TECHNICAL DECISION MAKER PRESENTATION

Cisco Catalyst 1000 Series Switches

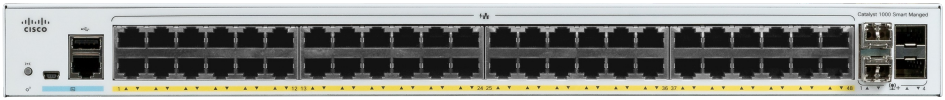
Prepared as a convenient PDF reference for network planning, platform evaluation, and procurement discussions.

Cisco Catalyst 1000 Series Switches

Enterprise quality for small deployments

Introducing Cisco Catalyst 1000 Series Switches

Enterprise quality for small deployments



Versatility

- 1G, 10G Uplinks
- Fanless and compact
- Partial and full PoE
- Single IP Device Management
- Day 0 Provisioning
- Layer 3 static routing

Reliability

- Cisco IOS
- Extended Temperature* (-5 to 50dC)
- Perpetual PoE
- TAC Support
- ELLW

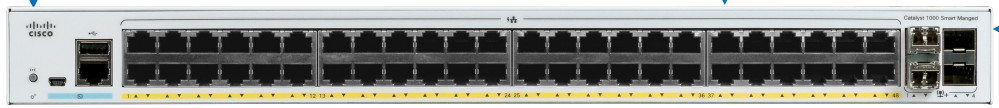
Security

- Private VLANs
- Expanded TCAM tables
- 802.1x authentication
- IPv6 First Hop Security

* with short time period operation only

Cisco Catalyst 1000 Series

Versatility and resiliency for a wide range of network environments



Signed Cisco IOS® images and secure boot

Extended Temperature**

Fanless*

PoE+ upto 740W

Shallow Depth

Bluetooth Manageability

2 x 1G or 4 x 1G or 4x10G

EEE compliant

8/16/24/48 1G downlinks

4 egress queues per port

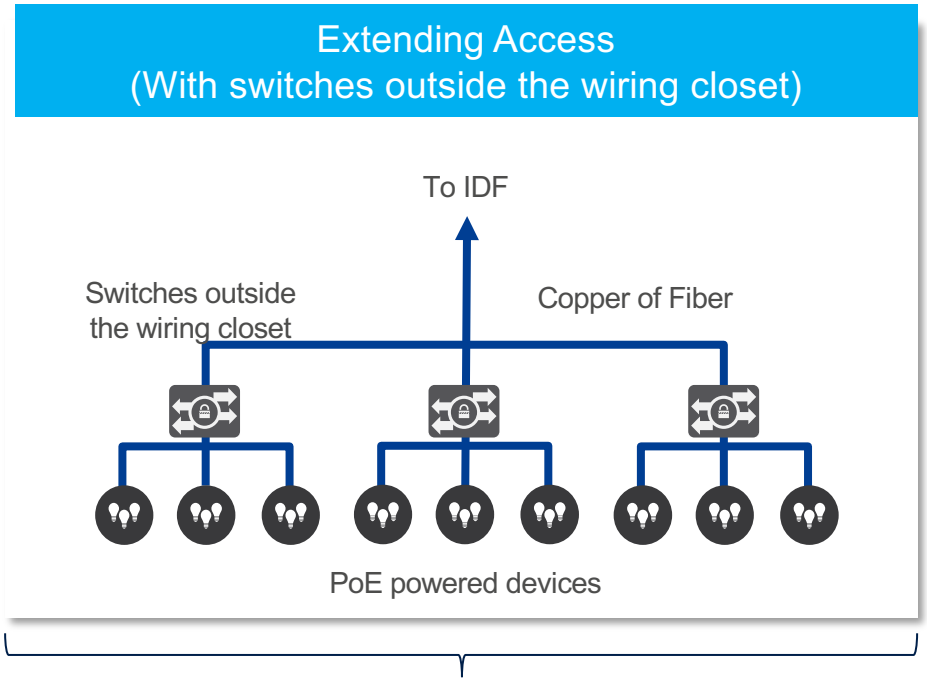
< 1-min boot time

1.5 Mb per ASIC

Web UI for configuration and management

Compact, fanless* and with PoE for deployment inside or outside the wiring closet

Design a Distributed network with Fanless and compact Catalyst 1000 SKU's



A distributed Network Design Enables

- Variety of PoE options for IoT
- Fanless SKU's for Whisper quiet
- Space optimization, by eliminating IDFs in each floor.

Catalyst 1000 Specification

- ✓ 800MHz CPU
- ✓ 256Mb – Flash
- ✓ 512Mb – DRAM
- ✓ 1.5 Mb Buffer
- ✓ Max 740W of PoE / PoE+
- ✓ Operating Temperature : -5C to 50C
- ✓ Altitude : up to 10000 ft
- ✓ Surge Protection
- ✓ IP20 Rated

- ✓ Fanless*
- ✓ Fixed and External Power Supplies
- ✓ Fixed 1G Downlinks - 8 /16 /24 /48
- ✓ Fixed Uplinks – 2x1G / 4x1G / 4x10G
- ✓ Auto Recovery
- ✓ Access of CLI and Web UI over Bluetooth
- ✓ 802.1x Multi Auth + IPv6 + MLD V1 & V2 snooping

Catalyst 1000 Overview

Feature	8 Ports	16 Ports	24 Ports	48 Ports
Forwarding bandwidths	10 Gbps	18 Gbps	28 Gbps	52 Gbps
Switching bandwidth	20 Gbps	36 Gbps	56 Gbps	104 Gbps
Forwarding rate (64-byte L3 packets)	14.88 Mpps	26.78 Mpps	41.67 Mpps	77.38 Mpps
Unicast MAC addresses	16K	16K	16K	16K
Maximum active VLANs	256	256	256	256
VLAN IDs available	4,096	4,096	4,096	4,096
Maximum STP instances	64	64	64	64
MTU-L3 packet	9198 bytes	9198 bytes	9198 bytes	9198 bytes
Jumbo Ethernet frame	10,240 bytes	10,240 bytes	10,240 bytes	10,240 bytes
Routes (Static Routes)	512	512	512	512
SVIs	64	64	64	64

Catalyst 1000 Series switching SKUs

48 ports Gigabit Ethernet

24 ports Gigabit Ethernet

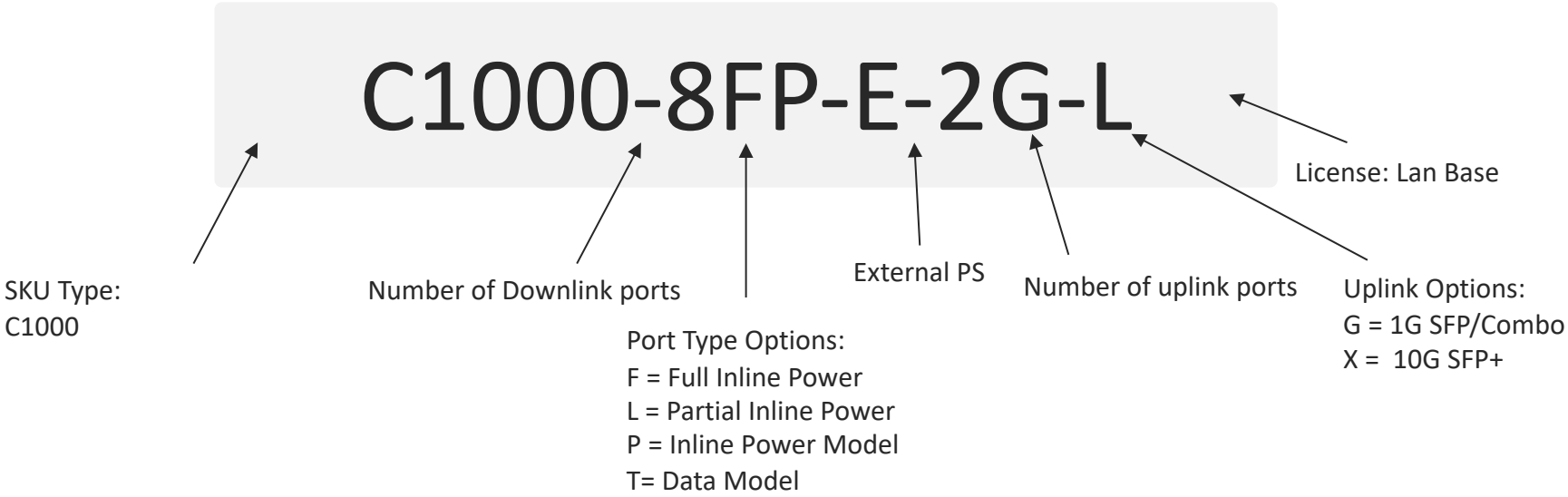
Uplinks	PoE	Power Supply	Management
4xSFP 4xSFP+	Full PoE+ Partial PoE+ Limited PoE Data	Internal	WebUI Only CLI and Web UI

16 ports Gigabit Ethernet

8 ports Gigabit Ethernet

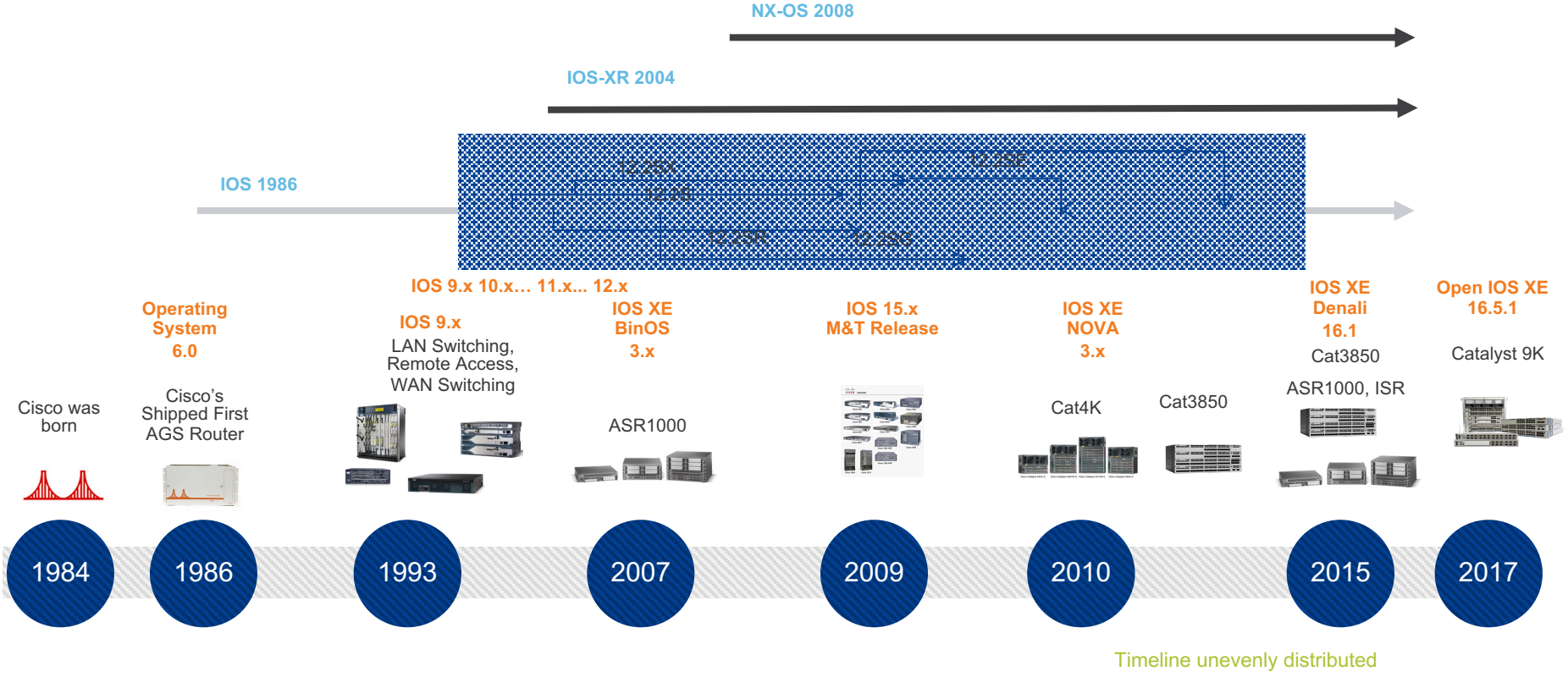
Uplinks	PoE	Power Supply	Management
2xSFP RJ45 Combo	Full PoE+ Partial PoE+ Limited PoE Data	Internal External	WebUI Only CLI and Web UI

How to read the SKU?



Cisco IOS

Cisco IOS – Powering Catalyst 1000 Series Switches



Timeline unevenly distributed

Cisco IOS built on 30+ years of industry experience providing the most resilient OS in its class

Cisco IOS Benefits

Trustworthy solution

Catalyst 1000 Series switches provides strong resistance against today's threats

HW Anchored Secure Boot

Image Signing and Secure Boot work together to ensures that authentic Cisco SW boots up on a Cisco Platform

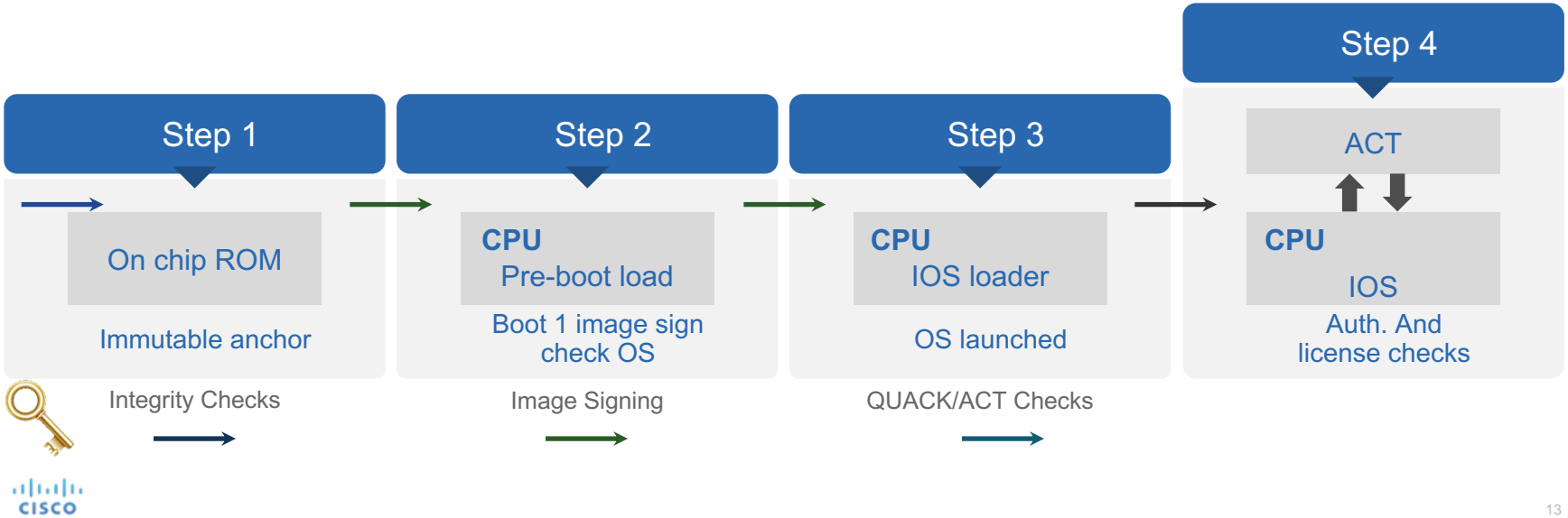
Trust Anchor Module

HW Authenticity Check

Cisco Trust Anchor Technology

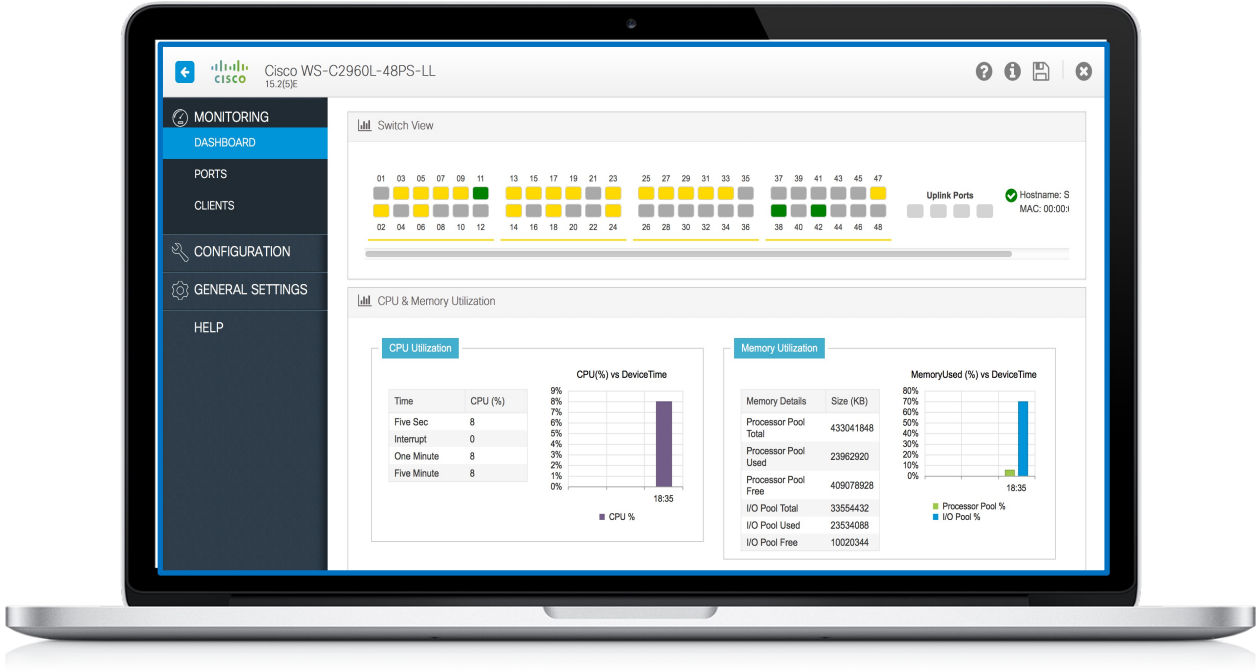
Benefits

- Universal Cisco IOS® Software image not encrypted - easy distribution
- Image signature validates authenticity of images - tamper-proof IOS



Ease of Management

Flexible Management with On-Box Web UI for Catalyst 1000



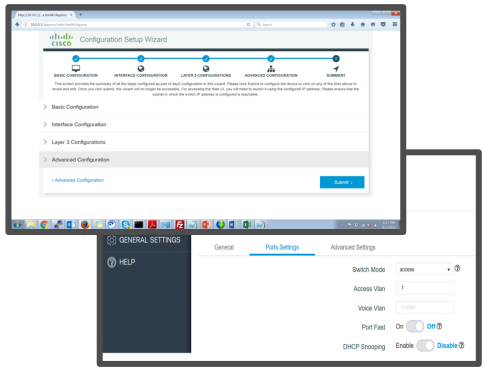
- Ease of access
- Build configurations
- Intuitive interface
- Network Monitoring
- Troubleshooting

Cisco Configuration Professional for Catalyst

Provisioning

Simple 4 Step UI to onboard the switch

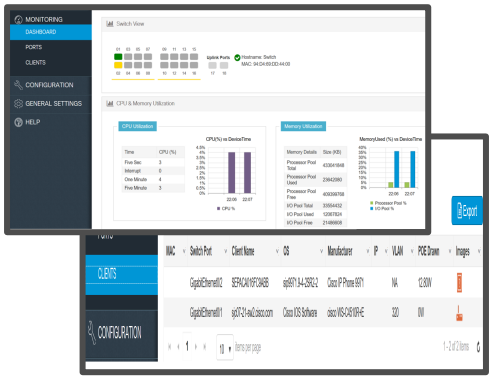
Minimal clicks to configure and onboard end clients



Monitoring

Single screen to monitor health statistics

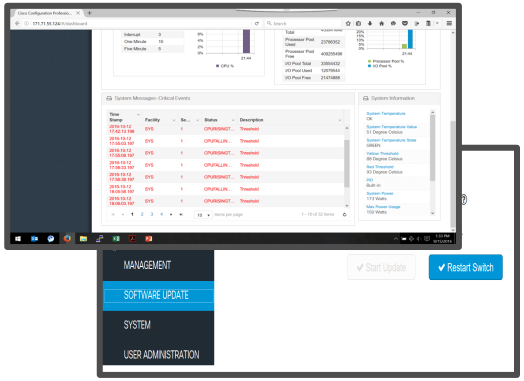
Easy pictorial view of all end points connected



Troubleshooting & Maintenance

Basic troubleshooting like ping , traceroute, diagnostics can be performed from the UI

Simple Software upgrade procedure

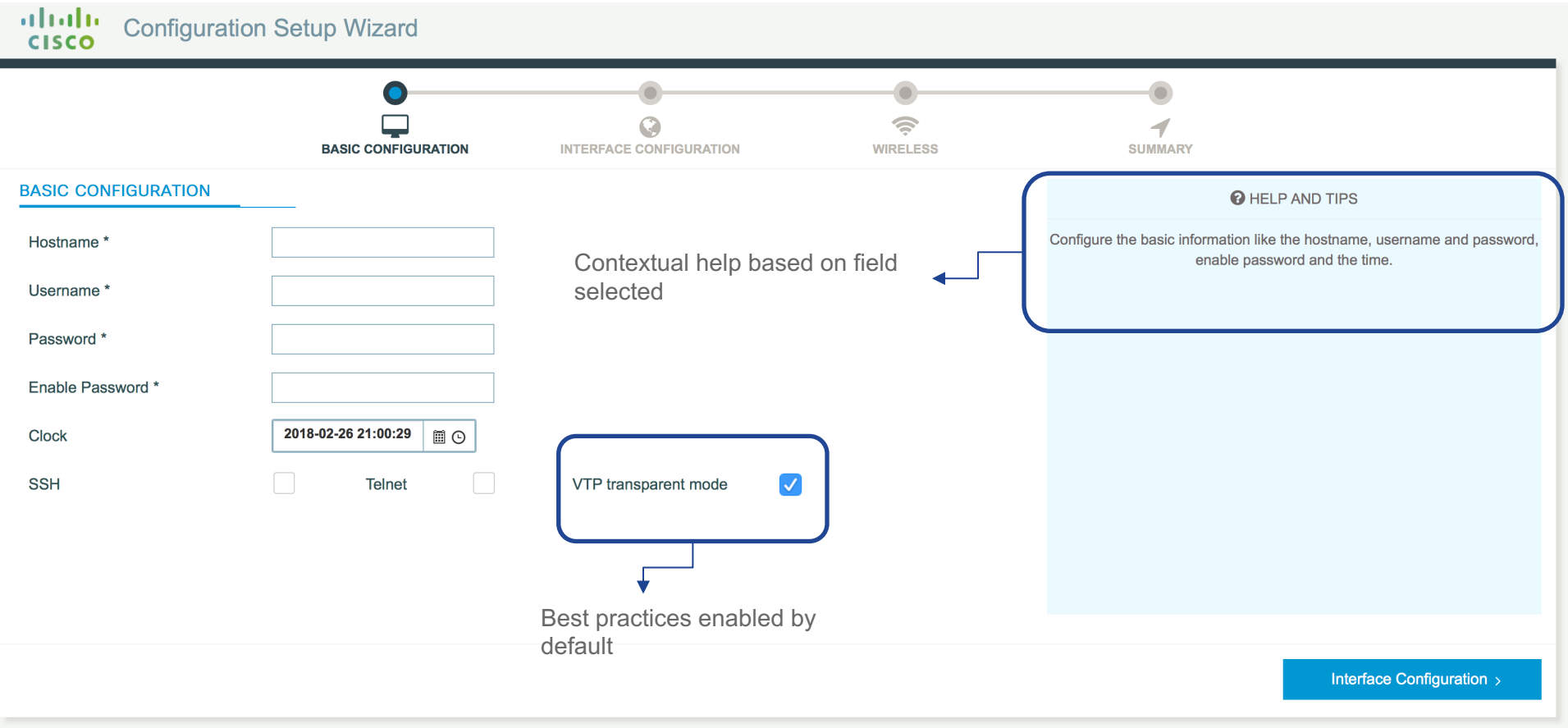


Available in English, Japanese, Chinese and Korean

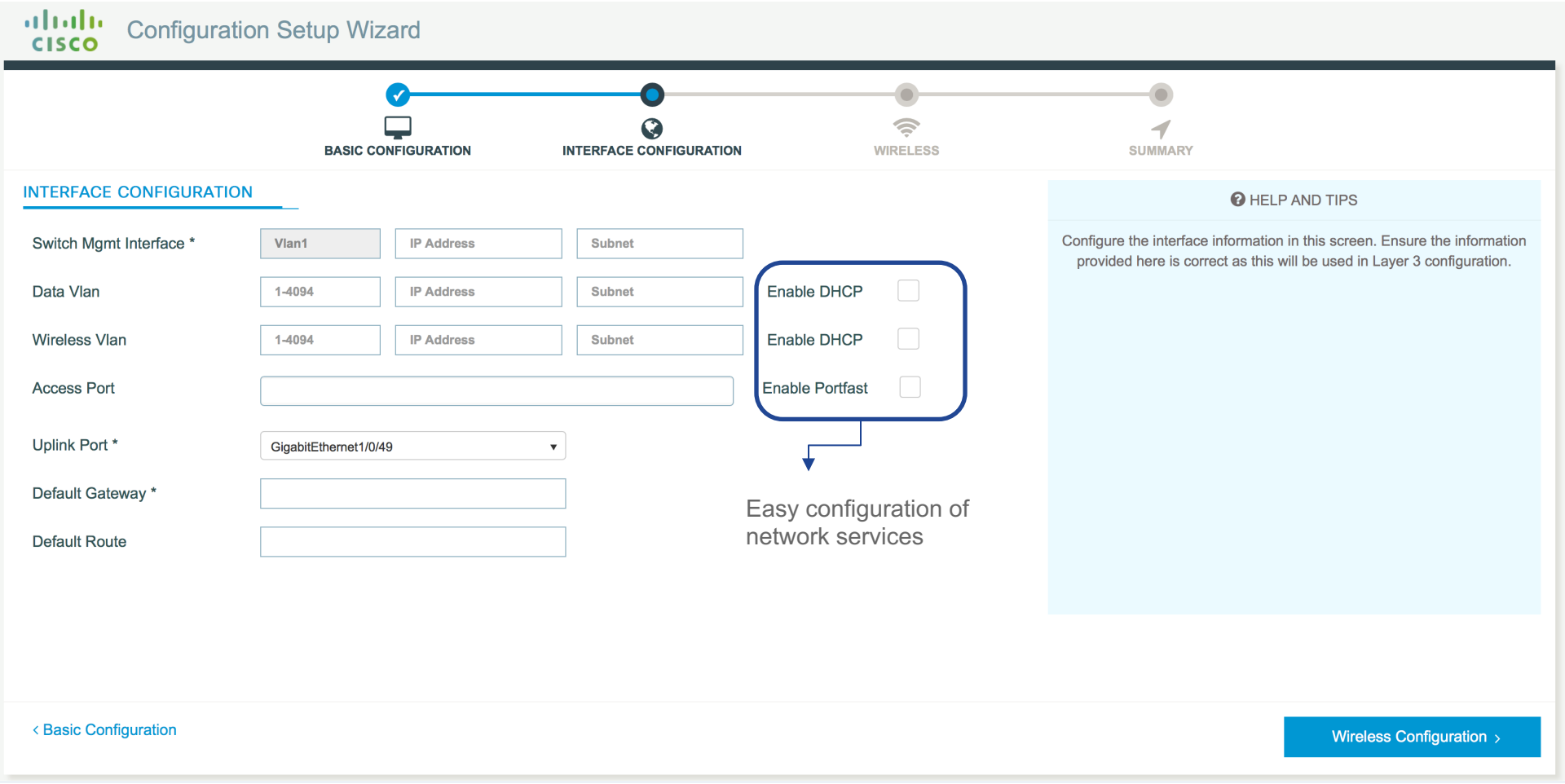
Wired-Wireless Day 0 Integration

- CCPC on Catalyst 1000 Series Switches can be used to configure Mobility Express based Access Points along with the switch.
- Existing Day 0 wizard has been simplified, allowing a user to set up wired and wireless network with just three steps.
- CCPC day 0 wizard hides the underlying complexity associated with setting up network by configuring the network with best practices

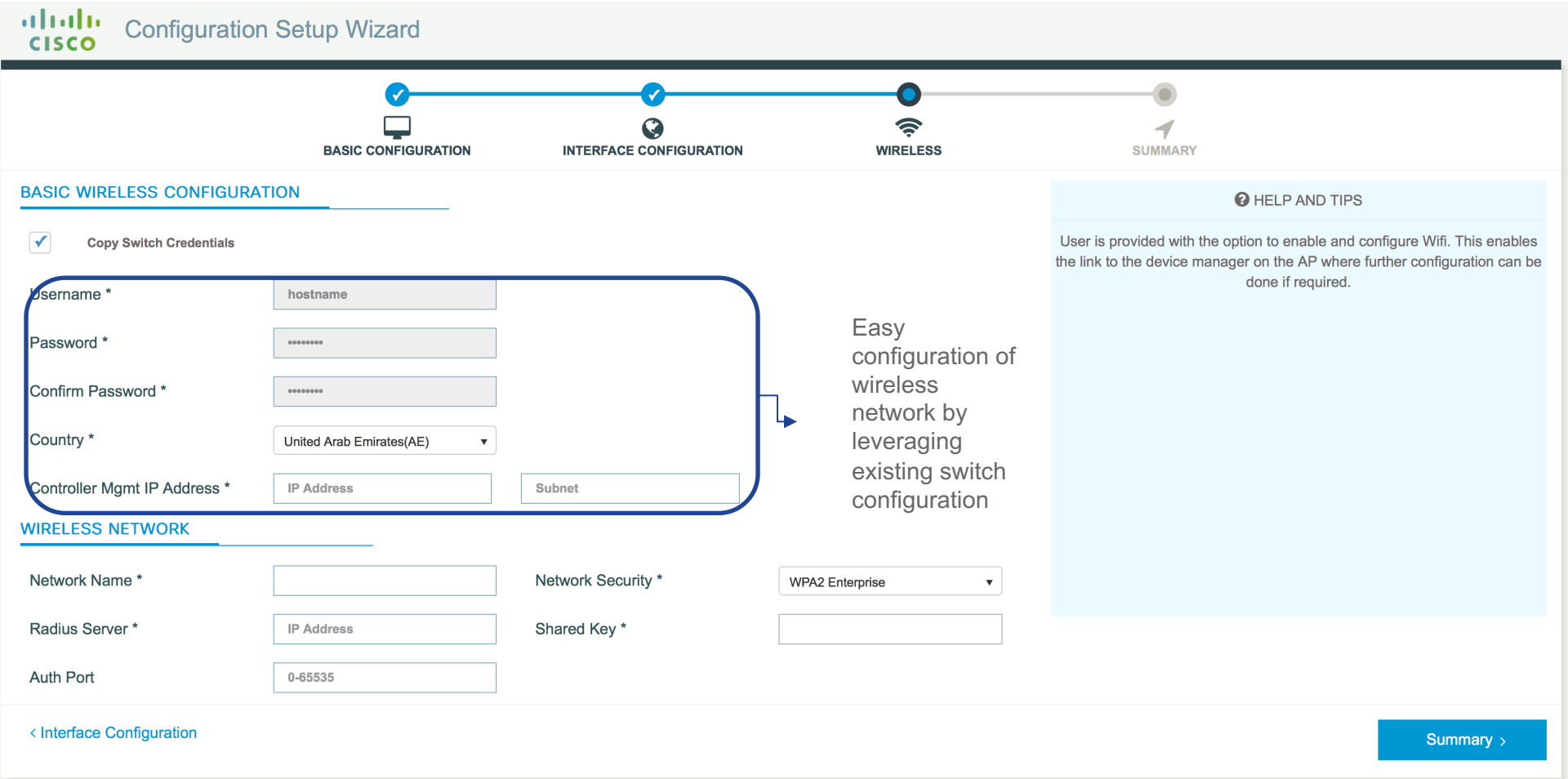
Day 0 Wizard: Basic Configuration



Day 0 Wizard: Interface Configuration



Day 0 Wizard: Wireless Configuration



Bluetooth for Over The Air (OTA) access

Configure*, monitor and troubleshoot with a tablet or Laptop with CCP for Catalyst or CLI over Bluetooth.

- ✓ Switch CLI or Web UI can be accessed over Bluetooth when Bluetooth dongle is connected
- ✓ The access can be restricted to AAA user or local user configured on the switch.

* Support for configuration post deployment only

Connecting to Switch using Bluetooth

Connect BT dongle to switch and power on

Turn on BT on PC and discover switch

Pair PC with the switch

Connect to switch as an access point

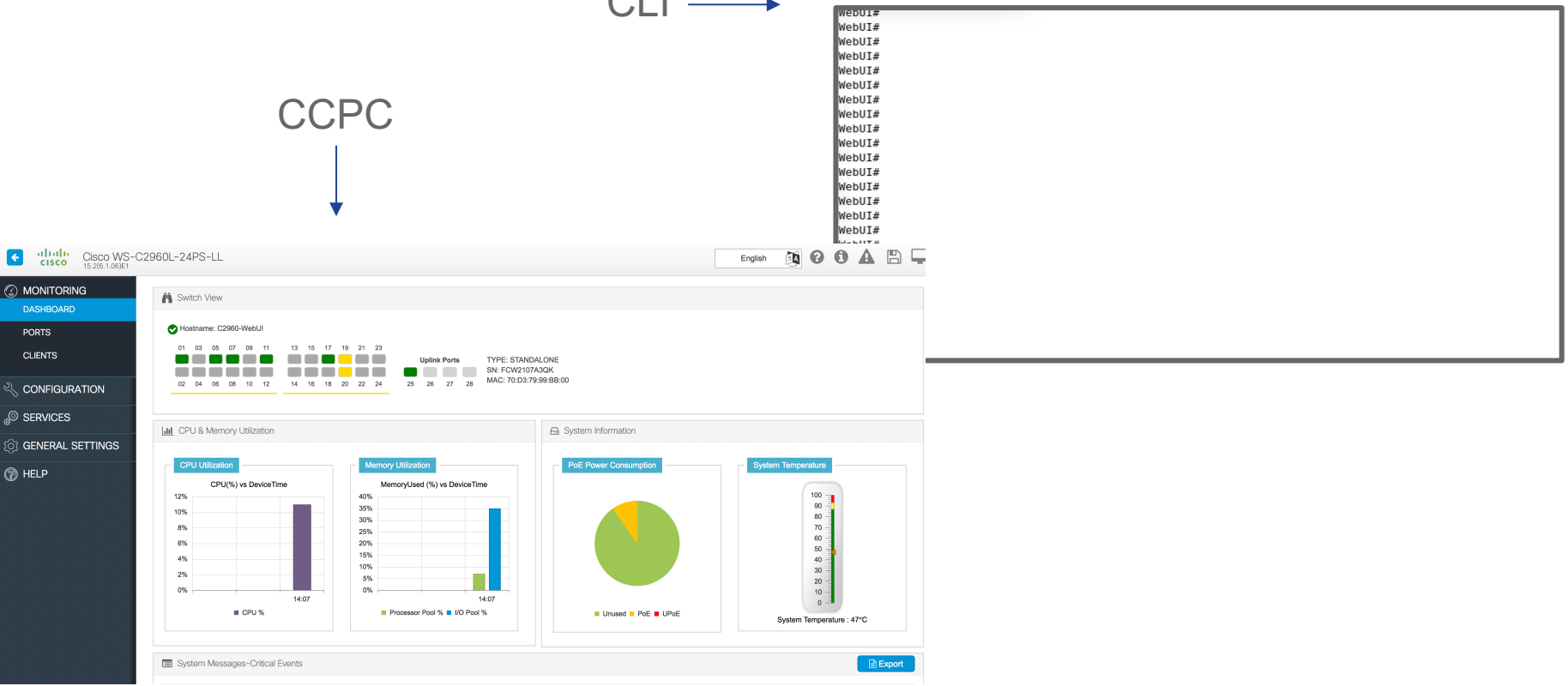
Open Management window and configure switch

CCPC

Modes of Accessing the switch

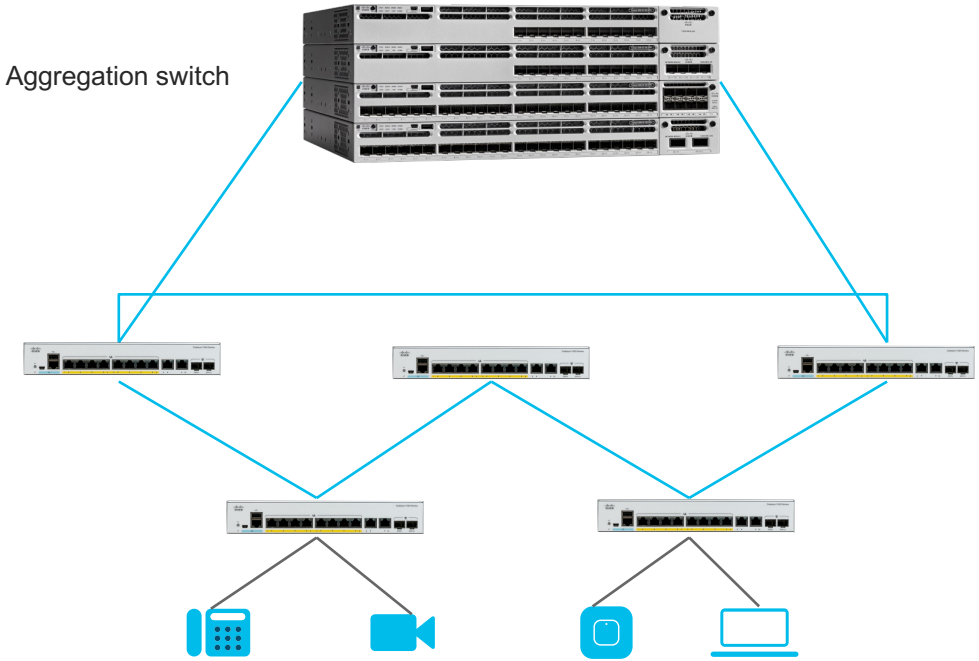
CLI →

CCPC ↓



Single IP Device Management

Ease of Device Management



- **Manage up to eight switches through single IP**
- **Mix and match models**
- **Management can be done over 10G SFP+/1G SFP uplinks**

Ease of Device Management

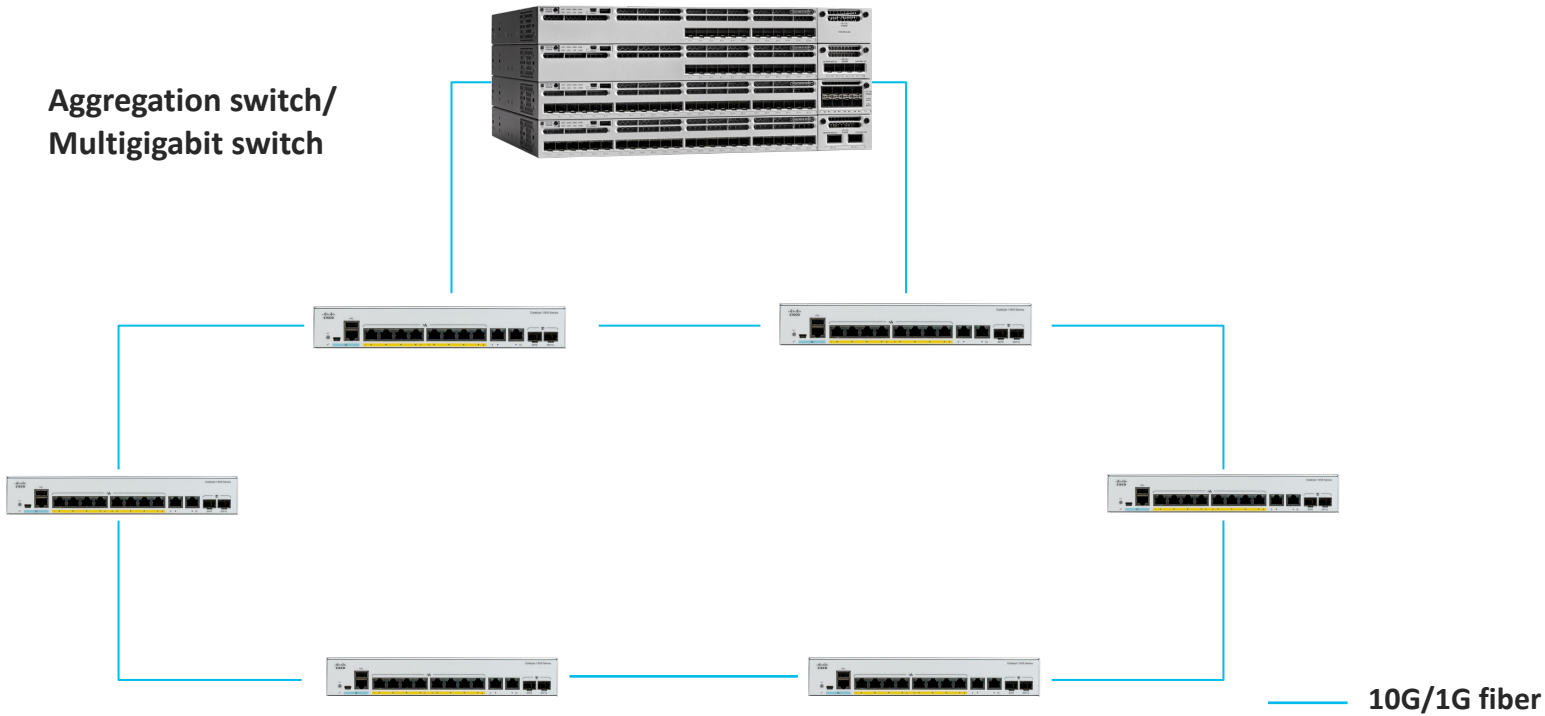
Application

- Management over standard fiber – longer distances
- Unit functions as a single switch – unified management and control

Details

- Supported on all SKUs
- 10G SFP+/1G SFP configured as for device management(up to two)
- Eight units managed via single IP
- One unit functions as master
- Single IP address, SNMP agent, configuration etc.
- Holds configuration of the unit
- New unit can automatically join – auto upgrade of firmware
- Mix between SFP/SFP+ is not supported

Topology – fiber ring, SFP/SFP+ uplink



Monitoring devices

```
C1K-1#show switch detail
Switch/Stack Mac Address : 6c5e.3b94.3c00
                                            H/W   Current
Switch#  Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master 6c5e.3b94.3c00     1      0       Ready
 2       Member 6c5e.3bb8.6d80     1      0       Ready


         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------------
  1        Ok         Ok               2        2
  2        Ok         Ok               1        1
```

```
C1K-1#show switch stack-ring speed


Stack Ring Speed        : 10G
Stack Ring Configuration: Full
Stack Ring Protocol     : FlexStack

C1K-2#show switch stack-ring speed


Stack Ring Speed        : 1G
Stack Ring Configuration: Half
Stack Ring Protocol     : FlexStack
```

```
C1K-1#show switch stack-ports
  Switch #    Port 1       Port 2
  --------    ------       ------
    1           Ok           Ok
    2           Ok           Ok


C1K-1#show switch neighbors
  Switch #    Port 1       Port 2
  --------    ------       ------
      1         2            2
      2         1            1
```

```
C1K-1#show switch hstack-ports
 Horizontal stack port status :
 Gi Ports   Stack Port   Operational Status   Next Reload Status   Media Type
 --------- ------------ -------------------- ------------------- -------
--
 Gi1/0/25      1            Stack Port         Stack Port          Fiber
 Gi1/0/26      2            Stack Port         Stack Port          Fiber
 Gi1/0/27      NA           N/W Port           N/W Port            Fiber
 Gi1/0/28      NA           N/W Port           N/W Port            Fiber
 Gi2/0/25      1            Stack Port         Stack Port          Fiber
 Gi2/0/26      2            Stack Port         Stack Port          Fiber
 Gi2/0/27      NA           N/W Port           N/W Port            Fiber
 Gi2/0/28      NA           N/W Port           N/W Port            Fiber
```

Network Visibility

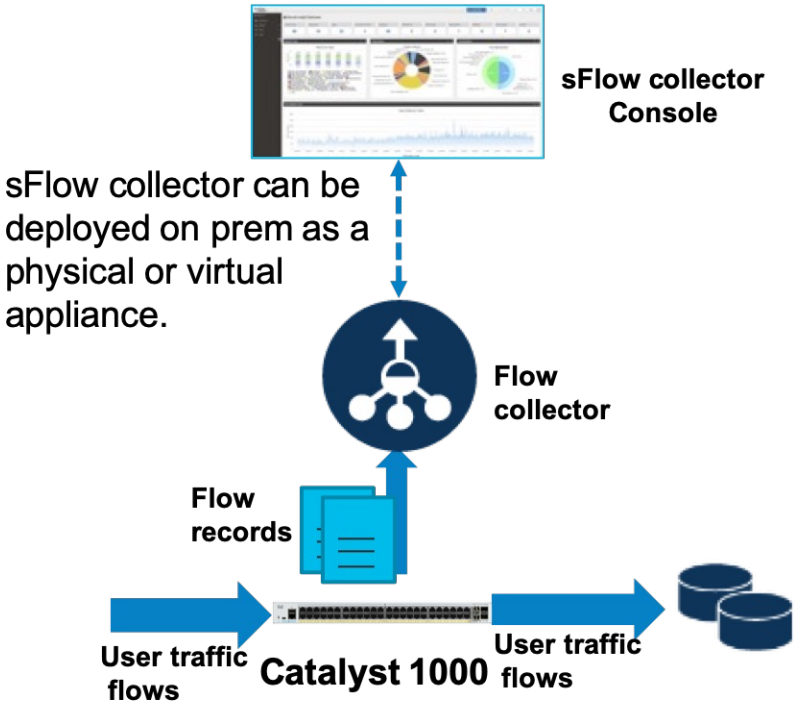
sFlow in Catalyst Catalyst 1000

- sFlow is a technology for monitoring traffic by using sampling mechanisms implemented as an agent on the switch for monitoring traffic

- sFlow agent on these switches will use the hardware functionality to mirror the sampled packets to the CPU and will have the software support to export the packets to the sFlow collector

- sFlow version 5 is supported and the implementation is in compliant with the RFC 3176

sFlow Configuration and Guidelines



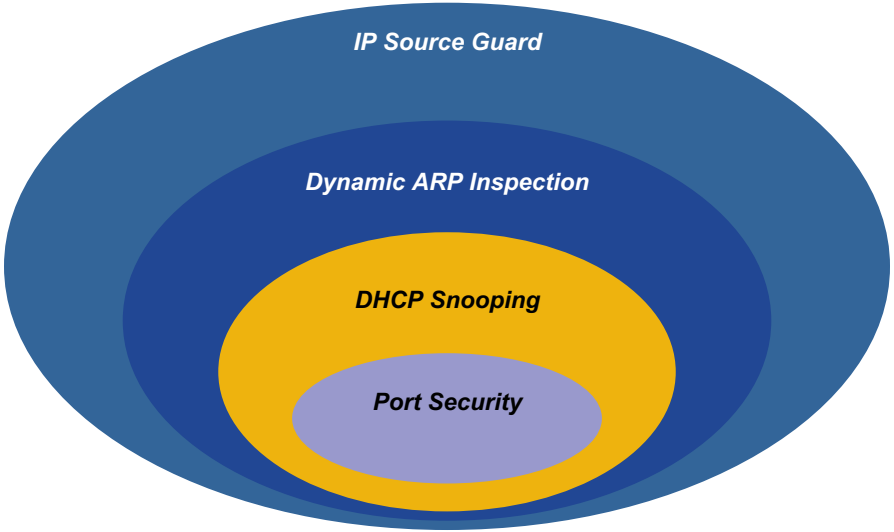
- Flows can be monitored both on ingress and egress direction
- Up to 2 flow collectors can be configured on a switch
- Monitoring is only supported on physical interface
- sFlow datagrams are exported to collectors as UDP flows
- The rate-limiting for ingress and egress sFlow packets is set at 1000 PPS per asic both directions inclusive.
- The flow sampling is enabled per direction by specifying the collector to which the packet samples from that interface needs to be sent to.
- The rate and the max header size are optional with default values being 1 out-of 2048 and 116 bytes respectively.

sFlow restrictions and considerations

- ip routing must be enabled before enabling sFlow
- sFlow is not supported in a stacked environment
- The rate limit for sflow sampled packets is set at 1000PPS per asic both directions inclusive (2000 PPS on a dual asic box)
- With the rate limiting in place, only 1000 packets per second for each asic will reach the CPU independent of the number of interfaces on which sflow is enabled and the sampling rate configured.
- ‘drops’, ‘sample pool’, ‘frame length’ in the flow sample header will not be exported with accuracy
- sFlow is not supported on Smart Managed SKUs

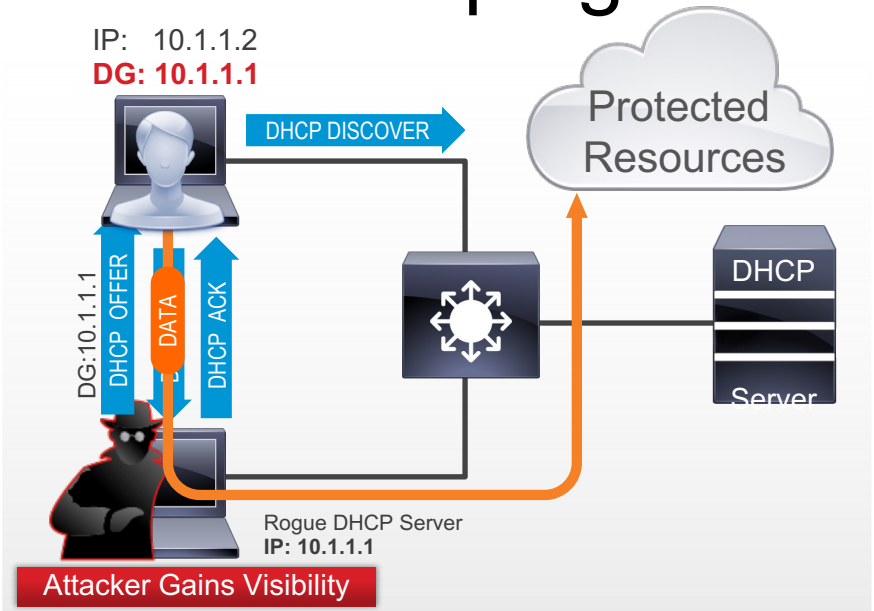
Security

Catalyst Integrated Security Features



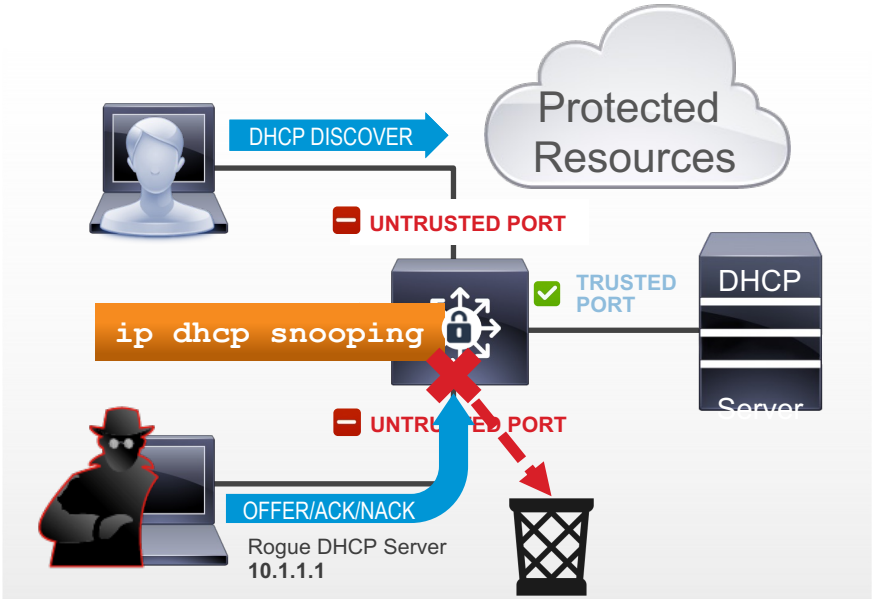
Attack	Catalyst Feature
MAC Address Flooding	Port Security
DHCP Rogue Server for Default Gateway Interception	DHCP Snooping
ARP Spoofing or ARP Poisoning	Dynamic ARP Inspection
IP Spoofing or MAC Spoofing	IP Source Guard

DHCP Snooping



Problem

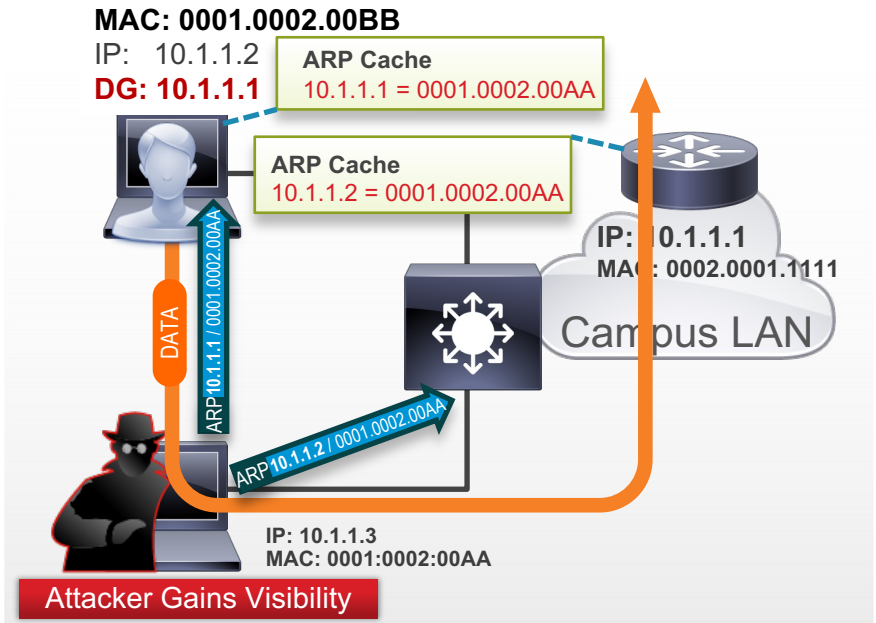
Rogue DHCP servers are often used in man-in-the-middle or denial of service attacks for malicious purposes



Solution

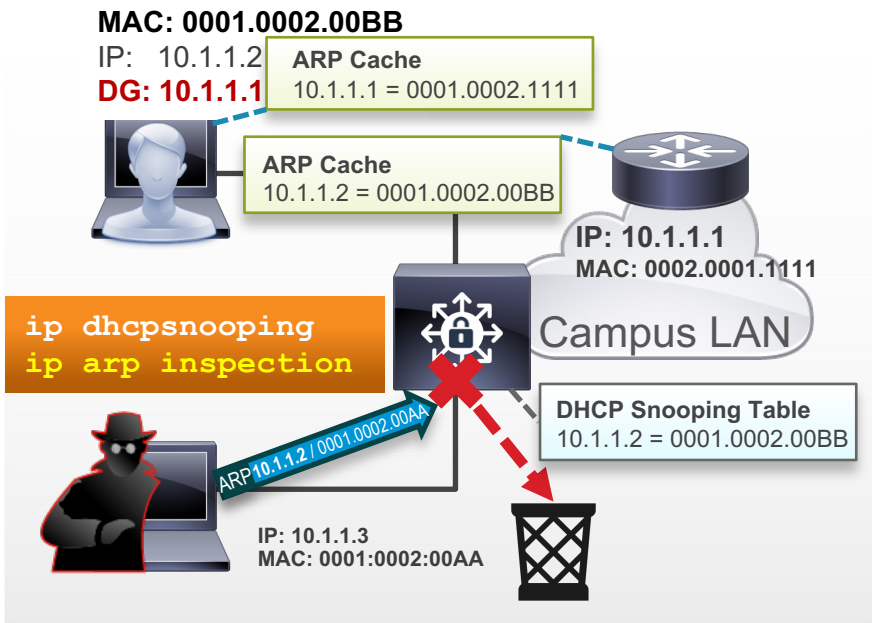
The DHCP snooping feature filters messages and rate limits rogue DHCP traffic from untrusted sources & builds DHCP binding table

CISF: Dynamic ARP Inspection (DAI)



Problem

Attackers can poison the ARP cache on the destination devices and engineer the network traffic to gain visibility into it

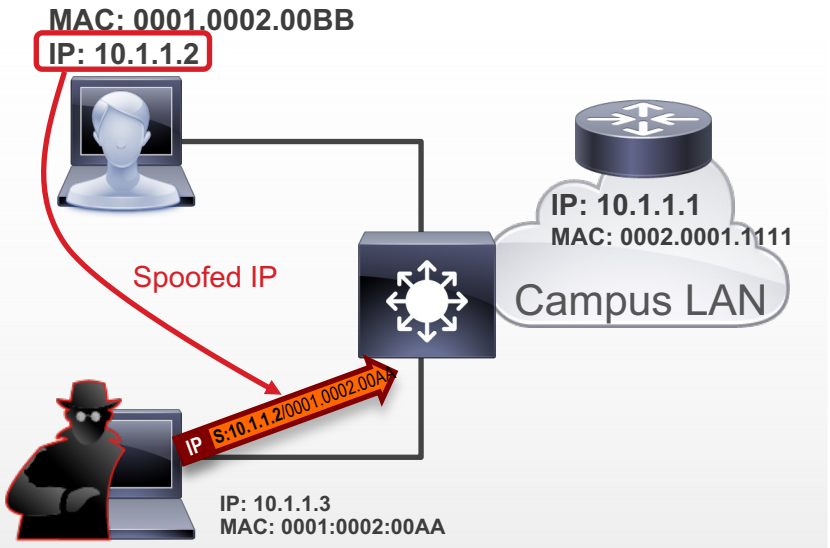


Solution

Dynamic ARP inspection (DAI) prevents ARP attacks by interception all ARP requests and responses at the access

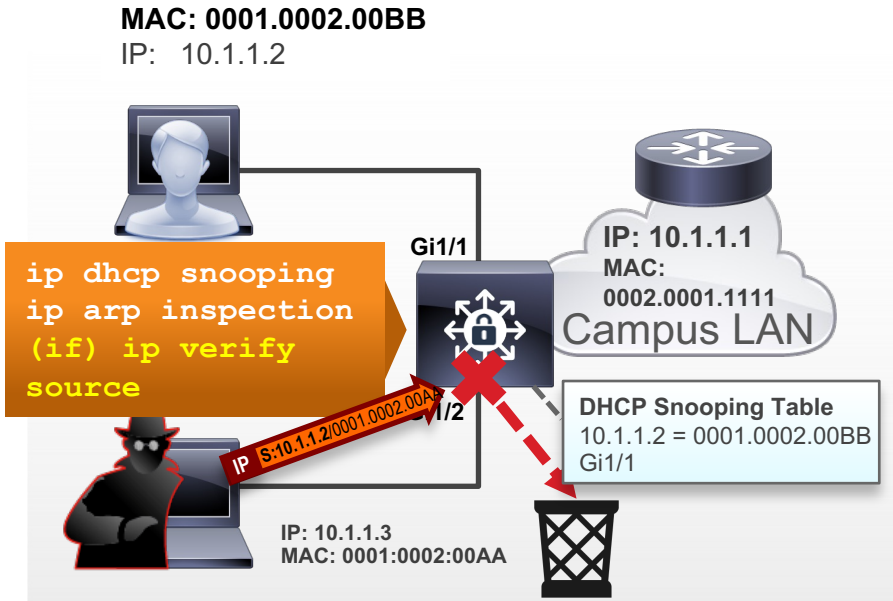
IP Source Guard

Catalyst Integrated Security



Problem

Illegitimate hosts can spoof IP addresses and MAC addresses of authorized hosts and gain illegal access into the network



Solution

IPSG Automatically configures a Port ACL for IP address and adds a MAC address to port security based on DHCP snooping binding table. Rouge traffic is blocked

Auto Secure

- 1 Line – ‘auto security’ applies 3 simple security features
  - DHCP Snooping
  - Dynamic ARP Inspection
  - Port Security
- Global Config enables on all ports as well
- Based on port mode – access OR trunk, it applies host config or uplink config

Auto Secure – Actual Config & Show Commands

```
auto security
!
interface GigabitEthernet3/3
 description Connected to wired PC
 switchport access vlan 11
 switchport mode access
 auto security-port host
!
interface TenGigabitEthernet1/1
 description Trunk Port
 switchport mode trunk
 auto security-port uplink
```

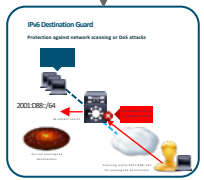
```
Switch#sh auto security configuration
%AutoSecure provides a single CLI config 'auto secure'
 to enable Base-line security Features like
 DHCP snooping, ARP inspection and  Port-Security

Auto Secure CLIs applied globally:
----------------------------------
ip dhcp snooping
ip dhcp snooping vlan 2-1005
no ip dhcp snooping information option
ip arp inspection vlan 2-1005
ip arp inspection validate src-mac dst-mac ip


Auto Secure CLIs applied on Access Port:
----------------------------------------
switchport port-security maximum 2
switchport port-security maximum 1 vlan access
switchport port-security maximum 1 vlan voice
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100


Auto Secure CLIs applied on Trunk Port:
---------------------------------------
ip dhcp snooping trust
ip arp inspection trust
switchport port-security maximum 100
switchport port-security violation restrict
switchport port-security
```

```
Switch#sh auto security
Auto Secure is Enabled globally

AutoSecure is Enabled on below
interface(s):
-----------------------------------
---------
   TenGigabitEthernet1/1
   GigabitEthernet3/1
   GigabitEthernet3/3
   GigabitEthernet3/4
   GigabitEthernet3/5
   GigabitEthernet3/6

Switch#
```

IPv6 First-Hop Security (FHS)

Securing Enterprise IPv6 Networks

IPv6 First-Hop Security

RA Guard	DHCPv6 Guard	Source/Prefix Guard	Destination Guard	ND Multicast Suppress
				
Protection: • Rogue or malicious RA • MiM attacks	**Protection:** • Invalid DHCP offers • DoS attacks • MiM attacks	**Protection:** • Invalid source address • Invalid prefix • Source address spoofing	**Protection:** • DoS attacks • Scanning • Invalid destination address	**Reduces:** • Control traffic necessary for proper link operations to improve performance

Core Features | Advance Features | Scalability and Performance

Robust Security for Emerging BYOD Trends

Secure BYOD with 802.1X

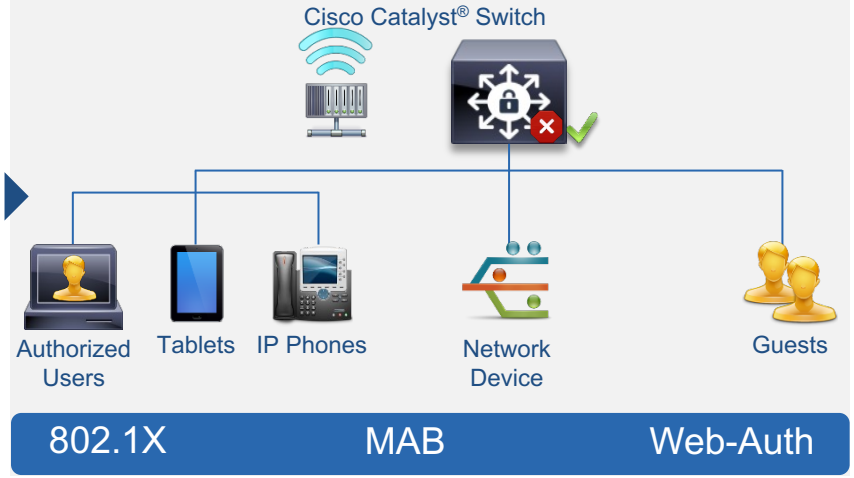
Identity Differentiators

- Monitor mode
  - Unobstructed access
  - No impact on productivity
  - Gain visibility
- MAC-based authentication
- Flexible authentication sequence
  - Helps enable single configuration for most use cases
  - Flexible fallback mechanism and policies

Rich and Robust 802.1X

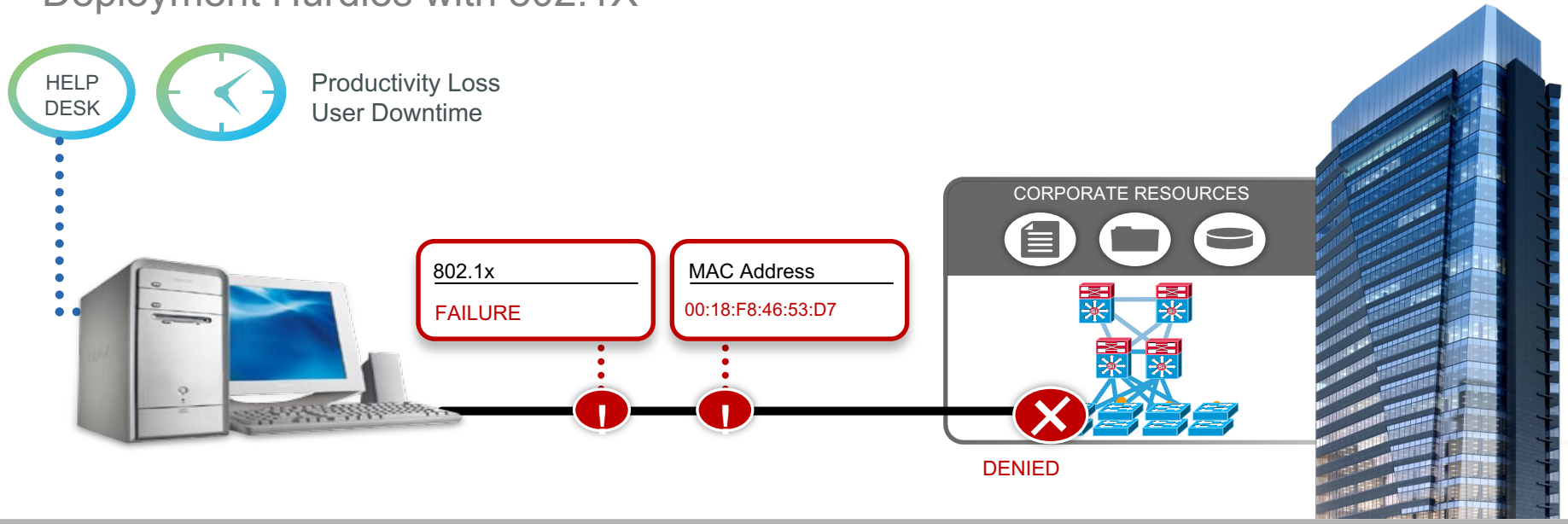
- IP telephony support
  Support for virtual desktop environments
  - Single host mode
  - Multi-host mode
  - Multi-auth mode
  - Multi-domain authentication
- Critical data and voice authentication
  - Business continuity in case of failure

Authentication Features



Authorized Access

Deployment Hurdles with 802.1X



The Challenge

Implement Identity-Based Access Control

Typical Deployment Scenario

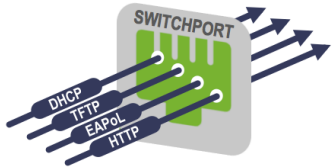
Deploy Access Control

Failed Access due to non 802.1X client, supplicant variation etc.

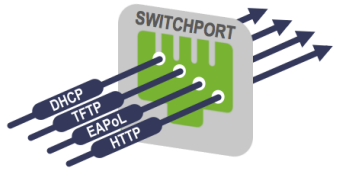
User contacts help desk for assistance

Troubleshooting problem results in loss of productivity

Start with Monitor Mode



Before Authentication



After Authentication

Traffic always allowed irrespective of authentication status

MONITOR MODE : GOALS

- No impact to existing network access
- See
  - What is on the network
  - Who has a supplicant
  - Who has good credentials
  - Who has bad credentials
- Deterrence through accountability

```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
switchport voice vlan 10
authentication host-mode multi-auth
authentication open
authentication port-control auto
mab
dot1x pae authenticator
authentication violation restrict
```

Monitor Mode

Basic 1X/MAB

MONITOR MODE : CONFIGURATION

- Enable 802.1X and MAB
- Enable Open Access

  All traffic in addition to EAP is allowed Like not having 802.1X enabled except authentications still occur
- Enable Multi-Auth host mode
- No Authorization

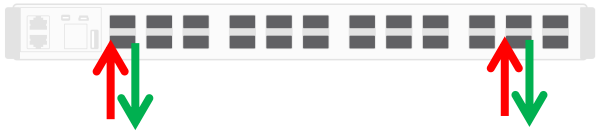
802.1X Is Not Just a Check Box

Cisco Simplifies 802.1X Deployments

Deployment Hurdle	Feature
How do you support non 802.1X clients and Guest users/devices?	• Guest VLAN • MAC Authentication Bypass, Web Authentication • Monitor Mode
How do you handle failed access?	• Failed Authentication VLAN • Monitor Mode
How do you support multiple users or devices on the same port?	• Multi domain Authentication • Multi-Authentication • MAC based VLAN assignment
How do you support various kinds of devices with different authentication mechanisms?	• Flexible Authentication via Automated 802.1X, MAB, web Auth • Different Supplicant types for different Client Operating Systems • Wake On LAN • IOS Sensor
How do you handle devices moving in your network?	• MAC Move/Replace
How do you handle Device proliferation?	• IOS Sensor • Monitor Mode

Cisco Has Many Features to Enhance 802.1x and Make Identity Networking Truly Deployable, Not Just a Check-Box

Port ACL



Security Boundary

Ports
VLANs

Attachment

Layer 2 Interface

Direction

Ingress

Supported ACL Types

MAC ACL, IP ACLs
(Standard & Extended)

Configuration

```
access-list 2 permit 36.48.0.3
access-list 2 deny 36.48.0.0 0.0.255.255
access-list 2 permit 36.0.0.0 0.255.255.255

interface gigabitethernet0/1
   switchport
   ip access-group 2 in
```

ACL assigned to a Layer-2 Interface

Group/Client ACL

Security Boundary

Client

Attachment

Client

Direction

Ingress Only

Supported ACL Types

MAC ACL, IP ACLs
(Standard & Extended)

Configuration

```
access-list 2 permit 36.48.0.3
access-list 2 deny 36.48.0.0 0.0.255.255
access-list 2 permit 36.0.0.0 0.255.255.255
```

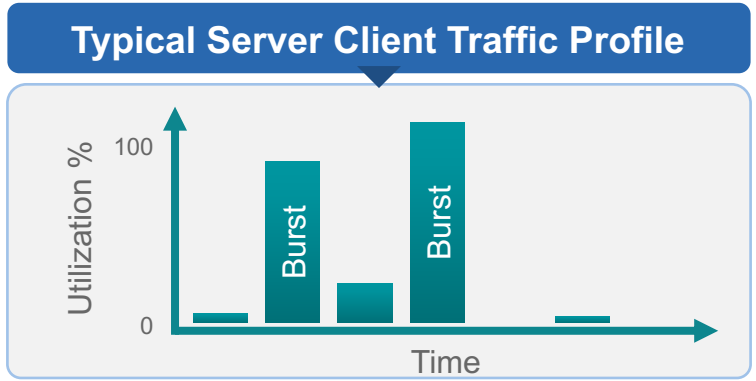
ACL dynamically assigned to a user group or client based on their identity

Power

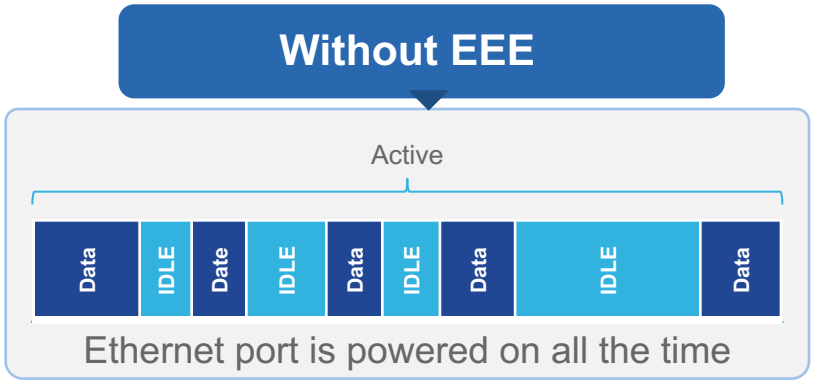
Energy Efficient Ethernet (EEE) - IEEE 802.3az

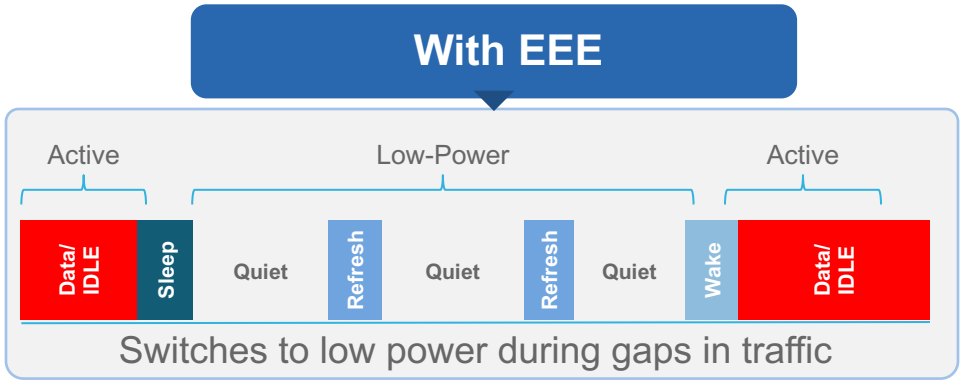
- Energy Efficient Ethernet saves power during gaps in data stream
- The Cisco Catalyst® 1000 Series Switches MAC instructs an attached PHY when to enter lower power idles (LPI) mode for power-saving
- LPIs are sent over the link, and the link remains up
- LPIs can be brief and frequent, without impacting the link traffic
- Both link partners must support EEE to see any savings
- EEE is disabled by default on the ports

Energy Efficient Ethernet (EEE) - 802.3az



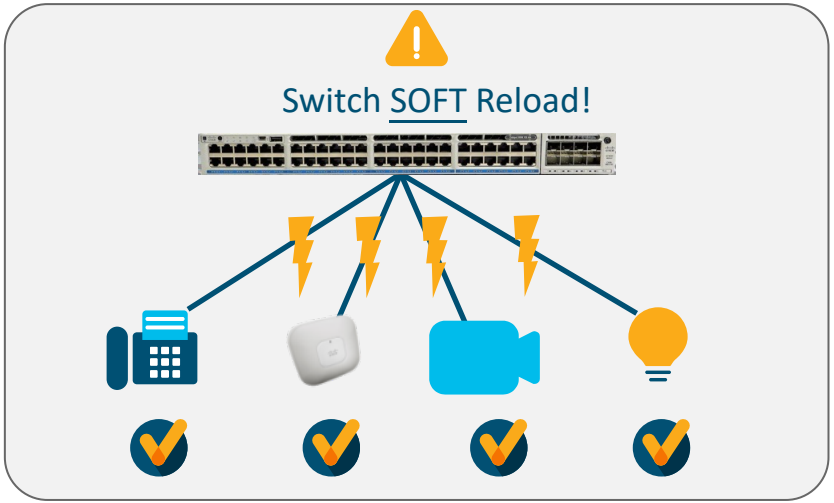
Energy Efficient Ethernet





Perpetual PoE

PoE devices connected to switch stay powered even on Switch Reload!

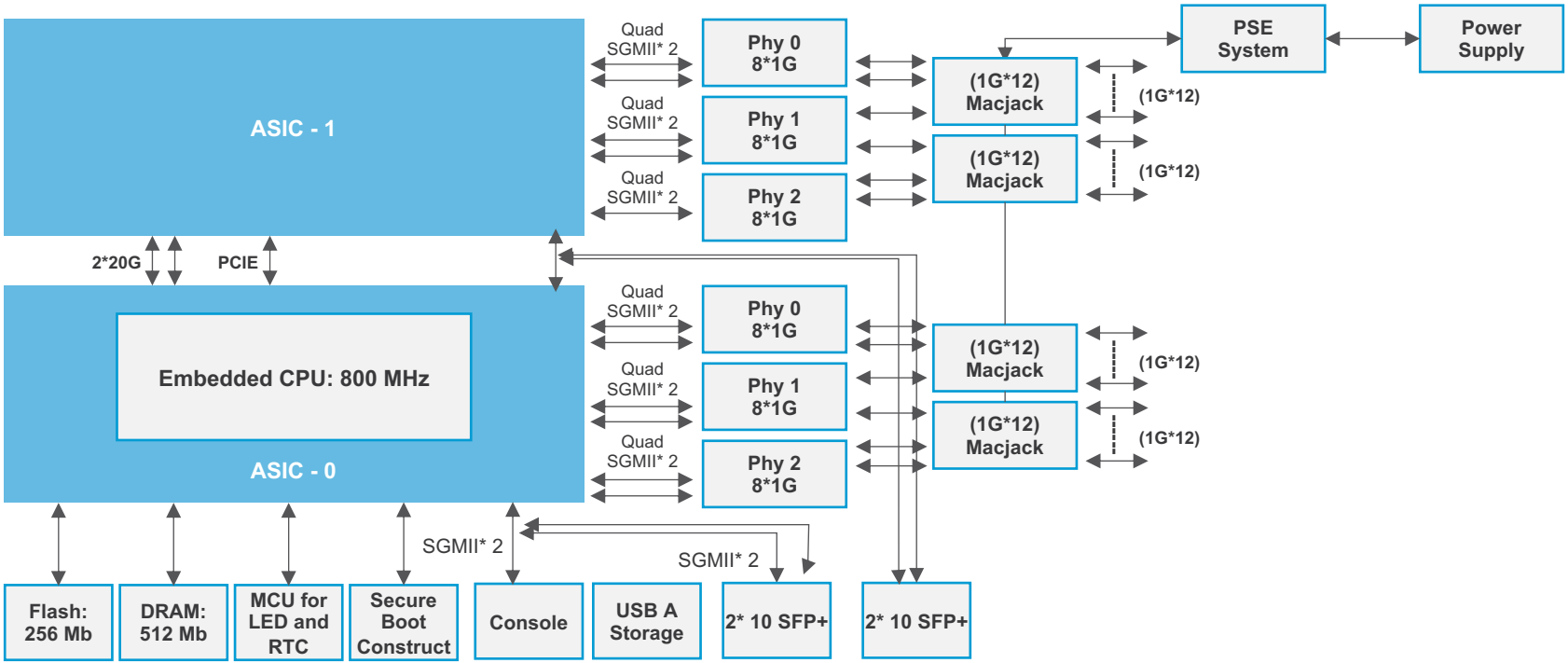



```
Switch> enable
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# power inline port perpetual-poe-ha
Switch(config-if)#end
```

- PoE devices continue to get Last Negotiated Power
- Applicable to “Soft” Reload – image upgrade, software crash, manual reboot
- Not applicable during power outage to switch/FEP removed

Catalyst 1000 Series Switching Architecture

Catalyst 1000 Series switch - 48 Port Layout



ASIC to port Mapping Catalyst 1000 Series – 24 Port

```
Catalyst1000#show platform pm if-numbers


interface gid  gpn  lpn  port slot unit slun port-type lpn-idb gpn-idb
------------------------------------------------------------------------
Gi0/1     1    1    1    0/1  1    1    1    local     Yes     Yes
Gi0/2     2    2    2    0/0  1    2    2    local     Yes     Yes
Gi0/3     3    3    3    0/3  1    3    3    local     Yes     Yes
Gi0/4     4    4    4    0/2  1    4    4    local     Yes     Yes
Gi0/5     5    5    5    0/5  1    5    5    local     Yes     Yes
Gi0/6     6    6    6    0/4  1    6    6    local     Yes     Yes
Gi0/7     7    7    7    0/7  1    7    7    local     Yes     Yes
Gi0/8     8    8    8    0/6  1    8    8    local     Yes     Yes
Gi0/9     9    9    9    0/9  1    9    9    local     Yes     Yes
|
|
|
|
Gi0/27    27   27   27   0/26 1    27   27   local     Yes     Yes
Gi0/28    28   28   28   0/27 1    28   28   local     Yes     Yes
Te0/1     29   29   29   0/24 1    1    29   local     Yes     Yes
Te0/2     30   30   30   0/25 1    2    30   local     Yes     Yes
Te0/3     31   31   31   0/26 1    3    31   local     Yes     Yes
Te0/4     32   32   32   0/27 1    4    32   local     Yes     Yes
St1       504  504  0    0/0  1    0    0    internal  Yes     Yes
```

Catalyst C1000-24P-4X-L

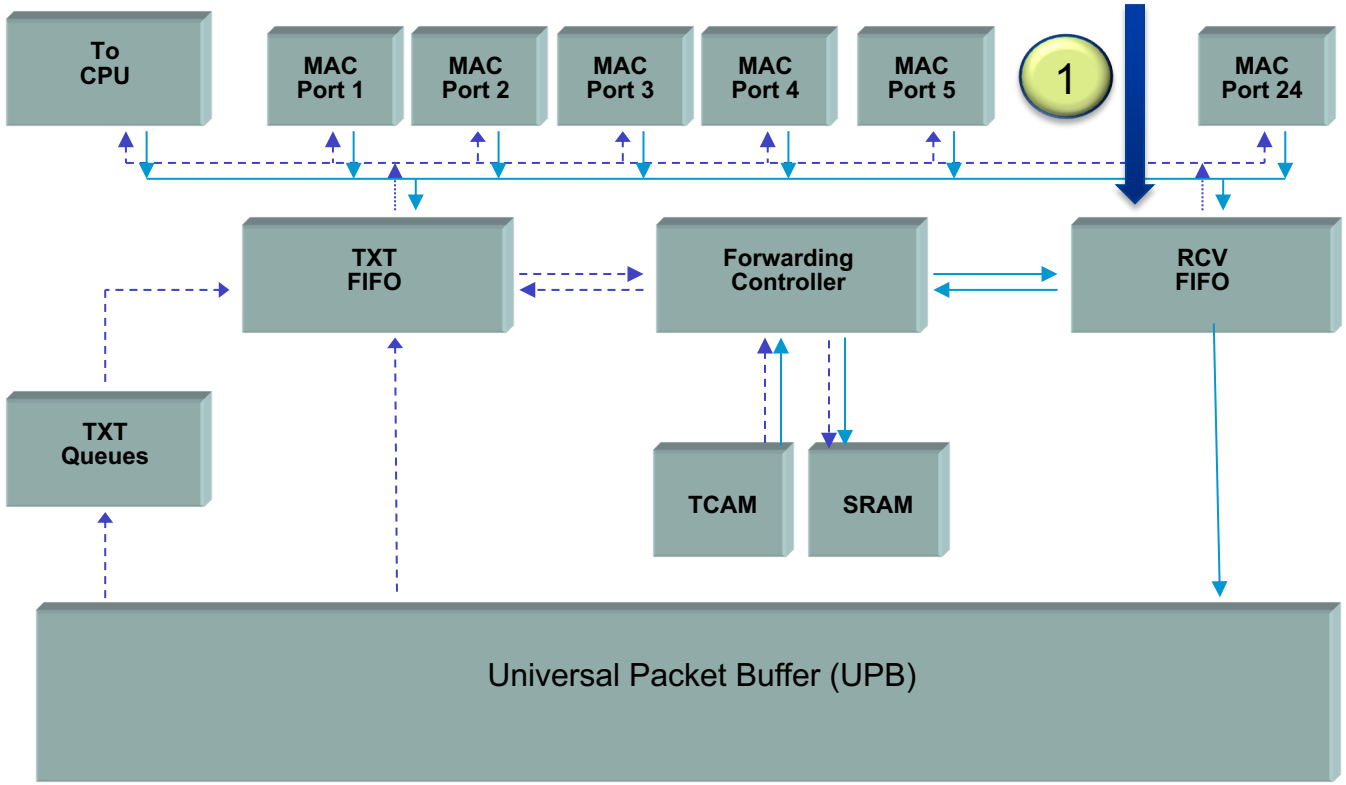
Switch	Ports	Model	SW Version	Mode
*1	28	C1000-24P-4X	15.2.7	Bundle

Console Access

- C1000 Supports USB (type B) console and traditional RJ45 console
- Each member can have 1 active media (RJ45 or USB)
- Stack member console automatically redirected to Master console
- Only active media will accept input
- Both Console media will echo output.
- USB console accepts input when both RJ45 & USB are connected
- RJ45 echo output only
- USB console timeout can be configured. “usb-inactivity-timeout” to prevent blocking of RJ45 media due to forgotten USB

Packet walks

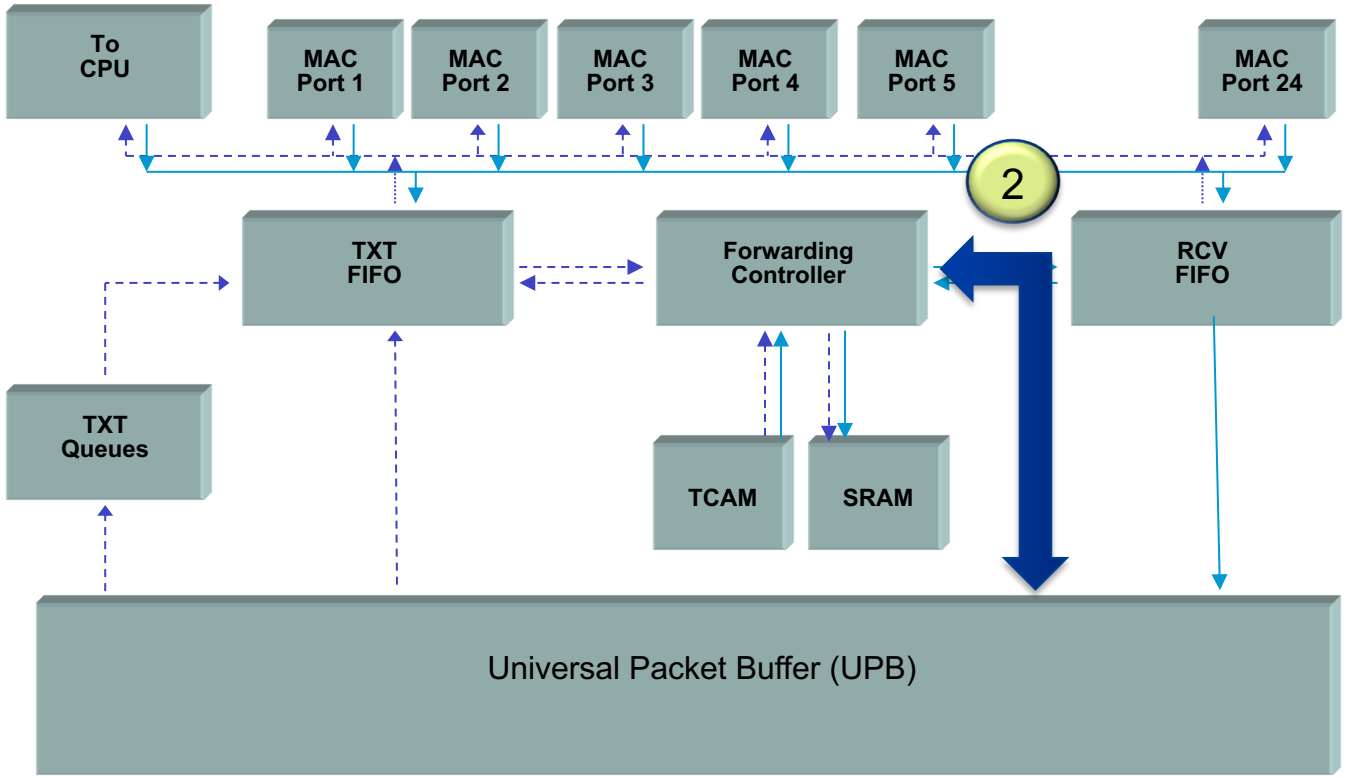
Packet walk - Ingress



1

Packets entering the switch are received by the Receive FIFO after VLAN decapsulation

Packet walk - Ingress

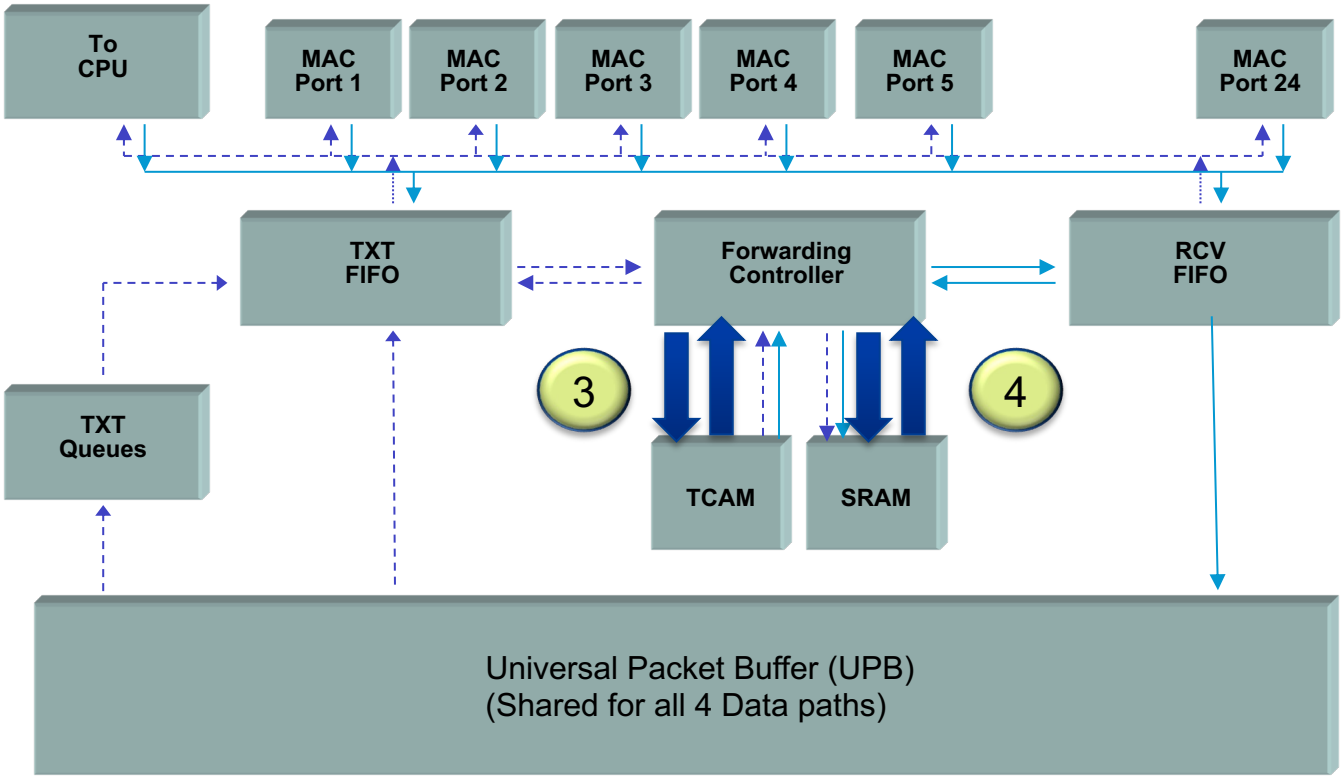


2

Copy of the first 200 bytes is sent into the Forwarding Controller for processing (forwarding, ACL, QOS lookups)

The whole packet is sent to UPB

Packet walk - Ingress



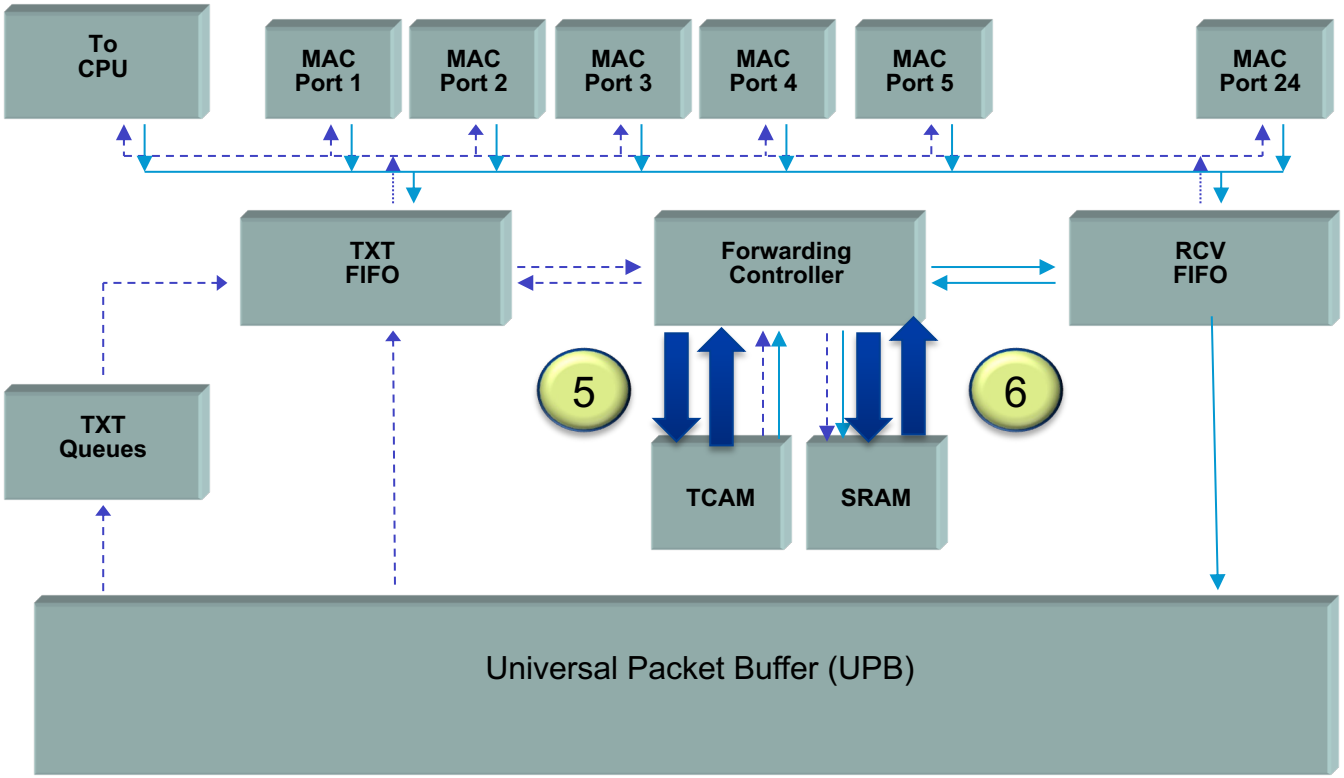
3

Search Engine in the Forwarding Controller does Learning lookup in TCAM and receives the index

4

The Forwarding Controller queries the SRAM with the index to get the L2 Address table info for learning .

Packet walk - Ingress



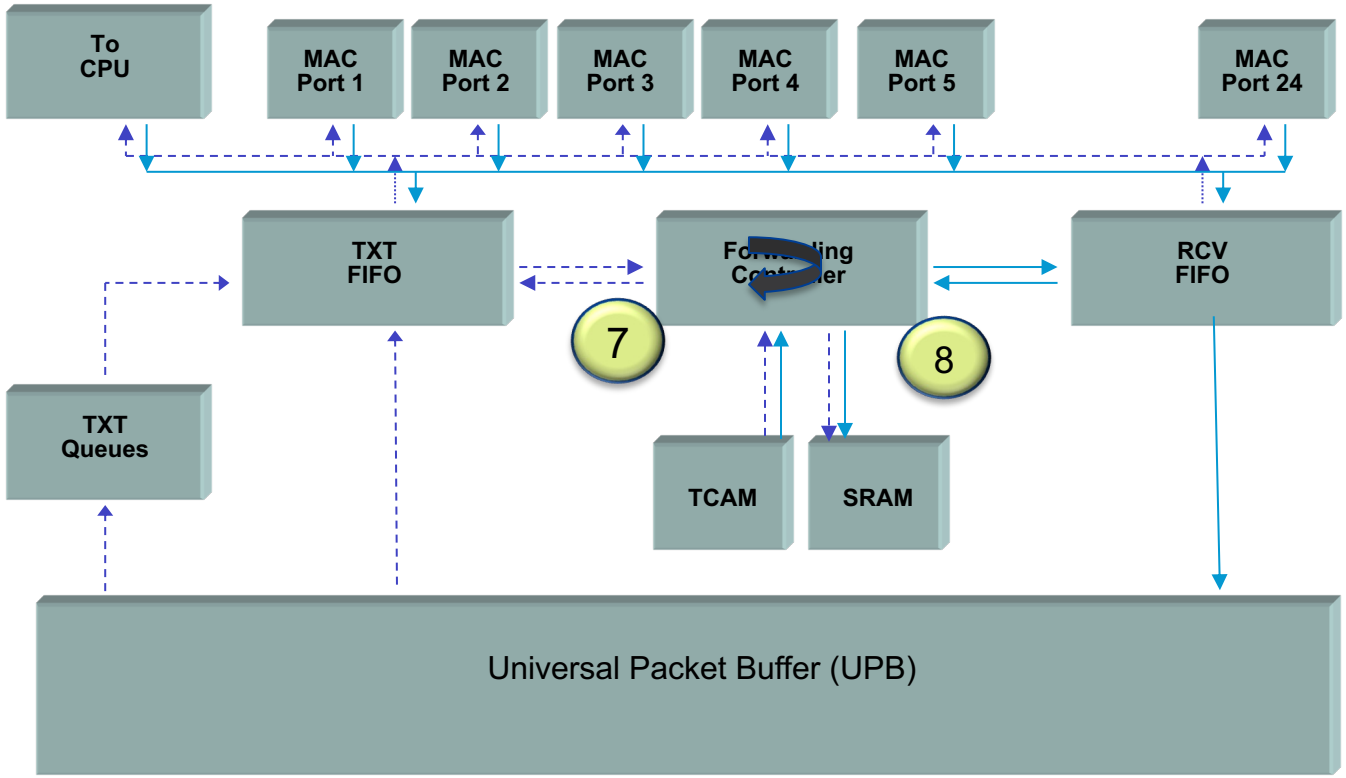
5

Search Engine in Forwarding Controller does QOS and ACL Look up in TCAM. Index returned

6

Forwarding Controller queries the SRAM for the respective Ingress ACL and QOS response

Packet walk - Ingress



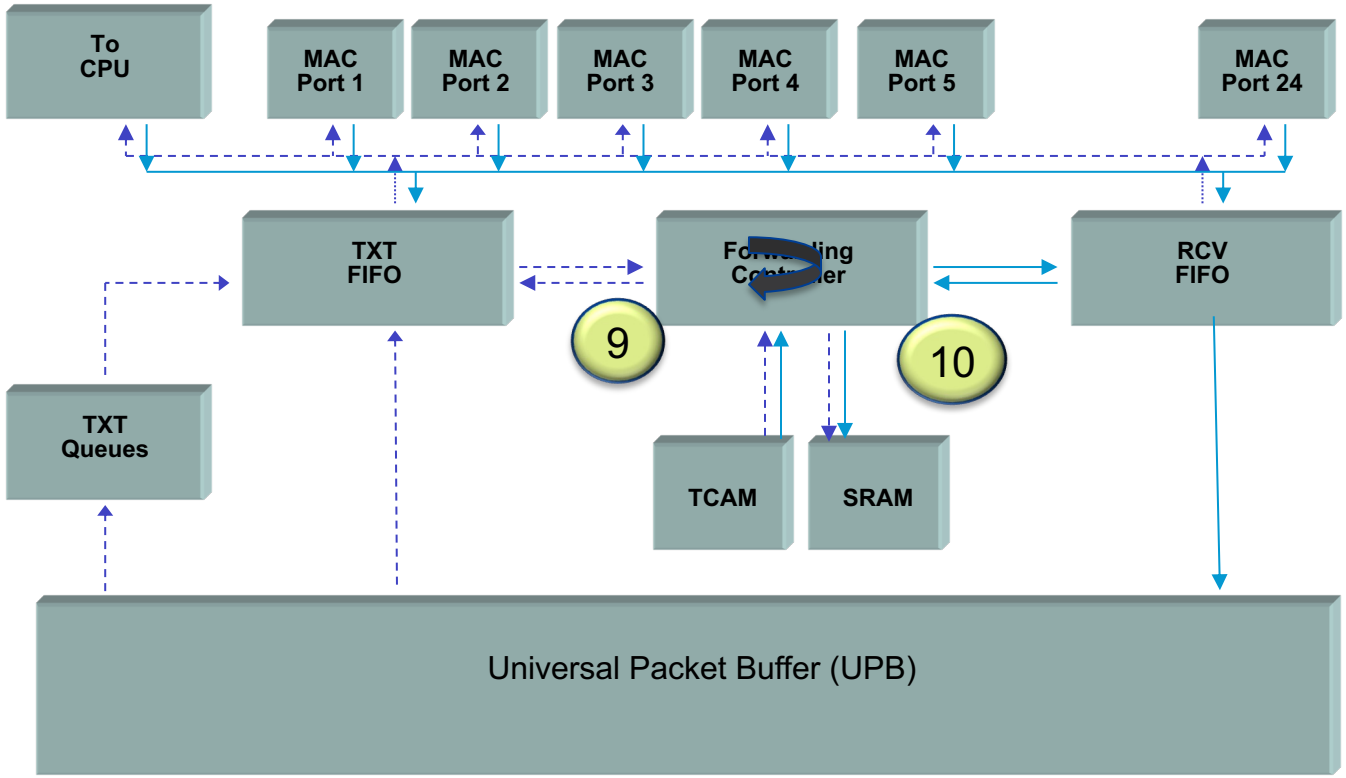
7

Look up to the policer. How much policing to do?

8

Policing information returned

Packet walk - Ingress



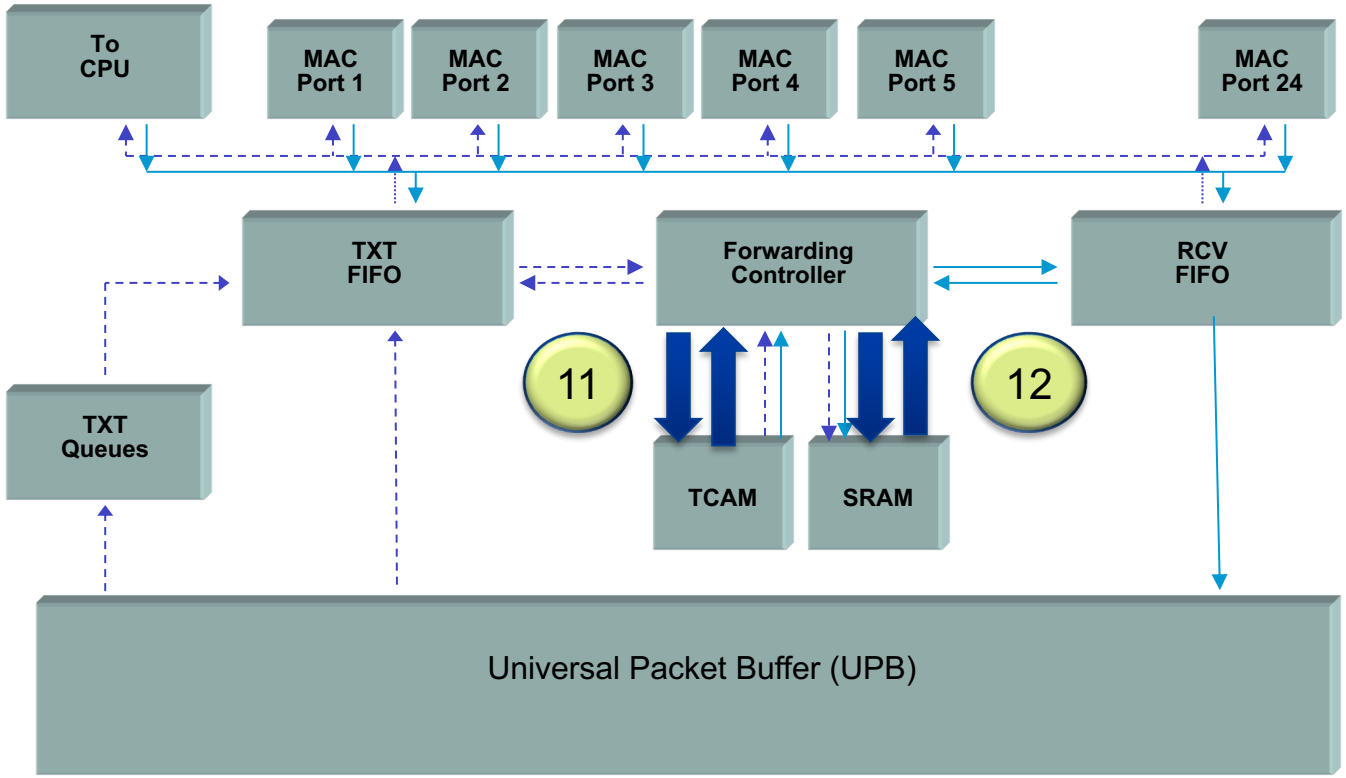
9

Look up to the sFlow record. Index retuned

10

Update the result table entry pointed by the Index

Packet walk - Ingress



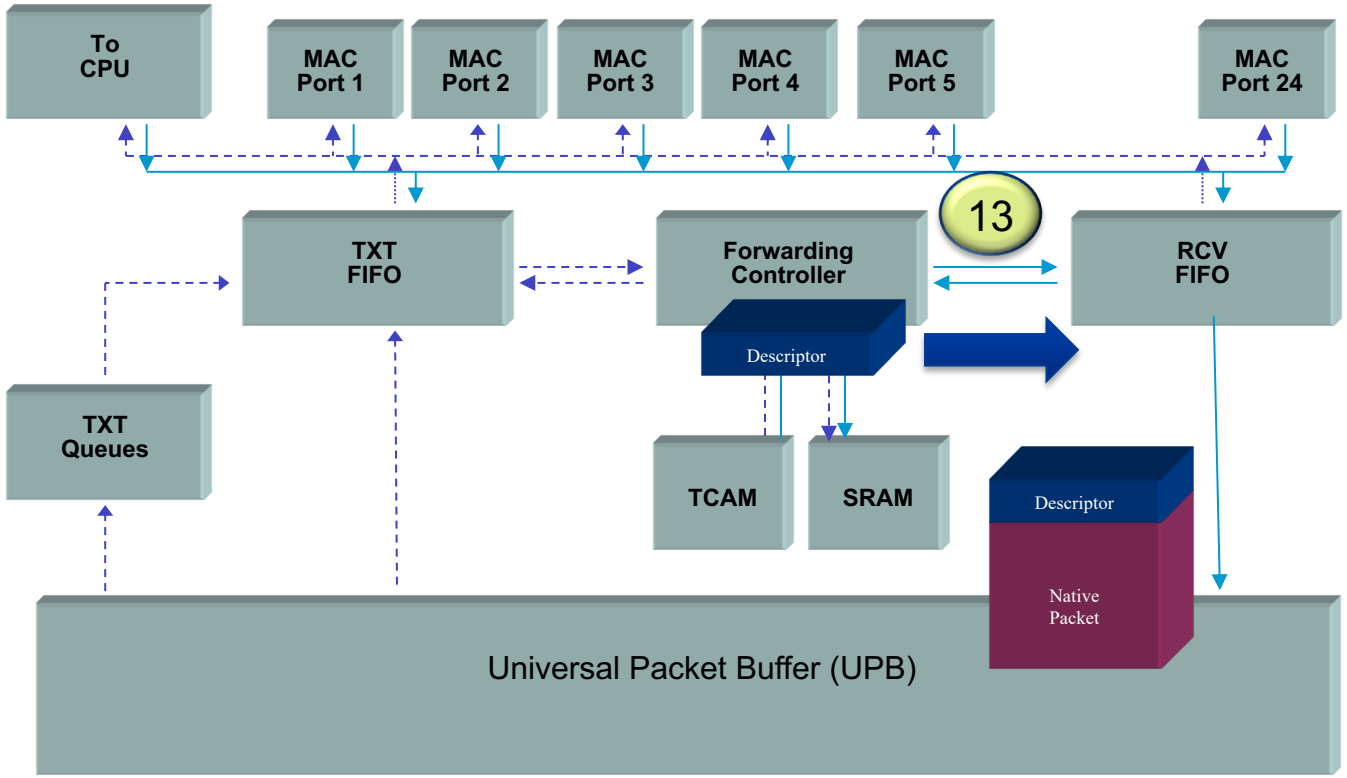
11

Search Engine in Forwarding Controller does L2/L3 Forwarding Look up in TCAM. Index returned

12

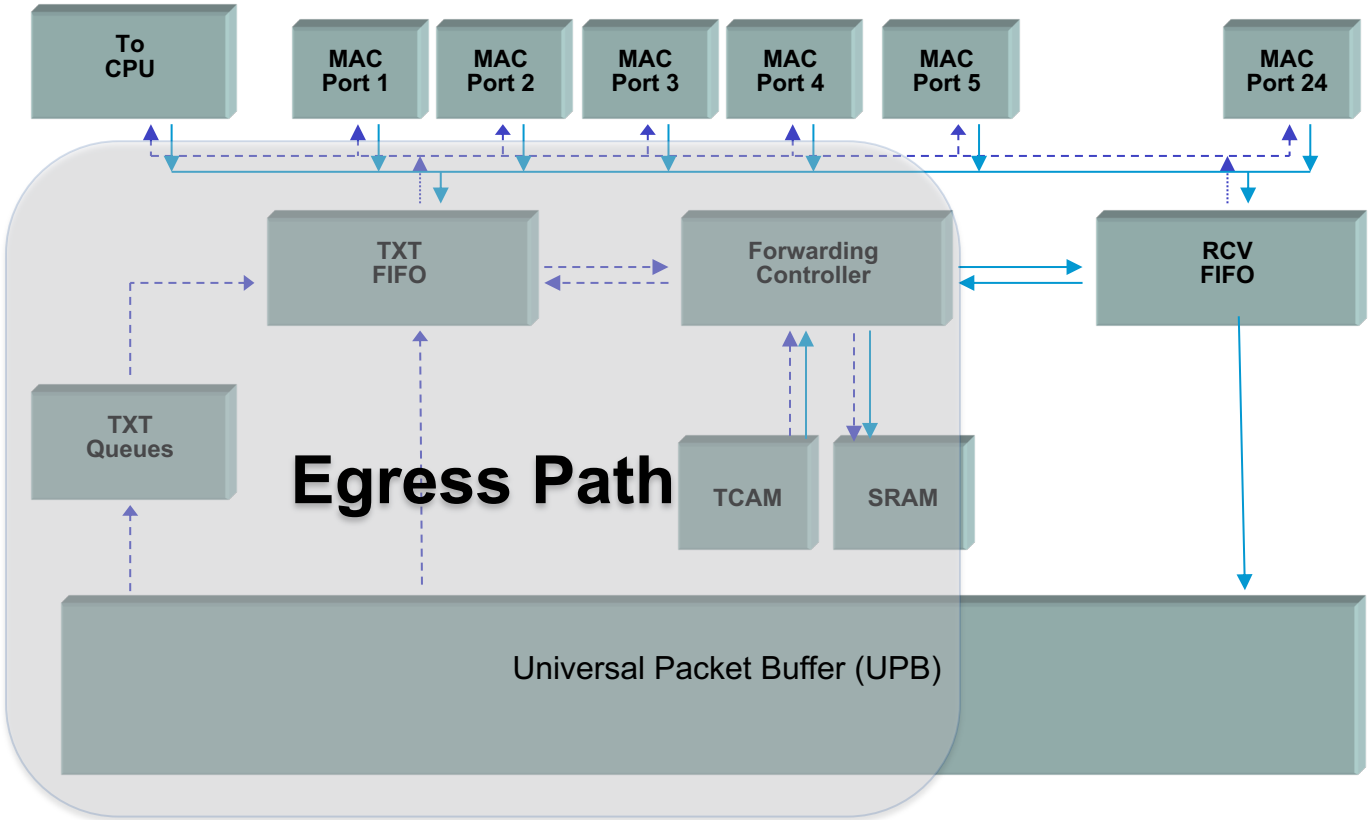
Forwarding Controller sends Index to the SRAM for destination details. Destination information returned

Packet walk - Ingress

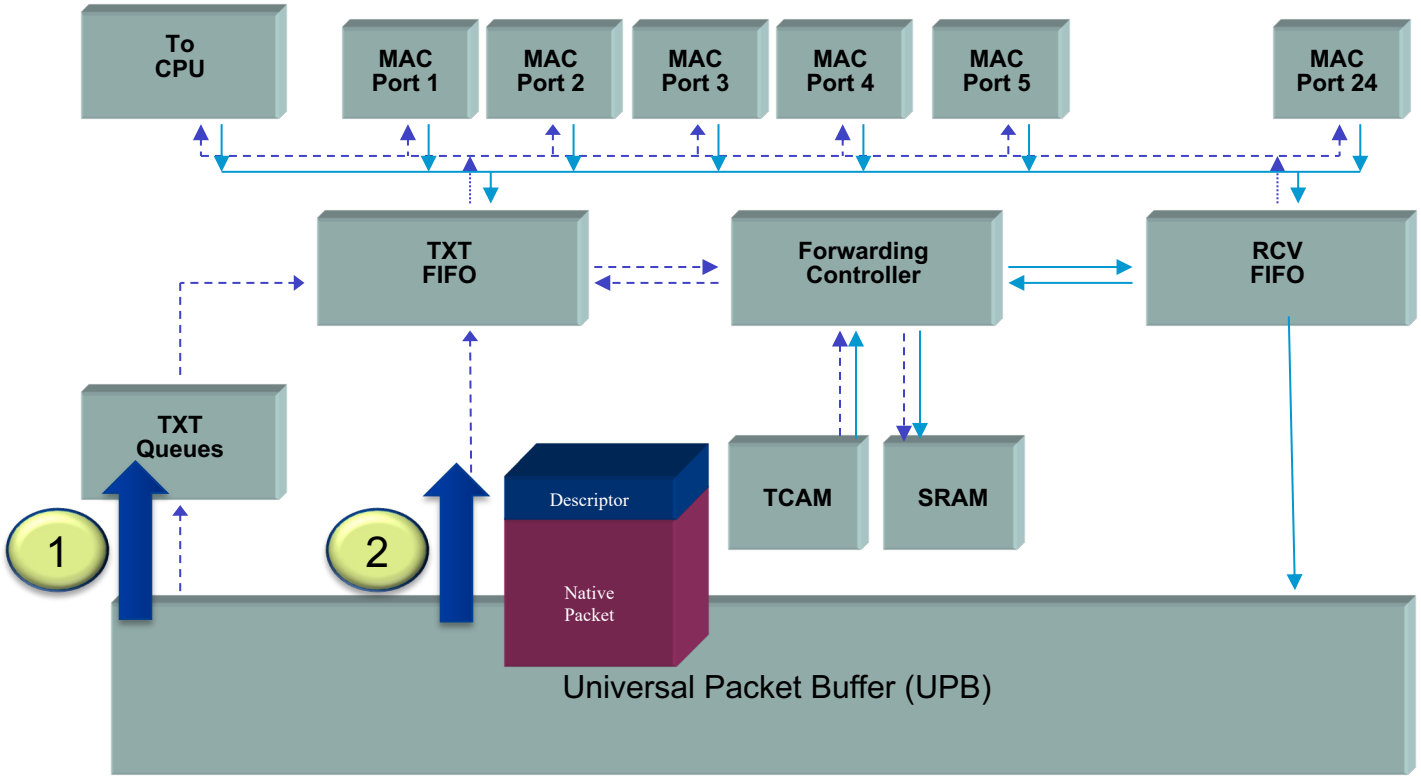


Descriptor with lookup results is appended to the original packet and stored in UPB

Within the ASIC – Single Data Path



Packet walk - Egress



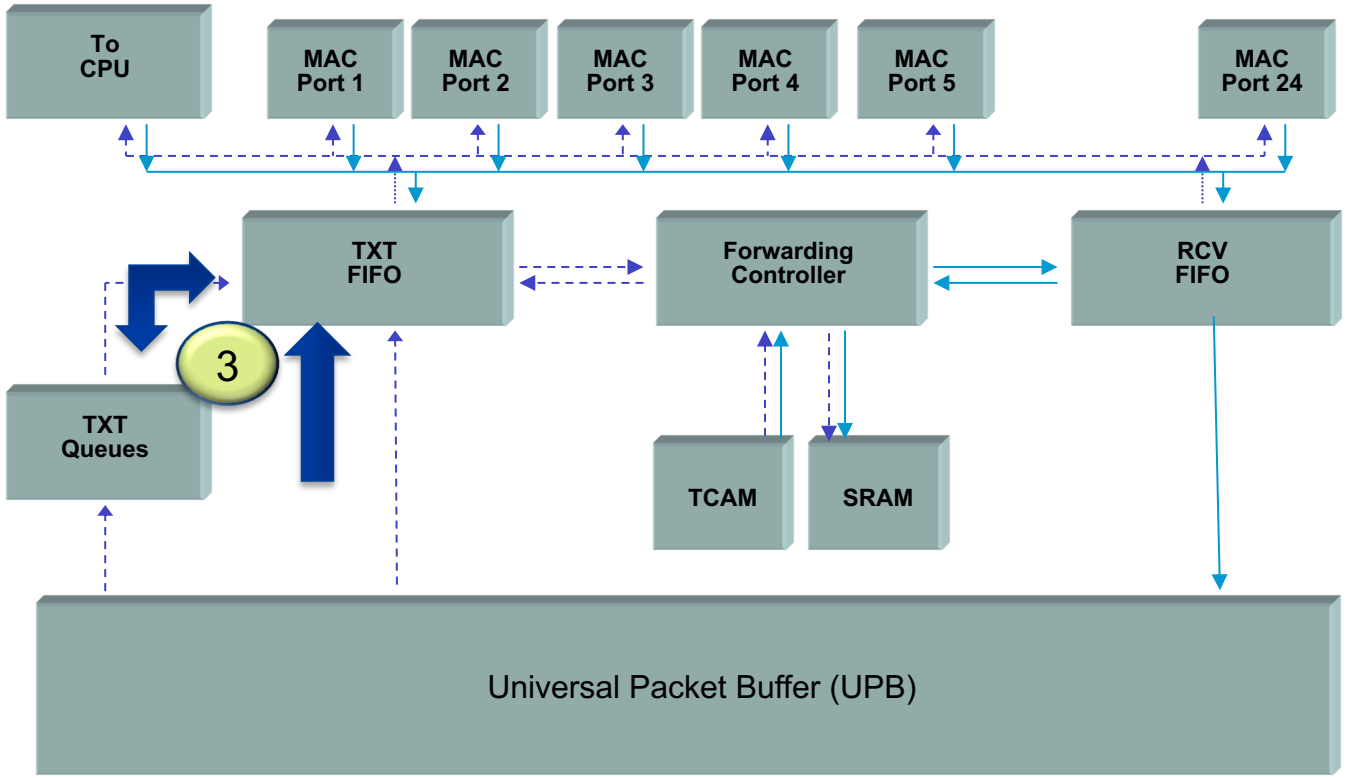
1

Pointer to the frame is placed on targeted Transmit Queue

2

Frame data from UPB is transferred to Transmit FIFO

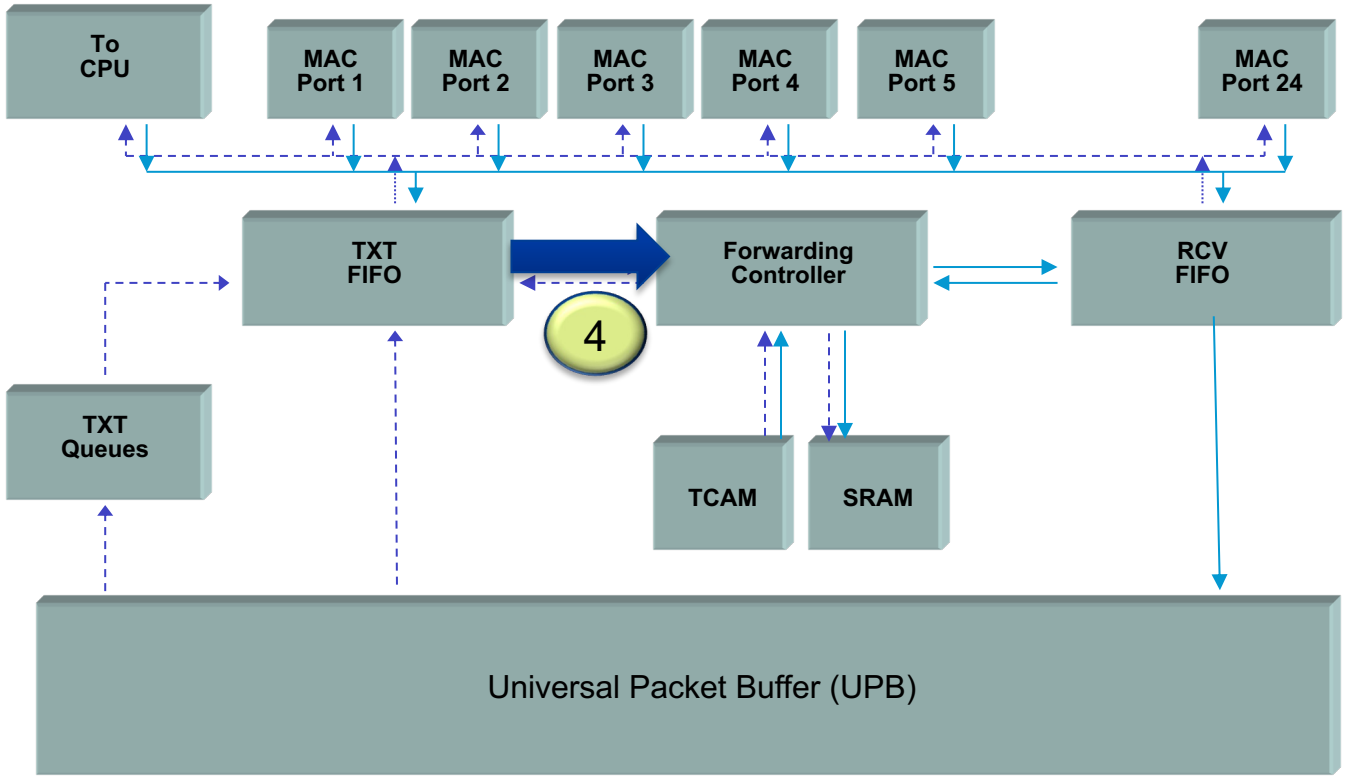
Packet walk - Egress



3

Packets egresses and is stored in the Transmit FIFO for egress processing

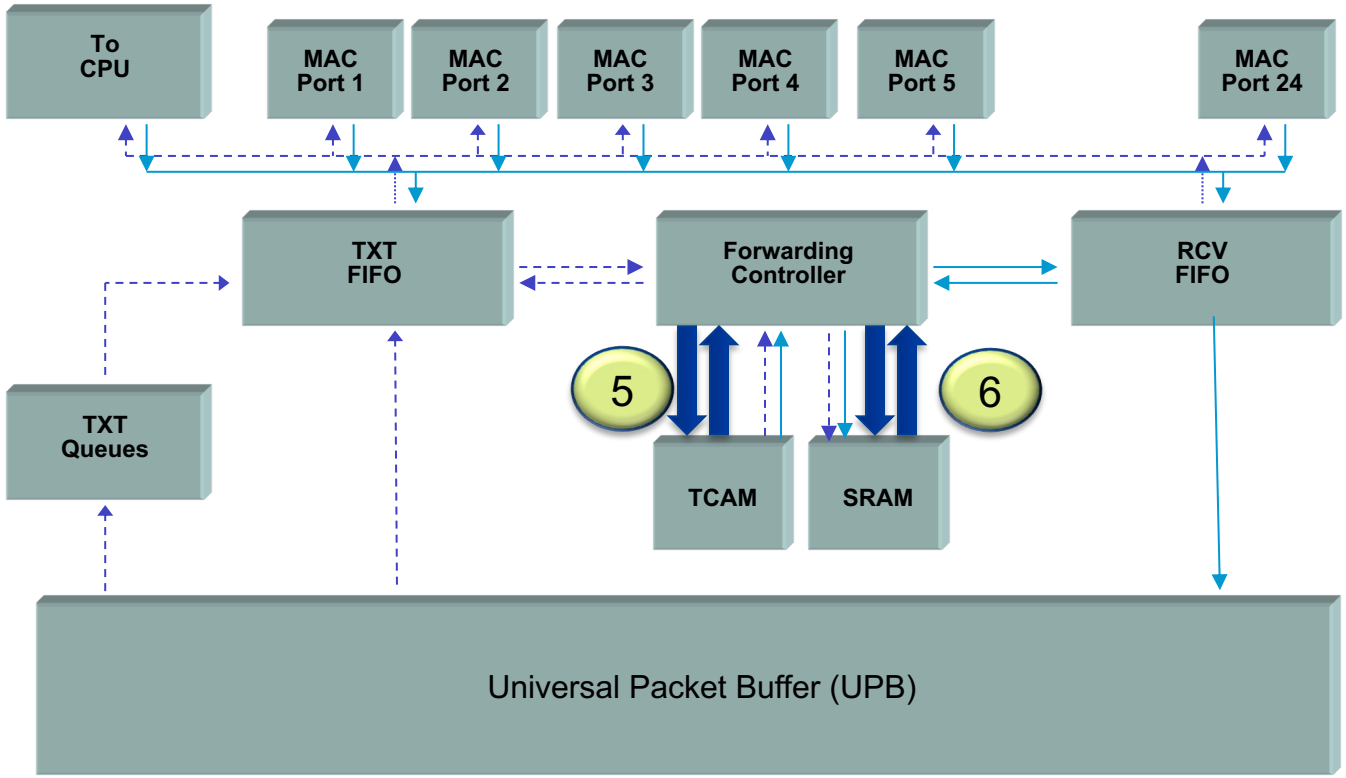
Packet walk - Egress



4

First 200 bytes & descriptor sent to the Forwarding Controller for egress processing

Packet walk - Egress



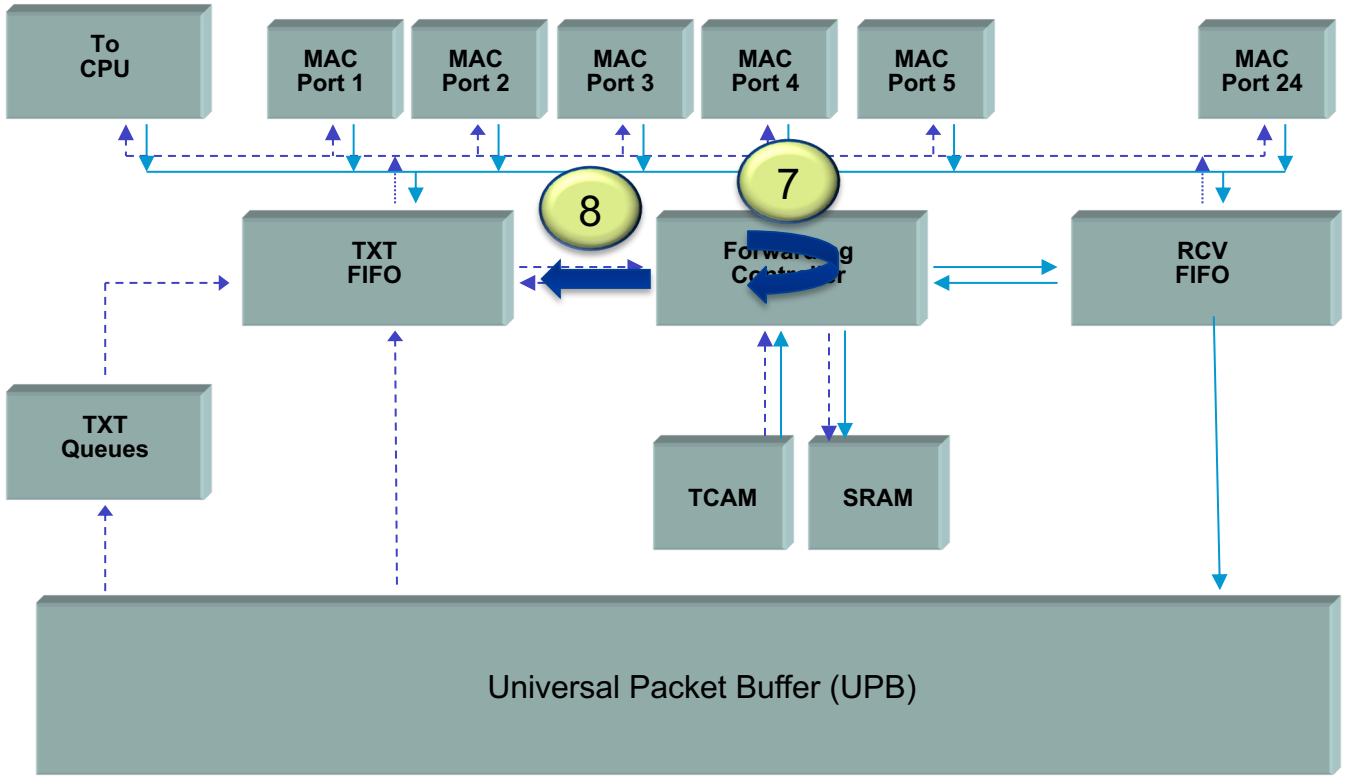
5

Search Engine in Forwarding Controller sends Destination Lookup to TCAM. Index returned.

6

Forwarding Controller uses index to get the L2/L3 forwarding info

Packet walk - Egress



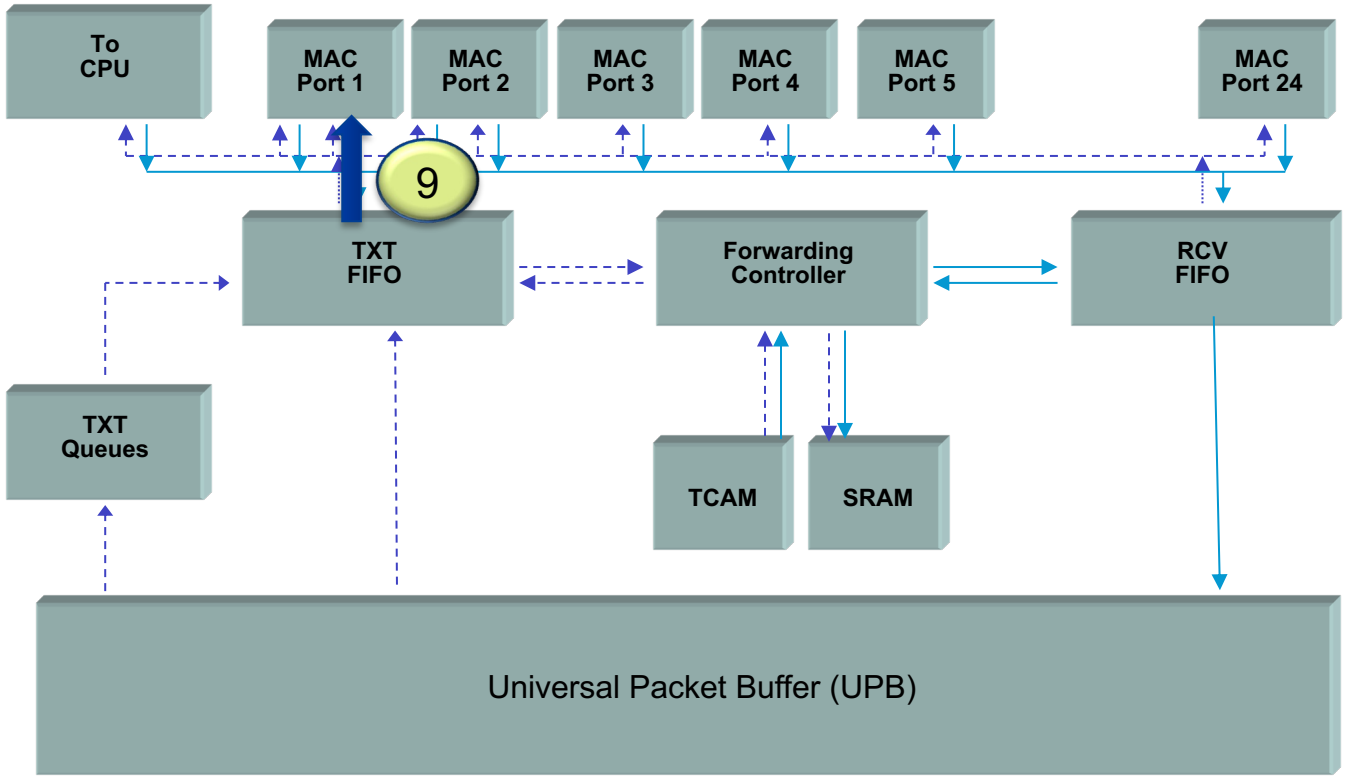
7

Packet Header prepared in the Forwarding Controller

8

Forwarding Controller sends the header info to the TXT FIFO where the final packet is assembled

Packet walk - Egress

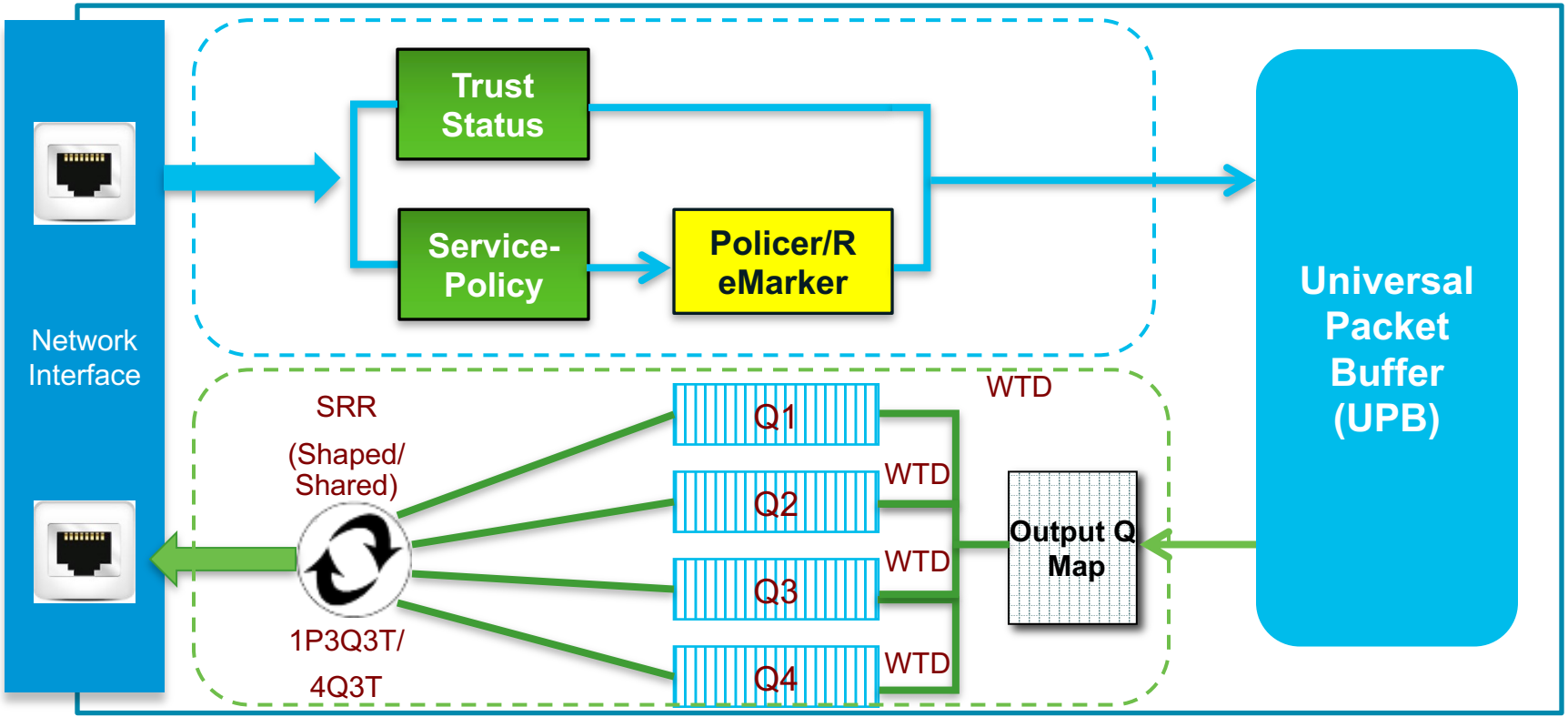


9

Final packet sent to the egress port.

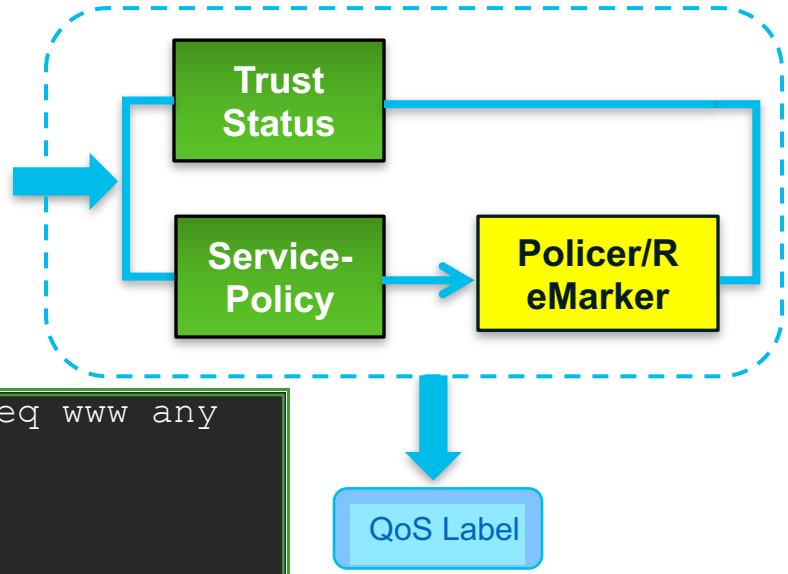
Quality of Service

Catalyst 1000 Switches- QoS Model



Trust, Classification & Marking

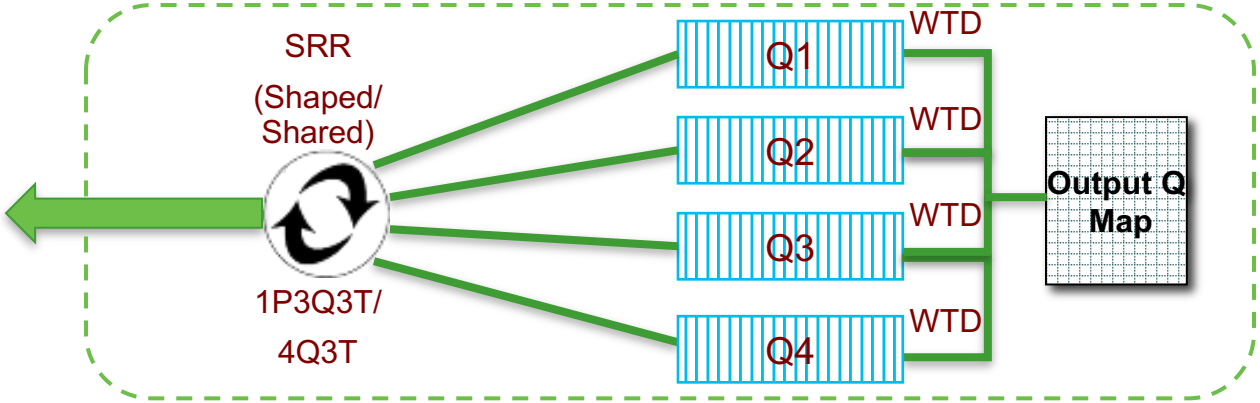
- Markings trusted by default – '`no mls qos`'
- '`mls qos`' enabled – all markings are set to BE
  - Trust Config
    - Trust COS/DSCP
    - Conditional Trust
    - Mark without trust




```
C1000(config)#access-list 101 permit tcp any eq www any
C1000(config)#class-map match-all http
C1000(config-cmap)#match access-group 101
C1000(config-cmap)#policy-map web-server
C1000(config-pmap)#class http
C1000(config-pmap-c)#police 500000 8000 exceed-act drop
C1000(config-pmap-c)#int gig1/0/11
C1000(config-if)#service-policy input web-server
```

Egress Queuing & Scheduling

- Queuing
  - Default Four egress queues/port
  - Queues assigned based on QoS label
  - 2 Queue-sets – 2 Queue configurations
- Dropping
  - WTD used for congestion avoidance
- Scheduling
  - Per Interface configuration
  - Strict Priority
  - SRR used to manage the queues



Automation with Cisco AutoQoS Switch Platforms

- Single command at the interface level configures interface and global QoS
  - Support for Cisco IP Phone & Cisco IP Soft Phone
  - Support for Cisco Telepresence, IP video surveillance camera & Media Player
  - Trust Boundary is disabled when IP Phone is moved / relocated
  - Buffer Allocation & Egress Queuing dependent on interface type (GE/FE)
- Supported on Static, dynamic-access, voice VLAN access, and trunk ports
- CDP must be enabled for AutoQoS to function properly
- Cisco Catalyst 1000 supports SRR, Strict Priority Scheduling, and Strict Priority Queuing

AutoQoS VoIP Model Example

```
C1000(config-if)#auto qos voip cisco-phone
```

Options:

auto qos voip cisco-phone

auto qos voip cisco-softphone

auto qos voip trust

auto qos video cts

auto qos video ip-camera

auto qos video media-player

```
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 3  3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3  2 4
mls qos srr-queue output cos-map queue 4 threshold 2  1
mls qos srr-queue output cos-map queue 4 threshold 3  0
mls qos srr-queue output dscp-map queue 1 threshold 3  40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3  24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3  48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3  56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3  16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3  32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 2  9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3  0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138
mls qos queue-set output 1 threshold 2 138 138 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
!
interface GigabitEthernet0/1
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 queue-set 2
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
!
```

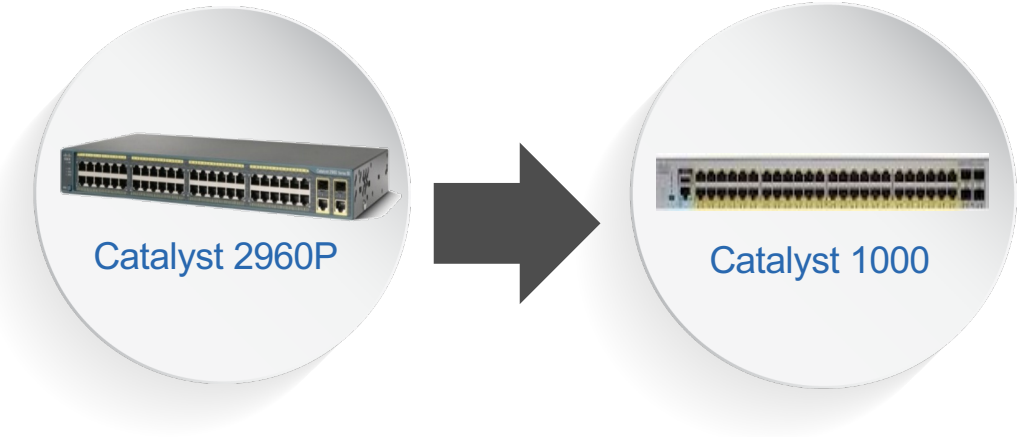
Technical Marketing Engineers

Reference

Catalyst 100 Series Switch Scale

Feature	Catalyst 1000 Series Switches
SVI and Vlans	64 SVIs and 256 VLANs.
number of Multicast groups	1024
number of Unicast MAC addresses	15360
number of MAC/IPv4 Access Control Entries	600
number of IPv6 Access Control Entries	600
number of IPv4 Direct Route Entries	542
number of IPv4 Indirect Route Entries	256
number of IPv6 Direct Route Entries	414
number of IPv6 Indirect Route Entries	128

Drive FE->GiGE Transition from 2960-P to C1000 for Superior Capability, Reliability and Performance with Comparable Software Features



Category	C1000	2960L	2960P
Downlinks	GE	GE	FE
Uplinks	1G/10G/Combo	1G/10G	1G
Perpetual PoE	√	√	X
Flexible PoE options	√	X	X
PoE+	√	√	X
Basic Layer3	√	√	X
IP Source Guard	√	√	X
Single IP management	√	X	X
sFlow	√	√	X
PVLAN	√	X	X
Bluetooth	√	√	X

Layer23 switch.com

Turn this technical overview into a purchase-ready BOM

Send the exact model or BOM and your deployment requirements. Layer23-Switch can review compatibility, availability, and quote options.

- Exact model or Cisco PID and quantity
- Port count, media type, PoE budget, and uplink speed
- Redundancy, licensing, support, and accessory needs
- Ship-to country, target date, and lead-time constraints

REQUEST A BOM REVIEW

www.layer23-switch.com

SCAN TO REQUEST A QUOTE