AutoConf & Interface Templates

- Best Practices
- Tips
- Caveats

Interface Template & AutoConf: Best Practice, tips

- Builtin templates must be modified for vlan config
  - All templates default to access vlan 1 ☹

```
Switchport access vlan X
Switchport voice vlan Y
Switchport trunk native vlan Z
```

- Once modified, builtin templates show in running and startup config
- AutoConf applied templates do not show in running config
- AutoConf enabled on all interfaces by default
  - Explicitly disable on interface "`access-session inherit disable autoconf`"

Auto Conf is Session Based

- Auto Conf and its service policies require Switch move to eEdge mode from the current Auth Mgr mode.
- Current dot1x config moves to access-session configuration.
  - The configuration move to access-session is not backwards compatible
- With AutoConf, Interface Templates and authentication services share the same session management infrastructure
  - Statically applied Interface Templates are the exception.
- How to convert from ASP macro to AutoConf Template?
  - Answer: it's a manual effort to port macro definitions.

AutoConf & Interface Templates: Performance , Scale

- Max Templates: unlimited (up to 4000 template definitions defined during test)
- Max template instances: unilmited
- Max Template size: 128 lines of configuration
- What is max Scale tested: 9 member 48 port switch tested.
- What causes the performance of the dynamic template binding to appear slow?
  - If the system does not have any statically bound templates, then first time dynamic binding would take longer time compared to consecutive templates provided other system factors are constant.
- First time if the feature is turned on and the time takes for the first template to get applied will be different from new devices get connected.

AutoConf: Interface & Service Templates

- Service Templates
  - Activated on Network Sessions
  - Policies in template apply to control and data packets of session only.
  - No impact to other hosts on same port
  - Exists for duration of session

- Interface Templates
  - Activated on Interfaces
  - Policies impact all traffic exchanged on Interface.
  - Exists for duration of session

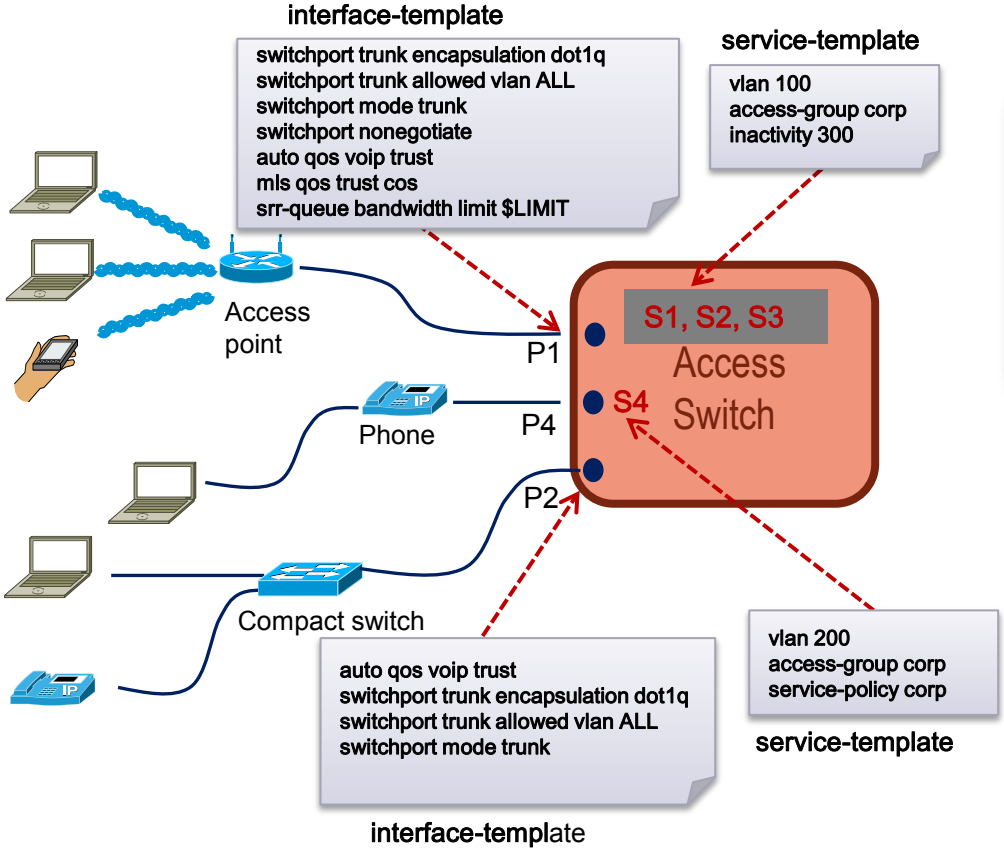
AutoConf: Methods to Apply Templates

- Service templates can be activated:
  - By reference in a user profile
  - As a control policy action (triggered by a session event)
  - Via a CoA command

- Interface templates can be activated:
  - Manually, via CLI
  - By reference in a user profile
  - By reference in a service template (see service activation triggers)
  - As a control policy action (triggered by a session event)
  - Via a CoA command

Auto conf – Use case

Platforms supported:4K/3K/2K/Compact



Interface Templates

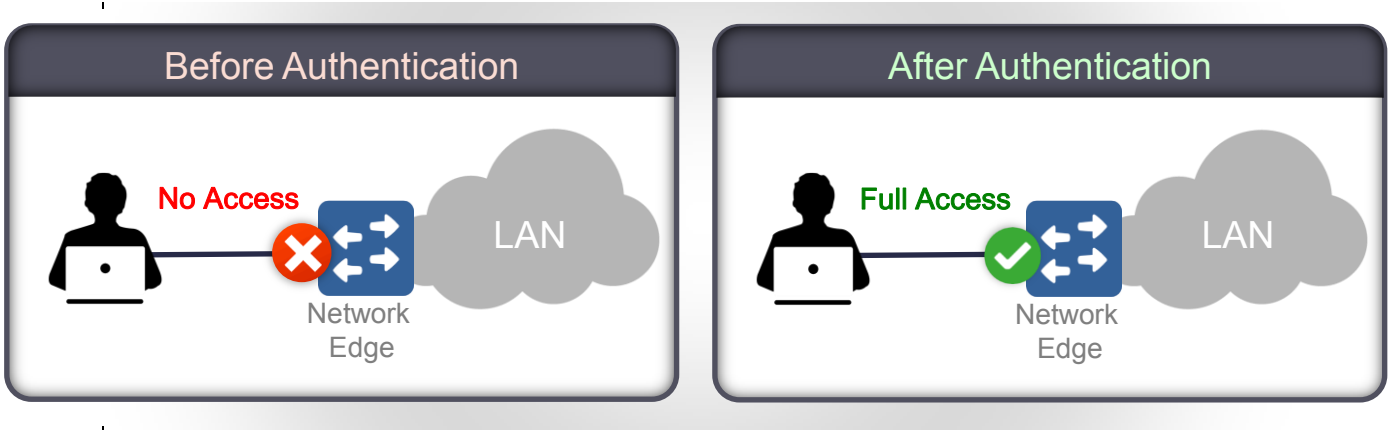
- Activated on INTERFACES
- Auto-conf one network device per port e.g. Switch or AP
- Impacts all the traffic exchanged via that interface
- Stays ON as long as activated

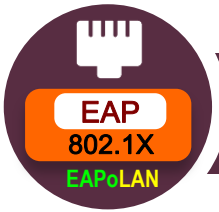
Service Templates

- Activated on NETWORK SESSIONS
- No impact on other session's sharing that port
- Stays ON as long as the session existS

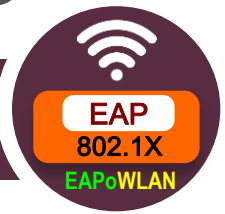
802.1X Based Identity Network

802.1X is an IEEE defined framework to address and provide, port-based access control using authentication





IEEE 802.1X is simply a standard for facilitating authentications over a wired or wireless LAN.



EAP: Extensible Authentication Protocol – We'll talk about it later

Identity Based Networking Services (IBNS)

Authentication

IEEE 802.1X

MAC Authentication

Web Authentication

Flexible Authentication

Authorization

Dynamic VLANs

Downloadable ACLs

Session Limits

Authorizing failures

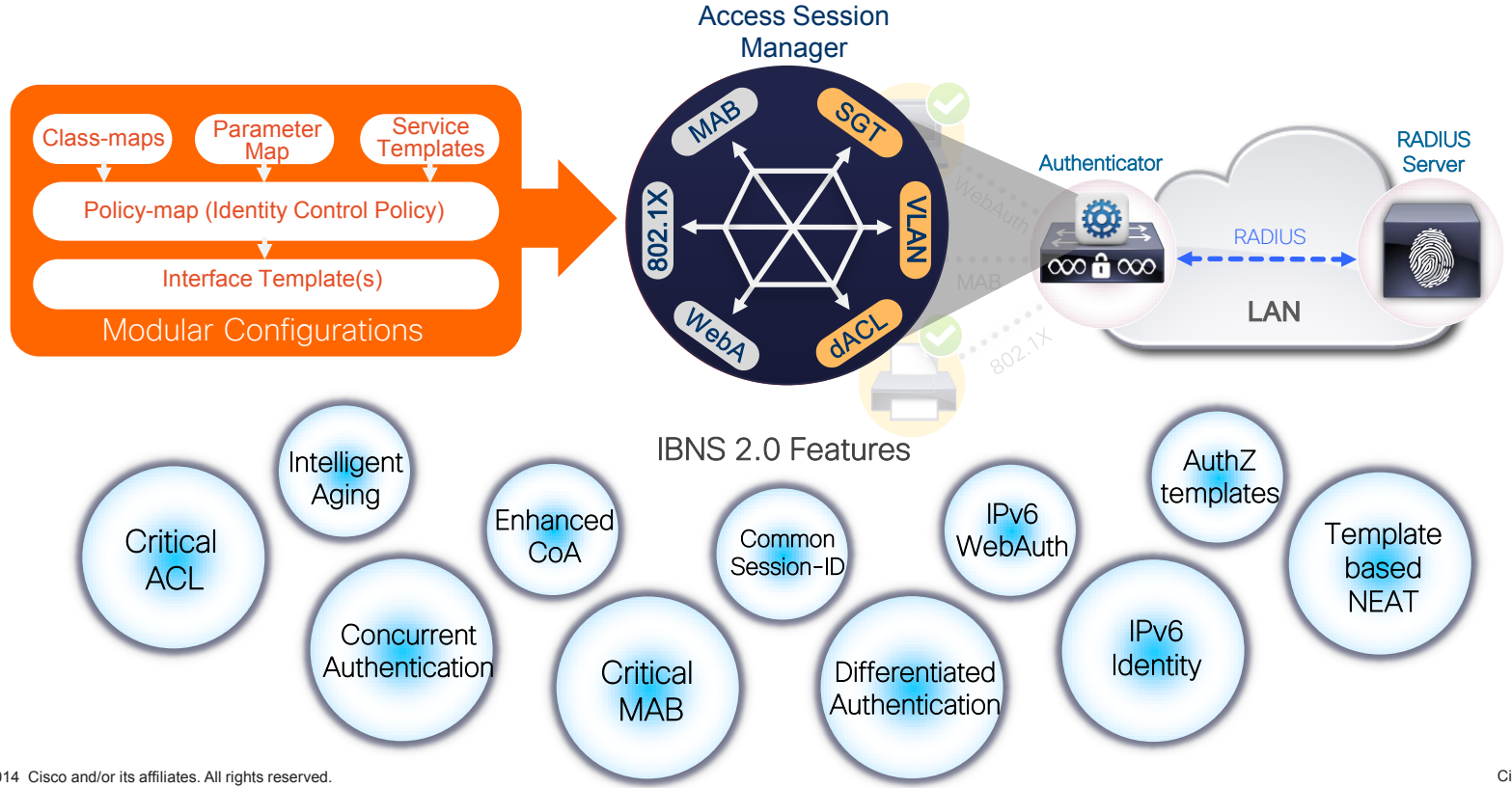
Deployment Modes

Phased deployments

- Monitor Mode
- Low-Impact Mode
- Closed Mode

IBNS 2.0 Overview

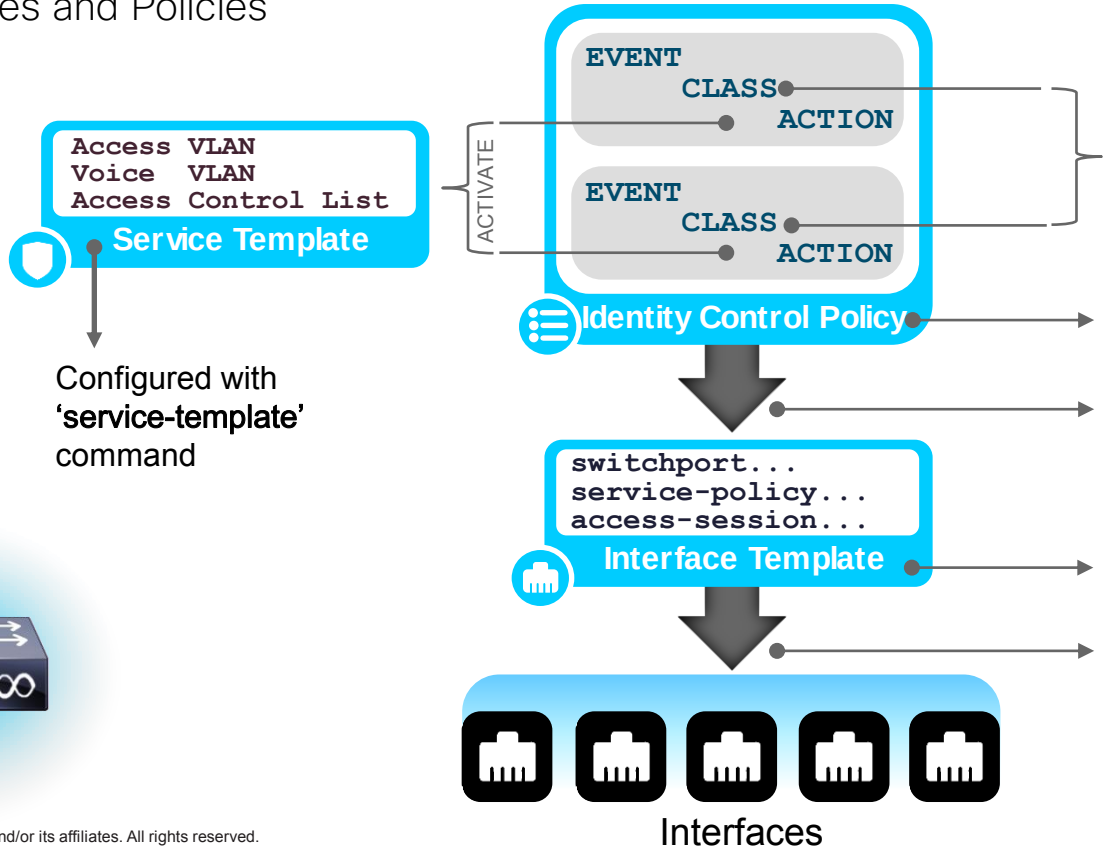
Any Authentication with Any Authorization on any Media (Wired / Wireless)



Configuring IBNS 2.0

Templates and Policies

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

Understanding Events, Classes and Action

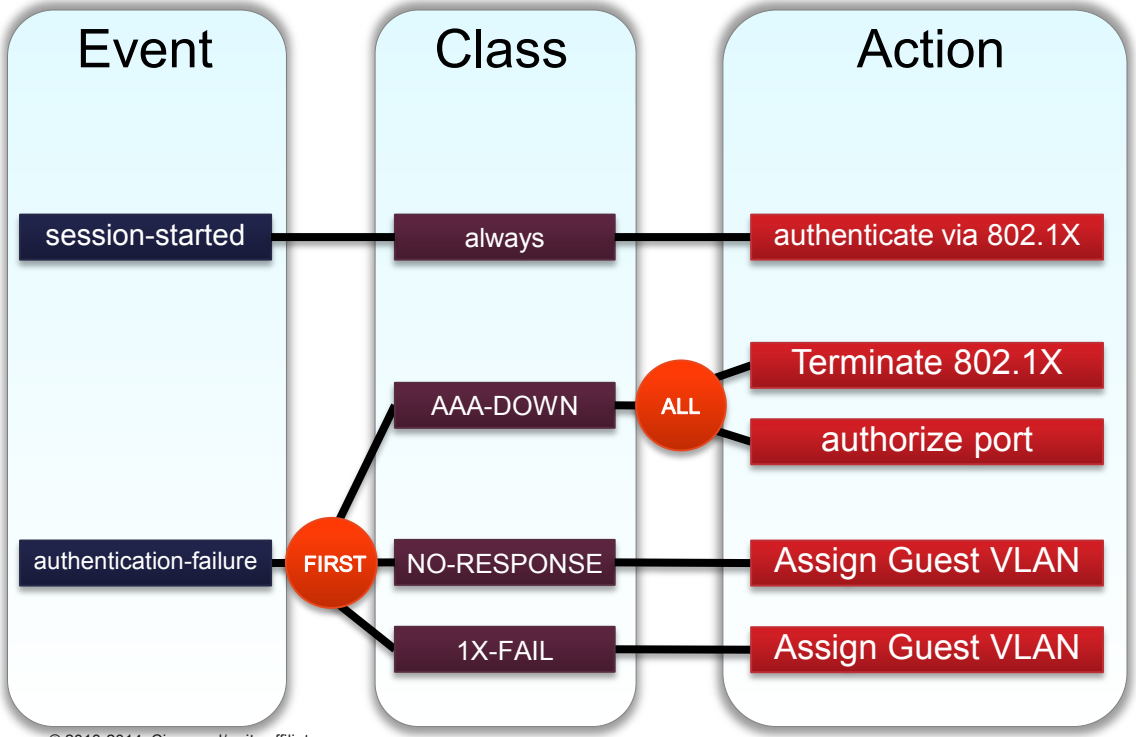
Your everyday Email Policy Management

E-Mail Policy (aka Inbox Filtering)

- **Event:** E-Mail arrives
- **Class:** additional Attributes
  - Sender is Wife
  - Mail is Spam
  - Mail is addressed to Mail List
- **Action:** Result, based on Class
  - Wife: 1) Mark Urgent 2) Put in Inbox
  - Spam: 1) Mark as Spam 2) Delete
  - Marketing 1) Put in Marketing Folder

From E-Mail Policy to Identity Control Policy

The concept still applies...



IDENTITY CONTROL POLICY

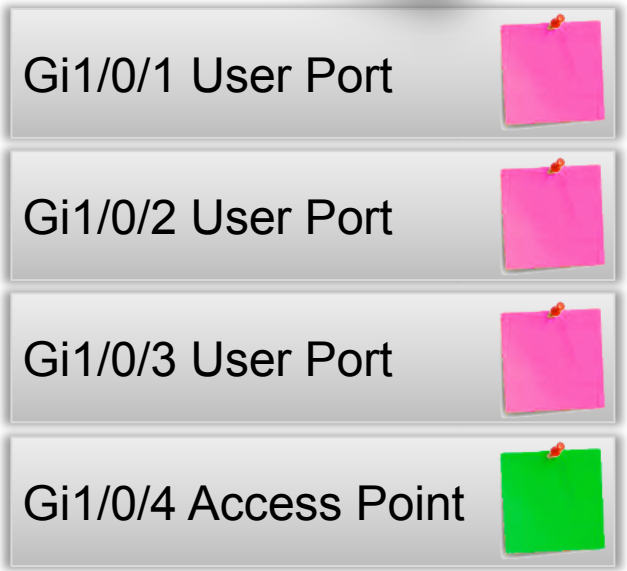
```
policy-map type control subscriber POLICY-A
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
 event authentication-failure match-first
  10 class AAA-DOWN do-all
   10 terminate dot1x
   20 authorize
  20 class DOT1X_NO_RESP do-until-failure
   10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

Templates

Dynamic Configuration Done the Right Way

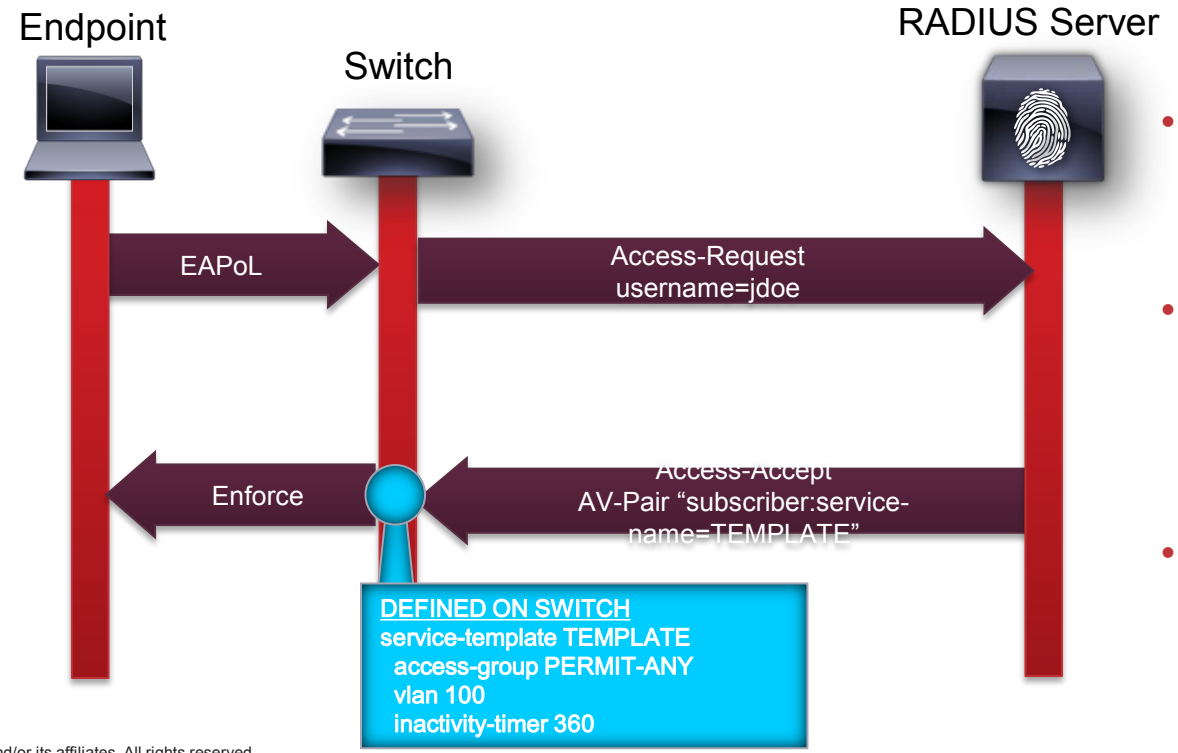
Configuration by Reference:

- 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



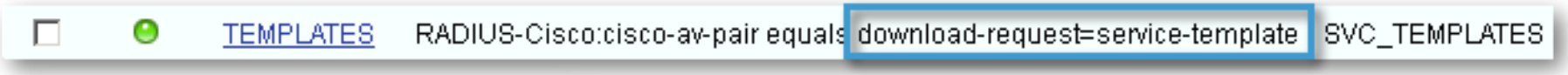
Applying a Template

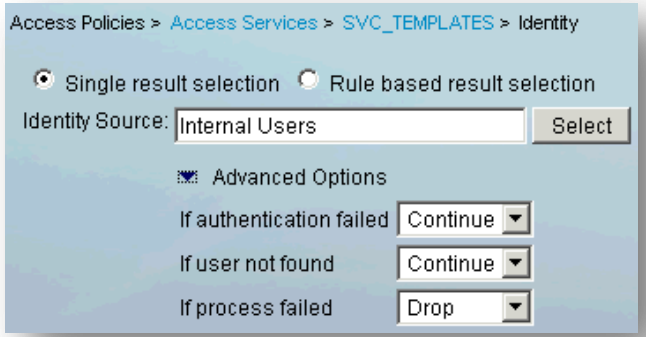
Similar to Applying a Port ACL via *filter-id*



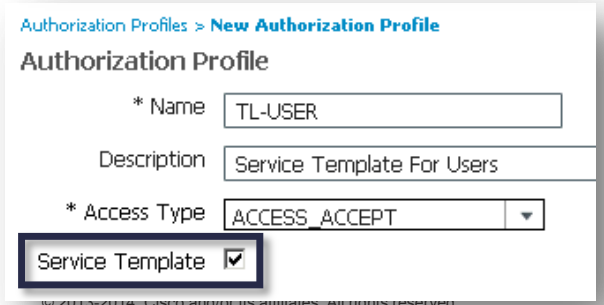
- Can also be triggered via RADIUS CoA
- Service-Templates activation can be a local Control Policy action
- If it doesn't exist, it can be downloaded like an dACL

Service Template Download from AAA





ACS



ISE

ACS / any RADIUS Server

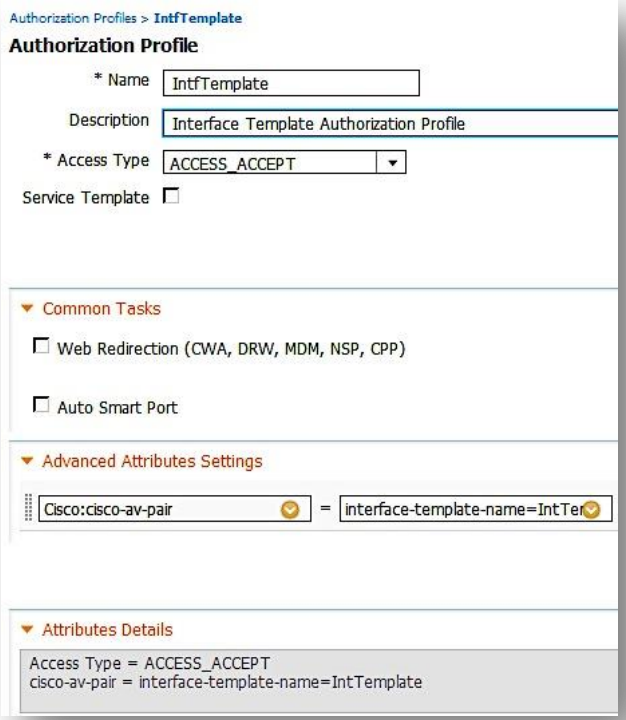
- Incoming request tagged with *cisco-av-pair="download-request=service-template"*
- Template-Name = Username
- Trivially Pass Authentication (username is the template name)
- Template Content is defined by AV pairs returned in authorization rules

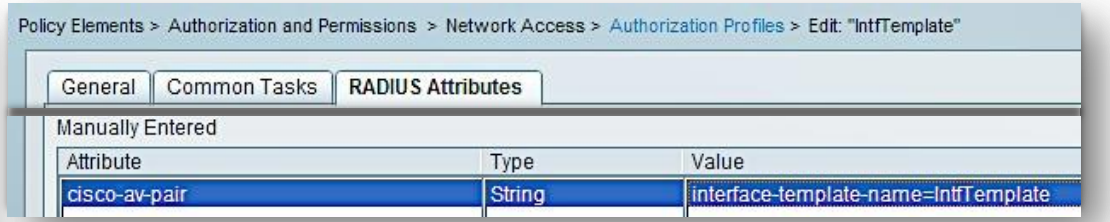
ISE 1.2 and newer

- Template support is built-in

Interface-Template Authorization from RADIUS

"cisco-av-pair = interface-template-name=<template>"





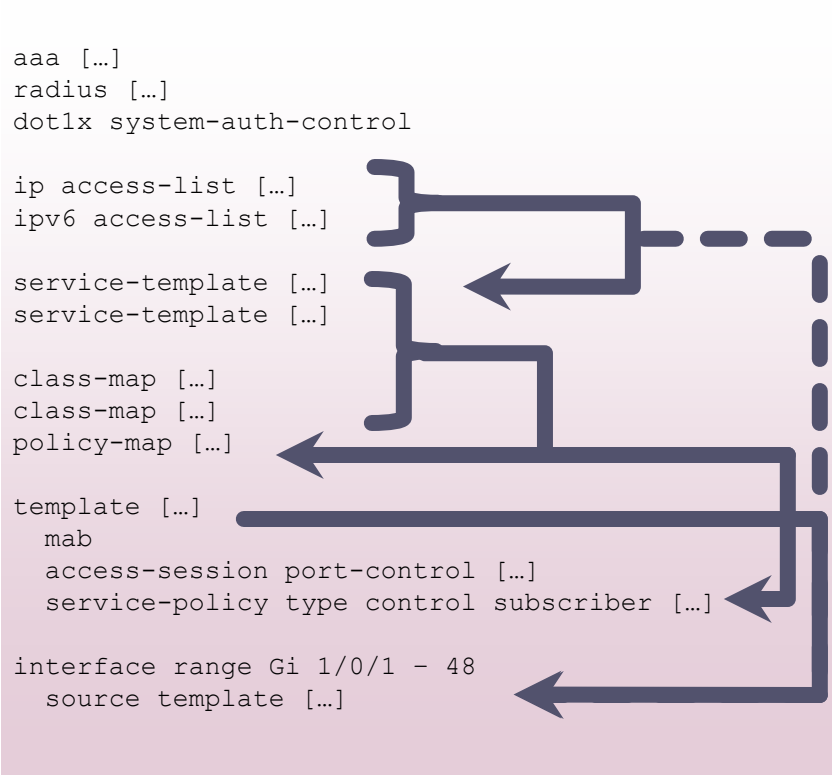
ACS

ISE

- The template must be configured locally on the switch
- Works similar to "Filter-ID" RADIUS attribute for authorizing 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



- 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’

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

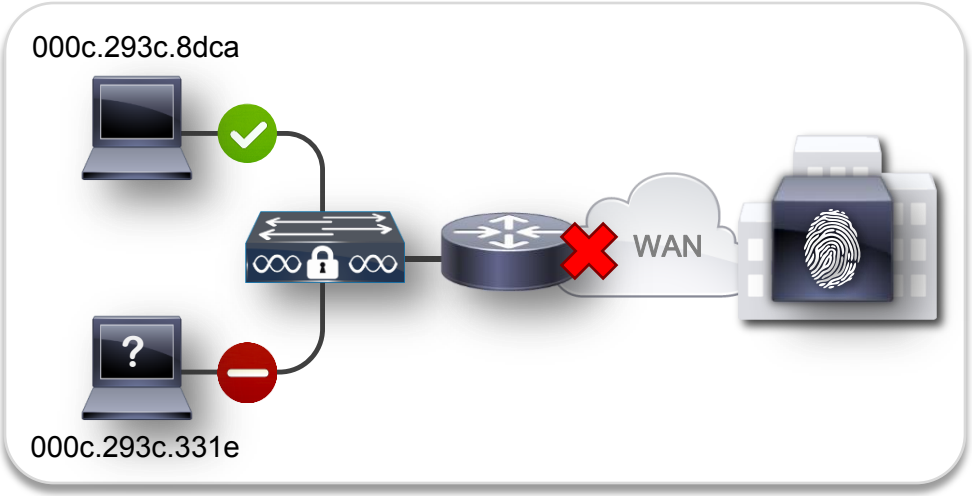
Tip: Start with known good configuration and see how changes in ‘legacy mode’ change the new configuration!

```
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).**

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 authorize hosts during a critical condition.
- EEM Scripts could be used for dynamic update of whitelist MAC addresses
- Sessions re-initialize once the server connectivity resumes.

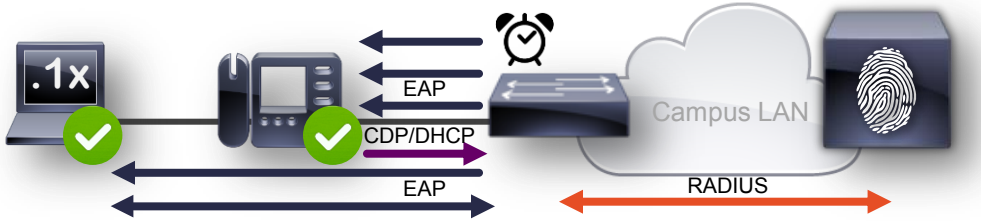
Demo Time!
Policy 802.1x med vlan x

Concurrent Authentication

Faster on-boarding of endpoints in to the network

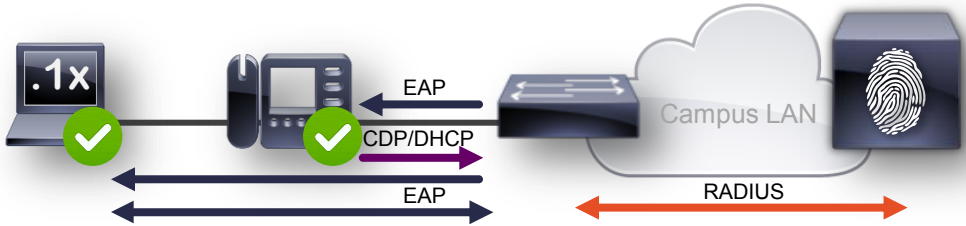
Sequential Authentication

```
authentication order dot1x mab
```



Concurrent Authentication

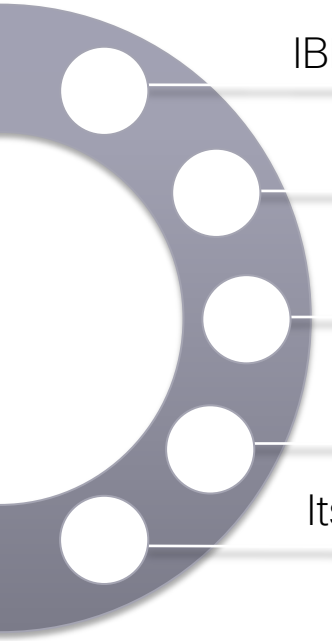
```
event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using mab priority 20
```



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

Key Takeaways

Key Takeaways



IBNS 2.0 is flexible and extensible

Create once use many approach

Service templates offer consistent on box and centralized authorizations

Interface templates keeps your running-config light and clean

Its ready, backward compatible and offers seamless migration to ‘new-style’

ISE versus Autoconf/interface templates:

Profile delen

MAC, MAC-OUI, CDP/LLDP, User-Role, Username.

Profile I ISE

+Prober, DHCP, HTTP, SNMP,DNS, NMAP,Radius,NetFlow = IOS sensor 3K/4K etc 6K.

Dynamisk vs Manuel

Dynamisk ACL og Service/interface template via ISE. Via central Radius/ISE server.

Interface templates er manuel og lægges lokalt på switchen men kan skubbes ud via Prime.

Ekstra ting i ISE

ISE har også BYOD, Posture check, link til MDM etc.

Thank you.