# TOMORROW starts here.

Cisco live!

# IBNS 2.0: New-style 802.1X and More

BRKSEC-2691

Hariprasad Holla
Technical Marketing Engineer, Cisco

#clmel

Cisco live!

# Secure Access Sessions

**BRKSEC-2690 - Deploying Security Group Tags**
- 105, Wednesday 18 Mar 1:00 PM - 2:30 PM by Kevin Regan - Product Manager, Cisco

**BRKSEC-2699 - Securing Your Network Simply with TrustSec**
- 212, Wednesday 18 Mar 1:00 PM - 2:30 PM by Brandon Johnson - Systems Engineer, Cisco

**BRKSEC-2044 - Building an Enterprise Access Control Architecure Using ISE and TrustSec**
- 207, Thursday 19 Mar 8:30 AM - 10:30 AM by Imran Bashir - Technical Marketing Engineer, Cisco

**BRKSEC-2691 - IBNS 2.0: New style 802.1X and more**
- 207, Thursday 19 Mar 4:30 PM - 6:00 PM by Hariprasad Holla - Technical Marketing Engineer, Cisco

**BRKSEC-3045 - Advanced ISE and Secure Access Deployment**
- 204, Friday 20 Mar 8:45 AM - 10:45 AM by Jatin Sachdeva - Consulting Systems Engineer, Cisco

**BRKSEC-3690 - Advanced Security Group Tags: The Detailed Walk Through**
- 203, Friday 20 Mar 8:45 AM - 10:45 AM by Darrin Miller - Distinguished Technical Marketing Engineer, Cisco

**BRKSEC-3697 - Advanced ISE Services, Tips and Tricks**
- 207, Friday 20 Mar 2:00 PM - 4:00 PM by Jason Kunst - Technical Marketing Engineer, Cisco

# Short History of Identity Services

In the Dark Ages, there was only IEEE 802.1X

Then we had MAB, Web Authentication, Auth-Fail VLAN, Guest VLAN, Flex-Auth, Deployment Modes and other features

We now have new way of doing Identity based access, with features like Critical ACL, Concurrent Authentication, Templates, and more.

**IEEE 802.1X**

**( EAPoLAN )**
**( EAPoWLAN )**

**IBNS**

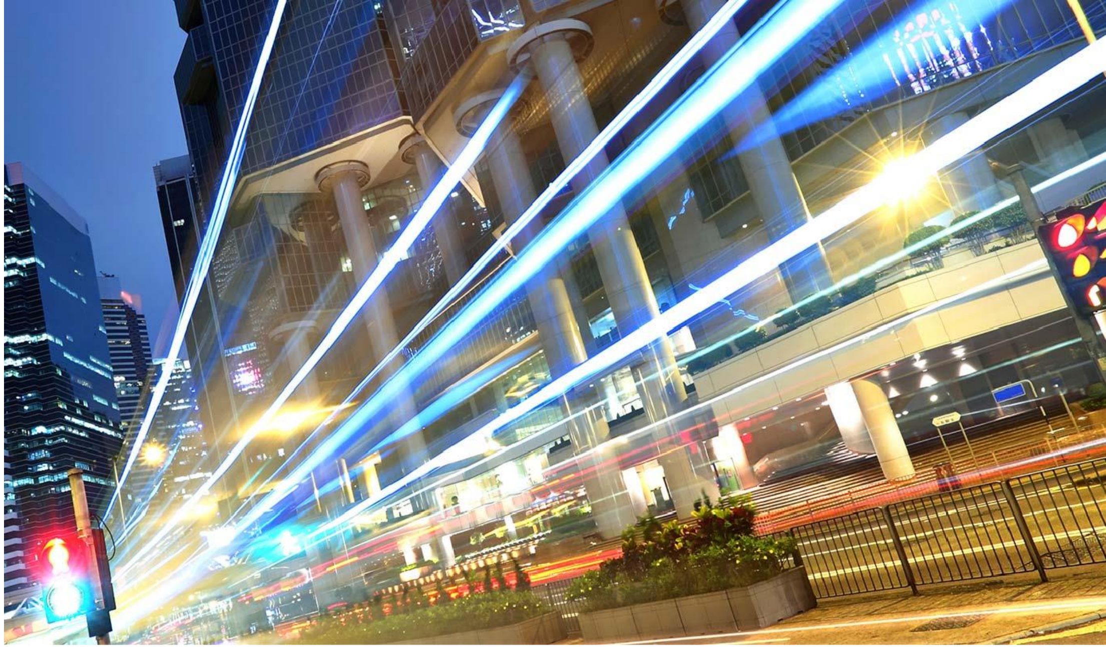
**( Identity Based Networking Services )**

**IBNS 2.0**

**( Identity Based Networking Services 2.0 )**

# Agenda

- Identity networking
- IBNS 2.0
- IBNS 2.0 Features
- Troubleshooting IBNS 2.0
- Additional things to know
- Conclusion



**Icons to remember**

**For Your Reference**

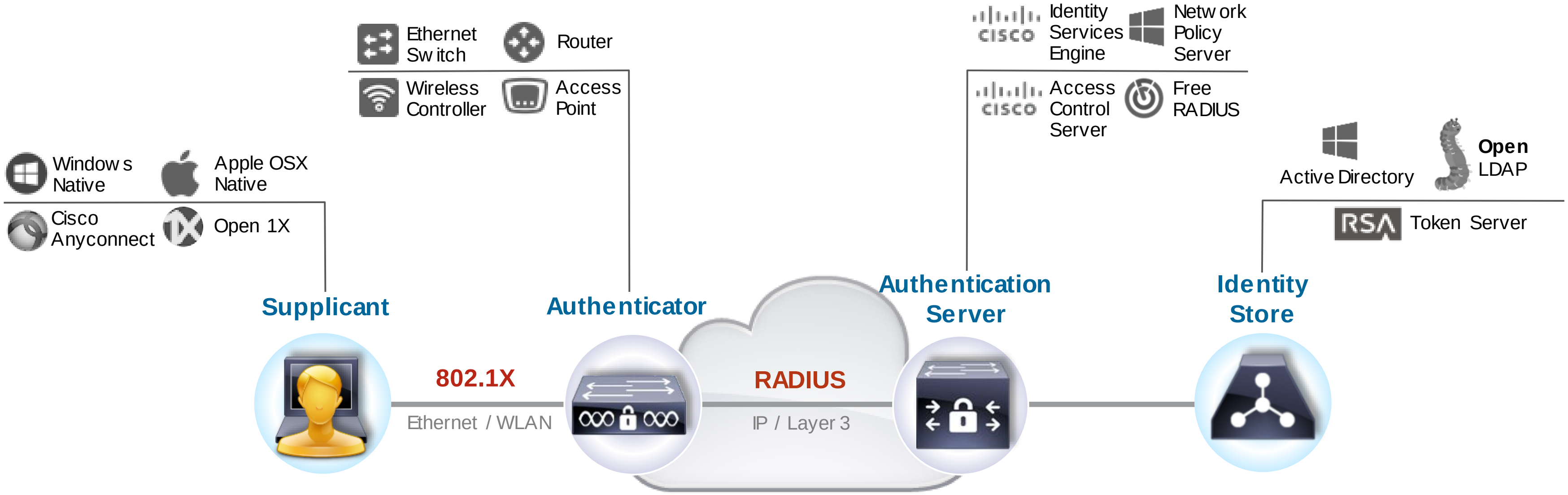
**Cisco Secure ACS / Generic RADIUS Server**

**Cisco ISE**

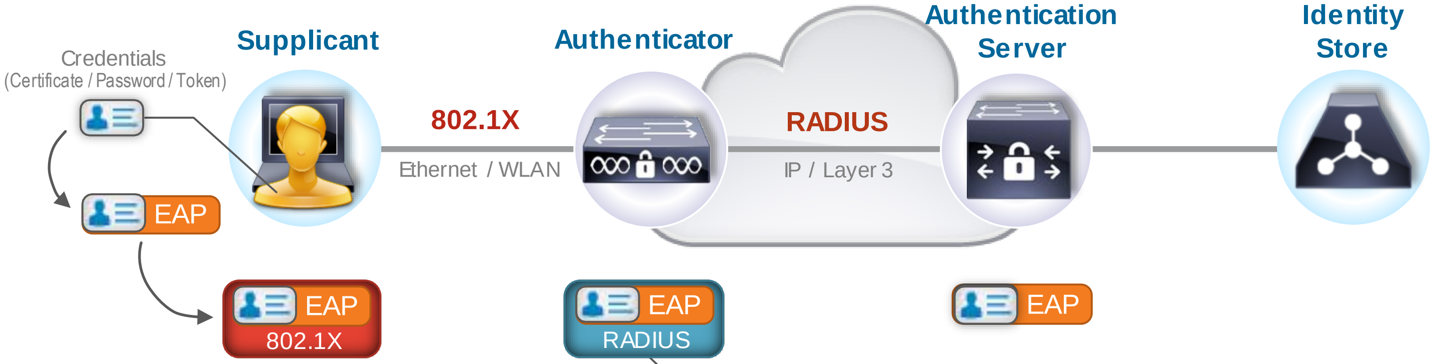
**Real-world Scenario**

# Identity Networking

# Fundamentals of 802.1X



# Fundamentals of 802.1X



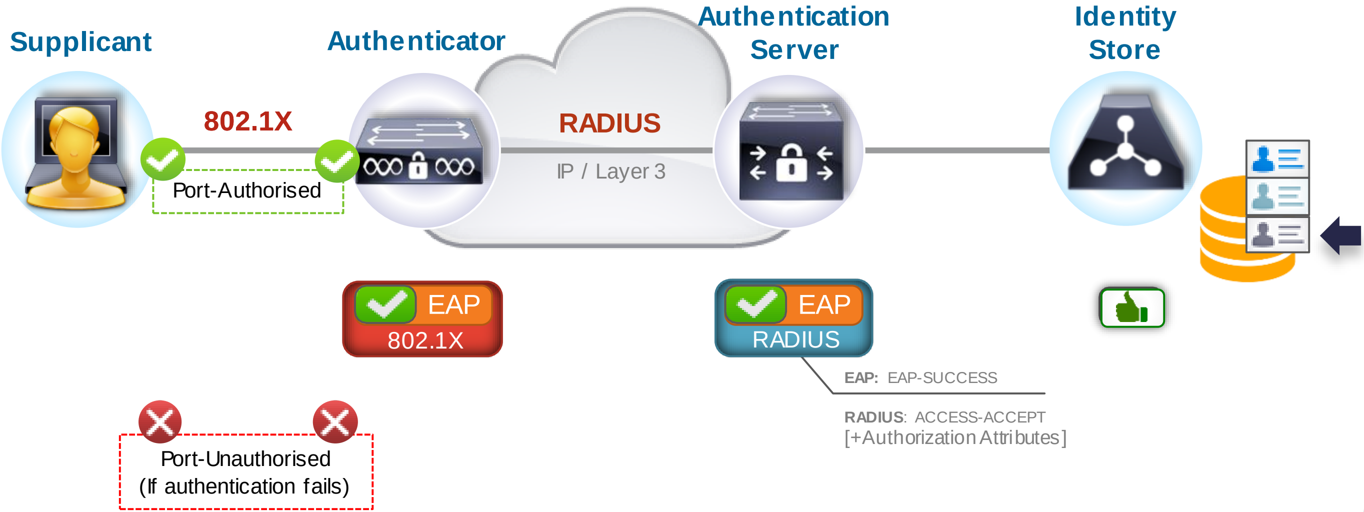
**RADIUS:** ACCESS-REQUEST

**RADIUS** SERVICE-TYPE: FRAMED

**EAP:** EAP-RESPONSE-IDENTITY

EAP: Extensible Authentication Protocol

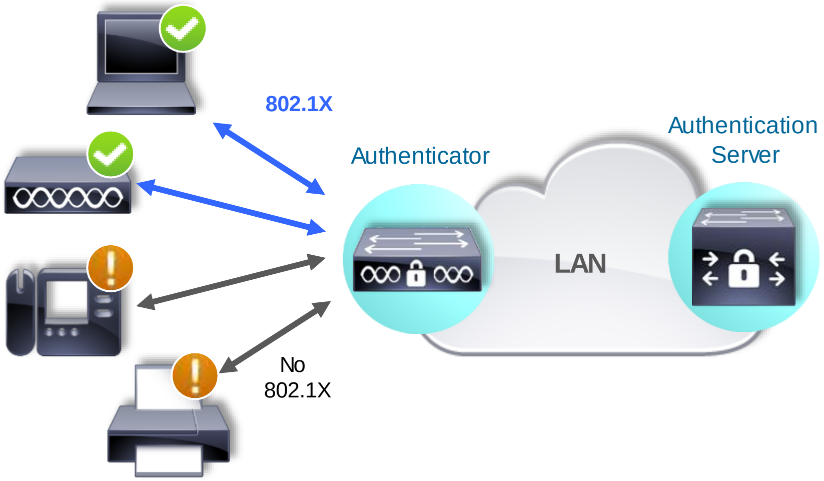
# Fundamentals of 802.1X



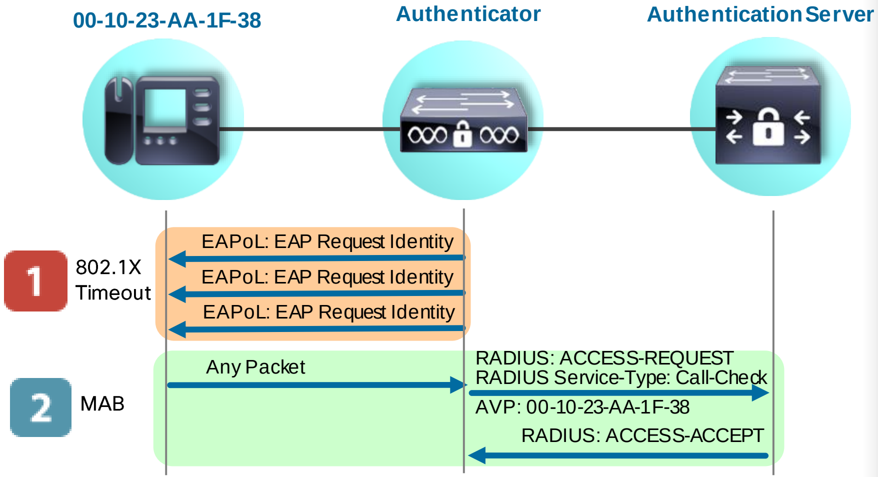
EAP: Extensible Authentication Protocol

# MAC Authentication Bypass

Endpoints without supplicant will fail 802.1X authentication!



Bypassing "Known" MAC Addresses

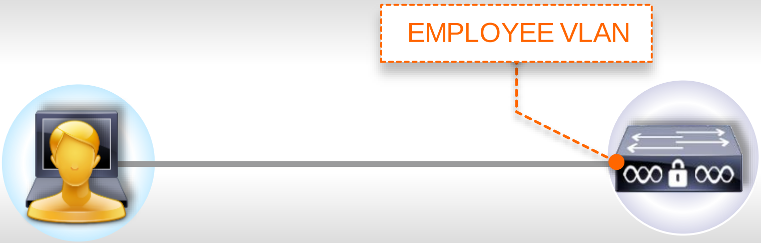


MAC Authentication Bypass (MAB) requires a MAC database | MAB may cause delayed network access due to EAP timeout

# Authorisation Options

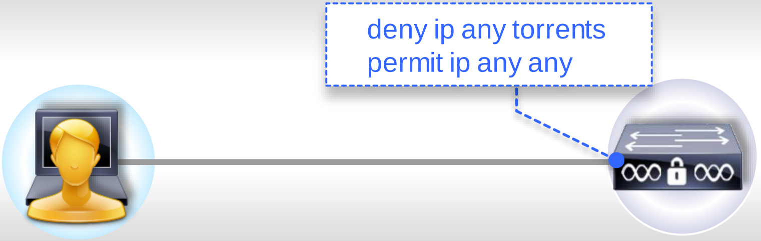
## Beyond ACCESS-ACCEPTs and ACCESS-REJECTs

### Dynamic VLAN Assignments


EMPLOYEE VLAN

### Access Control Lists

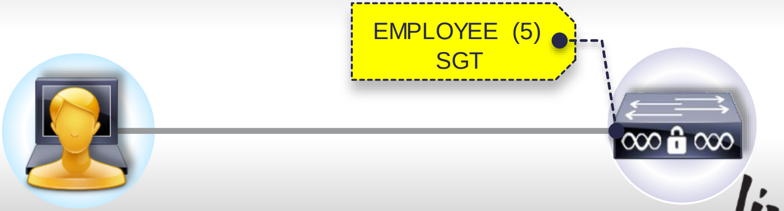
(Downloadable ACLs / Named ACLs)


deny ip any torrents
permit ip any any

### Security Group Tag (SGT)

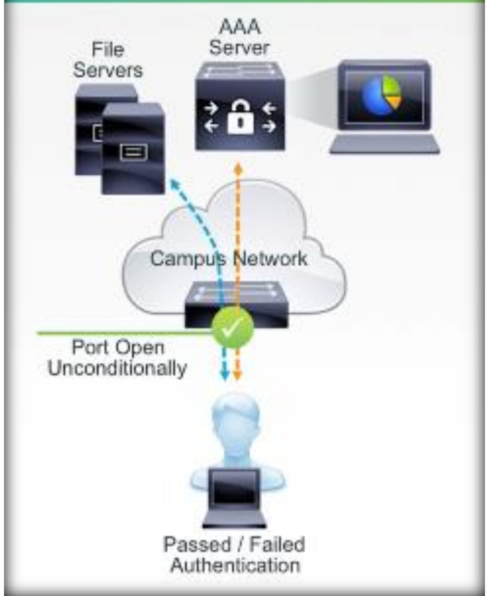
SGT, SXP Transport | SGACL, SGFW Enforcement

(More on SGTs: BRKSEC-2690, BRKSEC-3690)


EMPLOYEE (5)
SGT

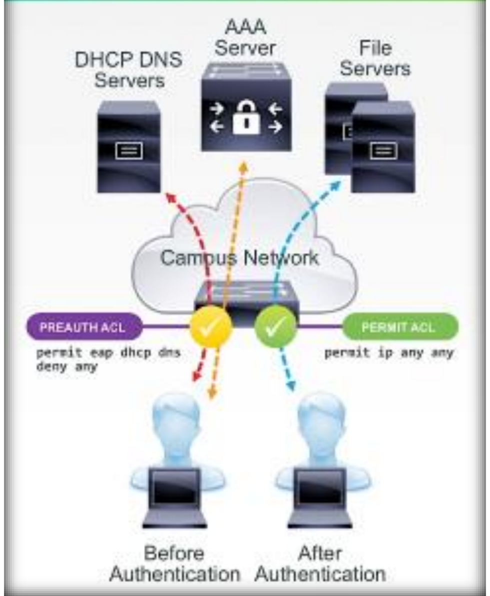
# Three Proven Deployment Modes

## Monitor Mode



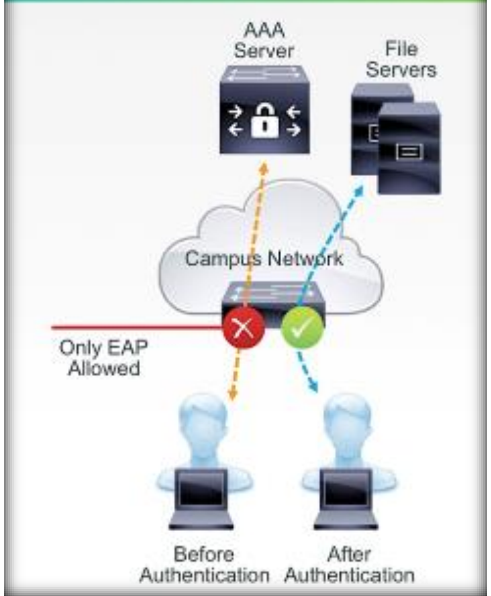
Authentication without Access control

## Low-Impact Mode



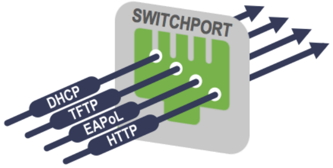
Minimal impact to users and the network

## Closed Mode

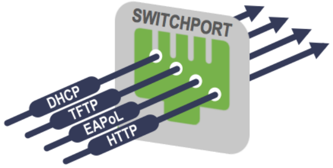


Highly Secure, Good for logical isolation

# 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

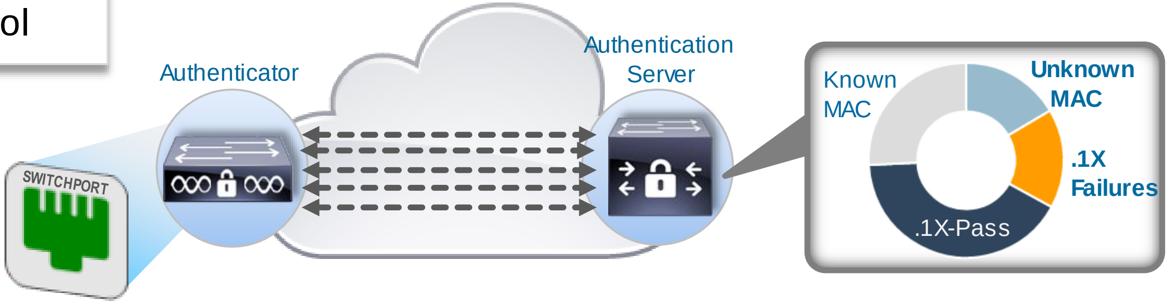
- Enable 802.1X and MAB
- Enable Open Access

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

# Monitor Mode – Next Steps

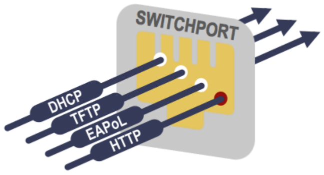
MONITOR MODE : NEXT STEPS

- Improve Accuracy
- Evaluate Remaining Risk
- Leverage Information
- Prepare for Access Control

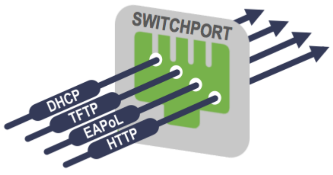


- RADIUS Authentication & Accounting Logs
- Passed / Failed 802.1X
  (Who has bad credentials? Misconfigurations?)
- Passed / Failed MAB attempts
  (What don't I know?)

# Low Impact Mode



Before Authentication



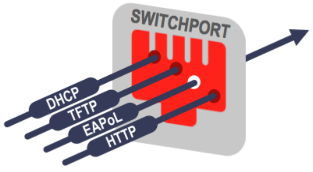
After Authentication

*Pre-Auth and Post-Auth Access controlled by IP ACLs*

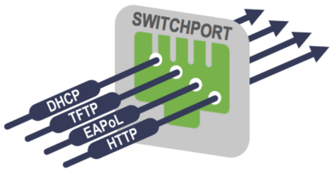
LOW-IMPACT MODE : GOALS

- Begin to control/differentiate network access
- Minimise Impact to Existing Network Access
- Retain Visibility of Monitor Mode
- "Low Impact" == no need to re-architect your network
- Keep existing VLAN design
- Minimise changes

# Closed Mode



Before Authentication



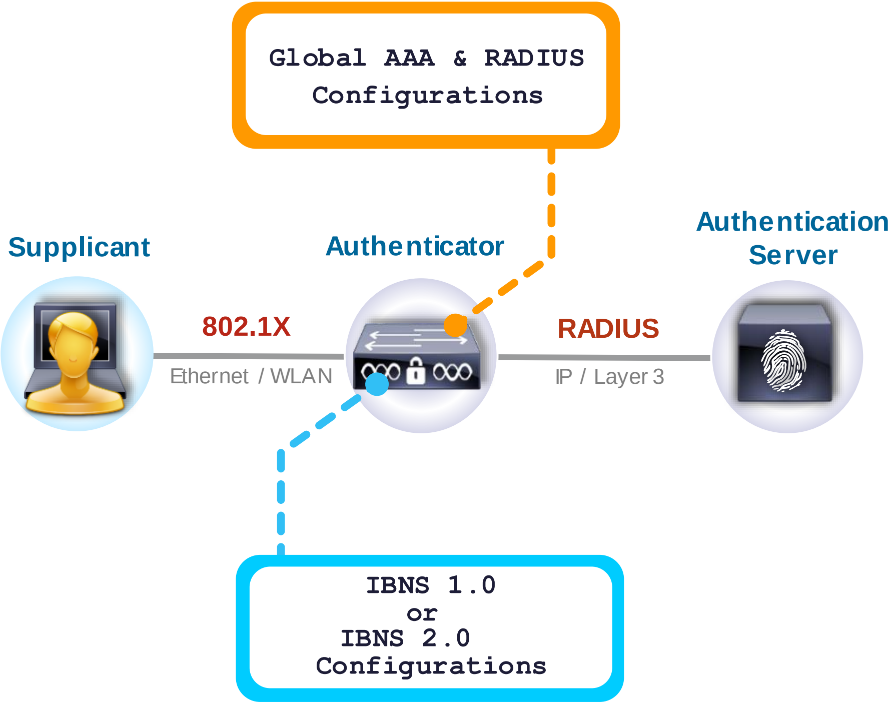
After Authentication

*No access prior authentication, Specific access on Auth-success*

CLOSED MODE : GOALS

- As per IEEE specification for 802.1X
- No access before authentication
- Rapid access for non-802.1X-capable corporate assets
- Logical isolation of traffic at the access edge (VLAN segmentation)

# Configuration You Should Care About



**Choose IBNS 2.0 for:**
**(Will discuss later)**

- Critical ACL
- Service-template Authorisations
- IPv6 Web Authentications*
- Interface Templates

* Currently only on 3650 and 3850 platforms

# Identity Configurations

Global AAA

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa session-id common
!
dot1x system-auth-control
!
radius server ise
 address ipv4 172.20.254.201 auth-port 1645 acct-port 1646
 key cisco
```

IBNS 1.0

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 authentication control-direction in
 authentication event fail action authorize vlan 100
 authentication event server dead action authorize vlan 100
 authentication event no-response action authorize vlan 100
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server dynamic
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
```

-Or-

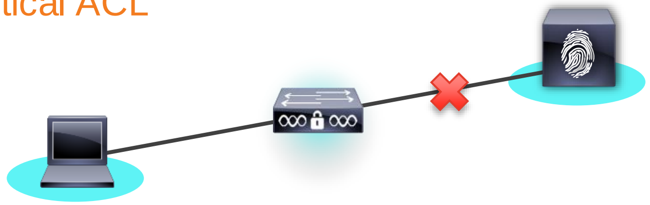
IBNS 2.0

```
class-map type control subscriber match-all DOT1X
 match method dot1x
class-map type control subscriber match-all MAB
 match method mab
....
!
policy-map type control subscriber POLICY_Gi1/0/1
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
....
!
template ACCESS-PORT
 ....
 access-session port-control auto
 service-policy type control subscriber POLICY_Gi1/0/1
 ....
!
interface GigabitEthernet1/0/1
 source template ACCESS-PORT
```

# IBNS 2.0

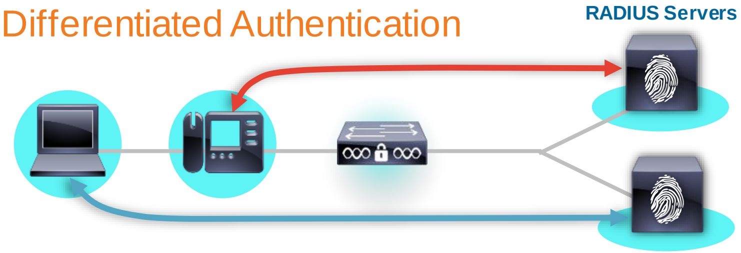
# Motivations for IBNS 2.0

## Critical ACL



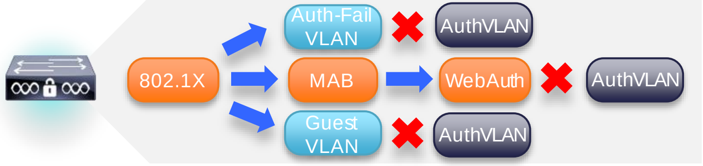
Need for a feature to locally activate an IP ACL during RADIUS Server outage

## Differentiated Authentication



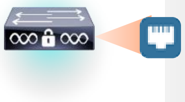
Switch should send authentication requests to specific RADIUS servers for specific methods

## Flexible Authorisations



Need more flexibility in moving between the authorisations for various authentication methods

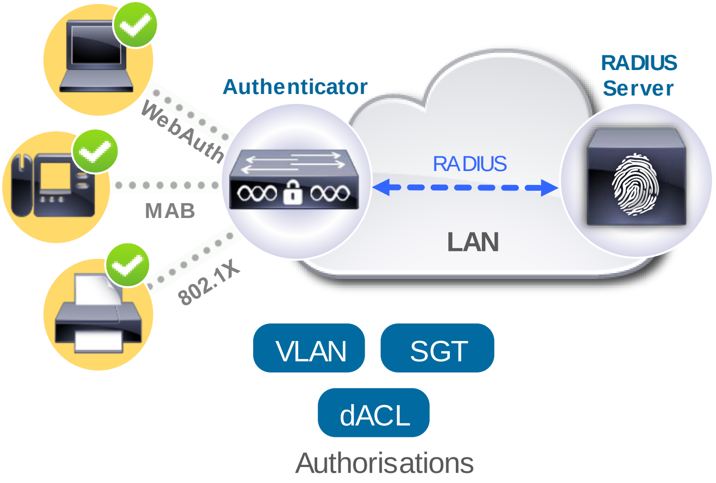
## Configuration Bloat



```
description...
switchport..
spanning-treee...
authentication...
dot1x...
mab
mls qos...
ip access-list...
...
```

Per port configurations grow making it difficult to manage system configurations. Cant ‘**write**’ at times

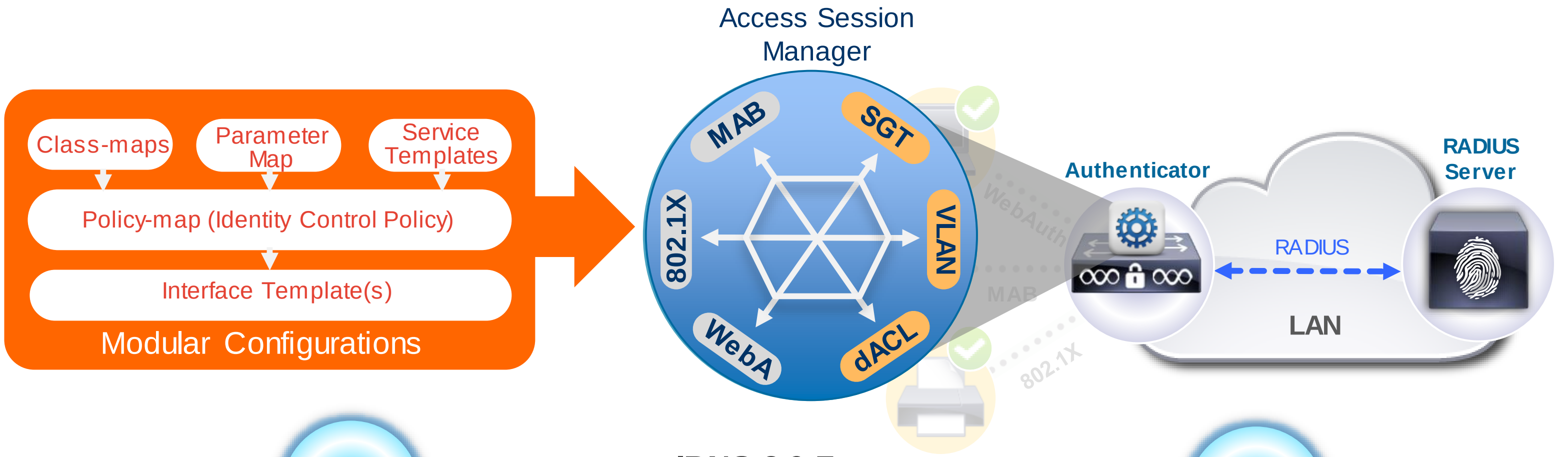
# IBNS 2.0


Authenticator
RADIUS Server
WebAuth
MAB
802.1X
RADIUS
LAN
VLAN
SGT
dACL
Authorisations

# IBNS 2.0

## Any Authentication with Any Authorisation on Any media

*From 15.2(1)E / 03.05.00E*
*C3850/C3650 FCS*
*15.2(1)SY on C6500*
*03.06.00E on Sup8E*

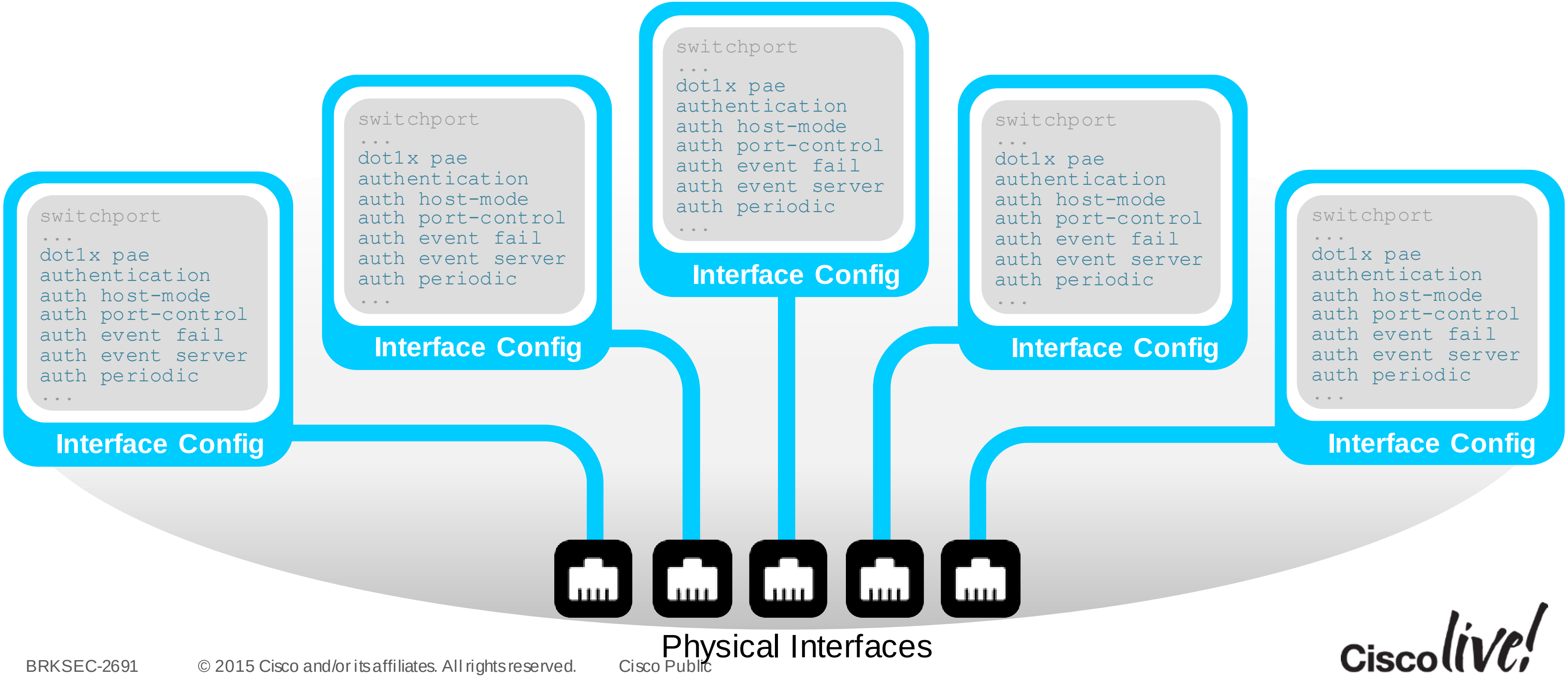


### IBNS 2.0 Features

- Critical ACL
- Intelligent Aging
- Concurrent Authentication
- Enhanced CoA
- Critical MAB
- Common Session-ID
- Differentiated Authentication
- IPv6 WebAuth
- AuthZ templates
- IPv6 Identity
- Template based NEAT

# IBNS 1.0 Configurations

Global AAA & RADIUS Configurations



```
switchport
...
dot1x pae
authentication
auth host-mode
auth port-control
auth event fail
auth event server
auth periodic
...
```

Interface Config

```
switchport
...
dot1x pae
authentication
auth host-mode
auth port-control
auth event fail
auth event server
auth periodic
...
```

Interface Config

```
switchport
...
dot1x pae
authentication
auth host-mode
auth port-control
auth event fail
auth event server
auth periodic
...
```

Interface Config

```
switchport
...
dot1x pae
authentication
auth host-mode
auth port-control
auth event fail
auth event server
auth periodic
...
```

Interface Config

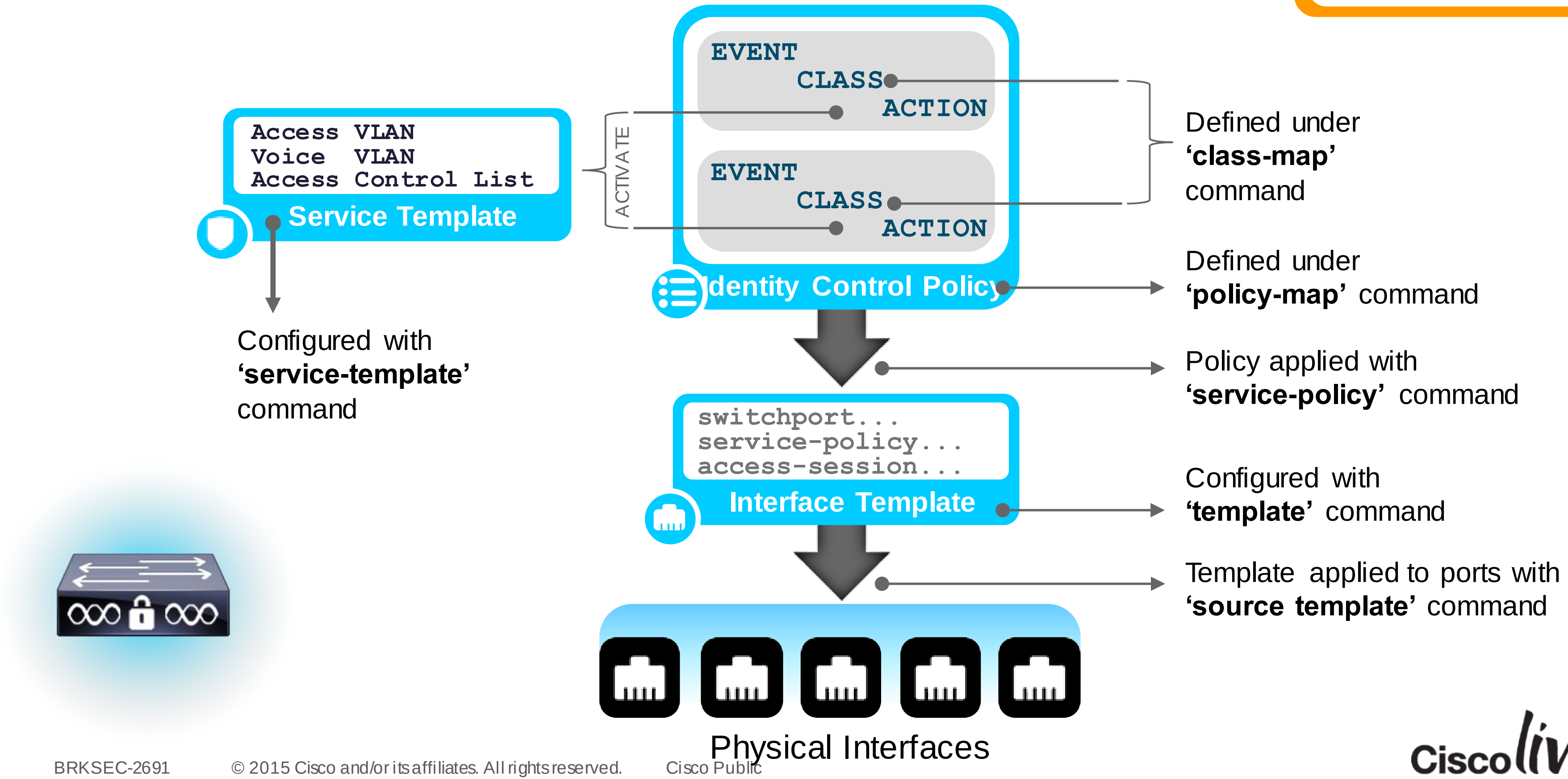
```
switchport
...
dot1x pae
authentication
auth host-mode
auth port-control
auth event fail
auth event server
auth periodic
...
```

Interface Config

Physical Interfaces

# Configuring IBNS 2.0

Global AAA & RADIUS Configurations



Configured with **'service-template'** command

Defined under **'class-map'** command

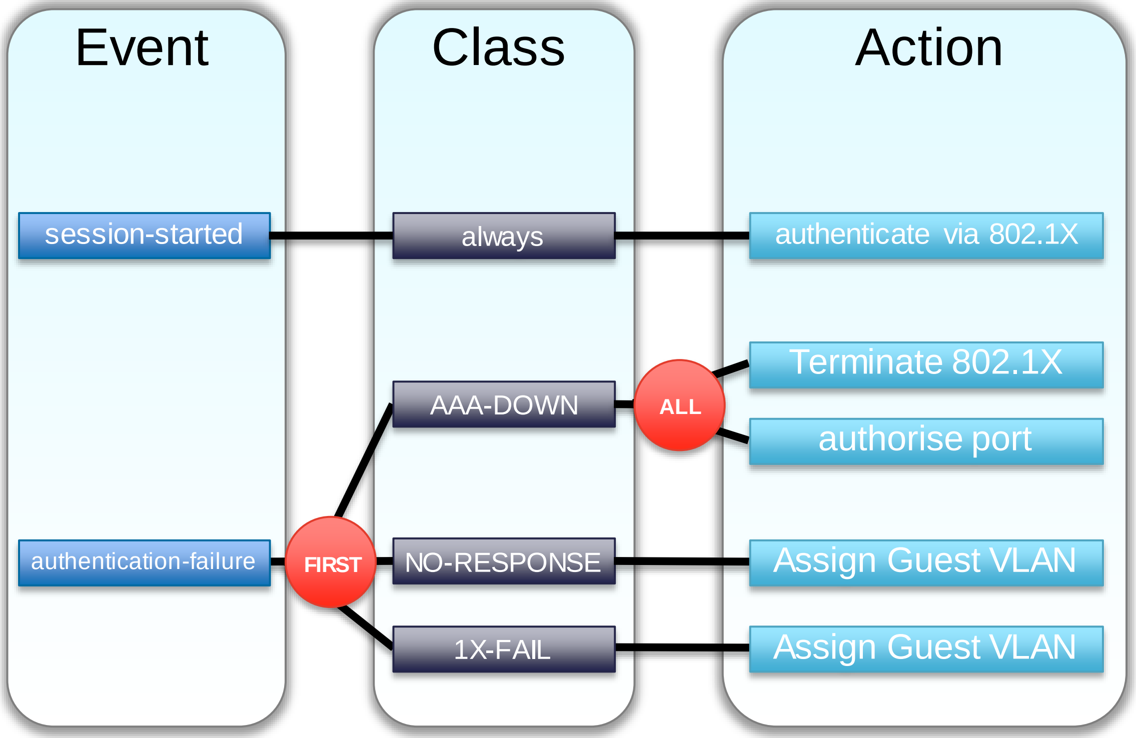
Defined under **'policy-map'** command

Policy applied with **'service-policy'** command

Configured with **'template'** command

Template applied to ports with **'source template'** command

# The Identity Control Policy



**IDENTITY CONTROL POLICY**

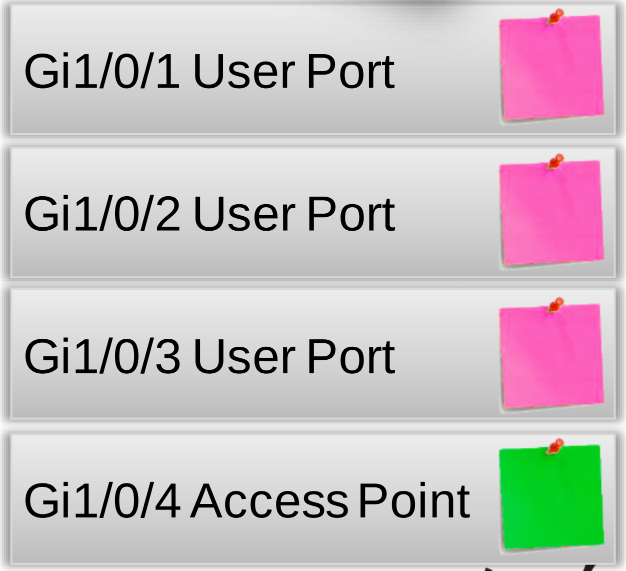
```
policy-map type control subscriber POLICY-A
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
 event authentication-failure match-first
  10 class AAA-DOWN do-all
   10 terminate dot1x
   20 authorize
  20 class DOT1X_NO_RESP do-until-failure
   10 activate service-template GUEST_VLAN
  30 class 1X-FAIL do-all
   10 activate service-template GUEST_VLAN
...
```

# Templates

## Dynamic Configuration Done the Right Way

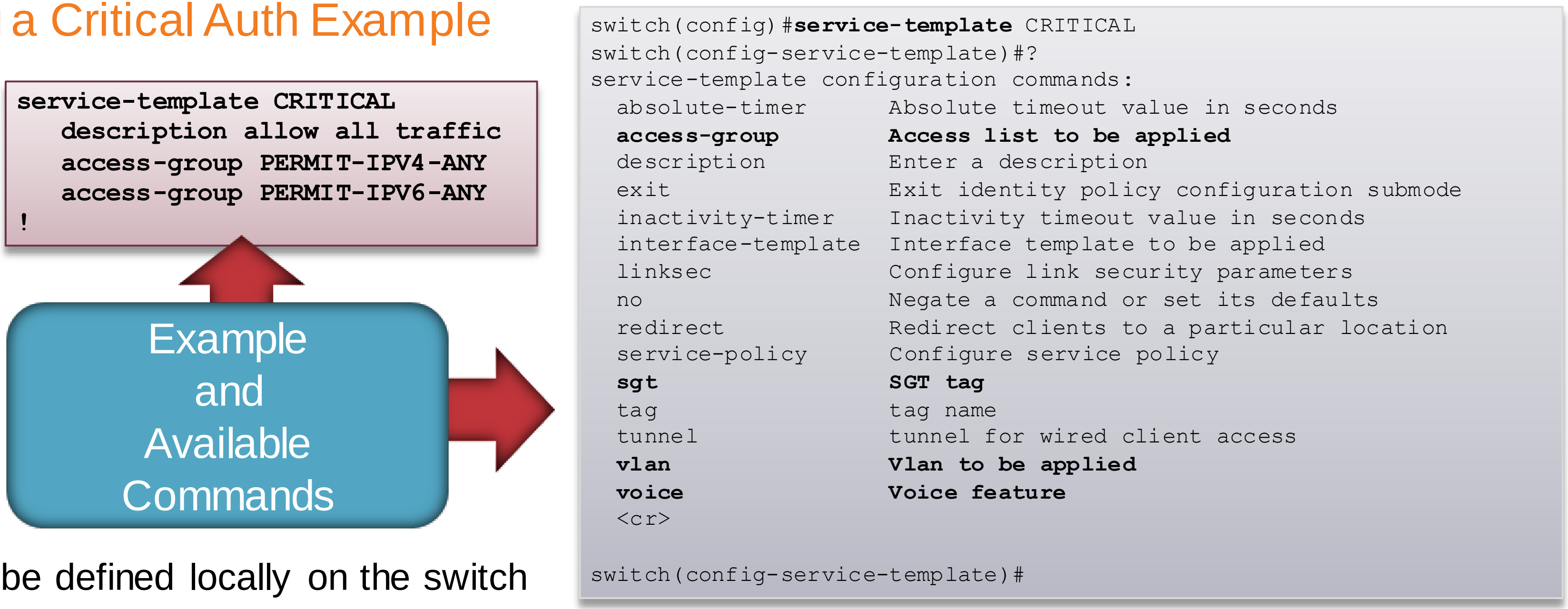
Configuration by Reference:

- Service Templates
  - will be dynamically assigned to a session
  - can be locally defined -or-
  - downloaded via RADIUS
- Interface Templates
  - Cure for the Configuration Bloat
  - Generic tool, not restricted to Session / Identity
  - Like Port Profiles on NX-OS



# Service Template Example

## Using a Critical Auth Example



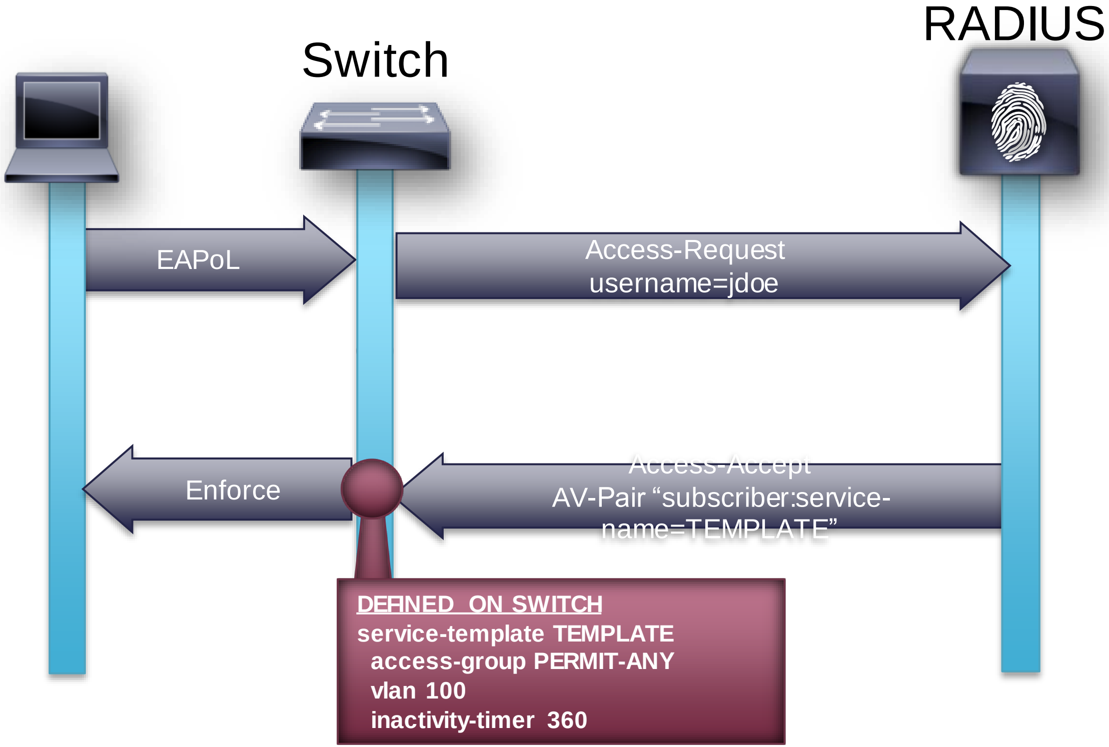
```
service-template CRITICAL
   description allow all traffic
   access-group PERMIT-IPV4-ANY
   access-group PERMIT-IPV6-ANY
!
```

```
switch(config)#service-template CRITICAL
switch(config-service-template)#?
service-template configuration commands:
  absolute-timer      Absolute timeout value in seconds
  access-group        Access list to be applied
  description         Enter a description
  exit                Exit identity policy configuration submode
  inactivity-timer    Inactivity timeout value in seconds
  interface-template  Interface template to be applied
  linksec             Configure link security parameters
  no                  Negate a command or set its defaults
  redirect            Redirect clients to a particular location
  service-policy      Configure service policy
  sgt                 SGT tag
  tag                 tag name
  tunnel              tunnel for wired client access
  vlan                Vlan to be applied
  voice               Voice feature
  <cr>

switch(config-service-template)#
```

- Can be defined locally on the switch
- Can also be defined on the RADIUS server and downloaded dynamically as needed per authorisation or during CoA (ISE 1.2 Feature)
- Used as one of the Actions per Control-Policy or as part of the RADIUS Authorisation (AV Pair)
- Templates via AAA can contain arbitrary AV Pairs

# Applying a Template

- Similar to Applying a Port ACL via *filter-id*

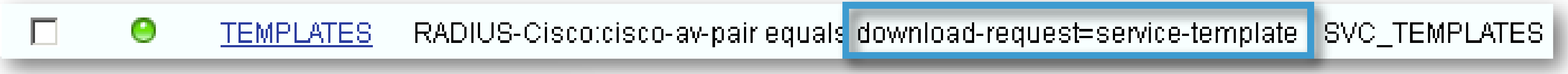


<u>DEFINED ON SWITCH</u>

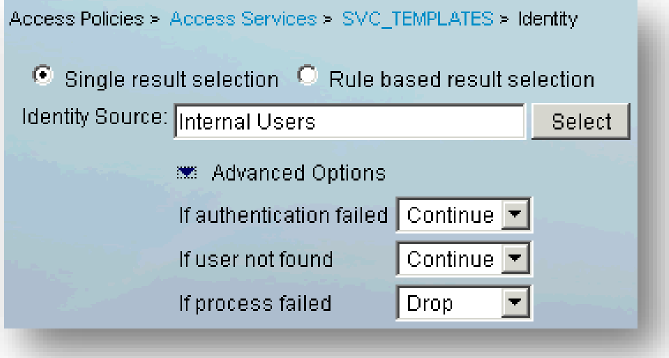
```
service-template TEMPLATE
  access-group PERMIT-ANY
  vlan 100
  inactivity-timer 360
```

- Can also be triggered via RADIUS CoA
- Service-Templates activation can be a local Control Policy action
- If it doesn’t exist, it can be downloaded like an dACL

# Service Template Download from AAA



| □ | ● | TEMPLATES | RADIUS-Cisco:cisco-av-pair equals | download-request=service-template | SVC_TEMPLATES |
|---|---|---|---|---|---|



Access Policies > Access Services > SVC_TEMPLATES > Identity

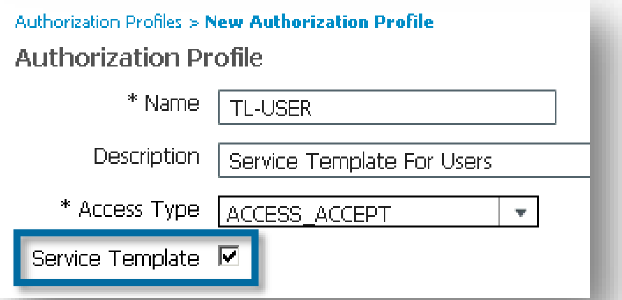
● Single result selection ○ Rule based result selection

| | | |
|---|---|---|
| Identity Source: | Internal Users | Select |

Advanced Options

| | |
|---|---|
| If authentication failed | Continue |
| If user not found | Continue |
| If process failed | Drop |

ACS



Authorization Profiles > **New Authorization Profile**

Authorization Profile

| | |
|---|---|
| * Name | TL-USER |
| Description | Service Template For Users |
| * Access Type | ACCESS_ACCEPT |
| Service Template | ☑ |

ISE

## ACS / any RADIUS Server

- Incoming request tagged with *cisco-av-pair="download-request=service-template"*
- Template-Name = Username
- Trivially Pass Authentication (username is the template name)
- Template Content is defined by AV pairs returned in authorisation rules

## ISE 1.2 and newer

- Template support is built-in

# Interface Templates

## Interface configuration container

NEW

15.2(2)E / 3.6.0E

```
Switch(config)#template Corp-Default-Access
Switch(config-template)#?
Template configuration commands:
  aaa               Authentication, Authorization and Accounting.
  access-session    Access Session specific Interface Configuration Commands
  authentication    Auth Manager Interface Configuration Commands
  carrier-delay     Specify delay for interface transitions
  dampening         Enable event dampening
  default           Set a command to its defaults
  description       Interface specific description
  dot1x             Interface Config Commands for IEEE 802.1X
  exit              Exit from template configuration mode
  hold-queue        Set hold queue depth
  ip                IP template config
  keepalive         Enable keepalive
  load-interval     Specify interval for load calculation for an interface
  mab               MAC Authentication Bypass Interface Config Commands
  mls               mls interface commands
  no                Negate a command or set its defaults
  peer              Peer parameters for point to point interfaces
  priority-queue    Priority Queue
  queue-set         Choose a queue set for this queue
  radius-server     Modify RADIUS query parameters
  service-policy    Configure CPL Service Policy
  source            Get config from another source
  spanning-tree     Spanning Tree Subsystem
  srr-queue         Configure shaped round-robin transmit queues
  storm-control     storm configuration
  subscriber        Subscriber inactivity timeout value.
  switchport        Set switching mode characteristics
```

- Interface level commands available for templates in 15.2(2)E / 3.6.0.E
- Only these commands can be used in Interface Templates
- Other interface level commands configured “the usual” way

# Interface Template Example

## Define and Source templates

```
template Corp-Default-Access
 dot1x pae authenticator
 spanning-tree portfast
 switchport access vlan 100
 switchport mode access
 mab
 access-session port-control auto
 service-policy type control subscriber ACCESS-POLICY
```

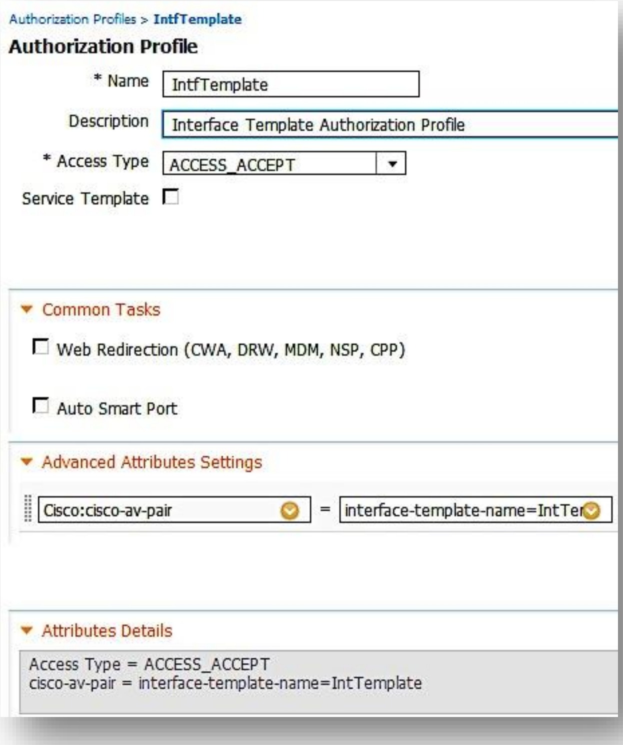
```
interface GigabitEthernet0/1
 source template Corp-Default-Access
!
interface GigabitEthernet0/2
 source template Corp-Default-Access
!
interface GigabitEthernet0/3
 source template Corp-Default-Access
!
.
.
interface GigabitEthernet0/46
 source template Corp-Default-Access
!
```

- All interface level configuration can be contained within the interface template
- The template can be applied on to the physical ports with "source template" interface config command
- Running configuration doesn't show all interface configs, use "show derived-config" exec command

```
Switch#show derived-config interface Gi 0/1
Building configuration...

Derived configuration : 234 bytes
!
interface GigabitEthernet0/1
 switchport access vlan 100
 switchport mode access
 access-session port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber ACCESS-POLICY
```

# Interface-Template Authorisation from RADIUS

“cisco-av-pair = interface-template-name=<template>”



Authorization Profiles > **IntfTemplate**

**Authorization Profile**

| | |
|---|---|
| * Name | IntfTemplate |
| Description | Interface Template Authorization Profile |
| * Access Type | ACCESS_ACCEPT |
| Service Template | □ |

▾ Common Tasks

□ Web Redirection (CWA, DRW, MDM, NSP, CPP)

□ Auto Smart Port

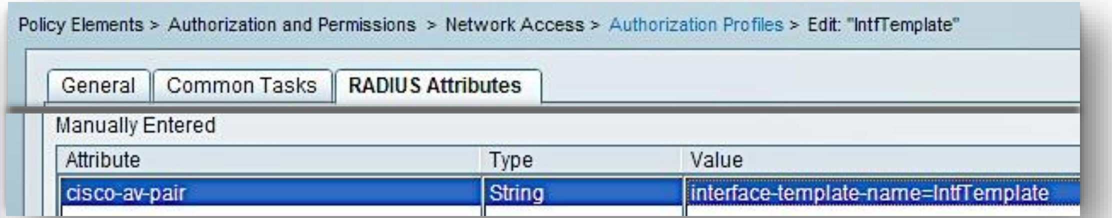
▾ Advanced Attributes Settings

Cisco:cisco-av-pair = interface-template-name=IntTe

▾ Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=IntTemplate

ISE



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "IntfTemplate"

Manually Entered

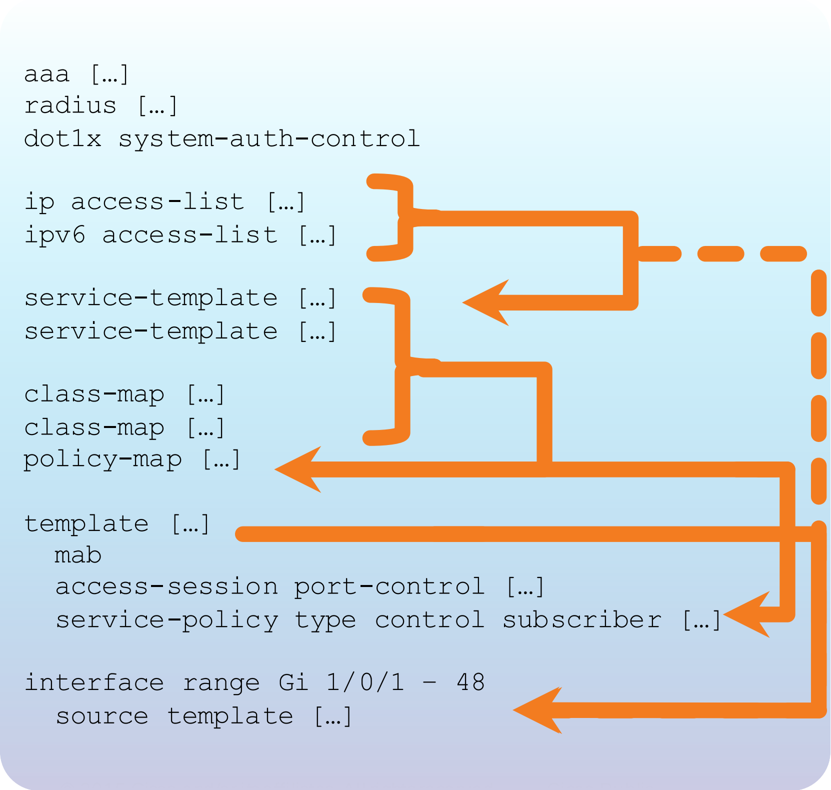
| Attribute | Type | Value |
|---|---|---|
| cisco-av-pair | String | interface-template-name=IntfTemplate |

ACS

- The template must be configured locally on the switch
- Works similar to “Filter-ID” RADIUS attribute for authorising set of interface commands for a session
- On session termination, the interface configuration reset to static template sourced on the interface

# Putting the Pieces Together

- Policy Configuration Elements



```
aaa […]
radius […]
dot1x system-auth-control

ip access-list […]
ipv6 access-list […]

service-template […]
service-template […]

class-map […]
class-map […]
policy-map […]

template […]
  mab
  access-session port-control […]
  service-policy type control subscriber […]

interface range Gi 1/0/1 - 48
  source template […]
```

- Global Configuration (AAA,802.1X, CoA, ACLs, etc.)
- Service Template Configuration (optional)
- Global Policy Configuration (policy-map referencing class-maps)
- Interface-template Configuration
- Per-Interface Configuration
- References to other Policy Elements (static or dynamic)

# Legacy Configuration to New-style Mode

**Typical Identity Configuration (today)**

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 ip access-group IPV4-PRE-AUTH-ACL in
 authentication control-direction in
 authentication event fail action authorize vlan 100
 authentication event server dead action authorize vlan 100
 authentication event no-response action authorize vlan 100
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server dynamic
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
```

```
switch# authentication display new-style
```

**New Policy mode**

```
interface GigabitEthernet1/0/1
 ....
 access-session port-control auto
 access-session host-mode single-host
 service-policy type control subscriber POLICY_Gi1/0/1
 ....
!
policy-map type control subscriber POLICY_Gi1/0/1
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
....
!
class-map type control subscriber match-all DOT1X
 match method dot1x
class-map type control subscriber match-all MAB
 match method mab
....
```

# Configuration Mode Display

- Bridging the Gap between ‘Old World’ and ‘New World’

**Tip:** Start with known good configuration and see how changes in ‘legacy mode’ change the new configuration!

- Existing configurations ‘simply work’
- Converting in the background to new Policy Mode
- Use CLI to change how configuration is shown:

```
– switch# authentication display ?
–   legacy      Legacy configuration
–   new-style   New style (c3pl) configuration
```

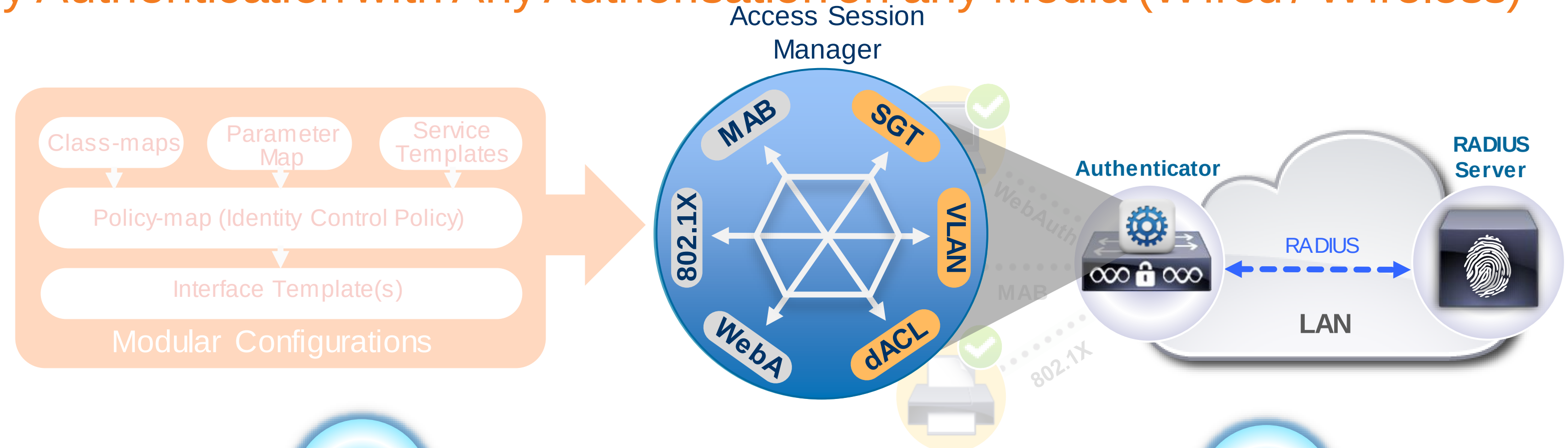
- If Policy Mode configuration is changed or rebooted in Policy Mode, the change is non-reversible
- No IPv6 capable WebAuth in Old Style Mode
- **This is transient and ‘Exec mode’ only (does not appear in configuration).**

# IBNS 2.0 Features

# IBNS 2.0 Features

*From 15.2(1)E / 03.05.00E*
*C3850/C3650 FCS*
*15.2(1)SY on C6500*
*03.06.00E on Sup8E*

## Any Authentication with Any Authorisation on any Media (Wired / Wireless)



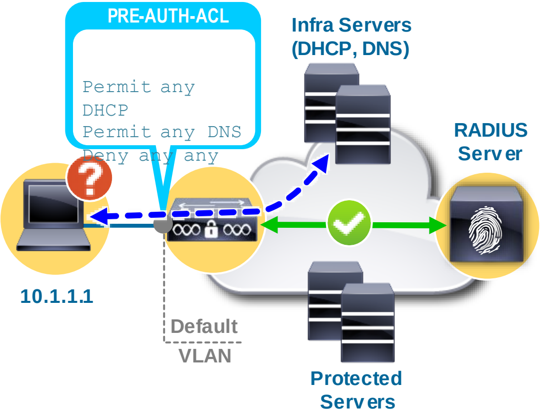
### IBNS 2.0 Features

- Critical ACL
- Intelligent Aging
- Concurrent Authentication
- Enhanced CoA
- Critical MAB
- Common Session-ID
- Differentiated Authentication
- IPv6 WebAuth
- AuthZ templates
- IPv6 Identity
- Template based NEAT

# Critical ACL

## Scenarios today with Low Impact Mode:

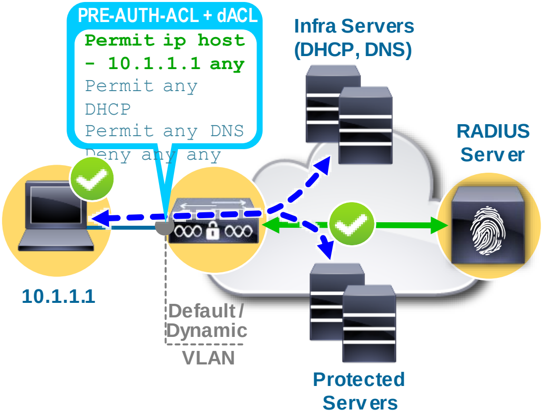
### Before Authentication



```
PRE-AUTH-ACL
Permit any
DHCP
Permit any DNS
Deny any any
```

Before authentication success, the endpoint has limited access to the network resources, defined by the PRE-AUTH-ACL on the port

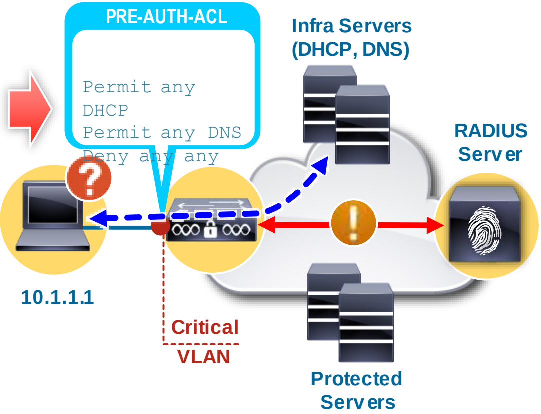
### Authentication Success



```
PRE-AUTH-ACL + dACL
Permit ip host
- 10.1.1.1 any
Permit any
DHCP
Permit any DNS
Deny any any
```

On authentication success, the RADIUS server authorises the endpoint with a dACL **(permit ip any any)** granting full access

### AAA Server Unreachable



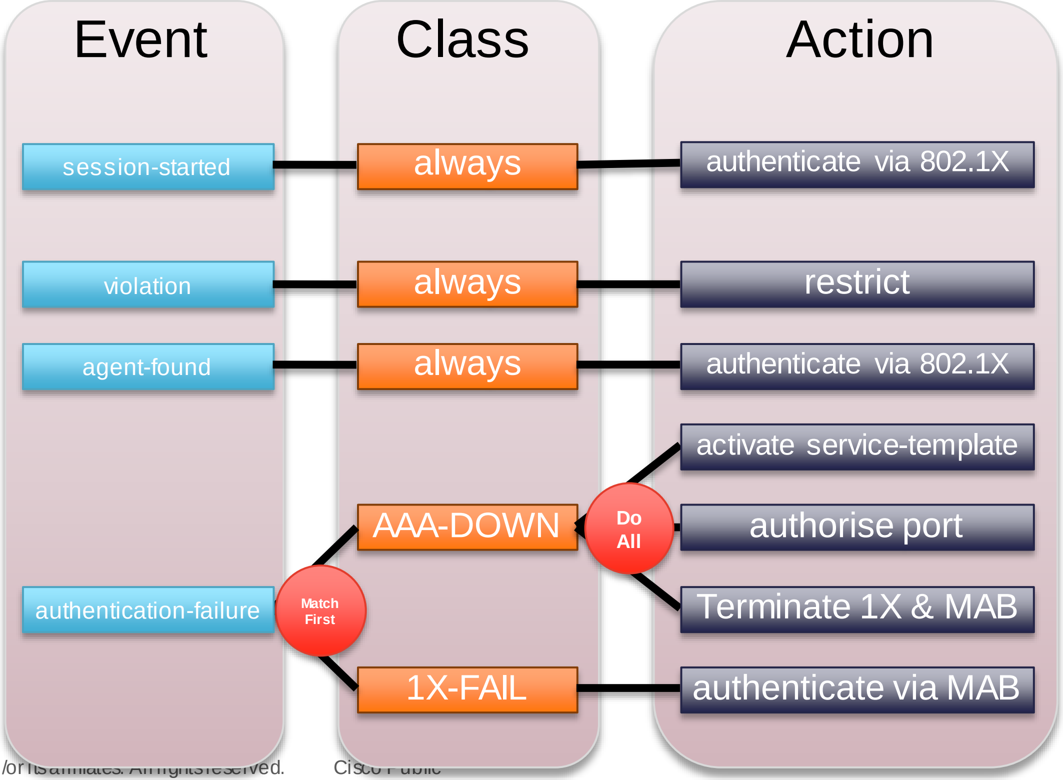
```
PRE-AUTH-ACL
Permit any
DHCP
Permit any DNS
Deny any any
```

The endpoint may be authorised to a critical VLAN, but the PRE-AUTH-ACL on the port would still block the access during AAA outage*

*** Critical authorisation wont apply to endpoints that were authorised by AAA server when it was reachable**

# Critical ACL

## Configuration Example



Event

Class

Action

session-started

always

authenticate via 802.1X

violation

always

restrict

agent-found

always

authenticate via 802.1X

authentication-failure

Match First

AAA-DOWN

Do All

activate service-template

authorise port

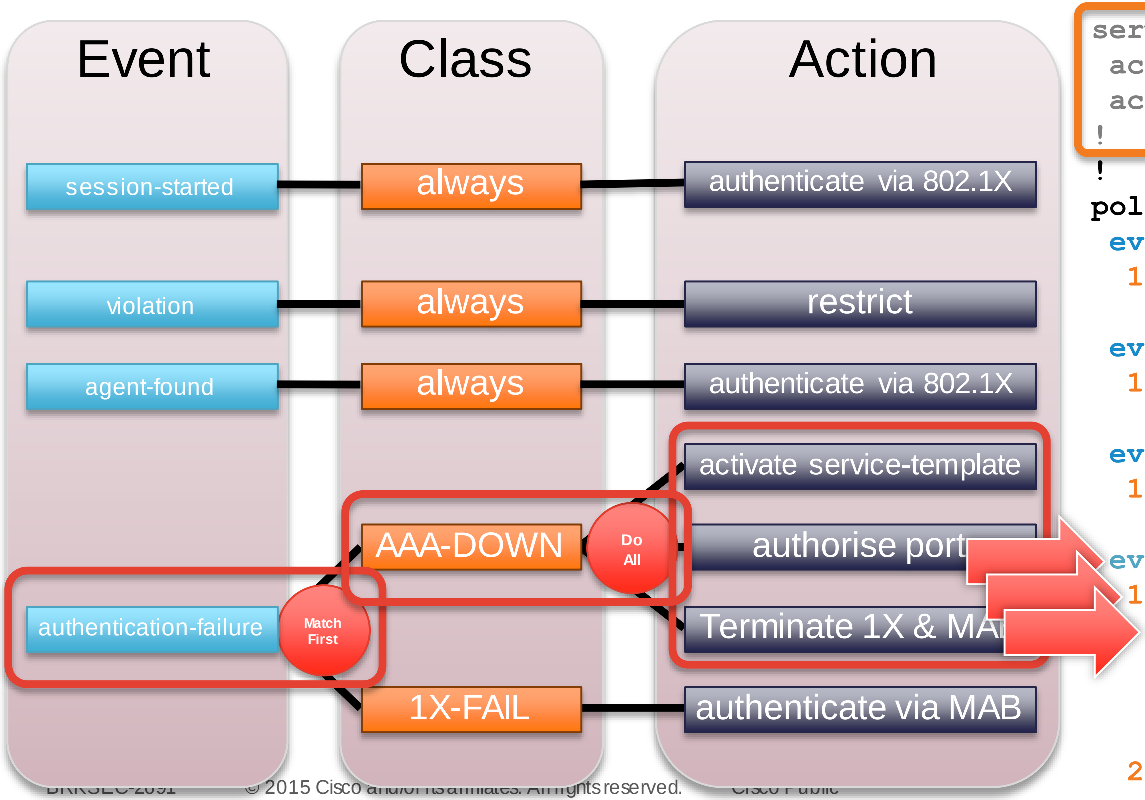
Terminate 1X & MAB

1X-FAIL

authenticate via MAB

# Critical ACL

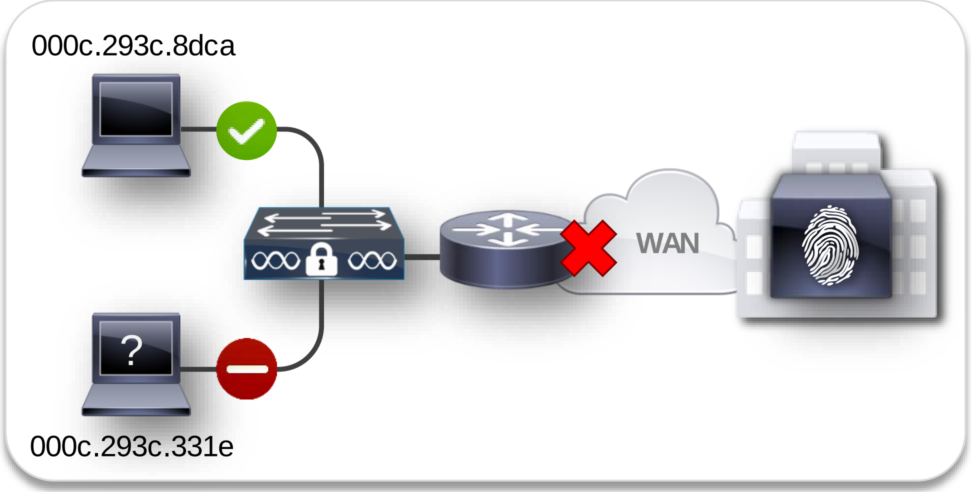
## Configuration Example



```
service-template CRITICAL
 access-group CRITICAL-V4
 access-group CRITICAL-V6
!
!
policy-map type control subscriber DOT1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
 event violation match-all
  10 class always do-all
   10 restrict
 event agent-found match-all
  10 class always do-all
   10 authenticate using dot1x
 event authentication-failure match-first
  10 class AAA-DOWN do-all
   10 activate service-template CRITICAL
   20 authorize
   30 terminate dot1x
   40 terminate mab
  20 class 1X-FAIL do-all
   10 authenticate using mab
```

# Critical MAB

## Local Authentication during Server failure



```
username 000c293c8dca password 0 000c293c8dca
username 000c293c8dca aaa attribute list mab-local
!
aaa local authentication default authorization mab-local
aaa authorization credential-download mab-local local
!
aaa attribute list mab-local
 attribute type tunnel-medium-type all-802
 attribute type tunnel-private-group-id "150"
 attribute type tunnel-type vlan
 attribute type inacl "CRITICAL-V4"
!
policy-map type control subscriber ACCESS-POL
...
event authentication-failure match-first
 10 class AAA_SVR_DOWN_UNAUTHD_HOST do-↵
          until-failure
  10 terminate mab
  20 terminate dot1x
  30 authenticate using mab aaa authc-↵
     list mab-local authz-list mab-local
...
```

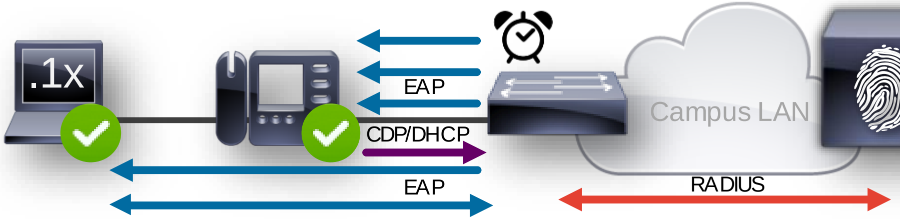
- Additional level of check to authorise hosts during a critical condition.
- EEM Scripts could be used for dynamic update of whitelist MAC addresses
- Sessions re-initialise once the server connectivity resumes.

# Concurrent Authentication

## Faster on-boarding of endpoints in to the network

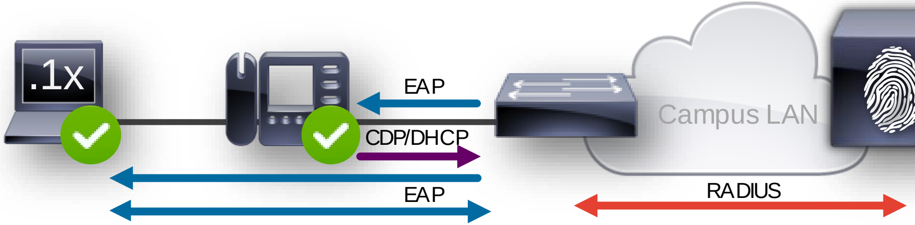
### Sequential Authentication

```
authentication order dot1x mab
```



### Concurrent Authentication

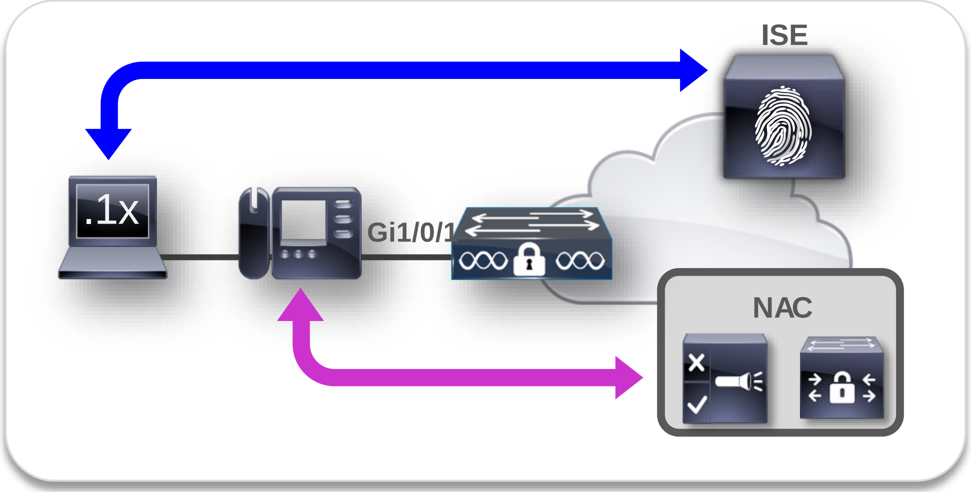
```
event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using mab priority 20
```



- Faster on-boarding, good for delay sensitive endpoints.
- An endpoint may be authenticated by both methods, but priority determines the ultimate authorisation.
- *Additional load to RADIUS Server. Multiple Authentication requests hit the server for same client*

# Differentiated Authentication

## Authenticate different methods with different Servers



```
aaa group server radius mab-servers
 server name ise01
!
aaa group server radius 1x-servers
 server name ise02
!
aaa authentication dot1x 1x-servers group 1x-servers
aaa authentication dot1x mab-servers group mab-servers
!
aaa authorization network 1x-servers group 1x-servers
aaa authorization network mab-servers group mab-servers
!
radius server ise02
 address ipv4 172.20.254.8 auth-port 1645 acct-port 1646
 key xxxxxx
!
radius server ise01
 address ipv4 172.20.254.4 auth-port 1645 acct-port 1646
 key xxxxxx
```

```
policy-map type control subscriber ent-access-pol
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x aaa authc-list 1x-servers authz-list
1x-servers
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab aaa authc-list mab-servers authz-list
mab-servers
......
```

**Requirement:** Authenticate 802,1X end-points with new RADIUS Server (ISE) and authenticate non-802.1X (MAB) devices with legacy NAC infra

# Intelligent Aging

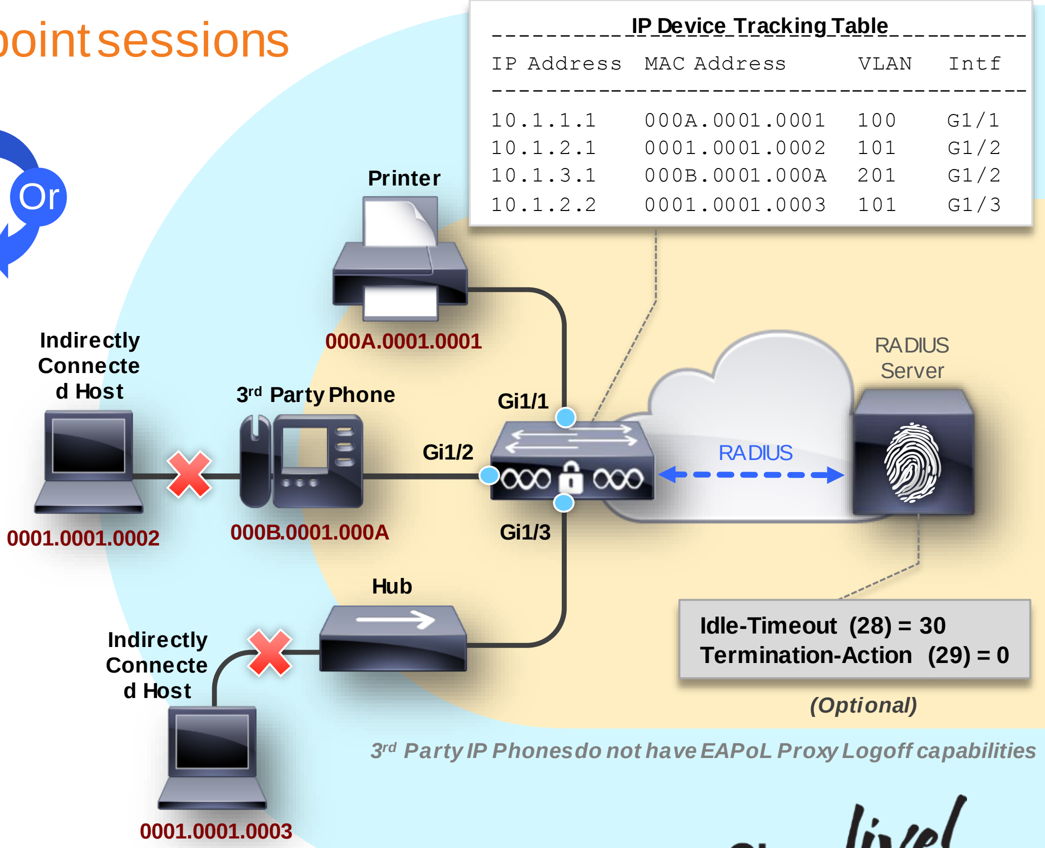
## Disconnect Indirectly connected endpoint sessions

```
Switch(config-if)subscriber aging
inactivity-timer 30 probe
```

Or

```
service-template IA-TIMER
inactivity-timer 60 probe
!
policy-map type control sub ACCESS-POL
...
event authentication-success match-all
 10 class always do-until-failure
  10 activate service-template IA-TIMER
event inactivity-timeout match-all
 10 class always do-until-failure
  10 unauthorise
...
```

IBNS 2.0 enhances ‘inactivity timer’ with ARP probes to ensure that an endpoint is indeed disconnected. ARP probes are sent based on ‘ip device tracking table’ data.



```
                    IP Device Tracking Table
----------------------------------------------------------
IP Address   MAC Address          VLAN    Intf
----------------------------------------------------------
10.1.1.1     000A.0001.0001       100     G1/1
10.1.2.1     0001.0001.0002       101     G1/2
10.1.3.1     000B.0001.000A       201     G1/2
10.1.2.2     0001.0001.0003       101     G1/3
```

Idle-Timeout (28) = 30
Termination-Action (29) = 0

*3rd Party IP Phones do not have EAPoL Proxy Logoff capabilities*

* Only on the next-gen platforms (C3650, C3850) only today

# IPv6 Identity*

## With Identity-Policy, both IPv4 & IPv6 endpoints can be securely on-boarded in a consistent manor

```
!
ipv6 snooping policy v6-snoop
 trusted-port
!
vlan configuration 100-180
 ipv6 nd suppress
 ipv6 snooping
!
interface TenGig1/1/1
 description *** Uplink ***
 [ ... ]
 ipv6 snooping attach-policy v6-snoop
!
```

- Enable IPv6 Device Tracking
- Make Identity Policy IPv6 aware
- Note: Define which VLANs to apply and also trust the uplink port

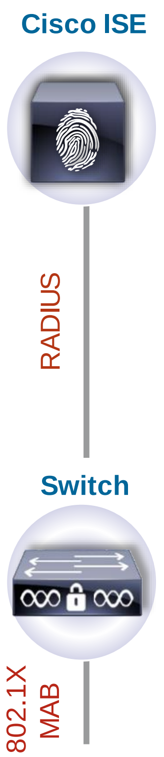
```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 access-session port-control auto
 ipv6 traffic-filter IPV6-PRE-AUTH-ACL in
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber ACCESS-POL
!
service-template CRITICAL
   description allow all traffic
   access-group PERMIT-IPV4-ANY
   access-group PERMIT-IPV6-ANY
!
```

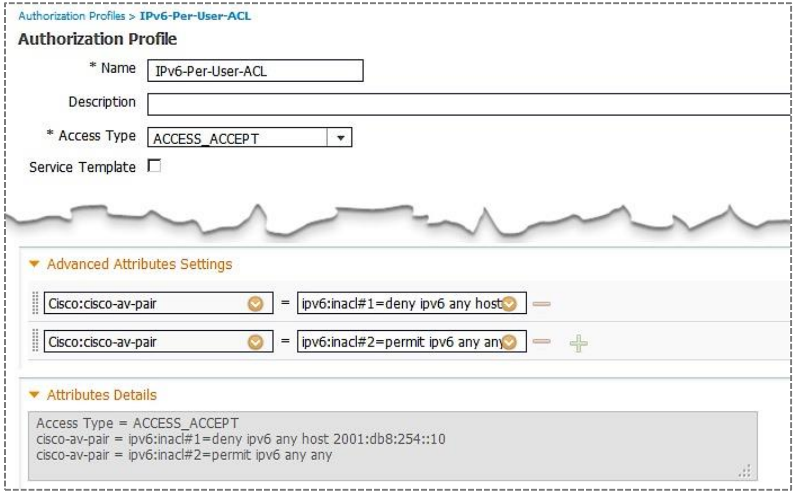
- IPv6 Pre-auth-acl limits IPv6 traffic prior to authentication
- Same identity control policy apply for both IPv4 & IPv6 clients
- Service-template provisions for IPv6 ACL for Post-Auth / Critical authorisation purposes.

# Low-Impact Mode with Per-User-ACL

Currently Supported only on Cisco Catalyst 3650 and 3850 Switches

- Centralised Deployment, ACL hosted on the AAA Server
- No. of ACE limited by RADIUS packet size (4000 char)





Authorization Profiles > IPv6-Per-User-ACL

**Authorization Profile**

| | |
|---|---|
| * Name | IPv6-Per-User-ACL |
| Description | |
| * Access Type | ACCESS_ACCEPT |
| Service Template | □ |

▼ Advanced Attributes Settings

| | | |
|---|---|---|
| Cisco:cisco-av-pair | = | ipv6:inacl#1=deny ipv6 any host |
| Cisco:cisco-av-pair | = | ipv6:inacl#2=permit ipv6 any any |

▼ Attributes Details

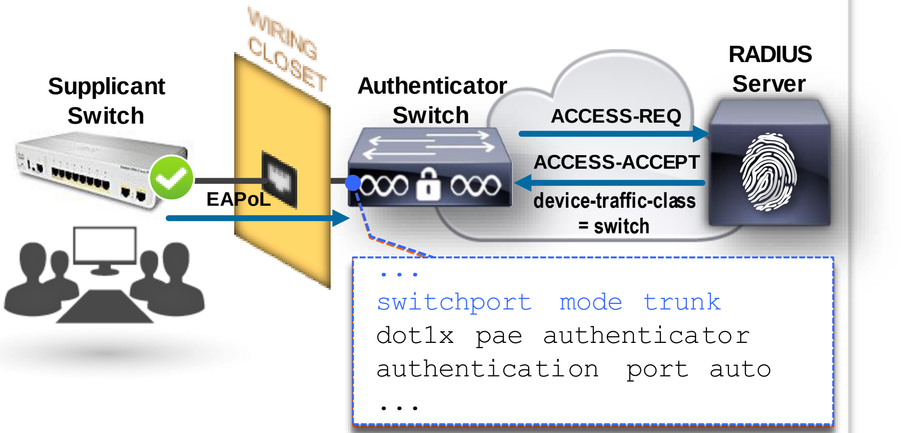
```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ipv6:inacl#1=deny ipv6 any host 2001:db8:254::10
cisco-av-pair = ipv6:inacl#2=permit ipv6 any any
```

```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
authentication host-mode multi-auth
authentication open
authentication port-control auto
ipv6 traffic-filter IPV6-PRE-AUTH-ACL in
mab
dot1x pae authenticator
dot1x timeout tx-period 5
```

```
Switch#show auth sessions interface gigabitEthernet 1/0/1 details
            Interface:  GigabitEthernet1/0/1
               IIF-ID:  0x103F700000000C2
          MAC Address:  000c.2998.13c8
         IPv6 Address:  FE80::7D2E:FC23:9230:B590,
2001:DB8:100:0:EC8F:8D64:33D2:213D
         IPv4 Address:  Unknown
            User-Name:  employee1@ibns.lab
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  AC14FE6500000FAD029BD96A
      Acct Session ID:  0x00000FA3
               Handle:  0x5F000002
       Current Policy:  POLICY_Gi1/0/1

Server Policies:
         Per-User ACL:  GigabitEthernet1/0/1#v6#37F2F598
                     :  deny ipv6 any host 2001:db8:254::10
                     :  permit ipv6 any any

Method status list:

       Method           State
       dot1x            Authc Success
```

# NEAT with Interface Template

## NEAT with Macro

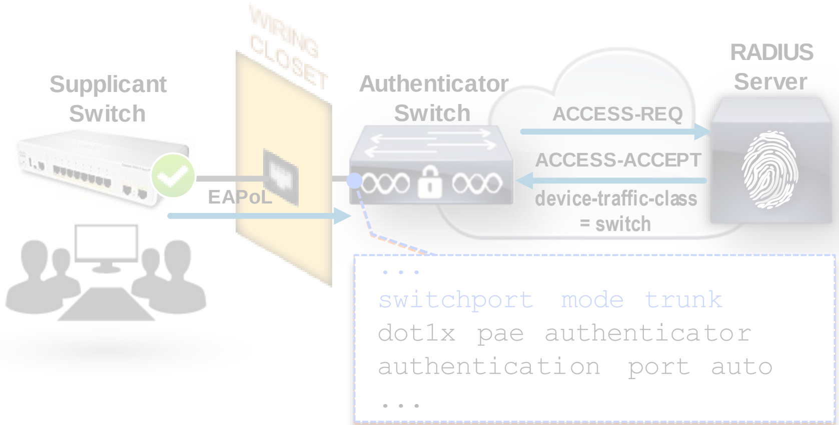


```
...
switchport mode trunk
dot1x pae authenticator
authentication port auto
...
```

Upon successful ‘Supplicant Switch’ authentication, the ‘Authenticator Switch’ applies a built-in Macro to change the interface (running) configuration from access to trunk

# NEAT with Interface Template

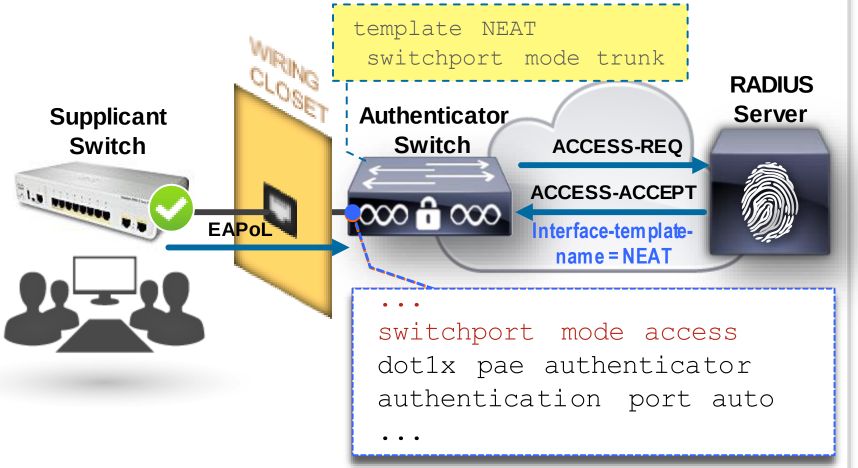
## NEAT with Macro



```
...
switchport mode trunk
dot1x pae authenticator
authentication port auto
...
```

Upon successful ‘Supplicant Switch’ authentication, the ‘Authenticator Switch’ applies a built-in Macro to change the interface (running) configuration from access to trunk

## NEAT with Template



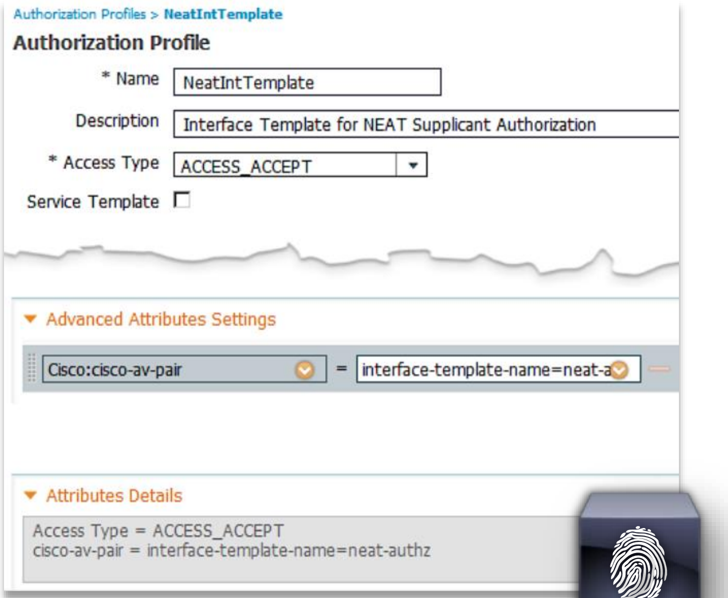
```
template NEAT
 switchport mode trunk
```

```
...
switchport mode access
dot1x pae authenticator
authentication port auto
...
```

Same output as the ‘Macro based NEAT’, but the interface running configuration remains intact, while the (runtime) ‘derived configuration’ changes from access to trunk

# NEAT with Interface Template

```
cisp enable
!
template neat-authz
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 254
 switchport mode trunk
```



Authorization Profiles > NeatIntTemplate

**Authorization Profile**

* Name: NeatIntTemplate

Description: Interface Template for NEAT Supplicant Authorization

* Access Type: ACCESS_ACCEPT

Service Template: □

▾ Advanced Attributes Settings

Cisco:cisco-av-pair = interface-template-name=neat-a

▾ Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=neat-authz

## Before SSw Authentication

```
ASw#show running-config int Gi0/12
Building configuration...

Derived configuration : 179 bytes
!
interface GigabitEthernet0/12
 description ** To SSw 0/12 **
 switchport access vlan 254
 switchport mode access
 dot1x pae authenticator
 spanning-tree portfast
!
ASw#show derived-config int Gi0/12
Building configuration...

Derived configuration : 179 bytes
!
interface GigabitEthernet0/12
 description ** To SSw 0/12 **
 switchport access vlan 254
 switchport mode access
 dot1x pae authenticator
 spanning-tree portfast
!
```

## After SSw Authentication

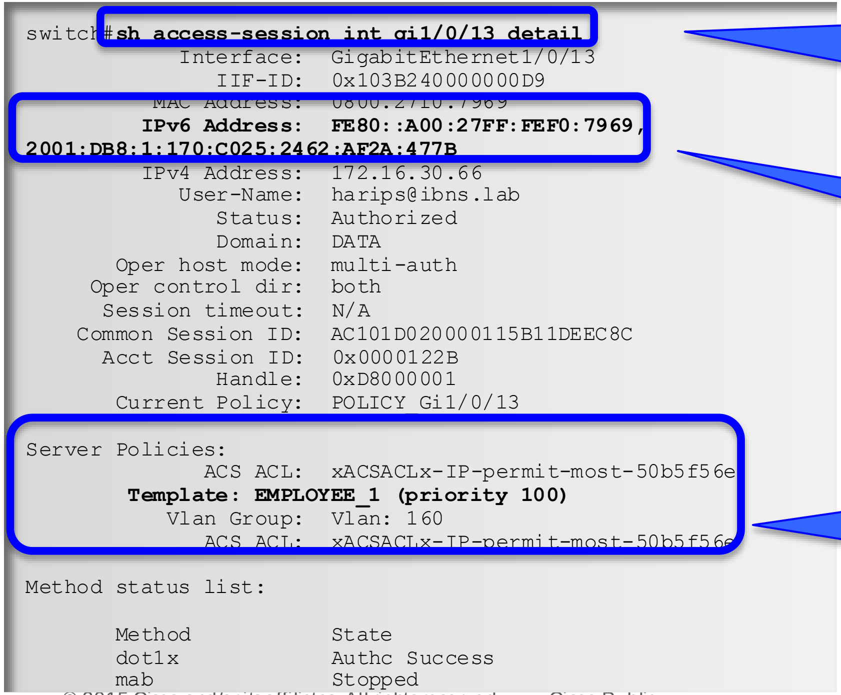
```
ASw#show running-config int Gi0/12
Building configuration...

Derived configuration : 179 bytes
!
interface GigabitEthernet0/12
 description ** To SSw 0/12 **
 switchport access vlan 254
 switchport mode access
 dot1x pae authenticator
 spanning-tree portfast
!
ASw#show derived-config int Gi0/12
Building configuration...

Derived configuration : 240 bytes
!
interface GigabitEthernet0/12
 description ** To SSw 0/12 **
 switchport access vlan 254
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 254
 switchport mode trunk
 dot1x pae authenticator
 spanning-tree portfast
!
```

# Troubleshooting IBNS 2.0

# Troubleshooting Control Policy

- New Session Display

Old Friends with new Names:



```
switch#sh access-session int gi1/0/13 detail
            Interface:  GigabitEthernet1/0/13
               IIF-ID:  0x103B240000000D9
          MAC Address:  0800.27F0.7969
         IPv6 Address:  FE80::A00:27FF:FEF0:7969,
2001:DB8:1:170:C025:2462:AF2A:477B
         IPv4 Address:  172.16.30.66
            User-Name:  harips@ibns.lab
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  AC101D020000115B11DEEC8C
      Acct Session ID:  0x0000122B
               Handle:  0xD8000001
       Current Policy:  POLICY_Gi1/0/13

Server Policies:
              ACS ACL:  xACSACLx-IP-permit-most-50b5f56e
        Template: EMPLOYEE_1 (priority 100)
           Vlan Group:  Vlan: 160
              ACS ACL:  xACSACLx-IP-permit-most-50b5f56e

Method status list:

       Method           State
       dot1x            Authc Success
       mab              Stopped
```

‘show access-session’ instead of ‘show authentication session’

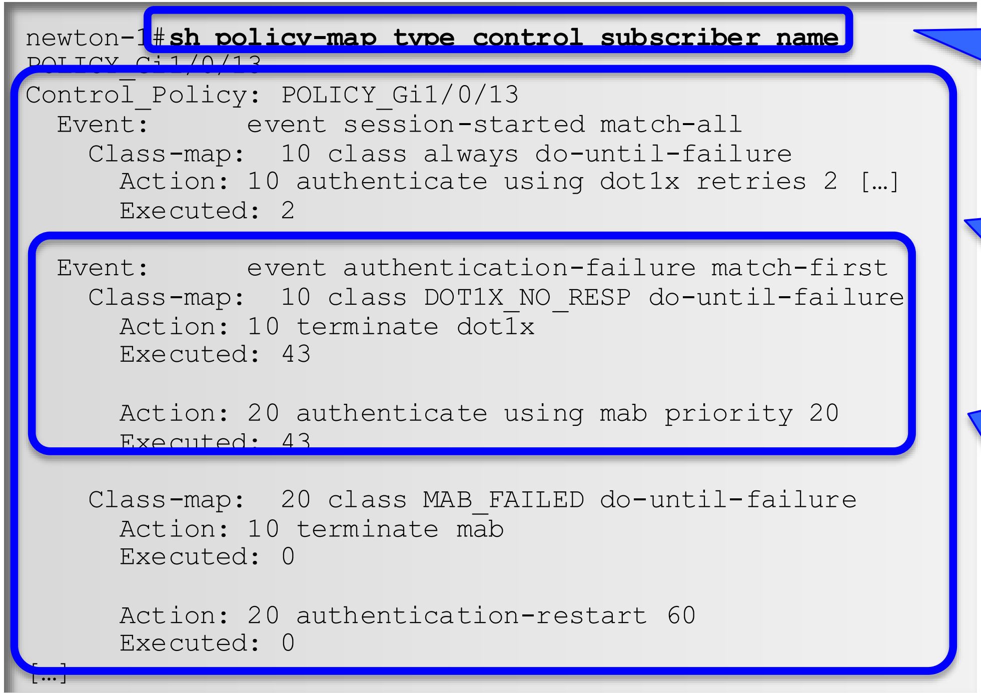
IPv6 awareness

Applied Policies (here: with server assigned Template)

# Troubleshooting Control Policy

- (cont.)

And new Friends:



```
newton-1#sh policy-map type control subscriber name
POLICY_Gi1/0/13
Control_Policy: POLICY_Gi1/0/13
  Event:      event session-started match-all
    Class-map:  10 class always do-until-failure
      Action: 10 authenticate using dot1x retries 2 […]
      Executed: 2

  Event:      event authentication-failure match-first
    Class-map:  10 class DOT1X_NO_RESP do-until-failure
      Action: 10 terminate dot1x
      Executed: 43

      Action: 20 authenticate using mab priority 20
      Executed: 43

    Class-map:  20 class MAB_FAILED do-until-failure
      Action: 10 terminate mab
      Executed: 0

      Action: 20 authentication-restart 60
      Executed: 0
[…]
```

‘show policy-map type control’ to show the control policy

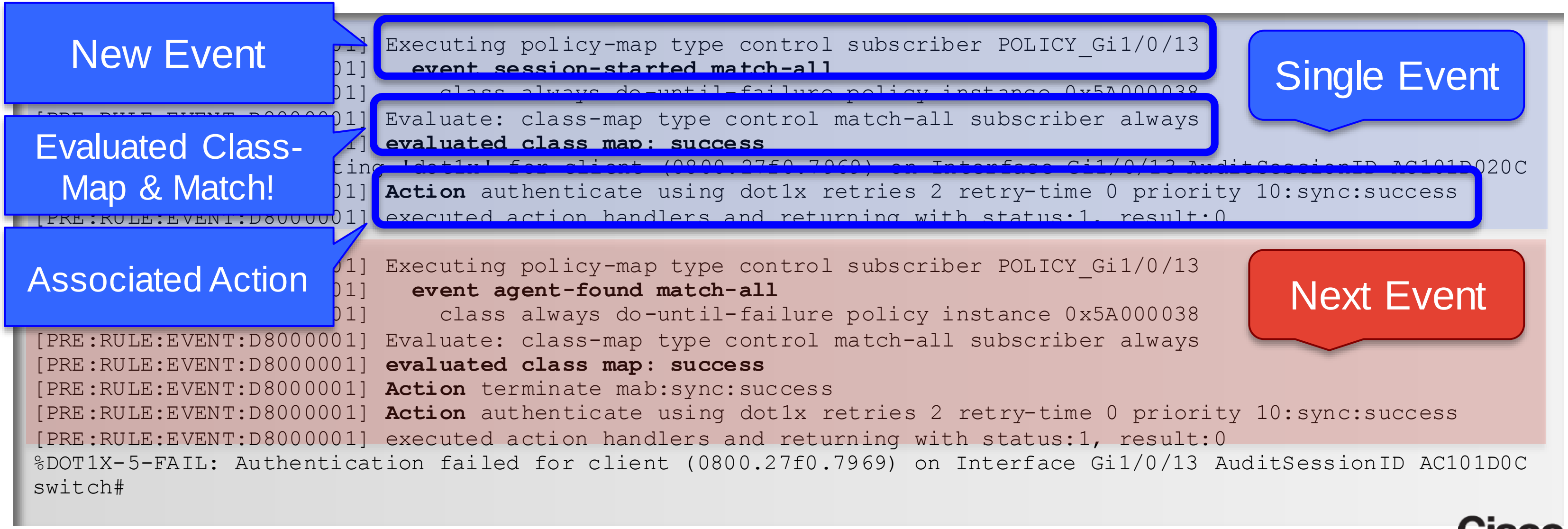
See complete Policy (Events, Classes, Actions)

Look for specific events and how often associated classes matched and actions have been executed

# Troubleshooting Control Policy

- (cont.)

- debug pre* all | error | **event** | ha | prr | **rule**
- To understand policy flow and identify events and actions
- Powerful in combination with conditional debugging (‘debug condition’)



New Event

Evaluated Class-Map & Match!

Associated Action

Single Event

Next Event

```
                          01] Executing policy-map type control subscriber POLICY_Gi1/0/13
                          01]   event session-started match-all
                          01]     class always do-until-failure policy instance 0x5A000038
[PRE:RULE:EVENT:D8000001] Evaluate: class-map type control match-all subscriber always
                          1] evaluated class map: success
                         ting 'dot1x' for client (0800.27f0.7969) on Interface Gi1/0/13 AuditSessionID AC101D020C
                          01] Action authenticate using dot1x retries 2 retry-time 0 priority 10:sync:success
[PRE:RULE:EVENT:D8000001] executed action handlers and returning with status:1, result:0
                          01] Executing policy-map type control subscriber POLICY_Gi1/0/13
                          01]   event agent-found match-all
                          01]     class always do-until-failure policy instance 0x5A000038
[PRE:RULE:EVENT:D8000001] Evaluate: class-map type control match-all subscriber always
[PRE:RULE:EVENT:D8000001] evaluated class map: success
[PRE:RULE:EVENT:D8000001] Action terminate mab:sync:success
[PRE:RULE:EVENT:D8000001] Action authenticate using dot1x retries 2 retry-time 0 priority 10:sync:success
[PRE:RULE:EVENT:D8000001] executed action handlers and returning with status:1, result:0
%DOT1X-5-FAIL: Authentication failed for client (0800.27f0.7969) on Interface Gi1/0/13 AuditSessionID AC101D0C
switch#
```

*PRE = Policy Rule Engine

# Control Log Verbosity

**Suppress ‘Success’ log messages, only log failure**

- `no authentication logging verbose`
- `no mab logging verbose`
- `no dot1x logging verbose`
- Default is ‘verbose’!
- Some ISE troubleshooting tools depends on seeing these messages

**Selectively Debug**

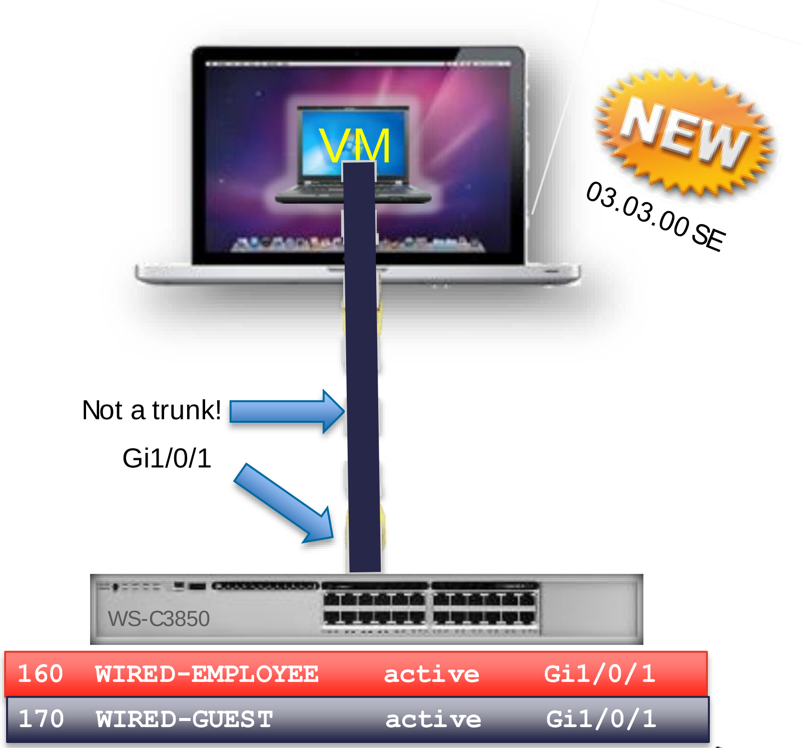
- `debug interface Gi1/0/1`
- Limits effect of debug to given interface

# Additional Things To Know

# Per MAC VLAN Assignment

“MAC based VLANs”

- Before Cat3850 / Cat3650: One port, one VLAN per access port (1:1)
- Exception: Voice (one Data Device untagged, one Voice Device tagged w/ VVLAN)
- Later: Allowing VLAN assignment on multi-authentication ports, but first device ‘rules’ the port.
- **Now with Catalyst 2960X, 3850 & 3650: Each session can have individual VLAN assigned**
  - 2960X → 15.2(2)E
  - C3850 → 03.03.00SE
  - C3650 → 03.03.00SE



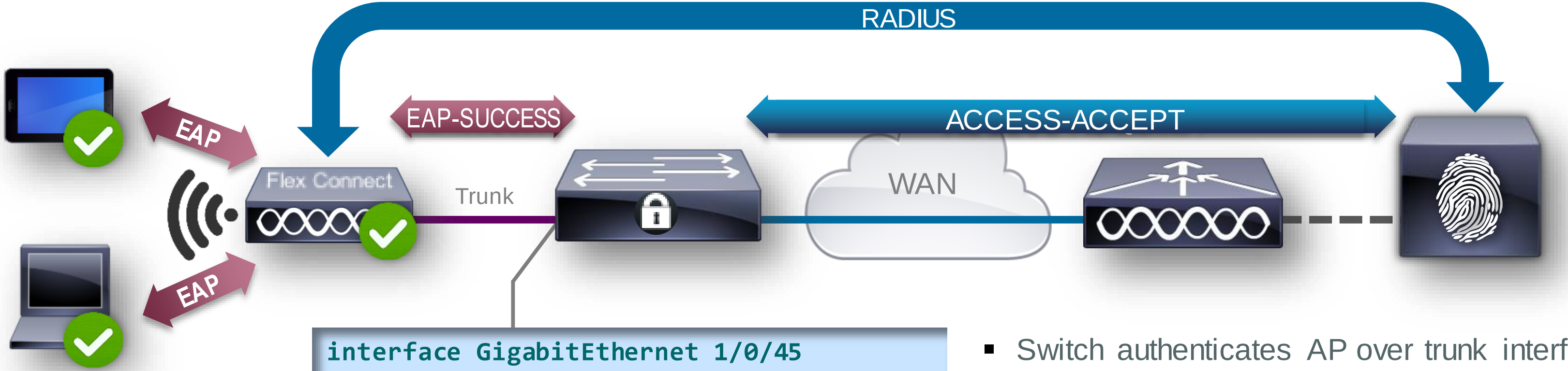
```
160   WIRED-EMPLOYEE      active     Gi1/0/1
170   WIRED-GUEST         active     Gi1/0/1
```

# 802.1X on Trunk Ports

NEW

15.2(1)E / 3.5.0E

Requirement: Authenticate Flex Connect AP over trunk interface and let the AP authenticate the wireless clients.



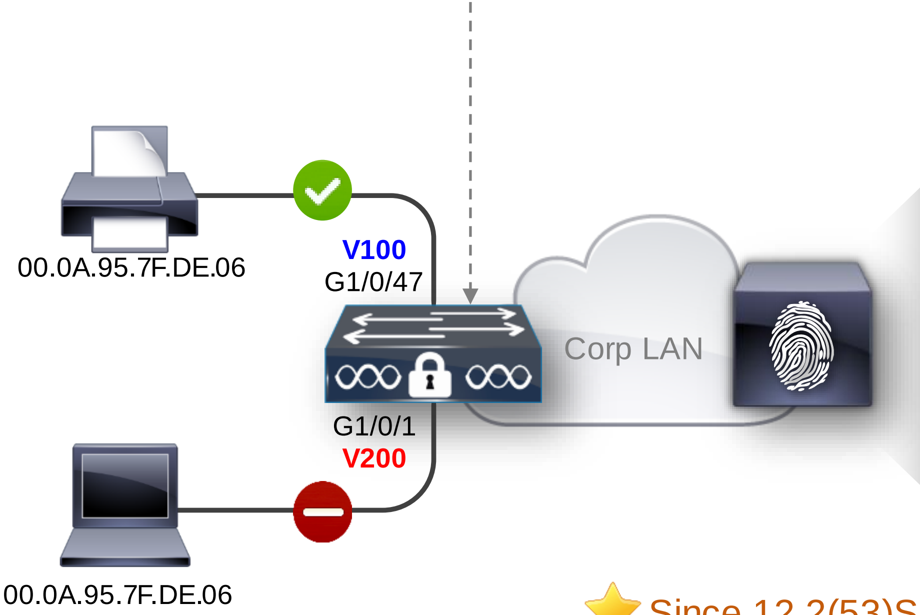
```
interface GigabitEthernet 1/0/45
 switchport mode trunk
 switchport trunk allowed vlan 200-205
 authentication host-mode multi-host
 authentication port-control auto
 dot1x pae authenticator
```

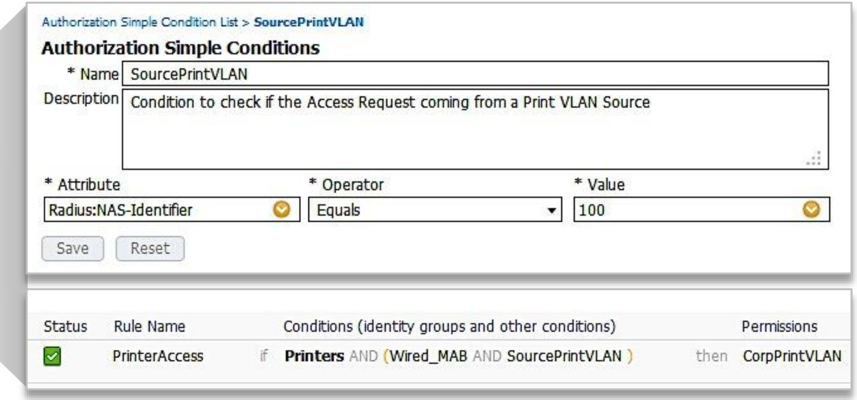
- Switch authenticates AP over trunk interface (802.1X / MAB)
- Flex-AP authenticates endpoints
- Switch accounts only AP MAC address for auth-session, rest allowed without authentication (multi-host mode)

# Ensure Printers Connect on Print Ports Only

```
Switch(config)#mab request format attribute
32 vlan access-vlan
```

Requirement: MAB Requests to printers must come on designated port only.




Authorization Simple Condition List > **SourcePrintVLAN**

**Authorization Simple Conditions**

| | |
|---|---|
| * Name | SourcePrintVLAN |
| Description | Condition to check if the Access Request coming from a Print VLAN Source |

| * Attribute | * Operator | * Value |
|---|---|---|
| Radius:NAS-Identifier | Equals | 100 |

| Status | Rule Name | | Conditions (identity groups and other conditions) | | Permissions |
|---|---|---|---|---|---|
| ☑ | PrinterAccess | if | **Printers** AND (Wired_MAB AND SourcePrintVLAN ) | then | CorpPrintVLAN |

Since 12.2(53)SE2, only for MAB

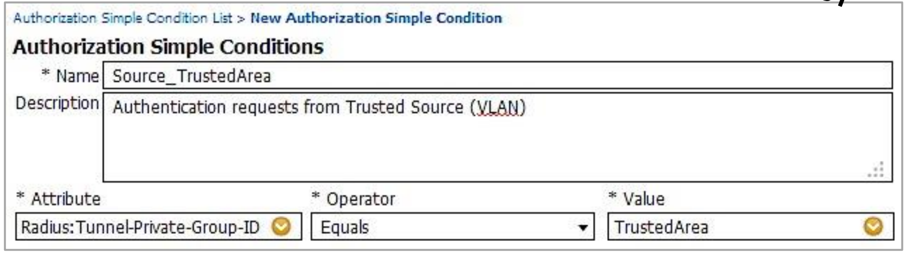
# New Access-session Attribute Feature

## Send source VLAN on the switchport to RADIUS Server

NEW

15.2(2)E / 3.6.0E
15.2(1)SY

```
Switch(config)#access-session attributes filter-list
list custom-name
Switch(config-com-filter-list)#vlan-id
Switch(config-com-filter-list)#exit
Switch(config)#
Switch(config)#access-session authentication
attributes filter-spec include list custom-name
```



Authorization Simple Condition List > **New Authorization Simple Condition**

**Authorization Simple Conditions**

| | |
|---|---|
| * Name | Source_TrustedArea |
| Description | Authentication requests from Trusted Source (VLAN) |

| * Attribute | * Operator | * Value |
|---|---|---|
| Radius:Tunnel-Private-Group-ID | Equals | TrustedArea |

```
*Feb 18 02:52:11.763: RADIUS(00000000): Send Access-Request to 172.20.254.4:1645 id 1645/22, len 442
*Feb 18 02:52:11.763: RADIUS:  authenticator 2D AD 1D 30 E0 63 29 D9 - 90 6C B0 BC 07 BE EB 82
*Feb 18 02:52:11.763: RADIUS:  User-Name           [1]    11   "employee1"
*Feb 18 02:52:11.763: RADIUS:  Service-Type        [6]    6    Framed                   [2]
...
*Feb 18 02:52:11.764: RADIUS:  Tunnel-Private-Group[81]   6    01:"100"
*Feb 18 02:52:11.764: RADIUS:  Tunnel-Type         [64]   6    01:VLAN                  [13]
*Feb 18 02:52:11.765: RADIUS:  Tunnel-Medium-Type  [65]   6    01:ALL_802               [6]
*Feb 18 02:52:11.765: RADIUS:  Tunnel-Private-Group[81]   16   02:"TrustdedArea"
*Feb 18 02:52:11.765: RADIUS:  Tunnel-Type         [64]   6    02:VLAN                  [13]
*Feb 18 02:52:11.765: RADIUS:  Tunnel-Medium-Type  [65]   6    02:ALL_802               [6]
...
```

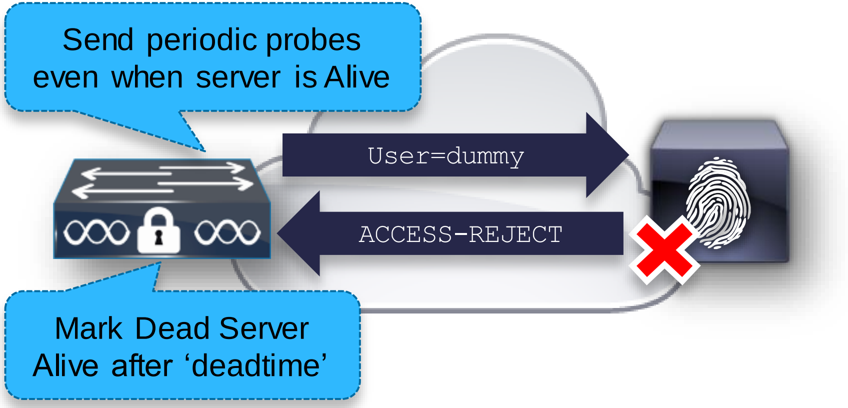
Match on any of these attributes in RADIUS Server

Applies to all authentication methods | System must be in IBNS 2.0 (policy) mode

# RADIUS Probe-on Feature

## Without Probe-on

```
radius server server-01
address ipv4 10.0.1.1 auth-port 1812 acct-port
1813
automate-tester username dummy
!
radius-server deadtime 15
radius-server dead-criteria 3 tries
```



Send periodic probes even when server is Alive

Mark Dead Server Alive after ‘deadtime’

2000 switches sending periodic probes = unnecessary overhead on the RADIUS Server

Want RADIUS server to be marked “ALIVE” only when reachable. Do not want to disturb clients in critical-auth

```
...
%RADIUS-6-SERVERALIVE: Group radius: Radius
server 10.0.1.1:1812,1813 is responding again
(previously dead).
%RADIUS-4-RADIUS_ALIVE: RADIUS server
10.0.1.1:1812,1813 is being marked alive.
...
```

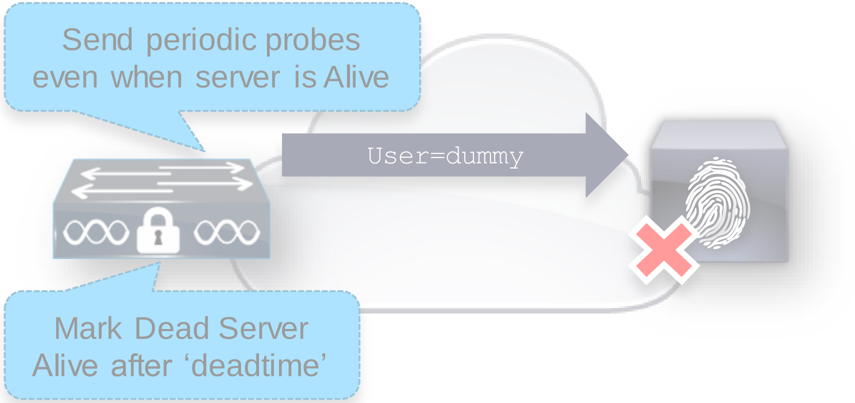
# RADIUS Probe-on Feature

NEW

15.2(2)E / 3.6.0E

## Without Probe-on

```
radius server server-01
address ipv4 10.0.1.1 auth-port 1812 acct-port
1813
automate-tester username dummy
!
radius-server deadtime 15
radius-server dead-criteria 3 tries
```

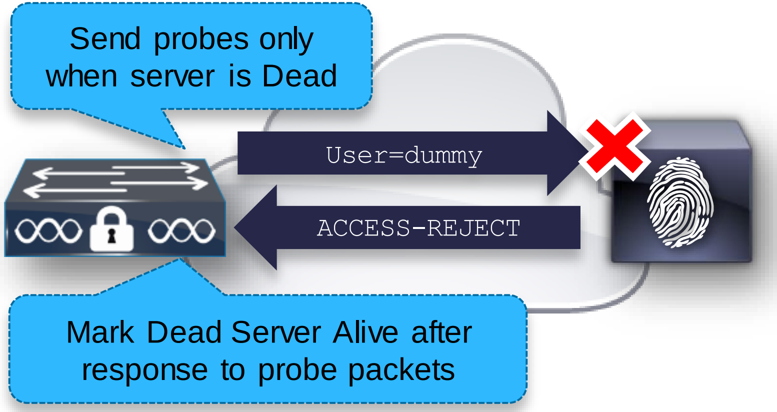


Send periodic probes even when server is Alive

Mark Dead Server Alive after 'deadtime'

## With Probe-on

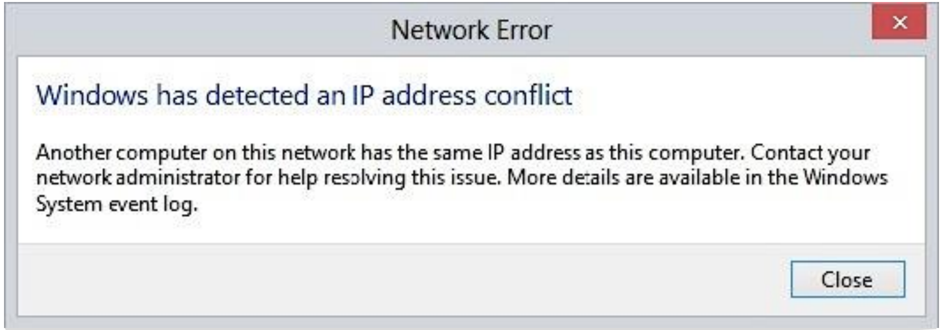
```
radius server server-01
address ipv4 10.0.1.1 auth-port 1812 acct-port 1813
automate-tester username dummy probe-on
!
radius-server deadtime 15
radius-server dead-criteria 3 tries
```



Send probes only when server is Dead

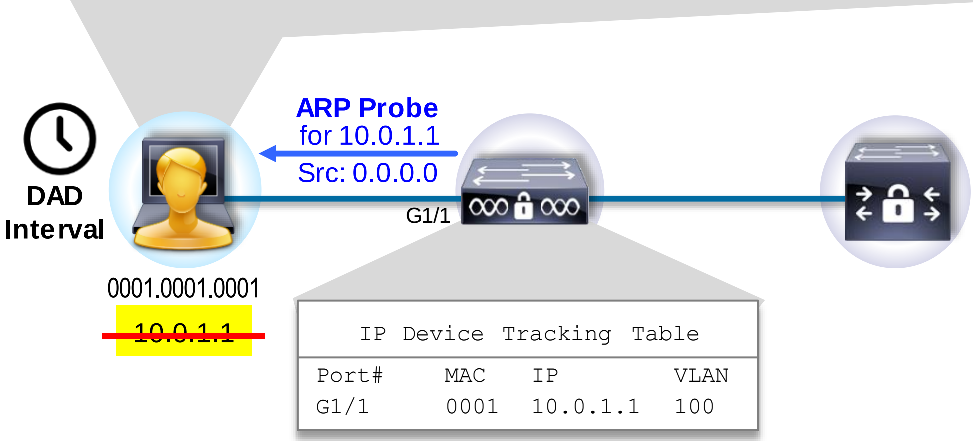
Mark Dead Server Alive after response to probe packets

# IPDT: Resolving ‘IP Address Conflict’ Issue



Windows has detected an IP address conflict

Another computer on this network has the same IP address as this computer. Contact your network administrator for help resolving this issue. More details are available in the Windows System event log.



IP Device Tracking Table

| Port# | MAC | IP | VLAN |
|---|---|---|---|
| G1/1 | 0001 | 10.0.1.1 | 100 |

DAD: Duplicate Address Detection

**RFC-5227** Explains the ARP probe and Duplicate address detection mechanisms

**Cisco IOS** uses the Address Resolution Protocol (ARP) Probe sourced from an address of 0.0.0.0 in order to maintain the IP device-tracking cache when IP device tracking and a feature that uses it is enabled (such as 802.1x) on a Cisco IOS switch.

## Solutions offered so far

```
ip device tracking probe delay <seconds>
```

Delay ARP probes from Switch by specified interval in seconds

```
ip device tracking probe use-svi
```

Use SVI IP address as source instead of the default 0.0.0.0 for ARP probes from the switch

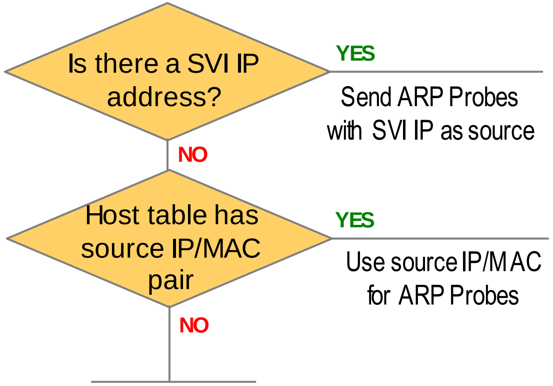
# IPDT: Resolving ‘IP Address Conflict’ Issue

NEW

15.2(2)E / 3.6.0E

```
ip device tracking probe auto-source
```

‘ip device tracking probe auto-source’



Is there a SVI IP address?

YES

Send ARP Probes with SVI IP as source

NO

Host table has source IP/MAC pair

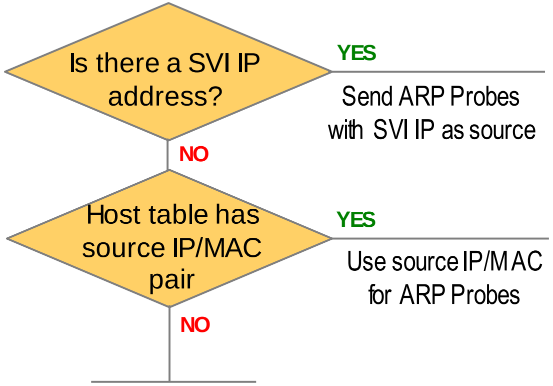
YES

Use source IP/MAC for ARP Probes

NO

Use default 0.0.0.0 and switch MAC address as source for ARP probes

‘ip device tracking probe auto-source **fallback 0.0.0.1 255.255.255.0**



Is there a SVI IP address?

YES

Send ARP Probes with SVI IP as source

NO

Host table has source IP/MAC pair

YES

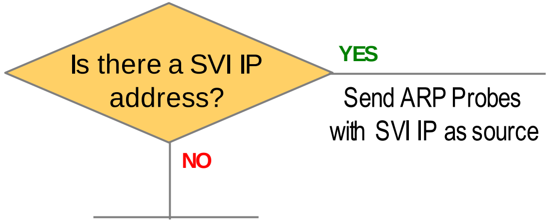
Use source IP/MAC for ARP Probes

NO

Derive source IP address for subnet based on wildcard bits and mask

E.g: For 192.168.1.0 (0.0.0.1) = 192.168.1.1

‘ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 **override**’



Is there a SVI IP address?

YES

Send ARP Probes with SVI IP as source

NO

Derive source IP address for subnet based on wildcard bits and mask

Examples:

For 192.168.1.0 (0.0.0.1) = 192.168.1.1

For 172.16.0.0 (0.0.0.100) = 172.16.0.100

# Conclusion

# Key Takeaways

Start simple, start with monitor mode.  Deploy in phases

IBNS 2.0 is flexible and extensible, Create once use many approach

Leverage IBNS 2.0 for enhanced capabilities; Critical ACL, Templates

Think of Identity, think of a system

# Q & A

# Complete Your Online Session Evaluation

**Give us your feedback and receive a Cisco Live 2015 T-Shirt!**

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

**Learn online with Cisco Live!**
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Cisco live!

# Thank you.

cisco