Cisco live!

What You Make Possible

BUILT FOR THE HUMAN NETWORK

CISCO

BRKARC-3445
Catalyst 4500E Deep Dive

Kedar Karmarkar CCIE# 6724

Technical Leader

Abstract

The Catalyst 4500E is the lead platform for Cisco's Campus Access with the latest Supervisor 7-E and its lighter cousin, the 7L-E. Take a close look at the ASIC and System Architecture, walk with the Unicast and Multicast packets as they traverse the system. Learn about Cisco UPOE technology and the eco-system that gets powered by it. Know more about Cisco Flexible NetFlow and Wireshark on IOS XE that enable application visibility from the access layer and help in capturing and viewing application packets on the switch itself. Pick up on how the 4500E hardware encrypts the traffic using Cisco MACSec. Gain insight into how Cisco Easy Virtual Network (EVN) on the 4500E helps you with Network Virtualization. Hear how the QoS capabilities on the 7-E and 7L-E help you prioritize and deliver voice, video and other critical traffic with minimum jitter and latency. Understand the High Availability features (SSO/NSF and ISSU) and other Hardware Redundancy components in the 4500E that help make the Access layer resilient than ever and lets you upgrade software with minimum downtime to traffic.

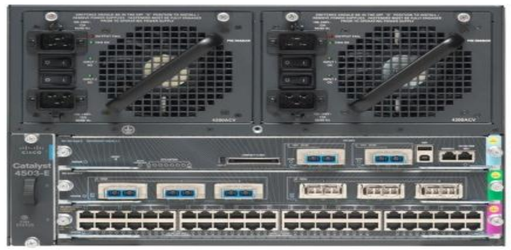
This session will cover the latest Supervisor 7-E and its lighter cousin, the 7L-E. The 6-E and 6L-E share a similar architecture like the 7-E minus the NetFlow ASIC. The session is for network designers and senior network operation engineers who have or are considering deploying Cisco Catalyst 4500 Series Switches in enterprise networks. At least a basic knowledge of routing protocols as well as traditional campus design is recommended.

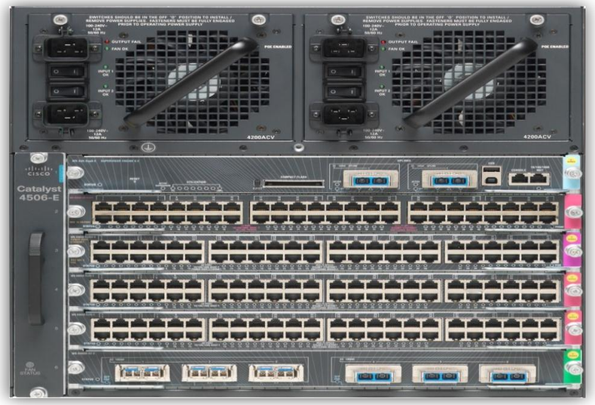
Agenda

- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and packet walk
- Quality of Service Overview
- Flexible NetFlow
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

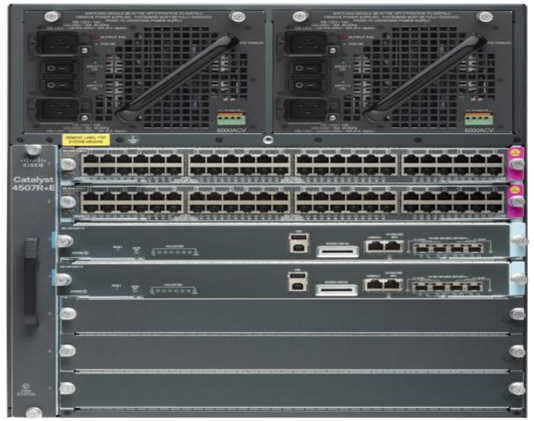
Catalyst 4500E Chassis

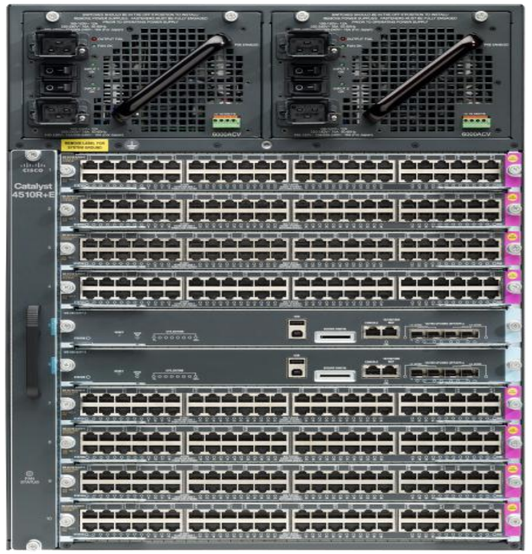
Catalyst 4500E Family





4503-E	4506-E
1 Supervisor	1 Supervisor
2 Line Cards	5 Line Cards
96 Ports of 10/100/1000	240 Ports of 10/100/1000
7 Rack Unit Height	10 Rack Unit Height
Supervisor 6LE, 6E, 7E and 7LE	
Dual Power Supplies	

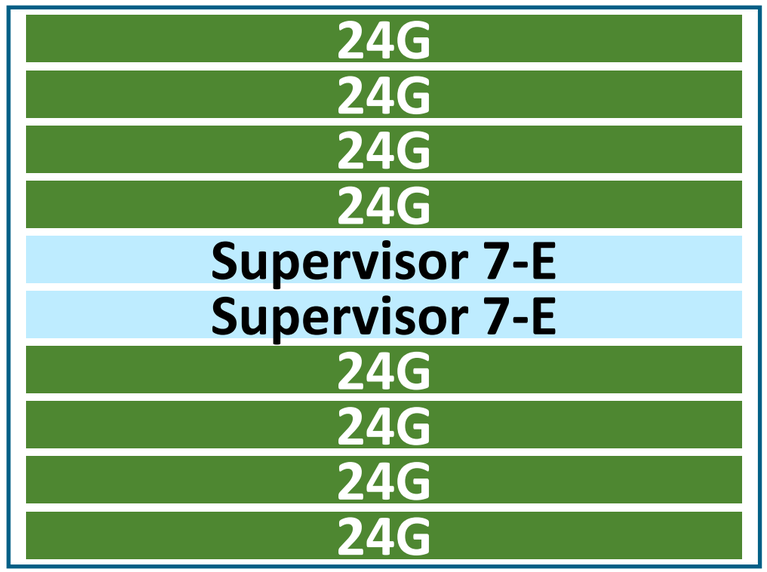




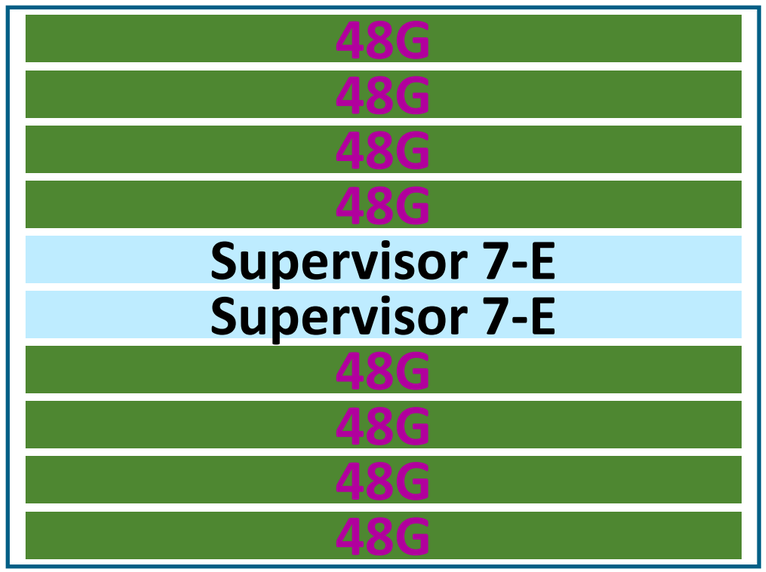
4507R+E	4510R+E
2 Supervisors	2 Supervisor
5 Line Cards	8 Line Cards
240 Ports of 10/100/1000	384 Ports of 10/100/1000
11 Rack Unit Height	14 Rack Unit Height
Supervisor 6LE, 6E, 7E and 7LE	Supervisor 6E, 7E
Dual Power Supplies	

Per Slot Bandwidth in 10 and 7 Slot Chassis

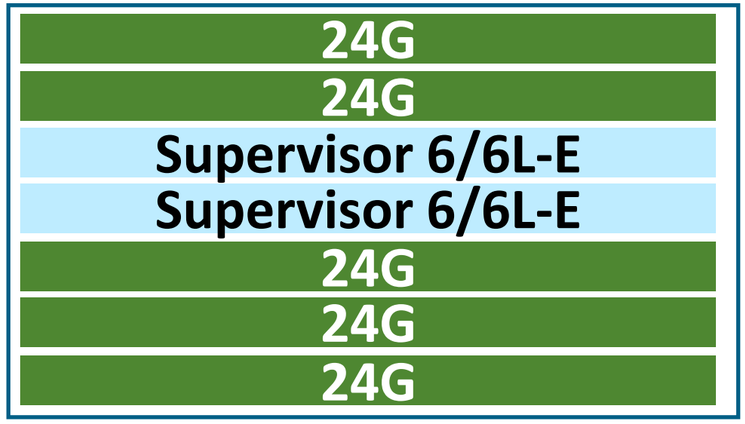
WS-C4510R-E



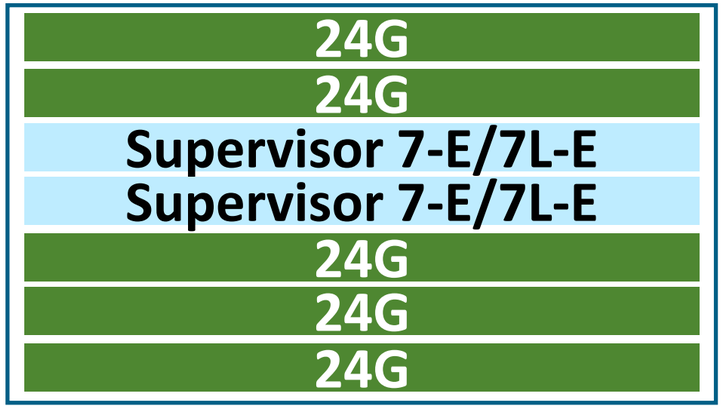
WS-C4510R-E



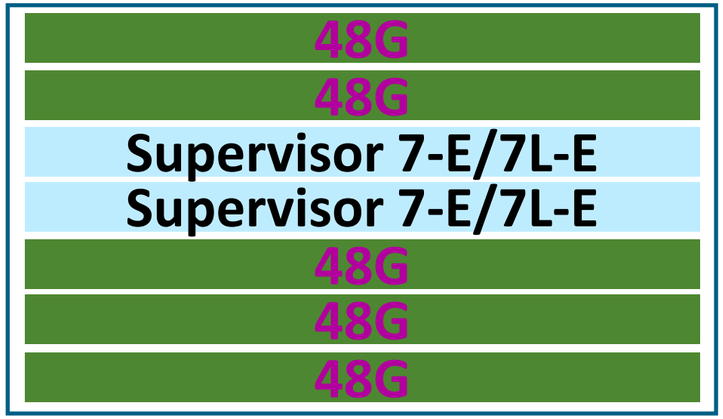
WS-C4510R+E



WS-C4507R-E



WS-C4507R-E



WS-C4507R+E

Catalyst 4500E Supervisors

Catalyst 4500E Supervisor 7-E

Hardware Elements

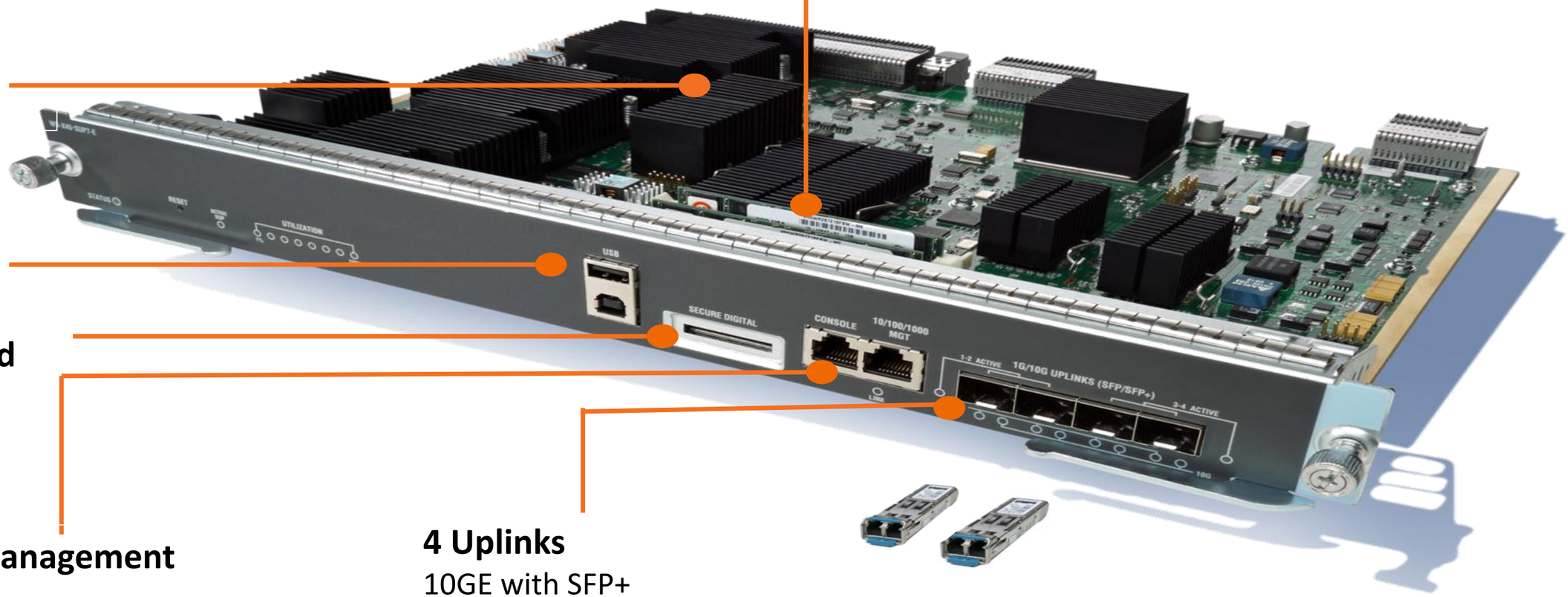
2G DRAM

Dual Core CPU

USB ports*

SD Memory Card

Console and Management Port

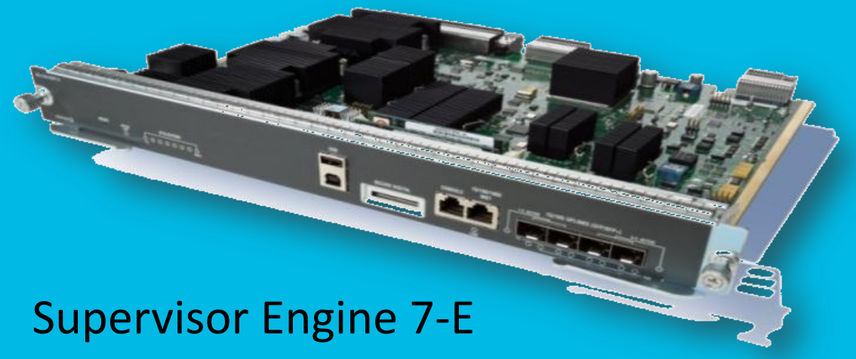


4 Uplinks
10GE with SFP+
1GE with SFP

**USB Type A is supported*
USB Type B is not supported

Catalyst 4500E Series Supervisors

Optimized for Large Enterprise Campus Deployments



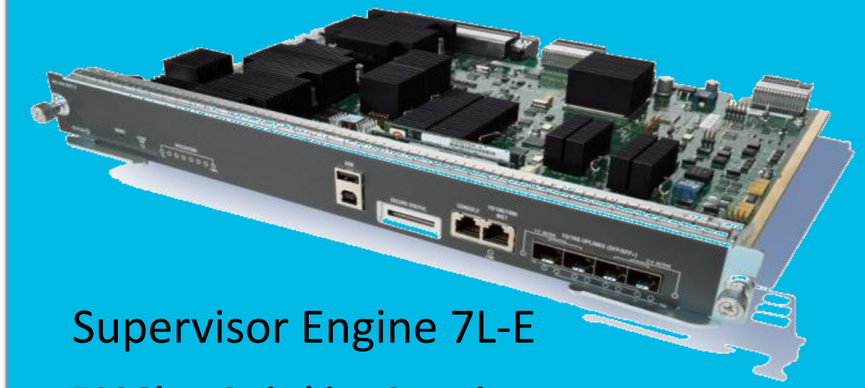
Supervisor Engine 7-E

848Gbps Switching Capacity

Scalability

- 4 x 10G Uplinks
- 384 10/100/1000 ports
- 3,6,7 and 10 slot chassis
- 96 10G LC Fiber ports
- 192 1G LC Fiber ports
- 256K Routes

Optimized for Small/Medium Sized Campus Deployments



Supervisor Engine 7L-E

520Gbps Switching Capacity

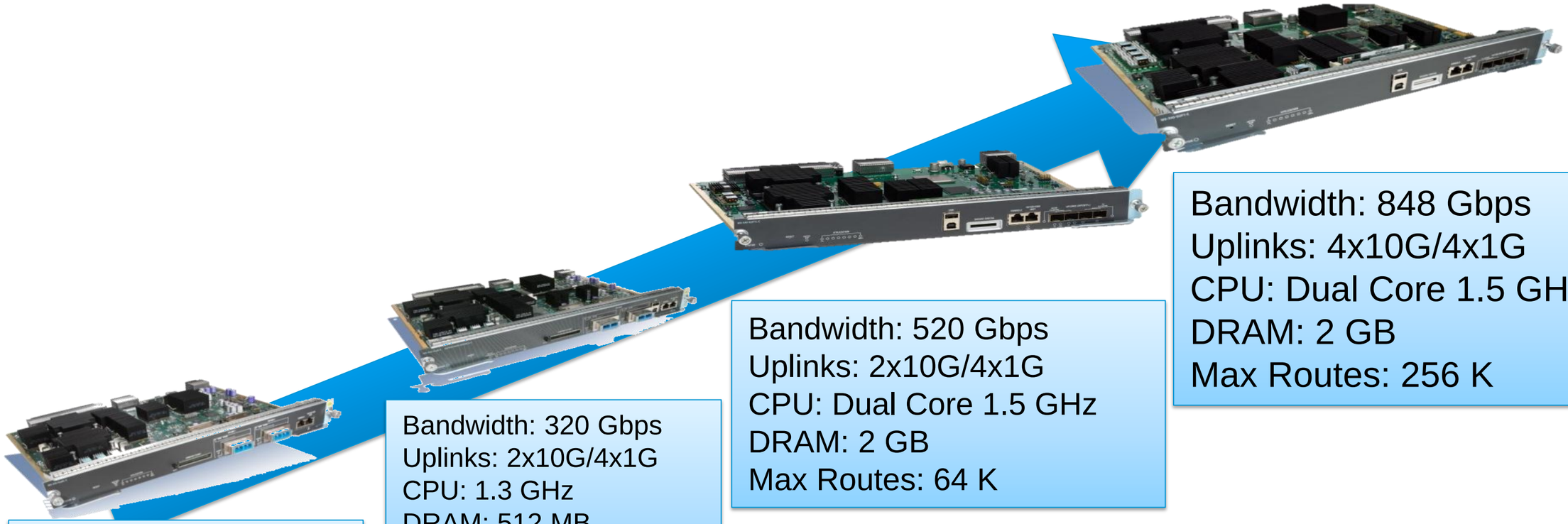
Scalability

- 2 x10G or 4 x 1G Uplinks
- 240 10/100/10000 ports
- 3,6 and 7 slot chassis
- 60 10G LC Fiber ports
- 120 1G LC Fiber ports
- 64K Routes

Platform Innovations

- 48G/slot
- Flexible NetFlow
- UPOE
- Hosted Applications
- VRF-Lite, EVN
- In Service Software Upgrade
- VSS*
- Cisco TrustSec (MACSec)
- Medianet

Catalyst 4500E Supervisor Comparison



Performance

Bandwidth: 280 Gbps
Uplinks: 2x10G/4x1G
CPU: 1 GHz
DRAM: 512 MB
Max Routes: 57K

Bandwidth: 320 Gbps
Uplinks: 2x10G/4x1G
CPU: 1.3 GHz
DRAM: 512 MB
Max Routes: 256 K

Bandwidth: 520 Gbps
Uplinks: 2x10G/4x1G
CPU: Dual Core 1.5 GHz
DRAM: 2 GB
Max Routes: 64 K

Bandwidth: 848 Gbps
Uplinks: 4x10G/4x1G
CPU: Dual Core 1.5 GHz
DRAM: 2 GB
Max Routes: 256 K

Supervisor 6L-E | **Supervisor 6-E** | **Supervisor 7L-E** | **Supervisor 7-E**

Catalyst 4500E Line Cards

Cisco Catalyst 4500E —10/100/1000 Line Cards

PoE Plus Linecards

WS-X4648-RJ45V+E

- E-Series (**24G/slot**) 48p 10/100/1000 RJ45
- 30W/ port (IEEE802.3at standard PoEP) on upto **24** ports
- Re-use existing chassis, power supplies
- PoE policing and monitoring
- EnergyWise
- Jumbo frame support

WS-X4748-UPOE+E

- E-Series (**48G/ slot**) 48p 10/100/1000 RJ45
- 30W/ port (IEEE802.3at standard PoE-P) on **48** ports
- **IEEE 802.1AE MACSec** on all ports
- **60W on 24 ports**, 1500W line card budget
- **Energy Efficient Ethernet (EEE) 802.3az**
- Jumbo frame support

Data

WS-X4648-RJ45-E

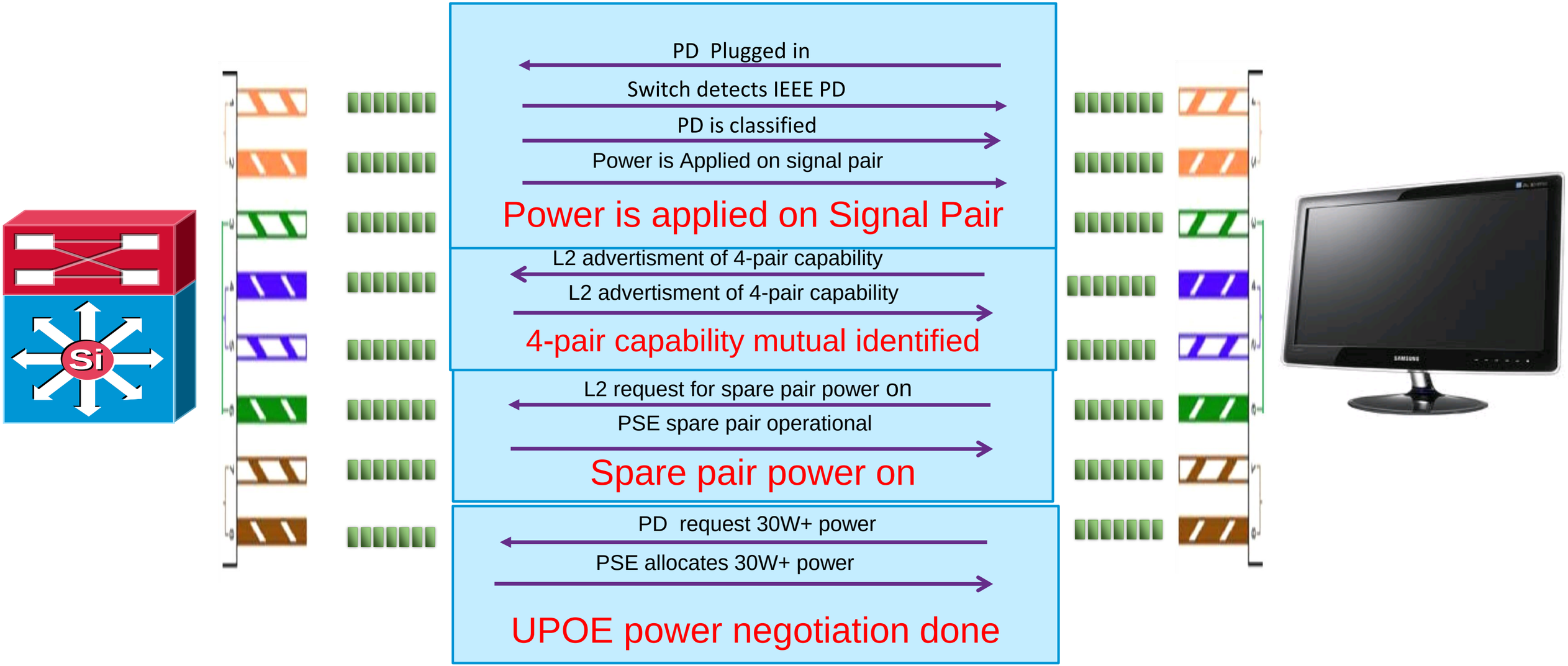
- E-Series (**24G/slot**) 48p 10/100/1000 RJ45
- E-series Supervisors only
- Jumbo frame support

WS-X4748-RJ45V-E

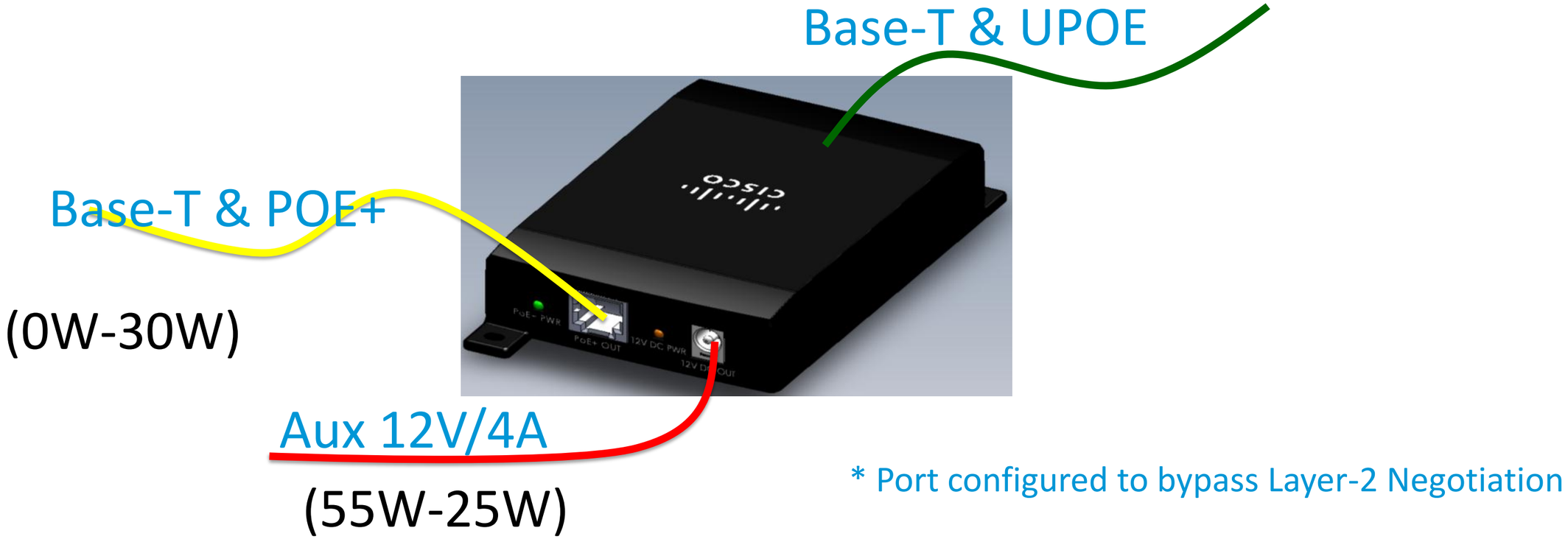
- E-Series (**48G/ slot**) 48p 10/100/1000 RJ45
- **Energy Efficient Ethernet (EEE) 802.3az**
- **IEEE 802.1AE MACSec** on all ports
- Jumbo Frame support

24G (E-Series) 48G (E-Series)

UPOE Power Negotiation



UPOE Splitter



* Port configured to bypass Layer-2 Negotiation

Why Splitter?	
▪ Market Enabler ▪ Power current devices	▪ 12V is prevalent Aux DC ▪ Power passive end points

Cisco UPOE Ecosystem

Announced July 2011

VIRTUAL DESKTOP

CISCO

SAMSUNG

FINANCIAL TRADING

BT

IP Trade

SPEAKERBUS

VIDEO

CISCO

HOSPITALITY, RETAIL

CISCO

Announced October 2011

FINANCIAL TRADING

IPC

BUILDING MANAGEMENT

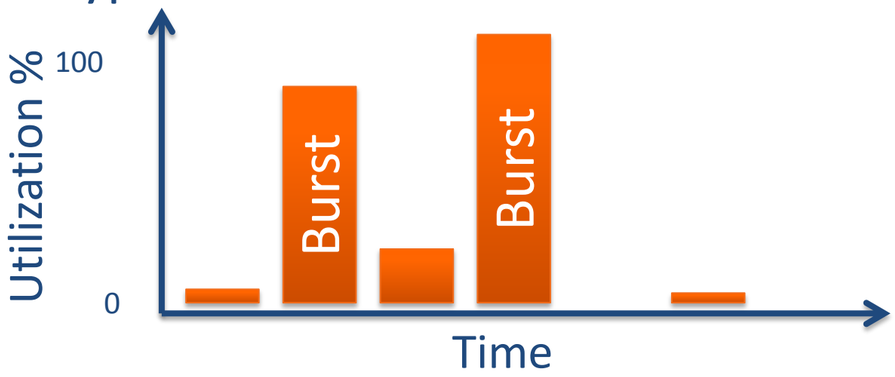
DEP LED Lighting
(Japan)

Deploy new applications with resilient network power on existing campus infrastructure

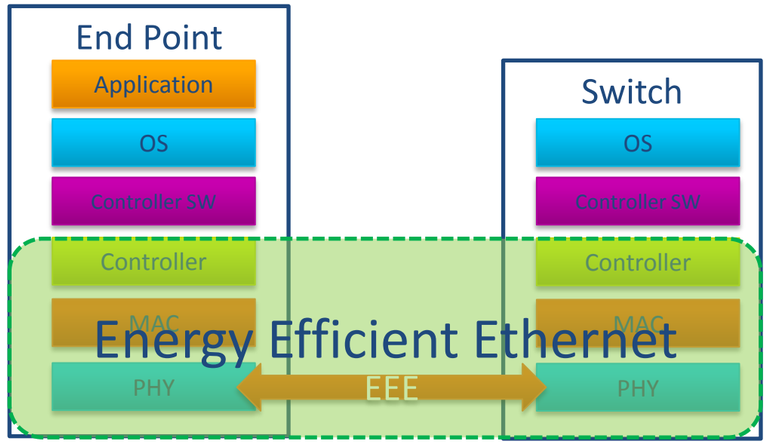
Energy Efficient Ethernet (EEE)

Energy Efficient Ethernet

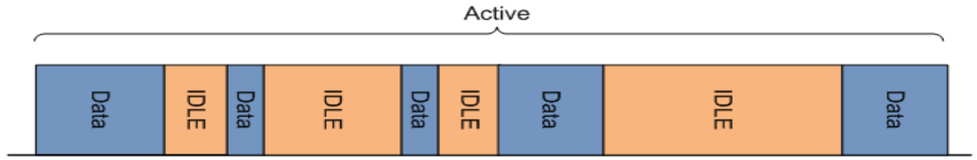
Typical Server Client Traffic Profile



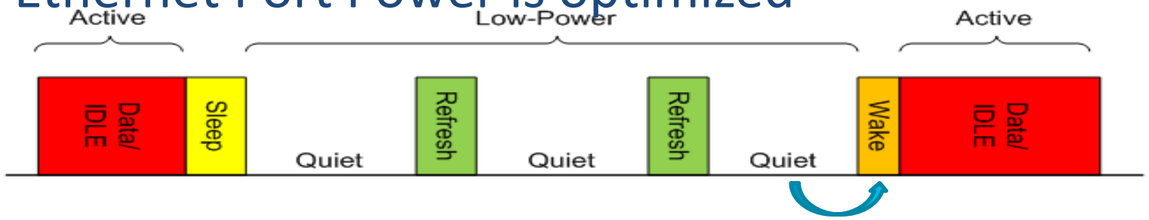
What does EEE do?



Ethernet Port is powered on all the time



Ethernet Port Power is optimized



Wake time: ~16us

intel

BROADCOM

1 Gbps Port Power Consumption

No EEE	EEE
1.0 W	0.47W

50% Power Savings

Energy Efficient Ethernet

Determine EEE Capability

```
4510_Sup7E#show interface gi 1/2 capabilities
GigabitEthernet1/2
  Model:                    WS-X4748-UPOE+E
  Type:                     10/100/1000-TX
  Speed:                    10,100,1000,auto
  Duplex:                   half,full,auto
  Auto-MDIX:                yes
  EEE:                      yes ( 100-Tx and 1000-T auto mode )

..<SNIP>..
```

Configure EEE

```
4510_Sup7E#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
4510_Sup7E(config)#int gi 1/2
4510_Sup7E(config-if)#power efficient-ethernet auto
```

Verify EEE

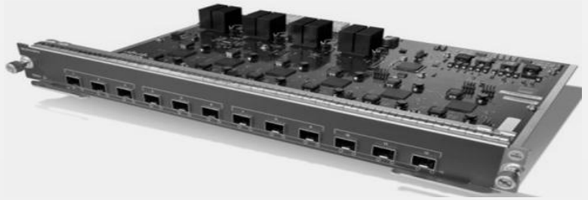
```
4510_Sup7E#show platform software interface gi 1/2 status
Switch Phyport Gi1/2 Software Status
EEE: Operational
```

Cisco Catalyst 4500E —Fiber 1G/10G Line Cards

Density

WS-X4624-SFP-E

- 24 ports 1:1 GE
- SX, LX GE SFP optics



WS-X4712-SFP+E

- 12 ports 2.5: 1, 10GE
- Mix and match 10G/ 1GE with SFP+
- **IEEE 802.1AE MacSec** on all ports
- GLC-T, LR, ER, SR, CX1 and LRM SFP+ Optics

Density

WS-X4612-SFP-E

- 12 ports, 1:1 GE SFP
- SX, LX GE SFP optics

WS-X4606-X2-E

- 6 ports, 2.5:1 10G
- Mix and match 10G/1GE with X2 (Twin-gig)
- LR, ER, SR, LX4 and LRM X2 optics

GE Fiber

10G Fiber

Catalyst 4500E Power Supplies

Catalyst 4500E 4200 W Power Supply

For Your Reference

Voltage	Inputs	Redundancy Mode	Max PoE (15W) Devices	Max PoEP (30W) Devices	Max UPOE (60W) Devices
110 V	Single	Redundant	54	27	13
		Combined	98	50	25
	Dual	Redundant	109	56	28
		Combined	198	102	51
220 V	Single	Redundant	109	56	28
		Combined	198	102	51
	Dual	Redundant	218	112	56
		Combined	384	204	90

Catalyst 4500E 6000 W Power Supply

For Your Reference

Voltage	Inputs	Redundancy Mode	Max PoE (15W) Devices	Max PoEP (30W) Devices	Max UPOE (60W) Devices
110 V	Single	Redundant	54	27	13
		Combined	98	50	25
	Dual	Redundant	109	56	28
		Combined	198	102	50
220 V	Single	Redundant	141	72	36
		Combined	257	132	65
	Dual	Redundant	283	145	70
		Combined	384	262	120

Cisco Power Calculator

http://tools.cisco.com/cpc

Combined PWR-C45-6000W with Single 220V inputs on each power supply	Data: 33.96% PoE: 62.34%	Data: 2641.76 PoE: 1641.80	Data: 333.33 PoE: 83.85	Data: 113.19 PoE: 52.27	Data: 220.15 PoE: 31.57
Combined PWR-C45-6000W with three 220V inputs	Data: 33.96% PoE: 41.18%	Data: 2641.76 PoE: 3881.80	Data: 333.33 PoE: 126.92	Data: 113.19 PoE: 52.27	Data: 220.15 PoE: 74.65
PWR-C45-1400DC-P	Data: 99.87% PoE: 37.65%	Data: 1.76 PoE: 4501.80	Data: 113.33 PoE: 138.85	Data: 113.19 PoE: 52.27	Data: 0.15 PoE: 86.57

[Top]

Configuration Details

Slot	Line Card	Output Current (A)	Output Power (W)	Typical Power Used (W)	Heat Dissipation (BTU/Hr)
Chassis	WS-C4510R+E	16.67	200.00	160.00	865.53
1	WS-X4748-RJ45V+E	6.24	74.88	59.90	300.84
2	WS-X4748-RJ45V+E	6.24	74.88	59.90	300.84
3	WS-X4748-RJ45V+E	6.24	74.88	59.90	300.84
4	WS-X4748-RJ45V+E	6.24	74.88	59.90	300.84
5	WS-X45-SUP7-E	23.30	279.60	223.68	1123.33
6	WS-X45-SUP7-E	23.30	279.60	223.68	1123.33
7	WS-X4748-RJ45V+E	6.24	74.88	59.90	300.84
8	WS-X4748-RJ45V+E	6.24	74.88	59.90	300.84
9	WS-X4748-RJ45V+E	6.24	74.88	59.90	300.84
10	WS-X4748-RJ45V+E	6.24	74.88	59.90	300.84
	Sub Total	113.19	1358.24	1086.59	5456.93
PoE Device	Quantity	Output Current (A)	Output Power (W)	Typical Power Used (W)	Heat Dissipation (BTU/Hr)
CP-7960G (6.3W)	384	52.27	2718.20	2174.56	4115.31
		Output Current (A)	Output Power (W)	Typical Power Used (W)	Heat Dissipation (BTU/Hr)
	Total	**165.46**	**4076.44**	**3261.15**	**9572.24**

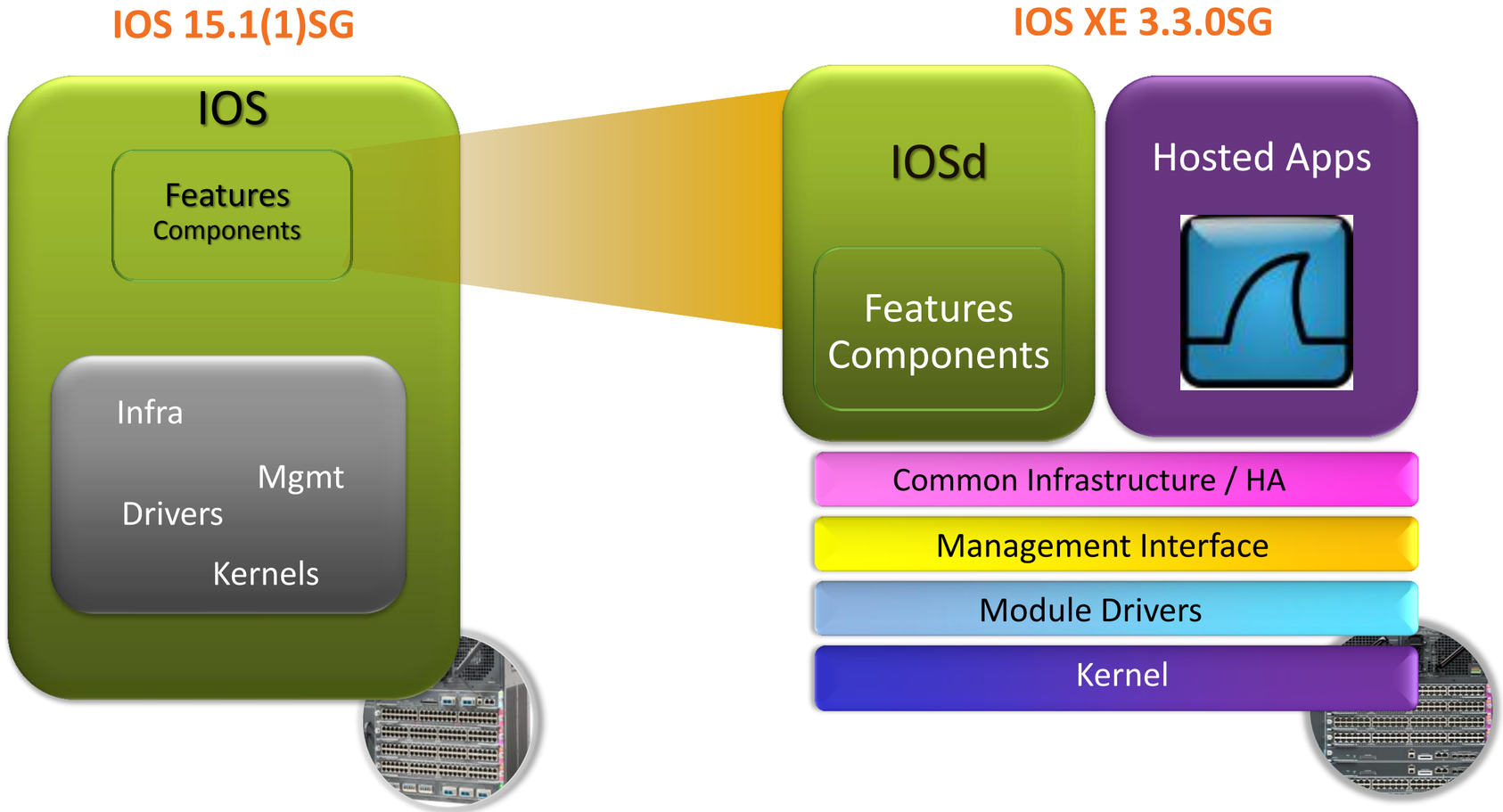
Agenda

- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and packet walk
- Flexible NetFlow
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

IOS XE Architecture

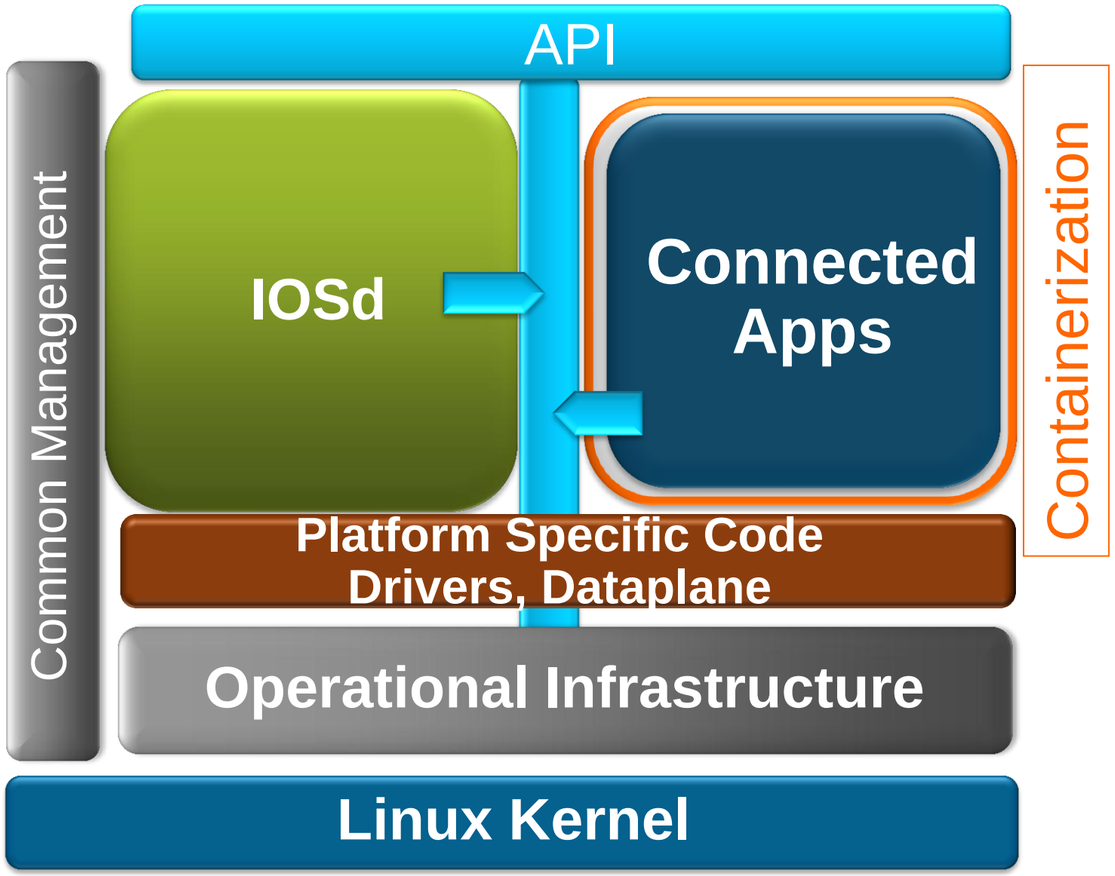
IOS-XE

- Modern IOS to enable multi-core CPU
- Easy customer migration
- while maintaining IOS functionality and look and feel
- Allow hosted applications like Wireshark



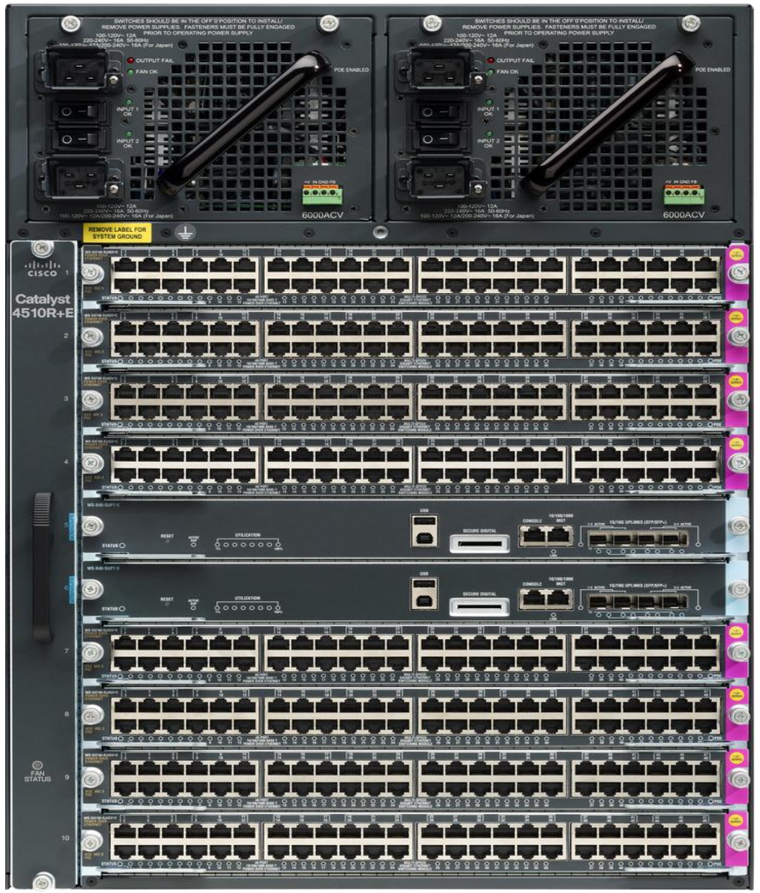
IOS XE Architecture

- Complete separation of control and data plane
- Service Integration through solid API framework
- Vastly improved resiliency between applications and IOSd



Learn more about IOS XE in BRKARC-2007 - IOS Strategy and Evolution

Why Wireshark on the SUP7-E?

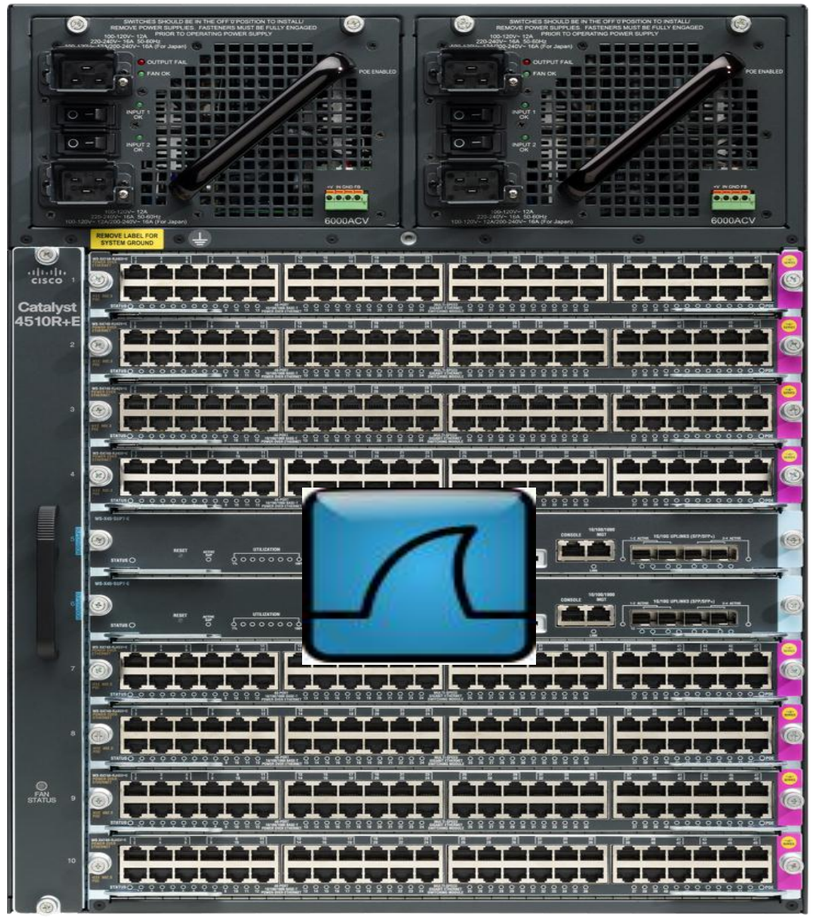


- SPAN/RSPAN
  - Packet Forward capability
  - No local display
  - Need external PC/sniffer to store and decode

Sits in between “debug ip packet” and SPAN/RSPAN

- Wireshark
  - Freeware
  - Supports wide variety of protocols
  - Bundled with switch Operating System
  - Onboard Capture and decode tool
  - Quick Analysis

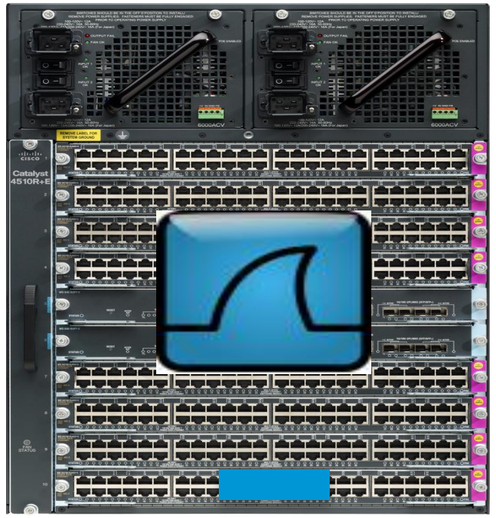
Wireshark Capabilities



- IOS XE on SUP7-E can host third-party apps
- Wireshark is a POSIX process in software
- Capture filters
- Display filters
- Store packets in PCAP file that user can manually TFTP/SSH to remote server.
- Support for up to 8 active capture points

How is it done?

Local Display



Store PCAP on Remote Server

- Original packets are hardware-switched to destination
- Copies of the interesting traffic are generated in hardware
- Processed by software at a rate-limited Packet per second, to protect CPU utilization
- The software interacts with the Wireshark module and writes the PCAP Files

Wireshark Configuration Examples

- Simple Capture and Display

```
Switch# monitor capture point mycapture interface g1/1 filter ip protocol tcp src
10.1.1.1 0.0.0.0 dest-port 80

Switch# monitor capture point mycapture start display brief
```

- Delete the Capture point

```
Switch# no monitor capture point mycapture
```

- Simple Capture and Store

```
Switch# monitor capture point mycapture interface g1/1 filter ip protocol tcp src
10.1.1.1 0.0.0.0 dest-port 80 associate file bootflash:mycapture.pcap

Switch# monitor capture point mycapture start

Switch# monitor capture point mycapture stop

Switch# show monitor capture file bootflash:mycapture.pcap
```

- Display packets from a .pcap file with a display filter

```
Switch# show monitor capture file bootflash:mycapture.pcap display-filter “net
10.1.1.0 0.0.0.255 and port 80”
```

Wireshark Buffer Capture

- Allows to capture packets and store them in a buffer:

```
monitor capture point mycap associate file location buffer
```

- Buffers can be cleared:

```
monitor capture point mycap clear
```

- Buffers can be paused:

```
monitor capture point mycap pause
monitor capture point mycap continue
```

- Buffer can be displayed:

```
show monitor capture buffer mycap brief
show monitor capture buffer mycap detailed
show monitor capture buffer mycap dump
```

- Buffer can be stored in a pcap file:

```
monitor capture point mycap store location filename
```

Sample Packet Capture displays

- Display packets in brief mode

Switch# show monitor capture file bootflash:mycapture.pcap

```
1   0.000000   192.85.1.3 -> 192.85.1.4   UDP Source port: 1024  Destination port: 28960
2   0.000000   192.85.1.3 -> 192.85.1.4   UDP Source port: 1024  Destination port: 28960
3   0.000000   192.85.1.3 -> 192.85.1.4   UDP Source port: 1024  Destination port: 28960
4   0.000000   192.85.1.3 -> 192.85.1.4   UDP Source port: 1024  Destination port: 28960
```

- Display packets in hexadecimal mode

Switch# show monitor capture file bootflash:mycapture.pcap dump

```
0000  00 00 94 00 00 04 00 00 94 00 00 03 08 00 45 c0   ..............E.
0010  05 1e 0f 28 00 00 ff 11 24 35 c0 55 01 03 c0 55   ...(....$5.U...U
0020  01 04 04 00 71 20 05 0a db 21 00 00 00 00 00 00   ....q ...!......
```

Sample Packet Capture Displays

- Display packets in detailed mode

Switch# show monitor capture file bootflash:mycapture.pcap detailed

```
Frame 1: 1328 bytes on wire (10624 bits), 1328 bytes captured (10624 bits)
    Arrival Time: Jan  1, 1970 00:00:00.000000000 Universal
    Epoch Time: 0.000000000 seconds
   <snip….snip>
    Frame Number: 1
    Frame Length: 1328 bytes (10624 bits)
    Capture Length: 1328 bytes (10624 bits)
  <snip….snip>
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:94:00:00:03 (00:00:94:00:00:03), Dst: 00:00:94:00:00:04 (00:00:94:00:00:04)
    Destination: 00:00:94:00:00:04 (00:00:94:00:00:04)
        Address: 00:00:94:00:00:04 (00:00:94:00:00:04)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:00:94:00:00:03 (00:00:94:00:00:03)
        Address: 00:00:94:00:00:03 (00:00:94:00:00:03)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
    Frame check sequence: 0x99c15111 [incorrect, should be 0x379d10df]
Internet Protocol, Src: 192.85.1.3 (192.85.1.3), Dst: 192.85.1.4 (192.85.1.4)
```

Just as it appears in the GUI with all fields collapsed

Sample Packet Capture Displays

```
Internet Protocol, Src: 192.85.1.3 (192.85.1.3), Dst: 192.85.1.4 (192.85.1.4)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
        1100 00.. = Differentiated Services Codepoint: Class Selector 6 (0x30)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1310
    Identification: 0x0f28 (3880)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x2435 [correct]
        [Good: True]
        [Bad: False]
    Source: 192.85.1.3 (192.85.1.3)
    Destination: 192.85.1.4 (192.85.1.4)
User Datagram Protocol, Src Port: 1024 (1024), Dst Port: 28960 (28960)
    Source port: 1024 (1024)
    Destination port: 28960 (28960)
    Length: 1290
    Checksum: 0xdb21 [validation disabled]
<snip…….snip>
```

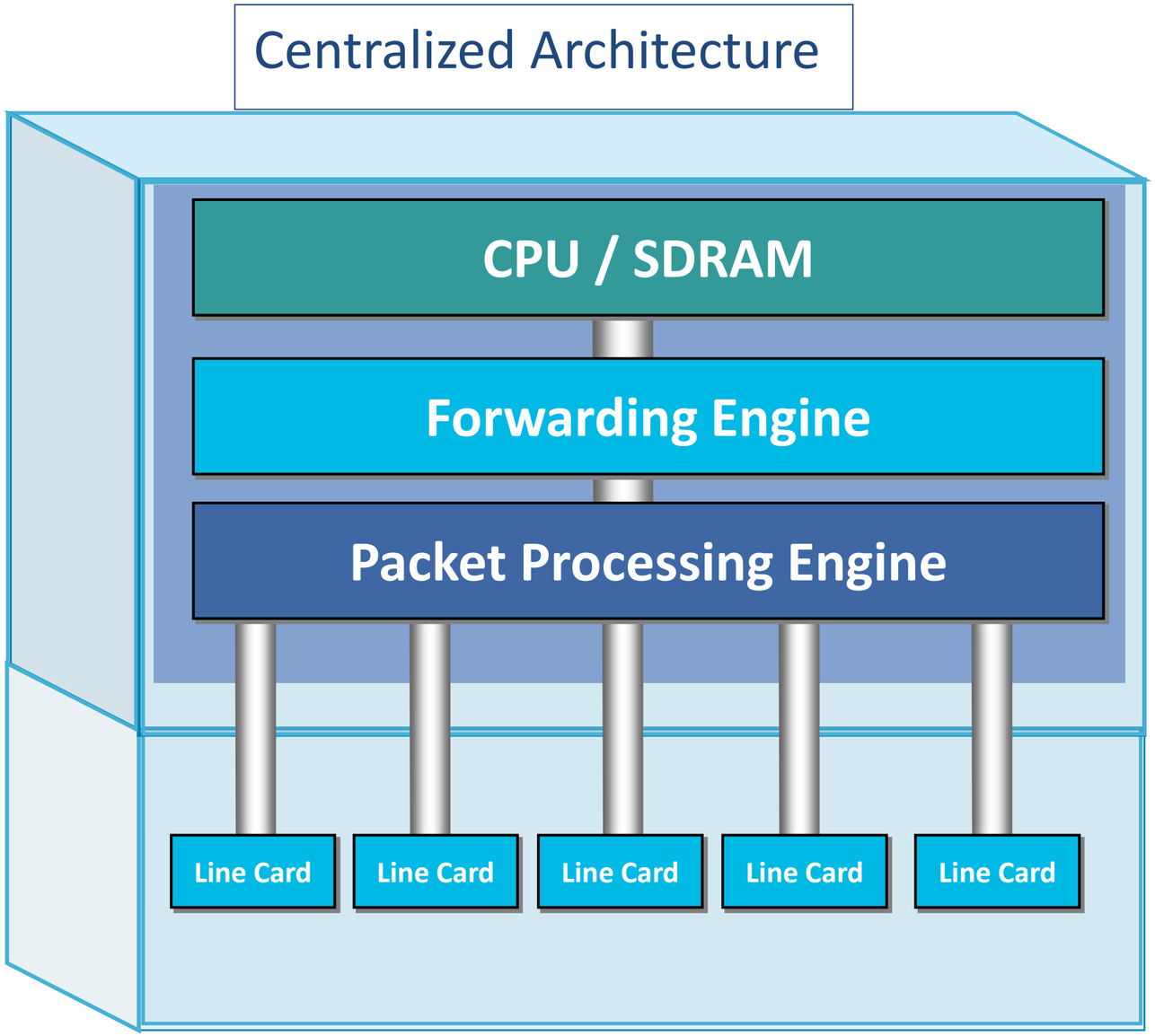
IP Protocol Stack Information

Layer 4 Information

Agenda

- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and Packet walk
- Quality of Service Overview
- Flexible NetFlow
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

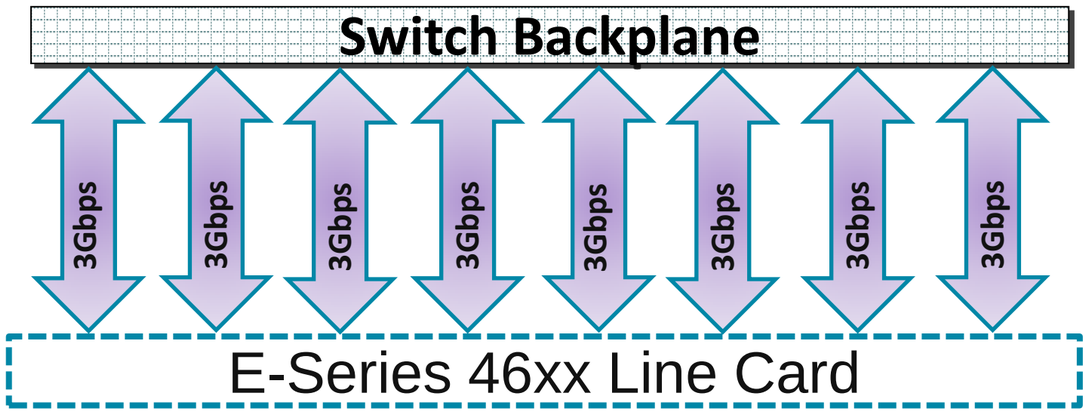
Catalyst 4500E Architecture



- Shared memory switch
  Passive Backplane
- All forwarding, queuing, security is implemented on the Supervisor
- The individual line cards are considered to be ‘transparent’ and contain “stub” ASICs and the PHYs
- Upgrade advantages
- Each 47XX-Series line card has 48 Gbps full- duplex connections to the central forwarding engine
- IOS XE that can leverage multi-core CPU, and ability to host applications separately outside IOS context

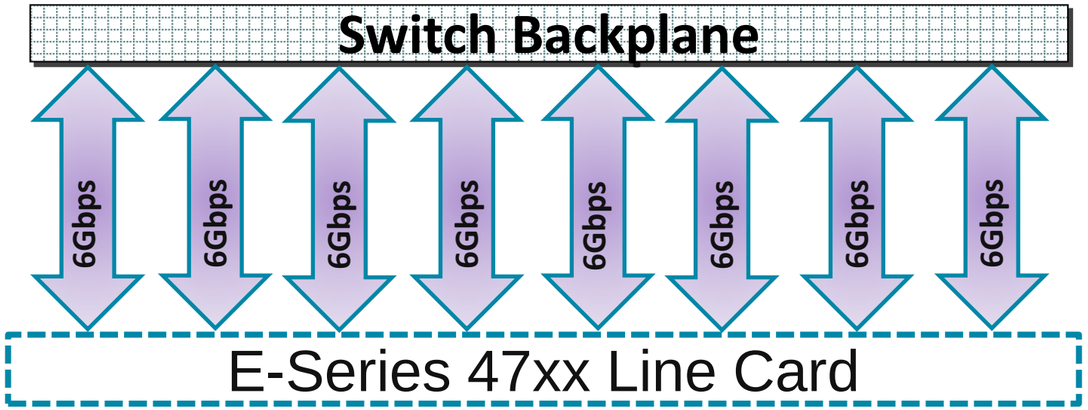
Catalyst 4500E Line Card Architecture

46xx and 47xx Line Card Backplane Speeds



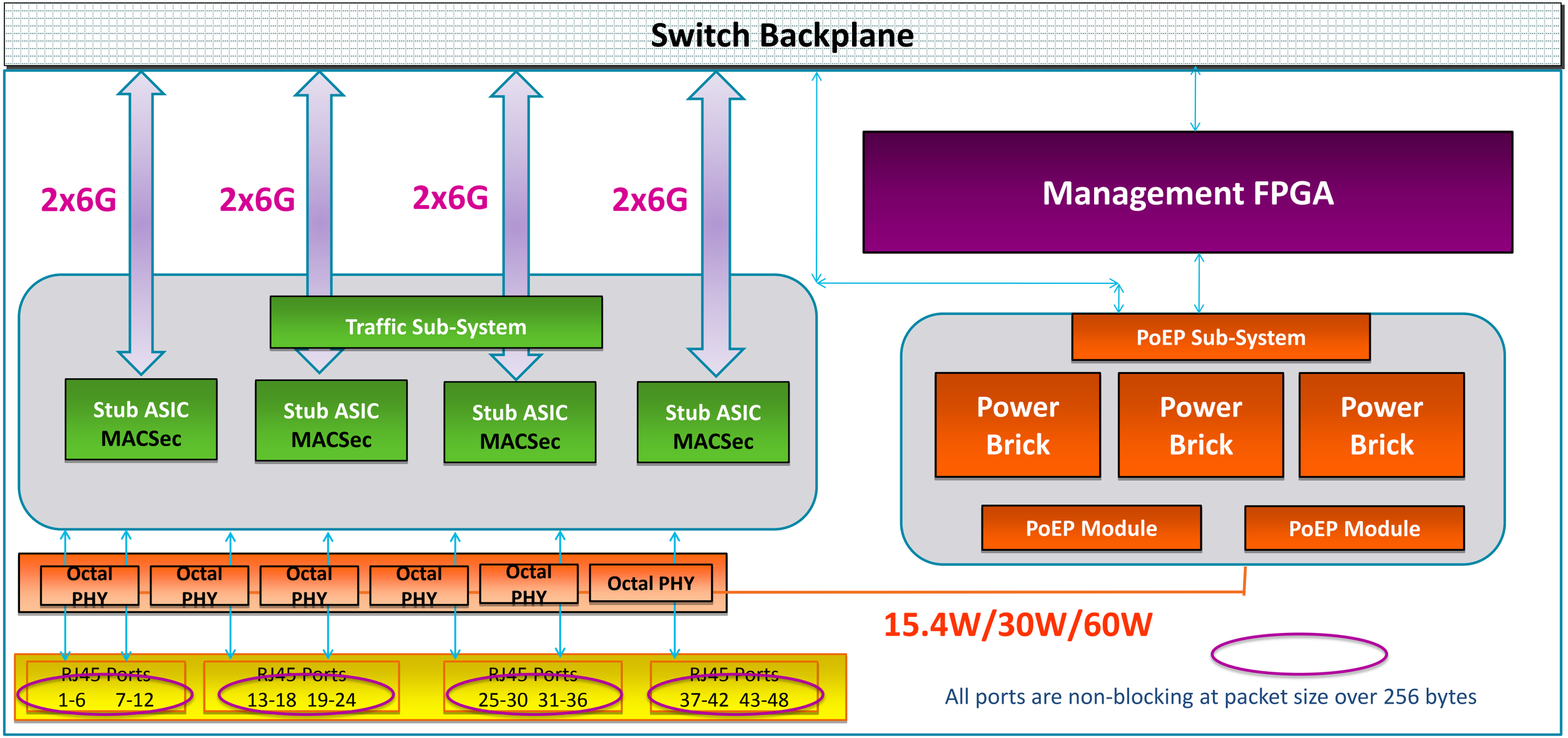
E-Series Chassis–Bandwidth per Slot with 46XX series line card:

- 8 dedicated lanes to Supervisor
- Each lane operates at 3Gbps

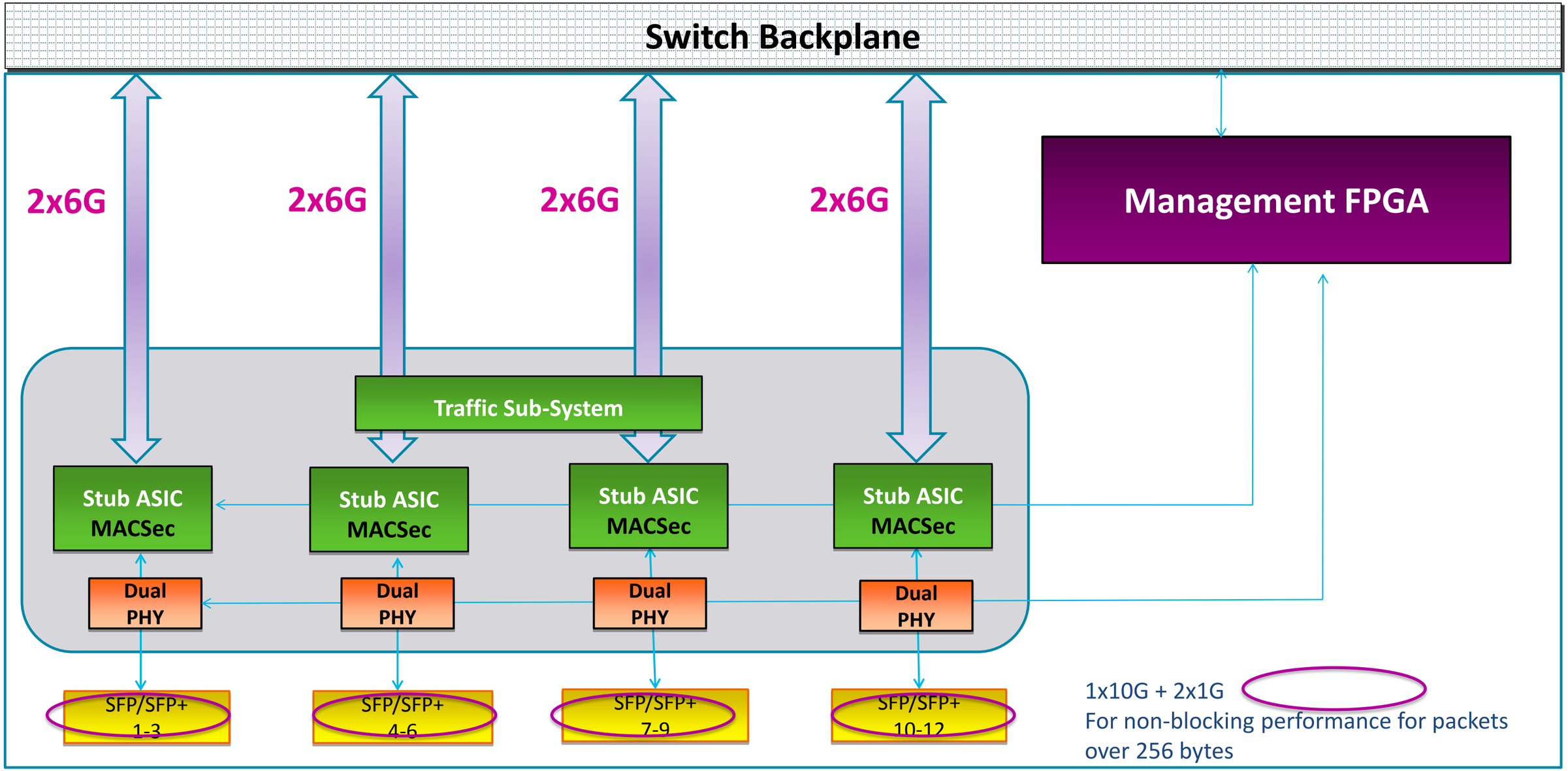


- E-Series Chassis–Bandwidth per Slot with 47xx series line cards
- 8 dedicated lanes to Supervisor
- Each lane runs at 6Gbps

WS-4748-UPOE+E Block Diagram

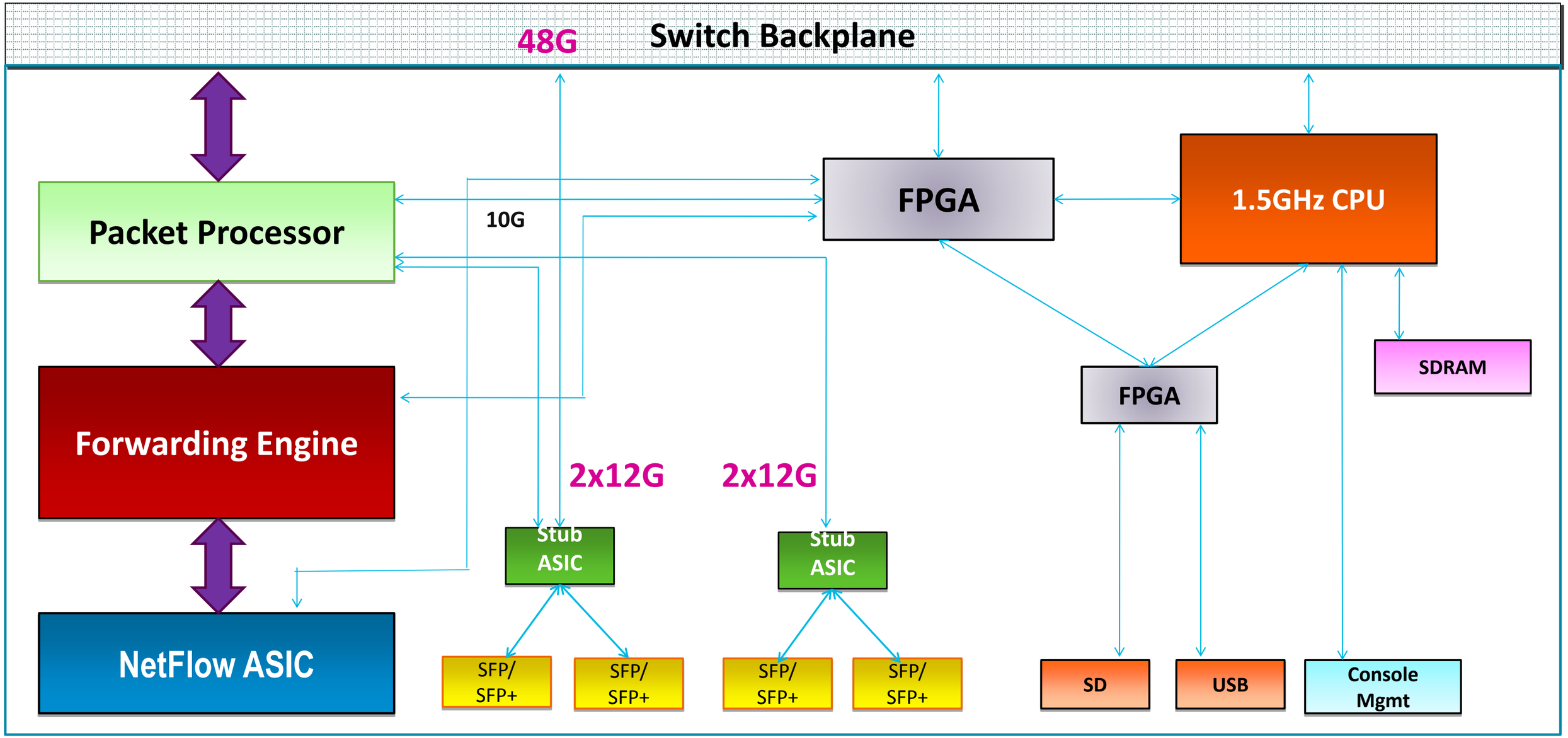


WS-X4712-SFP+E Block Diagram

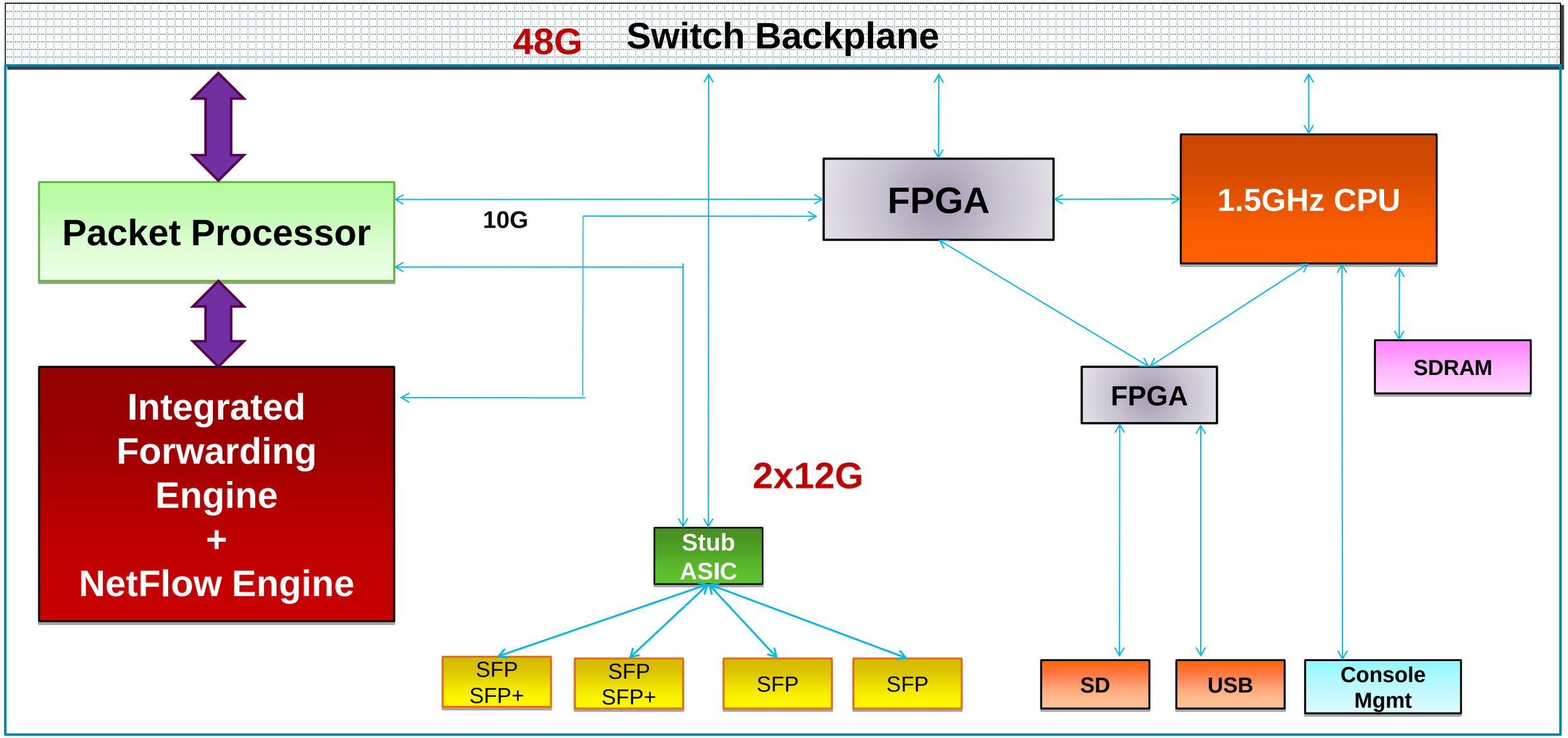


Catalyst 4500E Supervisor Architecture

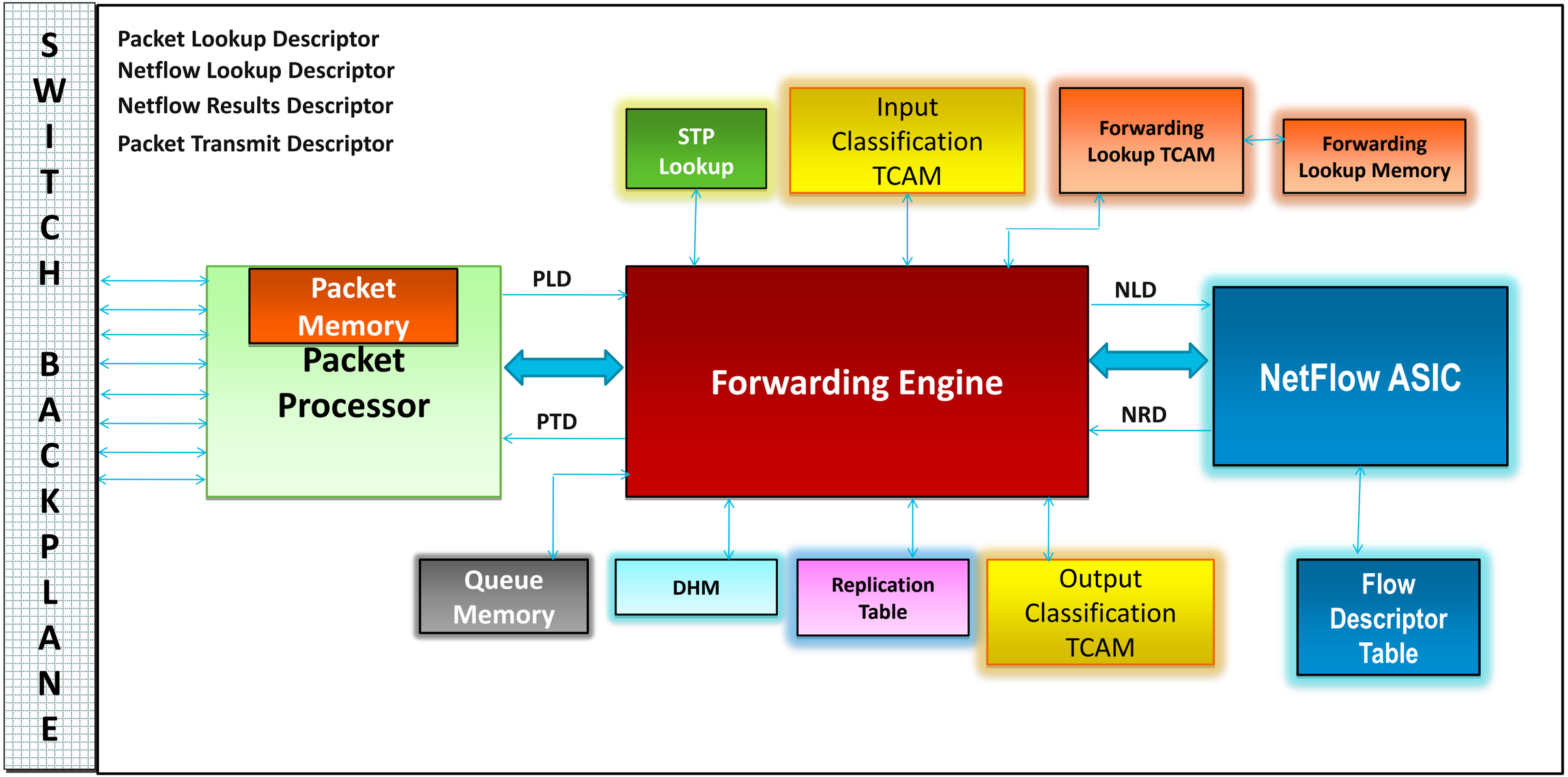
WS-X45-SUP7-E Block Diagram



Catalyst 4500E Supervisor 7L-E Block Diagram

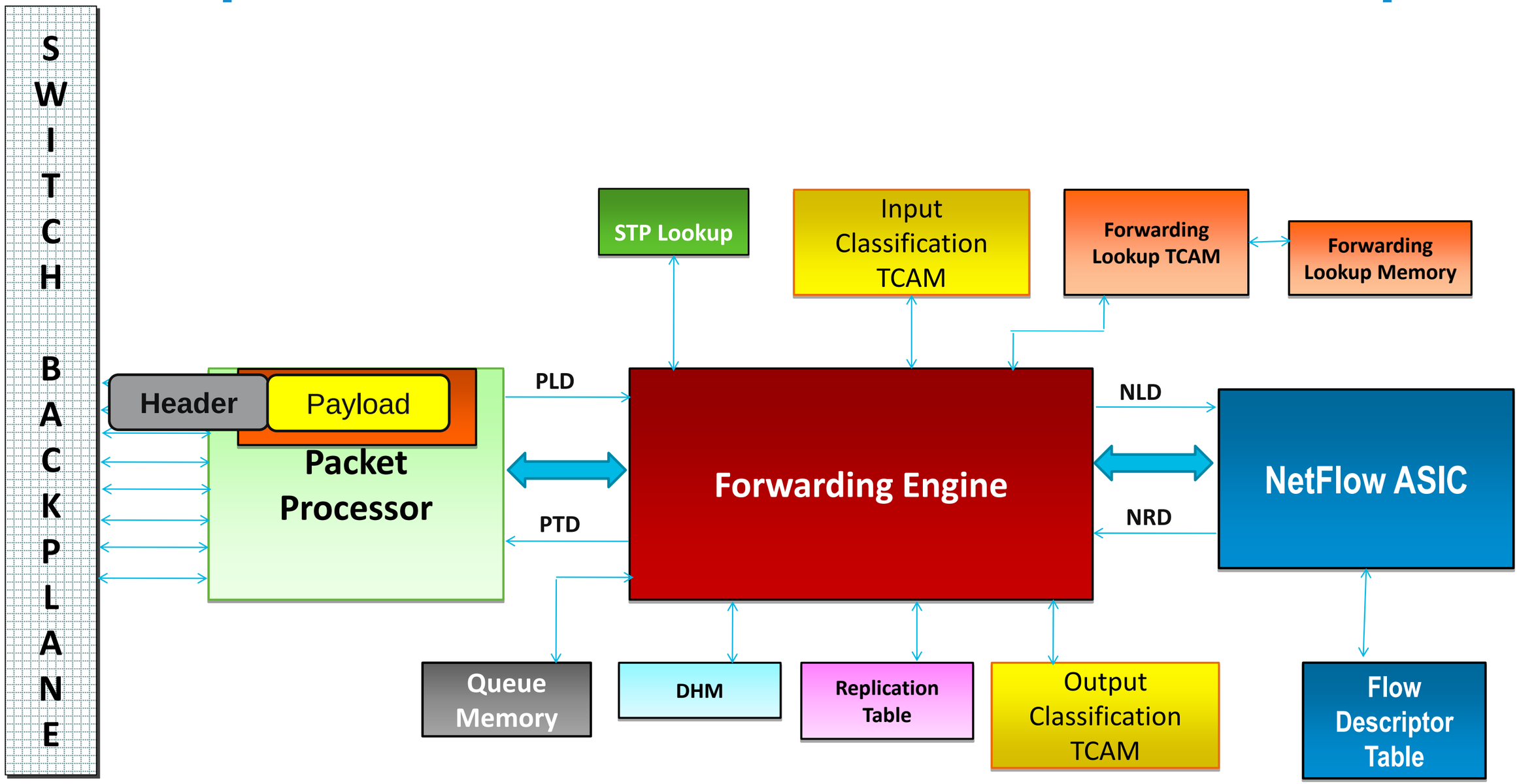


Supervisor 7-E Forwarding Engine Blocks

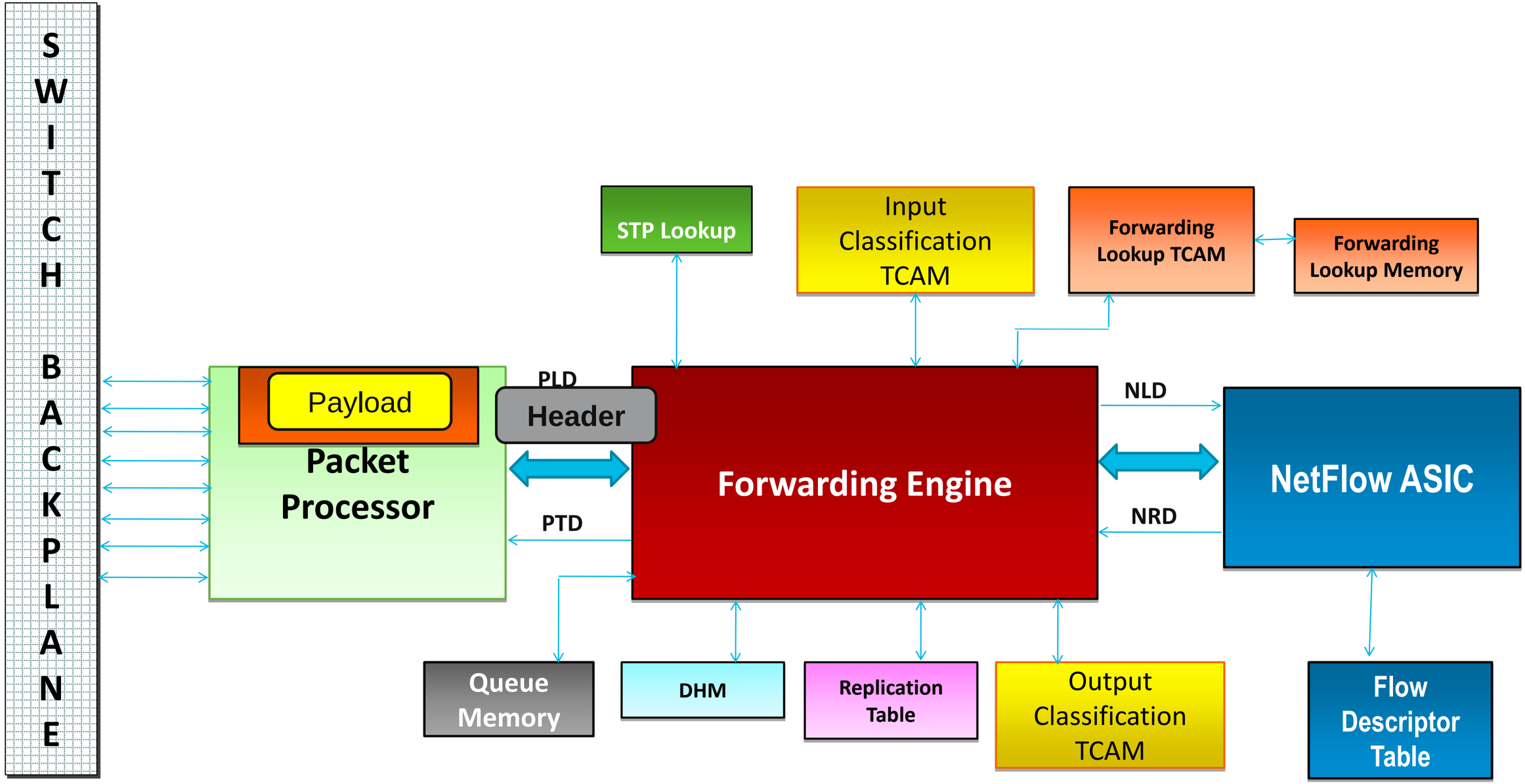


Catalyst 4500E Packet Walk

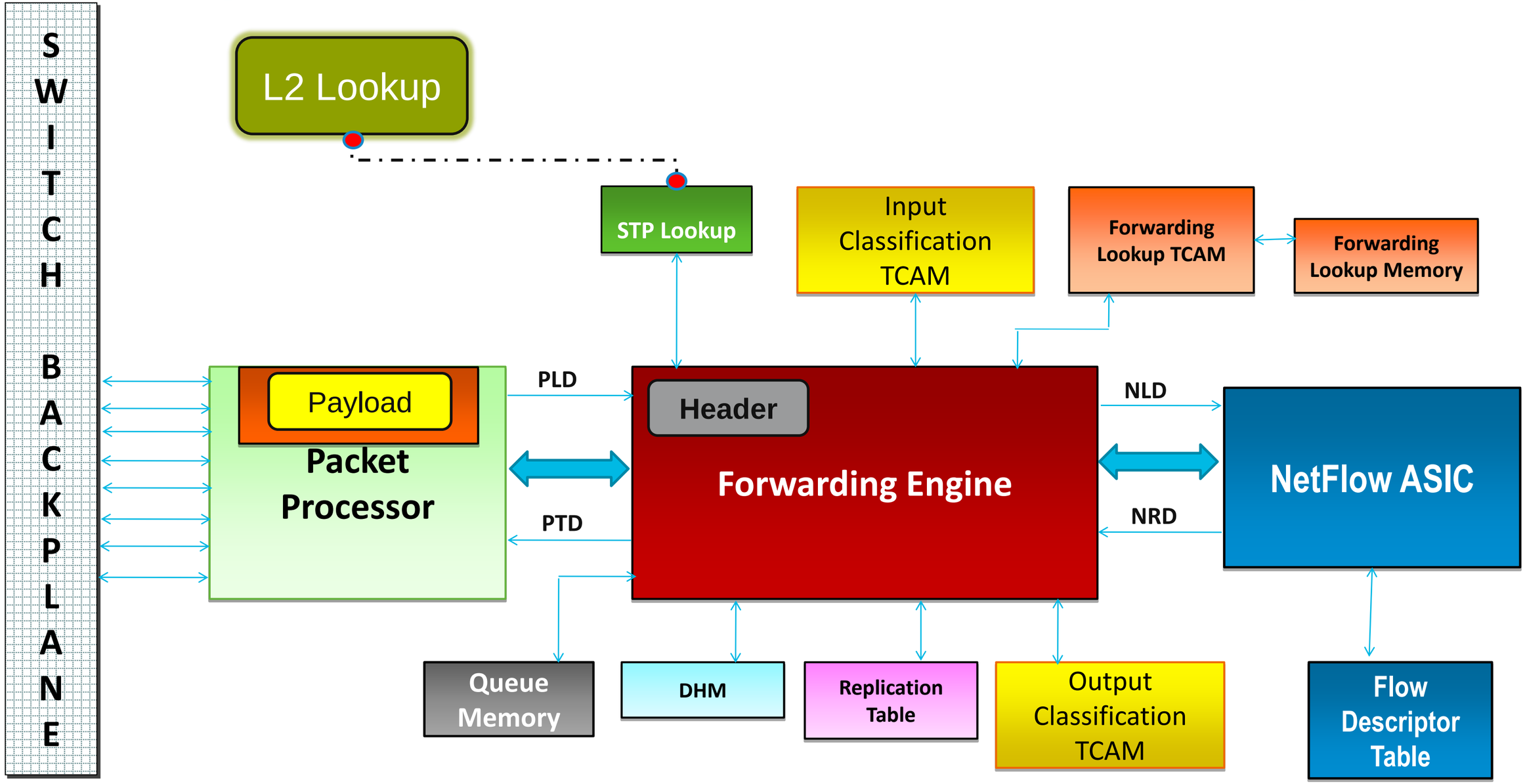
Supervisor 7-E Packet Walk: Packet Reception



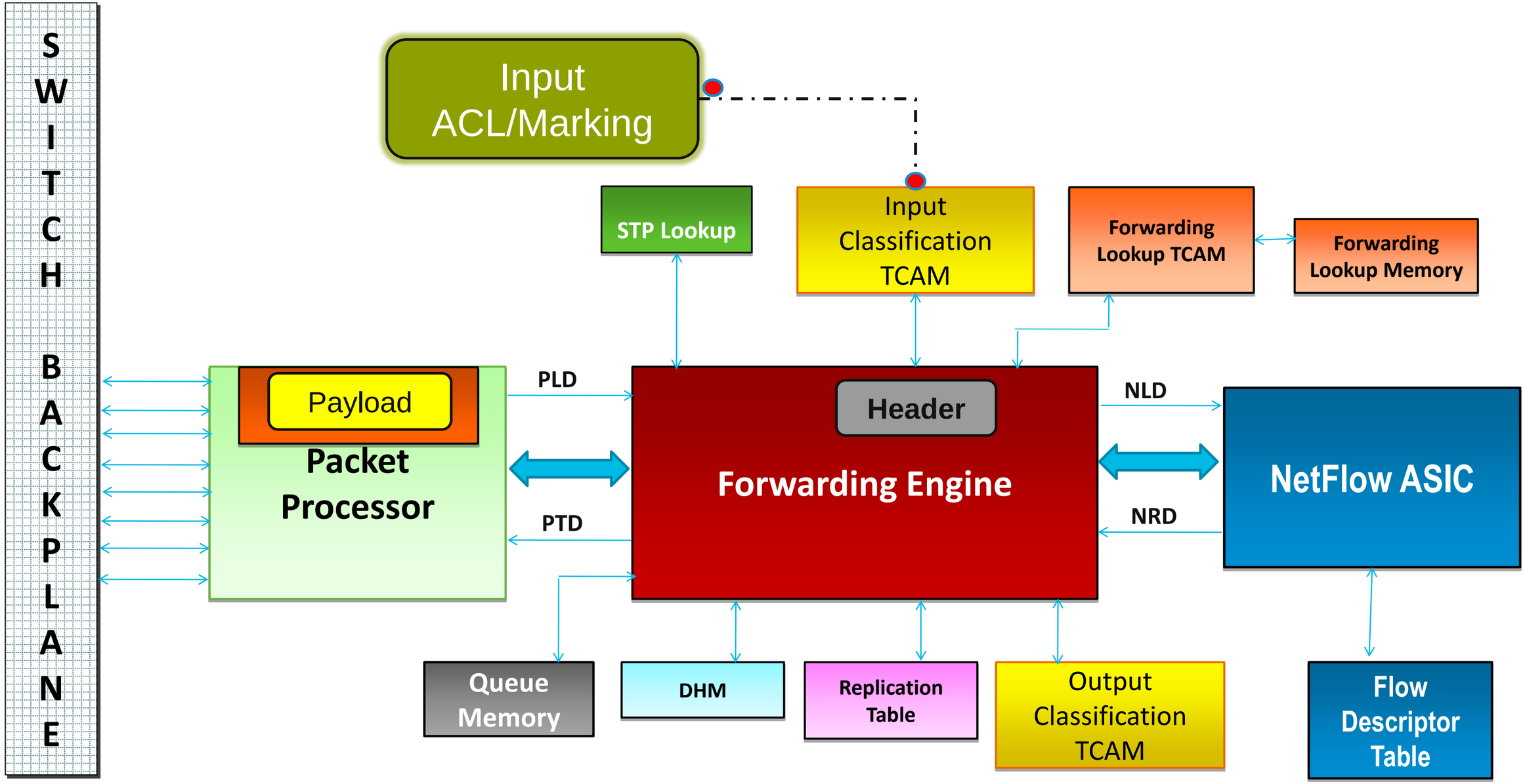
Supervisor 7-E Packet Walk: Pass PLD to FE



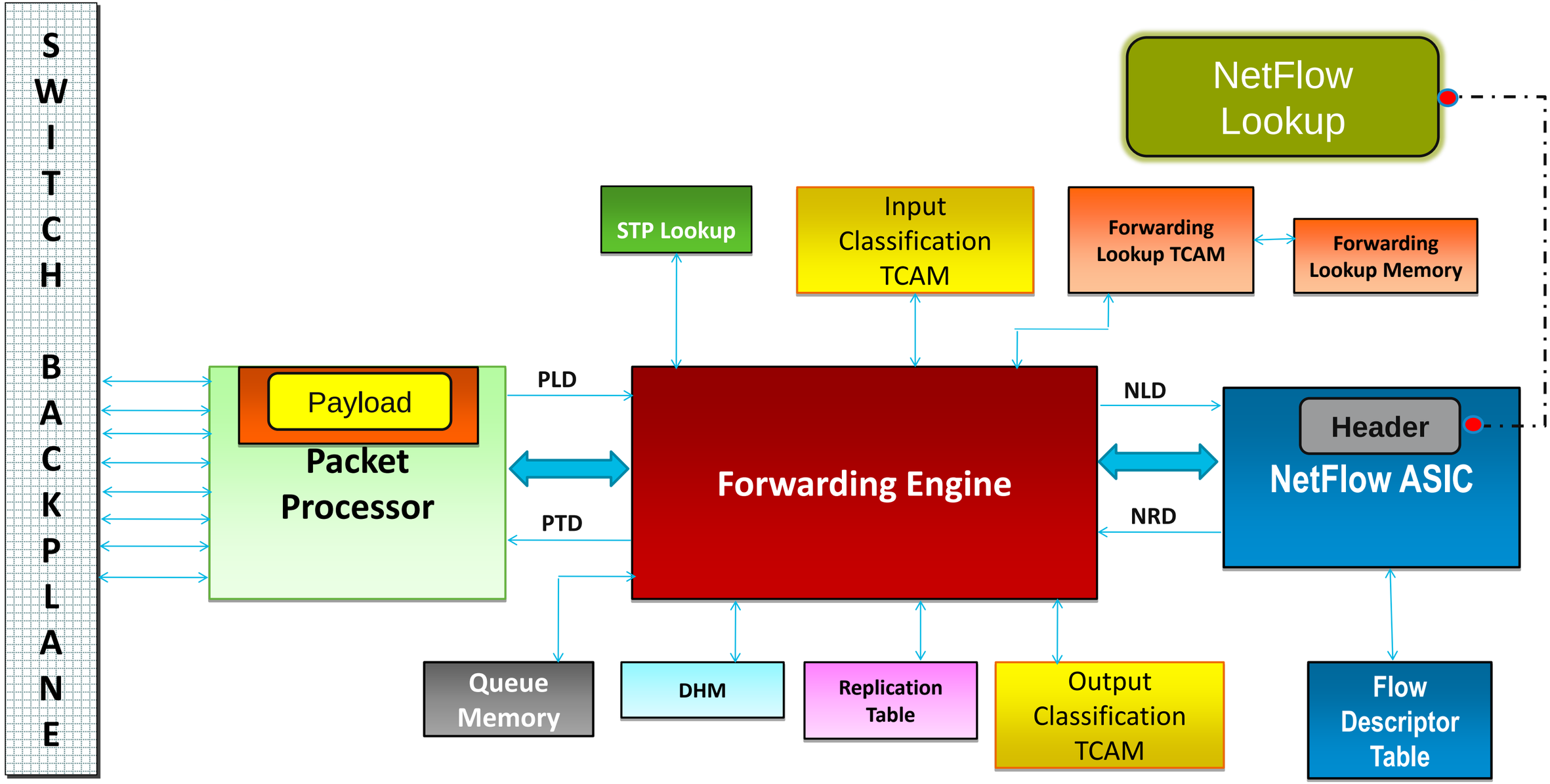
Supervisor 7-E Packet Walk: L2 Lookup



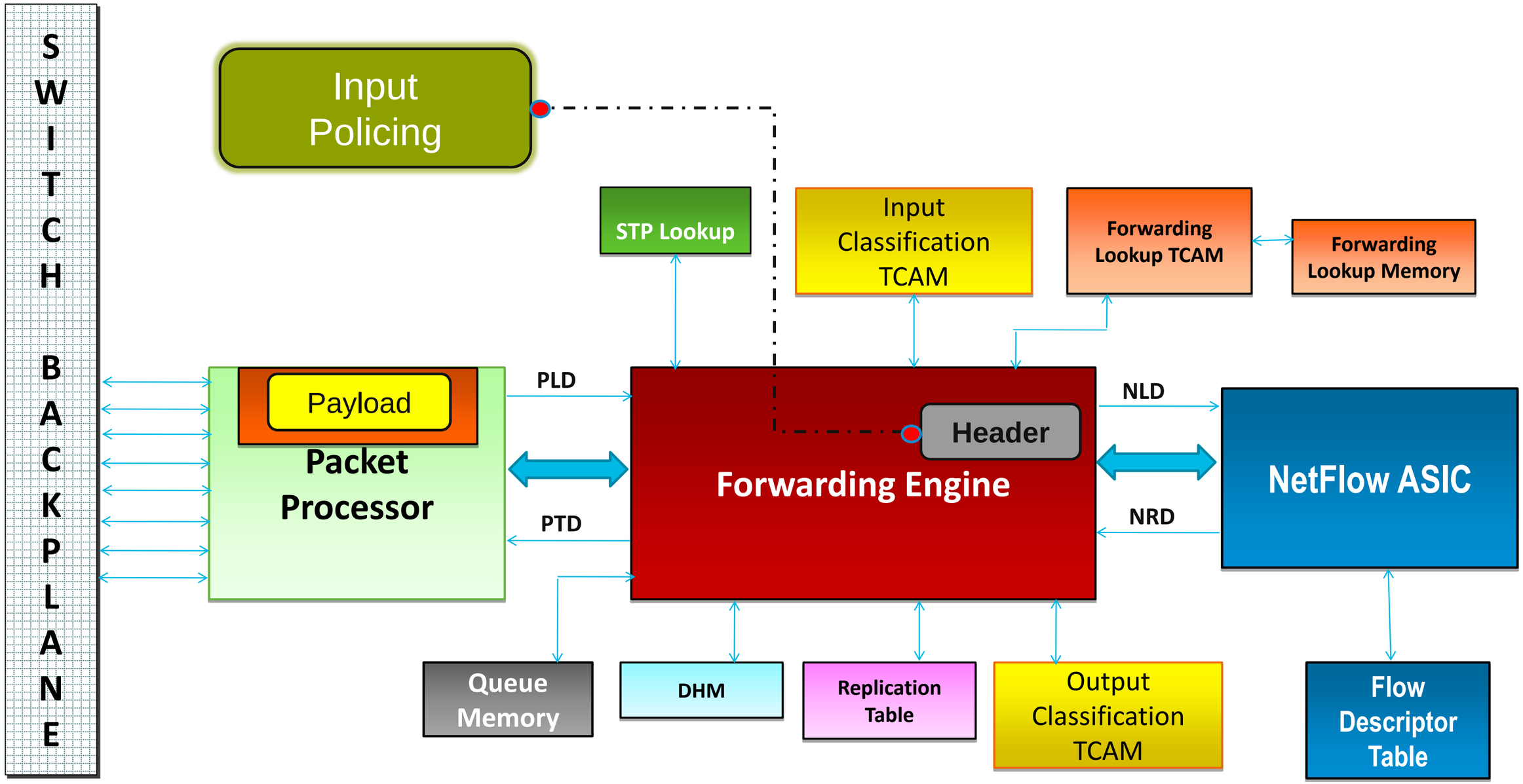
Supervisor 7-E Packet Walk: Input ACL/QoS



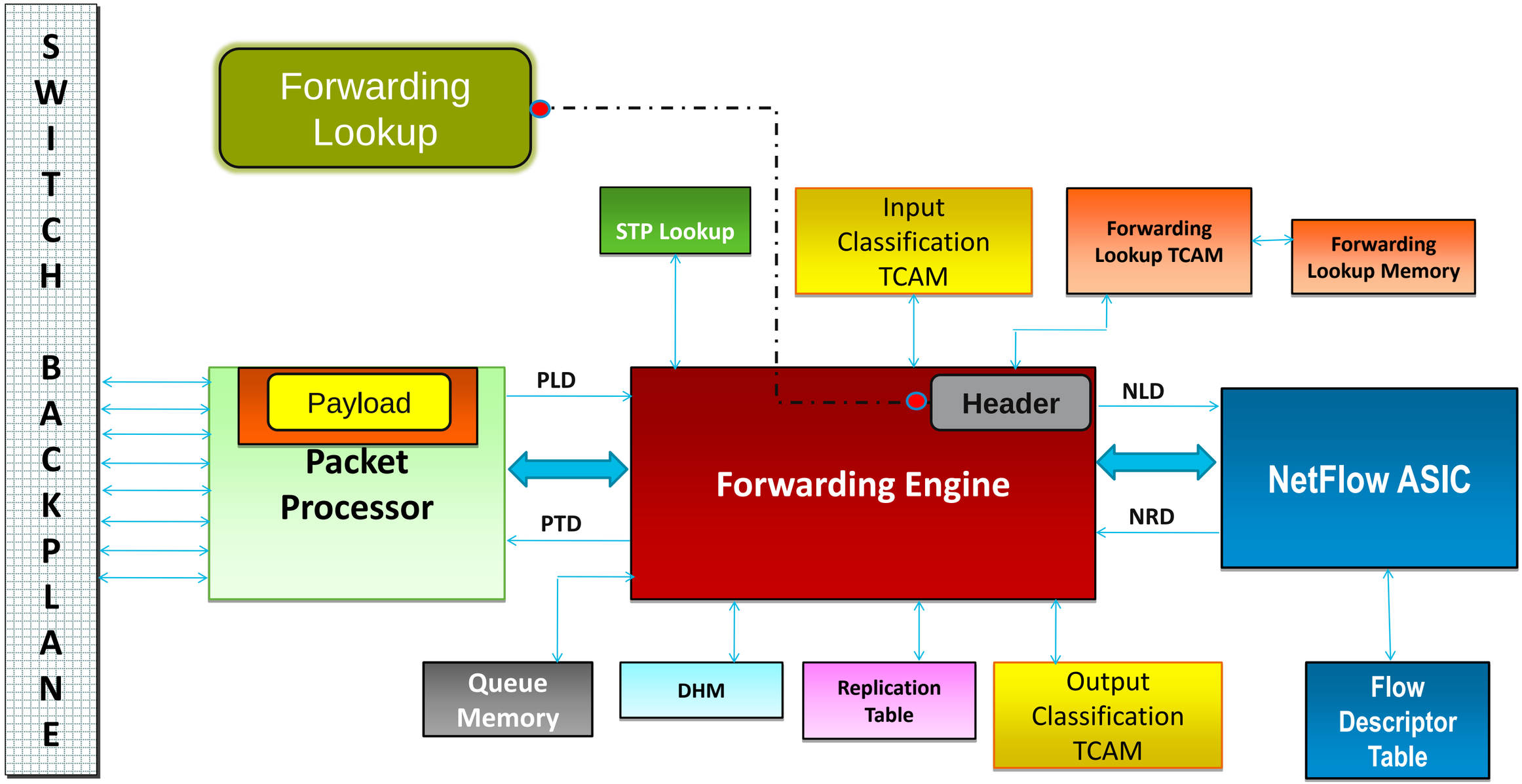
Supervisor 7-E Packet Walk: NetFlow Lookup



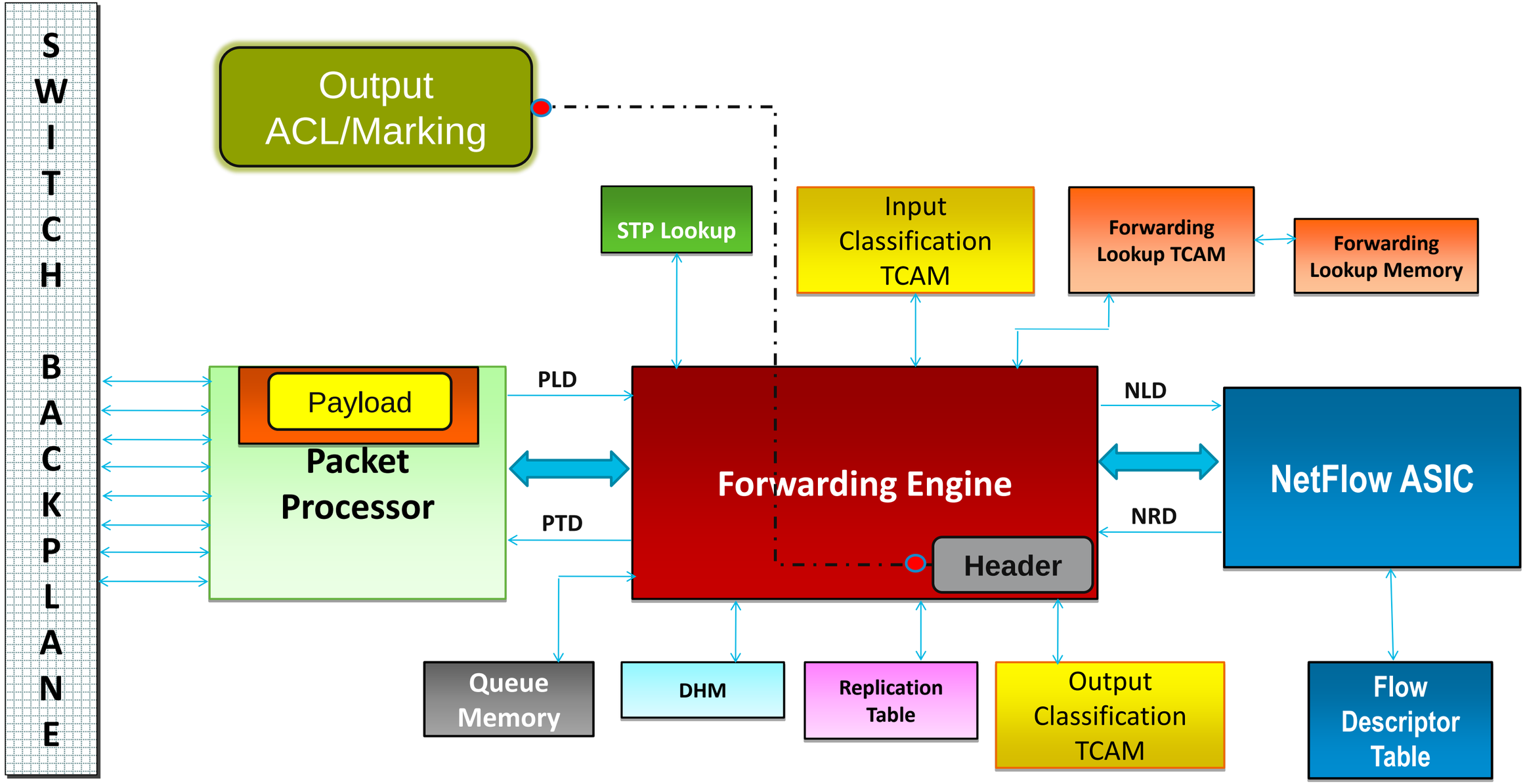
Supervisor 7-E Packet Walk: Input Policing



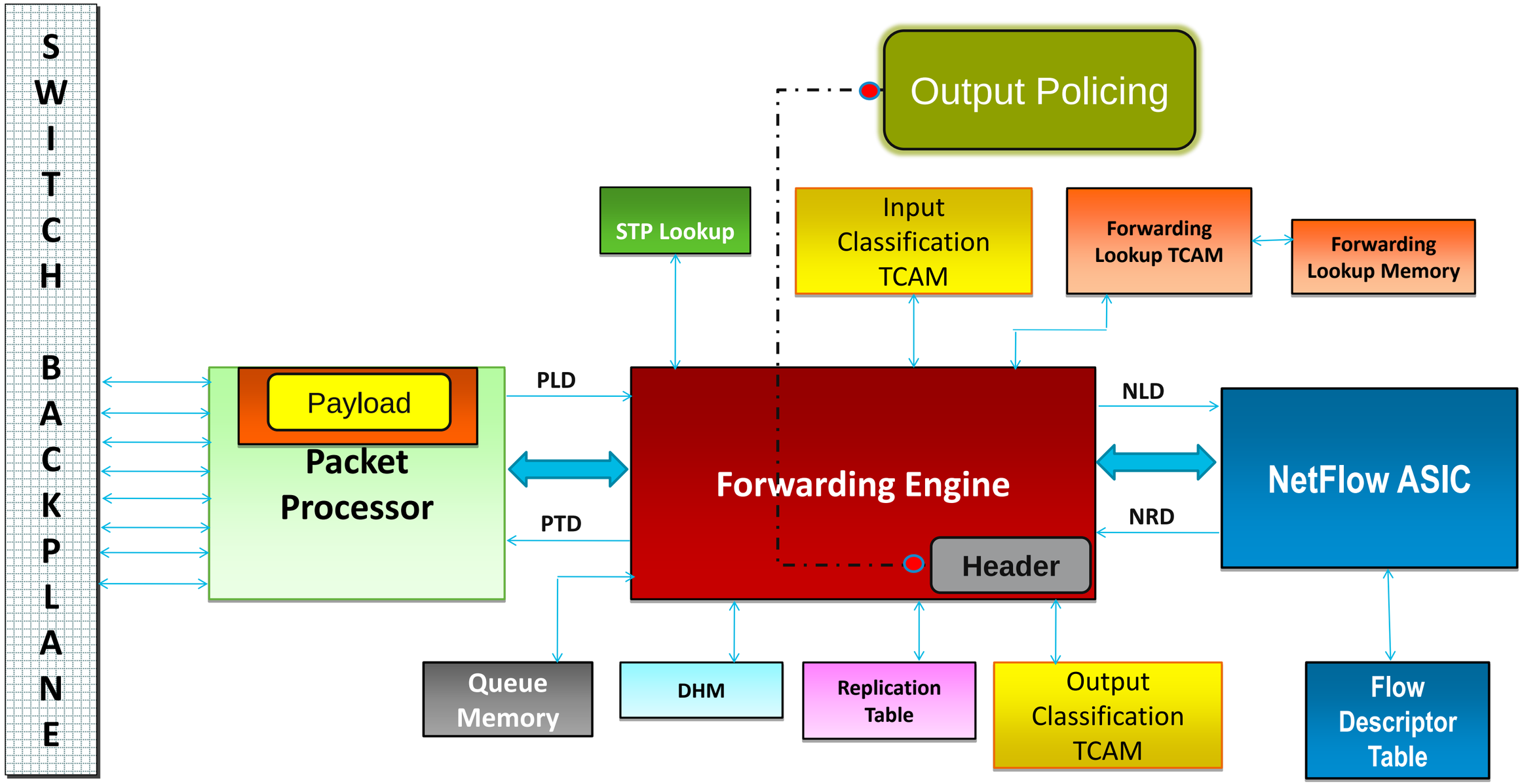
Supervisor 7-E Packet Walk: L3 Lookup



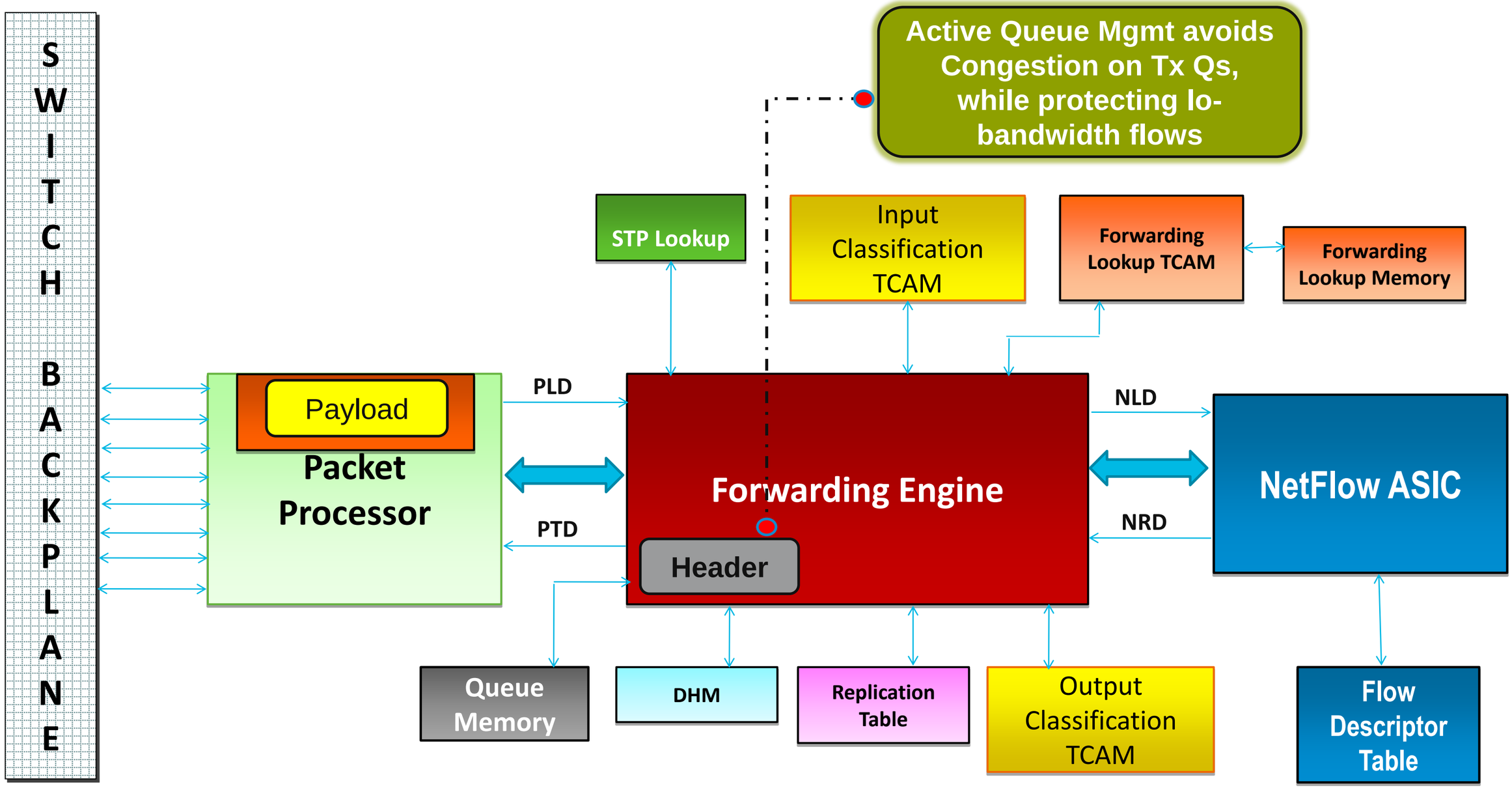
Supervisor 7-E Packet Walk: Output ACL/QoS



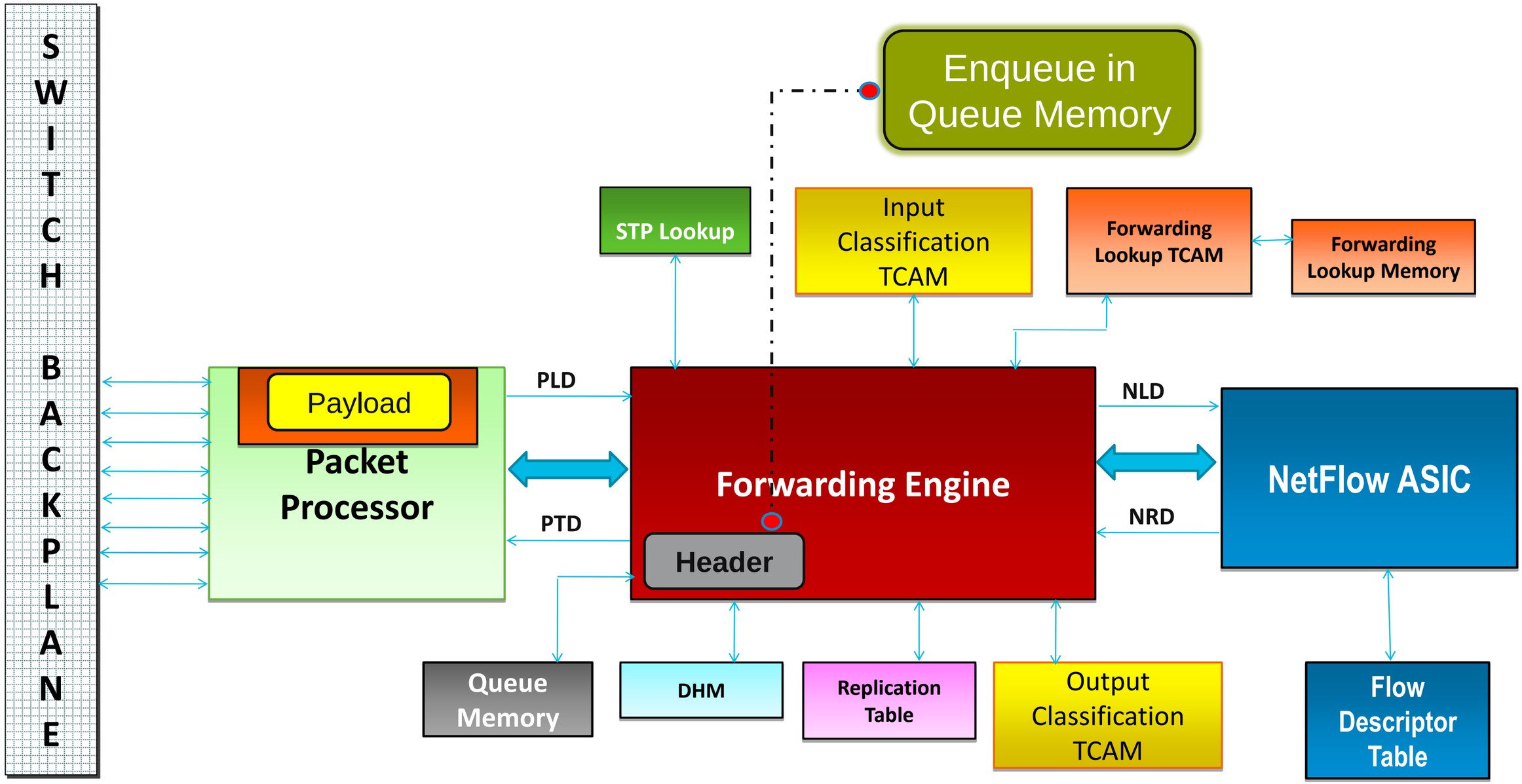
Supervisor 7-E Packet Walk: Output Policing



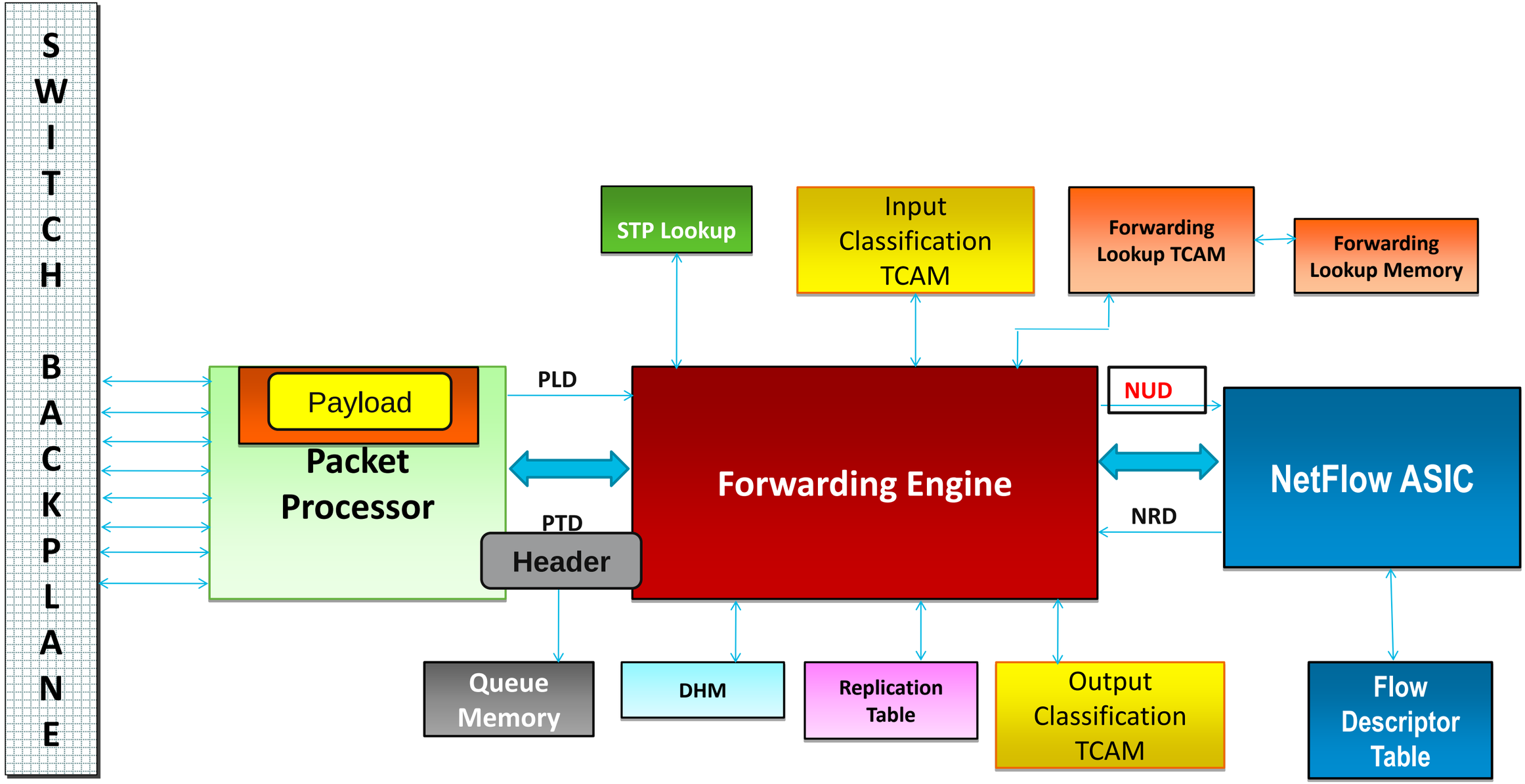
Supervisor 7-E Packet Walk: DBL Processing



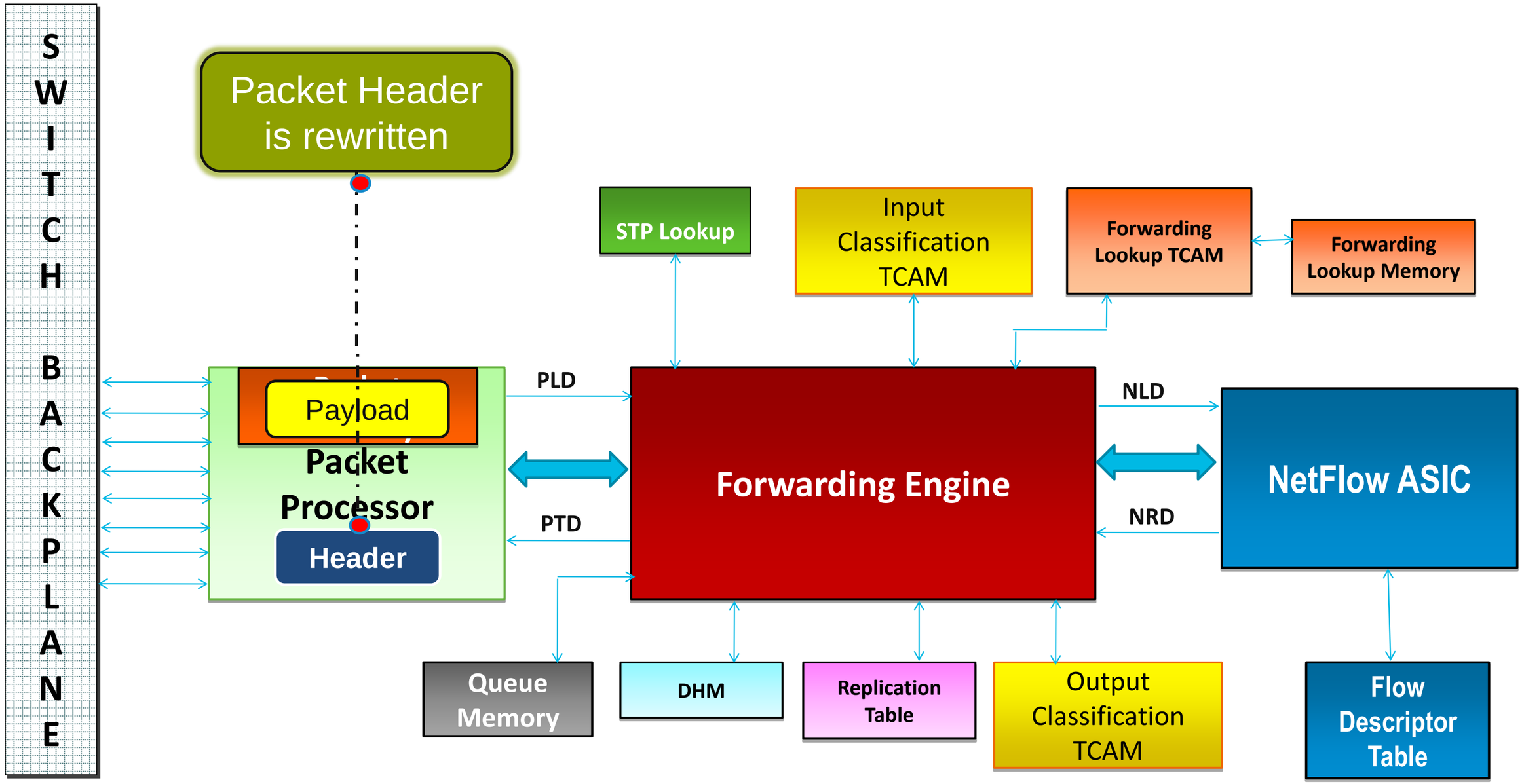
Supervisor 7-E Packet Walk: Enqueue



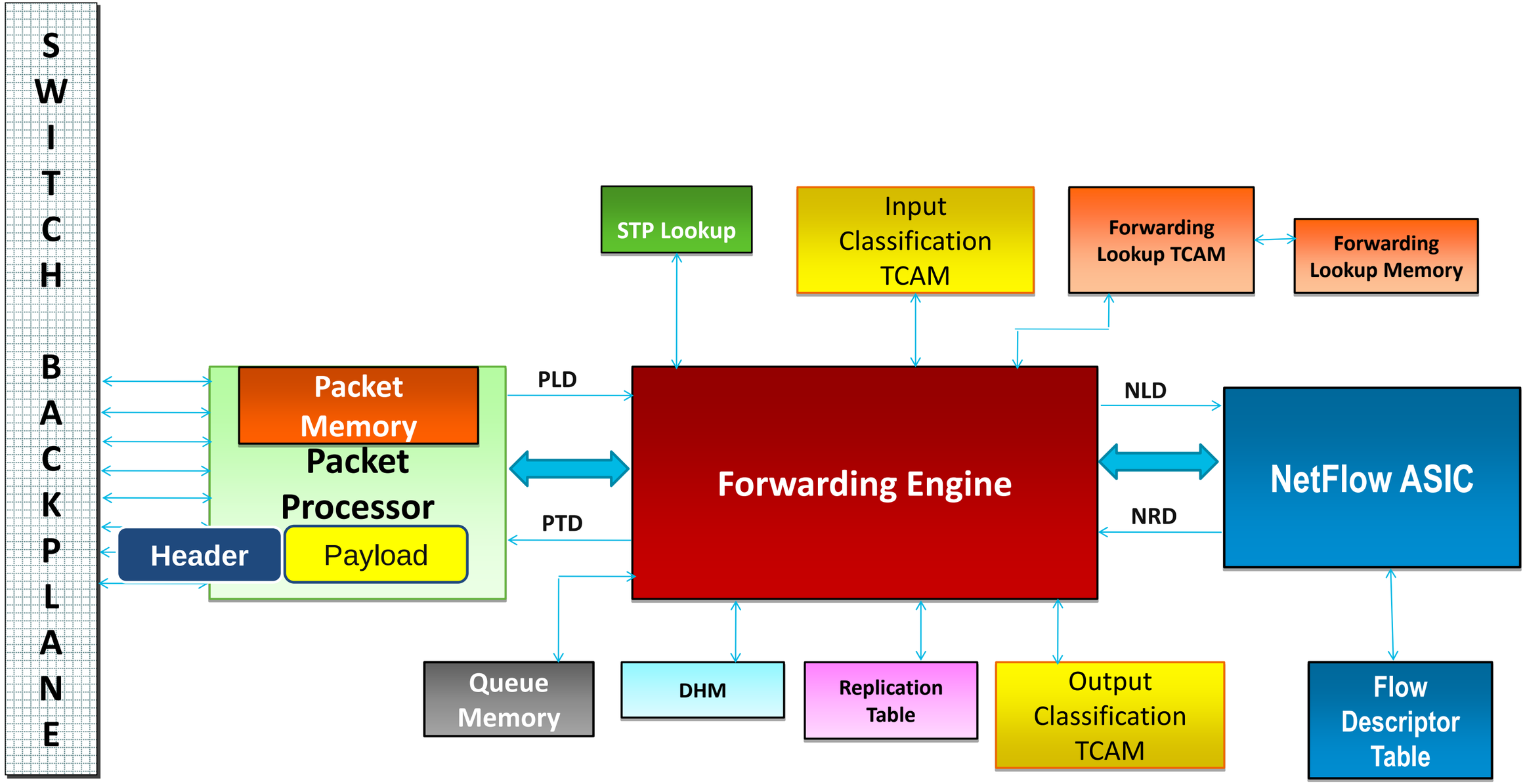
Supervisor 7-E Packet Walk: Header to PP



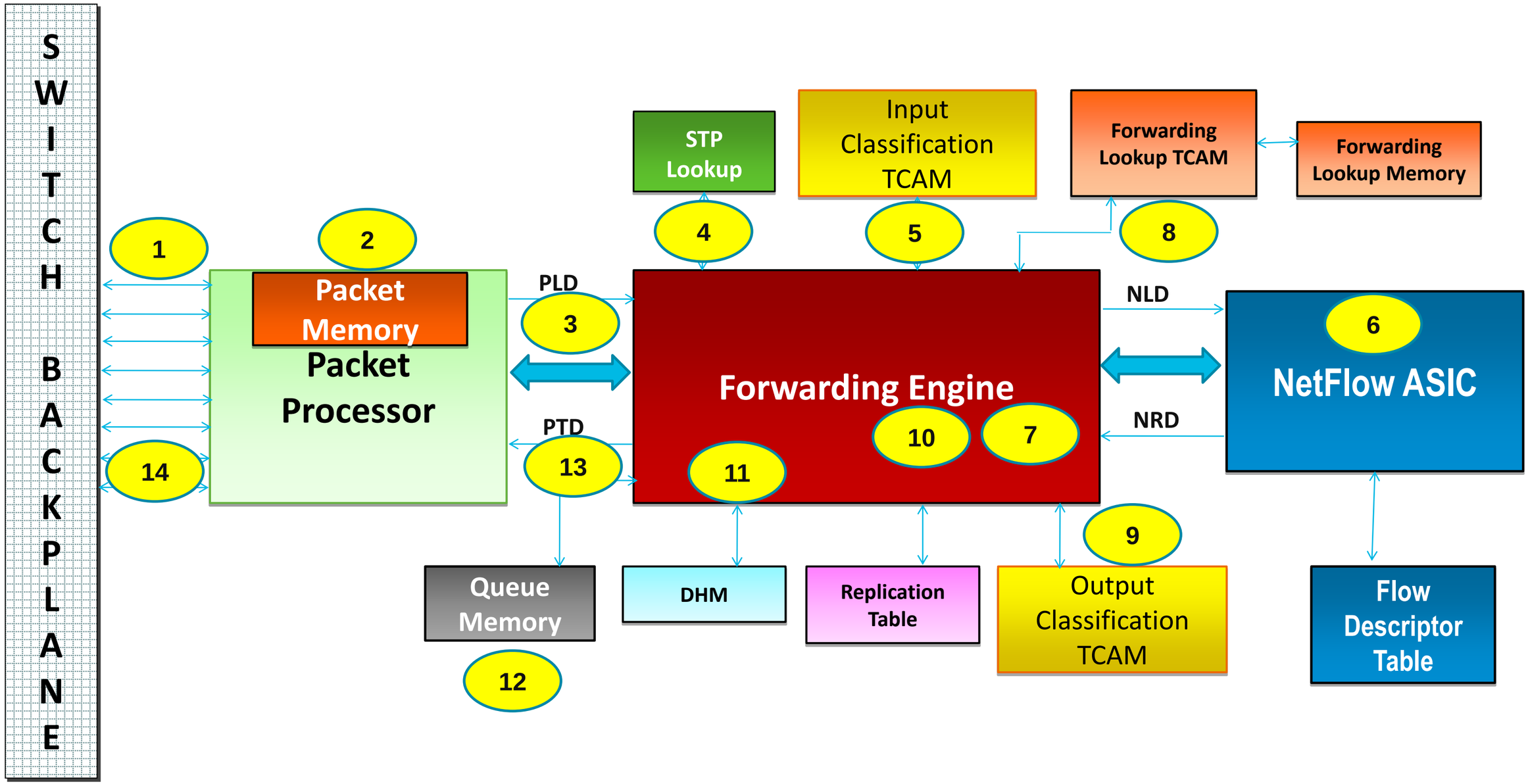
Supervisor 7-E Packet Walk: Packet Rewrite



Supervisor 7-E Packet Walk: Attach Payload



Supervisor 7-E Packet Walk: FE Blocks



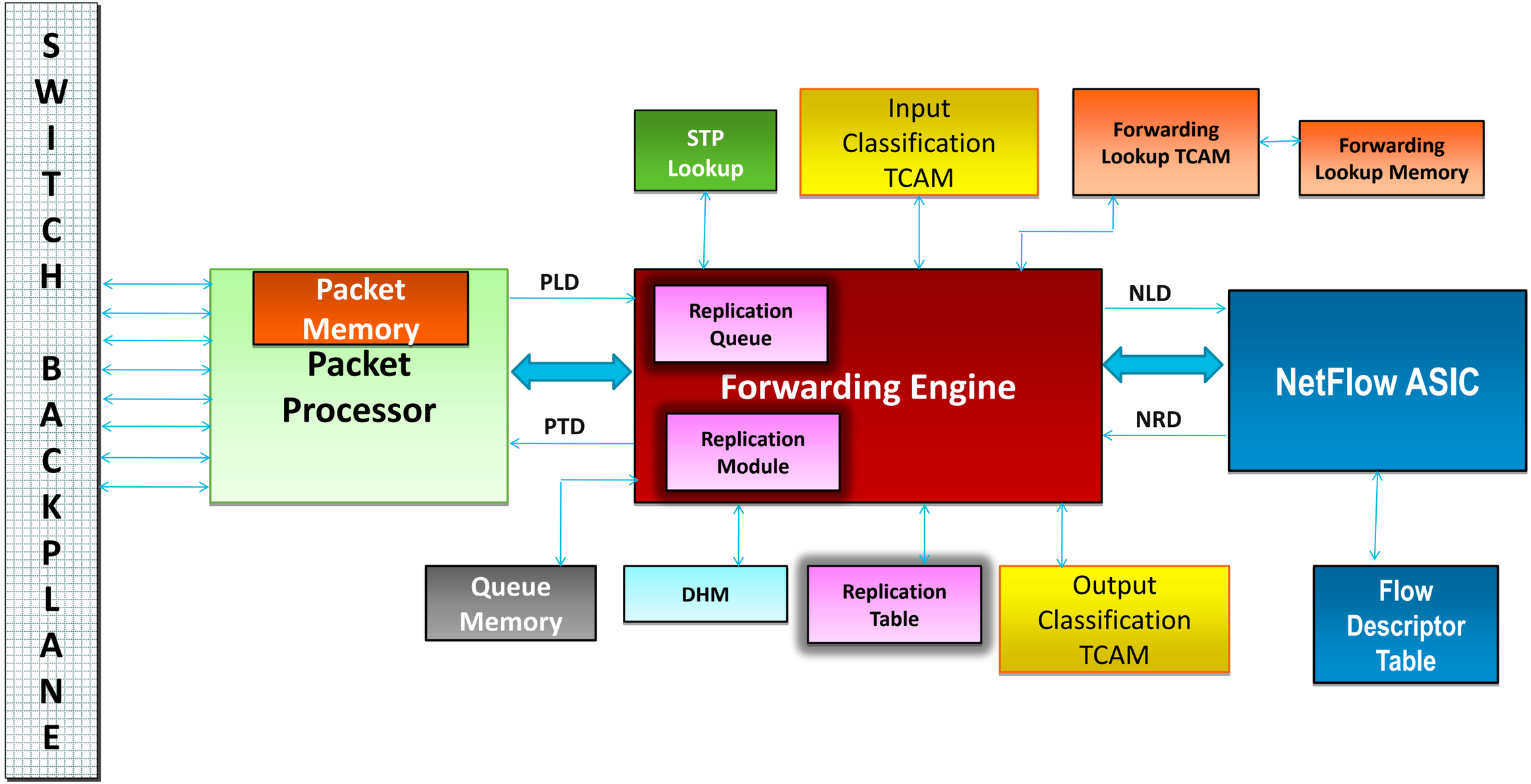
Supervisor 7-E – Unicast Packet Walk

1. A packet enters the PHY in the line module and travels across the backplane before reaching the supervisor
2. The packet enters the Supervisor and the Packet Processor performs parsing of VLAN tag and header and stores the packet into Packet Memory
3. The stripped header is used to construct a Packet Lookup Descriptor (PLD) and forwarded to the Forwarding Engine ASIC
4. The packet goes through L2 lookup. Spanning tree state is checked. Packet MAC source and MAC destination together with receive vlan ID are looked up in the L2 Hash Table. L2 lookup also determines whether the packet is destined for router functionality.
5. Input Classification is used to classify the packet via rules loaded into the Input Classification TCAM. ICC stores input ACL and QoS rules in TCAM4
6. A NLD (Netflow Lookup Descriptor) is created by the Forwarding Engine and fed into the NetFlow ASIC. Here new flow is created or updated; also microflow policing is done here.
7. NRD (Netflow Result Descriptor) is created by NetFlow ASIC and passed to the Forwarding Engine ASIC. Input Aggregate policing result from VFE and Ingress Microflow policing result from NetFlow ASIC are merged, and packet policed accordingly.
8. Header is looked up in the FLC for L3 Lookup. FLC stores L3 (or L2 lookup) forwarding and unicast RPF check rules. Contains mainly IPv4 and IPv6 FIB entries.

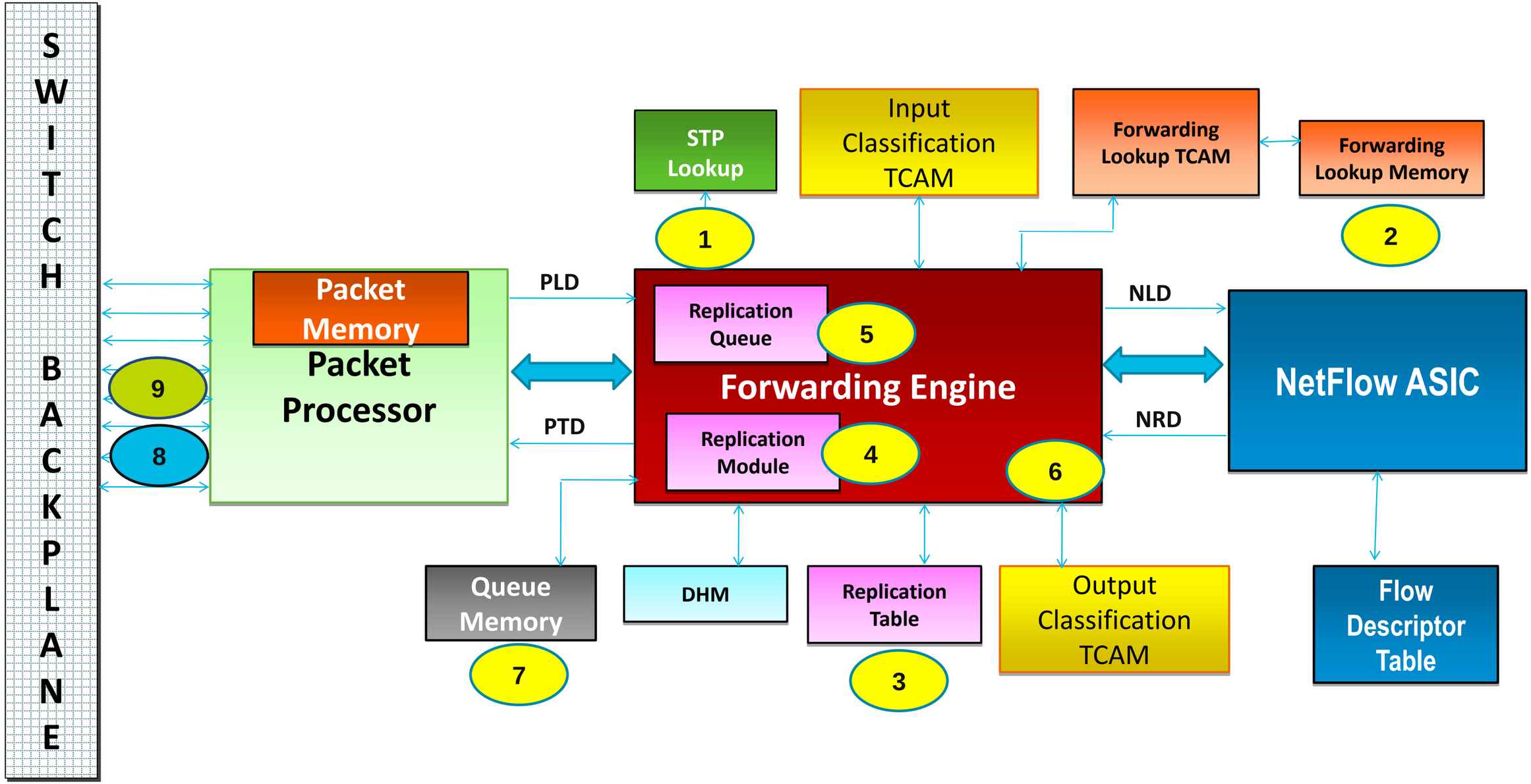
Supervisor 7-E – Unicast Packet Walk

9. OCC stores output ACL and QoS rules in TCAM4
10. Output policing is done at this stage.
11. DBL Hashing Memory is algorithm for avoiding congestion in the ASIC.
12. The transmit descriptor is enqueued in the queue memory
13. Packet Transmit Descriptor (PTD) is sent to the Packet Processor. A NetFlow Update Descriptor (NUD) is sent by the Forwarding Engine to the NetFlow ASIC to update Transmit Statistics for that flow.
14. Packet Processor transmits the packet across the backplane to the correct egress line card.

Supervisor 7-E Packet Walk: Multicast Architecture



Supervisor 7-E Packet Walk: Multicast Forwarding



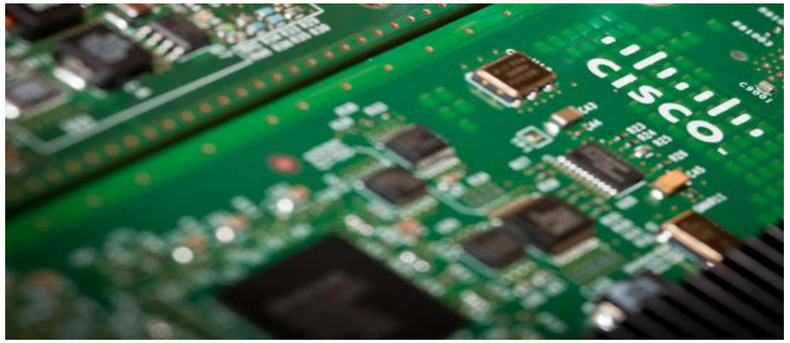
Supervisor 7-E – Multicast Packet Walk

1. Packet comes in as a Source packet. The payload is copied to packet memory, and the small header or Descriptor is stripped off. The L2 table will indicate that the DMAC is a multicast MAC.
2. The packet will be processed pretty much like a unicast packet would.
3. At some point, during the Forwarding Lookup, the destination Multicast Group address will be looked up. This will point to an Adjacency Entry in the FLC, which points to a RET Entry, in the Replication Table.
4. The REM consults the RET Table, it stores the information as to how many copies of this Descriptor need to be created and what are the forwarding interfaces for each copy of the Descriptor.
5. The REM creates the Header Copies and enqueues them in the Replication Request Queue.
6. This Descriptor traverses through the Forwarding Engine like before, but none of the Ingress Processing including Forwarding Lookups are done. It proceeds straight to OCC for applying egress features on each of those OIFs.
7. Once the features are applied and the packets are permitted out the OIF – they are enqueued into the Queue Memory.
8. The copies are then forwarded to their respective OIFs.

Agenda

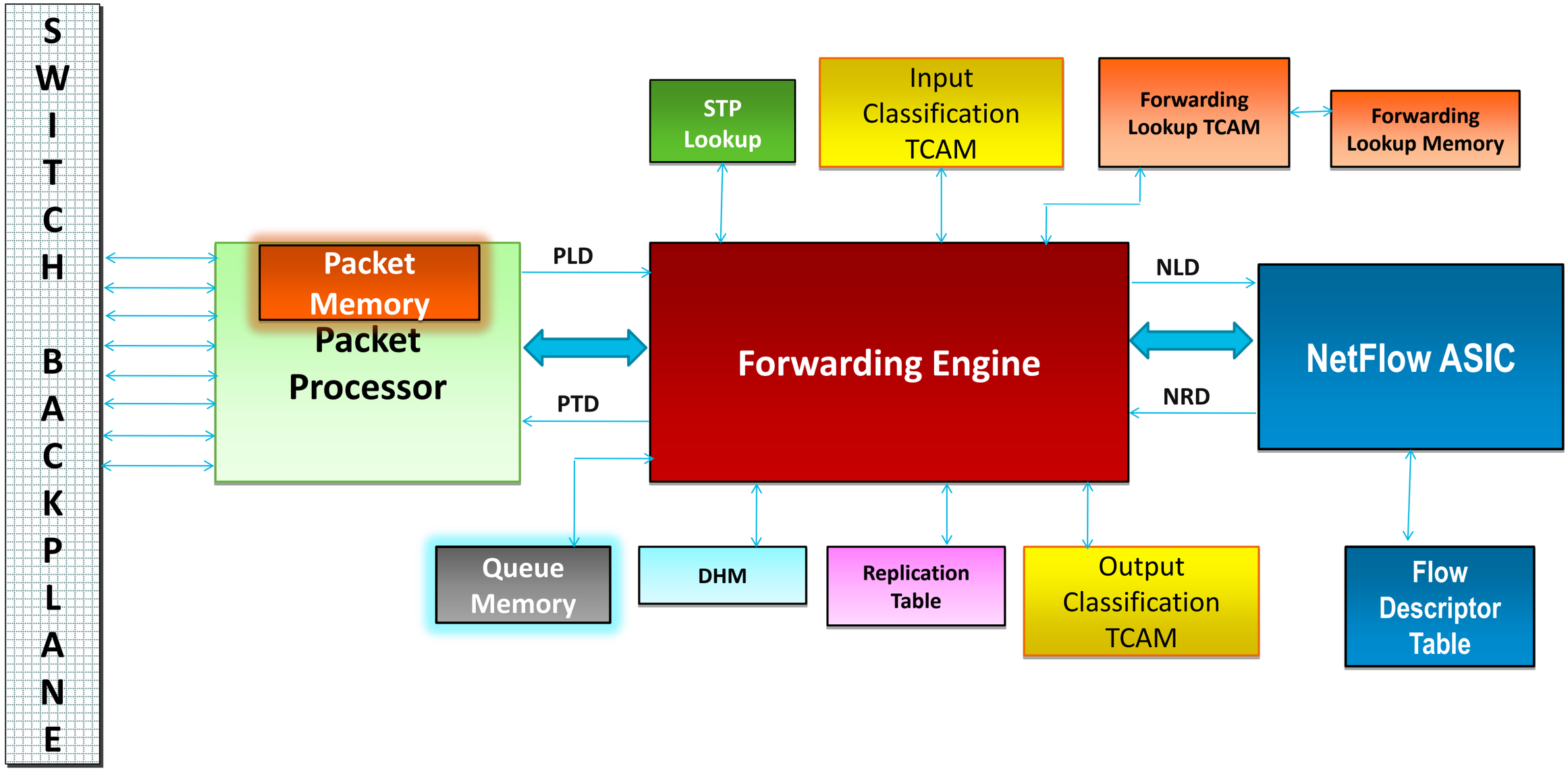
- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and Packet walk
- Quality of Service Overview
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

Catalyst 4500E QoS Overview

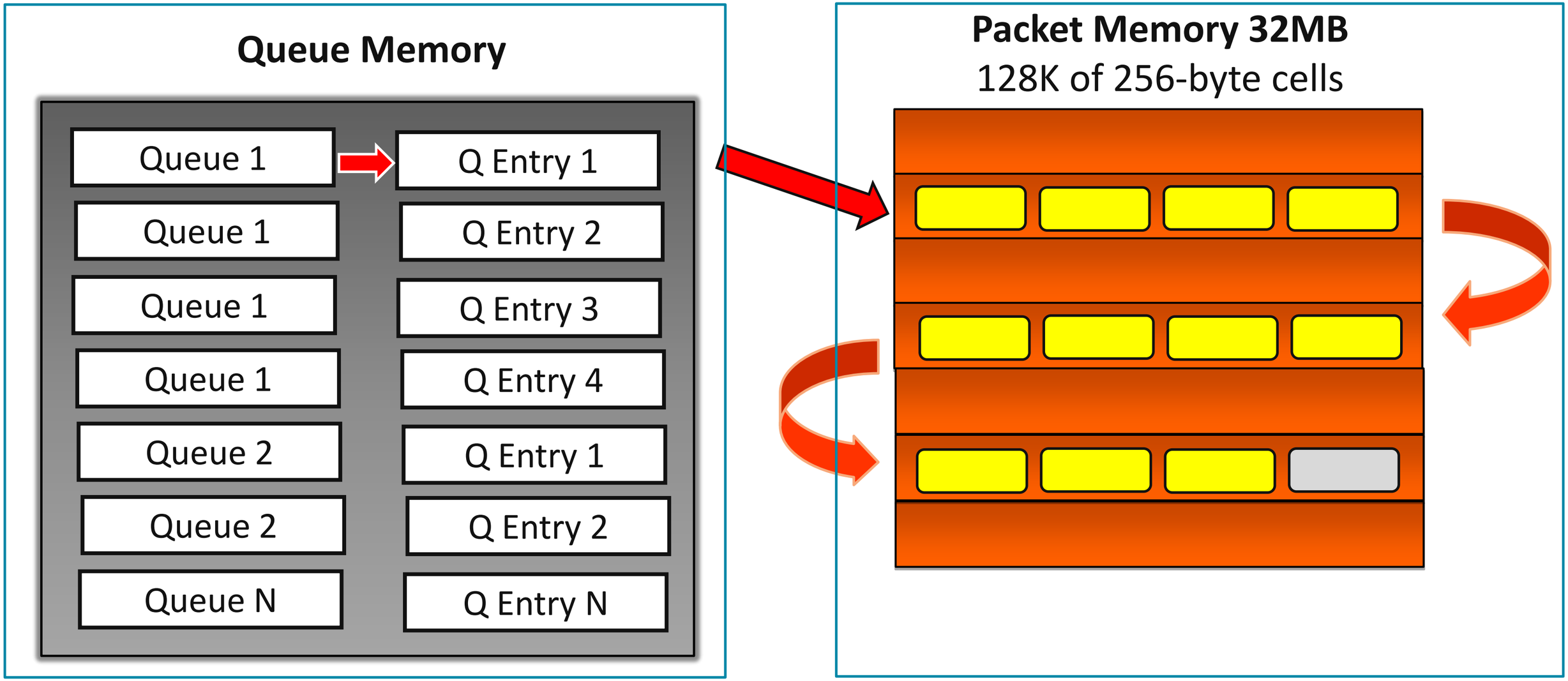


- QoS is enabled by default.
- Implicit Trust on all ports by default – Just like in traditional routers.
- Modular QoS CLI (MQC) compliant.
- User-Based Rate Limiting (UBRL) or Microflow policing support.
- Queuing is 1P7Q1T with Dynamic Buffer Limiting (DBL).
- Configurable queue size per port measured in terms of Number of Queue Entries (Packets).
- No Ingress Queuing, only Egress Queuing supported.
- All Front Panel Ports Queues are located in Forwarding Engine.

Supervisor 7-E: Packet & Queue Memory

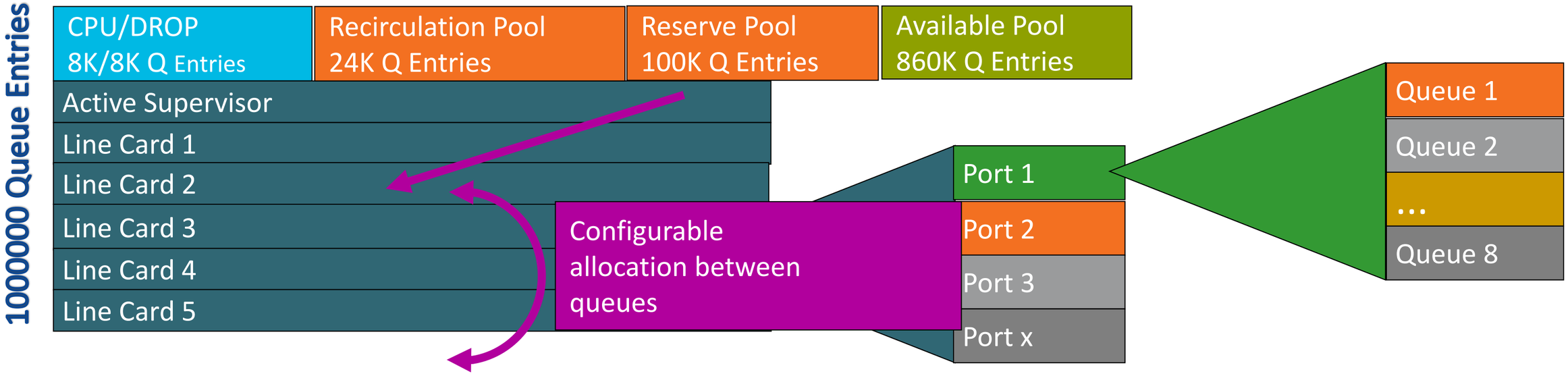


Supervisor 7-E: Packet & Queue Memory



Queue Memory
Queue Entries Allocation

1. CPU/Drop/Recirculation queue entries allocated
2. Queue entry allocation for slots is divided by number of slots *
3. Linecards divide entries equally per port
4. Port entries divided equally per queue



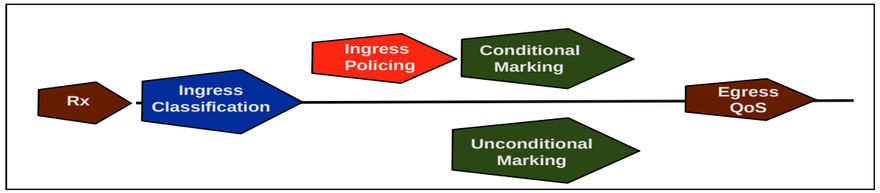
* For redundant chassis , sup slots are counted as 1 slot

Queue Structures and Size on different Supervisors

Supervisor Engines	Egress Queue and Drop Thresholds	Total Buffer Size	Total Queue Entries (Packets) per system	Queue Entries (Packets) per Default Queue per Port*
WS-X4516-10GE	1p3q1t	16MB	256K	260 Per Queue for all 4 queues.
WS-X45-SUP6-E	1p7q1t	17.5MB	512 K	1368
WS-X45-SUP7-E	1p7q1t	32MB	1 Million	3120

* - configuration based on a 7-slot system with one 48-port Linecard

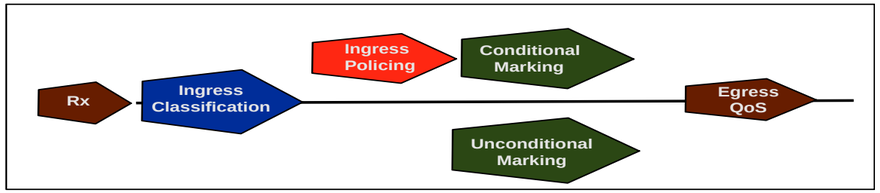
Classifying traffic



SCCP, SIP	= Multimedia Signaling	TCP Port 2000-2002, TCP/UDP Port 5060-5061
Webex	= Multimedia Conferencing	TCP Port 1270
Backup	= Bulk Data	TCP Port 16384, among various
ERP	= Transactional Data	TCP Port 1521, among various
Web	= Transactional Data	TCP Port 80
Email	= Bulk Data	TCP Port 143, 110, 389
iTunes, Youtube	= P2P	TCP Port 3689, UDP Port 5353

SCCP, SIP	= Multimedia Signaling	
RTP, RTCP	= Multimedia Traffic	UDP Port 5004, 5005 among various

Marking Policy



SCCP, SIP — CS3 — **Trust**

Webex — AF4

Backup — AF1

ERP — AF2

Web — AF1

Email — AF1

iTunes, Youtube — CS1

Trust AF3 — DMS, IP/TV

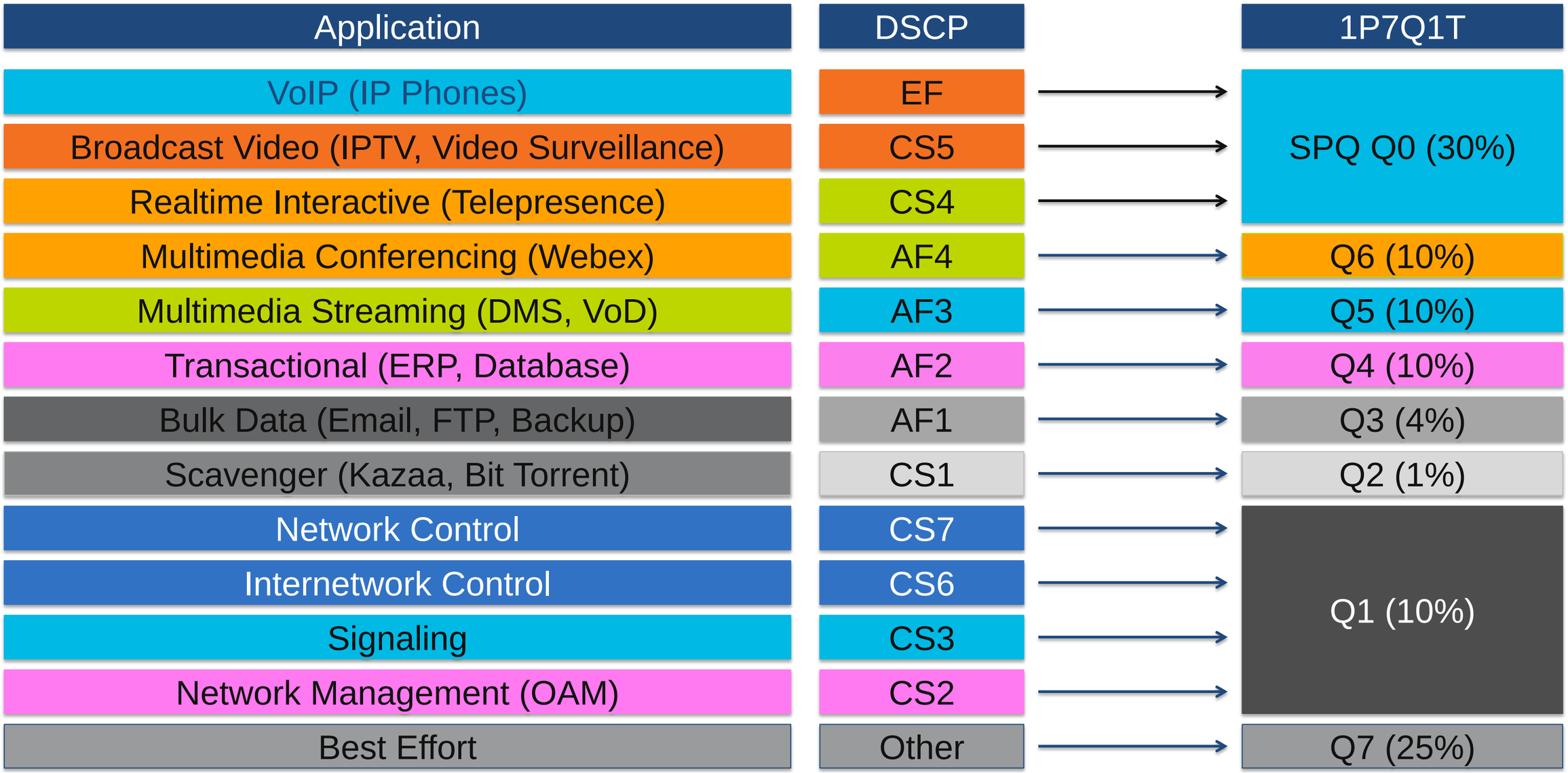
CS2 — OAM

CS6 — Control Plane

VoIP — EF — **Trust**

Telepresence — CS4 — **Trust**

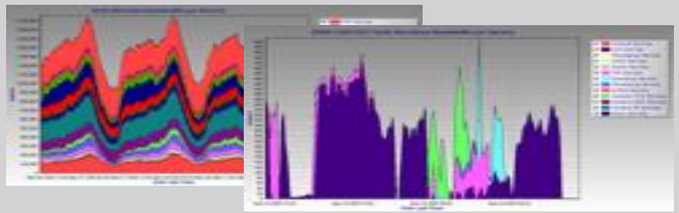
Egress Queuing Model



Agenda

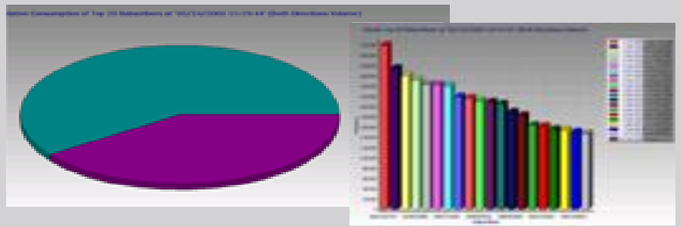
- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and Packet walk
- Quality of Service Overview
- Flexible NetFlow
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

Why NetFlow?



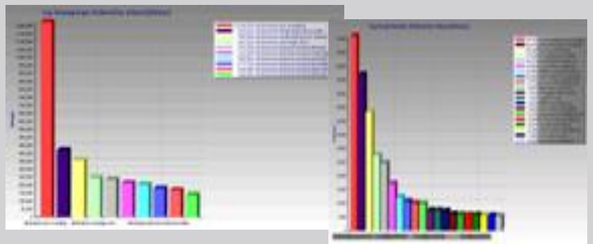
Bandwidth/Capacity Reports

- What is eating up my network resources?
- When do I need a capacity upgrade?
- What is causing congestion?



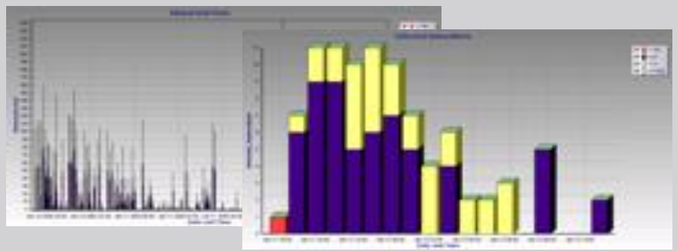
Subscriber Demographic Reports

- What percentage is using P2P/gaming application?
- What are the usage patterns of different subscriber groups?
- What is the cost impact of my top subscribers?



Server Activity

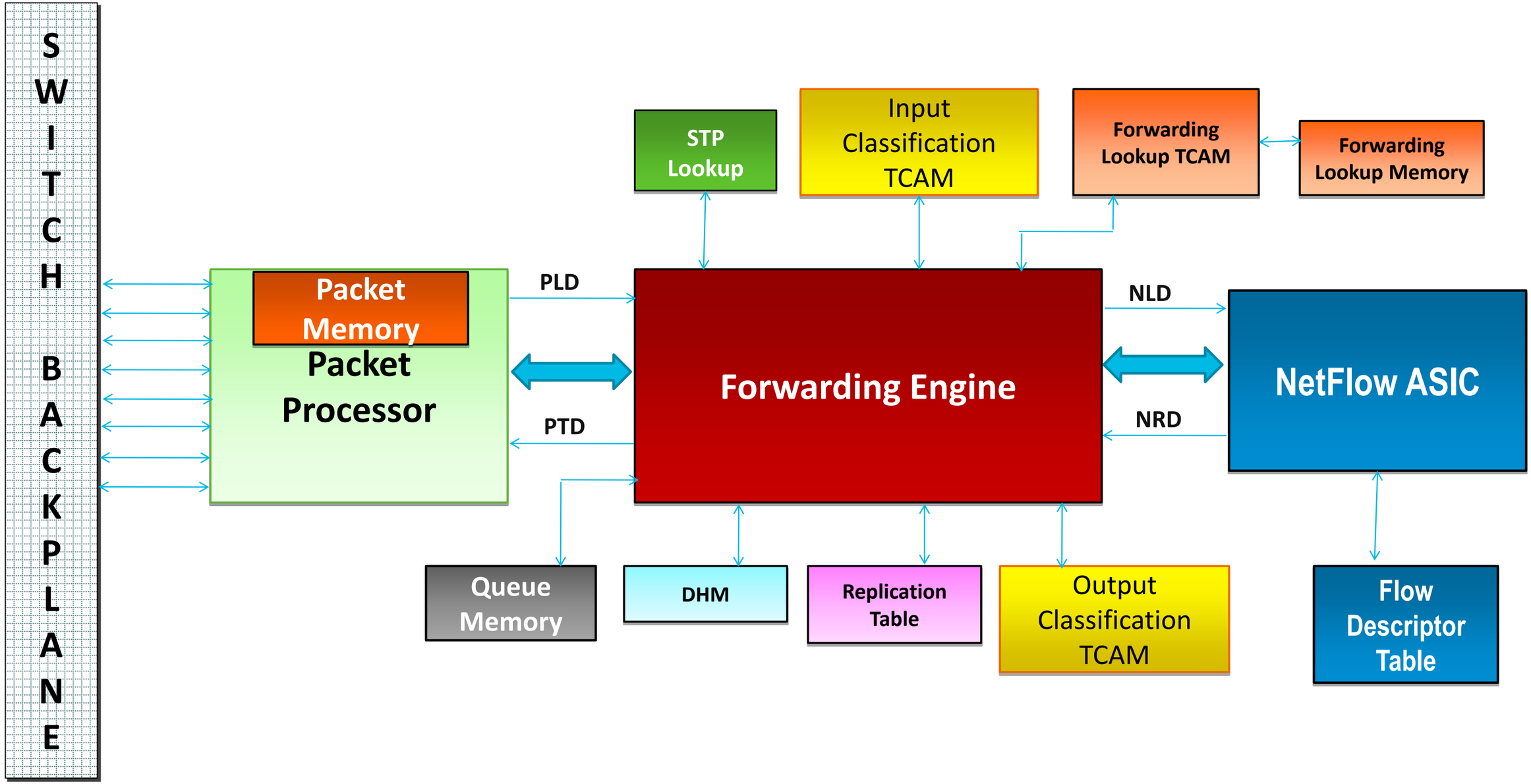
- What are the popular Web hosts used?
- What are the popular streaming sites?



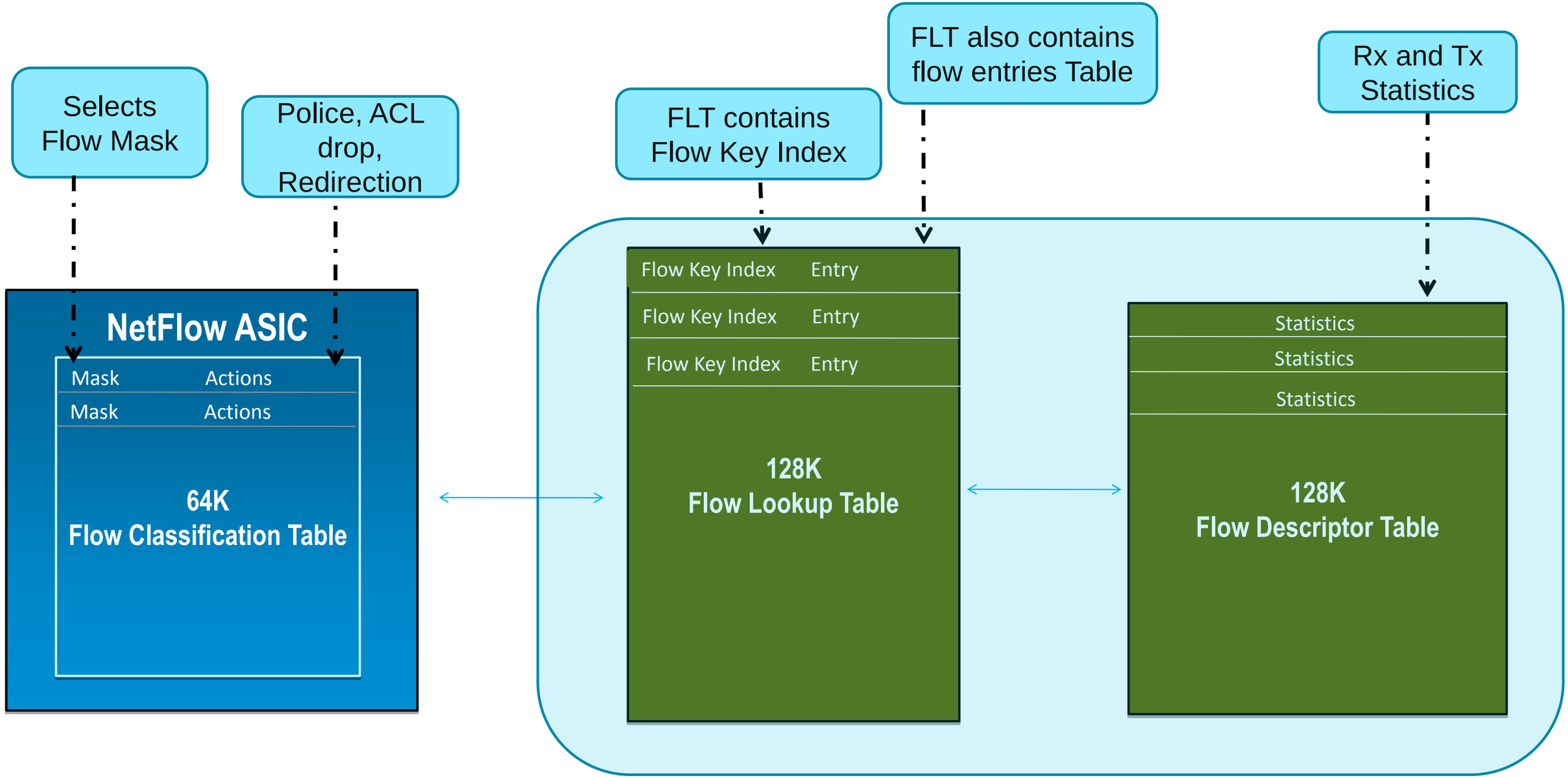
Security Reports

- Which subscribers are infected and attacking others?
- Which subscribers are spamming?
- Which subscriber is attacking network resources?

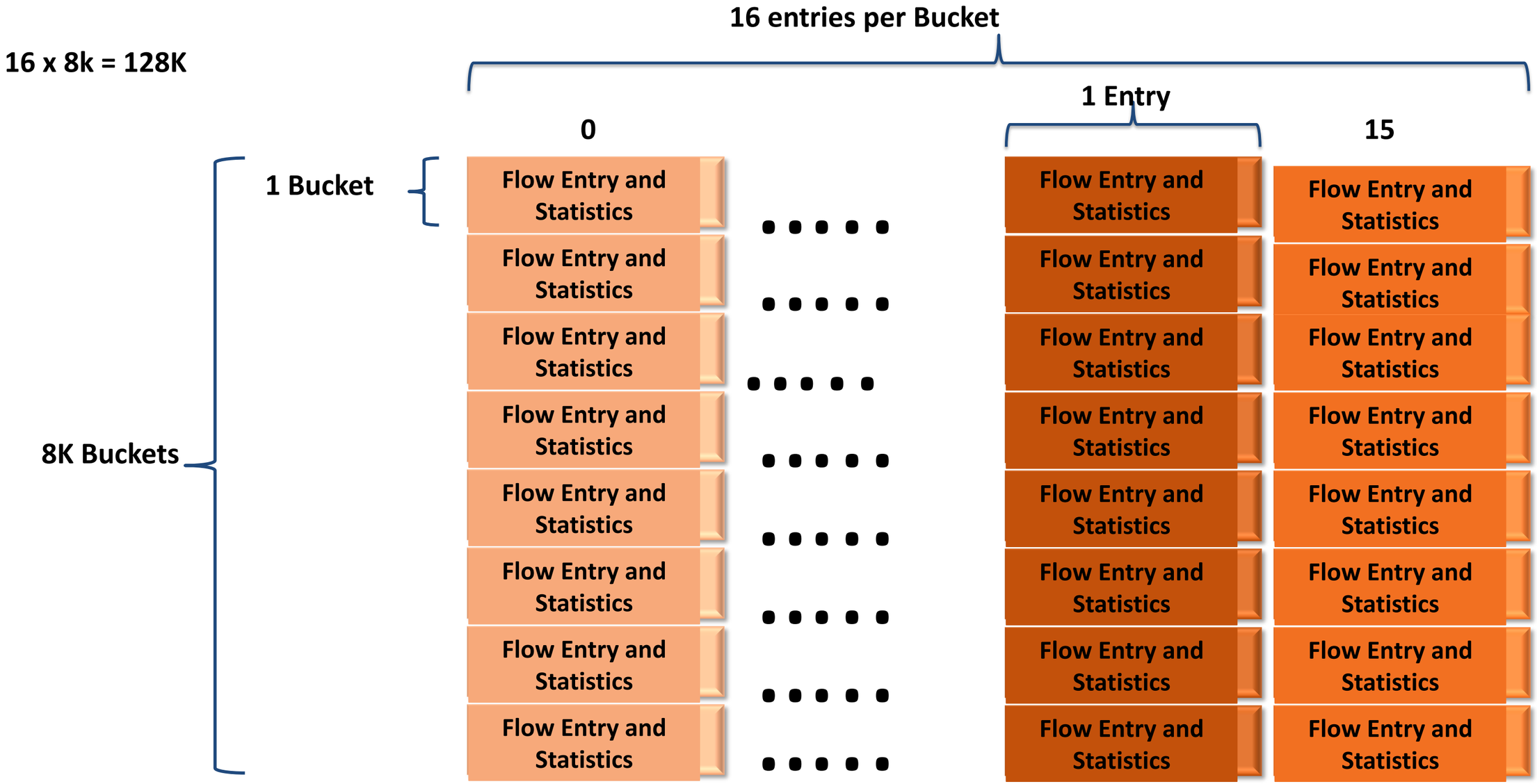
Supervisor 7-E: FE Block



NetFlow ASIC Architecture



NetFlow ASIC Architecture



Traditional NetFlow vs. Flexible NetFlow

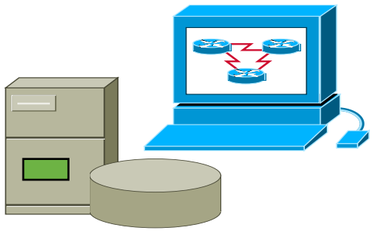
Traditional NetFlow

Fixed 7 keys

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	SrcPort	DstPort
Fa1/0	173.100.2	Fa0/0	10.0.227.1	11	00A2	00A2
Fa1/0	173.100.3	Fa0/0	10.0.227.1	6	15	15
Fa1/0	173.100.2	Fa0/0	10.0.227.1	11	00A1	00A1
Fa1/0	173.100.6	Fa0/0	10.0.227.1	6	19	19

NetFlow Cache

Export



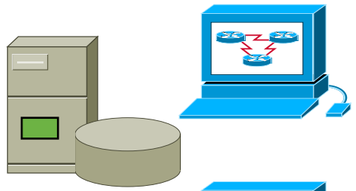
Flexible NetFlow

Flow Monitor 1

Flow cache 1

DstIPadd	Protocol	TOS
10.0.227.12	11	80
10.0.227.12	6	40
10.0.227.12	11	80
10.0.227.12	6	40

Export → Destination 1

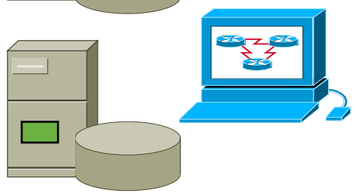


Flow Monitor 2

Flow cache 2

Protocol	TOS	Flgs
11	80	10
6	40	0
11	80	10
6	40	0

Export → Destination 2

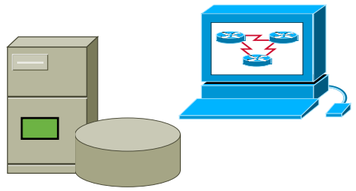


Flow Monitor 3

Flow cache 3

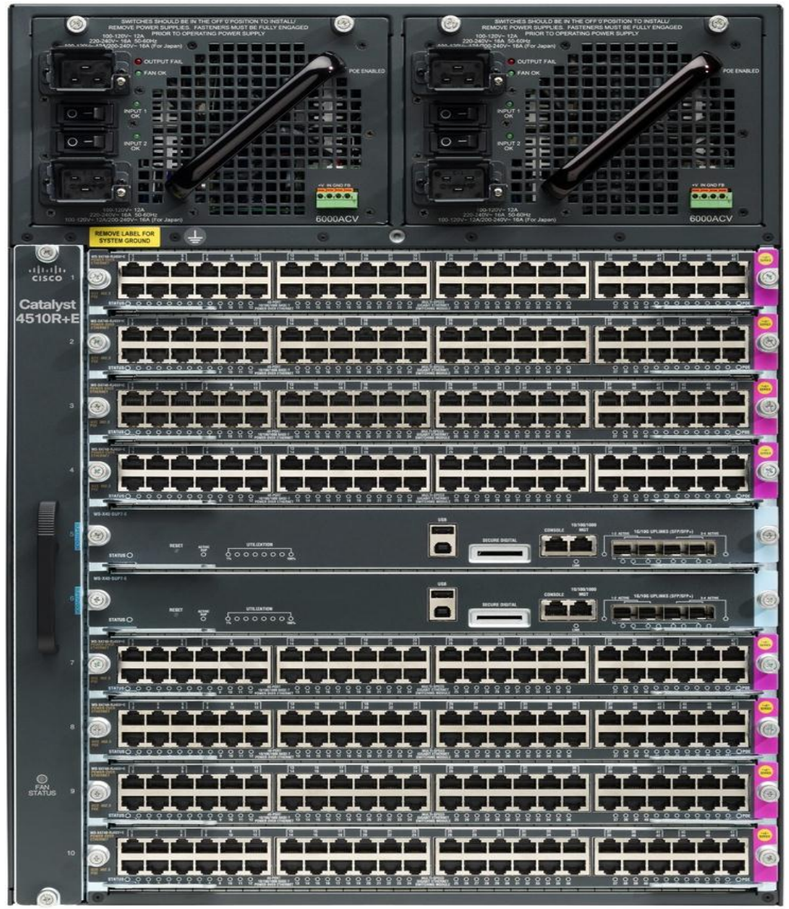
SrcIf	SrcIPadd	DstIf
Fa1/0	173.100.21.2	Fa0/0
Fa1/0	173.100.3.2	Fa0/0
Fa1/0	173.100.20.2	Fa0/0
Fa1/0	173.100.6.2	Fa0/0

Export → Destination 3



Virtual Cache For each monitor | **Only Interesting Information** | **Monitor Types of Protocols**

Flexible NetFlow on Catalyst 4500E



- System Scalability. Up to **~100K** (with 85% utilization efficiency) cached flows for Forwarding Engine
- Bridged NetFlow. Capability of creating and tracking bridged flows
- TCP Flags are now exported as part of the flow information. Very useful to understand TCP flow directions and to detect denial of service attacks
- Export version 9 (the most flexible) and version 5 (legacy)supported
- Flexible NetFlow CLI look & feel

Flexible NetFlow Record: Key Fields

Based on Catalyst 4500 Supervisor 7-E at FCS

Interface
Input

Layer 2
Dot1q priority
Dot1q Vlan ID
Source MAC address
Destination MAC address

IPv4
Source IP address
Destination IP address
Protocol
Precedence
DSCP
TTL
Total Length

IPv6
Source IP address
Destination IP address
Protocol
Traffic Class
Flow Label
Total Length
Extension Headers**
DSCP
Next-header*
Hop-Limit
Is-multicast

Transport
ICMP Code
ICMP Type
IGMP Type
TCP Source Port
TCP Destination Port
UDP Source Port
UDP Destination Port

--- New Key Fields in FnF

- Only first header is reported

** TBD

Flexible NetFlow Record: Non-Key Fields

Based on Catalyst 4500 Supervisor 7-E at FCS

Counters

- Bytes (32 bit counters)
- Bytes Long (64 bit counters)
- Packets (32 bit counters)
- Packets Long (64 bit counters)

Interface

- Output

IPv4

- TTL Minimum
- TTL Maximum
- Fragmentation Flags*
- ToS

Transport

- TCP Flags: ACK, FIN, PSH, RST, SYN, URG

Timestamp

- First Seen
- Last Seen

IPv6

- Total Length Minimum
- Total Length Maximum
- Option Header
- Hop-limit minimum
- Hop-limit maximum

Routing

- Forwarding Status
- Is-multicast

--- New Non-Key Fields in FnF

*more fragment fields

Flexible NetFlow Capabilities and Caveats

- User-defined flow records supported
- Per-port, Per-Vlan, Per-Port-Per-Vlan
- Supports 64 flow masks
- Two monitors (IPv4, and IPv6) can be applied simultaneously to one interface
- Cos/ToS, TTL, and interface option not supported in one flow record
- Flow-based QoS (UBRL) and FnF not supported on the same interface
- Match “interface out” option is not supported – instead use “collect interface out” for getting the Transmit/Egress interface information.

Flexible NetFlow Configuration Example

1

Configure the Flow Record

```
flow record my-app-traffic
  match transport tcp source-port
  match transport tcp destination-port
  match ipv4 source address
  match ipv4 destination address
  collect counter bytes
  collect counter packets
```

2

Configure the Exporter

```
flow exporter my-exporter
  destination 10.1.1.1
```

3

Configure the Flow Monitor

```
flow monitor my-monitor
  exporter my-exporter
  record my-app-traffic
```

4

Configure the Interface

```
Int gi1/1
  ip flow monitor my-monitor input
```

Top Talkers

- Top ten IP addresses that are sending the most packets

```
Switch# show flow monitor <monitor> cache
        aggregate ipv4 source address
        sort highest counter bytes top 10 format table
```

- Top five destination addresses to which we're routing most traffic from the 10.10.10.0/24 prefix

```
Switch# show flow monitor <monitor> cache
        filter ipv4 source address 10.10.10.0/24
        aggregate ipv4 destination address
        sort highest counter bytes top 5
```

- Top 20 sources of one-packet flows:

```
Switch# show flow monitor <monitor> cache
        filter counter packet 1
        aggregate ipv4 source address
        sort highest counter flows top 20
```

Embedded Event Manager 3.2
Flexible NetFlow Event Detector

```
flow record <my-record>
        match ipv4 ttl
        match ipv4 source address
        match ipv4 destination address

flow monitor <my-monitor>
        record <my-record>
```

```
event manager applet security-applet
        event nf monitor-name "<my-monitor>" event-type create event1
entry-value “2" field ipv4 ttl entry-op lt    action 1.0 syslog msg
"Flow Monitor $_nf_monitor_name reported Low TTL for
$_nf_source_address to $_nf_dest_address"
```

```
Mar 18 22:15:08.036: %HA_EM-6-LOG: ttl: Flow Monitor ttl reported Low
TTL for 10.1.3.2 to 10.1.3.102
```

Embedded Event Manager 3.2
Flexible NetFlow Event Detector

```
flow record rate
 match ipv4 source address
 match ipv4 destination address
 collect counter packets

flow monitor <my-monitor>
        record <my-record>
```

```
 event nf monitor-name "rate" event-type update event1 entry-value
"10000" field counter packets rate-interval 15 entry-op gt event2
entry-value "10.1.3.102" field ipv4 destination address entry-op eq
 action 1.0 syslog msg "Flow Monitor $_nf_monitor_name reported
Unusually High Rate of traffic to $_nf_dest_address from
$_nf_source_address"
```

```
Mar 18 22:17:13.033: %HA_EM-6-LOG: rate: Flow Monitor rate reported
Unusually High Rate of traffic to 10.1.3.102 from 10.1.3.2
```

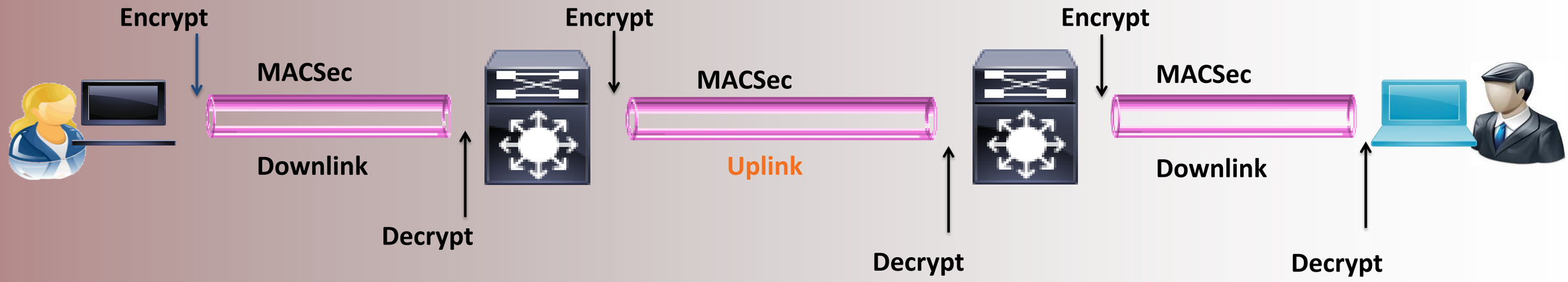
More info on NetFlow

BRKNMS-3132 Advanced NetFlow

Agenda

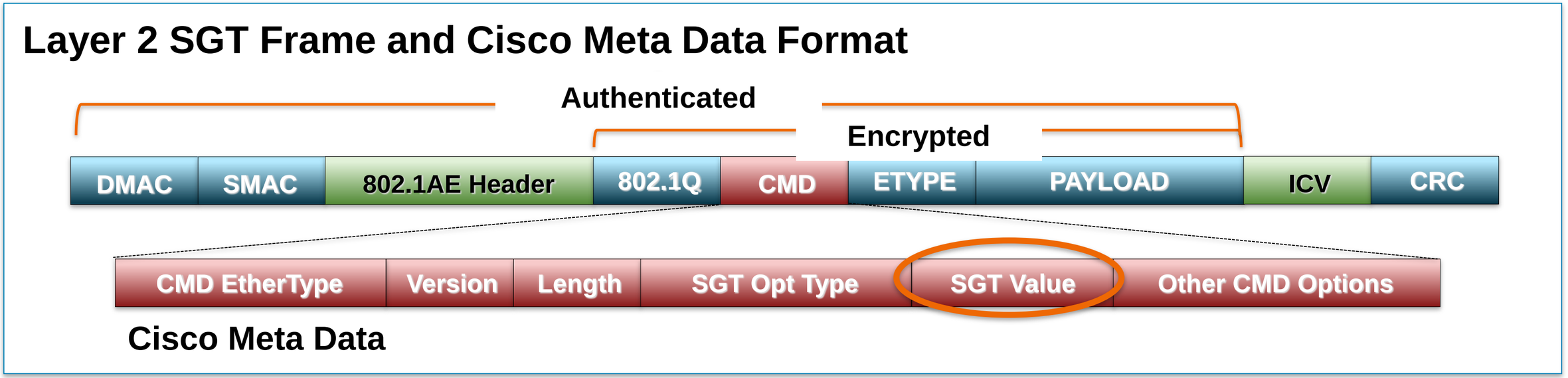
- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and Packet walk
- Quality of Service Overview
- Flexible NetFlow
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

What is MACSec?



- Encryption mitigates packet eavesdropping, tampering, and injection
- Supports 802.1AE-based strong encryption technology
  - 128-bit AES-GCM, NIST-approved, 10Gb line-rate encryption
- Hop-by-hop encryption supports data and packet inspection
- Works in shared media environments (IP Phones, Desktops)

MACSec Frame



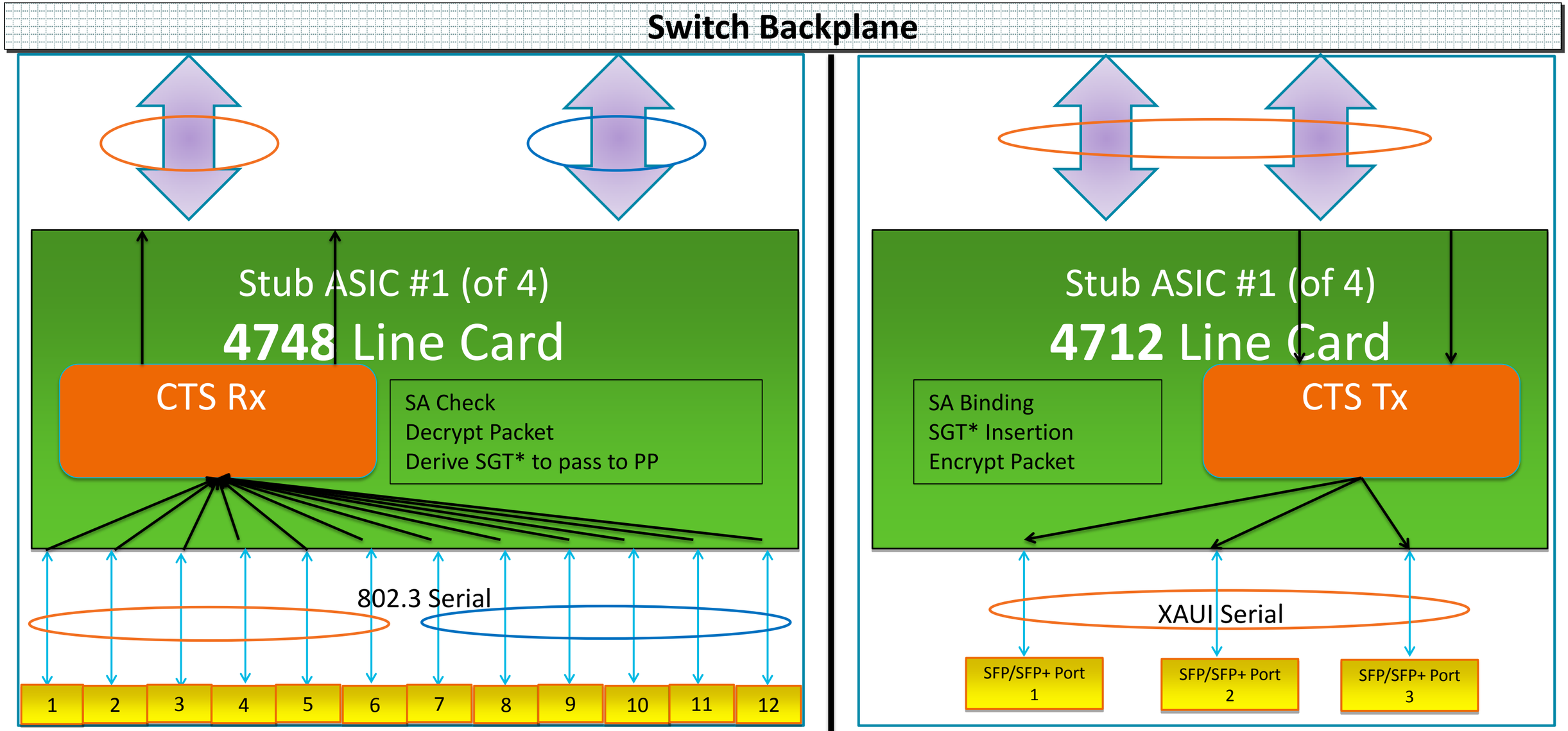
- 802.1AE Header | CMD | ICV — the L2 802.1AE + TrustSec overhead (=~40bytes)
- Tagging process prior to other L2 service such as QoS
- SGT namespace is managed on central policy server (ACS 5.x, or ISE)
- No impact IP MTU/Fragmentation.

Normal Ethernet Frame

More info about TrustSec

- BRKSEC-2046 Cisco Trustsec and Security Group Tagging
- BRKSEC-2050 Secure Mobility

MACSec: Under the covers



How To Deploy Downlink MACSec Switch Configurations

Global Configuration Commands:

```
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
!
dot1x system-auth-control
!
radius-server host 10.3.1.21 key XxXxXxXxXx
radius-server vsa send authentication
```

How To Deploy Downlink MACSec Switch Configurations

Interface Configuration Commands:

```
interface GigabitEthernet4/1
 description AnyConnect Interface to MACSEC XP 1
 switchport access vlan 903
 switchport mode access
 mtu 9198
 logging event link-status
 authentication priority dot1x
 authentication port-control auto
 macsec
 dot1x pae authenticator
 mka default-policy
 spanning-tree portfast
 authentication linksec policy should-secure
```

Default is “should-secure”, other options are “must-not-secure” and “must-secure”

How to Deploy Downlink MACSec
Difference from “Just Dot1X”

```
RAFALE#show authentication session interface gigabitEthernet 4/1
            Interface:  GigabitEthernet4/1
          MAC Address:  0050.569c.0008
           IP Address:  10.3.1.200
            User-Name:  cisco
               Status:  Authz Success
               Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
      Authorized By:  Authentication Server
        Vlan Policy:  N/A
     Session timeout:  N/A
       Idle timeout:  N/A
   <snip……snip>

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

How to Deploy Downlink MACSec
After the fact

```
RAFALE#show authentication session interface gigabitEthernet 4/1
            Interface:  GigabitEthernet4/1
          MAC Address:  0050.569c.0008
           IP Address:  10.3.1.200
            User-Name:  blackbird
               Status:  Authz Success
               Domain:  DATA
     Security Policy:  Must Secure
     Security Status:  Secured
      Oper host mode:  single-host
    Oper control dir:  both
      Authorized By:  Authentication Server
        Vlan Policy:  N/A
     Session timeout:  N/A
       Idle timeout:  N/A
   <snip……snip>

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

How To Deploy Uplink MACSec
Switch Configurations

Interface Configuration Commands on back-to-back connected interfaces:

```
interface GigabitEthernet3/2
switchport mode trunk
cts manual
no propagate sgt
sap pmk 12345678 mode-list gcm-encrypt
end
!
Switch#show cts interface summary
Global Dot1x feature is Disabled
CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache
-------------------------------------------------------------
Gi3/2      MANUAL  OPEN      unknown    unknown    invalid

CTS Layer3 Interfaces
---------------------
Interface   IPv4 encap       IPv6 encap       IPv4 policy      IPv6 policy
-------------------------------------------------------------------------
```

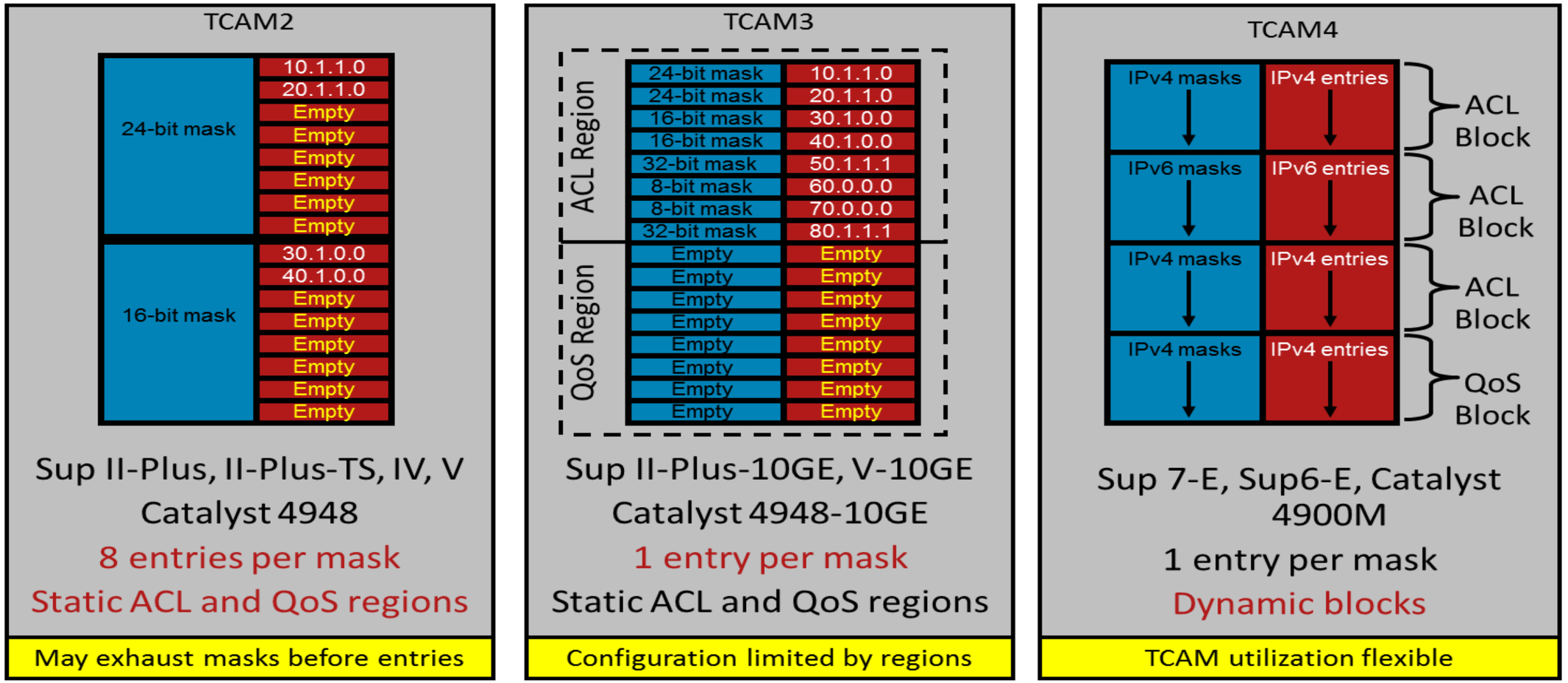
Agenda

- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and Packet walk
- Quality of Service Overview
- Flexible NetFlow
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

TCAM Overview

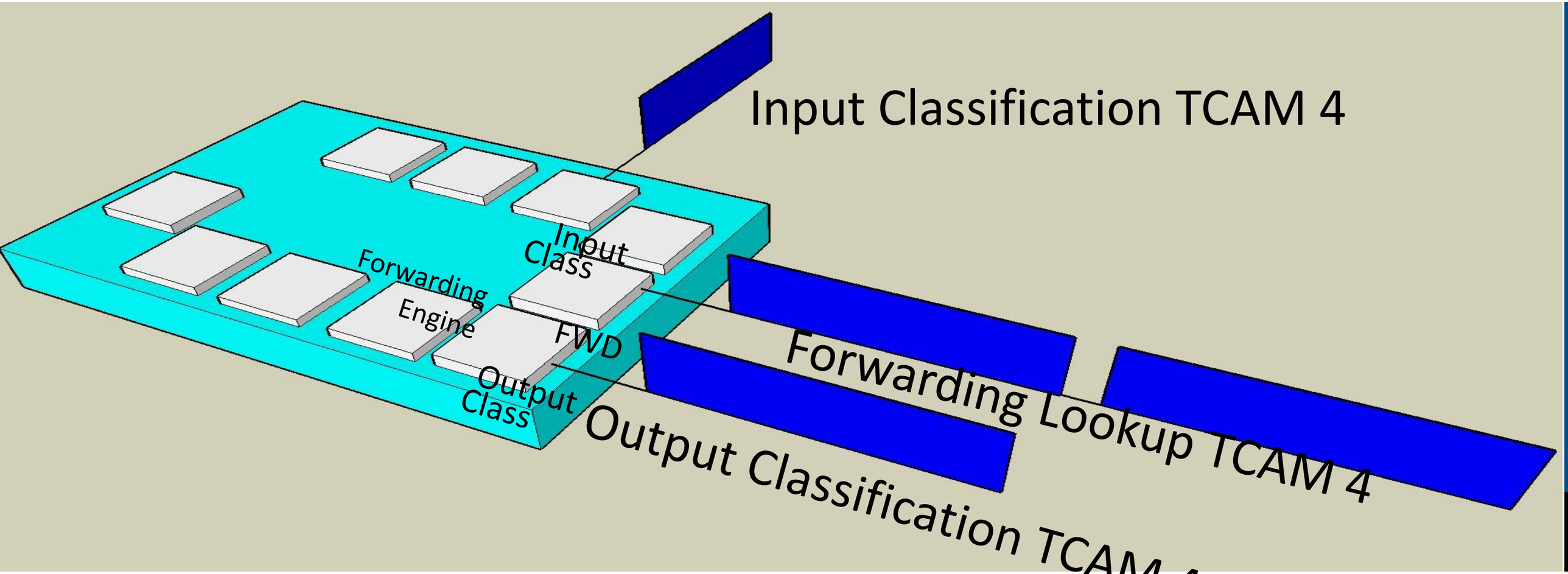
Ternary Content Addressable Memory

Stores ACLs, QoS policies, and L3 forwarding information*



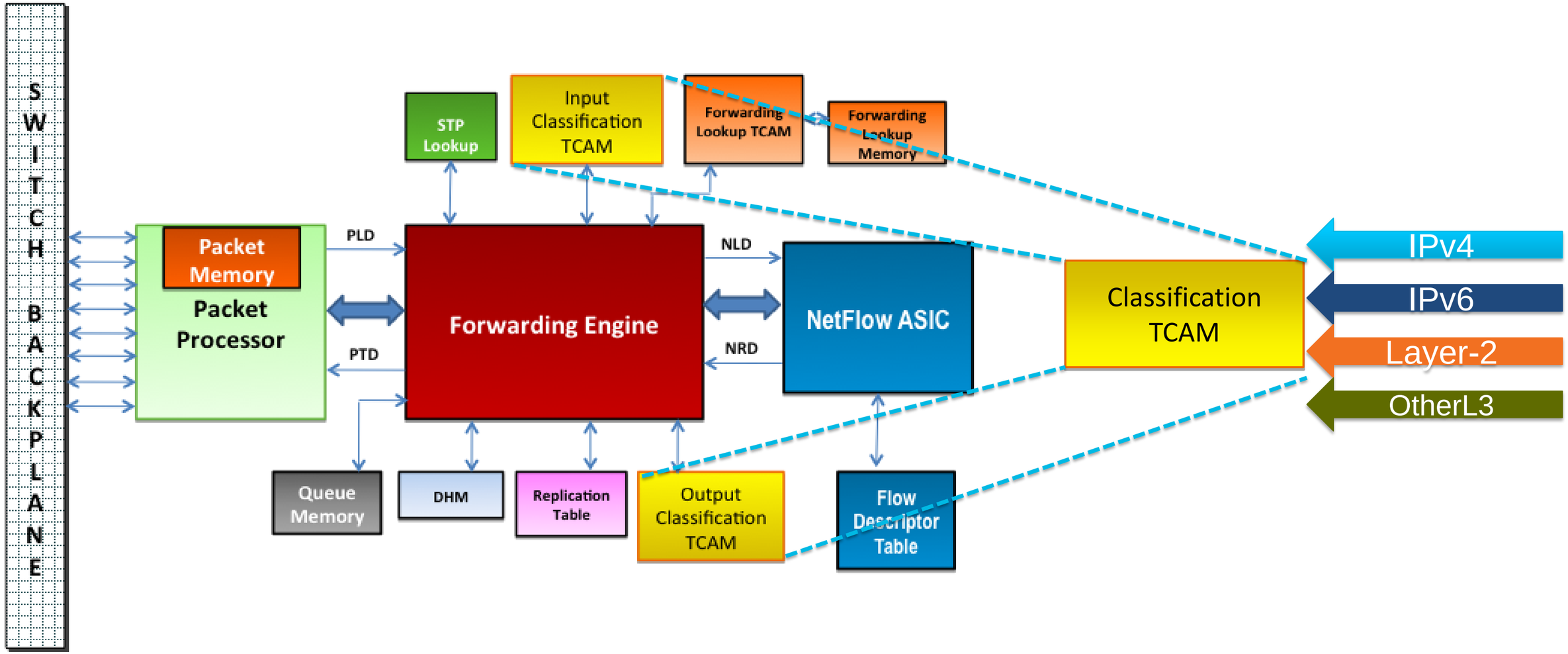
* Not shown

TCAM 4 Layout

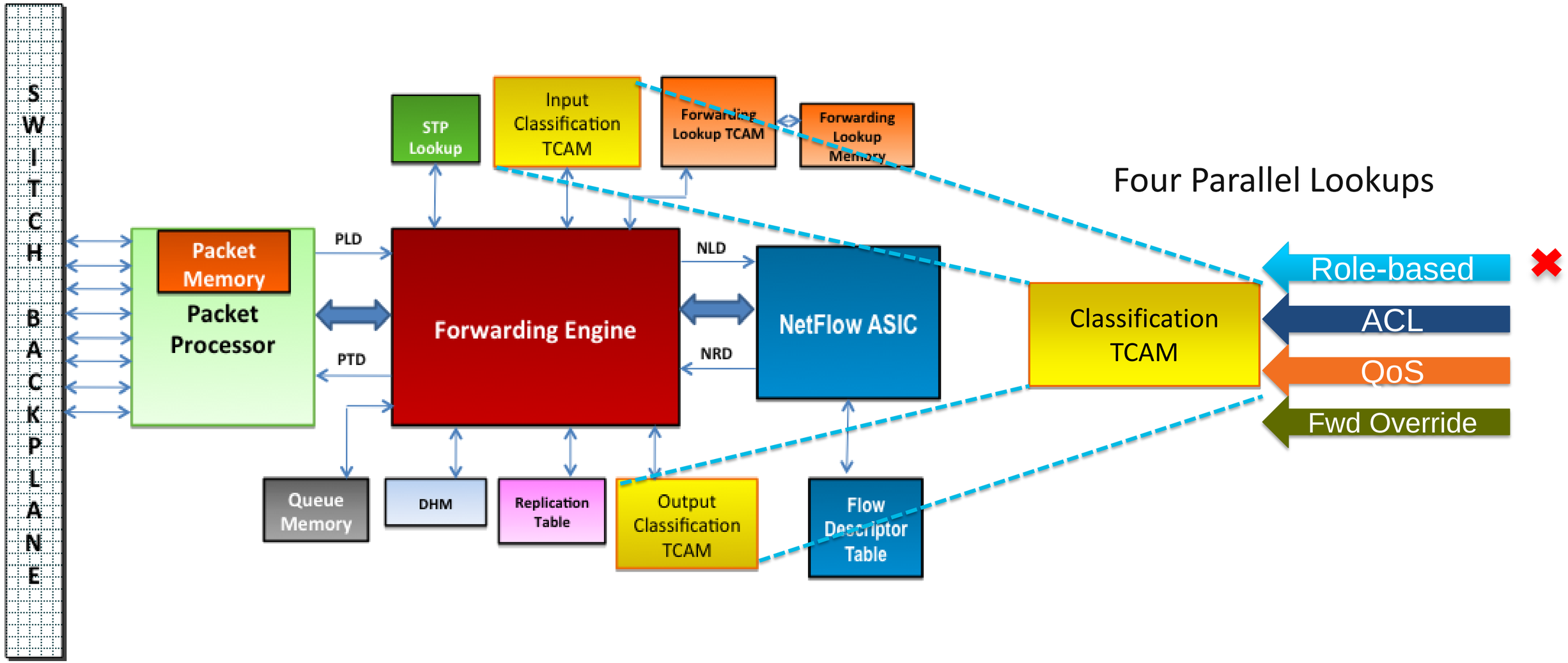


- 256K IPv4 routes, 128K IPv6 routes
- 64K Security/QoS each direction

Packet Types

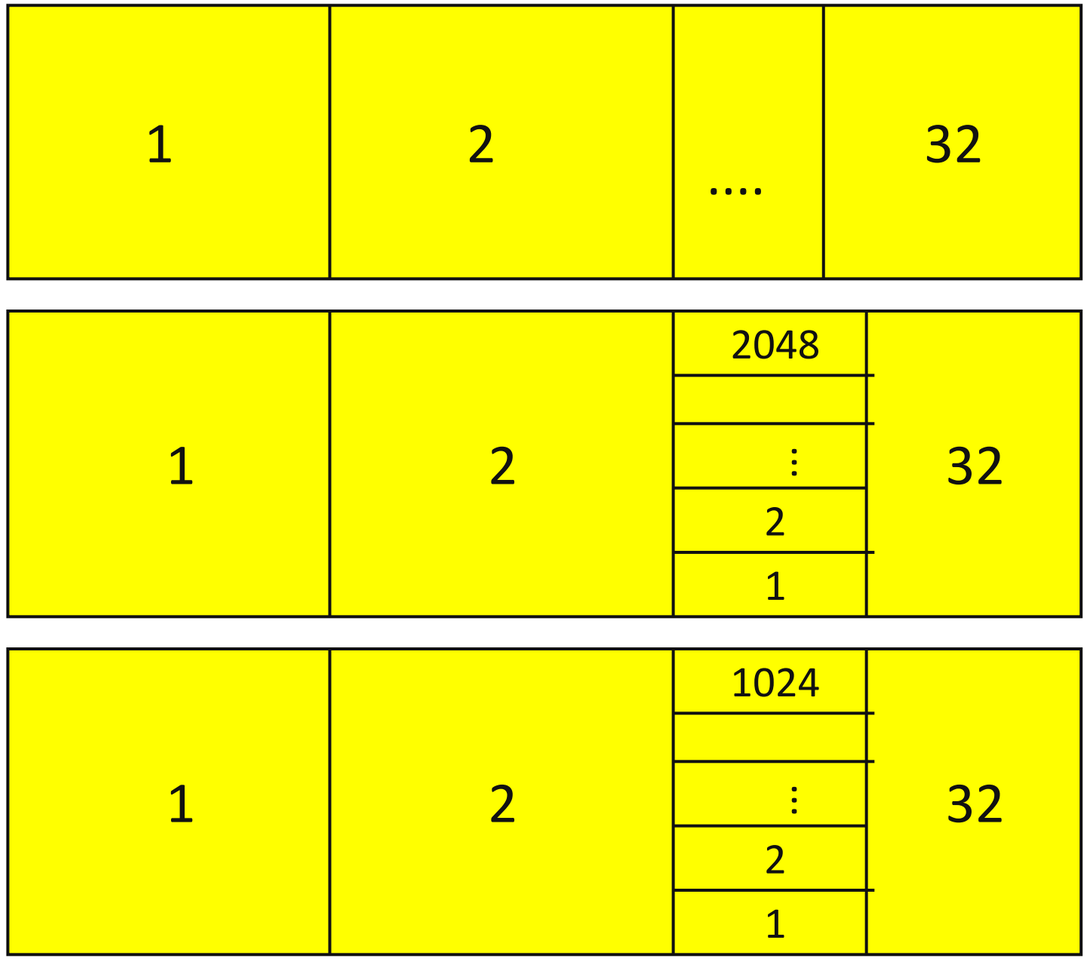


Lookup Types



TCAM Blocks

Each Classification TCAM4 has 32 Blocks

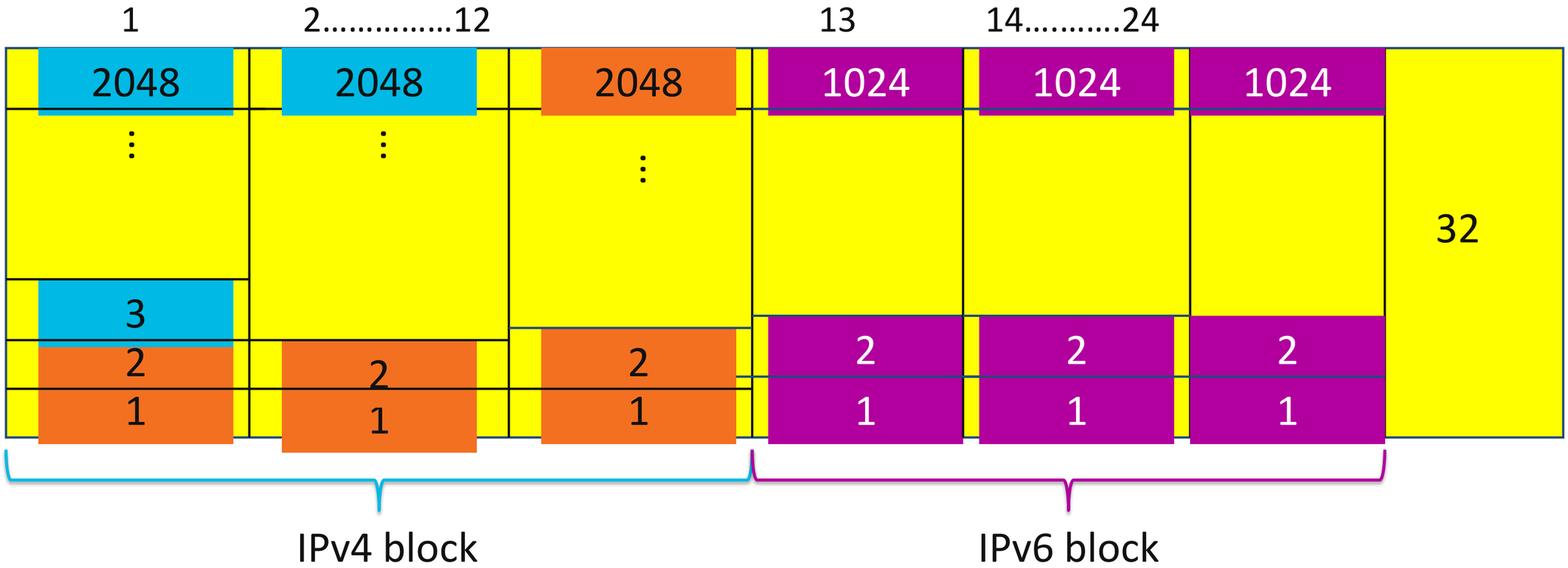


160-bit wide for IPv4
Max is 64K entries

320-bit wide for IPv6
Max is 32K entries

Shared across all packet types

Restricted Block Usage



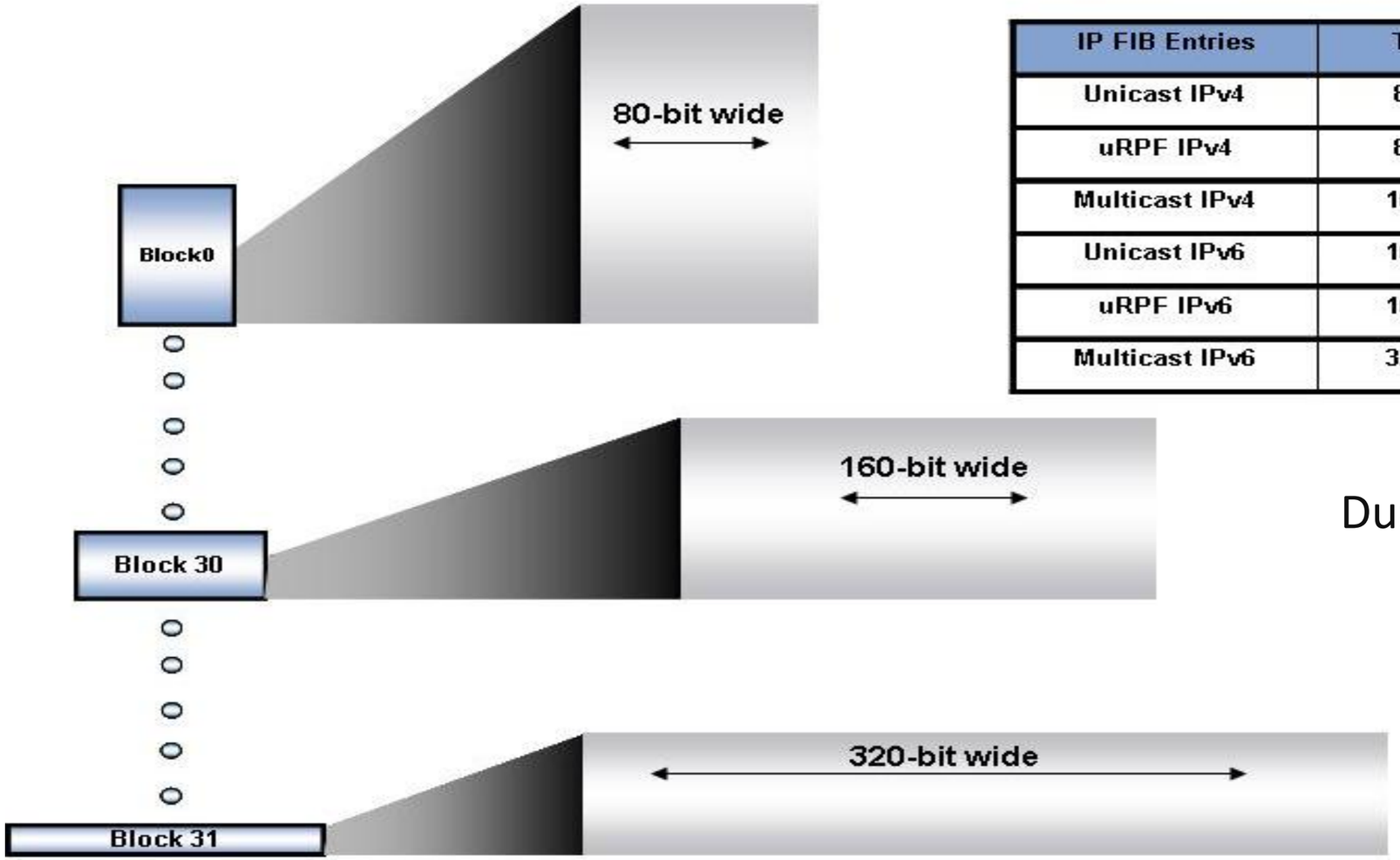
Maximum is 12 blocks

- Maximum number of Access Control Entries (ACE) in all policies combined on a single ACL path cannot exceed 24K ACEs
- IPv6 ACEs are double the width of IPv4; you cannot have an IPv6 ACL with more than 12K ACEs

Agenda

- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and Packet walk
- Quality of Service Overview
- Flexible NetFlow
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

TCAM4 Forwarding Blocks



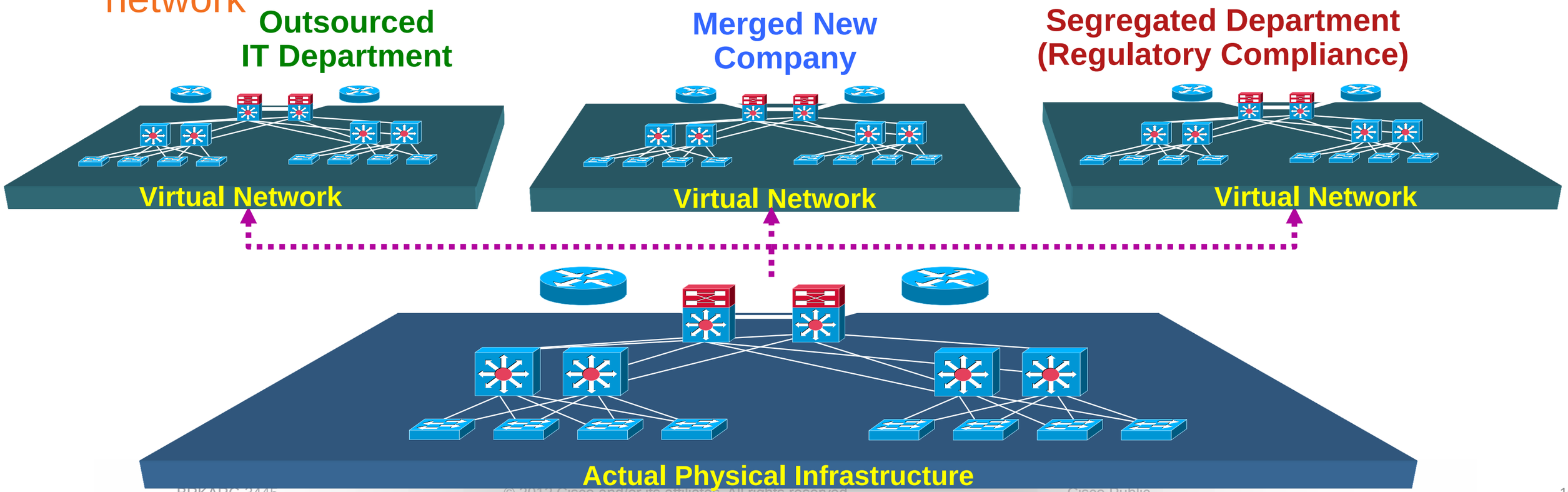
IP FIB Entries	TCAM Mode	Entries / Block
Unicast IPv4	80-bit mode	4000
uRPF IPv4	80-bit mode	4000
Multicast IPv4	160-bit mode	2000
Unicast IPv6	160-bit mode	2000
uRPF IPv6	160-bit mode	2000
Multicast IPv6	320-bit mode	1000

Dual Forwarding CAMs provide 64 blocks to
store IPv4 and IPv6 Unicast
Multicast Routes -
256,000 IPv4 Routes
128,000 IPv6 Routes

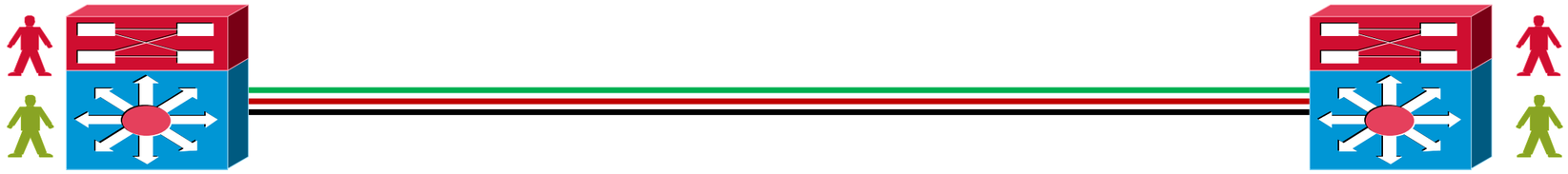
Optimized Space Allocation for IPv4 and IPv6 Configurations!
Hardware Support for IPv6

Network Virtualization

- Creation of Logical Partitions
  - Virtualization: one-to-many (one network supports many virtual networks)
  - End-user perspective is that of being connected to a dedicated network (security, independent set of policies, routing decisions…)
  - Must have a rock-solid campus design in place before adding virtualization to the network



EVN Trunk Configuration



VRF-Lite Subinterface Config

```
interface TenGigabitEthernet1/1
 ip address 10.122.5.1 255.255.255.252
 ip pim query-interval 1
 ip pim sparse-mode
 logging event link-status

interface TenGigabitEthernet1/1.101
 description Subinterface for Red VRF
 encapsulation dot1Q 101
 ip vrf forwarding red
 ip address 10.122.5.1 255.255.255.252
 ip pim query-interval 1
 ip pim sparse-mode
 logging event subif-link-status

interface TenGigabitEthernet1/1.102
 description Subinterface for Green VRF
 encapsulation dot1Q 102
 ip vrf forwarding green
 ip address 10.122.5.1 255.255.255.252
 ip pim query-interval 1
 ip pim sparse-mode
 logging event subif-link-status
```

VNET Trunk config

```
interface TenGigabitEthernet1/1
 vnet trunk
 ip address 10.122.5.2 255.255.255.252
 ip pim query-interval 1
 ip pim sparse-mode
 logging event link-status
```

Both routers have VRFs defined
VNET router has tags

Global Config:

```
vrf definition red
 vnet tag 101

vrf definition green
 vnet tag 102
```

EVN – Show ip int brief

```
vrf definition red
 vnet tag 101

vrf definition green
 vnet tag 102
!
interface Ethernet1/0
 vnet trunk
 ip address 10.1.95.1 255.255.255.0
!
interface Ethernet2/0
 vnet trunk
 ip address 10.1.96.1 255.255.255.0
```

show ip int brief - displays all subinterfaces

```
Router# show ip int brief
Interface              IP-Address      OK?  Method  Status     Protocol
Ethernet1/0            10.1.95.1       YES  NVRAM     up           up
Ethernet1/0.101        10.1.95.1       YES  NVRAM     up           up
Ethernet1/0.102        10.1.95.1       YES  NVRAM     up           up
.
Ethernet2/0            10.1.96.1       YES  NVRAM     up           up
Ethernet2/0.101        10.1.96.1       YES  NVRAM     up           up
Ethernet2/0.102        10.1.96.1       YES  NVRAM     up           up
```

VRF Shared Services

Before: Sharing services in existing technologies

```
ip vrf SHARED
 rd 3:3
 route-target export 3:3
 route-target import 1:1
 route-target import 2:2
!
ip vrf RED
 rd 1:1
 route-target export 1:1
 route-target import 3:3
!
ip vrf GREEN
 rd 2:2
 route-target export 2:2
 route-target import 3:3
!
router bgp 65001
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf SHARED
 redistribute ospf 3
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf RED
 redistribute ospf 1
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf GREEN
 redistribute ospf 2
 no auto-summary
 no synchronization
 exit-address-family
!
```

After: Simple shared service definition

```
vrf definition SHARED
  address-family ipv4
   route-replicate from vrf RED unicast all route-map red-map
   route-replicate from vrf GREEN unicast all route-map grn-map
```

```
vrf definition RED
  address-family ipv4
   route-replicate from vrf SHARED unicast all
```

```
vrf definition GREEN
  address-family ipv4
   route-replicate from vrf SHARED unicast all
```

Route-Replication Advantage:

- No BGP required
- No Route Distinguisher required
- No Route Targets required
- No Import/Export required
- Simple Deployment
- Supports both Unicast/Mcast

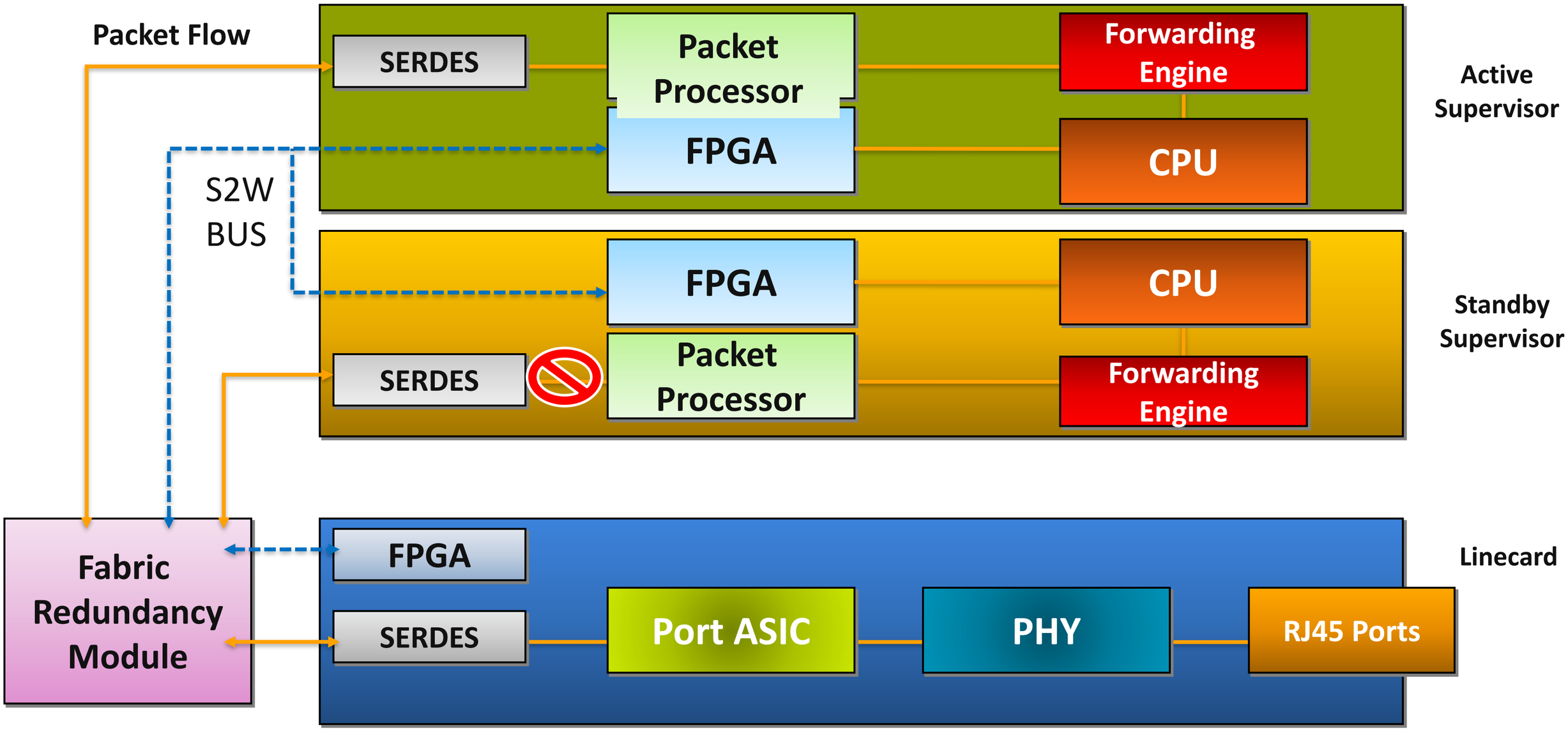
More Information about EVN

- BRKCRS-2034 - Case Study in Network Infrastructure Virtualization
- BRKCRS-2035 - Simplifying Campus Network Virtualization with EVN

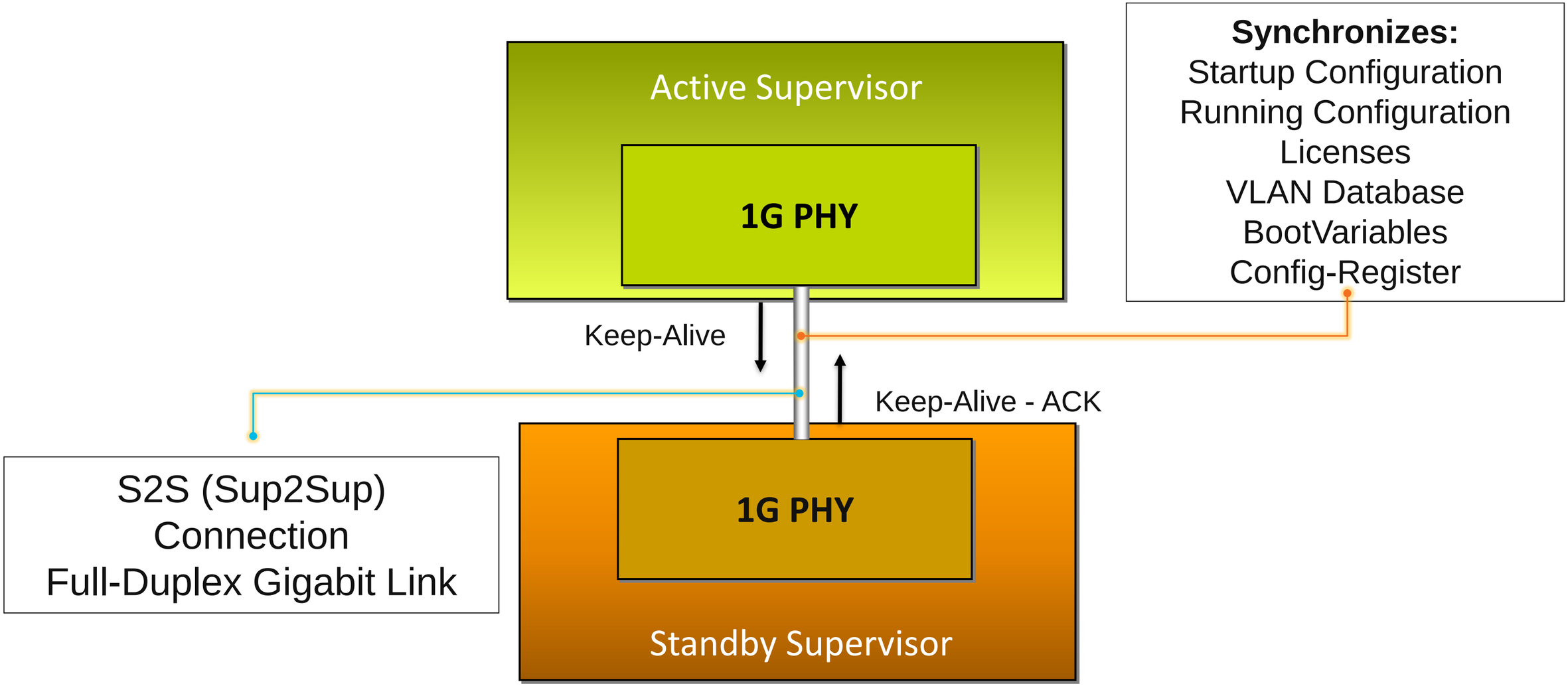
Agenda

- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and Packet walk
- Quality of Service Overview
- Flexible NetFlow
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

Chassis + Sup–Packet Flow



Redundant Supervisor Communication



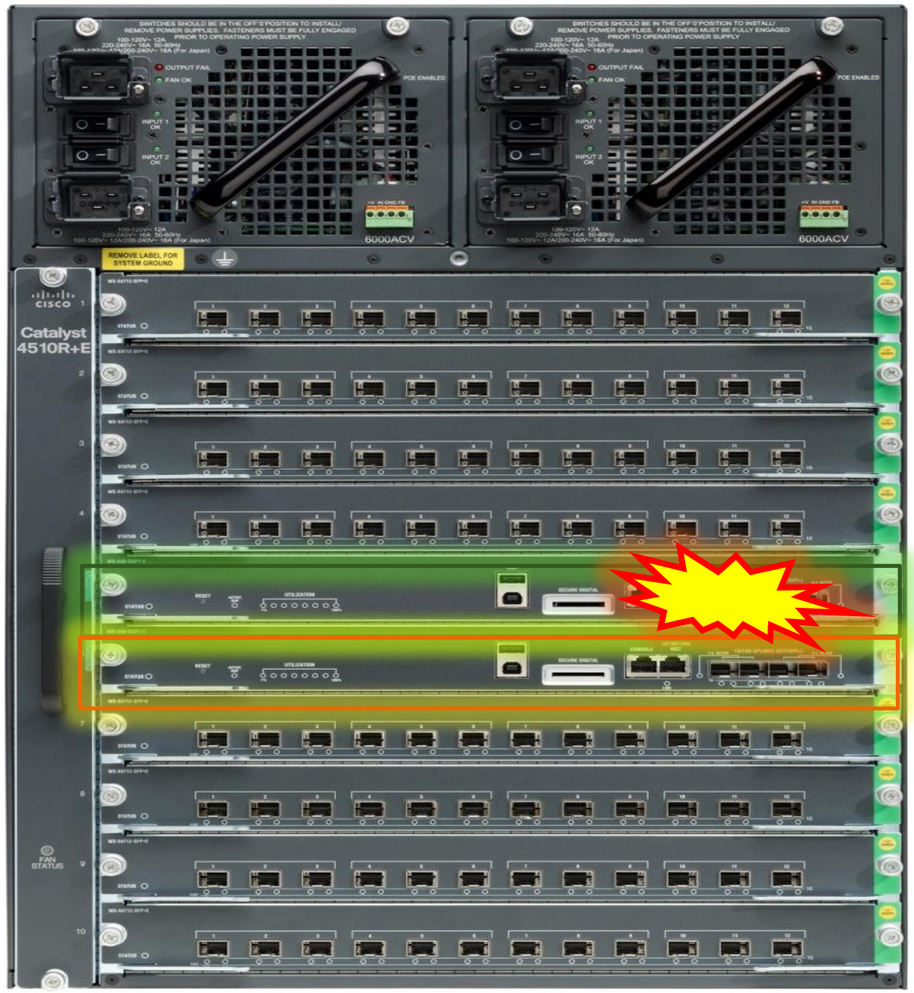
Redundant Supervisor Uplinks

Active Ports

Inactive Ports

SSO–Stateful SwitchOver

SSO allows Redundant Supervisors to run a stateful IOS and stateful applications to exchange state in order to minimize outage at the time of switchover from Active to Standby Supervisor.



SSO – supported in Cisco IOS Release 12.2(46)SG with Sup6-E, and now with Sup7-E

Default Redundancy Mode – Redundant Supervisor fully initialized

Upon Switchover **Physical Links stay up** - Protocols do not reset

Traffic Interruption: **Sub-Second (<150ms)**

IOS Images need to be identical

Redundancy Configuration Status - SSO

```
Switch#show module
Chassis Type : WS-C4510R+E
Power consumed by backplane : 40 Watts
Mod Ports Card Type                                  Model               Serial No.
---+-----+--------------------------------------+------------------+-----------
 2    48  10/100/1000BaseT Premium POE E Series  WS-X4748-RJ45V+E   CAT1418L036
 3    48  10/100/1000BaseT Premium POE E Series  WS-X4748-RJ45V+E   CAT1352L00L
 4    48  10/100/1000BaseT Premium POE E Series  WS-X4748-RJ45V+E   CAT1352L00Y
 5     4  Sup 7-E 10GE (SFP+), 1000BaseX (SFP)   WS-X45-SUP7-E      CAT1418L08C
 6     4  Sup 7-E 10GE (SFP+), 1000BaseX (SFP)   WS-X45-SUP7-E      CAT1418L08R
 7    12  10GE SFP+                              WS-X4712-SFP+E     CAT1413L01G
 8    48  10/100/1000BaseT Premium POE E Series  WS-X4748-RJ45V+E   CAT1352L030
 9    48  10/100/1000BaseT Premium POE E Series  WS-X4748-RJ45V+E   CAT1418L03A

 M MAC addresses                       Hw   Fw           Sw                Status
--+---------------------------------+---+------------+-----------------+---------
 2 0026.9927.eaa0 to 0026.9927.eacf 0.4                                    Ok
 3 0026.9927.c9a0 to 0026.9927.c9cf 0.3                                    Ok
 4 0026.9927.cc10 to 0026.9927.cc3f 0.3                                    Ok
 5 c47d.4f81.8a40 to c47d.4f81.8a43 0.8 15.0(1r)SG(0 03.00.00.1.66         Ok
 6 c47d.4f81.8a44 to c47d.4f81.8a47 0.8 15.0(1r)SG(0 03.00.00.1.66         Ok
 7 0026.0b79.7469 to 0026.0b79.7474 0.4                                    Ok
 <snip…..snip>

Mod  Redundancy role     Operating mode      Redundancy status
----+------------------+------------------+------------------------------
 5   Active Supervisor   SSO                 Active
 6   Standby Supervisor  SSO                 Standby hot
```

Redundancy Configuration Status - SSO

```
Switch#show redundancy states
          my state = 13 -ACTIVE
         peer state =  8 -STANDBY HOT
               Mode = Duplex
               Unit = Primary
            Unit ID = 5

     Redundancy Mode (Operational) = Stateful Switchover
      Redundancy Mode (Configured) = Stateful Switchover
                Redundancy State = Stateful Switchover
                    Manual Swact = enabled

      Communications = Up

        client count = 64
      client_notification_TMR = 240000 milliseconds
               keep_alive TMR = 9000 milliseconds
            keep_alive count = 0
       keep_alive threshold = 18
               RF debug mask = 0
```

SSO-Aware Features

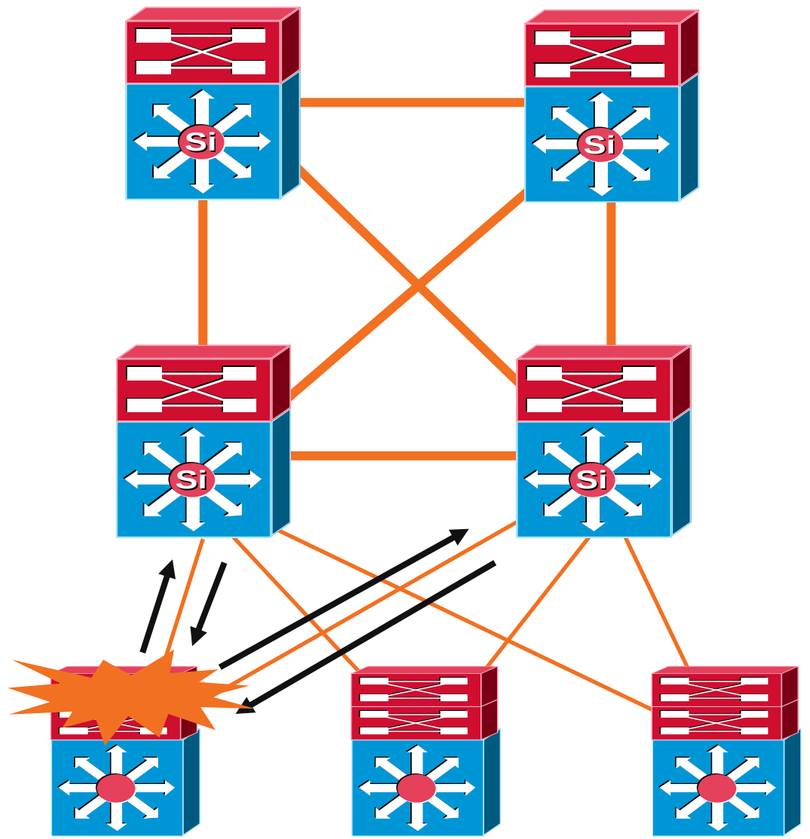
SSO supports stateful switchover of the following Layer 2 features. The state of the features are preserved between both Active and Standby Supervisor Engines

Non-Exhaustive list of SSO-Aware Features			
802.3	802.1p	VTP	HSRP
802.3u	802.1q	Dynamic ARP Inspection	MST/ PVST+
802.3x	802.1X	DHCP Snooping	Rapid-PVST
802.3ab	802.1D	IP Source Guard	Spanning Tree Toolkit
CDP / LLDP	802.3af	IGMP Snooping v1 / v2	Voice VLAN
802.3ad	PAgP	DTP (802.1q and ISL)	Port Security
Unicast MAC Filtering	ACL (VACLs, PACLs, RACLs)	Multicast/Broadcast Storm Control	QoS (DBL)

System High Availability

NSF Recovery (Routing Protocol Recovery)

- Non-Stop Forwarding (NSF) provides the capability for the routing protocols to gracefully restart after an SSO fail-over
- The newly active redundant supervisor continues forwarding traffic using the synchronized
HW forwarding tables
- The NSF capable Routing Protocol requests a graceful neighbor start
- Routing neighbors reform
with no loss of traffic



No Route Flaps During Recovery

Enabling NSF Configuration–Routing

```
Switch(config)#router eigrp 100
Switch(config-router)#nsf
Switch(config-router)#timers nsf ?
  converge    EIGRP time limit for convergence after switchover
  route-hold  EIGRP hold time for routes learned from nsf peer
  signal      EIGRP time limit for signaling NSF restart
```

EIGRP Example

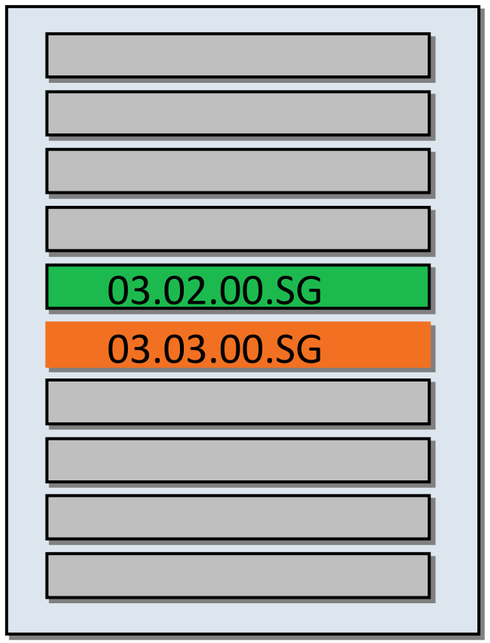
```
Switch(config)#router ospf 100
Switch(config-router)#nsf ?
  cisco  Cisco Non-stop forwarding
  ietf   IETF graceful restart

Switch(config-router)#nsf cisco ?
  enforce  Cancel NSF restart when non-NSF-aware neighbors detected
  helper   helper support

Switch(config-router)#nsf ietf ?
  helper            helper support
  restart-interval  Graceful restart interval
```

OSPF Example

```
Switch(config-router)#bgp graceful-restart ?
  restart-time    Set the max time needed to restart and come back up
  stalepath-time  Set the max time to hold onto restarting peer's stale paths
```

BGP Example

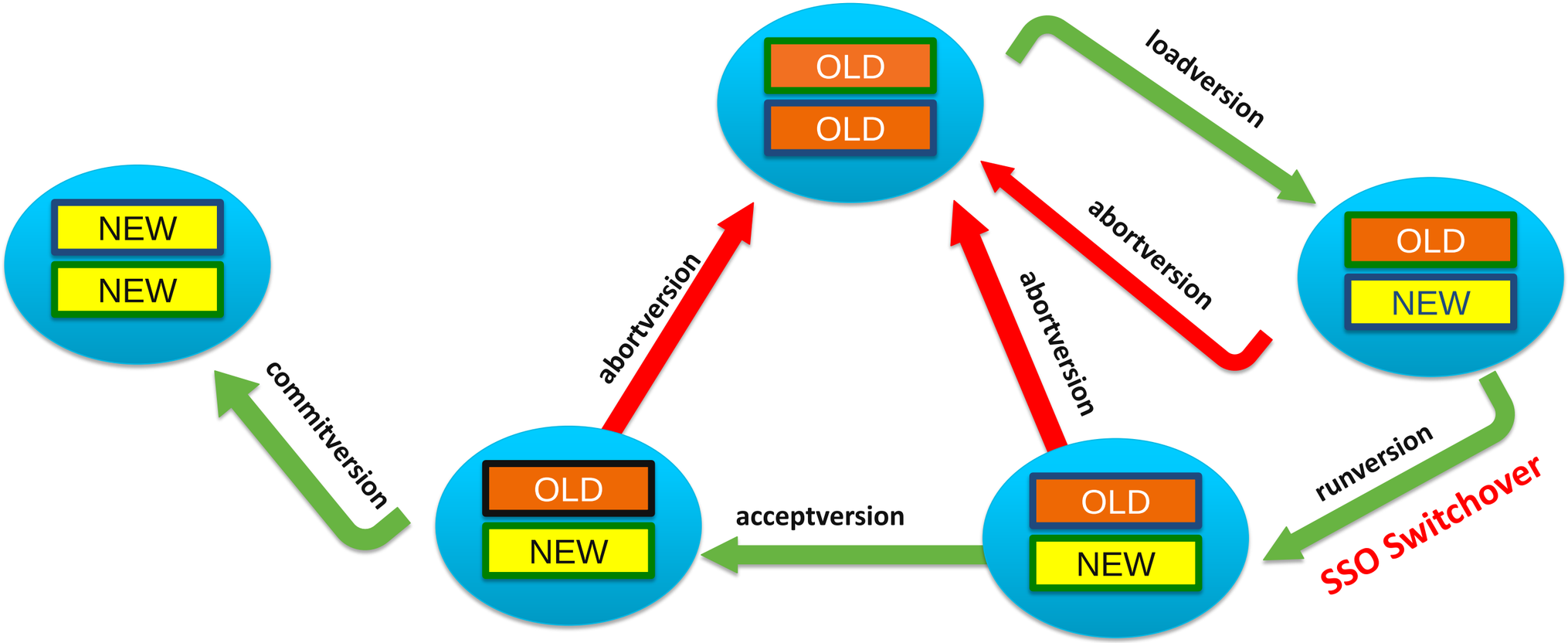
Catalyst 4500–In Service Software Upgrade



Targets Planned Downtime
Due to Software Upgrades

- Software Maintenance Windows are significant case of downtime
- On redundant systems, the ISSU process allows the running IOS software to be upgraded while packet forwarding continues
- ISSU mechanism leverages architecture for High Availability
  - NSF / SSO
- Catalyst 4500 utilizes full image upgrades for the addition of new features, defects, and PSIRTs
- Increases network availability and reduces downtime caused by planned upgrades

In Service Software Upgrade Process



There is a 4-Step Traditional Method:

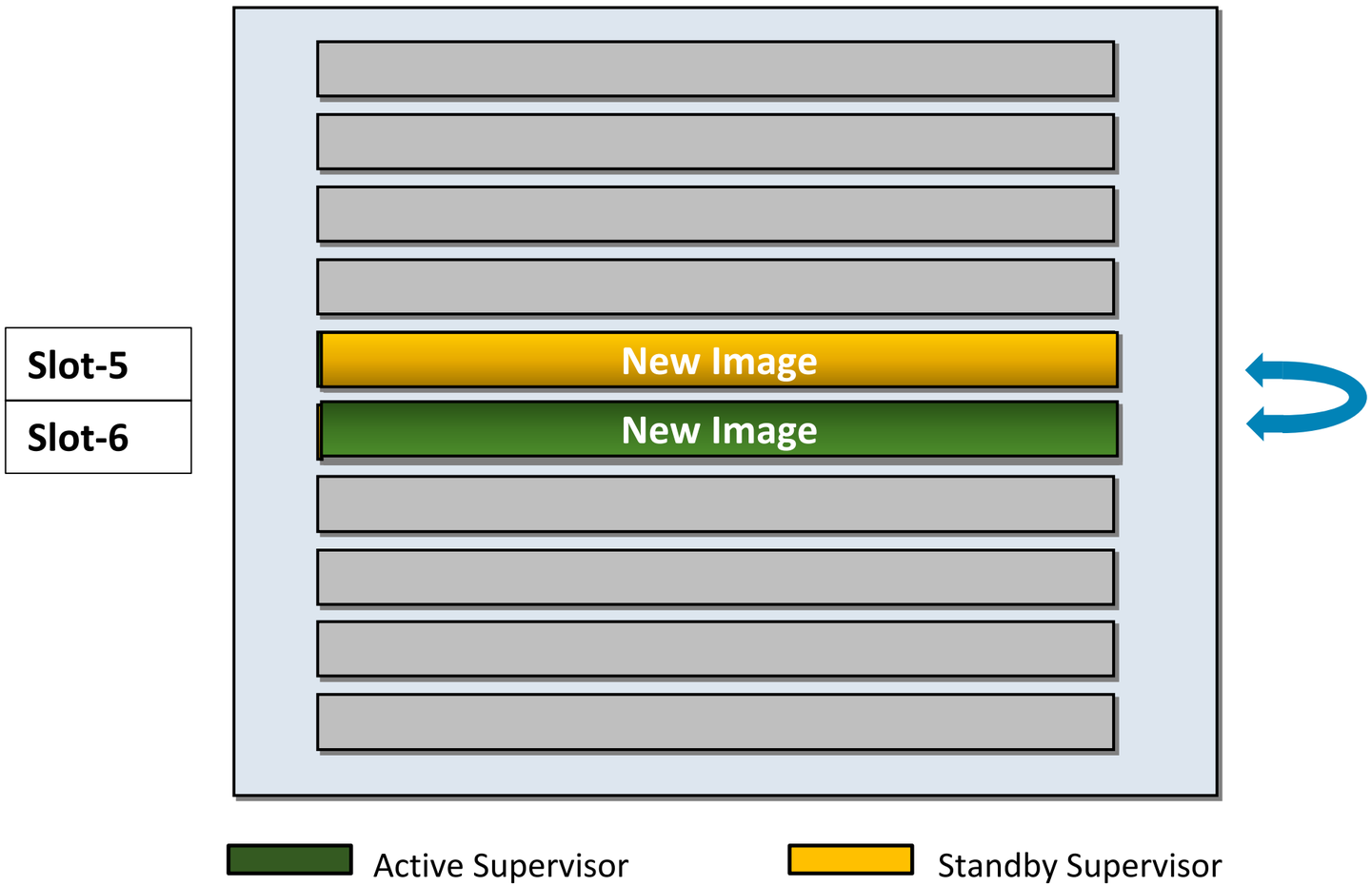
- Load Version
- Run Version
- Accept Version
- Commit Version

Active

Standby

Supervisor 7-E – Single Line ISSU

issu changeversion bootflash:New_Image quick



Standby Supervisor in Slot-6 is Reset and…..

Boots with New Image

Initiate SSO Switchover between Active Supervisor in Slot-5 and Standby Supervisor in Slot-6

Active Supervisor in Slot-5 resets

Standby Supervisor in Slot-6 takes over as Active Supervisor

Supervisor in Slot-5 boots up as a Standby Supervisor with the New_Image……

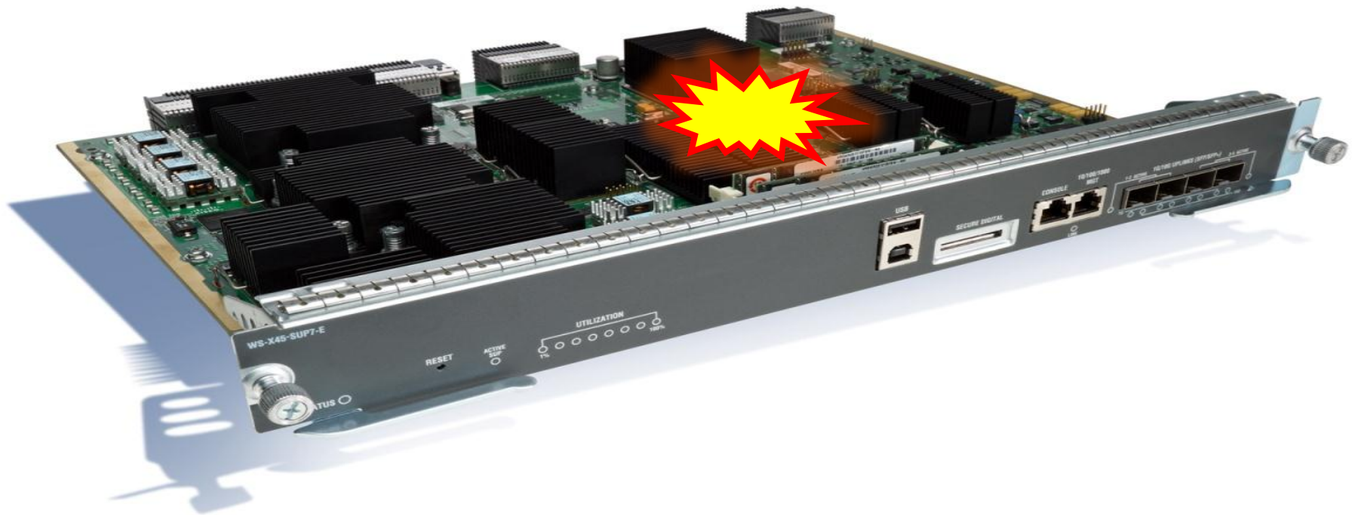
Completing the ISSU Process

ISSU System Status

```
Switch#show issu state detail
                              Slot = 5
                         RP State = Standby
                        ISSU State = Init
                   Operating Mode = Stateful Switchover
                    Current Image = bootflash:xo166
            Pre-ISSU (Original) Image = N/A
           Post-ISSU (Targeted) Image = N/A

                              Slot = 6
                         RP State = Active
                        ISSU State = Init
                   Operating Mode = Stateful Switchover
                    Current Image = bootflash:xo166
            Pre-ISSU (Original) Image = N/A
           Post-ISSU (Targeted) Image = N/A
```

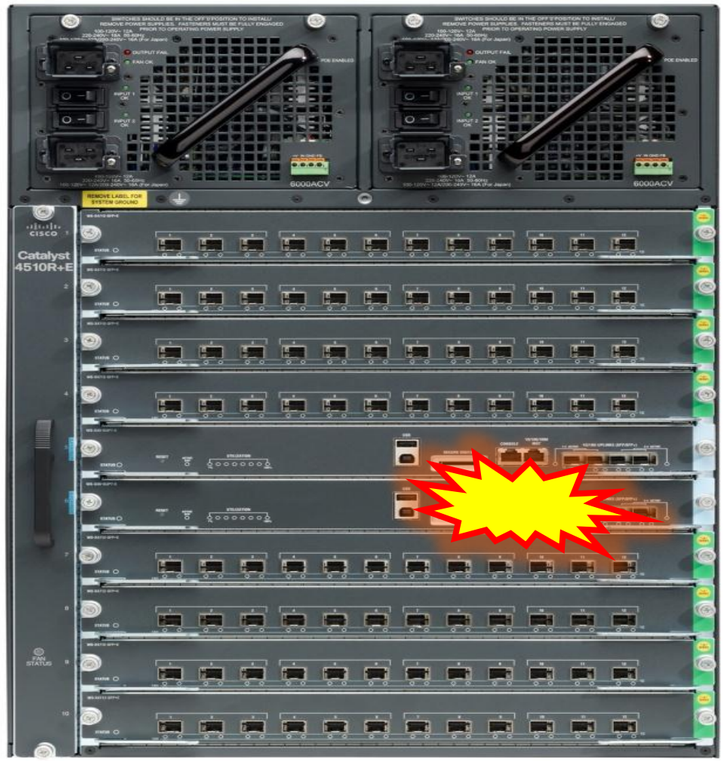
Generic Online Diagnostics–What is it?

GOLD defines a common framework for diagnostics operations across Cisco Platforms running IOS software. The goal is to check the health of hardware components and verify proper operation of the system control and data plane at run-time and boot…



Power-On Diagnostics
Supervisor, Backplane
L2 ASIC, L3 ASIC
Memory, CPU, Port

Runtime Diagnostics
Line Card Module, Temperature,
Power Supply, Fan Tray

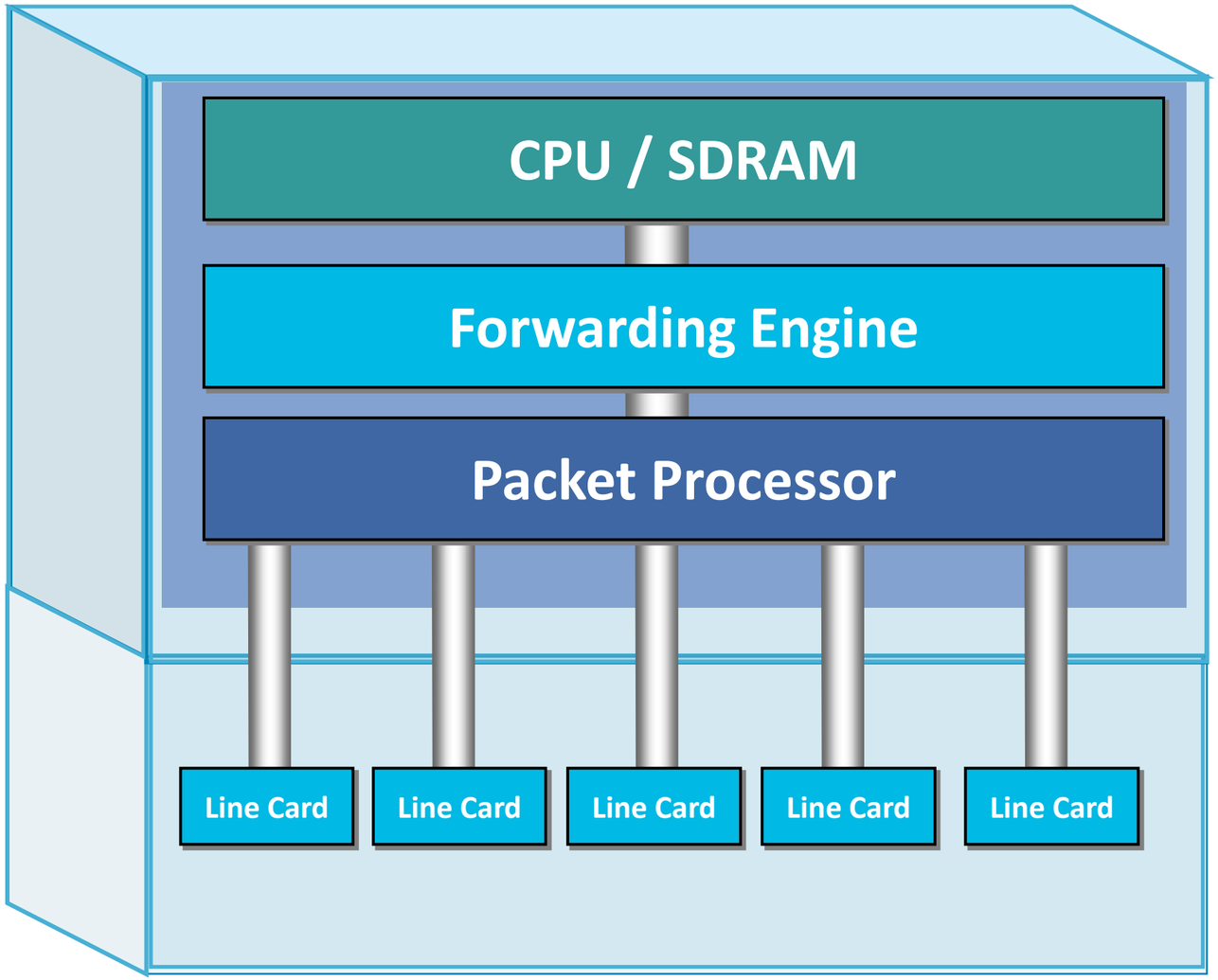


Agenda

- Catalyst 4500E overview
- IOS XE and Wireshark Overview
- System Architecture and Packet walk
- Flexible NetFlow
- Secure via MACSec
- ACL/QoS TCAM
- Forwarding TCAM
- High Availability
- Summary

Catalyst 4500E Architecture - Summary

Centralized Architecture



- Catalyst 4500E provides a centralized architecture
  - 848Gbps Switching capacity with 48Gbps/slot
  - IOS XE modular IOS hosting applications like Wireshark
  - UPOE Support enabling host of applications
  - MACSec Support in Hardware securing data
  - Application Visibility with Flexible NetFlow
  - Network Virtualization with EVN
  - Enable Voice/Video deployment with rich QoS capabilities
  - Highly resilient platform with SSO/NSF support
  - Upgrading Switch software with ISSU leading to minimal disruption of traffic

Complete Your Online Session Evaluation

- Receive 25 Cisco Preferred Access points for each session evaluation you complete.
- Give us your feedback and you could win fabulous prizes. Points are calculated on a daily basis. Winners will be notified by email after July 22nd.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.
- Don’t forget to activate your Cisco Live and Networkers Virtual account for access to all session materials, communities, and on-demand and live activities throughout the year. Activate your account at any internet station or visit www.ciscolivevirtual.com.
- This is session **BRKARC-3445**

BUILT FOR
THE HUMAN
NETWORK

Appendix

Catalyst 4500E Supervisor Comparison

For Your Reference

System

SUPERVISOR	SUP7-E	SUP7L-E	SUP6-E	SUP6L-E
Switch Fabric Capacity	**848 Gbps**	**520 Gbps**	336 Gbps	320 Gbps
CPU	**1.5 GHz (Dual Core)**	**1.5 GHz (Dual Core)**	1.3 GHz (Single Core)	1 GHz (Single Core)
Forwarding Rate	250 Mpps	225 Mpps	250 Mpps	225 Mpps
Bandwidth Per Slot	**48 Gbps**	**48 Gbps**	24 Gbps	24 Gbps
Unicast MAC Table	55K	55K	55K	55K
Chassis Support	3, 6, 7R, 10R chassis	3, 6, 7R chassis	3, 6, 7R, 10R chassis	3, 6, 7R chassis
Active redundant 10G uplinks	4	2	4	2
Max DRAM	**2G (4G option)**	**2G (4G Option)**	1G	1G

Catalyst 4500E Supervisor Comparison

For Your Reference

Performance

SUPERVISOR	SUP7-E	SUP7L-E	SUP6-E	SUP6L-E
Packet Memory	**32 MB**	**32 MB**	17.5 MB	17.5 MB
Packet Buffer Cells	**128K**	**128K**	64K	64K
Queue Enteries	**1 Million**	512K	512K	512K
Replication Table Size	102K	50K	102K	69K
Bootflash Size	**1 GB**	**1 GB**	128 MB	128 MB

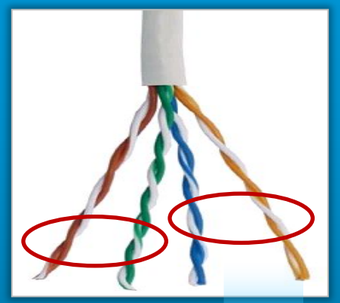
Scalability

SUPERVISOR	SUP7-E	SUP7L-E	SUP6-E	SUP6L-E
Number of IPv4 Routes	256K	64K	256K	57K
10 GB Port Density	**100**	**62**	34	32
1 GB Port Density	388	244	392	244
Netflow Entries	**128K**	**128K**	NA	NA
# of VRFs/EVNs	64/32	64/32	64/32	64/32
Unicast MAC Table	55K	55K	55K	55K

Cisco Universal PoE (UPOE)

IEEE 802.3at (PoE+)

Cat5e

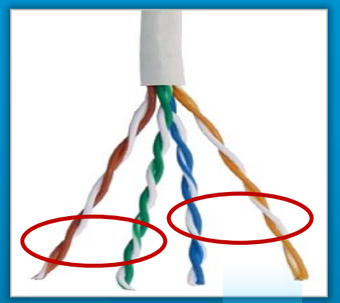


30W

- Maximum power sourced = 30W

UPOE

Cat5e



30W 30W

60W

- Maximum power sourced = 60W
- Supported by all cabling standards
- Compatible with PoE and PoE+

Universal Nature

- Standard RJ45 Connector
- No Cabling Change from PoE+

High Availability

- Uptime for critical apps (e911)
- Low TCO with UPS consolidation

Green

- 10% more efficient than bricks
- Management with EnergyWise

Cable and Heating

- TIA TR42 & ISO IEC: 2 Standards for Structured Cabling
  - **Published data that supports 60W over Cat5e cabling**
- Both committees studied temperature rise on PoE powered cables
  - Used a cable bundle of 100 cables
  - Used worst case scenario of cable passing through conduits
  - All study was done with all conductors in the cable powered

TIA TR-42 Recommendation

Temperature Rise	Max Current per twisted Pair	Max Power @ 50V
5	420mA	37.5W
7.5	520mA	45.2W
10	600mA	51.0W
12.5	670mA	55.8W
15	720mA	59.0W

ISO/IEC Recommendation

Temperature Rise	Max Current per twisted Pair	Max Power @ 50V
5	420mA	37.5W
7.5	550mA	47.4W
10	600mA	51.0W
12.5	680mA	56.4W
15	720mA	59.0W

The requirement for UPOE is no different than IEEE 802.3 specification

Power Negotiation – UPOE

- 802.3at specifies the LLDP protocol for Layer 2 based inline power negotiation up to 30W
- Cisco devices may use CDP for power negotation
- For UPOE, new TLVs are introduced for LLDP and CDP specific to the 4-pair POE
- Any PD requiring 4-Pair PoE (60W) power need to implement one of these

TLV Type	TLV Information String Length	Cisco OUI Identifier	Cisco OUI Subtype	PSE/PD Capabilities
7 bits	9 bits	3 octets	1 octet	1 octet

UPOE LLDP TLV

TLV Type	TLV Information String Length	Cisco OUI Identifier	Cisco OUI Subtype	PSE/PD Capabilities
7 bits	9 bits	3 octets	1 octet	1 octet

- PSE/PD capability field used to negotiate power in both LLDP and CDP

Bit	Function	Value/Meaning
0	4-pair PoE Supported	0 = No 1 = Yes
1	Spare pair Detection/Classification required	0 = No 1 = Yes
2	PD Spare Pair Desired State	0 = Disabled 1 = Enabled
3	PSE Spare Pair Operational State	0 = Disabled 1 = Enabled
B 4:7	Reserved	

Cisco UPOE and Virtual Desktop Clients

Integrated Display Client

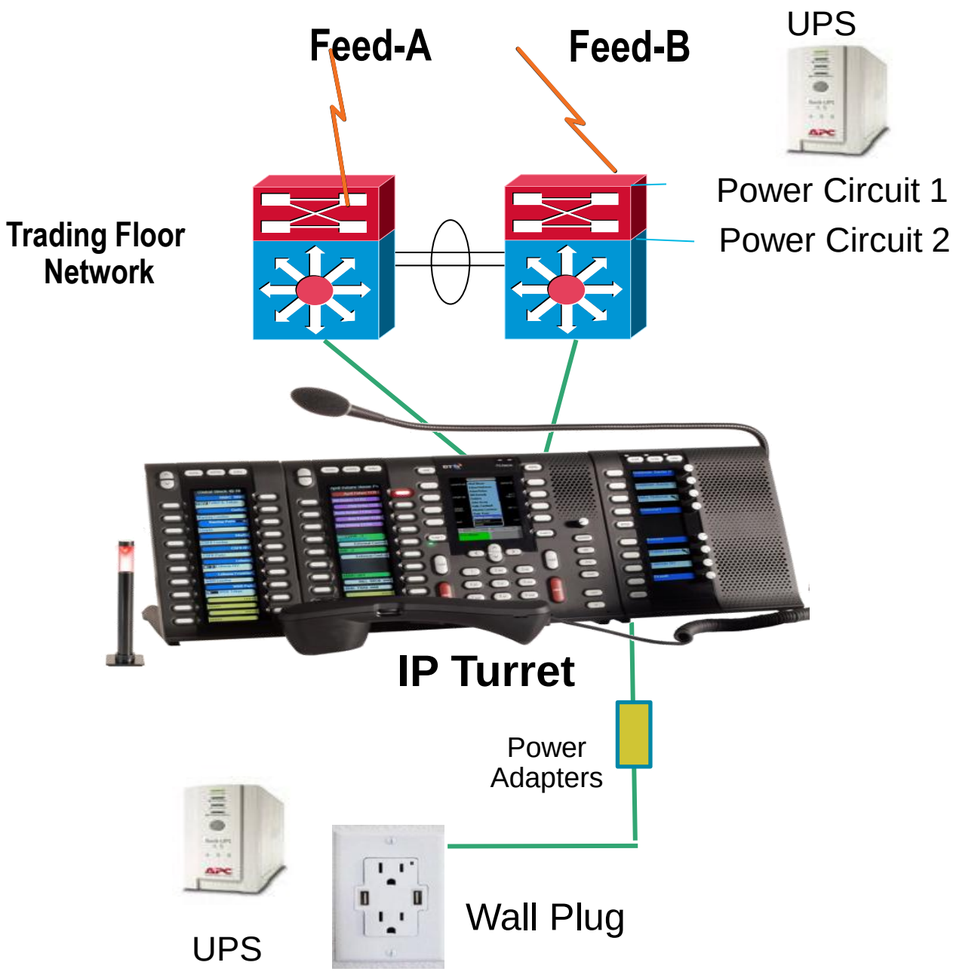
Standalone Client

Integrated Phone Client

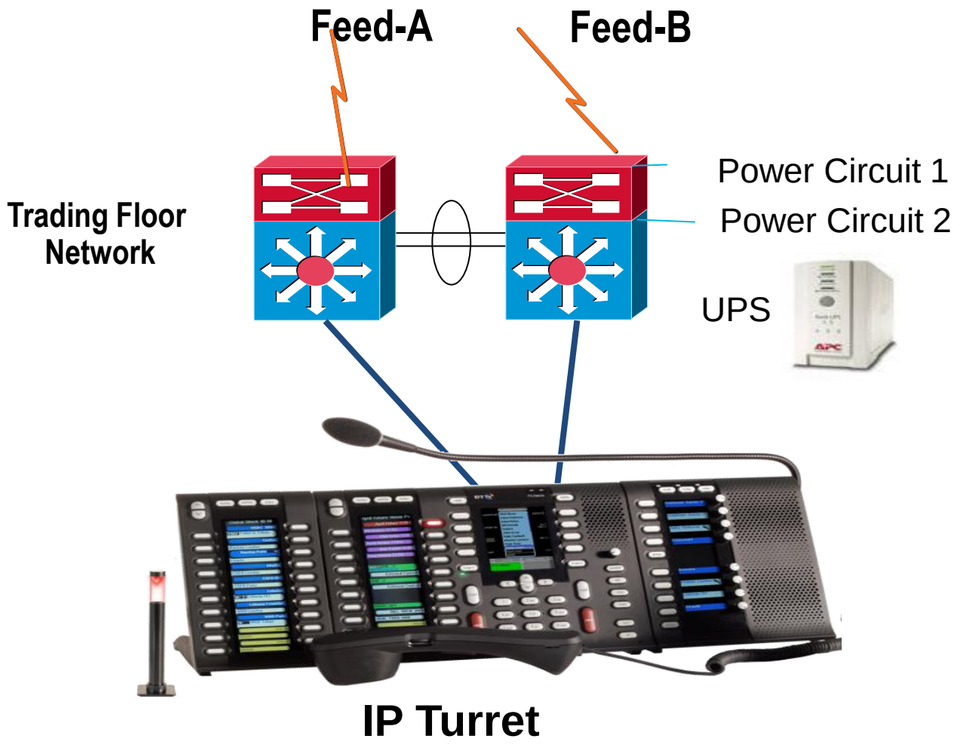
Power resiliency for Phone and VDI

Transforming Financial Trading Floors

Current Trading Floor Architecture



Next Generation Trading Floor Architecture



Transforming Retail Networks

Reduce Wiring Constraints & Enable Network Consolidation

LAN Infrastructure

Traditional Access

With PoE

LAN Edge

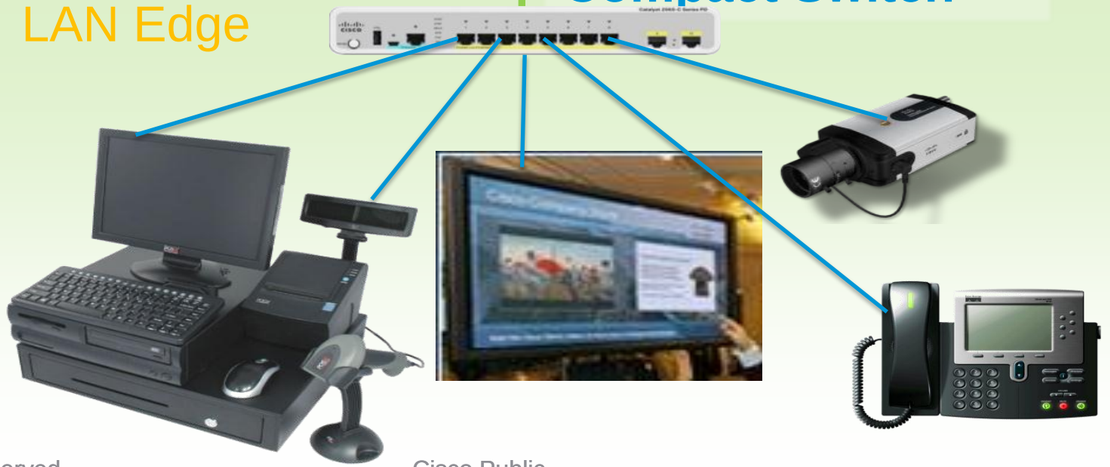
LAN Infrastructure

Catalyst 4500E

UPOE

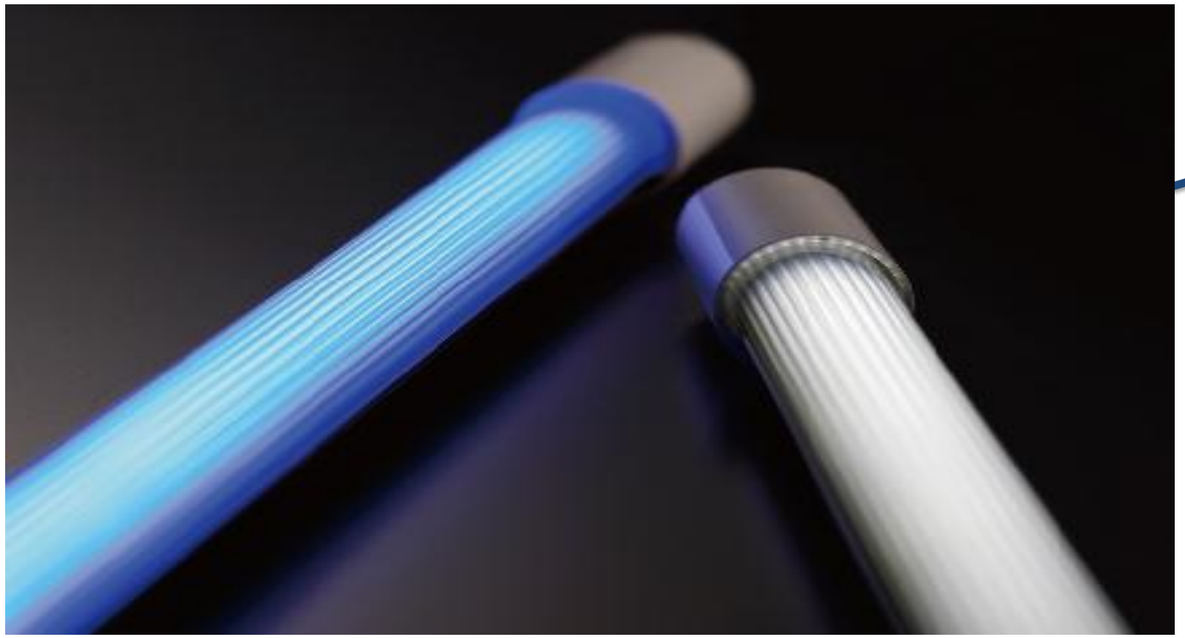
Compact Switch

LAN Edge



LED Lighting using UPOE

Manufacturing
Office Building
Lighting



LED Lights

60W
UPOE

Access Layer
Switch (Catalyst 4500E)

- Easy and Fast Installation
- Centralized Power Management
- Backup power consolidated as UPS in wiring closet

Wireshark Caveats

- Security:
  - Wireshark is run from IOS XE interface
  - Cannot invoke Wireshark directly
  - Wireshark runs in its own normal user space, hence no access to root user
  - Latest version will be bundled with a new IOS XE release to plug existing security holes in Wireshark
  - Wireshark crash does not take down IOS XE with it, so switch remains operational even if Wireshark does not
- Memory and Performance Impact:
  - 20-30MB usage in memory
  - The first instance will use more memory, while subsequent instances can share the same memory space. Upto 8 instances
  - Deleting a capture point, will exit the Wireshark process, and release memory back to the system
  - Interesting traffic is copied to CPU, hence this might be CPU intensive
  - The copied packets are policed via an internal policer in hardware, to protect CPU utilization, on a separate queue, out of the 64 queues
  - This might result in a not-so-contiguous packet capture

Wireshark Example

```
Sup7-E#monitor capture mycap int gi 6/1 in match ipv4 protocol tcp 10.1.1.1/32 any file
location bootflash:mycap.pcap limit duration 3
Sup7-E#show monitor capture
Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet6/1, Direction: in
  Status : Inactive
  Filter Details:
   IPv4
    Source IP:  10.1.1.1/32
    Destination IP:  any
   Protocol: tcp
  File Details:
   Associated file name: bootflash:mycap.pcap
  Buffer Details:
   Buffer Type: LINEAR (default)
  Limit Details:
   Packet Capture duration: 3
```

Wireshark Example

```
Sup7-E#monitor capture mycap start
monitor capture mycap start
*Apr  2 18:10:18.238: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
Sup7-E#
*Apr  2 18:10:21.473: %BUFCAP-6-DISABLE_ASYNC: Capture Point mycap disabled. Reason :
Wireshark session ended
Sup7-E#dir bootflash:mycap.pcap
14596  -rw-       32856   Apr 2 2012 18:10:21 +00:00  mycap.pcap
```

- Packet header display

```
Sup7-E#show monitor capture file bootflash:mycap.pcap
1  0.000000  10.1.1.1 -> 10.1.2.10  TCP [TCP ZeroWindow] 0 > 0 [<None>] Seq=1 Win=0 Len=70
```

- Packet detailed display

```
Sup7-E#show monitor capture file bootflash:mycap.pcap detailed
Frame 141: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
    Arrival Time: Apr  2, 2012 18:10:19.965938000 Universal
Ethernet II, Src: aa:bb:cc:dd:ee:ff , Dst: 01:00:00:00:01:01
    Time to live: 50
Frame 139: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
    Arrival Time: Apr  2, 2012 18:10:19.941937000 Universal
    Time to live: 100
Sup7-E#show monitor capture file bootflash:mycap.pcap display-filter "ip.ttl == 100"
```

Display Filter

Wireshark Commands

Troubleshooting Steps	Commands
Create a monitor	monitor capture mycap int gi x/y …
Display monitor details	show monitor capture
Start/stop a monitor session	monitor capture mycap start | stop
Display a pcap file	show monitor capture file <filename>
Display a pcap file in detail	show monitor capture file <filename> detailed
Display a pcap file with filter	show monitor capture file <filename> display-filter “filter-detail>
Check if wireshark is running	show proc cpu | inc dumpcap

QoS – Classification Examples

```
Switch(config)#ip access-list extended mmedia_conference
Switch(config-ext-nacl)#remark RTP
Switch(config-ext-nacl)#permit udp any any range 16384 32767
Switch(config-ext-nacl)#exit
Switch(config)#ip access-list extended signaling
Switch(config-ext-nacl)#remark SCCP
Switch(config-ext-nacl)#perm tcp any any range 2000 2002
Switch(config-ext-nacl)#remark SIP
Switch(config-ext-nacl)#perm tcp any any range 5060 5061
Switch(config-ext-nacl)#perm udp any any range 5060 5061
Switch(config-ext-nacl)#exit
Switch(config)#ip access-list extended transactions
Switch(config-ext-nacl)#remark HTTPS
Switch(config-ext-nacl)#permit tcp any any eq 443
Switch(config-ext-nacl)#remark Oracle SQLNet
Switch(config-ext-nacl)#permit tcp any any range 1521 1526
Switch(config-ext-nacl)#permit udp any any range 1521 1526
Switch(config-ext-nacl)#exit
```

QoS Classification - Continued

```
Switch(config)#ip access-list extended bulk
Switch(config-ext-nacl)#permit tcp any any eq ftp
Switch(config-ext-nacl)#permit tcp any any eq ftp-data
Switch(config-ext-nacl)#remark SSH/SFTP
Switch(config-ext-nacl)#permit tcp any any eq 22
Switch(config-ext-nacl)#remark SMTP/Secure SMTP
Switch(config-ext-nacl)#permit tcp any any eq smtp
Switch(config-ext-nacl)#permit tcp any any eq 465
<snip…..snip>
Switch(config-ext-nacl)#permit tcp any any eq 995
Switch(config-ext-nacl)#remark Connected CLM Backup
Switch(config-ext-nacl)#permit tcp any eq 1914 any
Switch(config-ext-nacl)#permit tcp any any eq 16384
Switch(config-ext-nacl)#exit
Switch(config)#
Switch(config)#ip access-list extended scavenger
Switch(config-ext-nacl)#remark Kazaa
Switch(config-ext-nacl)#permit tcp any any eq 1214
Switch(config-ext-nacl)#permit udp any any eq 1214
<snip……snip>
Switch(config-ext-nacl)#remark BitTorrent
Switch(config-ext-nacl)#permit tcp any any range 681 6999
Switch(config-ext-nacl)#remark Yahoo Gaming
Switch(config-ext-nacl)#permit tcp any any eq 11999
<snip…….snip>
```

QoS Classification – Examples Continued

```
Switch(config)#class-map vvlan-voip
Switch(config-cmap)#match dscp ef
Switch(config)#exit
Switch(config)#class-map vvlan-signaling
Switch(config-cmap)#match dscp cs3
Switch(config-cmap)#exit
Switch(config)#class-map mmedia_conference
Switch(config-cmap)#match access-group name mmedia_conference
Switch(config-cmap)#
Switch(config-cmap)#class-map signaling
Switch(config-cmap)#match access-group name signaling
Switch(config-cmap)#
Switch(config-cmap)#class-map transactions
Switch(config-cmap)#match access-group name transactions
Switch(config-cmap)#
Switch(config-cmap)#class-map bulk
Switch(config-cmap)#match access-group name bulk
Switch(config-cmap)#
Switch(config-cmap)#class-map scavenger
Switch(config-cmap)#match access-group name scavenger
```

Ingress Policing and Marking - Examples

```
Switch(config)#policy-map Input-Policy
Switch(config-pmap)#class vvlan-voip
Switch(config-pmap-c)#police 128k
Switch(config-pmap-c-police)#conform-action set-dscp-transmit ef
Switch(config-pmap-c-police)#conform-action set-cos-transmit 5
Switch(config-pmap-c-police)#exceed-action drop

Switch(config-pmap)#class vvlan-signaling
Switch(config-pmap-c)#police 32k
Switch(config-pmap-c-police)#conform-action set-dscp-transmit cs3
Switch(config-pmap-c-police)#conform-action set-cos-transmit 3
Switch(config-pmap-c-police)#exceed-action drop

Switch(config-pmap-c)#class mmedia_conference
Switch(config-pmap-c)#police 5m
Switch(config-pmap-c-police)#conform-action set-dscp-transmit af41
Switch(config-pmap-c-police)#conform-action set-cos-transmit 4
Switch(config-pmap-c-police)#exceed-action drop
```

Ingress Policing and Marking - Examples

```
Switch(config-pmap-c)#class signaling
Switch(config-pmap-c)#police 32k
Switch(config-pmap-c-police)#conform-action set-dscp-transmit cs3
Switch(config-pmap-c-police)#conform-action set-cos-transmit 3
Switch(config-pmap-c-police)#exceed-action drop

Switch(config-pmap-c)#class transactions
Switch(config-pmap-c)#police 10m
Switch(config-pmap-c-police)#conform-action set-dscp-transmit af21
Switch(config-pmap-c-police)#conform-action set-cos-transmit 2
Switch(config-pmap-c-police)#exceed-action set-dscp-transmit cs1
Switch(config-pmap-c-police)#exceed-action set-cos-transmit 1

Switch(config-pmap-c)#class bulk
Switch(config-pmap-c)#police 10m
Switch(config-pmap-c-police)#conform-action set-dscp-transmit af11
Switch(config-pmap-c-police)#conform-action set-cos-transmit 1
Switch(config-pmap-c-police)#exceed-action set-dscp-trasmit cs1
 Switch(config-pmap-c-police)#exceed-action set-dscp-transmit cs1
Switch(config-pmap-c-police)#exceed-action set-cos-transmit 1
```

Ingress Policing and Marking - Examples

```
Switch(config-pmap-c)#class scavenger
Switch(config-pmap-c)#police 10m
Switch(config-pmap-c-police)#conform-action set-dscp-transmit cs1
Switch(config-pmap-c-police)#conform-action set-cos-transmit 1
Switch(config-pmap-c-police)#exceed-action drop
Switch(config-pmap-c-police)#
Switch(config-pmap-c-police)#exit
Switch(config-pmap-c)#class class-default
Switch(config-pmap-c)#police 10m
Switch(config-pmap-c-police)#conform-action transmit
Switch(config-pmap-c-police)#exceed-action set-dscp-transmit cs1
Switch(config-pmap-c-police)#exceed-action set-cos-transmit 1
```

QoS – Queuing Examples

```
Switch(config)#class-map Priority-Q
Switch(config-cmap)#match dscp ef cs5 cs4
Switch(config-cmap)#exit
Switch(config)#class-map match-any Control-Mgmt-Q
Switch(config-cmap)#match dscp cs2 cs3 cs6 cs7
Switch(config-cmap)#match cos 6 7
Switch(config-cmap)#exit
Switch(config)#class-map Mmedia-Conf-Q
Switch(config-cmap)#match dscp af41 af42 af43
Switch(config-cmap)#exit
Switch(config)#class-map Mmedia-Stream-Q
Switch(config-cmap)#match dscp af31 af32 af33
Switch(config-cmap)#exit
Switch(config)#class-map Transactional-Q
Switch(config-cmap)#match dscp af21 af22 af23
Switch(config-cmap)#exit
Switch(config)#class-map Bulk-Q
Switch(config-cmap)#match dscp af11 af12 af13
Switch(config-cmap)#exit
Switch(config)#class-map Scavenger-Q
Switch(config-cmap)#match dscp cs1
```

QoS – Queuing Examples

```
Switch(config)#policy-map Queuing
Switch(config-pmap)#class Priority-Q
Switch(config-pmap-c)#priority
Switch(config-pmap)#class Control-Mgmt-Q
Switch(config-pmap-c)#bandwidth remaining percent 10
Switch(config-pmap)#class Mmedia-Conf-Q
Switch(config-pmap-c)#bandwidth remaining percent 10
Switch(config-pmap)#class Mmedia-Stream-Q
Switch(config-pmap-c)#bandwidth remaining percent 10
Switch(config-pmap)#class Transactional-Q
Switch(config-pmap-c)#bandwidth remaining percent 10
Switch(config-pmap-c)#dbl
Switch(config-pmap)#class Bulk-Q
Switch(config-pmap-c)#bandwidth remaining percent 4
Switch(config-pmap-c)#dbl
Switch(config-pmap)#class Scavenger-Q
Switch(config-pmap-c)#bandwidth remaining percent 1
Switch(config-pmap-c)#dbl
Switch(config-pmap)#class class-default
Switch(config-pmap-c)#bandwidth remaining percent 25
Switch(config-pmap-c)#dbl
```

NetFlow Flow Record Configuration Examples

Application traffic flow record:

```
flow record app-keys
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect transport tcp flags
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
```

Protocol, L3, L4, Interface fields as Key Field

TCP Flags, Packet counters, Timestamps as Non-Key Field

Server Utilization flow record:

```
flow record server-keys
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect interface output
 collect counter bytes
 collect counter packets
```

Protocol, L3, L4, Interface fields as Key Field

Tx Interface, Packet and Byte counters as Non-Key Field

NetFlow Flow Record Configuration Examples

Security flow record:

```
flow record security-keys
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect transport icmp ipv4 type
 collect transport icmp ipv4 code
 collect transport tcp flags
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
```

Protocol, L3, L4, TTL fields as Key Field

ICMP Codes and Types, TCP Flags, Packet counters, Timestamps as Non-Key Field

Capacity Planning flow record:

```
flow record capacity-keys
 match ipv6 protocol
 match ipv6 source address
 match ipv6 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect interface output
 collect counter bytes
 collect counter packets
```

Protocol, L3, L4, Rx Interface fields as Key Field

Tx Interface, Packet and Byte Counter as Non-Key Field

Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com

Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: https://www.facebook.com/ciscoliveus
  - Twitter: https://twitter.com/#!/CiscoLive
  - LinkedIn Group: http://linkd.in/CiscoLI

BUILT FOR
THE HUMAN
NETWORK