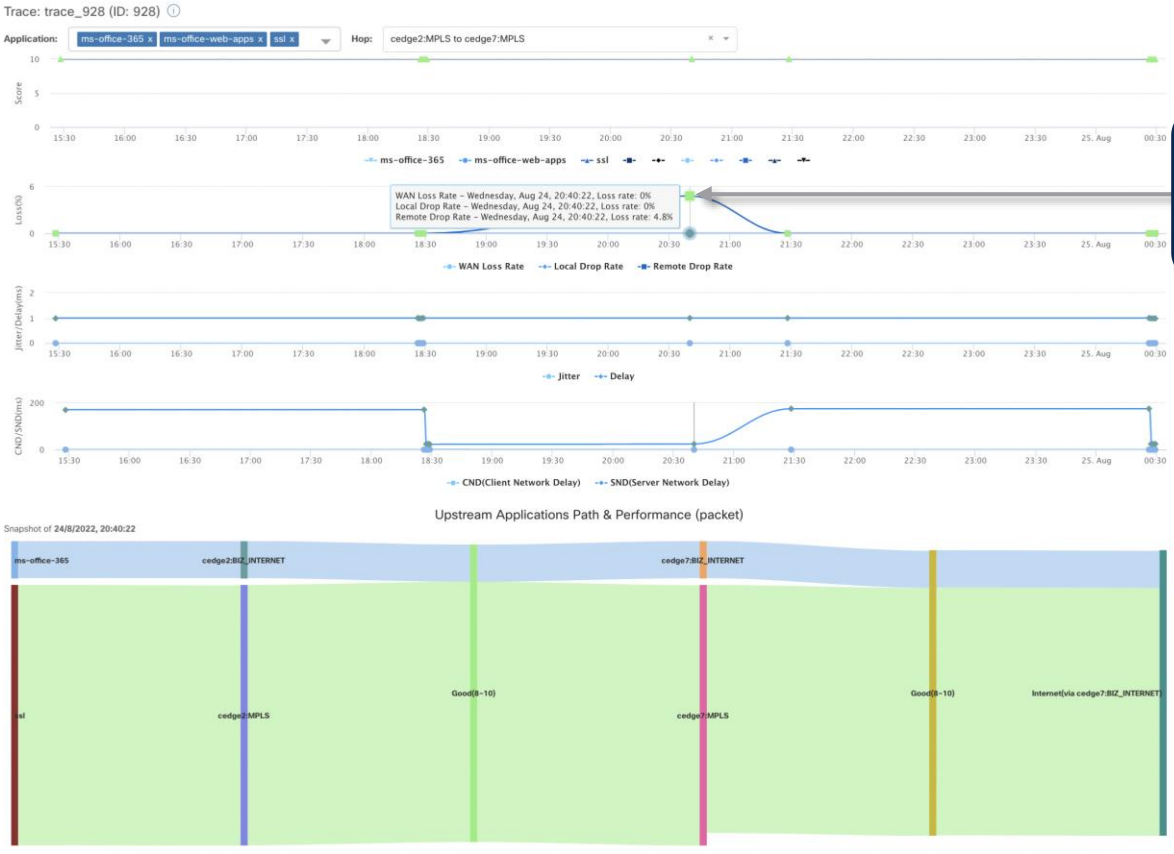
Hubs:

- cedge7
- cedge8

Service side

DIA

Insight Summary: Application path and performance



Trace: trace_928 (ID: 928)

Application: ms-office-365 x ms-office-web-apps x ssl x

Hop: cedge2:MPLS to cedge7:MPLS

WAN Loss Rate – Wednesday, Aug 24, 20:40:22, Loss rate: 0%
Local Drop Rate – Wednesday, Aug 24, 20:40:22, Loss rate: 0%
Remote Drop Rate – Wednesday, Aug 24, 20:40:22, Loss rate: 4.8%

Upstream Applications Path & Performance (packet)

Snapshot of **24/8/2022, 20:40:22**

Clicking on the graph will display the application path and performance taken at that exact time.

Insight Summary – QoS Insight

Tips

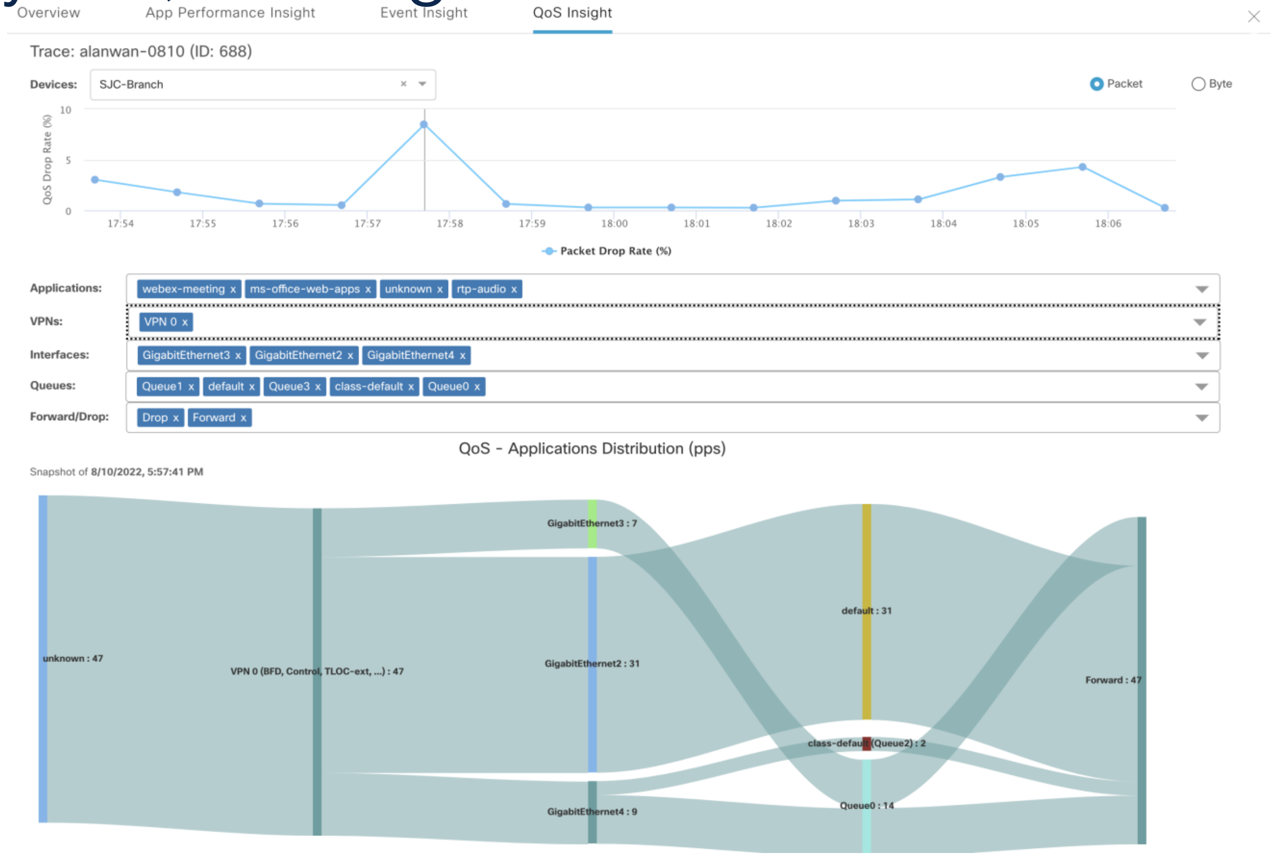
Traffic in VPN0 may compete bandwidth with user traffic.

- 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



Trace: alanwan-0810 (ID: 688)

Devices: SJC-Branch

● Packet ○ Byte

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

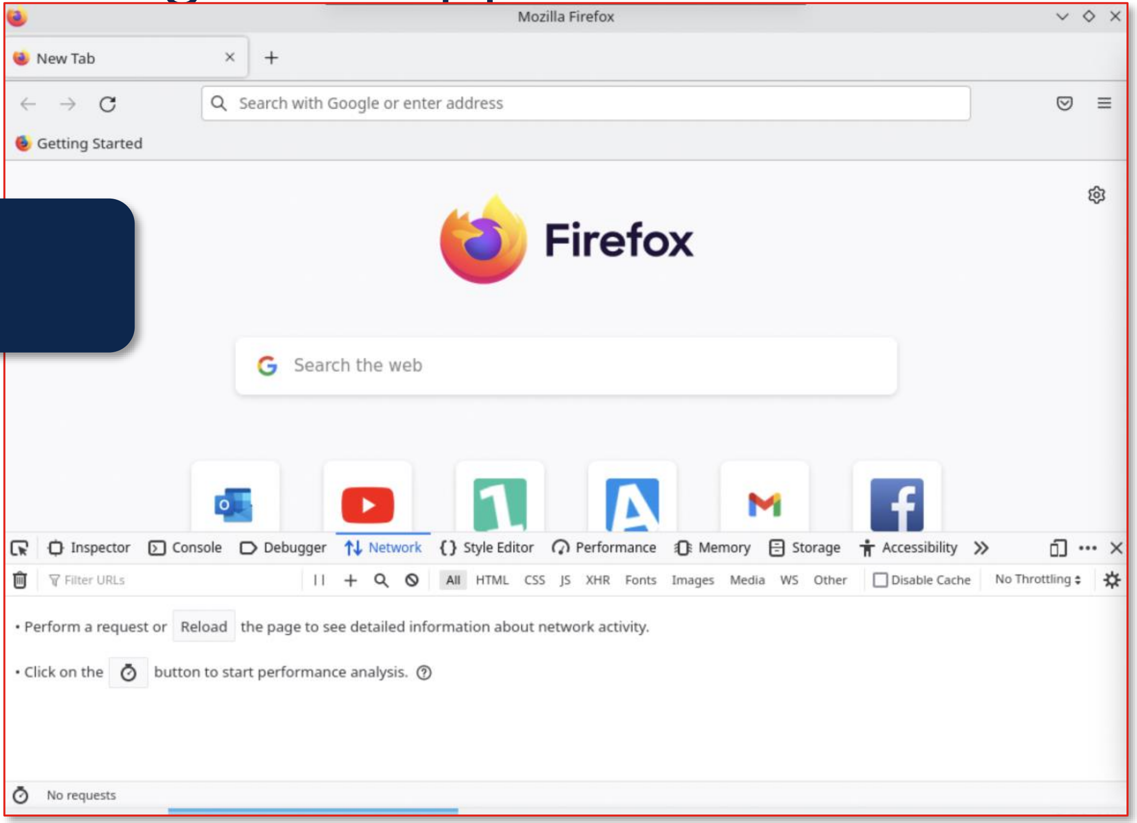
Forward/Drop: Drop x Forward x

QoS - Applications Distribution (pps)

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

DNS discovery tracing

Troubleshooting web application



• Perform a request or Reload the page to see detailed information about network activity.

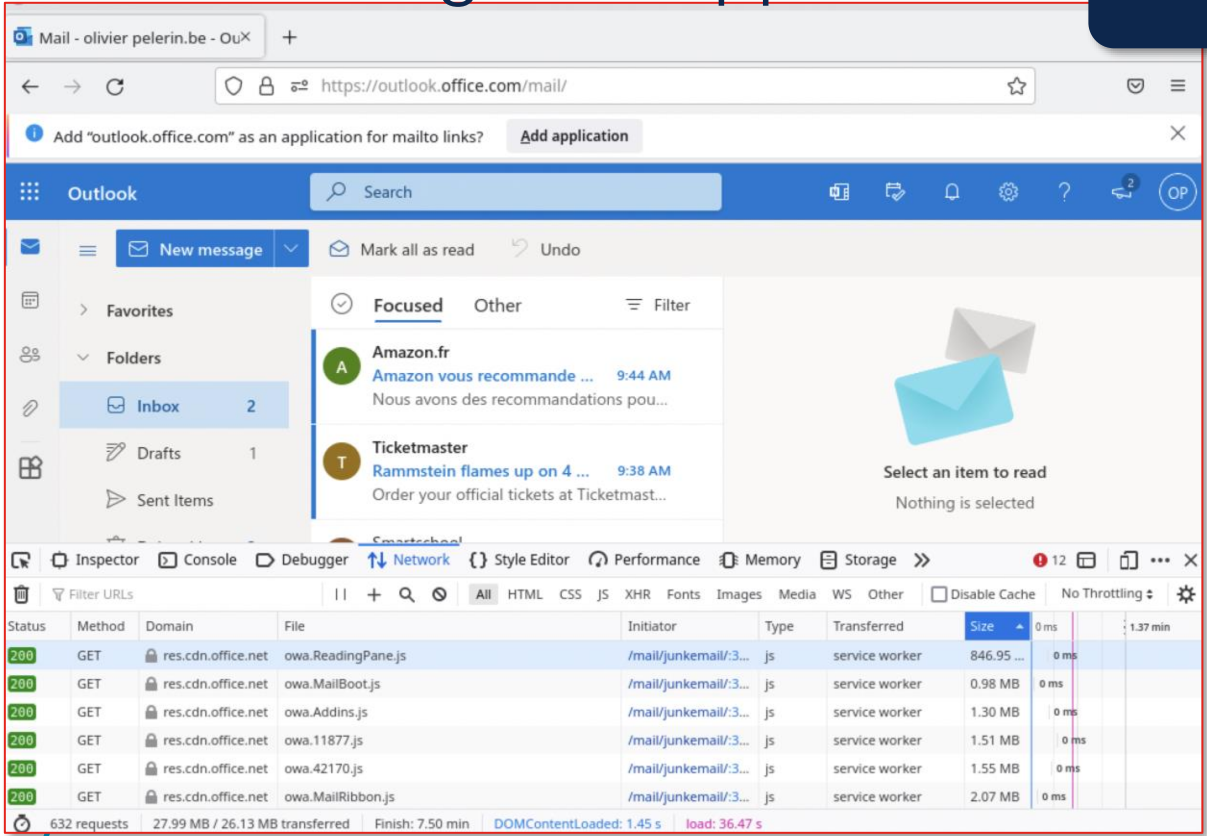
• Click on the ⏱ button to start performance analysis.

No requests

1) Enabling web developer tools
2) Look at the network tab

Troubleshooting web application

Stack by size

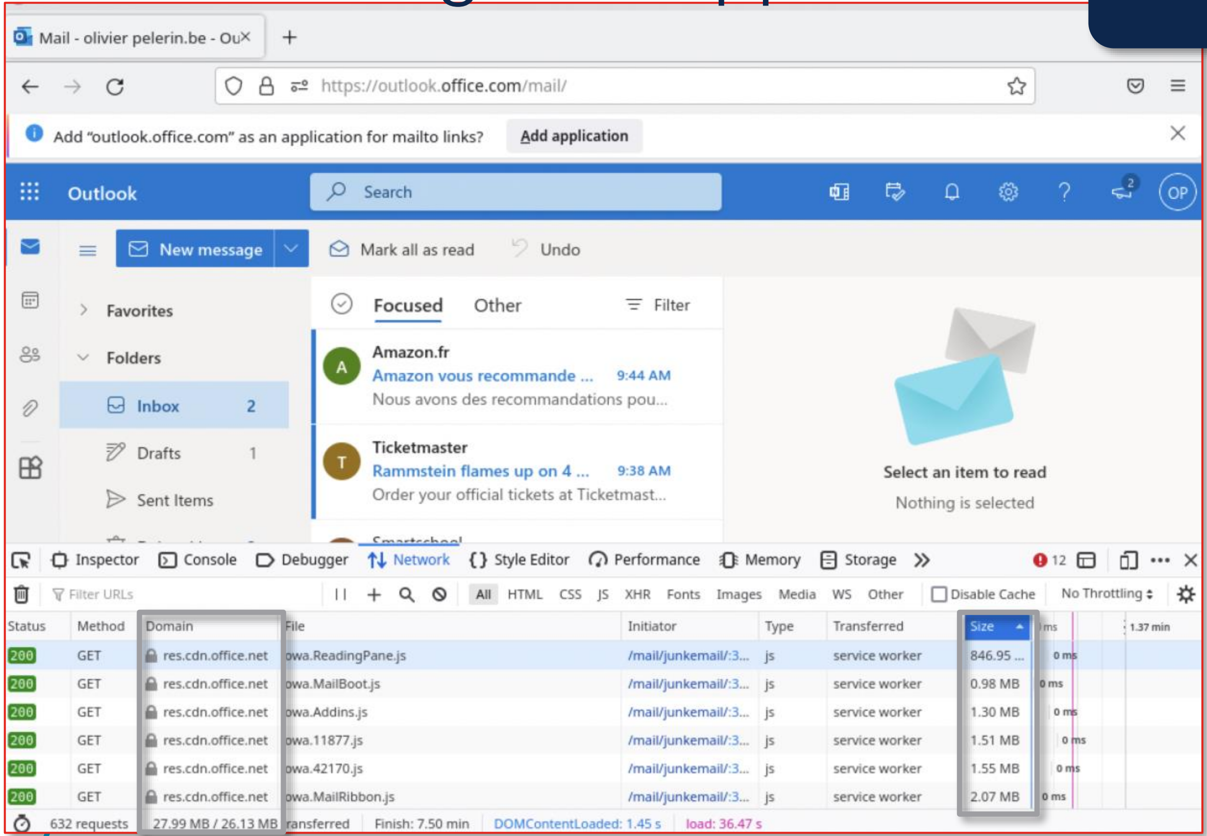


Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	res.cdn.office.net	owa.ReadingPane.js	/mail/junkemail/:3...	js	service worker	846.95 ...	0 ms
200	GET	res.cdn.office.net	owa.MailBoot.js	/mail/junkemail/:3...	js	service worker	0.98 MB	0 ms
200	GET	res.cdn.office.net	owa.Addins.js	/mail/junkemail/:3...	js	service worker	1.30 MB	0 ms
200	GET	res.cdn.office.net	owa.11877.js	/mail/junkemail/:3...	js	service worker	1.51 MB	0 ms
200	GET	res.cdn.office.net	owa.42170.js	/mail/junkemail/:3...	js	service worker	1.55 MB	0 ms
200	GET	res.cdn.office.net	owa.MailRibbon.js	/mail/junkemail/:3...	js	service worker	2.07 MB	0 ms

632 requests | 27.99 MB / 26.13 MB transferred | Finish: 7.50 min | DOMContentLoaded: 1.45 s | load: 36.47 s

Troubleshooting web application

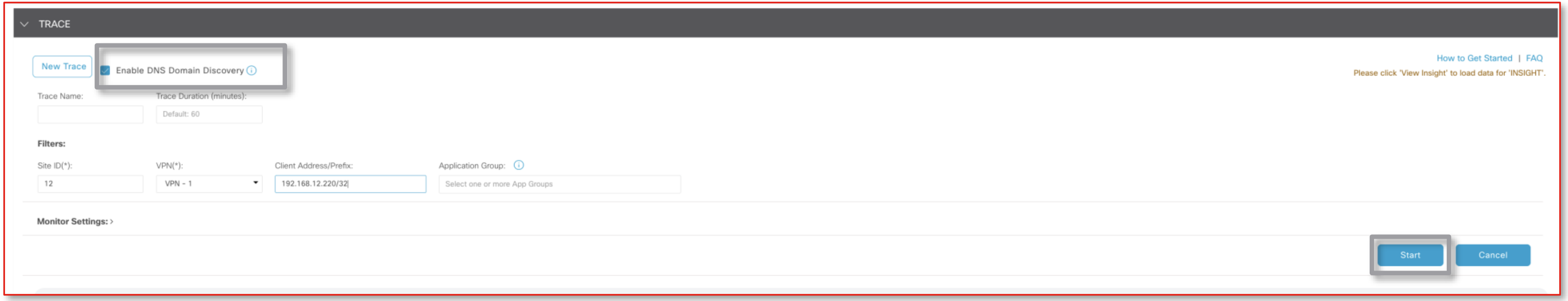
Stack by size



Status	Method	Domain	File	Initiator	Type	Transferred	Size	
200	GET	res.cdn.office.net	owa.ReadingPane.js	/mail/junkemail/:3...	js	service worker	846.95 ...	0 ms
200	GET	res.cdn.office.net	owa.MailBoot.js	/mail/junkemail/:3...	js	service worker	0.98 MB	0 ms
200	GET	res.cdn.office.net	owa.Addins.js	/mail/junkemail/:3...	js	service worker	1.30 MB	0 ms
200	GET	res.cdn.office.net	owa.11877.js	/mail/junkemail/:3...	js	service worker	1.51 MB	0 ms
200	GET	res.cdn.office.net	owa.42170.js	/mail/junkemail/:3...	js	service worker	1.55 MB	0 ms
200	GET	res.cdn.office.net	owa.MailRibbon.js	/mail/junkemail/:3...	js	service worker	2.07 MB	0 ms

632 requests | 27.99 MB / 26.13 MB ransferred | Finish: 7.50 min | DOMContentLoaded: 1.45 s | load: 36.47 s

Starting NWPI



☑ Enable DNS Domain Discovery

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

Trace Name:

Trace Duration (minutes): Default: 60

Filters:

Site ID(*): 12

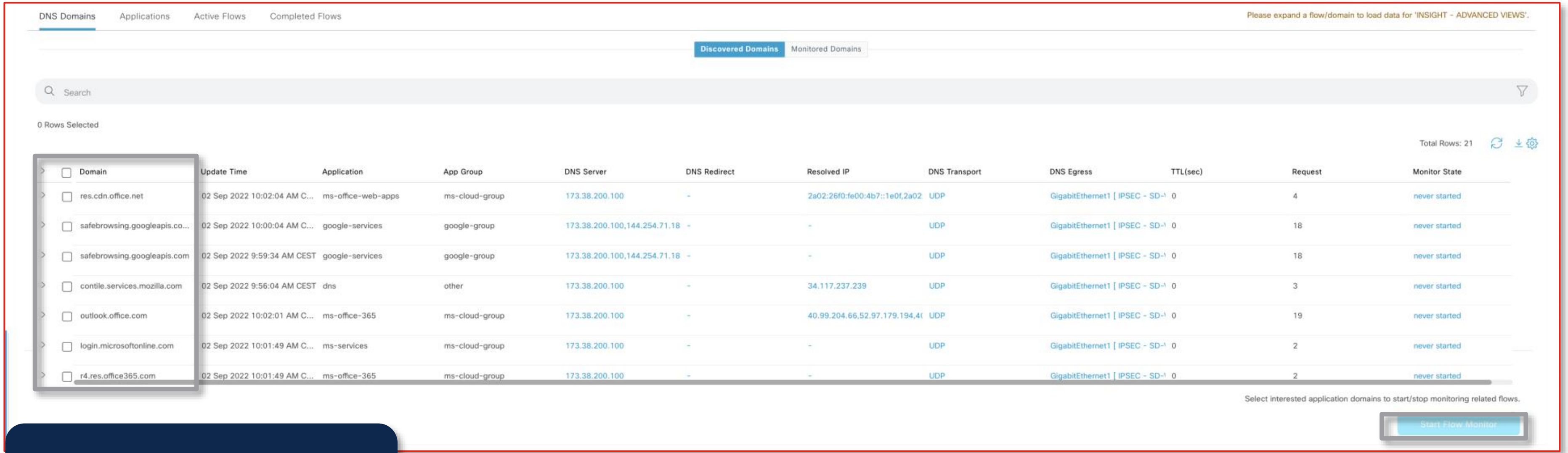
VPN(*): VPN - 1

Client Address/Prefix: 192.168.12.220/32

Application Group: Select one or more App Groups

Monitor Settings: >

Monitoring dns traffic



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

0 Rows Selected

Total Rows: 21

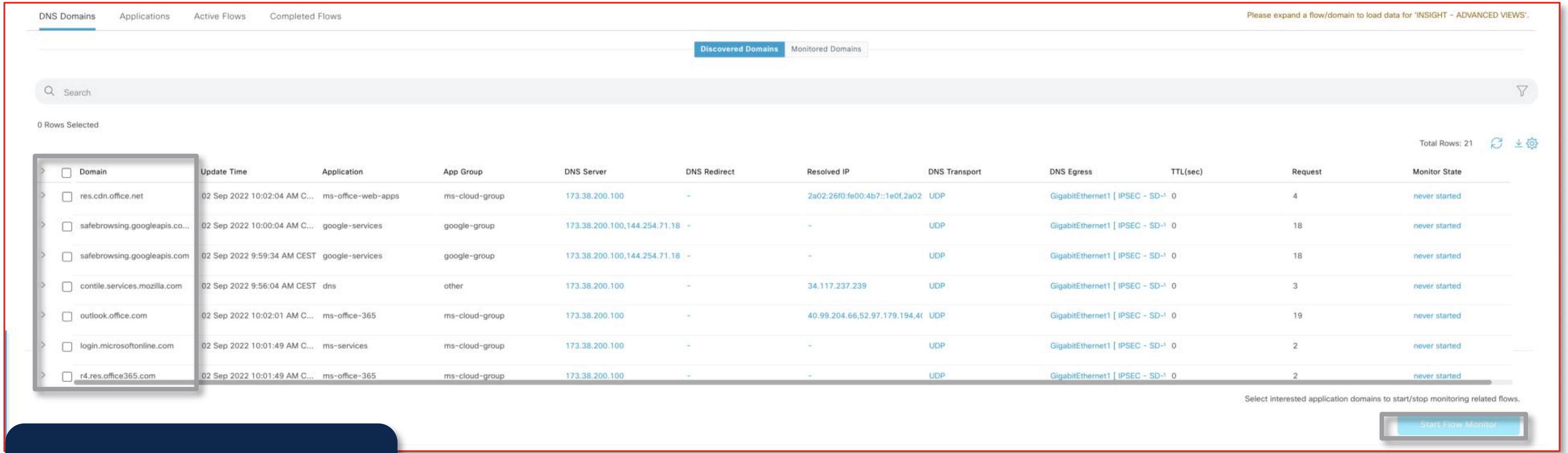
	Domain	Update Time	Application	App Group	DNS Server	DNS Redirect	Resolved IP	DNS Transport	DNS Egress	TTL(sec)	Request	Monitor State
□	res.cdn.office.net	02 Sep 2022 10:02:04 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-	2a02:26f0:fe00:4b7::1e0f,2a02	UDP	GigabitEthernet1 [IPSEC - SD-\	0	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-\	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-\	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-\	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	-	40.99.204.66,52.97.179.194,4(	UDP	GigabitEthernet1 [IPSEC - SD-\	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-\	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-\	0	2	never started

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

Lots of “stuff” let’s focus on o365

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

Monitoring dns traffic



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

0 Rows Selected

Total Rows: 21

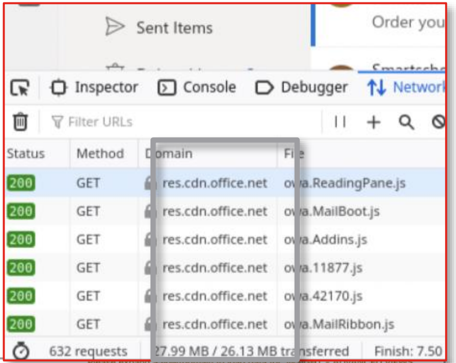
	Domain	Update Time	Application	App Group	DNS Server	DNS Redirect	Resolved IP	DNS Transport	DNS Egress	TTL(sec)	Request	Monitor State
□	res.cdn.office.net	02 Sep 2022 10:02:04 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-	2a02:26f0:fe00:4b7::1e0f,2a02	UDP	GigabitEthernet1 [IPSEC - SD-\	0	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-\	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-\	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-\	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	-	40.99.204.66,52.97.179.194,4(	UDP	GigabitEthernet1 [IPSEC - SD-\	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-\	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-\	0	2	never started

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

Lots of “stuff” let’s focus on o365

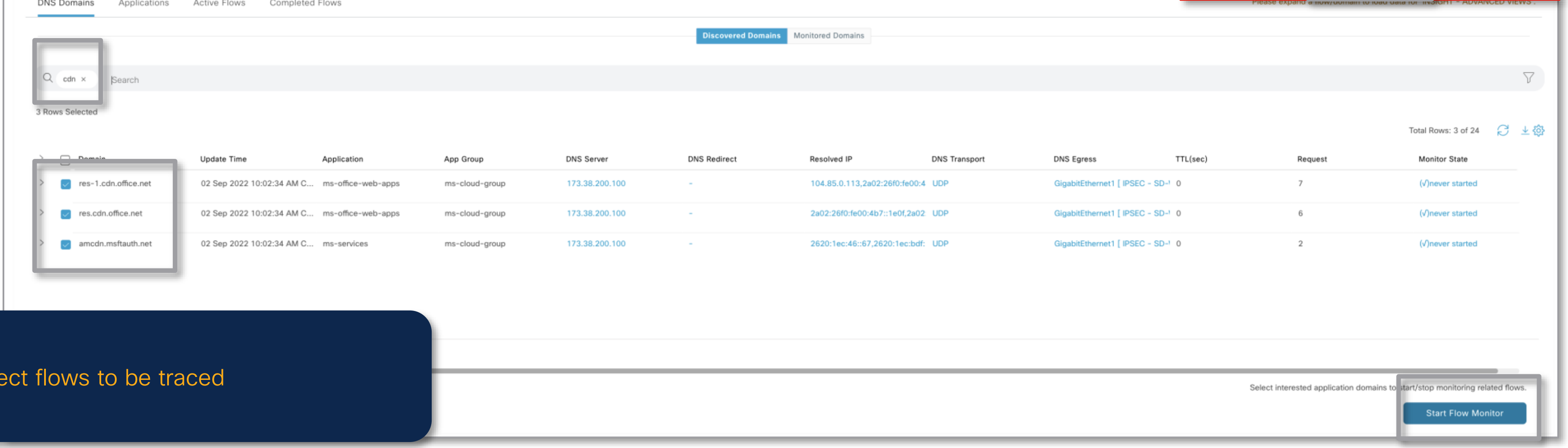
Start monitoring to effectively trace TCP or UDP flows to those fully qualified domain names [FQDN]

Drill down and enable flow tracing



Status	Method	Domain	File
200	GET	res.cdn.office.net	owa.ReadingPane.js
200	GET	res.cdn.office.net	owa.MailBoot.js
200	GET	res.cdn.office.net	owa.Addins.js
200	GET	res.cdn.office.net	owa.11877.js
200	GET	res.cdn.office.net	owa.42170.js
200	GET	res.cdn.office.net	owa.MailRibbon.js

632 requests | 27.99 MB / 26.13 MB transferred | Finish: 7.50



3 Rows Selected

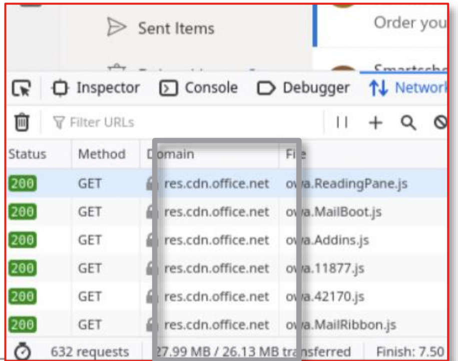
Total Rows: 3 of 24

	Domain	Update Time	Application	App Group	DNS Server	DNS Redirect	Resolved IP	DNS Transport	DNS Egress	TTL(sec)	Request	Monitor State
☑	res-1.cdn.office.net	02 Sep 2022 10:02:34 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-	104.85.0.113,2a02:26f0:fe00:4	UDP	GigabitEthernet1 [IPSEC - SD-'	0	7	(√)never started
☑	res.cdn.office.net	02 Sep 2022 10:02:34 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-	2a02:26f0:fe00:4b7::1e0f,2a02:	UDP	GigabitEthernet1 [IPSEC - SD-'	0	6	(√)never started
☑	amcdn.msftauth.net	02 Sep 2022 10:02:34 AM C...	ms-services	ms-cloud-group	173.38.200.100	-	2620:1ec:46::67,2620:1ec:bdf:	UDP	GigabitEthernet1 [IPSEC - SD-'	0	2	(√)never started

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

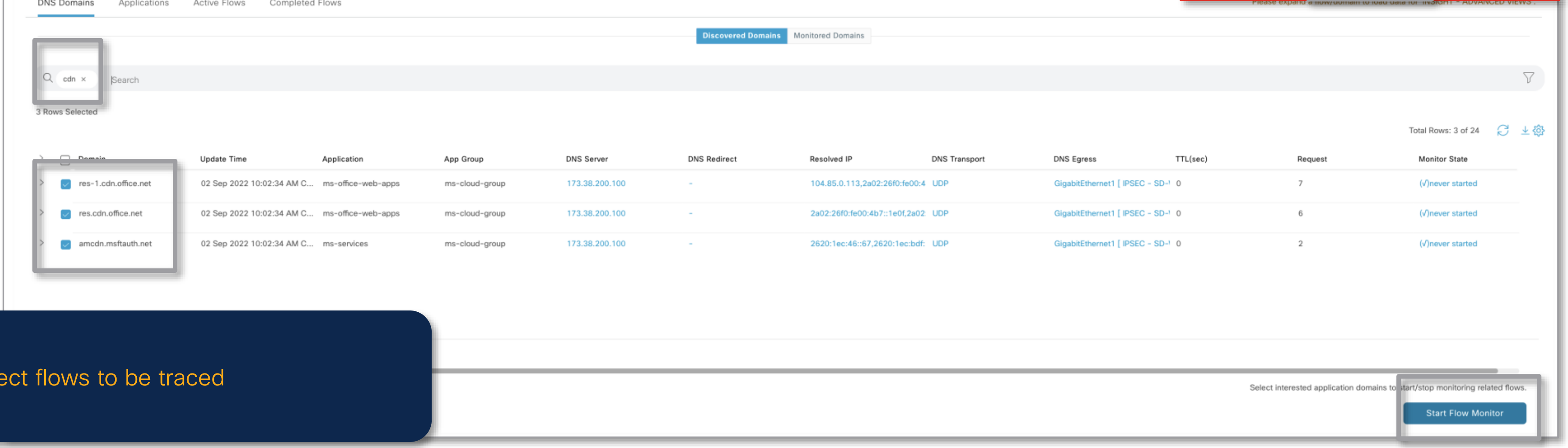
Select flows to be traced

Drill down and enable flow tracing



Status	Method	Domain	File
200	GET	res.cdn.office.net	owa.ReadingPane.js
200	GET	res.cdn.office.net	owa.MailBoot.js
200	GET	res.cdn.office.net	owa.Addins.js
200	GET	res.cdn.office.net	owa.11877.js
200	GET	res.cdn.office.net	owa.42170.js
200	GET	res.cdn.office.net	owa.MailRibbon.js

632 requests | 27.99 MB / 26.13 MB transferred | Finish: 7.50



3 Rows Selected

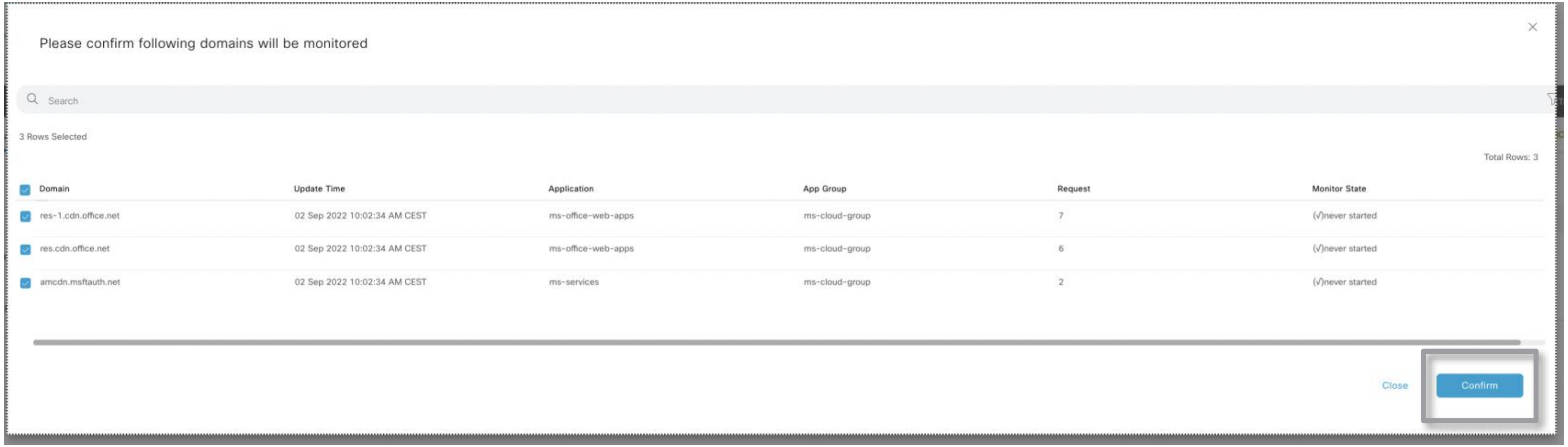
Total Rows: 3 of 24

	Domain	Update Time	Application	App Group	DNS Server	DNS Redirect	Resolved IP	DNS Transport	DNS Egress	TTL(sec)	Request	Monitor State
☑	res-1.cdn.office.net	02 Sep 2022 10:02:34 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-	104.85.0.113,2a02:26f0:fe00:4	UDP	GigabitEthernet1 [IPSEC - SD-'	0	7	(√)never started
☑	res.cdn.office.net	02 Sep 2022 10:02:34 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-	2a02:26f0:fe00:4b7::1e0f,2a02	UDP	GigabitEthernet1 [IPSEC - SD-'	0	6	(√)never started
☑	amcdn.msftauth.net	02 Sep 2022 10:02:34 AM C...	ms-services	ms-cloud-group	173.38.200.100	-	2620:1ec:46::67,2620:1ec:bdf:	UDP	GigabitEthernet1 [IPSEC - SD-'	0	2	(√)never started

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

Select flows to be traced

Confirm and start monitoring



Please confirm following domains will be monitored

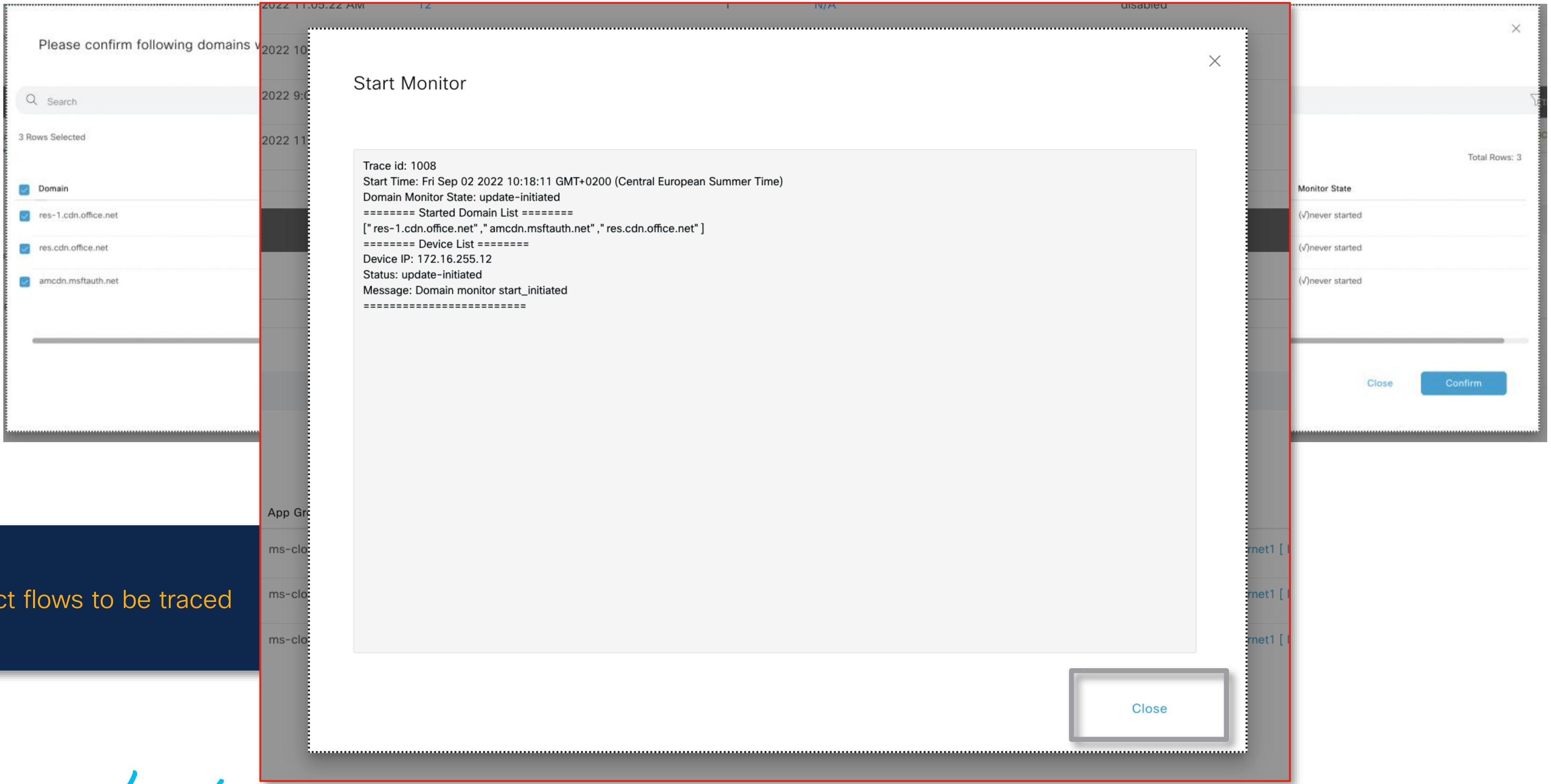
Search

3 Rows Selected

Total Rows: 3

☑ Domain	Update Time	Application	App Group	Request	Monitor State
☑ res-1.cdn.office.net	02 Sep 2022 10:02:34 AM CEST	ms-office-web-apps	ms-cloud-group	7	(√)never started
☑ res.cdn.office.net	02 Sep 2022 10:02:34 AM CEST	ms-office-web-apps	ms-cloud-group	6	(√)never started
☑ amcdn.msftauth.net	02 Sep 2022 10:02:34 AM CEST	ms-services	ms-cloud-group	2	(√)never started

Confirm and start monitoring



Please confirm following domains v

Search

3 Rows Selected

Total Rows: 3

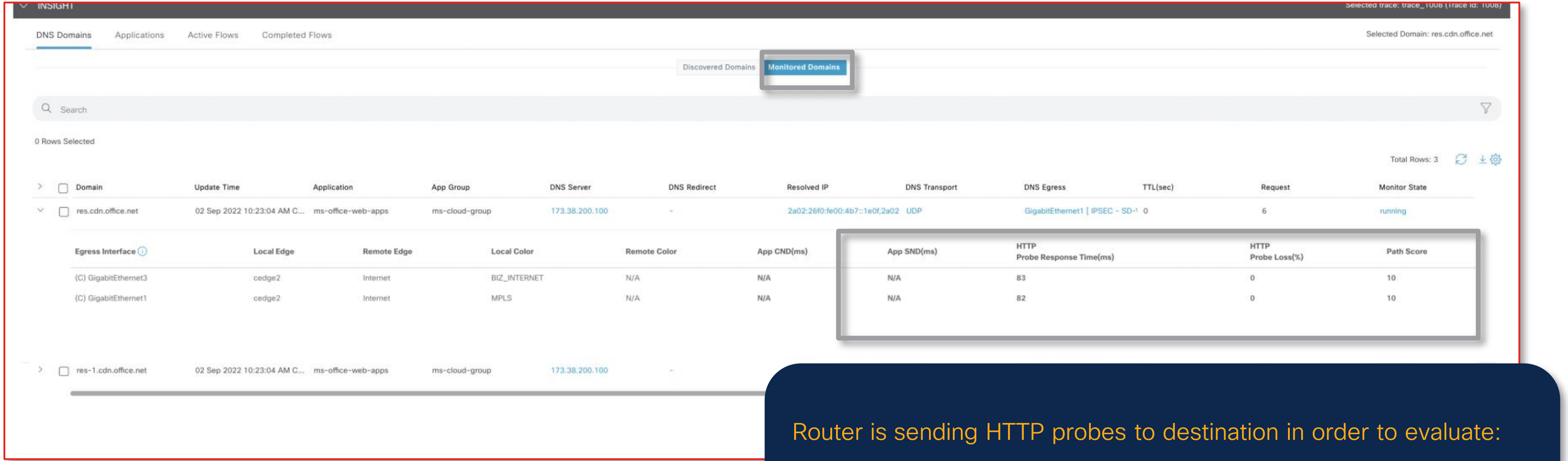
☑ Domain	Monitor State
☑ res-1.cdn.office.net	(√)never started
☑ res.cdn.office.net	(√)never started
☑ amcdn.msftauth.net	(√)never started

Start Monitor

```
Trace id: 1008
Start Time: Fri Sep 02 2022 10:18:11 GMT+0200 (Central European Summer Time)
Domain Monitor State: update-initiated
======== Started Domain List ========
[" res-1.cdn.office.net" ," amcdn.msftauth.net" ," res.cdn.office.net" ]
======== Device List ========
Device IP: 172.16.255.12
Status: update-initiated
Message: Domain monitor start_initiated
=========================
```

Select flows to be traced

Switch to monitored domains



Selected trace: trace_1008 (Trace Id: 1008)

Selected Domain: res.cdn.office.net

0 Rows Selected

Total Rows: 3

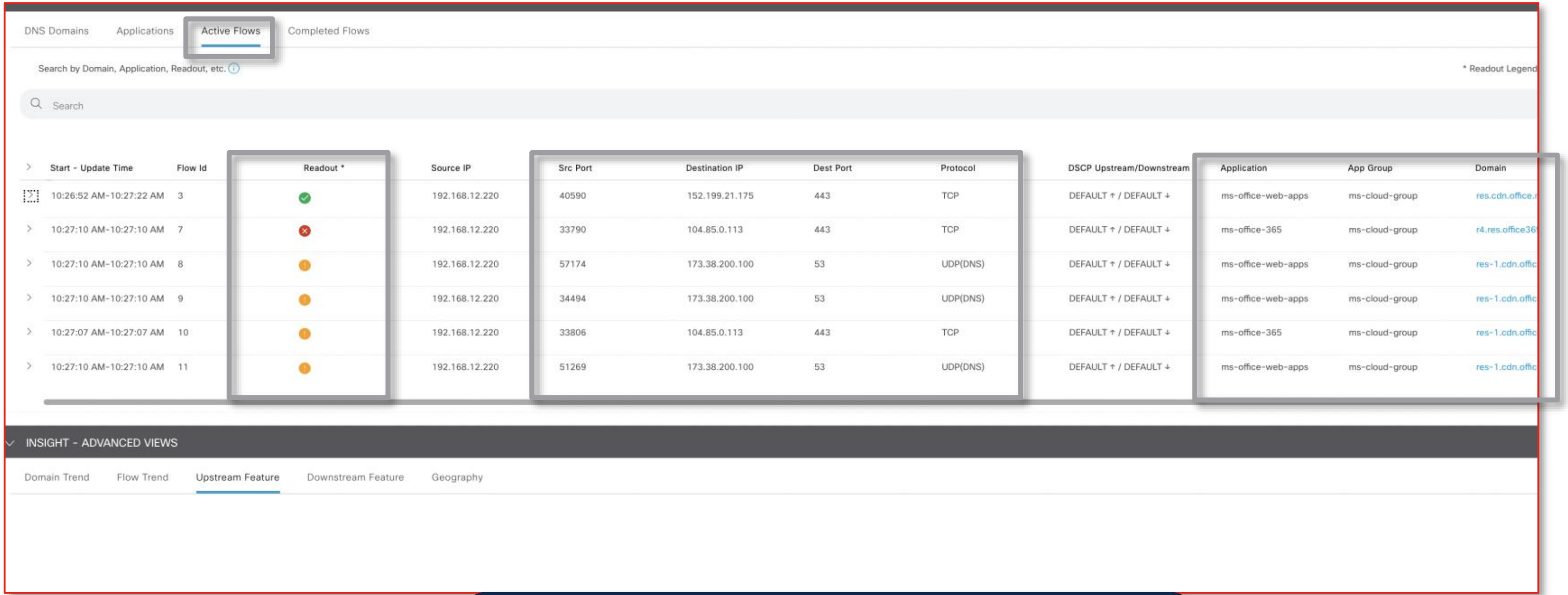
Domain	Update Time	Application	App Group	DNS Server	DNS Redirect	Resolved IP	DNS Transport	DNS Egress	TTL(sec)	Request	Monitor State
res.cdn.office.net	02 Sep 2022 10:23:04 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-	2a02:26f0:fe00:4b7::1e0f,2a02	UDP	GigabitEthernet1 [IPSEC - SD-'	0	6	running
res-1.cdn.office.net	02 Sep 2022 10:23:04 AM C...	ms-office-web-apps	ms-cloud-group	173.38.200.100	-						

Egress Interface	Local Edge	Remote Edge	Local Color	Remote Color	App CND(ms)	App SND(ms)	HTTP Probe Response Time(ms)	HTTP Probe Loss(%)	Path Score
(C) GigabitEthernet3	cedge2	Internet	BIZ_INTERNET	N/A	N/A	N/A	83	0	10
(C) GigabitEthernet1	cedge2	Internet	MPLS	N/A	N/A	N/A	82	0	10

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



Search by Domain, Application, Readout, etc.

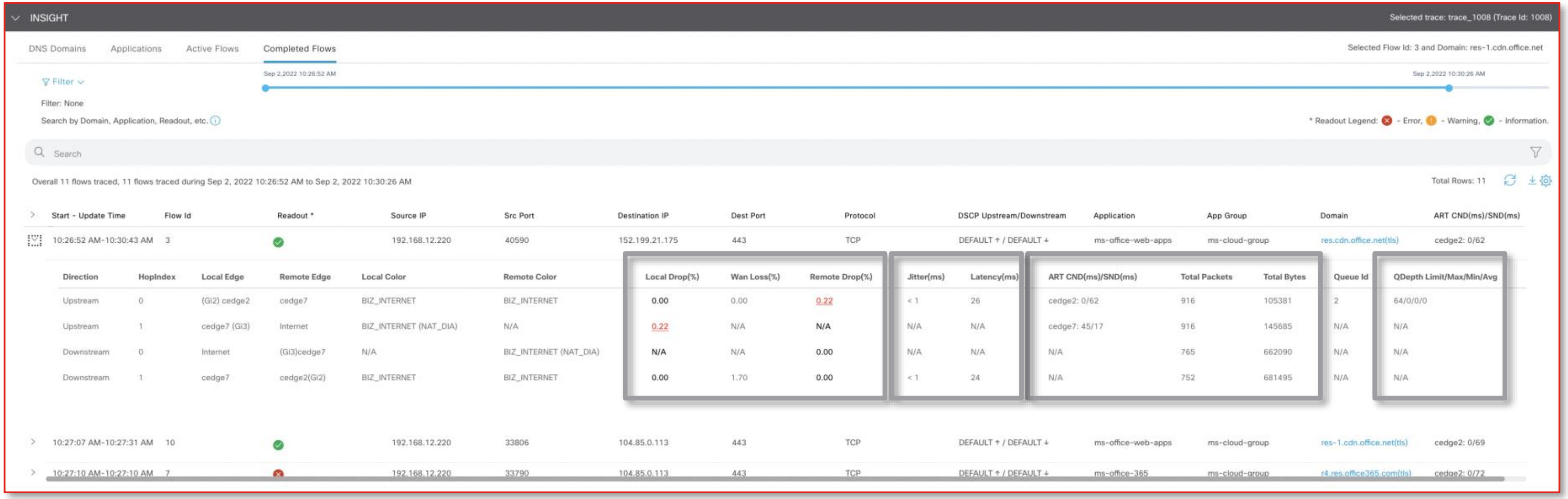
* Readout Legend

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.r
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	r4.res.office36
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.offic
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.offic
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.offic
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.offic

INSIGHT - ADVANCED VIEWS

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



INSIGHT

Selected trace: trace_1008 (Trace Id: 1008)

DNS Domains | Applications | Active Flows | Completed Flows

Selected Flow Id: 3 and Domain: res-1.cdn.office.net

Filter

Sep 2,2022 10:26:52 AM

Sep 2,2022 10:30:26 AM

Filter: None

Search by Domain, Application, Readout, etc.

* Readout Legend: ✗ - Error, ! - Warning, ✓ - Information.

Search

Overall 11 flows traced, 11 flows traced during Sep 2, 2022 10:26:52 AM to Sep 2, 2022 10:30:26 AM

Total Rows: 11

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)
10:26:52 AM-10:30:43 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.net(tls)	cedge2: 0/62

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	0.00	0.22	< 1	26	cedge2: 0/62	916	105381	2	64/0/0/0
Upstream	1	cedge7 (Gi3)	Internet	BIZ_INTERNET (NAT_DIA)	N/A	0.22	N/A	N/A	N/A	N/A	cedge7: 45/17	916	145685	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	765	662090	N/A	N/A
Downstream	1	cedge7	cedge2(Gi2)	BIZ_INTERNET	BIZ_INTERNET	0.00	1.70	0.00	< 1	24	N/A	752	681495	N/A	N/A

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)
10:27:07 AM-10:27:31 AM	10	✓	192.168.12.220	33806	104.85.0.113	443	TCP	DEFAULT ↑ / DEFAULT ↓	ms-office-web-apps	ms-cloud-group	res-1.cdn.office.net(tls)	cedge2: 0/69
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	r4.res.office365.com(tls)	cedge2: 0/72

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

Workflows – validating a AAR policy

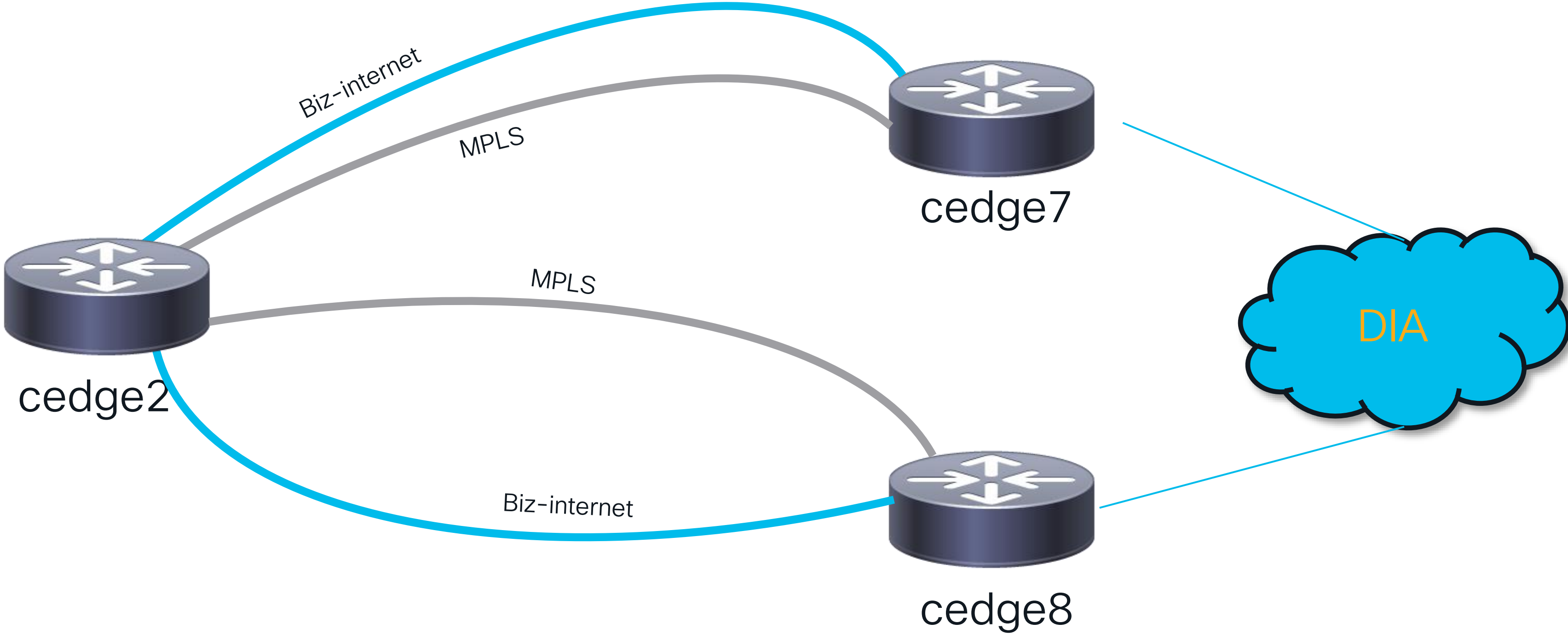
AAR policy

```
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

Preparing the UCS lab - topology



Preparing the UCS lab

```
root@UCS-Olivier:/home/olpeleri# virsh domiflist cedge2
 Interface   Type      Source          Model     MAC
-------------------------------------------------------------
 vnet183     bridge    br0             virtio    52:54:00:56:9c:b3
 <removed>
 vnet185     bridge    WAN-CEDGE2      virtio    52:54:00:06:43:f8
<removed>
root@UCS-Olivier:/home/olpeleri# virsh domiflist cedge7
 Interface   Type      Source          Model      MAC
--------------------------------------------------------------
 vnet207     bridge    br0             virtio     52:54:00:d6:37:d4
 <removed>
 vnet209     bridge    WAN-CEDGE7      virtio     52:54:00:e4:fa:df
<removed>
root@UCS-Olivier:/home/olpeleri# virsh domiflist cedge8
 Interface   Type      Source          Model     MAC
-------------------------------------------------------------
 vnet212     bridge    br0             virtio    52:54:00:27:95:89
 <removed>
 vnet214     bridge    WAN-CEDGE8      virtio    52:54:00:74:f0:9c
 <removed>
```

MPLS link

Internet link

MPLS link

Internet link

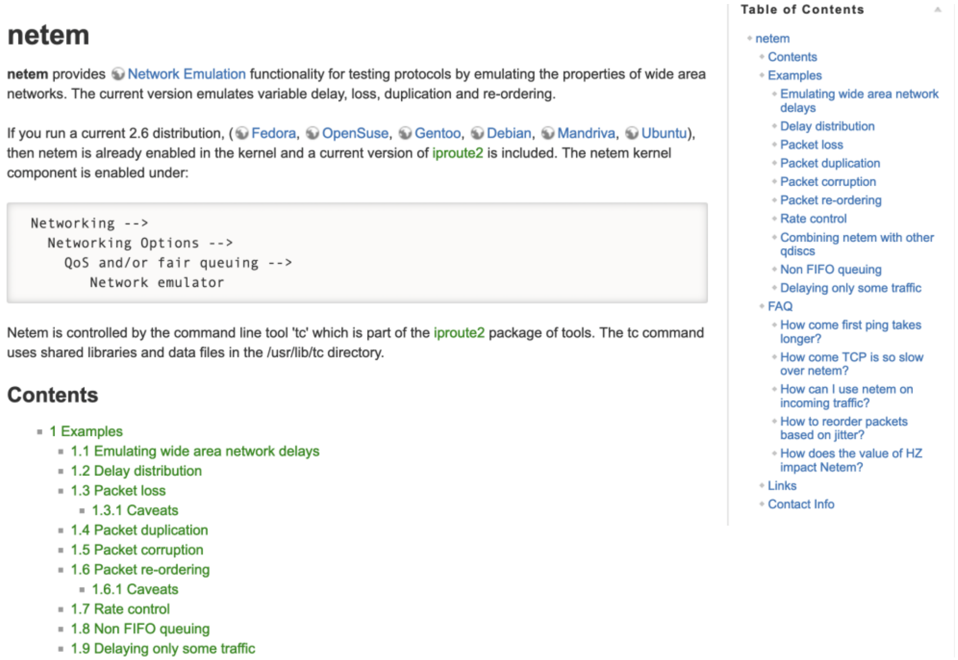
MPLS link

Internet link

Some words about netem

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

Amazing network emulation tool to recreate real life network problems.



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:

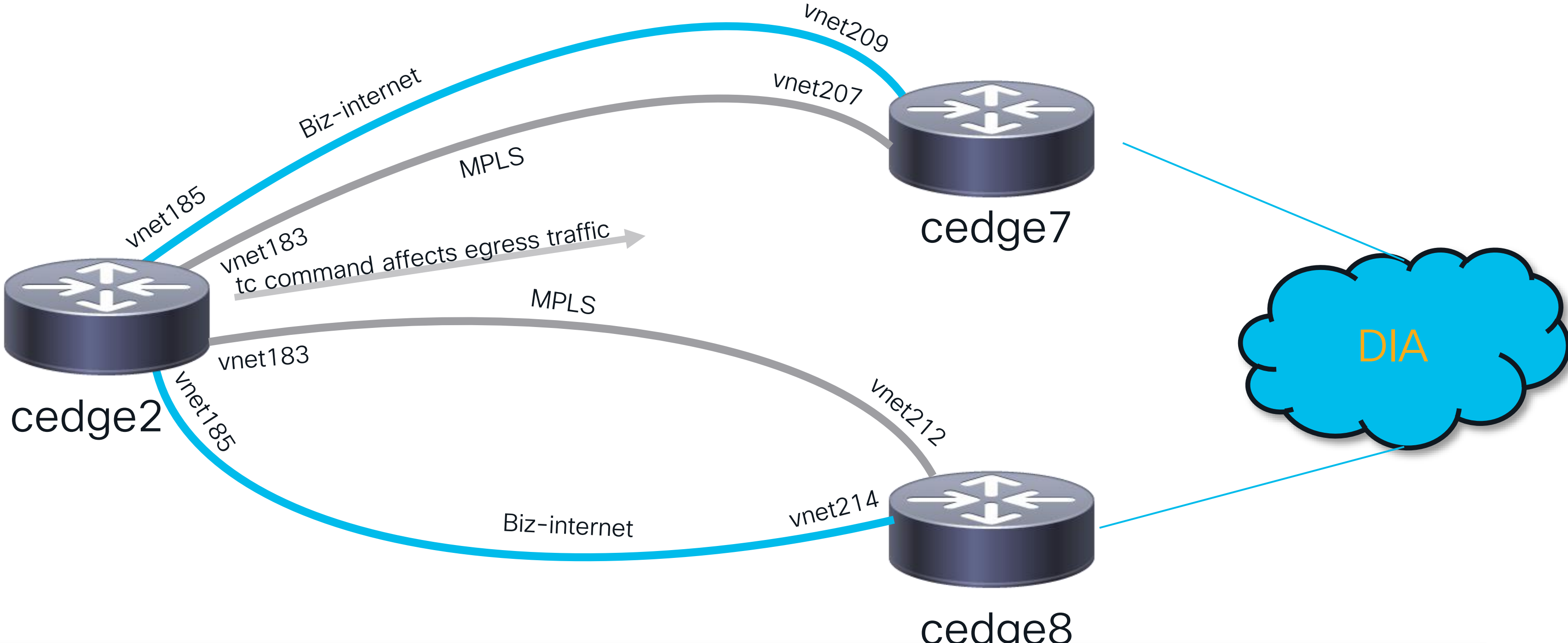
```
Networking -->
  Networking Options -->
    QoS and/or fair queuing -->
       Network emulator
```

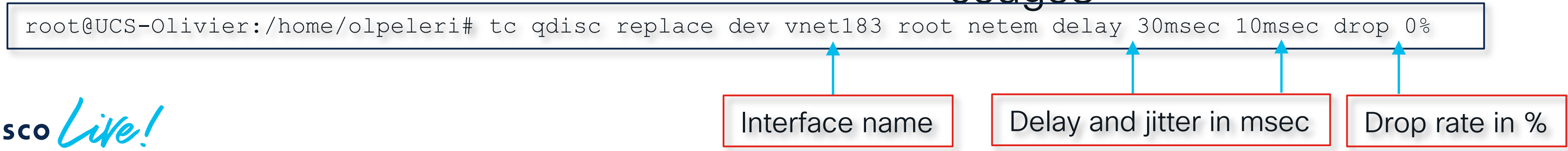
Netem is controlled by the command line tool 'tc' which is part of the iproute2 package of tools. The tc command uses shared libraries and data files in the /usr/lib/tc directory.

Contents

Table of Contents

Some words about netem (cont) -





```
root@UCS-Olivier:/home/olpeleri# tc qdisc replace dev vnet183 root netem delay 30msec 10msec drop 0%
```

Interface name

Delay and jitter in msec

Drop rate in %

Preparing the crime scene

Internet delay to 30 msec in each direction [60msec total delay] – 2msec delay in each direction

```
tc qdisc replace dev vnet185 root netem delay 30msec 2msec drop 0%
tc qdisc replace dev vnet209 root netem delay 30msec 2msec drop 0%
tc qdisc replace dev vnet214 root netem delay 30msec 2msec drop 0%
```

mpls delay to 20 msec in each direction [40msec total delay] – 5msec delay in each direction

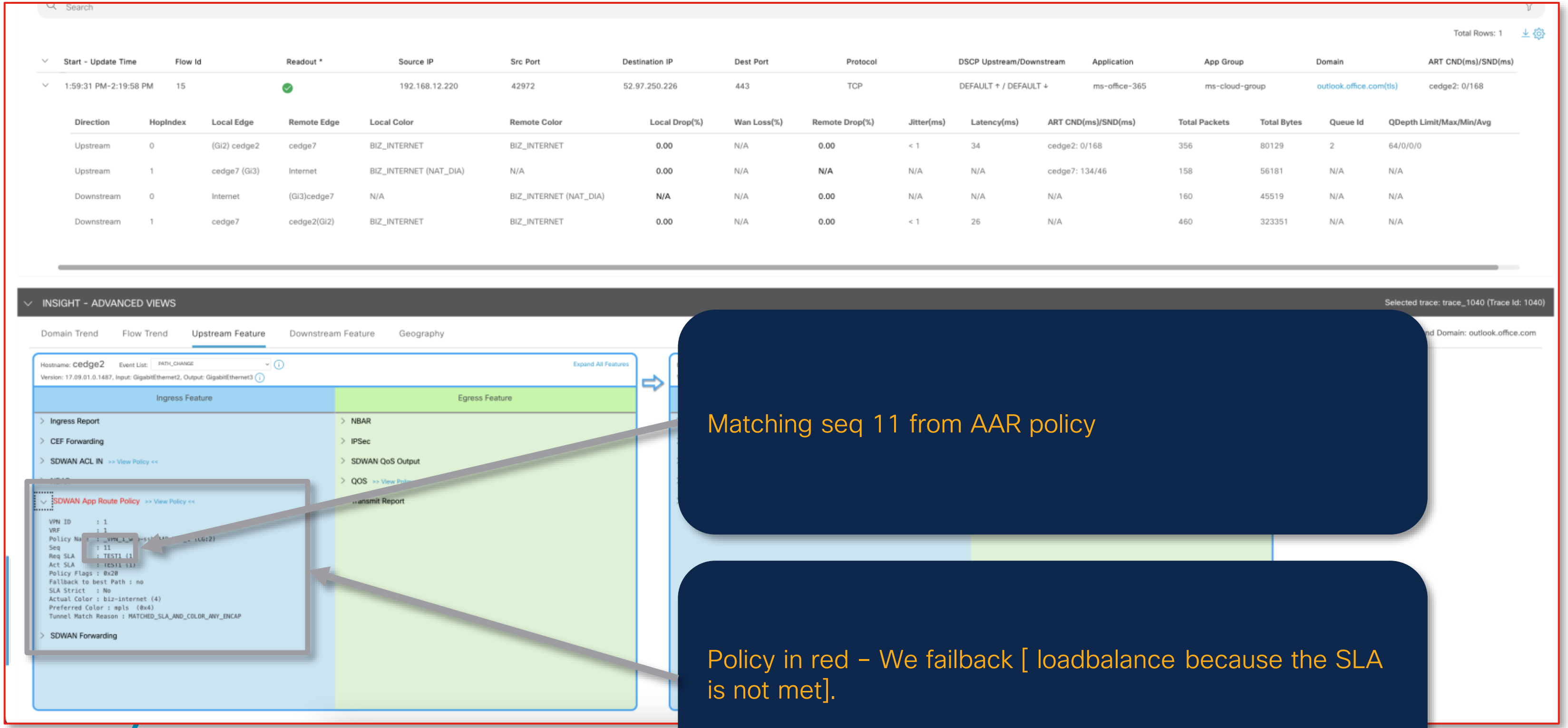
```
tc qdisc replace dev vnet183 root netem delay 20msec 2msec drop 0%
tc qdisc replace dev vnet207 root netem delay 20msec 2msec drop 0%
tc qdisc replace dev vnet212 root netem delay 20msec 2msec drop 0%
```

Run NWPI – everything seems normal

Increasing MPLS delay WAY above 100msec

```
tc qdisc replace dev vnet183 root netem delay 110msec 2msec drop 0%
tc qdisc replace dev vnet207 root netem delay 110msec 2msec drop 0%
tc qdisc replace dev vnet212 root netem delay 110msec 2msec drop 0%
```

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(tls)	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)

nd Domain: outlook.office.com

Hostname: cedge2 Event List: PATH_CHANGE

Version: 17.09.01.0.1487, Input: GigabitEthernet2, Output: GigabitEthernet3

Expand All Features

Ingress Feature	Egress Feature
Ingress Report	NBAR
CEF Forwarding	IPSec
SDWAN ACL IN >> View Policy <<	SDWAN QoS Output
NBAR	QOS >> View Poli
SDWAN App Route Policy >> View Policy <<	ransmit Report

```
VPN ID        : 1
VRF           : 1
Policy Na[illegible] : _VPN_1_w[illegible] (LG:2)
Seq           : 11
Req SLA       : TEST1 (1
Act SLA       : TEST1 (1)
Policy Flags : 0x20
Fallback to best Path : no
SLA Strict   : No
Actual Color : biz-internet (4)
Preferred Color : mpls  (0x4)
Tunnel Match Reason : MATCHED_SLA_AND_COLOR_ANY_ENCAP
```

SDWAN Forwarding

Matching seq 11 from AAR policy

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

NWPI over releases

17.4.1 (Phase I)

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

17.6.1 (Phase II)

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

17.9.1 (Phase III)

Enhancing Phase II
Monitoring over time

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”

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

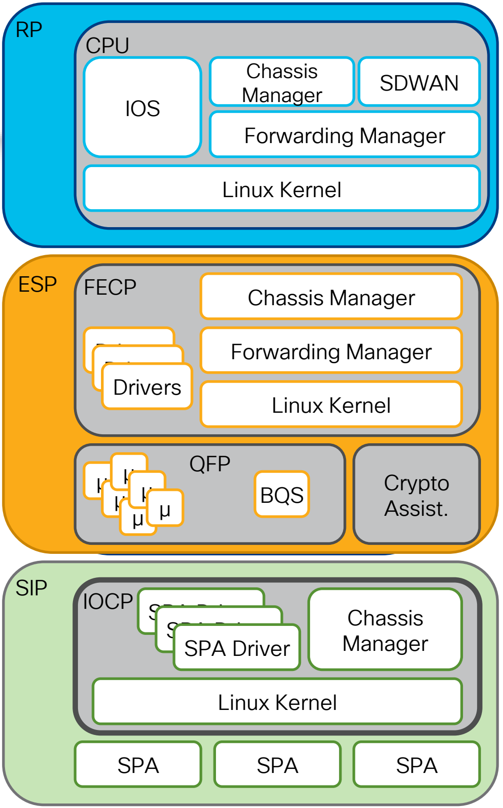
Thousand Eyes	NWPI
Probe based	Real^{TM} traffic traced
Network wide visibility based on agents /tests distributed on each sides	Network transitive condition applied initially on a single site ID
No packet processing visility	packet processing visibility

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

Resources: simplified view

```
cat8000v#show platform resources
**State Acronym: H - Healthy, W - Warning, C - Critical
Resource                 Usage                Max              Warning          Critical         State
----------------------------------------------------------------------------------------------------
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
```



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

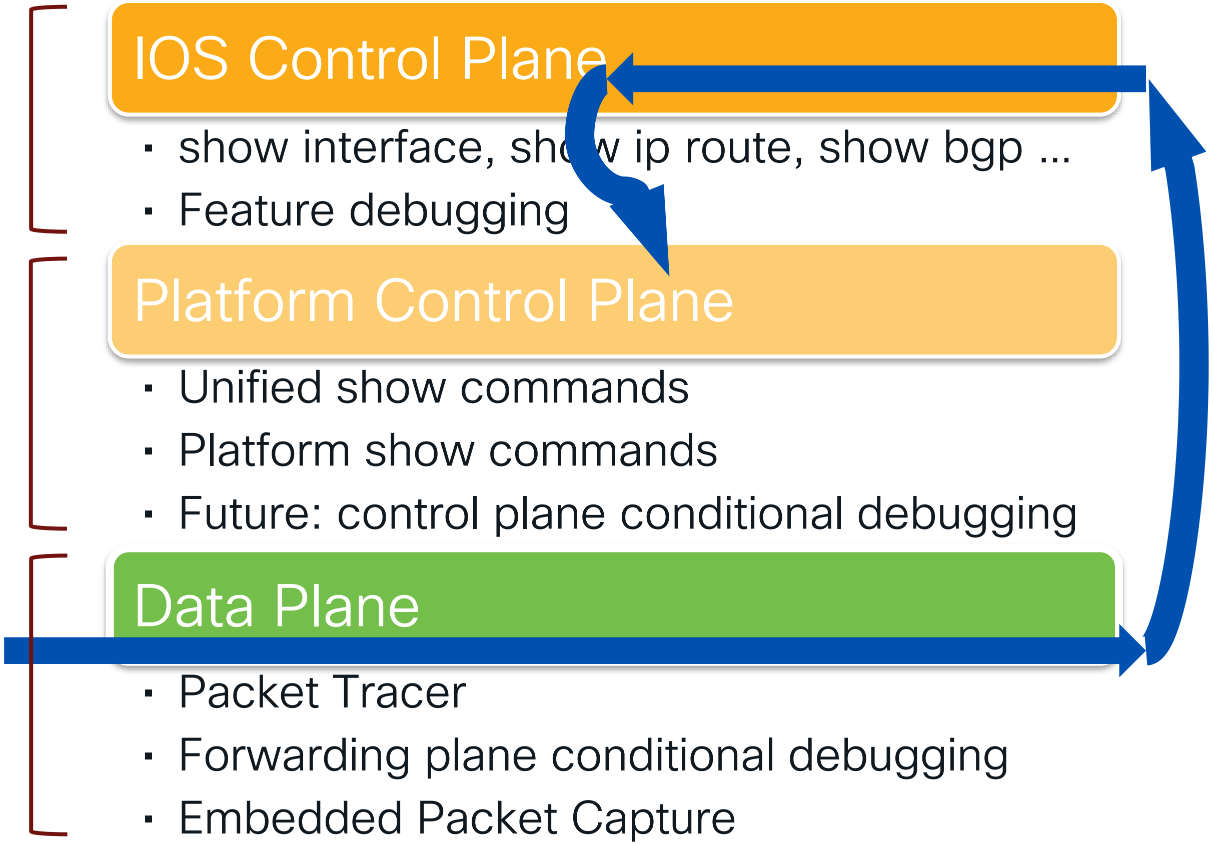
```
cedge2#show platform packet-trace fia-statistics
Feature                                     Count   Min(ns)    Max(ns)    Avg(ns)
---------------------------------------------------------------------------------
IPV4_OUTPUT_STILE_SDWAN_LAN_EXT                 1     11828      11828      11828
IPV4_INPUT_IPSEC_INLINE_PROCESS              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

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

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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

CISCO The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

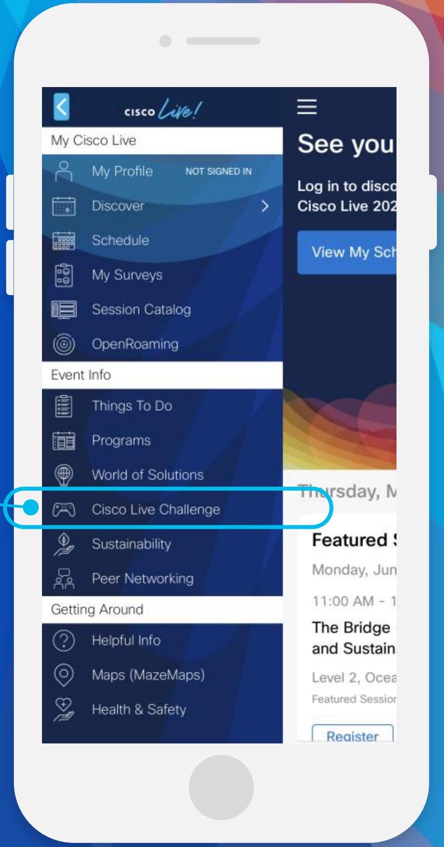
How:

1 Open the Cisco Events App.

2 Click on 'Cisco Live Challenge’ in the side menu.

3 Click on View Your Badges at the top.

4 Click the + at the bottom of the screen and scan the QR code:



cisco Live!

cisco Live!

Let's go

#CiscoLive