Cisco Catalyst 9000 Series Switch Practical Guide
(Security Features)
(Telemetry)

March 25, 2021

Catalyst 9000 Security Features

Visibility

- Mission-critical application visibility (NBAR)*
- Full NetFlow telemetry

Segmentation

- Highest level of macro and micro segmentation with SD-Access
- Multidomain policy integration

Threat defense

- MACsec 256-bit link encryption
- Encrypted Traffic Analytics*
- Trustworthy solutions

Consistently delivered throughout the Cisco® Catalyst® 9000 family

* Roadmap on Cisco Catalyst 9500 High Performance and Catalyst 9600 Series

Security

DAI

IP Source Guard

First Hop Security

SISF

MACsec

Network authentication

Segmentation

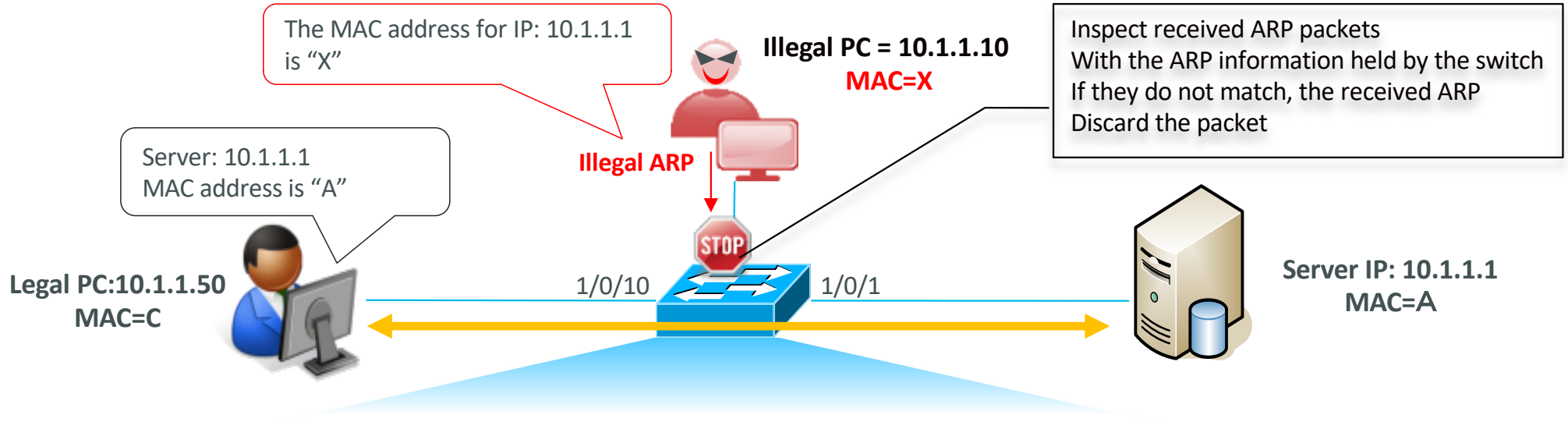
Trustworthy solutions

Embedded Security Features – to refresh

Dynamic ARP Inspection (DAI)

Dynamic ARP Inspection is a function that manages the mapping between MAC address and IP address on the switch and protects the network from attacks using malicious ARP packets. This feature protects your network by detecting / dropping rogue ARP packets sent by attackers. This function can also be used when assigning an IP address by DHCP when used in combination with the DHCP Snooping function.

When DAI function is applied



MAC address	IP address	VLAN	Interface
A	10.1.1.1	10	GigabitEthernet1/0/1
C	10.1.1.50	10	GigabitEthernet1/0/10

Dynamic ARP inspection - example

Enable DHCP Snooping and DAI

```
ip dhcp snooping vlan 211
ip dhcp snooping

ip arp inspection vlan 211
```

* The device-tracking setting is automatically set according to the snooping setting.

show device-tracking policy DT-PROGRAMMATIC

```
Policy DT-PROGRAMMATIC configuration:
  security-level glean
  device-role node
 gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target        Type  Policy          Feature      Target range
vlan 211      VLAN  DT-PROGRAMMATIC  Device-tracking vlan all
```

Enable device tracking on Interface

```
interface GigabitEthernet1/0/1
 switchport access vlan 211
 switchport mode access
 device-tracking
```

* For C9k, change from ip device-tracking to device-tracking.

show device-tracking policy default

```
Policy default configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
Policy default is applied on the following targets:
Target        Type  Policy          Feature      Target range
Gi1/0/17      PORT  default         Device-tracking vlan all
```

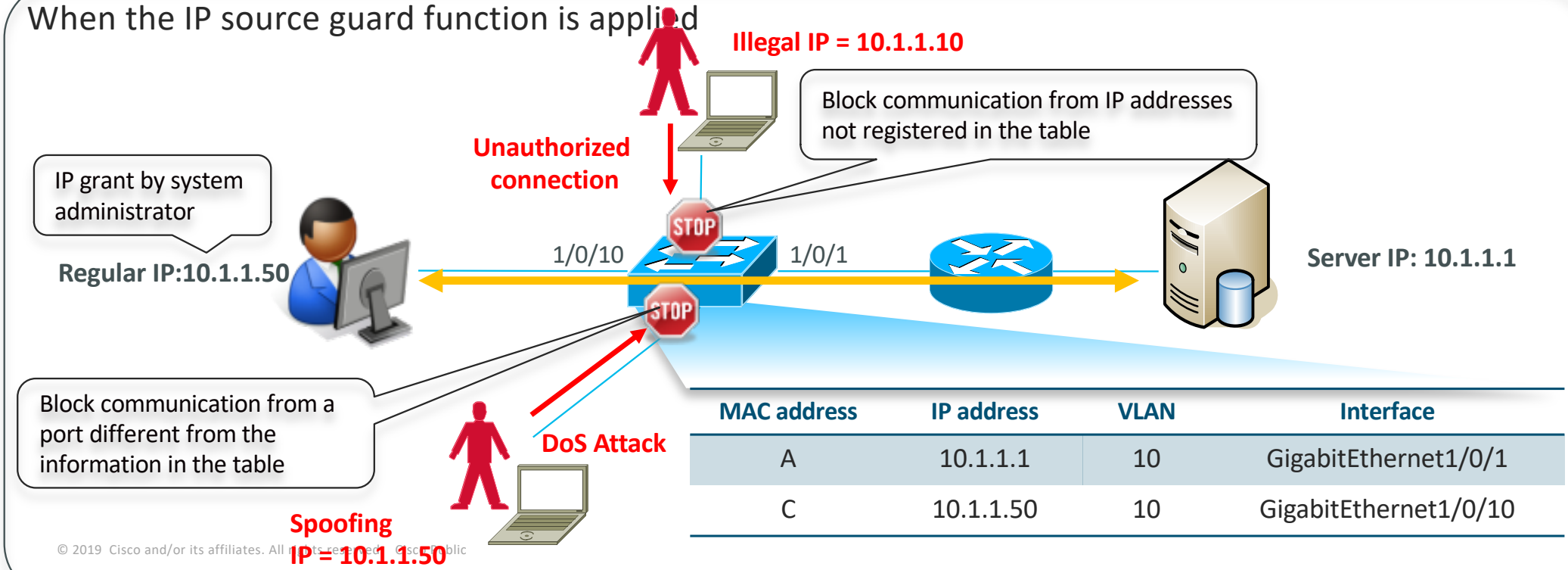
* The policy applied to the physical interface has priority over DT-PROGRAMMATIC.

IP Source Guard

The IP Source Guard feature is a security feature that limits communication from rogue IP addresses by maintaining an IP address-port mapping table and blocking IP traffic that does not match this table. You can use this feature to prevent an attacker from invading your network.

This function can also be used when assigning an IP address by DHCP when used in combination with the DHCP Snooping function.

When the IP source guard function is applied



MAC address	IP address	VLAN	Interface
A	10.1.1.1	10	GigabitEthernet1/0/1
C	10.1.1.50	10	GigabitEthernet1/0/10

IP Source Guard – config example

- **Activation of DHCP Snooping**

```
ip dhcp snooping vlan 211
ip dhcp snooping
```

- **Create a policy for Device Tracking**

```
device-tracking policy TEST01
 limit address-count 100
 no protocol arp
 tracking enable
```

no protocol arp

- Set ARP not to snoop
- Required for IP Source Guard operation

- **Enable IP source guard on Interface**

```
interface GigabitEthernet1/0/1
 switchport access vlan 211
 switchport mode access
 device-tracking attach-policy TEST01
 ip verify source tracking
```

* Apply policy to physical interface

show device-tracking policy TEST01

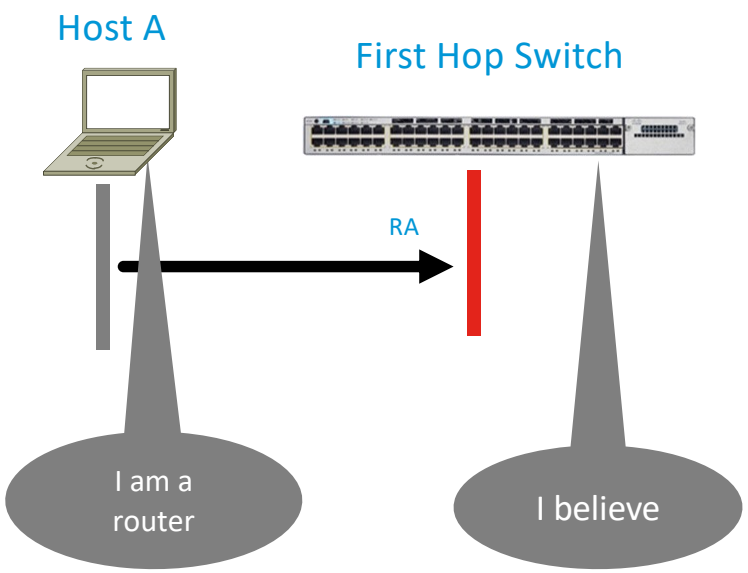
```
Policy TEST01 configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  NOT gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count 100
  tracking enable
Policy TEST01 is applied on the following targets:
Target        Type  Policy      Feature        Target range
Gi1/0/17      PORT  TEST01      Device-tracking vlan all
```

IPv6 First Hop Security - RA Guard

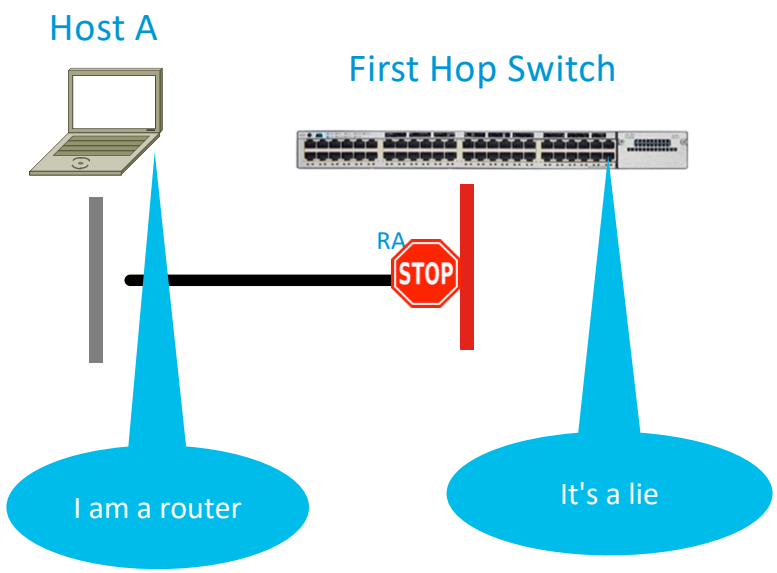
Router Theft (and session hijacking!)

Stop rogue Router Advertisements

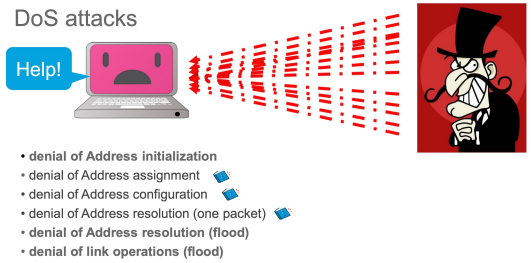
<no RA Guard>



<With RA Guard>

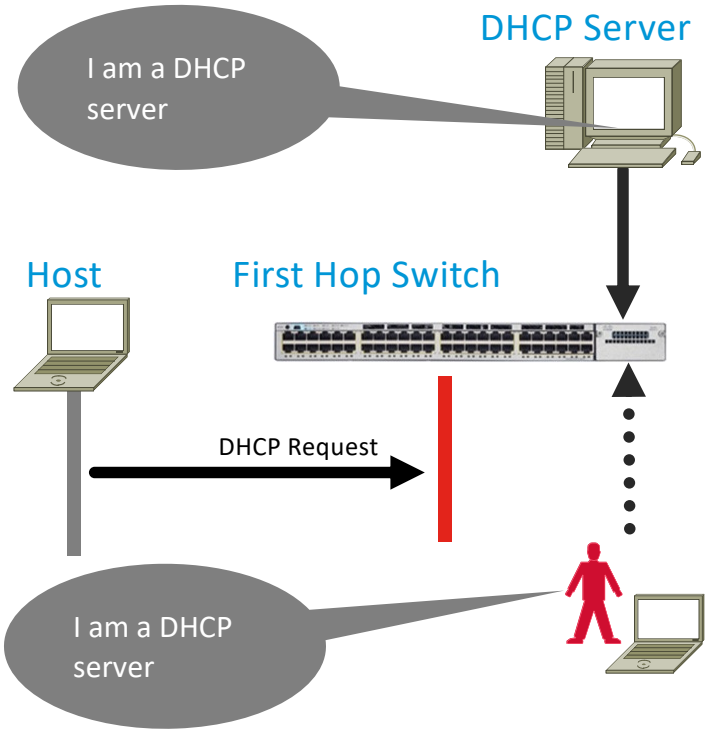


IPv6 First Hop Security - DHCP Guard

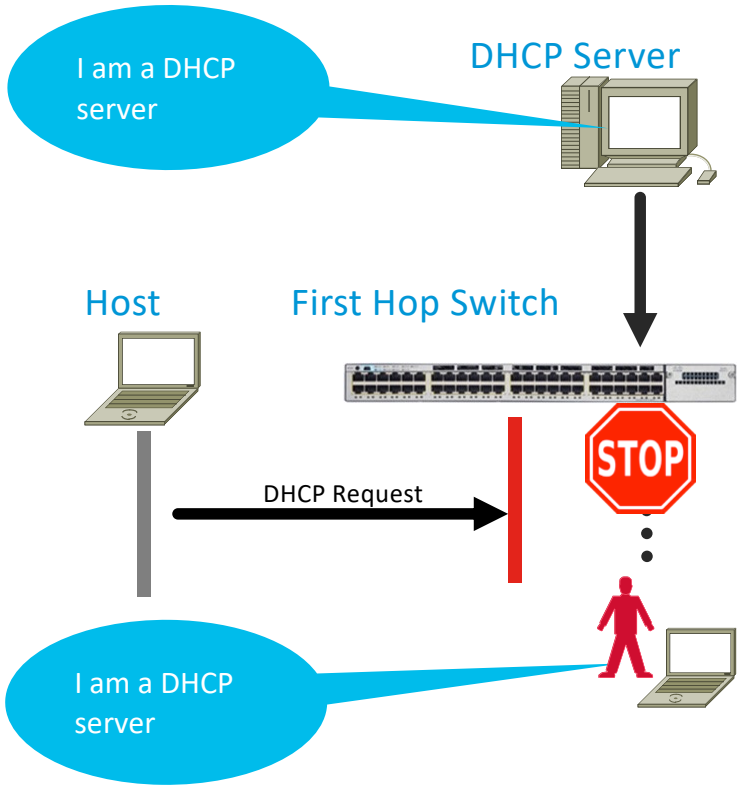


Stop rogue DHCP response

<no DHCP Guard >



<With DHCP Guard>



RA Guard / DHCP Guard - config

＜RA Guard＞

- **Create RA guard policy**

```
ipv6 nd raguard policy TEST01
 device-role host
```

* Manually set the RA guard policy

- **Attach RA guard policy to Interface**

```
interface GigabitEthernet1/0/1
 switchport access vlan 211
 switchport mode access
 device-tracking
 ipv6 nd raguard attach-policy TEST01
```

* Enable Device-Tracking

＜DHCP Guard＞

- **Create DHCP guard policy**

```
ipv6 dhcp guard policy TEST01
 device-role client
```

* Manually set the DHCP guard policy

- **Attach DHCP guard policy to Interface**

```
interface GigabitEthernet1/0/1
 switchport access vlan 211
 switchport mode access
 device-tracking
 ipv6 dhcp guard attach-policy TEST01
```

* Enable Device-Tracking

SISF-based Device-Tracking

- The Switch Integrated Security Feature based (SISF-based) Device Tracking feature is a feature that supplements new device information to replace the traditional IP Device-Tracking and IPv6 Snooping (IOS-XE 16.3.x and later) .
- SISF snoops the traffic received by the switch, extracts the device IDs (MAC and IP addresses) and stores them in the binding table.
- Many features such as IEEE 802.1X, Web Authentication, Cisco TrustSec, and LISP use this feature.
- SISF-based device tracking supports both IPv4 and IPv6
- SISF-based Device-Tracking must be used as an alternative to IP Device-Tracking on the Cisco Catalyst 9000 Series

show device-tracking database — output example

Network Layer Address	Link Layer Address	Interface	vlan	prlvl	age	state	Time left
L 192.168.202.254	0000.0c9f.f460	Vl1025	1025	0100	1684mn	DOWN	
L 192.168.201.254	0000.0c9f.f461	Vl1026	1026	0100	1683mn	REACHABLE	
ARP 192.168.201.51	50f7.22ae.25c1	Gi1/0/2	1026	0005	4mn	REACHABLE	39 s try 0
ARP 192.168.201.14	000c.29ec.d0b4	Gi1/0/1	1026	0005	91s	REACHABLE	210 s try 0
DH4 192.168.201.13	000c.29bd.d112	Gi1/0/1	1026	0025	3mn	REACHABLE	86 s try 0(590324 s)
ARP 192.168.201.12	000c.29dc.e708	Gi1/0/1	1026	0005	29s	REACHABLE	286 s try 0
DH4 192.168.201.11	000c.298f.15e1	Gi1/0/1	1026	0025	65s	REACHABLE	247 s try 0(590330 s)

SISF-based Device-Tracking - config

- **Manual creation**

You can create your own Profile.

Higher priority than auto-generated

Profiles can be created with device-tracking policy and applied to VLAN Configuration or physical interfaces

Physical interfaces take precedence over VLANs

- **Automatically generated**

Created automatically in each of the following cases:

IEEE 802.1X, web authentication, Cisco TrustSec, and IPSG features: enter the ip dhcp snooping vlan vlan command.

Cisco Locator/ID Separation Protocol.

EVPN on VLAN

Automatically generated policy sample

```
C9200-1#show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC configuration:
  security-level glean
  device-role node
  gleaning from Neighbor Discovery        ←ipv6 ND information collection enabled
  gleaning from DHCP                      ←ipv6 DHCP information collection enabled
  gleaning from ARP                       ←ipv4 ARP information collection enabled
  gleaning from DHCP4                     ←ipv4 DHCP information collection enabled
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target          Type  Policy          Feature      Target range
vlan 211         VLAN  DT-PROGRAMMATIC     Device-tracking vlan all
vlan 212         VLAN  DT-PROGRAMMATIC     Device-tracking vlan all
vlan 213         VLAN  DT-PROGRAMMATIC     Device-tracking vlan all
vlan 214         VLAN  DT-PROGRAMMATIC     Device-tracking vlan all
vlan 215         VLAN  DT-PROGRAMMATIC     Device-tracking vlan all
```

IP Device Tracking - differences

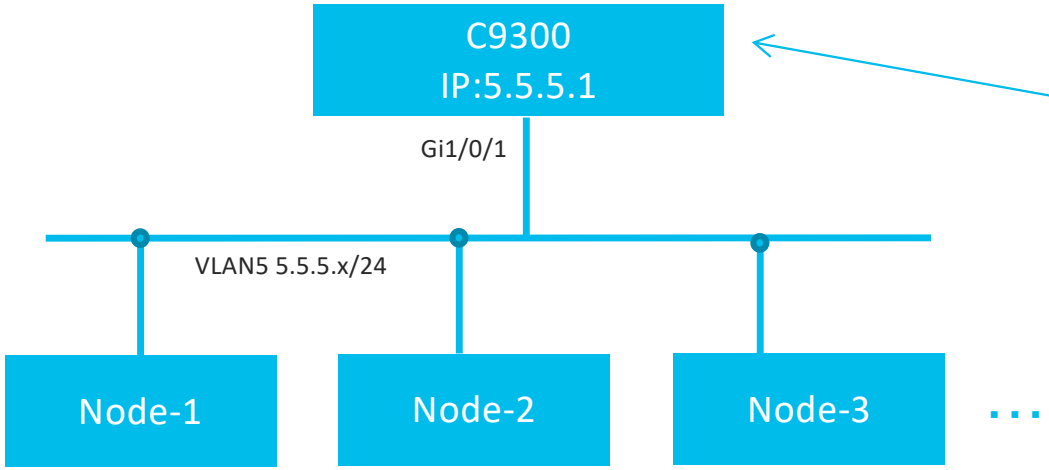
IP Device Tracking (IPDT) config	SISF-Based config (Cisco IOS XE Denali 16.3.7 or later)
ip device tracking probe count	It is set to the default value (3 times) and cannot be changed.
ip device tracking probe delay	It is set to the default value (10 seconds) and cannot be changed.
ip device tracking probe interval	device-tracking binding reachable-lifetime
ip device tracking probe use-svi	It is set as the default behaviour and cannot be changed
ip device tracking probe auto-source [fallback host-ip-address subnet-mask] [override]	device-tracking tracking auto-source [fallback host-ip-address subnet-mask] [override]
ip device tracking trace-buffer	Not supported
ip device tracking maximum n	device-tracking policy <Policy name> limit address-count <n>
ip device tracking maximum 0	Not supported
clear ip device tracking all	Not supported

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-9/configuration_guide/sec/b_169_sec_3850_cg/configuring_sisf_based_device_tracking.html

SISF-Device Tracking Operation check

Check the state of the Device Tracking database when SISF-DT is enabled and the operation when the Limit Address Count is exceeded.

Topology




```
ip dhcp snooping vlan 1-4094
ip dhcp snooping

device-tracking policy TEST
 limit address-count 2
 no protocol udp
 tracking enable

interface GigabitEthernet1/0/1
 switchport access vlan 5
 switchport mode access
 device-tracking attach-policy TEST
```

*** The maximum DT value of C9300 can be set up to 32,000.**

Device Tracking – check the database

Limit address - count 2

```
C9300-1#show device-tracking database
Binding Table has 3 entries, 2 dynamic (limit 100000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


   Network Layer Address          Link Layer Address Interface       vlan prlvl  age   state     Time left
ARP 5.5.5.11                      502f.a8b0.f701  Gi1/0/1         5  0005  150s  REACHABLE  155 s try 0
ARP 5.5.5.7                       580a.2013.ebc1  Gi1/0/1         5  0005    3mn REACHABLE  126 s try 0
L   5.5.5.1                       701f.5301.2cc7  Vl5             5  0100   58mn REACHABL
```

Third and subsequent device IPs are not stored in the database except for the Local SVI

Check the communication status when Limit address count 2

- **Check the communication status from each device to the gateway**

```
Node-1#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Node-2#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
Node-3#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Communication to SVI (5.5.5.1) of C9300 is possible even if the Device Tracking Table Limit is exceeded.

Set IP Source Guard and check the communication status

```
Node-1#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Node-2#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
Node-3#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

- **Add IP Source Guard to C9300**

```
interface GigabitEthernet1/0/1
 switchport access vlan 5
 switchport mode access
 device-tracking attach-policy TEST
 ip verify source tracking
```

IPs that are not on the device tracking database will be incommunicable

Check the Device Tracking database

Limit address - count 3

```
C9300-1#show device-tracking database
Binding Table has 4 entries, 3 dynamic (limit 100000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk          0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


   Network Layer Address          Link Layer Address Interface       vlan prlvl  age   state     Time left
ARP 5.5.5.11                       502f.a8b0.f701  Gi1/0/1         5  0005    3mn REACHABLE  128 s try 0
ARP 5.5.5.8                        b08b.cf48.a901  Gi1/0/1         5  0005    2s  REACHABLE  307 s
ARP 5.5.5.7                        580a.2013.ebc1  Gi1/0/1         5  0005    3mn REACHABLE  98 s try 0
L   5.5.5.1                        701f.5301.2cc7  Vl5             5  0100   68mn REACHABLE
```

Except for the Local SVI, the addresses of 3 hosts are listed on the table.

Check the communication status when Limit address count 3

- **Check the communication status from each device to the gateway**

```
Node-1#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Node-2#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Of course, any terminal can communicate with the gateway

```
Node-3#ping 5.5.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

MACSEC

MACsec (MAC security)

The technology that encrypts Ethernet communication and prevents the contents from being stolen even if the communication is intercepted.
The Cisco Catalyst 9200 / 9200L is the first entry level access switch to support MACsec.

Equipped with MACsec encryption chip
Line rate performance hardware processing

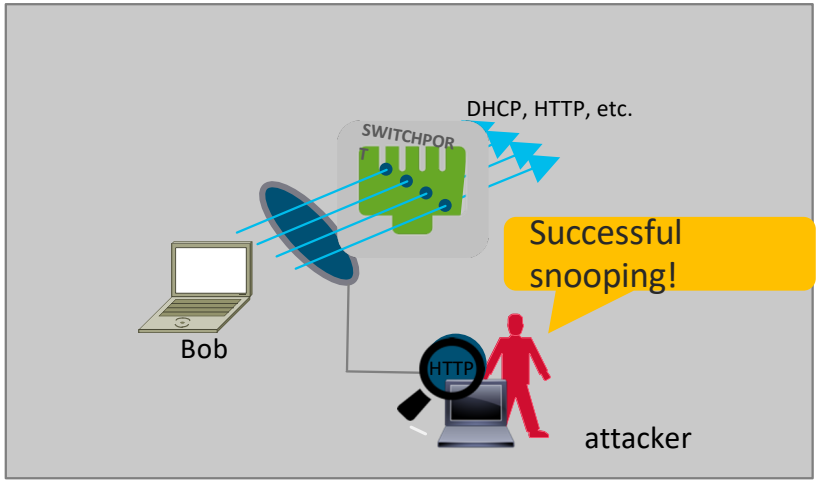
Where applicable	MACsec	Cat 9200		Cat9200L	
		IOS-XE	License	IOS-XE	License
Between switches	128 Bits SAP	16.10.1	Network Essentials	16.9.1	Network Essentials
	128 Bits MKA	16.10.1	Network Essentials	16.9.1	Network Essentials
Switch to host	128 Bits MKA	TBD		TBD	

■ **Important**
- Please note that if the MACsec settings do not match each other, Link will be Down.
- HA configuration and MACsec from the host to the switch are supported from 16.12.1.

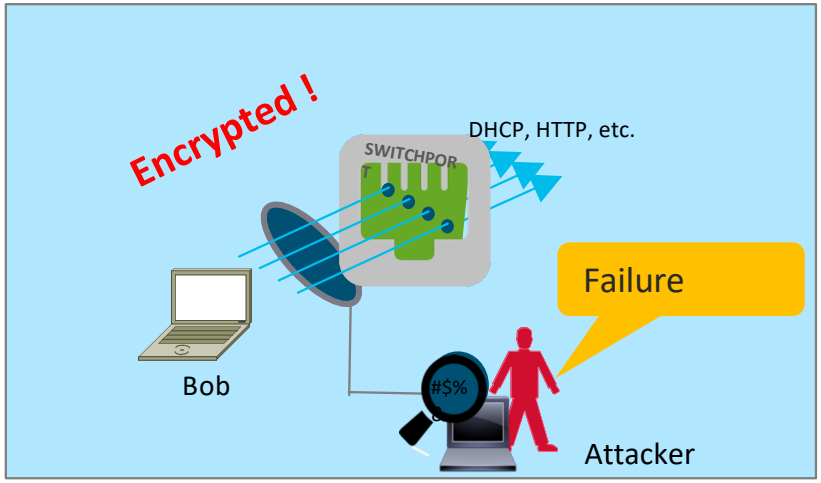
MACsec encryption between switch and host

Host-to-switch encryption (using IEEE 802.1X)

No MACsec



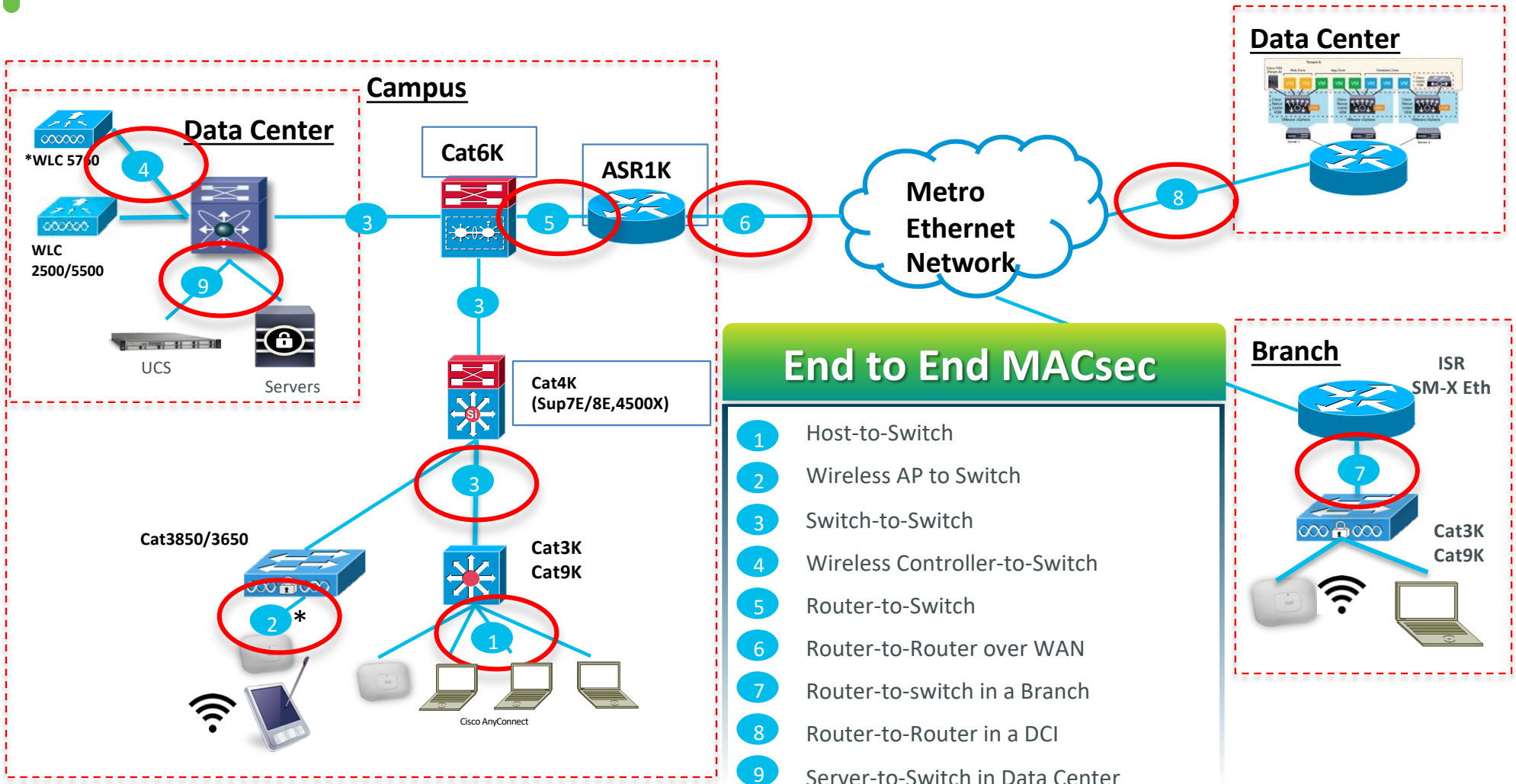
With MACsec



Step1
IEEE 802.1X authenticates the endpoint and transfers the required encryption key information (MKA) to both sides.
Step2
MACsec encrypts the communication using a master key derived from authentication

* Use AnyConnect as a supplicant (IOS-XE 16.10.1 or later)

Where MACsec is:



End to End MACsec

1. Host-to-Switch
2. Wireless AP to Switch
3. Switch-to-Switch
4. Wireless Controller-to-Switch
5. Router-to-Switch
6. Router-to-Router over WAN
7. Router-to-switch in a Branch
8. Router-to-Router in a DCI
9. Server-to-Switch in Data Center

MACsec key derivation scheme

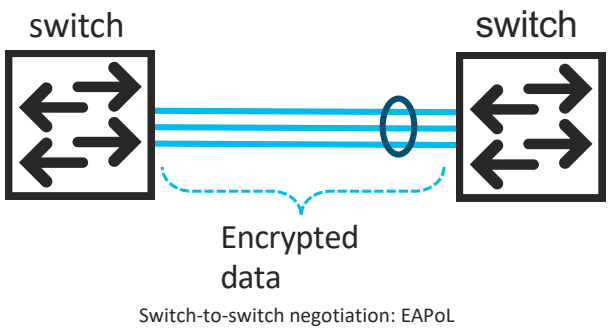
MACsec has two main mechanisms for key derivation schemes.

	SAP **(Security Association Protocol)**	**MKA** **(MACsec Key Agreement)**
General	Cisco's proprietary key negotiation protocol	Defined in IEEE802.1X-2010
Where applicable	Used only for encryption between switches	Used between switches, between terminals and switches, and between routers
Usage mode	Manual mode IEEE802.1x mode	Manual mode IEEE802.1x mode

How to configure MACsec

Encryption between switches (1/2)

```
key chain macsectest macsec
 key 111111
   cryptographic-algorithm aes-128-cmac
  key-string 0123456789abcdef0123456789abcdef
   lifetime local 12:12:12 Jan 1 2019 infinite

mka policy macsectest
 key-server priority 200
 macsec-cipher-suite gcm-aes-128                    #default

Interface gi1/0/10
 switchport mode trunk
 macsec network-link
 mka policy macsectest
 mka pre-shared-key key-chain macsectest
 macsec replay-protection window-size 10
```



Since it is a setting between switches, select "network-link"

How to check MACsec

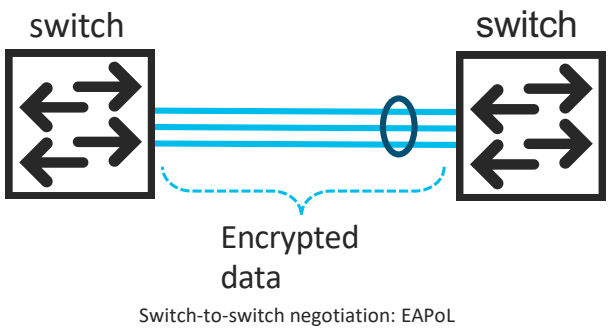
Encryption between switches (2/2)

```
C9200L#show macsec interface gi1/0/10
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Use ES Enable : no
  Use SCB Enable : no
  Admin Pt2Pt MAC : forceTrue(1)
  Pt2Pt MAC Operational : no
  Cipher : GCM-AES-128
  Confidentiality Offset : 0

 Capabilities
  ICV length : 16
  Data length change supported: yes
  Max. Rx SA : 16
  Max. Tx SA : 16
  Max. Rx SC : 8
  Max. Tx SC : 8
  Validate Frames : strict
  PN threshold notification support : No
  Ciphers supported : GCM-AES-128
```

MACsec Activated

Encrypt with AES128 bit

GCM-AES-128 is the only supported encryption suite for the 9200 series.

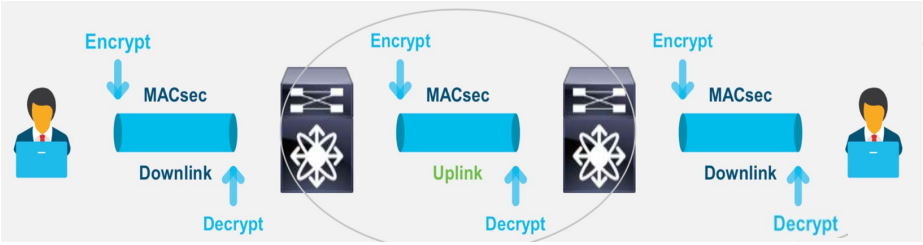


* Note: When using MACsec on a multi-chassis EtherChannel, if a master switch fail, the MKA will not be retained and it will take several tens of seconds to reestablish the session, during which the link will not be able to communicate.

Media Access Control Security (MACsec 256)

Enhanced Security with 256b MACsec, Encrypted Data Plane

1. Extended Packet Numbering
2. Standard MKA Key Exchange (802-1ae)
3. "AES-256" keys Stronger Security



	C9200	C9300	C9400	C9500 / 9600
Switch to Switch	Supported (128b)	Supported (128b, 256b)	Supported (128b, 256b)	Supported (128b, 256b)
Switch to Host	Supported (128b)	Supported (128b, 256b)	Supported (128b, 256b)	Supported (128b, 256b)

Benefits

Complete Access security

Complete cross platform alignment with Uplink/Downlink support

Protection against "Inside threats"

Securing campus infra

Hop by Hop Ethernet Encryption

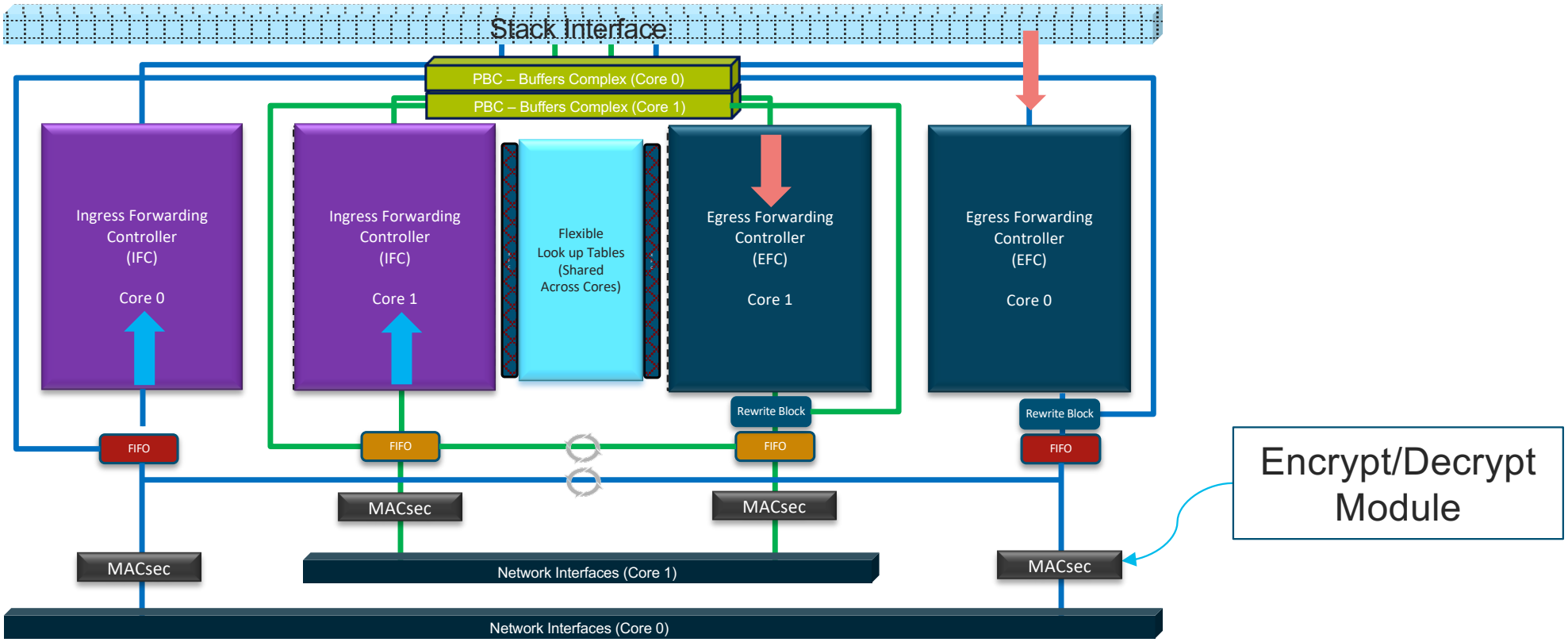
Line Rate Performance on all ports

256bit MACsec – Network Advantage

128bit MACsec – Network Essentials

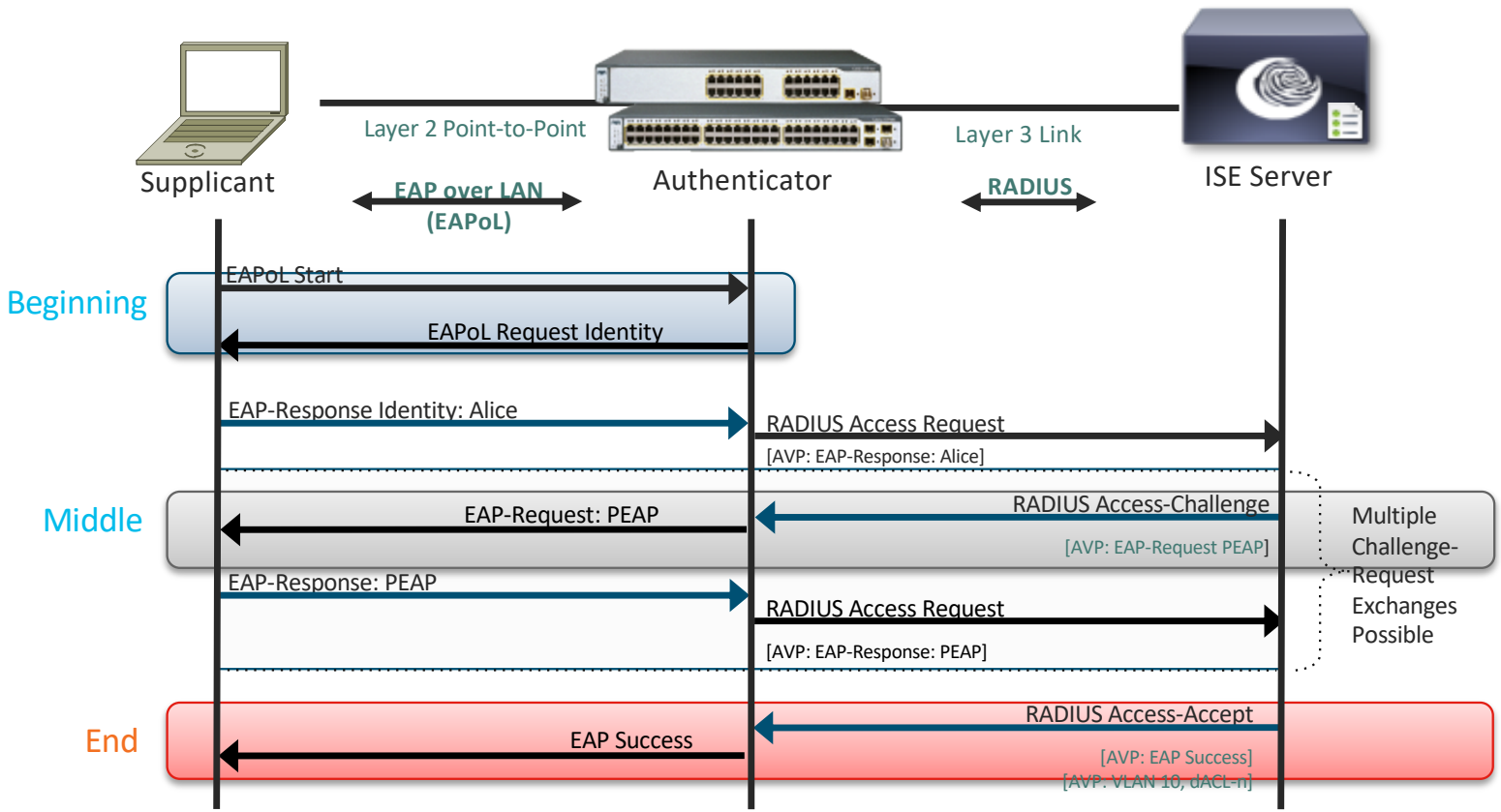
Where is MACsec performed in Hardware?

Applicable for UADP 2.0/3.0/Mini ASIC



Network Authentication IEEE802.1x

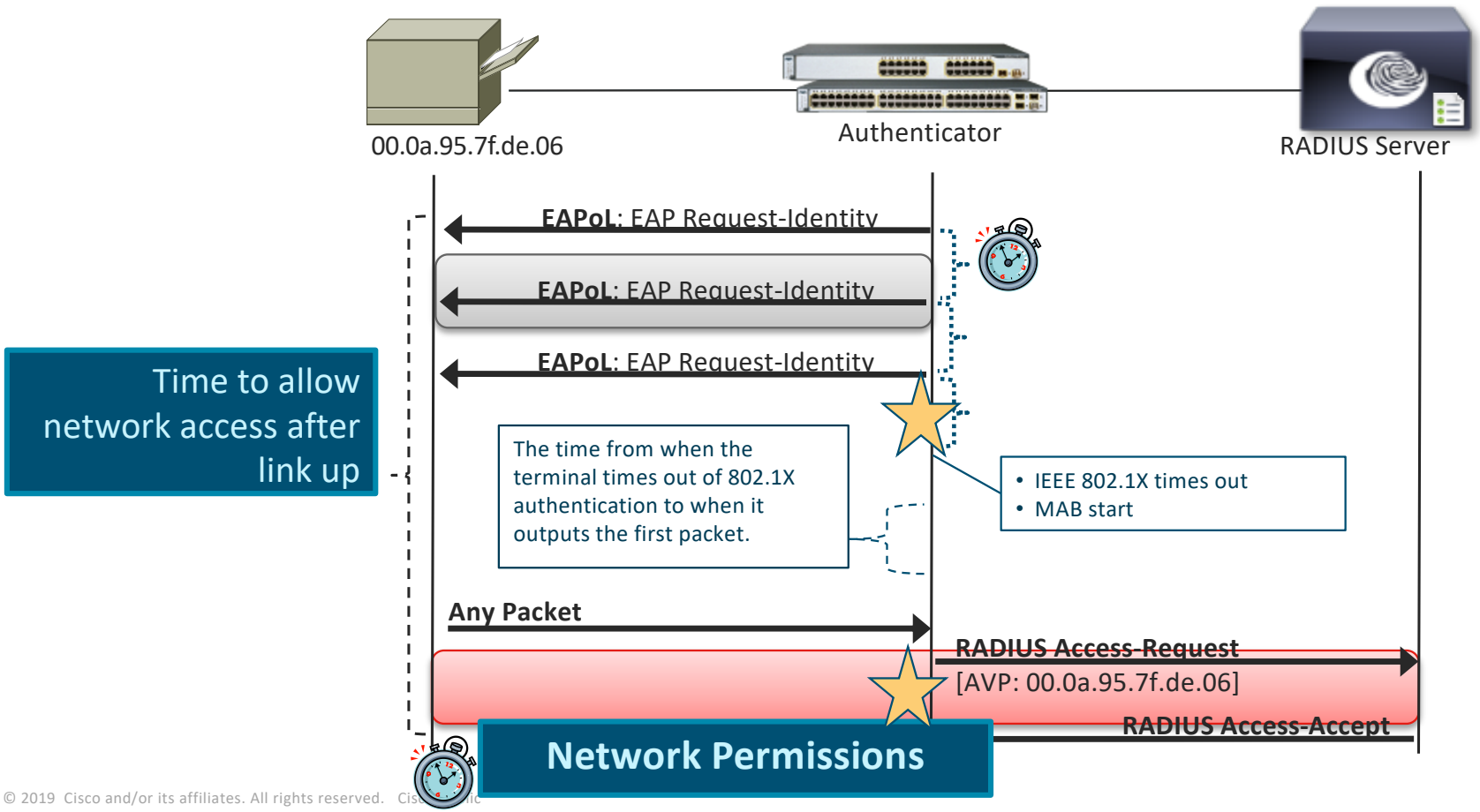
Network Authentication
General Flow of IEEE 802.1X Authentication



- EAPoL refers to the forwarding mechanism and does not provide a mechanism for authentication
- If you want to use 802.1X authentication, you need to select his EAP type on the terminal supplicant side.
- EAP-TLS (client certificate), PEAP (username / password), etc.

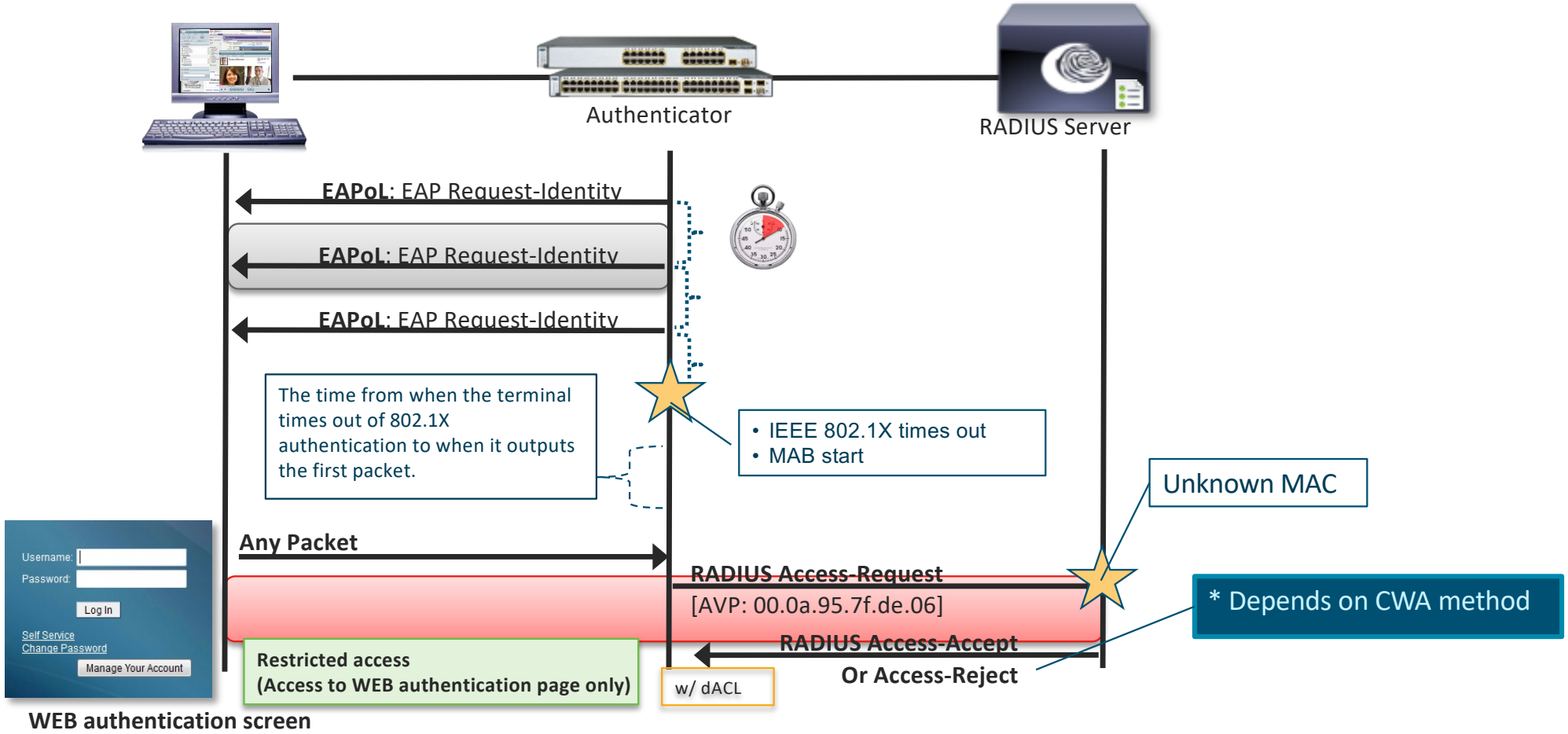
Network authentication

MAC Authentication Bypass（MAB）Flow



Network authentication

Central Web Authentication（CWA）Flow



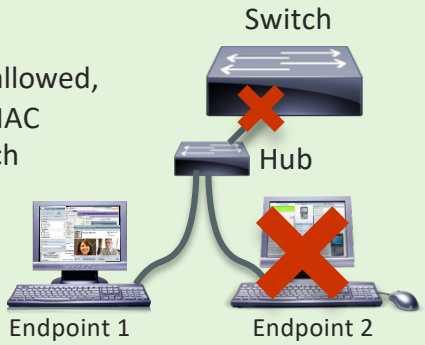
Network authentication host mode

There are four main modes for network authentication:

Single Host

Only a single MAC address is allowed, the second and subsequent MAC addresses are a security breach

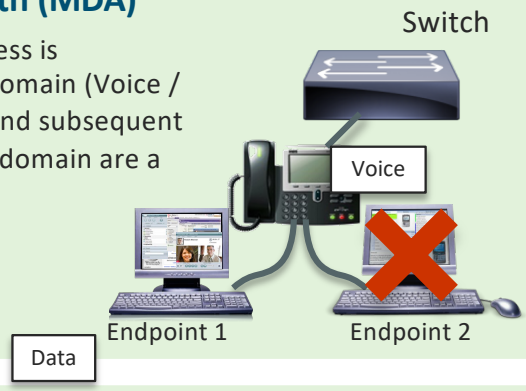
VLAN | dACL



Multi-Domain Auth (MDA)

Only a single MAC address is authenticated in each domain (Voice / Data), and the second and subsequent MAC addresses in each domain are a security breach.

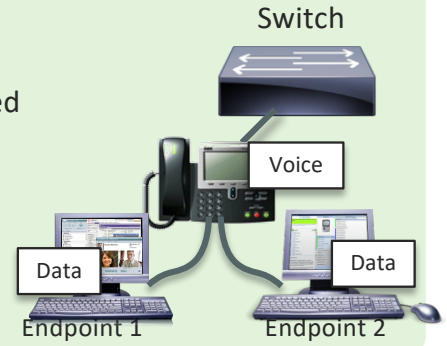
VLAN | dACL



Multi-Authentication

One voice terminal and multiple data terminals can be authenticated at the same time, and different dACL / dVLAN policies can be applied to each host.

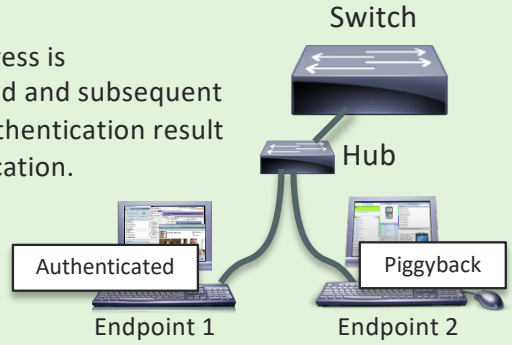
VLAN* | dACL



Multi-Host

When the first MAC address is authenticated, the second and subsequent hosts ride on the first authentication result and bypass the authentication.

VLAN*

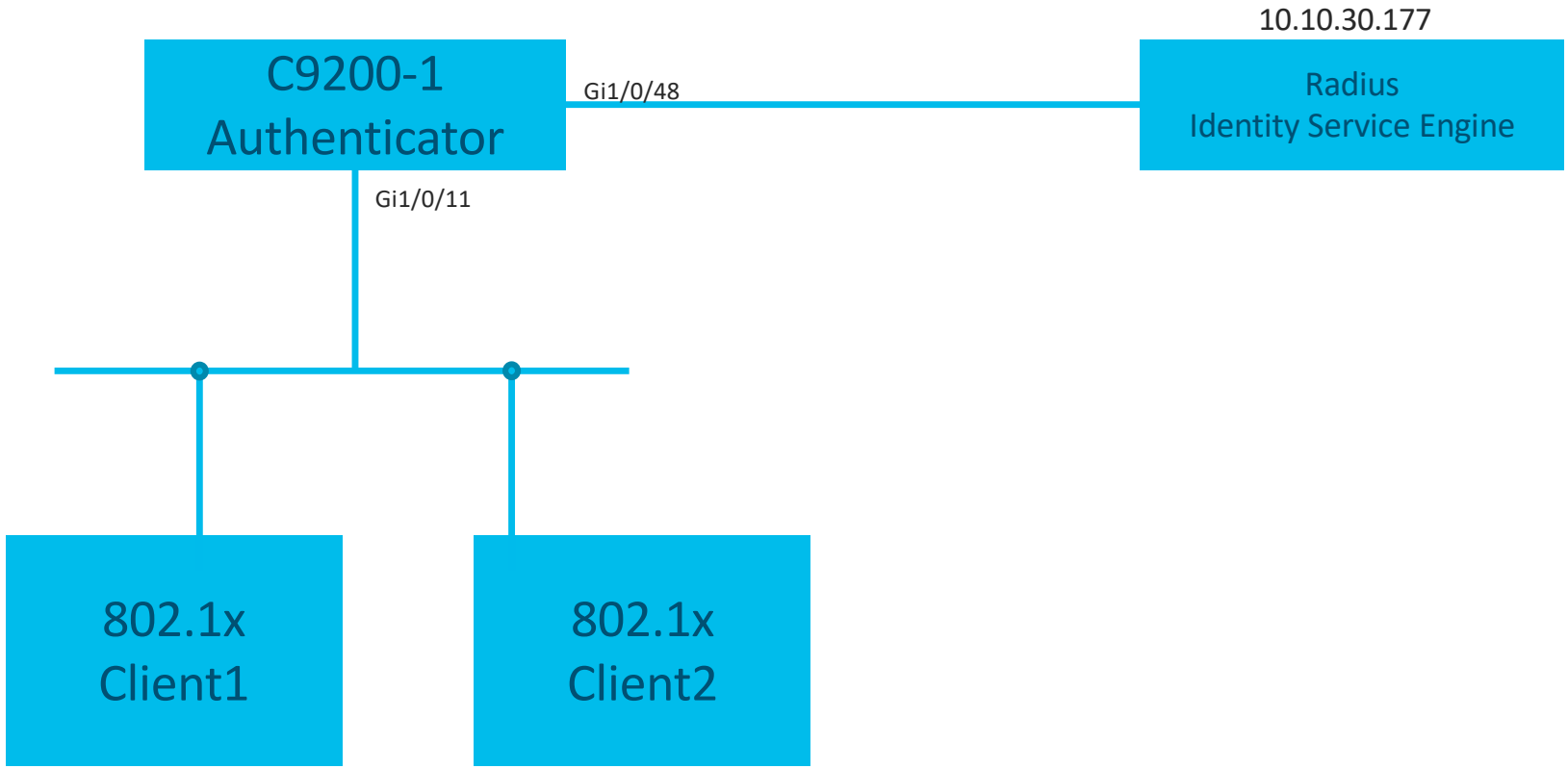


Cisco Catalyst 9200L Series Verification Results Summary

Host mode	VLAN assignment	dot1x	MAB	CWA
Single Host	None	○	○	○
	Dynamic vlan	○	○	○
Multi-Authentication	None	○	○	○
	Dynamic vlan	○	○	○

Config example (1)
802.1X Multi authentication + Dynamic VLAN

802.1X Multi Authentication on Cisco Catalyst 9200 L → Configure Dynamic VLAN Per User



ISE configuration example

User info

Username	Identity Group
user1	vlan211
user2	vlan212

Authorization Profile settings

AuthZ Profiles	Vlan
vlan211_permit	211
vlan212_permit	212

Authorization rule settings

Identity Group	Results
vlan211	vlan211_permit
vlan212	vlan212_permit

Network Access Users

Edit | Add | Change Status | Import | Export | Delete | Duplicate

Status	Name	User Identity Groups	Admin
Enabled	ad01	staff-group	
Enabled	caadmin	ALL_ACCOUNTS (default)	
Enabled	sponsor	ALL_ACCOUNTS (default)	
Enabled	user1	vlan211	
Enabled	user2	vlan212	
Enabled	user3	ALL_ACCOUNTS (default)	
Enabled	user4	ALL_ACCOUNTS (default)	

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:211
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:212
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	vlan211	if **vlan211**	then vlan211_permit
	vlan212	if **vlan212**	then vlan212_permit
	Permit_all	if **Any**	then PermitAccess
	Default	if no matches, then DenyAccess	

Configuring 802.1X

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

aaa server radius dynamic-author
 client 10.10.30.177 server-key cisco
 auth-type all

dot1x system-auth-control

radius server ISE
 address ipv4 10.10.30.177 auth-port 1812 acct-port 1813
 key cisco
```

Enable AAA

Specify a server group to be used for authentication, authorization, and accounting

Specify Radius server information and shared key information

Define a server group

```
interface GigabitEthernet1/0/11
 switchport mode access
 device-tracking
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication port-control auto
 authentication periodic
 mab
 dot1x pae authenticator
 spanning-tree portfast
```

Enable authentication on Interface and specify multi-authentication mode

<Important>

- The authentication port of C9200L is set by mode access.
- You need to create a VLAN to assign with Dynamic vlan on the C9200L

Cisco Catalyst 9200 L show command 1

Multi-authentication succeeds on Cisco Catalyst 9200 L and you can see two devices

```
Switch#show authentication sessions int gi1/0/11
Interface            MAC Address    Method  Domain  Status Fg  Session ID
-----------------------------------------------------------------------------------------
Gi1/0/11             2852.6168.d101 dot1x   DATA    Auth       A51E0A0A0000004D35EC5E80
Gi1/0/11             2c0b.e9ad.ad81 dot1x   DATA    Auth       A51E0A0A0000004C35EC5378

Key to Session Events Blocked Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
```

Cisco Catalyst 9200 L show command 2

```
Switch#show authentication sessions int gi1/0/11 details
Interface:  GigabitEthernet1/0/11
          IIF-ID:  0x1AA0AC98
      MAC Address:  2c0b.e9ad.ad81
     IPv6 Address:  Unknown
     IPv4 Address:  Unknown
       User-Name:  user1
          Status:  Authorized
          Domain:  DATA
    Oper host mode:  multi-auth
   Oper control dir:  both
    Session timeout:  3600s (local), Remaining: 2972s
     Timeout action:  Reauthenticate
  Common Session ID:  A51E0A0A0000004C35EC5378
    Acct Session ID:  0x00000009
          Handle:  0x1a00000c
    Current Policy:  POLICY_Gi1/0/11


Local Policies:
     Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
    Security Policy:  Should Secure

Server Policies:
      Vlan Group:  Vlan: 211


Method status list:
    Method         State
     dot1x        Authc Success
```

User ID of the terminal with MAC address 2c0b.e9ad.ad81

VLAN 211 assigned to User1

```
Interface:  GigabitEthernet1/0/11
          IIF-ID:  0x1D17F138
      MAC Address:  2852.6168.d101
     IPv6 Address:  Unknown
     IPv4 Address:  Unknown
       User-Name:  user2
          Status:  Authorized
          Domain:  DATA
    Oper host mode:  multi-auth
   Oper control dir:  both
    Session timeout:  3600s (local), Remaining: 2975s
     Timeout action:  Reauthenticate
  Common Session ID:  A51E0A0A0000004D35EC5E80
    Acct Session ID:  0x0000000a
          Handle:  0xc000000d
    Current Policy:  POLICY_Gi1/0/11


Local Policies:
     Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
    Security Policy:  Should Secure

Server Policies:
      Vlan Group:  Vlan: 212


Method status list:
    Method         State
     dot1x        Authc Success
```

User ID of the terminal with MAC address 2852.6168.d101

VLAN 212 assigned to User2

Check the authentication log

Identity Services Engine | Home | Operations | Policy | Guest Access | Administration | Work Centers

RADIUS Livelog | TACACS Livelog | Reports | Troubleshoot | Adaptive Network Control

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped
0	0	8	0

Show Live Sessions | Add or Remove Columns | Refresh | Reset Repeat Counts

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2019-01-10 05:47:56.460			5	08:CC:A7:5F:06:(	08:CC:A7:5F:06:08	Unknown	Wired_C9200L >> Wired_MAB >> Default	Wired_C9200L >> Permit_all	PermitAccess
2019-01-10 05:46:59.912			6	user2	28:52:61:68:D1:01	Unknown	Wired_C9200L >> Wired_dot1x >> Default	Wired_C9200L >> vlan212	vlan212_permit
2019-01-10 05:46:57.288			4	user1	2C:0B:E9:AD:AD:81	Unknown	Wired_C9200L >> Wired_dot1x >> Default	Wired_C9200L >> vlan211	vlan211_permit
2019-01-10 05:44:36.602			0	28:52:61:68:D1:4	28:52:61:68:D1:41	Unknown	Wired_C9200L >> Wired_MAB >> Default	Wired_C9200L >> Permit_all	PermitAccess

Check the authentication log 1

Overview

Event	5200 Authentication succeeded
Username	user2
Endpoint Id	28:52:61:68:D1:01
Endpoint Profile	Unknown
Authentication Policy	Wired_C9200L >> Wired_dot1x >> Default
Authorization Policy	Wired_C9200L >> vlan212
Authorization Result	vlan212_permit

Result

State	ReauthSession:A51E0A0A0000004735E2C9F0
Class	CACS:A51E0A0A0000004735E2C9F0:ise20a/336458508/30
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 212
cisco-av-pair	profile-name=Unknown
LicenseTypes	1

Authentication Details

Source Timestamp	2019-01-10 04:01:41.787
Received Timestamp	2019-01-10 04:01:41.788
Policy Server	ise20a
Event	5200 Authentication succeeded
Username	user2
User Type	User
Endpoint Id	28:52:61:68:D1:01
Calling Station Id	28-52-61-68-D1-01
Endpoint Profile	Unknown
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:vlan212,Unknown
Authentication Method	dot1x
Authentication Protocol	EAP-MD5
Service Type	Framed
Network Device	C9200L
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.10.30.165
NAS Port Id	GigabitEthernet1/0/11
NAS Port Type	Ethernet
Authorization Profile	vlan212_permit
Response Time	7

Segmentation

Cisco TrustSec

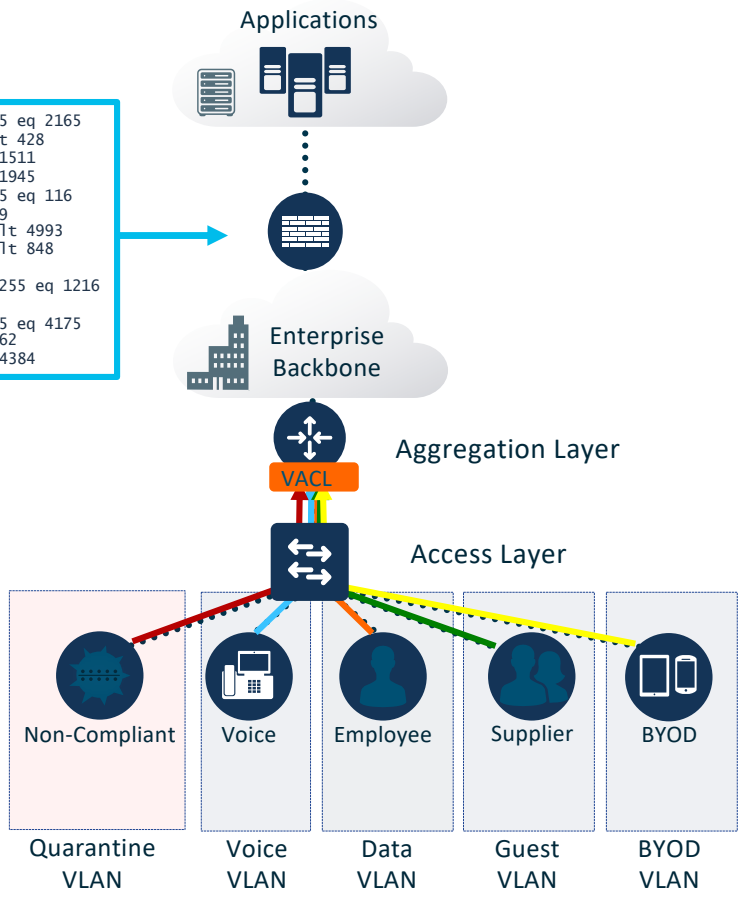
Traditional access control is extremely complex

```
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 136.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 136.196.101.101 0.0.0.255 lt 2361 90.186.112.213 0.0.31.255 eq 116
access-list 102 deny udp 242.4.189.142 0.0.1.255 eq 1112 19.94.101.166 0.0.0.127 eq 959
access-list 102 deny tcp 82.1.221.1 255.255.255.255 eq 2587 174.222.14.125 0.0.31.255 lt 4993
access-list 102 deny tcp 103.10.93.140 255.255.255.255 eq 970 71.103.141.91 0.0.0.127 lt 848
access-list 102 deny ip 32.15.78.227 0.0.0.127 eq 1493 72.92.200.157 0.0.0.255 gt 4878
access-list 102 permit icmp 100.211.144.227 0.0.1.255 lt 4962 94.127.214.49 0.255.255.255 eq 1216
access-list 102 deny icmp 88.91.79.30 0.0.0.255 gt 26 207.4.250.132 0.0.1.255 gt 1111
access-list 102 deny ip 167.17.174.35 0.0.1.255 eq 3914 140.119.154.142 255.255.255.255 eq 4175
access-list 102 permit tcp 37.85.170.24 0.0.0.127 lt 3146 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt 1843 239.16.35.19 0.0.1.255 lt 4384
```

- Static ACL
- Routing
- Redundancy
- DHCP Scope
- Address
- VLAN

Limits of Traditional Segmentation

- Security Policy based on Topology (Address)
- High cost and complex maintenance



Enforcement
IP Based Policies - ACLs, Firewall Rules

Propagation
Carry "Segment" context through the network using VLAN, IP address, VRF

Classification
Static or Dynamic VLAN assignments

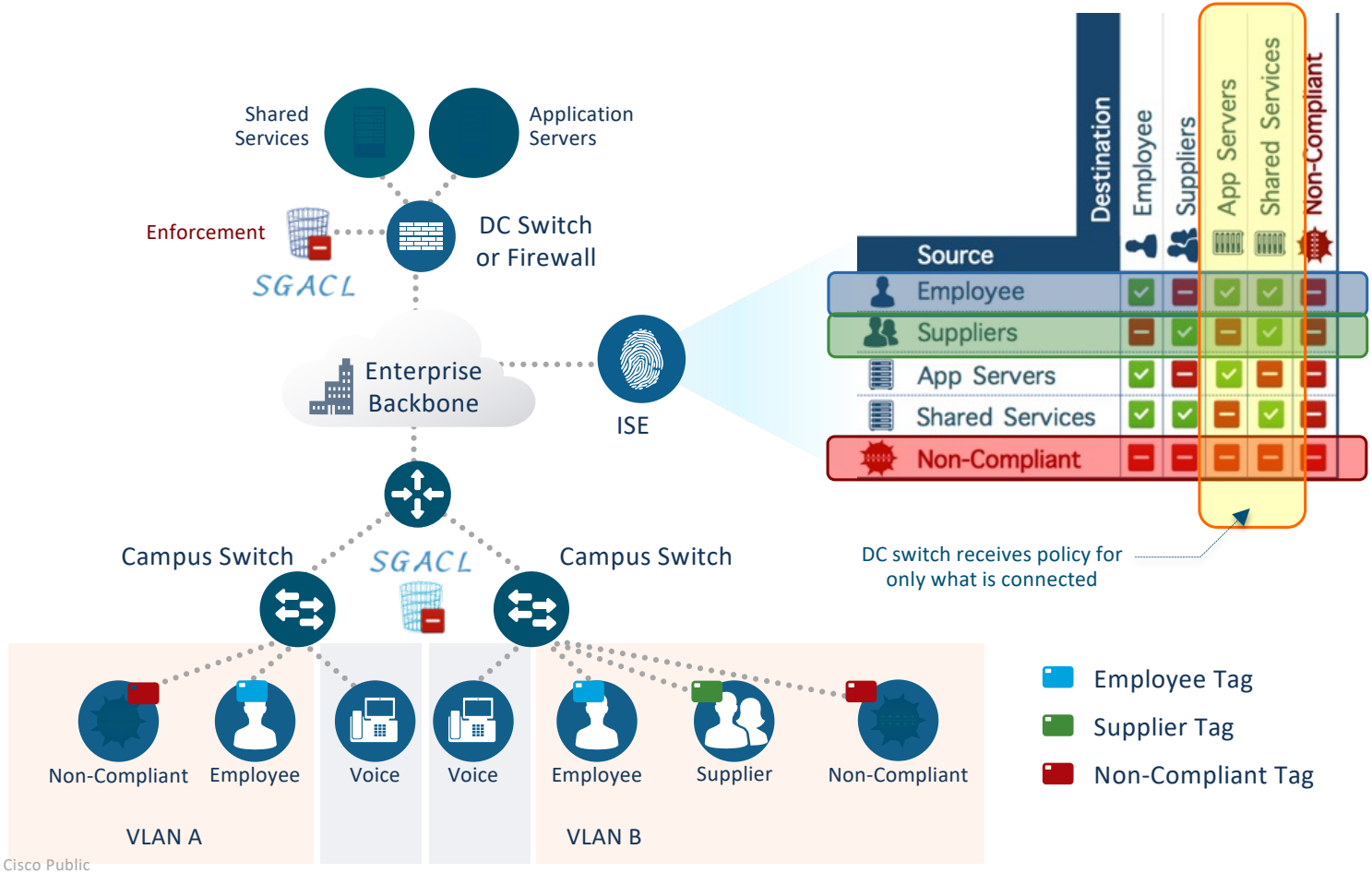
Cisco TrustSec

Simplified access control with Group Based Policy

Enforcement
Group Based Policies
ACLs, Firewall Rules

Propagation
Carry "Group" context through the network using only SGT

Classification
Static or Dynamic SGT assignments



Security-Trustworthy Solutions

Trustworthy system

During the equipment manufacturing process and equipment startup / operation
A general term for mechanisms that ensure the integrity of hardware and software.

What is the guarantee of integrity?
Is the hardware genuine, provided by the manufacturer, and is the software tampered with?
Check / validate the device during "startup" and "running".

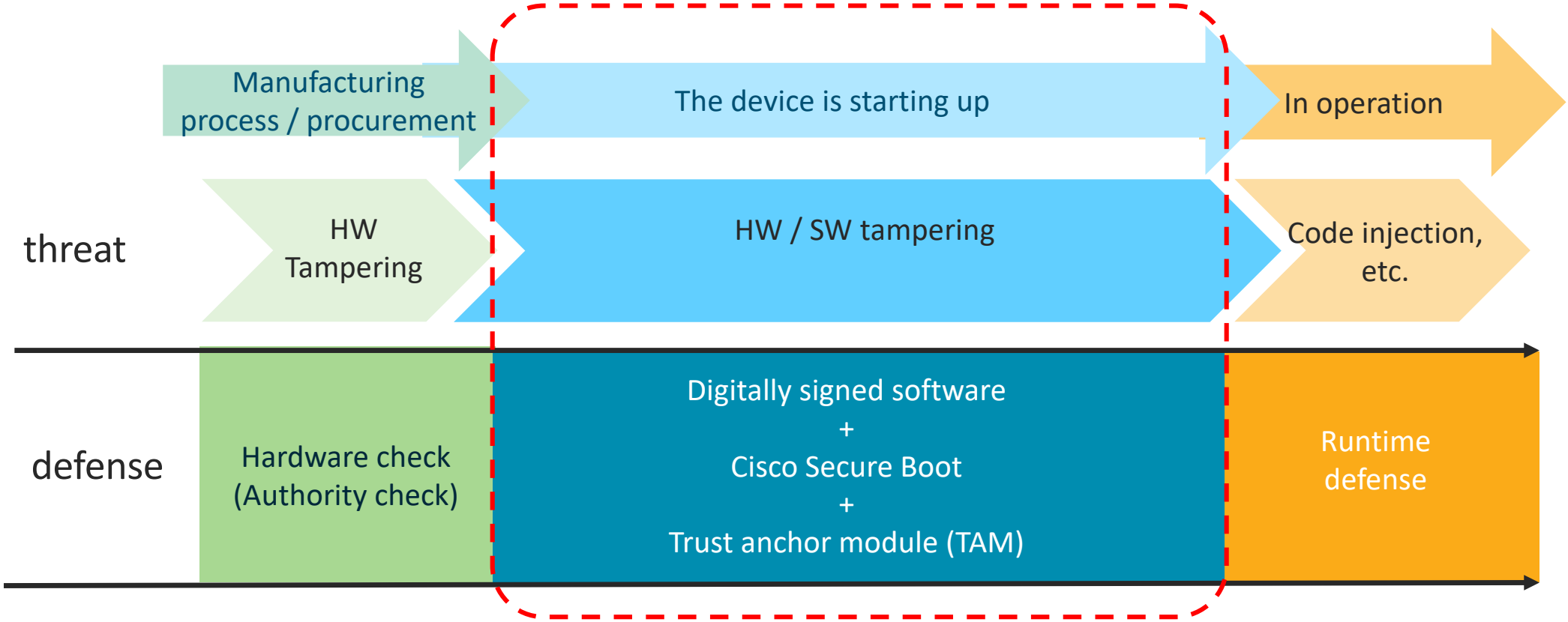
Risk reduction

Visualization of device integrity

Early detection of threats

Trustworthy System Overview

Trustworthy system =
Mechanism for ensuring the integrity of HW / SW during equipment procurement, startup and operation



Cisco Catalyst 9000 Platform Trustworthy Solutions

Design/ Develop → Plan/ Order → Source → Make → Quality → Delivery → Service/End of Life (EOL)

Physical security practices + security technology innovations + logical security processes

PnP SUDI support
Two-way trust

Image signing
Authentic OS

Hardware authenticity
Genuine hardware

Secure boot
Boot sequence check

Integrity verification
Malware protection

Runtime defenses
64-bit ASLR

Cisco® trustworthy systems use industry best practices to help ensure full development lifecycle integrity and end-to-end security

Cisco Trust Anchor Module (TAm)

Integrity Applications

TAM Services Libraries

- HW Based Entropy
- HW Authenticity Check
- Secure PnP
- Integrity Verification

Crypto Functions

Tamper-Proof Storage

Boot Measurements

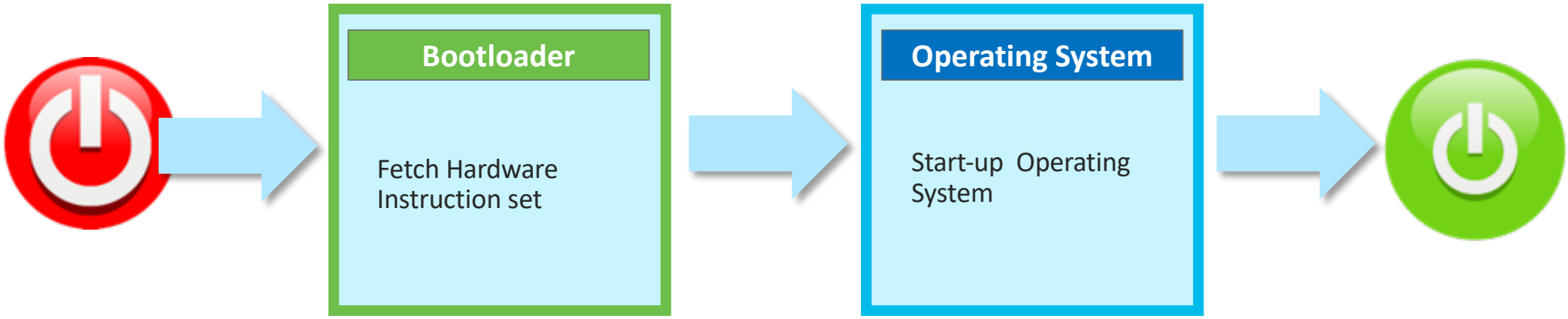
SUDI

- Anti-Tamper Chip Design
- Built-In Crypto Functions
- Secure Storage

Secure Unique Device Identification (SUDI)

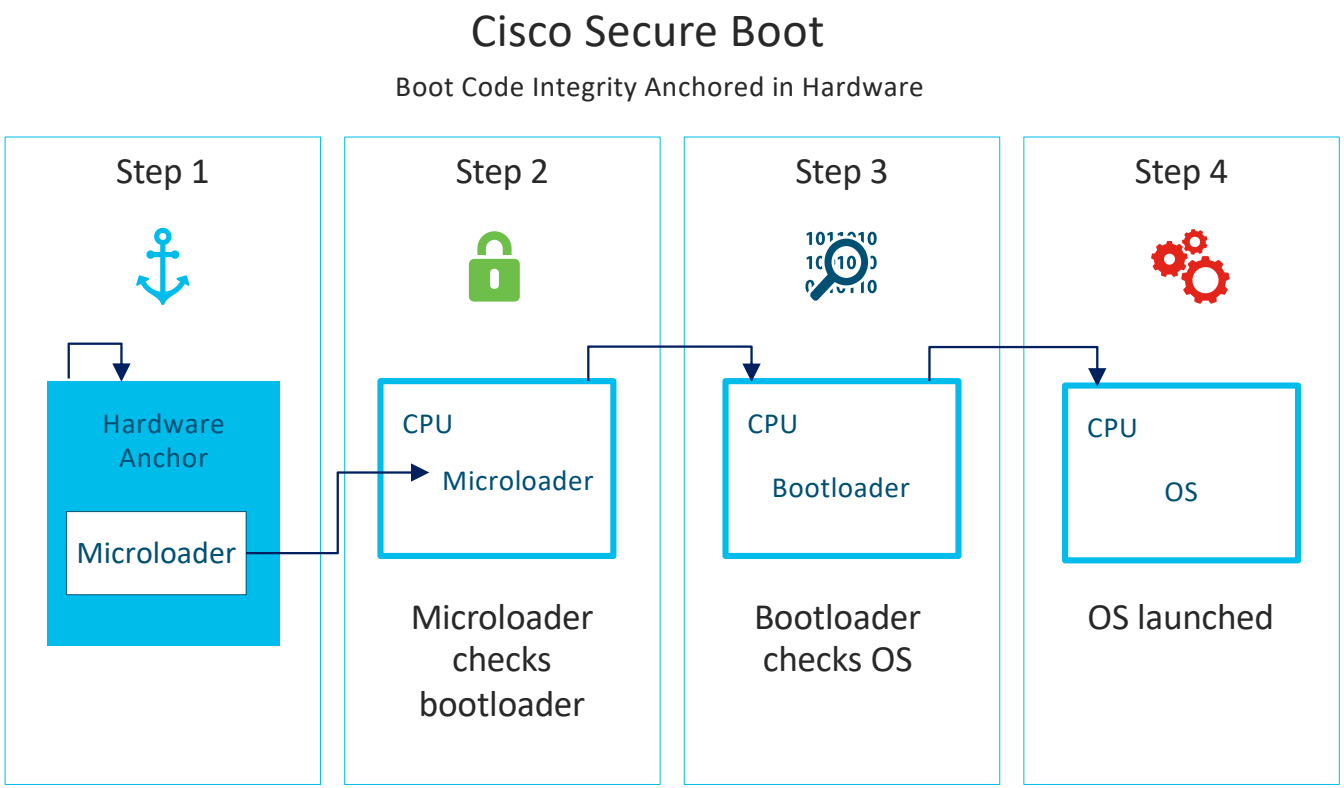
- Tamperproof ID for the device
- Binds the hardware identity to a key pair in a cryptographically secure X.509 certificate PID during manufacturing
- Connections with the device can be authenticated by the SUDI credential
- IEEE 802.1AR Compliant

Boot Sequence



Cisco Secure Boot

Anchors Secure Boot in Hardware to Create a Chain of Trust



- Only authentic signed Cisco software boots up on a Cisco platform
- The boot process stops if any step fails to authenticate
- IOS “show software authenticity” command illustrates the results

Secure Boot Verification during boot up

Microloader doesn't display verification, if verification fails then the box doesn't boot at all.

```
Initializing Hardware ...

System integrity status: 00000610
Rom image verified correctly


System Bootstrap, Version 15.4(3r)S, RELEASE SOFTWARE (fc1)
Copyright (c) 1994-2014  by cisco Systems, Inc.
<snip>
```

1 2

ROMMON Secure boot verification

IOS Secure boot verification

```
<snip>
##########################################################
Boot image size = 425853700 (0x19620304) bytes

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
        calculated 334207fa:464503d3:2e7abd5f:160919d0:b425523b
        expected   334207fa:464503d3:2e7abd5f:160919d0:b425523b

RSA Signed RELEASE Image Signature Verification Successful.
Package Load Test Latency : 6511 msec
Image validated
<snip>
```

3 4

Secure Boot Verification after bootup

```
Switch#show software authenticity running
<snip> (other packages not displayed)

PACKAGE cat3k--universalk9.16.03.05..SPA.pkg
-----------------------------------------------------------------
Image type                    : Production
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 54F33A2E
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : mono
        Verifier Version      : 16.03.05

SYSTEM IMAGE
------------
Image type                    : Production
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 54F33B36
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : System Bootstrap, Version 15.4(3r
```

4

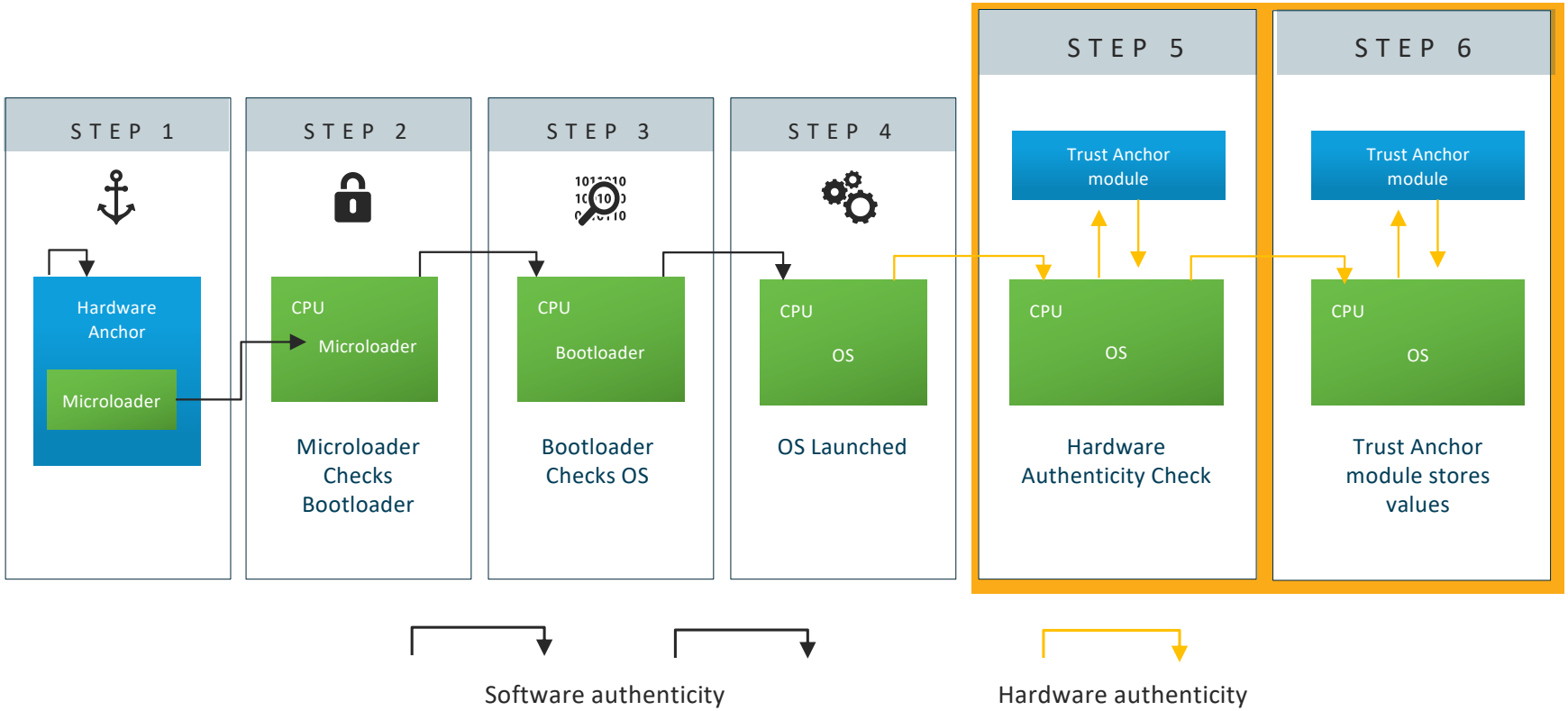
3

```
ROMMON
------
Image type                    : Production
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 53A3B3D2
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : System Bootstrap, Version 15.4(3r

Microloader
-----------
Image type                    : Release
    Signer Information
        Common Name           : CiscoSystems
        Organization Name     : CiscoSystems
    Certificate Serial Number : f01632135f43ae4bc1c4ca63a289b727
    Hash Algorithm            : HMAC-SHA256
    Verifier Information
        Verifier Name         : Hardware Anchor
        Verifier Version      : F01023R12.1817bb4af2014-05-23
```

2

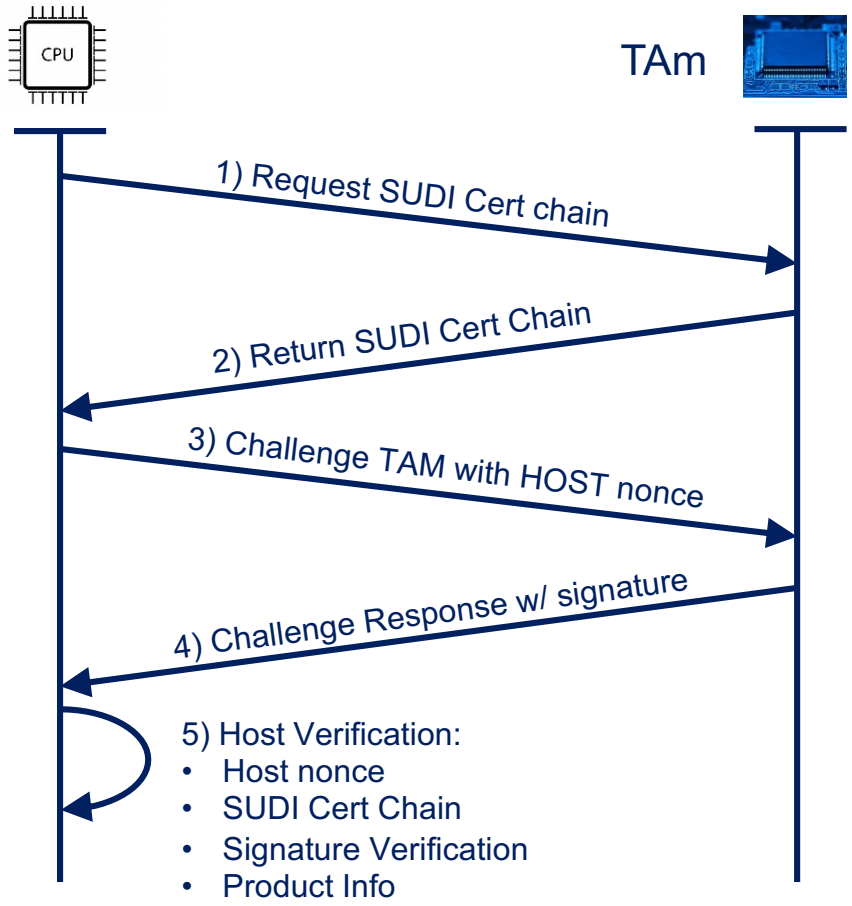
1

After Secure Boot, IOS Software Verifies that Hardware is Authentic



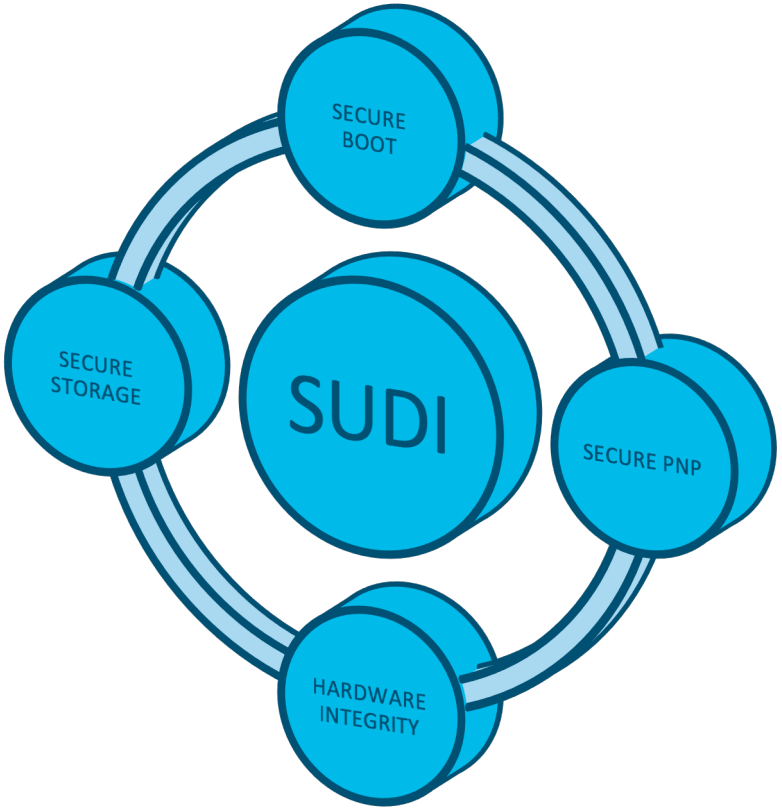
HW Authenticity Check

- Trust Anchor Module (TAm) securely stores HW Identity (SUDI)
- After the operating system is up and running…
- IOS-XE automatically verifies that the HW is genuine



Trustworthy Features on Cat 9000 Family

Features	Catalyst 9000 Family (Open IOS-XE)
Image Signing	Yes
Secure Boot	Yes
Anti-Counterfeit Check	Yes
Trust Anchor Module	Yes
PnP SUDI Support	Yes
Run Time Defenses	Yes
X.509v3 SSH Authentication	Yes



Secure, Resilient Campus with Catalyst 9000

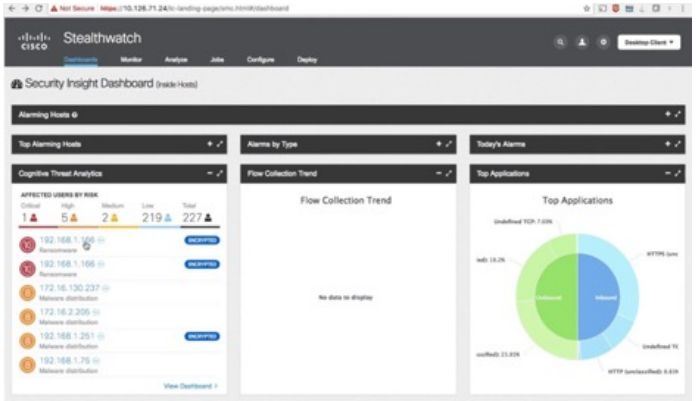
Secure Infrastructure | Security | Secure Transport

Trustworthy Systems

Hardware Authenticity

Two Way Trust

Run-time Defense



Encrypted Traffic Analytics

Traffic Analytics

Malware Detection

Compliance

MACSEC 256

Man-in-the-Middle

Wire-tapping

Impersonation

Telemetry

AVC

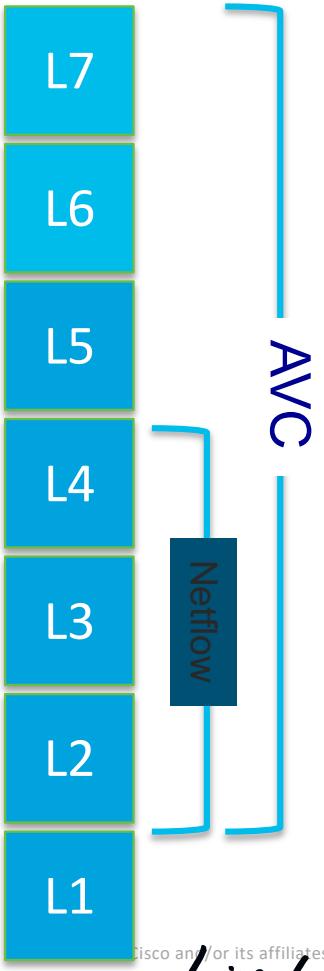
NBAR2

Netflow

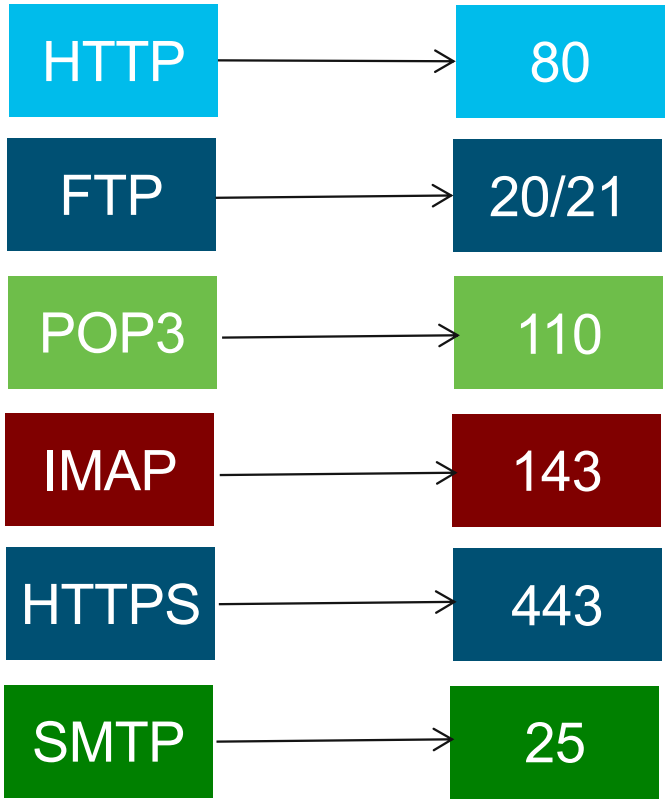
3.6 AVC

AVC

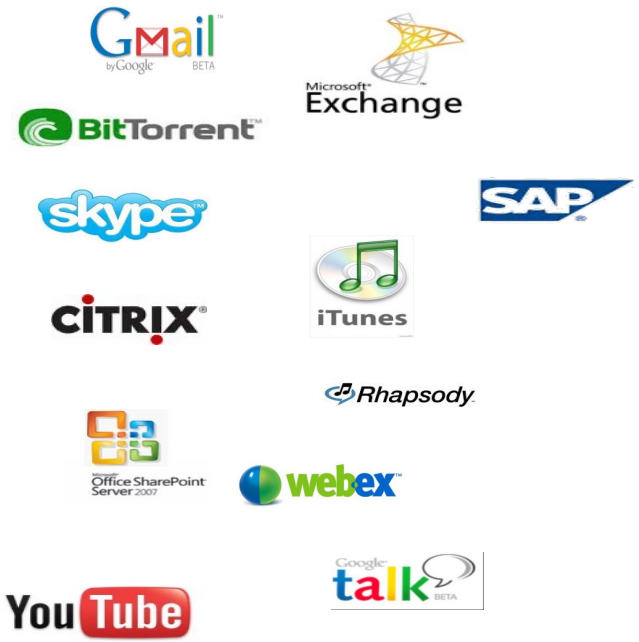
Challenges of Today's Network



Yesterday's Applications



Today's Applications



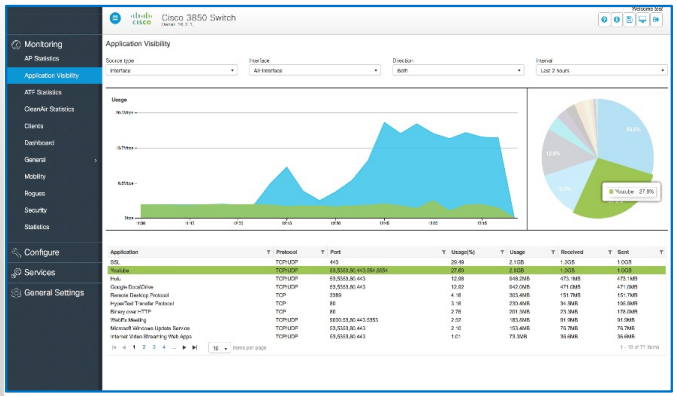
Know, Monitor & Control Your Applications

Granular Detection, Advanced Monitoring & Business Logic Based Policies

Know Your Applications

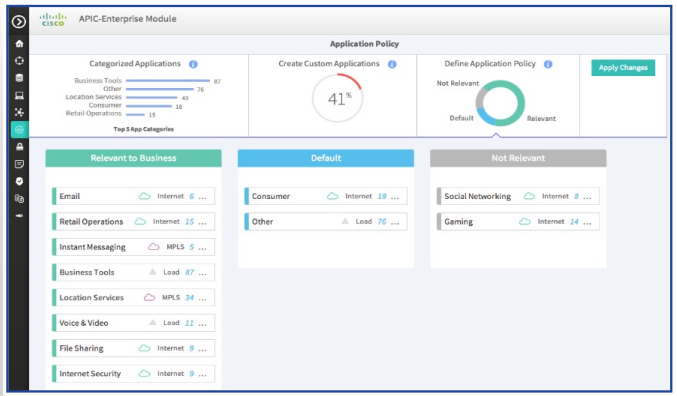
Granular App Detection
Encrypted Application

Monitor Your Applications



Fault Isolation, Troubleshooting
Performance Assessment

Control Your Applications



Prioritized Applications,
Bandwidth Management

AVC Features

Application Recognition

- Generation Deep Packet Inspection Technology
- NBAR2: Network Based Application Recognition 2
- Dynamic / Protocol Packup Grade
- Custom application

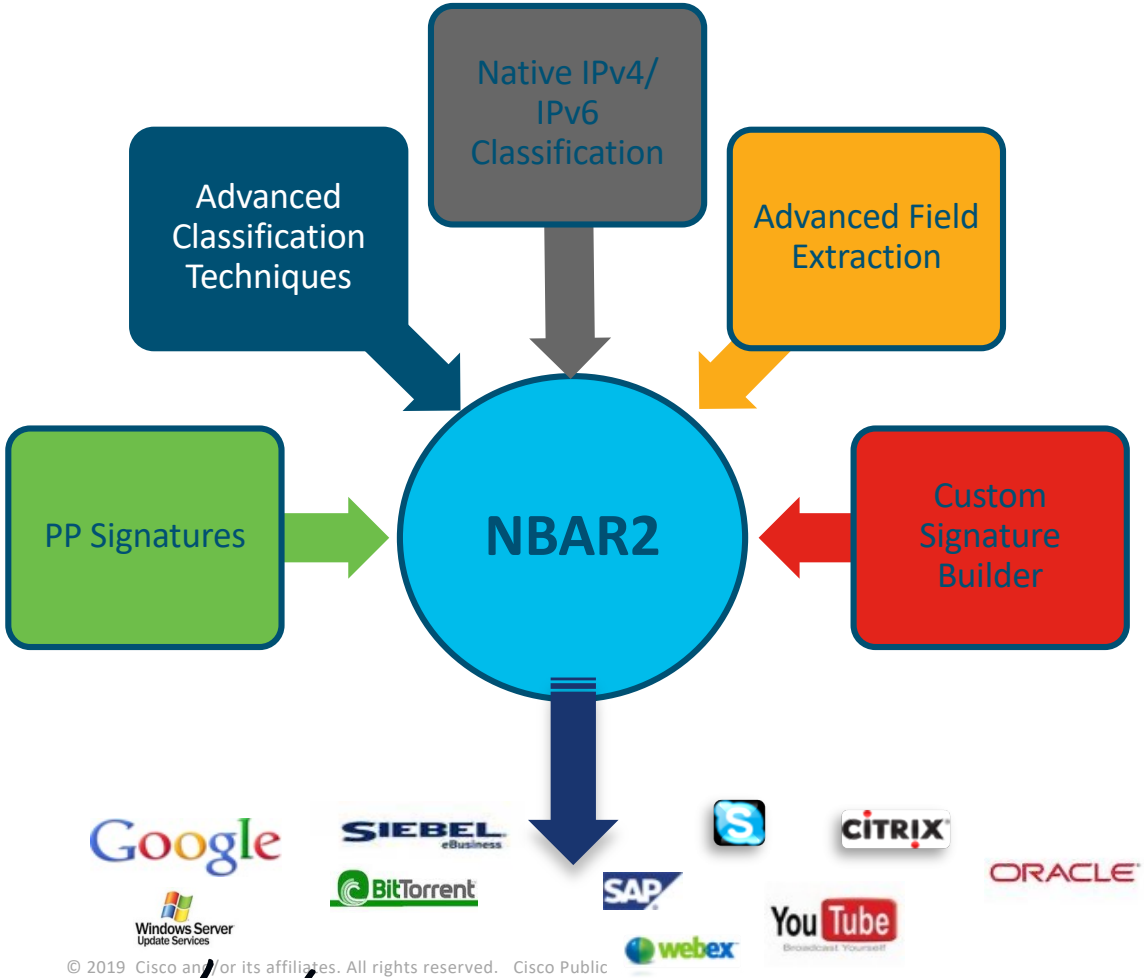
Visibility

- Protocol Discovery – per interface, per direction
- FNF with application name as match/collect

Control

- Application based QOS

Network Based Application Recognition 2 (NBAR2)



- Optimize the Application experience in the network
- Hitless Protocol Pack update allows adding more applications.
- Supported devices :
  - from 16.6(3): **Catalyst 9300**
  - from 16.9.1: **Catalyst 9400**
  - from 16.11.1: **Catalyst 9200**
- Requires a Cisco DNA Advantage license

Recognizes
~1500 Apps
~140 Encrypted Apps

NBAR2 on Catalyst 9000 – How is it done?

Performance and scale

2000 cps with max 10000 flows (24 port switch)

2000 cps with max 20000 flows (48 port switch)

CPU varies from 10% - 40%

NBAR2 lookup

- Original packets of a flow are hardware-switched to destination
- Copies of the initial few packets of a flow to CPU
- The software interacts with the NBAR2 module and detect the Application.

How will it work in Campus?

NBAR2 Protocol Library

Print

Updated: June 23, 2018

Downloading NBAR2 Protocol Packs

NBAR2 Protocol Packs are available for download on the Cisco.com software download page, here:

http://www.cisco.com/cisco/software/navigator.html

On the download page, specify a platform model to display software available for download. One software option is NBAR2 Protocol Packs.

Example:

To display protocol packs available for the Cisco ASR 1001 platform, open the link provided above and navigate as follows:

Products > **Routers** > **Service Provider Edge Routers** > **ASR 1000 Series Aggregation Services Routers** > **ASR 1001 Router**

DOWNLOAD HERE

NBAR2 Protocol Packs for Cisco IOS and IOS-XE Releases

Protocol Pack	Supported Releases	Supported From...
Protocol Pack 38.0.0 Release Notes	**Releases supported by Protocol Pack upgrade**: IOS-XE Everest 16.6.2	2018-06-22
Protocol Pack 37.0.0 Release Notes	**Releases supported by Protocol Pack upgrade**: IOS-XE Everest 16.6.2	2018-05-01
Protocol Pack 36.0.0	**Built into**:	

SKYPE

Name/CLI Keyword	skype
Full Name	Skype
Description	Skype software uses a proprietary Internet telephony (VoIP) network called the Skype protocol. Part of the Skype technology relies on the Global Index peer-to-peer protocol belonging to the Joltid Ltd. corporation. Skype is software that contains several features such as telephone calls over the Internet, instant messaging, file transfer and video conferencing.
Reference	http://www.skype.com
Global ID	L7:83
ID	83
Known Mappings	
UDP Port	53,5353
TCP Port	53,80,443,5353, 33033
IP Protocol	-
IP Version	
IPv4 Support	Yes
IPv6 Support	Yes
Application Group	skype-group
Business Relevance	business-irrelevant. From Cisco IOS XE 3.16S and IOS 15.5(3)M only.
Category	voice-and-video
Sub Category	voice-video-chat-collaboration
P2P Technology	Yes
Encrypted	Yes
Traffic-class	multimedia-conferencing. From Cisco IOS XE 3.16S and IOS 15.5(3)M only.
Tunnel	No
Underlying Protocols	dns,http,ssl

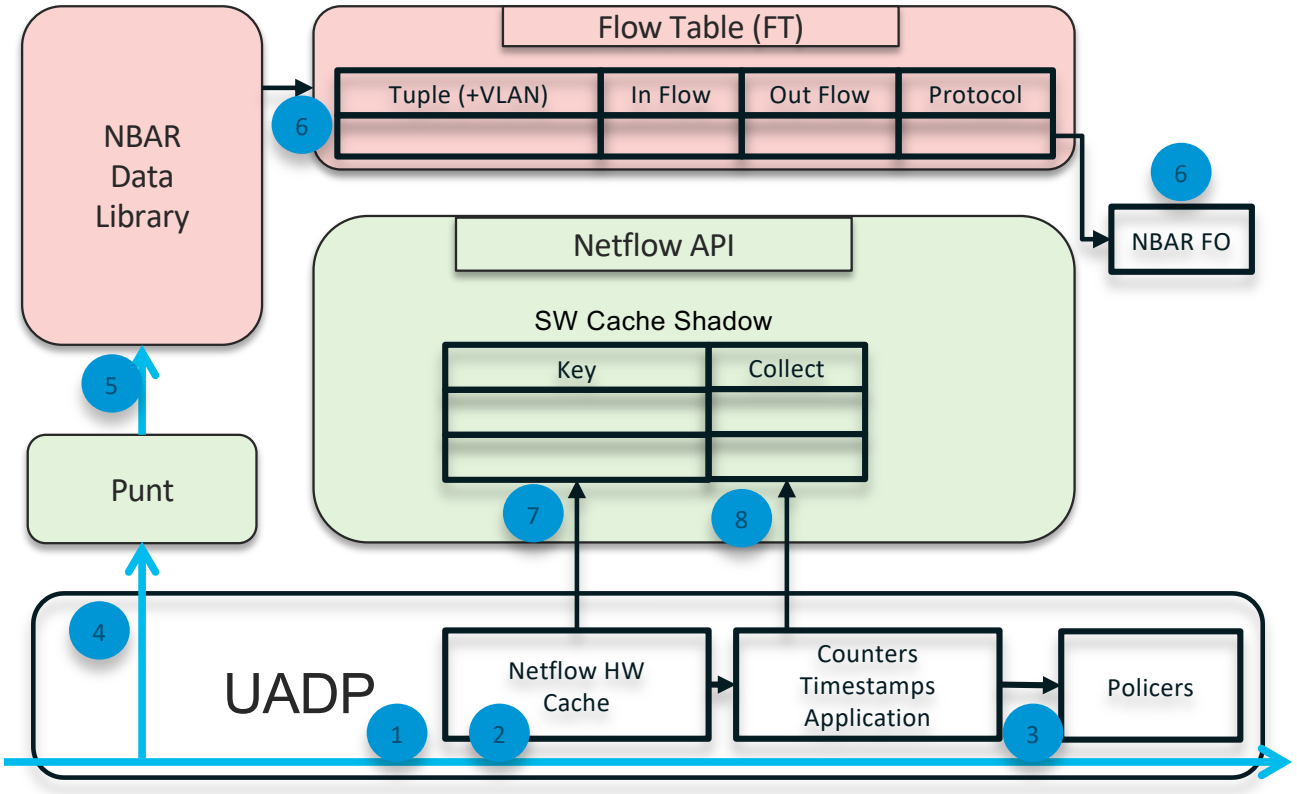
Updatable packs are available from 16.6(4) for

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

For Your Reference

NBAR2 Data Path – First Packet in Flow

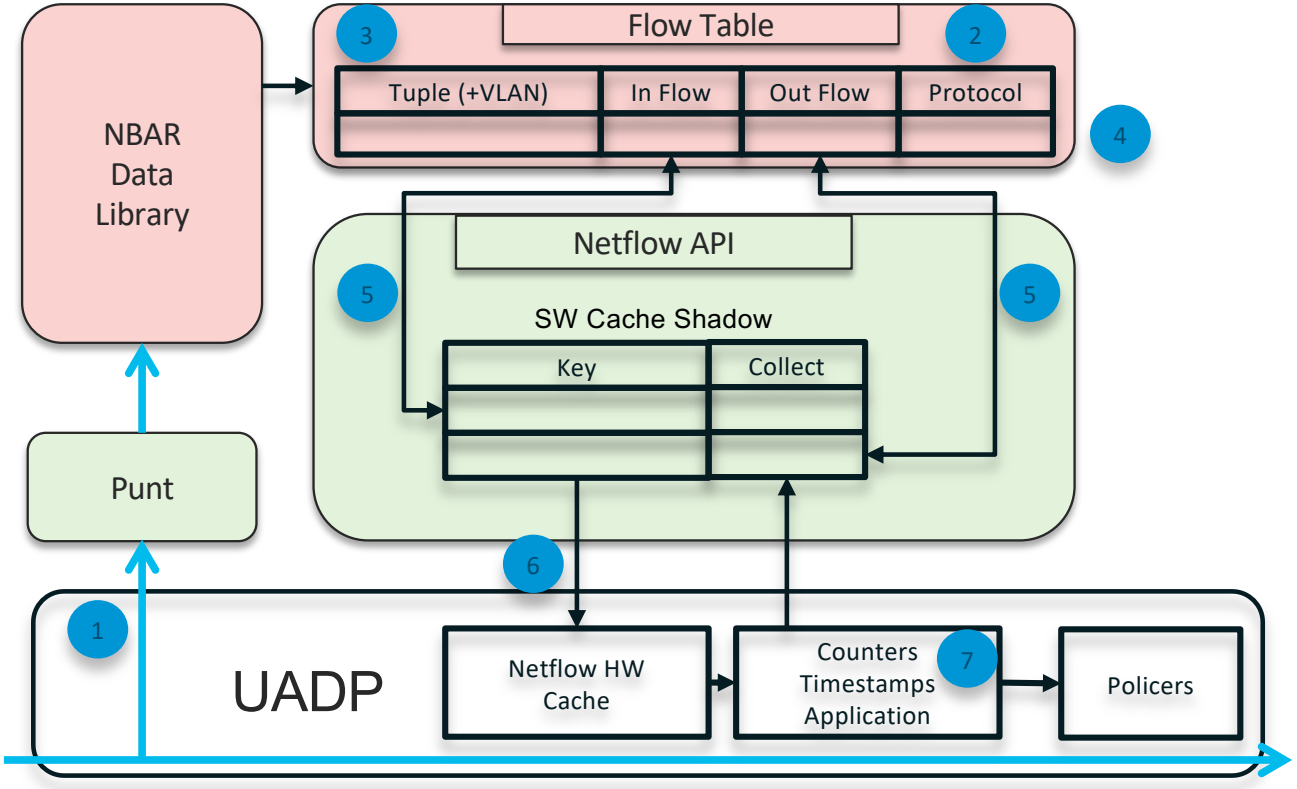
1. NBAR is enabled on interface. Flow table activates the monitor. First packet of a flow is seen.
2. A new Neflow entry is created with 'Copy to CPU' attribute.
3. Original packet continues normal processing.
4. Duplicated packet is punted to CPU with some packet metadata like interface ID.
5. Packet forwarded to NBAR Library.
6. NBAR creates a flow in the flow table. Default idle timeout is configured for the FT flow.
7. In parallel, new netflow entry is reported to the software cache.
8. Counters, timestamps and TCP flags are offloaded periodically to the software cache.



For Your Reference

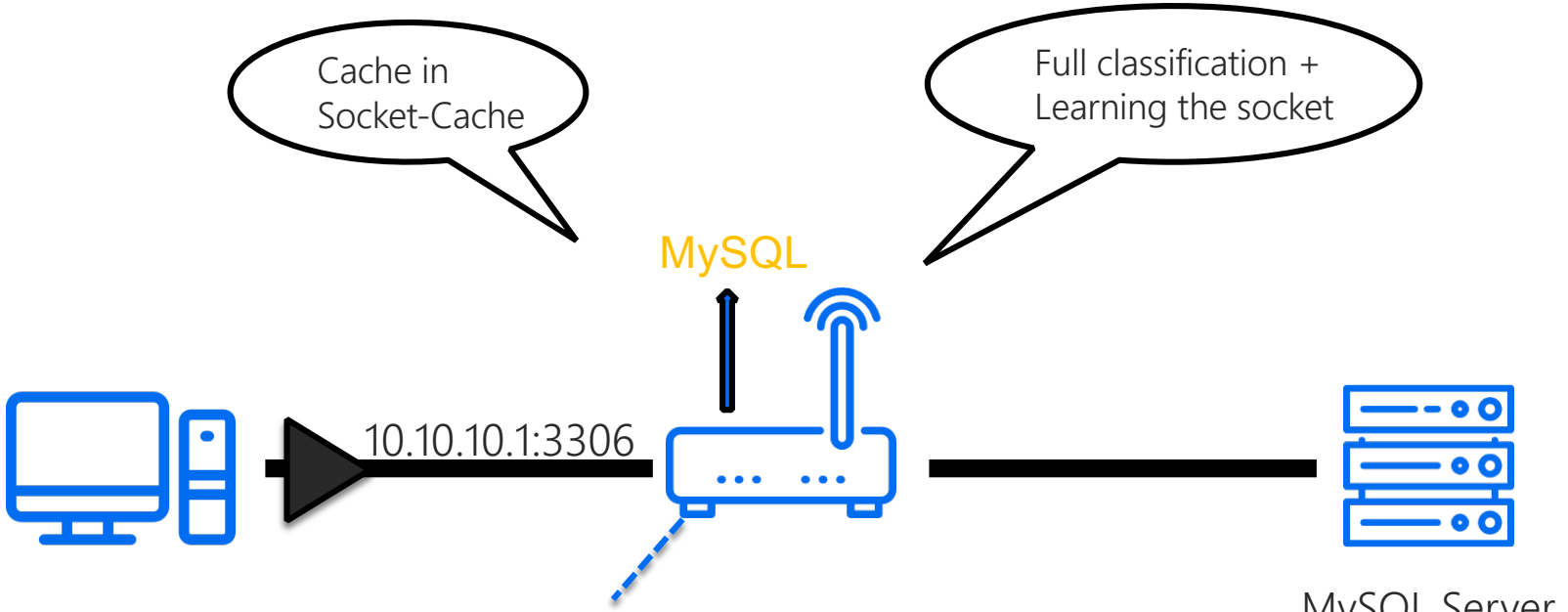
NBAR2 Data Path – App Resolution Packet

1. Packet of application resolution arrives.
2. NBAR updates protocol in the Flow Table.
3. NBAR updates Flow Table idle timeout for this flow, based on the identified application.
4. NBAR scratch pad (Feature Object) is freed and cloned packet is discarded.
5. Flow table 'sync' the flow with Netflow cache: Update indexes of netflow entries for both direction.
6. Mark Netflow entries to stop cloning packets.
7. Update App ID in FNF HW cache for QOS usage.



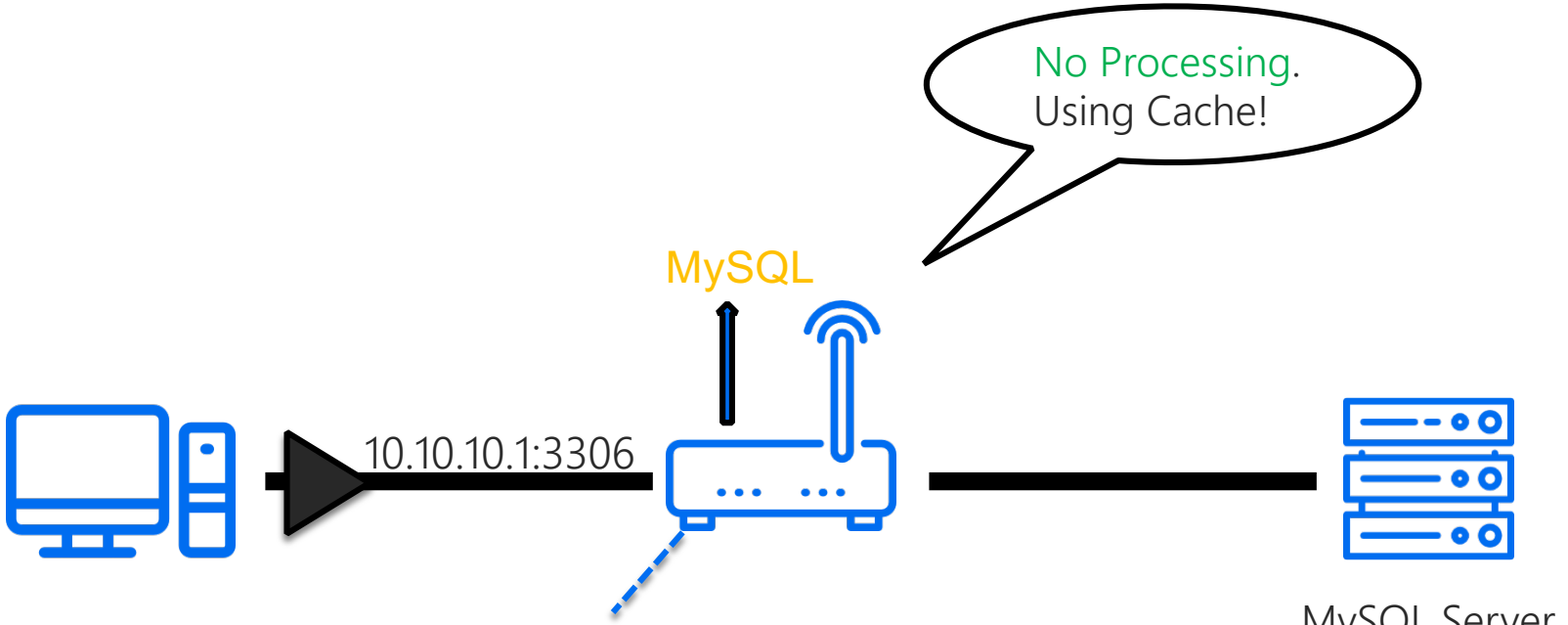
EXAMPLE

NBAR2 Socket Cache Classification - Example



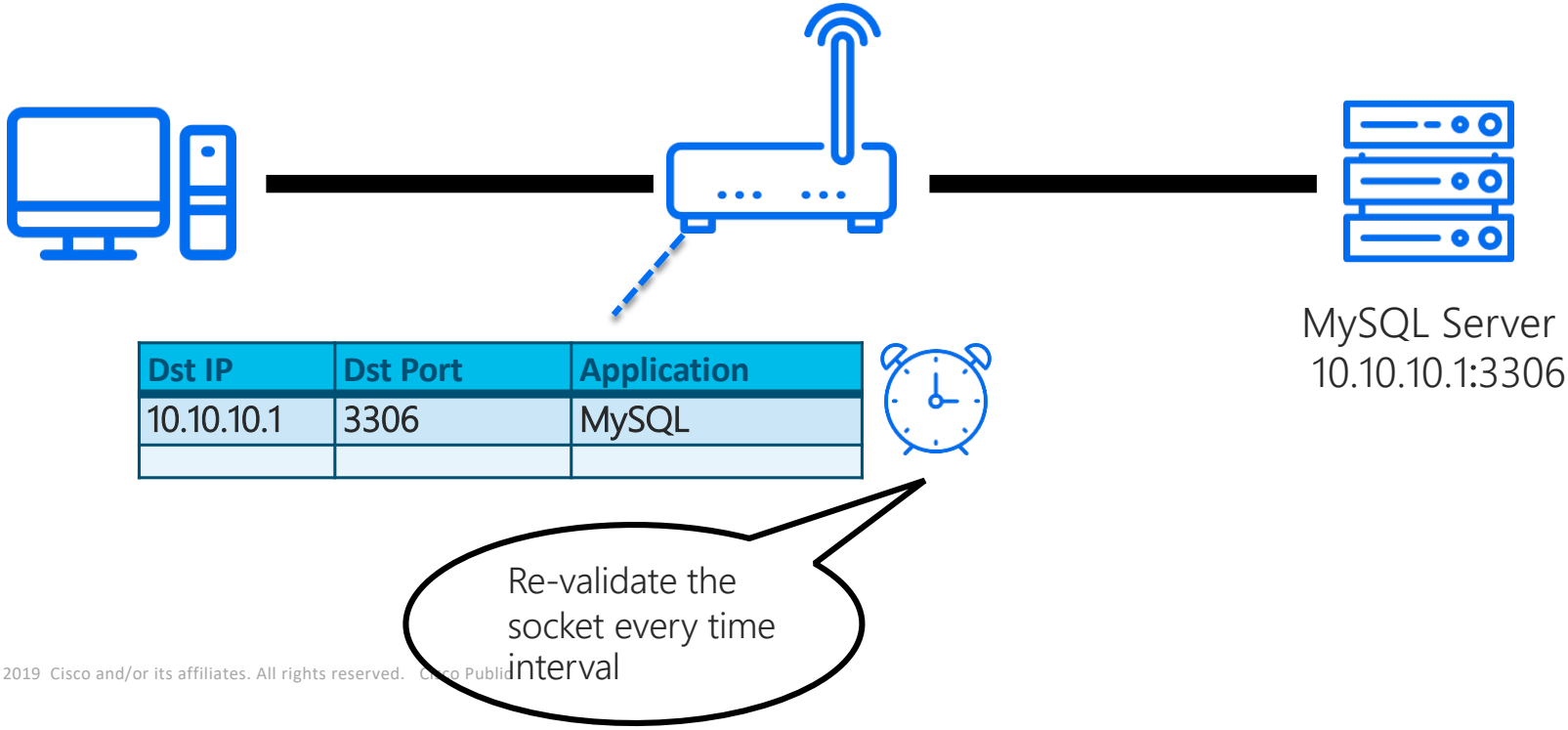
Dst IP	Dst Port	Application
10.10.10.1	3306	MySQL

NBAR2 Socket Cache Classification - Example



Dst IP	Dst Port	Application
10.10.10.1	3306	MySQL

NBAR2 Socket Cache Classification - Example



Dst IP	Dst Port	Application
10.10.10.1	3306	MySQL

Classification and Encryption

NBAR2 Encrypted traffic – techniques

For Your Reference

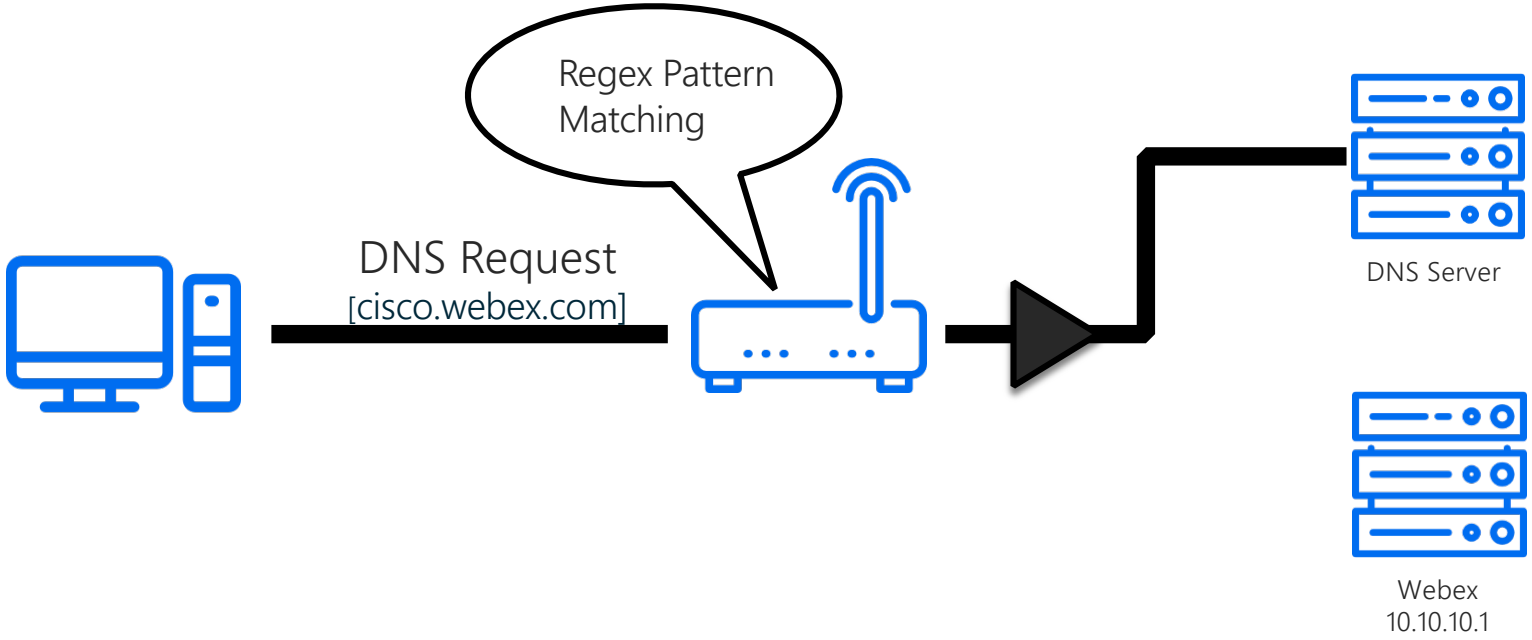
Outside the organization (usually non collaborative):

- SSL handshake analysis – certificate, Server Name Indication (SNI)
- DNS traffic analysis
- Machine learning/Statistical classification

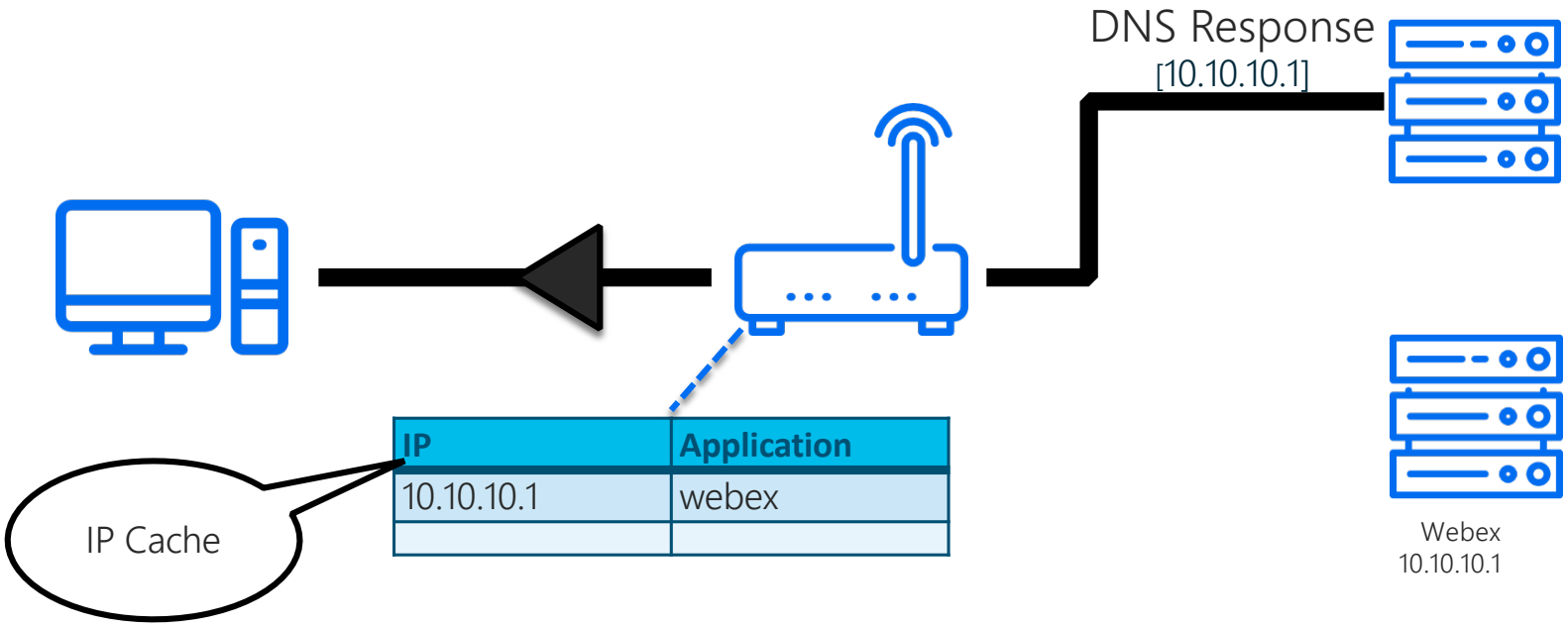
Inside the organization (usually collaborative):

- Customization of SSL certificates and DNS domains
- Server and client discovery based on NBAR2
- SD-AVC External Sources

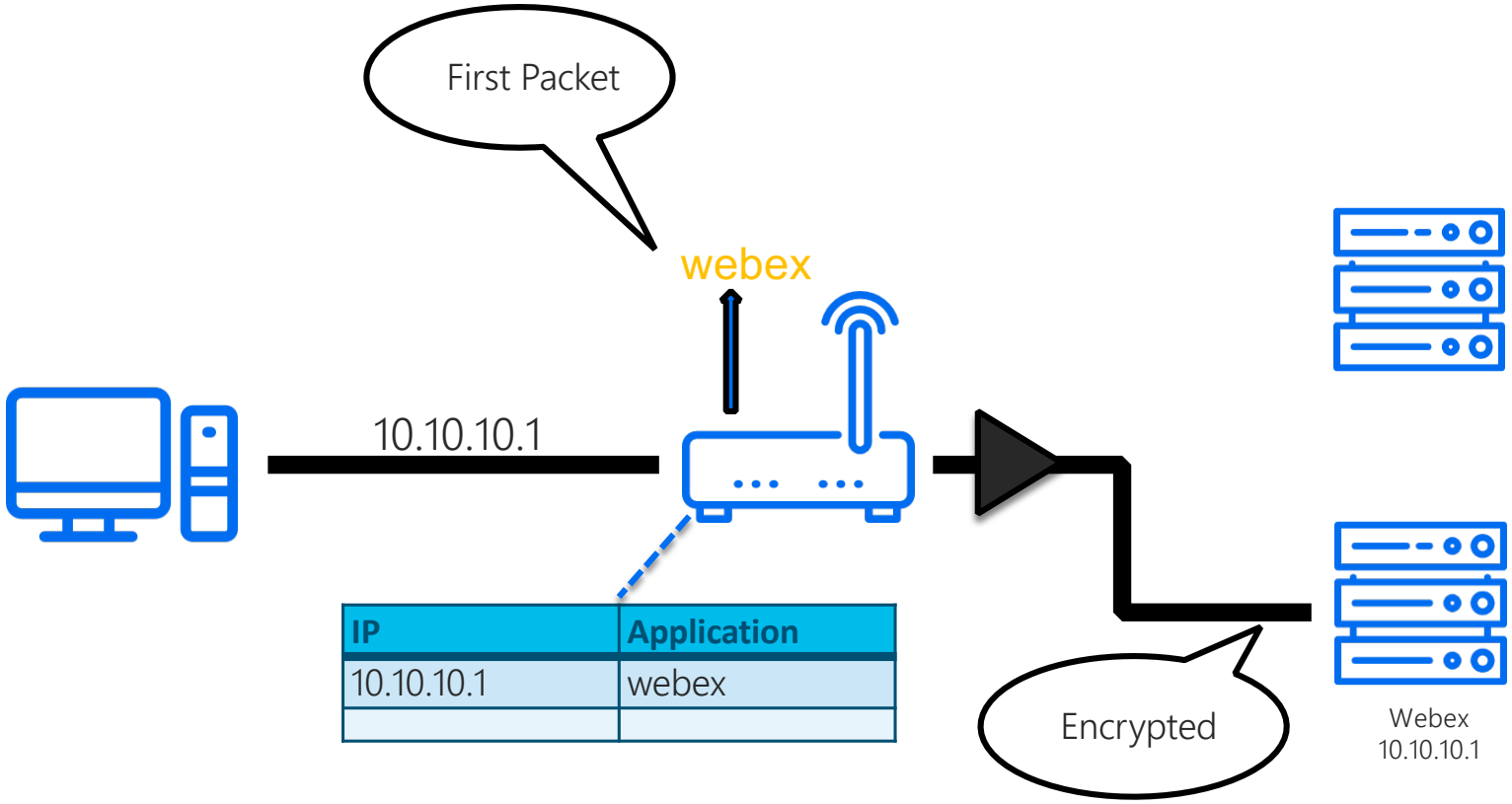
NBAR2 DNS Classification - Example



NBAR2 DNS Classification - Example



NBAR2 DNS Classification - Example



IP	Application
10.10.10.1	webex

NBAR2 Encryption Classification

For Your Reference

Automatic (Signature)

```
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 167
    ⊟ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 163
        Version: TLS 1.0 (0x0301)
      ⊞ Random
        Session ID Length: 0
        Cipher Suites Length: 72
      ⊞ Cipher Suites (36 suites)
        Compression Methods Length: 1
      ⊞ Compression Methods (1 method)
        Extensions Length: 50
      ⊟ Extension: server_name
          Type: server_name (0x0000)
          Length: 20
        ⊟ Server Name Indication extension
            Server Name list length: 18
            Server Name Type: host_name (0)
            Server Name length: 15
            Server Name: www.youtube.com
```

Custom

```
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 188
    ⊟ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 184
        Version: TLS 1.2 (0x0303)
      ⊞ Random
        Session ID Length: 0
        Cipher Suites Length: 74
      ⊞ Cipher Suites (37 suites)
        Compression Methods Length: 1
      ⊞ Compression Methods (1 method)
        Extensions Length: 69
      ⊟ Extension: server_name
          Type: server_name (0x0000)
          Length: 27
        ⊟ Server Name Indication extension
            Server Name list length: 25
            Server Name Type: host_name (0)
            Server Name length: 22
            Server Name: schoolnet.ccsocdev.net
```

"(.*[.])?((youtube(-nocookie)?|ytimg|googlevideo)[.]com)|youtu[.]be"

cisco(config)#*ip nbar custom CCSOC composite server-name "*ccsocdev.net"*

NBAR2 Encrypted Traffic Classification Summary

For Your Reference

- Most of the traffic is encrypted traffic and is SSL/TLS
- Testing shows more than 80% of SSL traffic is classified by NBAR2
- All major internet/cloud applications are supported
- NBAR2 classifies both cloud and local encrypted traffic
- NBAR2 use a variety of techniques to classify encrypted traffic

CISCO