Understanding Identity Based Network Services IBNS 2.0

Rafael Leiva-Ochoa

BRKCRT-3002

Cisco Webex App

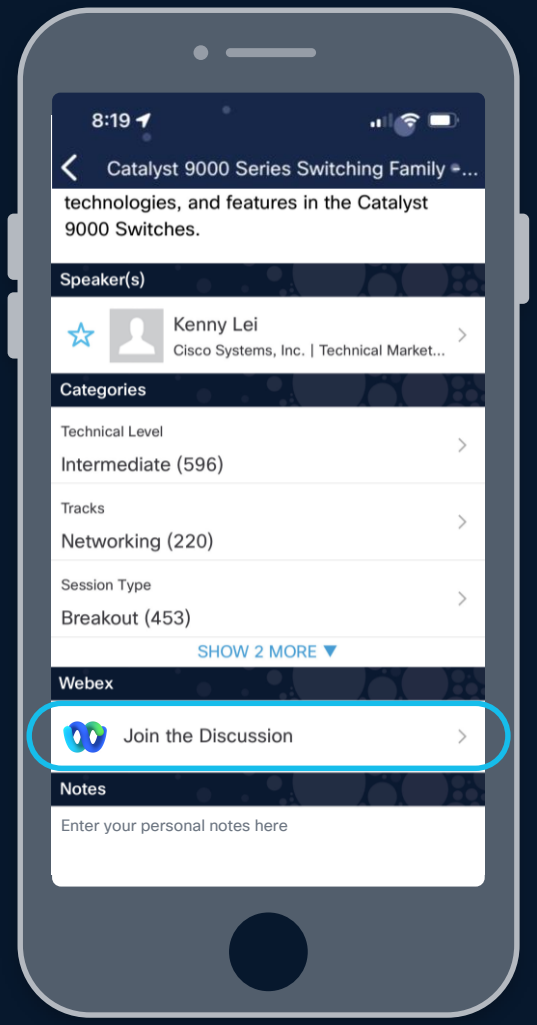
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKCRT-3002

Agenda

01 Introduction

02 Overview on IBNS 2.0

- What is IBNS?
- IBNS 1.0 vs 2.0

03 IBNS 2.0 Structure

04 Single Host Deployment

05 Multi-Domain Deployment

06 IBNS Troubleshooting

07 Automated Deployment Plans

Introduction

Introduction

- Rafael Leiva-Ochoa
- @Cisco since Oct 2000
- Works in the Learning & Development (Part of Learn with Cisco)
- Delivers courses on Security to Global TAC Centers and Customers
- CCIE 19322 Security since 2007 (19 years!!)

What is the Goal?

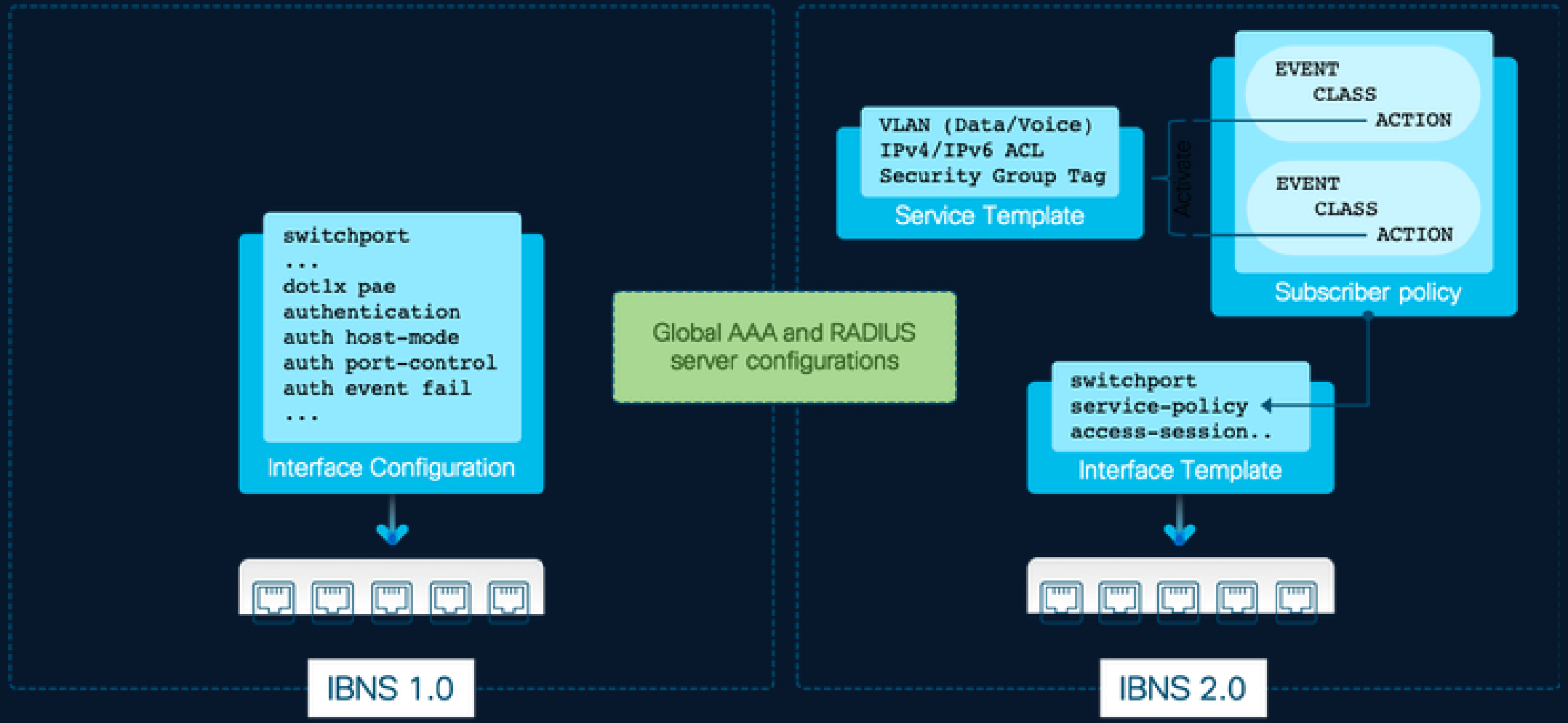
- To give the administrator/operator a better understating of the IBNS framework, and the differences between 1.0 vs 2.0.
- Prep for the SCOR exam

Overview on IBNS 2.0

What is IBNS?

- Identity-Based Network Services is a framework that delivers flexible and scalable services to subscribers when using 802.1x, MAB, and Webauth. It does this by taking a response to specified conditions based on subscriber **events**. These responses can also act when the ISE Server goes down.

IBNS 1.0 vs 2.0



IBNS 1.0 vs 2.0

- IBNS 1.0 has always suffered from configuration complexity, and out-of-control interface configuration bloat!!!

IBNS 1.0

```
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 40
 ip access-group PRE-AUTH in
 authentication event fail action next-method
 authentication event server dead action authorize vlan 88
 authentication event server dead action authorize voice
 authentication event server alive action reinitialize
 authentication host-mode multi-domain
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server mab
 dot1x pae authenticator
 spanning-tree portfast
```

IBNS 2.0

```
class-map type control subscriber match-all AAA_SVR_DOWN
    match result-type aaa-timeout
    match authorization-status unauthorized
class-map type control subscriber
    match-all DOT1X
    match method dot1x
......
policy-map type control subscriber POLICY
  event session-started match-all
   10 class always do-until-failure
     10 authenticate using dot1x priority 10
     20 authenticate using mab priority 20
.....
template DOT1X_PORTS
.....
   service-policy type control subscriber POLICY

interface range GigabitEthernet1/0/1 - 20
   source template DOT1X_PORTS
......
```

IBNS 1.0 vs 2.0

- IBNS 2.0 was created to resolve not only the configuration complexity and bloat of 1.0, but also to address problems we might not be able to control.
- For example:
  - What if the authentication server is not responding or fails the authentication?
  - Is MAC Authentication Bypass (MAB) failing?
  - Is the 802.1x supplicant not responding because it is not configured correctly?
  - What if the 802.1x supplicant configuration issue gets fixed and now it is attempting to authenticate?

IBNS 1.0 vs 2.0

Identity Control Policy

- Uses Cisco Common Classification Policy Language (C3PL)
- Used to create class-map, policy-map, and service-policy configurations

Service Template

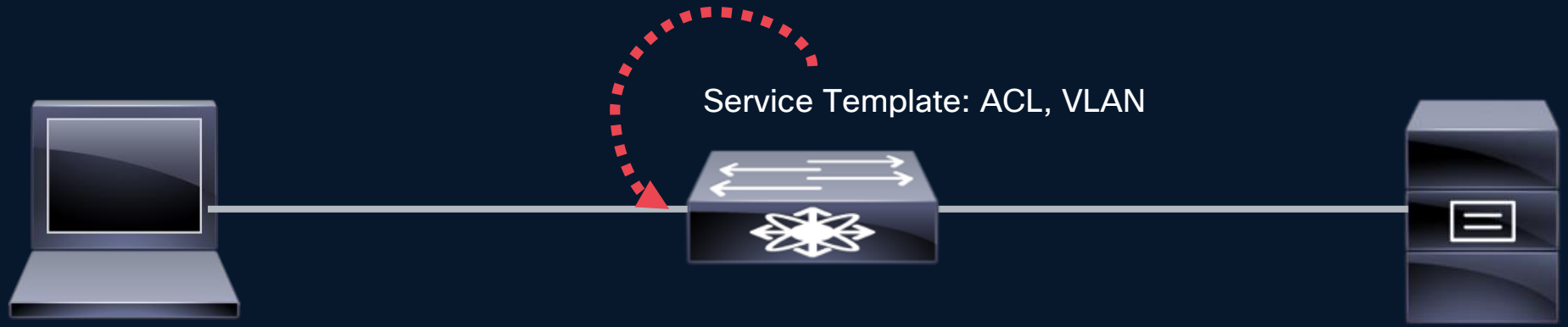
- Used to apply policy attributes to a subscriber session
- For example, ACL, VLAN, and other restrictions

Interface Template

- Used to configure common interface settings
- For example, 802.1x setting, and apply the service-policy to an interface

IBNS 1.0 vs 2.0

- Service Template
  - switch(config)# service-template LIMITED_ACCESS_AUTH_VLAN
  - switch(config-service-template)# access-group LIMTED_ACL
  - switch(config-service-template)# vlan 50

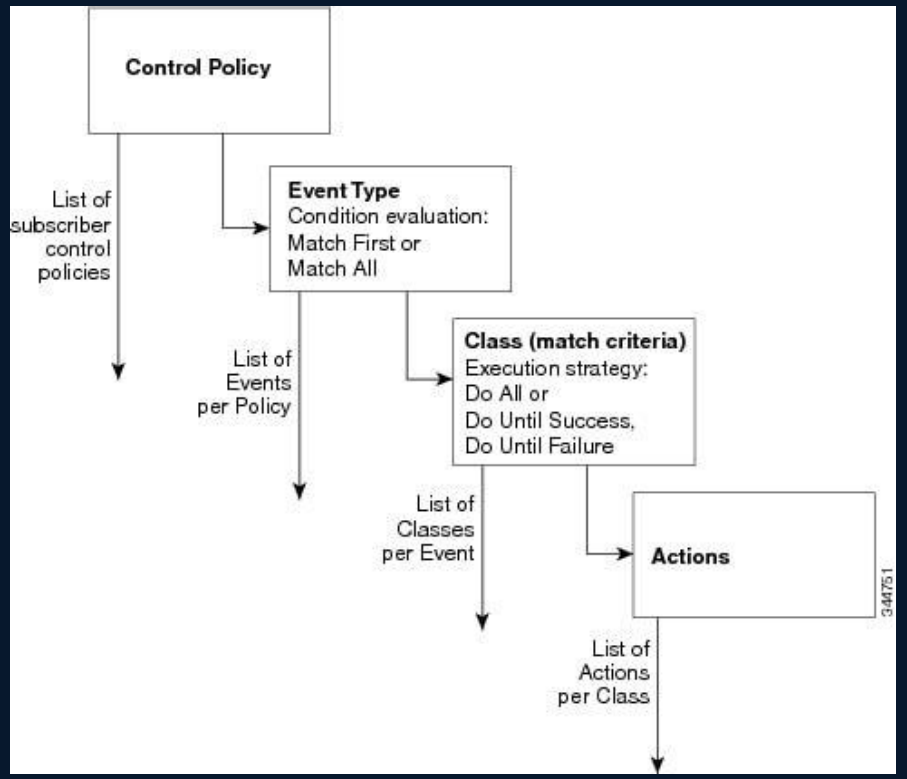


IBNS 1.0 vs 2.0

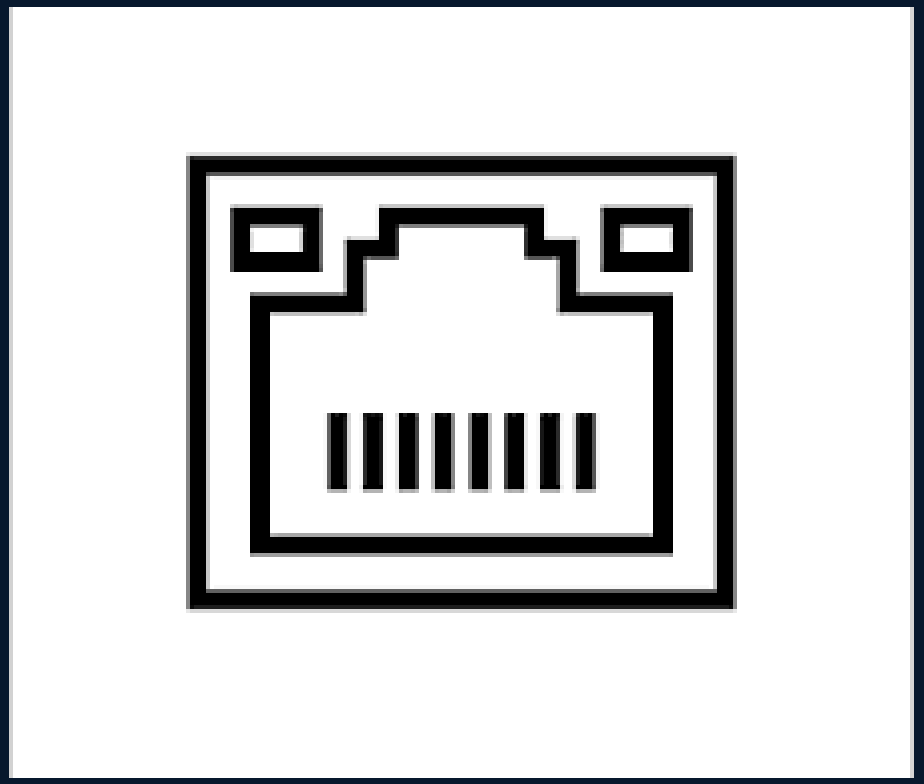
- Control Policy Structure

```
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
  match result-type aaa-timeout
  match authorization-status unauthorized
class-map type control subscriber
  match-all DOT1X match method dot1x

policy-map type control subscriber POLICY
event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
```



IBNS 1.0 vs 2.0



- Interface Template

```
switch(config)# template DOT1X_PORTS
switch(config-template)# switchport mode access
switch(config-template)# spanning-tree portfast
switch(config-template)# switchport access vlan 10
switch(config-template)# switchport voice vlan 40
switch(config-template)# access-session host-mode multi-domain
switch(config-template)# access-session port-control auto
switch(config-template)# mab
switch(config-template)# authentication periodic
switch(config-template)# authentication timer reauthenticate server
switch(config-template)# dot1x pae authenticator
switch(config-template)# service-policy type control subscriber POLICY
```

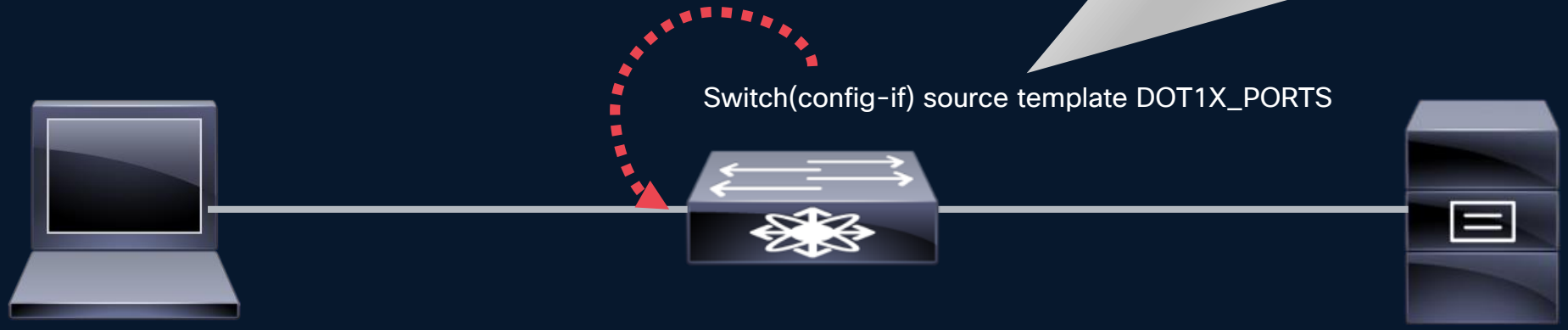
IBNS 1.0 vs 2.0

- Interface

  switch(config)# **interface range GigabitEthernet1/0/1 - 20**

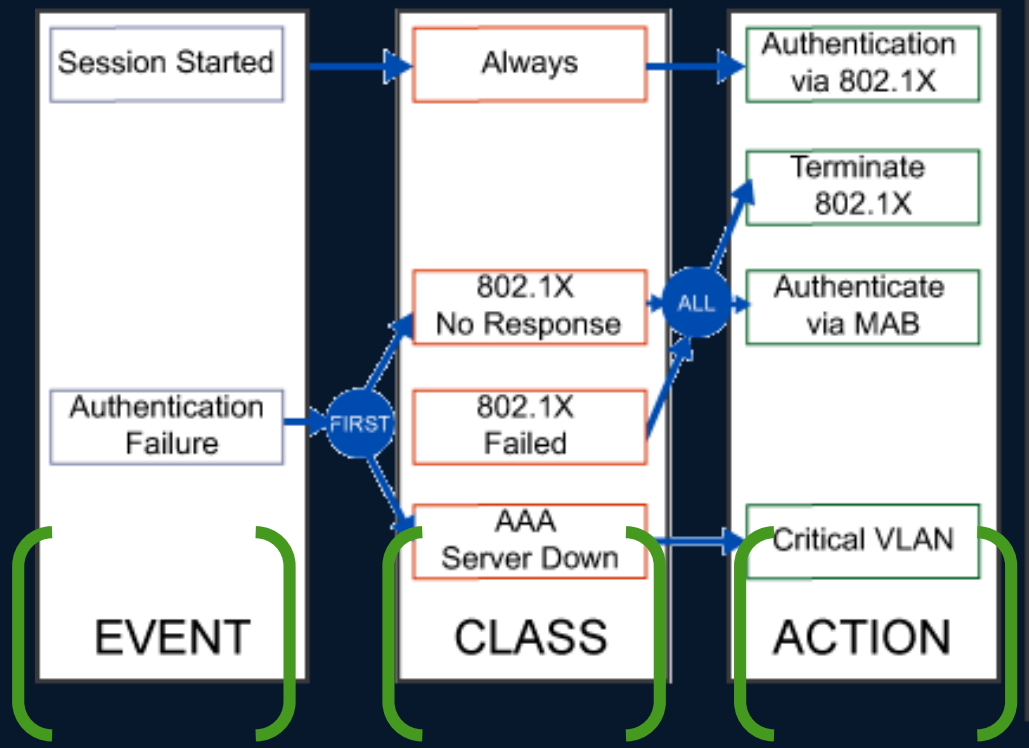
  switch(config-if)# **source template DOT1X_PORTS**

```
switch(config)# template DOT1X_PORTS
switch(config-template)# switchport mode access
switch(config-template)# spanning-tree portfast
switch(config-template)# switchport access vlan 10
switch(config-template)# switchport voice vlan 40
switch(config-template)# access-session host-mode multi-domain
switch(config-template)# access-session port-control auto
switch(config-template)# mab
switch(config-template)# authentication periodic
switch(config-template)# authentication timer reauthenticate server
switch(config-template)# dot1x pae authenticator
switch(config-template)# service-policy type control subscriber POLICY
```



IBNS 2.0 Structure

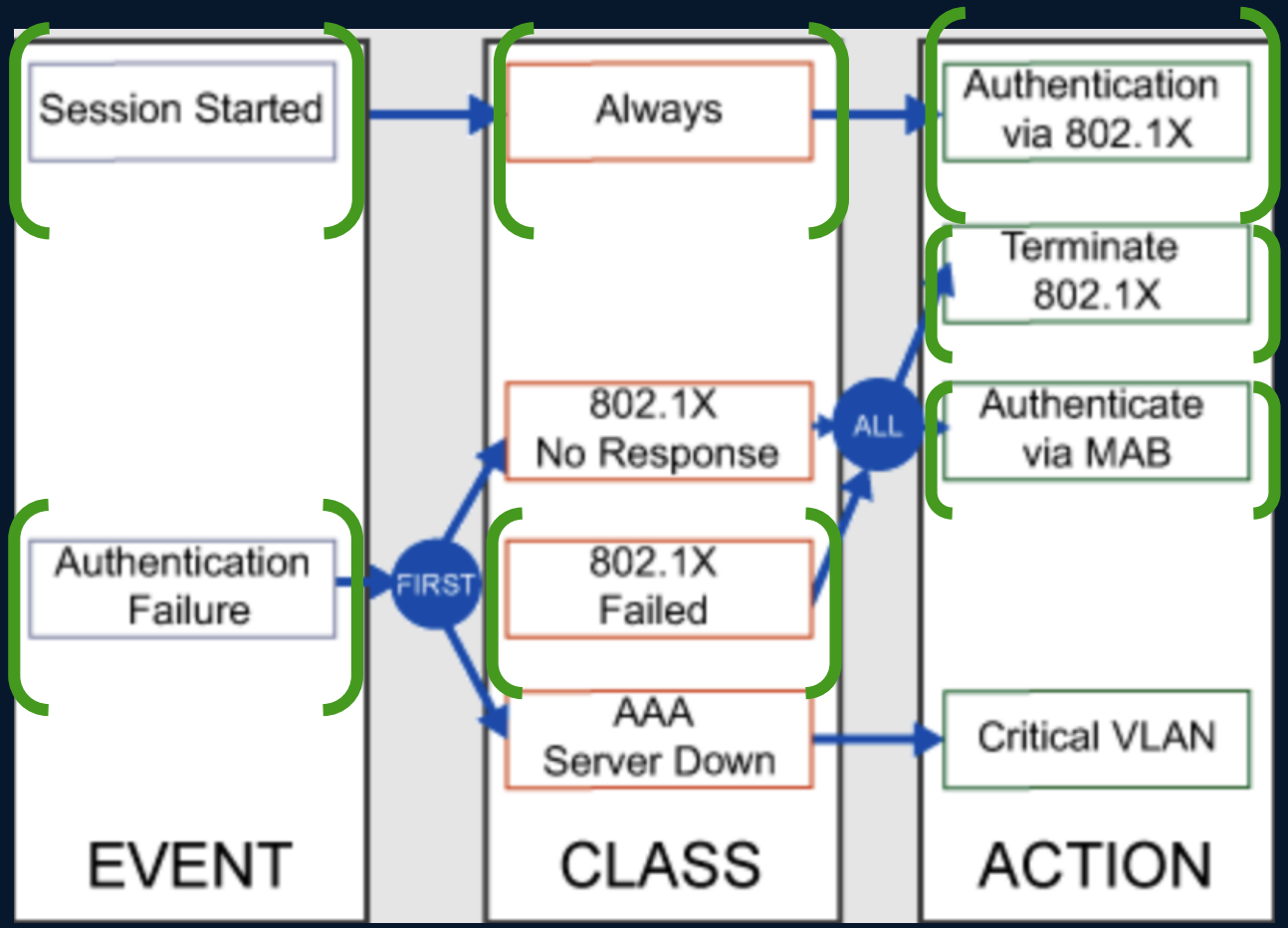
Policy Flow




```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template CRITICAL_VOICE_VLAN
   30 authorize
   40 pause reauthentication
  20 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
```

Policy-Map

```
policy-map type control subscriber Policy
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN_Gi1/0/11
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
```



Class Behaviors

```
policy-map type control subscriber Policy
 event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
    5 class DOT1X_FAILED do-until-failure
     10 terminate dot1x
     20 authenticate using mab priority 20
   10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
     10 activate service-template CRITICAL_AUTH_VLAN_Gi1/0/11
     20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
     30 authorize
     40 pause reauthentication
   20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
     10 pause reauthentication
     20 authorize
```

- **do-all** - attempts all actions regardless of success or failure
- **do-until-failure** (**Default**)- each action will be executed in sequence, if an action fails, it will evaluate the next event
- **do-until-success** - stops on the first successful action

Class-Map

- The class map is a set of conditions that must equal true to execute actions.

  class-map type control subscriber <matching options> <name of class-map>

    match <conditions>

- Match options:
  - match-all
  - match-any
  - match-none

Class-Map (cont.)

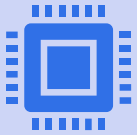
```
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
    match result-type aaa-timeout
    match authorization-status authorized
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
    match result-type aaa-timeout
    match authorization-status unauthorized
class-map type control subscriber match-all DOT1X
    match method dot1x
class-map type control subscriber match-all DOT1X_FAILED
    match method dot1x
    match result-type method dot1x authoritative
```

Policy-Map

- Is a sequence of events that defines actions that are taken in response to specified conditions and endpoint events.

```
policy-map type control subscriber <policy name>
  events
    class
      actions
  events
    class
      actions
  events
    class
      actions
```

IBNS 1.0 to 2.0 Migration



If you currently have a IBNS 1.0 configuration, it can be migrated to the new IBNS 2.0 with one command

authentication display new-style

To go back to IBNS 1.0 it can be done with the following command

authentication display legacy

The “authentication display legacy” will not work with IBNS 2.0 commands that were typed in.

Single Host Deployment

Single Host Deployment

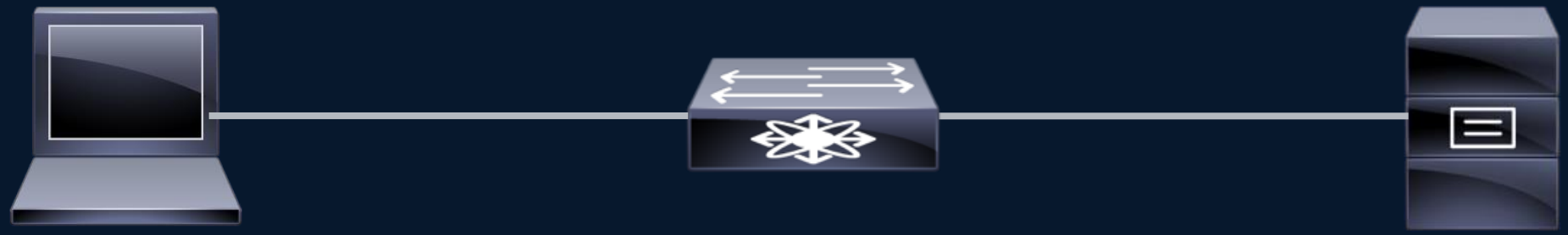
- In a single host deployment, the administrator can use a simple design that does not require a class-map configuration, but only a policy map.

```
policy-map type control subscriber SINGLE_HOST
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
```

```
interface GigabitEthernet1/0/1
  switchport access vlan 50
  switchport mode access
  access-session host-mode single-host
  access-session port-control auto dot1x pae authenticator
  service-policy type control subscriber SINGLE_HOST
```

Single Host Deployment Design Limitations

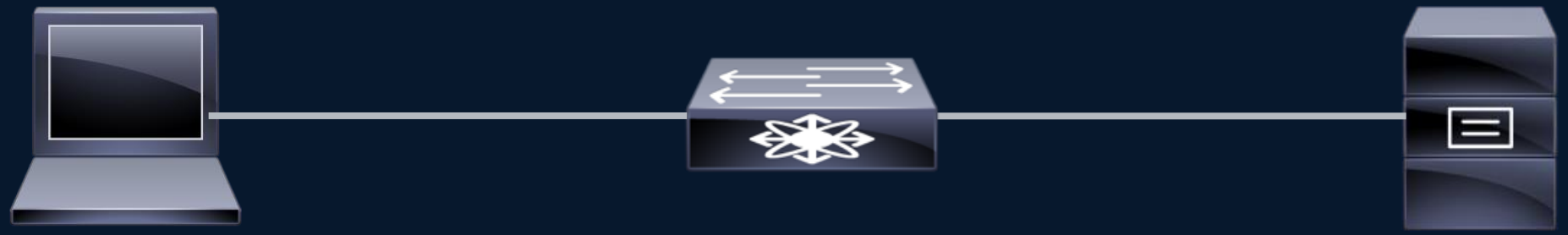
- Limited to only one event which is the start of a session
- No back-up events if the server goes down
- No recovery from failure events
- Not scalable when deployed in a multi-domain deployment
- No back-up access to the network



Multi-Domain Deployment

Multi-Domain Deployment

- A single design will not work if a computer is attached to an IP Phone that has its own 802.1x supplicant authentication.
- A multi-domain deployment provides multi-event scenarios that addresses the possibility that the switch also has printers, or non-supplicant devices attached that require MAB.



Service-Template Options

A service-template is used to apply a collection of network access policies, such as ACLs and VLAN assignments, that can be applied to user sessions based on events that happen during the session.

A service template should not replace the ISE box authorization it is only a backup.

```
service-template MAIN_AUTH_VLAN
  vlan 80
```

Service-Template Options (cont.)

- The Service Template options:

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

Service-Template Options (cont.)

- The Service Template options most used:
  - **access-group** Access list to be applied
  - **sgt** SGT tag
  - **tag** tag name
  - **vlan** Vlan to be applied
  - **voice** Voice feature
- In most cases, the access group and vlan are used in one service template to allow limited access to the network..

```
service-template MAIN_AUTH_VLAN
 vlan 80
 access-group LIMITED_ACL
```

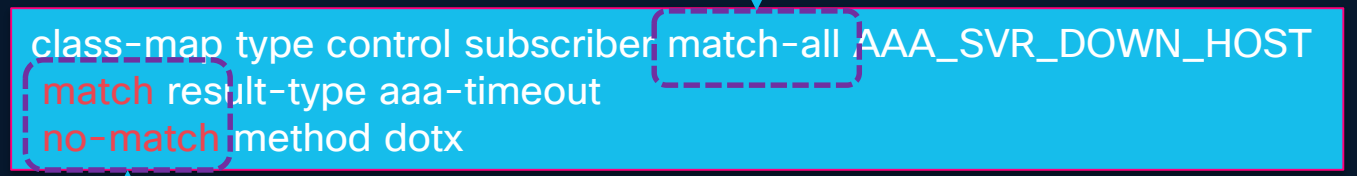
Class-Map Options

- The class-map defines the conditions that need to be true for an action to be executed.
- The system can have many class-maps based on the events that are being created on a policy-map.

```
class-map type control subscriber match-all AAA_SVR_DOWN_HOST
 match result-type aaa-timeout
 match authorization-status authorized
```

Class-Map Options (cont.)

- Outside the Class-map it used to match filters
  - match-all
  - match-any
  - match-none
- Inside the Class-maps it uses filters
  - match
  - no-match
- Using many filters is not considered better. **Use what is needed**.



Class-Map Options (cont.)

- The class-map match options:

activated-service-template	match name of service template activated on session
authorization-failure	match the type of authorization failure from an authorization failed event
authorization-status	match the authorization status of the session
authorizing-method-priority	match the priority against the authorizing method's priority
client-type	match the type of device from an event

current-method-priority	match the priority against the current method's priority
device-type	match name of the device-type
interface	match the session interface
ip-address	match the IP address from an event
ipv6-address	match the IPv6 address from an event
mac-address	match the MAC address from an event
method	match the type of authentication **method from an event**

Class-Map Options (cont.)

- The class-map match options:

oui	match the oui address from an event
port-type	match the type interface from an event
result-type	match the result type, optionally for a specific method
service-template	match name of service template from an event
session-type	match the session type
sgt	match the sgt session

ssid	match the ssid of the session
tag	match tag from an event
timer	match the type of timer
user-role	match the user-role
username	match the username
vlan	match the VLAN from an event

Class-Map Options (cont.)

- The class-map filters most used:
  - **result-type** match the result type, optionally for a specific method
  - **authorization-status** match the authorization status of the session
  - **activated-service-template** match name of service template activated on session
  - **mac-address** match the MAC address from an event
  - **session-type** match the session type (wried, or wireless)

```
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match result-type aaa-timeout
 match authorization-status unauthorized
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
```

Policy-Map Options (cont.)

- The event options:

aaa-available	aaa-available event
absolute-timeout	absolute timeout event
agent-found	agent found event
authentication-failure	authentication failure event
authentication-success	authentication success event
authorization-failure	authorization failure event
authorization-success	authorization success event
identity-update	identity update event
inactivity-timeout	inactivity timeout event
remote-authentication-failure	authentication failure event
remote-authentication-success	authentication remote success event
session-disconnected	session disconnected event
session-started	session started event
tag-added	tag to apply event
tag-removed	tag to remove event
template-activated	template activated event
template-activation-failed	template activation failed event
template-deactivated	template deactivated event
template-deactivation-failed	template deactivation failed event
timer-expiry	timer-expiry event
violation	session violation event

Policy-Map Options (cont.)

- The policy-map is used to apply the class-maps to events that could happen during the user session, and actions that are applied
- The policy-map starts with selecting an event type.
- The events most offen used are:
  - session-started **(Start)**
  - authentication-failure
  - agent-found
  - aaa-available
  - authorization-success (Only used to apply local policy)

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
 ....
```

```
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
```

- **authoritative -Authorization failed.**

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

```
event authentication-failure match-first
....
10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN_Gi1/0/1
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
....
```

```
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
      match result-type aaa-timeout
      match authorization-status unauthorized
```

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
event authentication-failure match-first
....
  20 class AAA_SVR_DOWN_HOST do-until-failure
   10 pause reauthentication
   20 authorize
```

```
class-map type control subscriber match-all AAA_SVR_DOWN_HOST
 match result-type aaa-timeout
 match authorization-status authorized
```

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
event authentication-failure match-first
 ....
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
```

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

```
event authentication-failure match-first
....
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
```

```
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
```

- **authoritative -Authorization failed.**

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

```
event authentication-failure match-first
....
50 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
```

- **Class Always:**
  - If **authentication** fails beyond the other classes stated, then apply the actions below.

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

```
....
event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
```

- **Class Always:**
  - If the host starts an EAP session, then apply the actions below.

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

```
....
event aaa-available match-all
  10 class IN_CRITICAL_VLAN do-until-failure
   10 clear-session
```

```
class-map type control subscriber match-any IN_CRITICAL_VLAN
 match activated-service-template CRITICAL_AUTH_VLAN_Gi1/0/1
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
```

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

```
event aaa-available match-all
....
20 class NOT_IN_CRITICAL_VLAN do-until-failure
   10 resume reauthentication
```

```
class-map type control subscriber match-none NOT_IN_CRITICAL_VLAN
 match activated-service-template MAIN_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
```

Policy-Map Configuration (cont.)

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

```
 event authentication-success match-all
```

- Used to apply other policy restrictions such as MACsec or polices that will not be centralized on the ISE box.

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN_Gi1/0/1
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  50 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
```

```
event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event aaa-available match-all
  10 class IN_CRITICAL_VLAN do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_VLAN do-until-failure
   10 resume reauthentication
 event authentication-success match-all
```

Interface Template

```
template DOT1X_PORTS
 switchport mode access
 spanning-tree portfast
 switchport access vlan 50
 switchport voice vlan 40
 access-session host-mode multi-domain
 access-session port-control auto
 mab
 authentication periodic
 authentication timer reauthenticate server
 dot1x pae authenticator
 service-policy type control subscriber POLICY
```

```
policy-map type control subscriber POLICY
.....
```

```
interface range GigabitEthernet1/0/1 - 20
 source template DOT1X_PORTS
```

- The interface template can be used for 802.1x configurations
- Other interface settings can also be shared across interfaces when the template is applied
- The access-session command is now used for most dot1x settings

Verification Commands

```
switch# show derived-config interface GigabitEthernet0/9

Building configuration...


Derived configuration : 260 bytes
!
interface GigabitEthernet0/9
 description Client Port
 switchport mode access
 authentication periodic
 access-session host-mode multi-domain
 access-session port-control auto
 mab
 dot1x pae authenticator
 service-policy type control subscriber POLICY
end
```

- The **derived-config interface <interface>** command used to display interface template information.
- Filtering the output can be done using **| section**
- **Example:**
  - **show derived-config interface GigabitEthernet0/9 | section access-session**

IBNS 2.0 Troubleshooting

IBNS Debugging

1

debug mab all – Displays all mab authentications

2

debug dot1x all – Displays all dot1x packet info

3

debug pre all* –

Enables PRE level debugs flows

* PRE - Platform Entry Event

IBNS Debugging

Feb 26 19:08:25.482: dot1x-ev:[Gi0/9] Interface state changed to UP

Feb 26 19:08:25.486: dot1x-ev:DOT1X Supplicant not enabled on GigabitEthernet0/9

Feb 26 19:08:27.475: %LINK-3-UPDOWN: Interface GigabitEthernet0/9, changed state to up

Feb 26 19:08:28.474: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/9, changed state to up

IBNS Debugging

```
Feb 26 19:08:43.463: [PRE:RULE:EVENT:C6000001] Executing policy-map type control subscriber POLICY
Feb 26 19:08:43.463: [PRE:RULE:EVENT:C6000001]   event (id:13 name:session-started) match-all
Feb 26 19:08:43.463: [PRE:RULE:EVENT:C6000001]   class always do-until-failure policy instance 0x36010043
Feb 26 19:08:43.463: [PRE:RULE:EVENT:C6000001] Evaluate: class-map type control match-all subscriber always
Feb 26 19:08:43.463: [PRE:RULE:EVENT:C6000001] evaluated class map: success
Feb 26 19:08:43.470:  dot1x_auth Gi0/9: initial state auth_initialize has enter
Feb 26 19:08:43.470: dot1x-sm:[685b.35ab.ac5f, Gi0/9] 0x07000001: initialising
```

```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

IBNS Debugging

```
Feb 26 20:03:09.043: dot1x-ev:[685b.35ab.ac5f, Gi0/9] Dot1x authentication started for 0xDE000006 (685b.35ab.ac5f)
Feb 26 20:03:09.043: [PRE:RULE:EVENT:81000006] Action authenticate using dot1x retries 2 retry-time 0 priority 10:sync:success
Feb 26 20:03:09.047: [PRE:RULE:EVENT:81000006] executed action handlers and returning with status:1, result:0
Feb 26 20:03:09.047: [PRE:RULE:EVENT:81000006] Executing policy-map type control subscriber POLICY
```

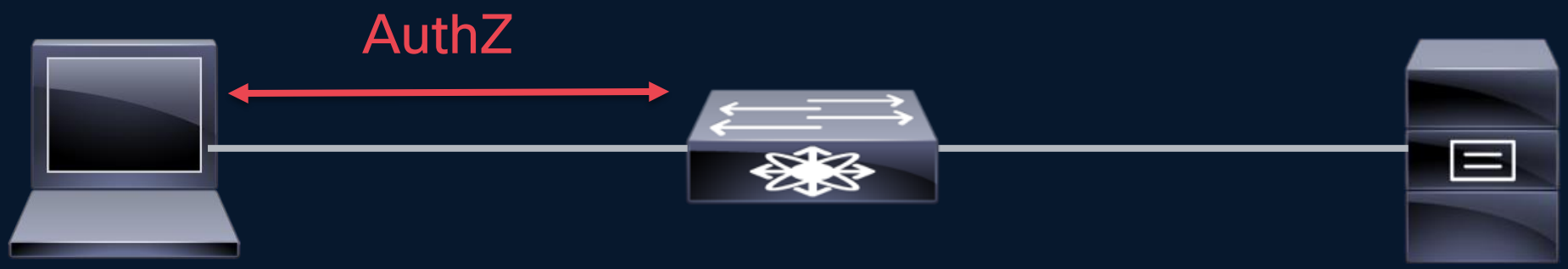
```
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
```

IBNS Debugging

```
Feb 26 20:03:09.047: dot1x-ev:[685b.35ab.ac5f, Gi0/9] Sending out EAPOL packet to MAC 685b.35ab.ac5f
Feb 26 20:03:09.047: dot1x-packet:EAPOL pak Tx - Ver: 0x3  type: 0x0
Feb 26 20:03:09.047: dot1x-packet: length: 0x0005
Feb 26 20:03:09.047: dot1x-packet:EAP code: 0x1  id: 0x1  length: 0x0005
Feb 26 20:03:09.047: dot1x-packet: type: 0x1
Feb 26 20:03:09.047: dot1x-packet:[685b.35ab.ac5f, Gi0/9] EAPOL packet sent to client 0xDE000006
Feb 26 20:03:09.047: dot1x-sm:[685b.35ab.ac5f, Gi0/9] 0xDE000006:idle request action
Feb 26 20:03:09.099: dot1x-packet:[685b.35ab.ac5f, Gi0/9] Queuing an EAPOL pkt on Authenticator Q
Feb 26 20:03:09.099: dot1x-packet:EAPOL pak rx - Ver: 0x1  type: 0x0
Feb 26 20:03:09.099: dot1x-packet: length: 0x0008
Feb 26 20:03:09.099: dot1x-ev:[Gi0/9] Dequeued pkt: Int Gi0/9 CODE= 2,TYPE= 1,LEN= 8
```

IBNS Debugging

```
Feb 26 20:03:10.696  dot1x-ev:[685b.35ab.ac5f, Gi0/9] Received Authz Success for the client 0xDE000006 (685b.35ab.ac5f)
Feb 26 20:03:10.703: dot1x-sm:[685b.35ab.ac5f, Gi0/9  Posting AUTHZ_SUCCESS on Client 0xDE000006
Feb 26 20:03:10.703: dot1x_auth Gi0/9: during state auth_authc_result, got event 23(authzSuccess)
Feb 26 20:03:10.703: @@@ dot1x_auth Gi0/9: auth_authc_result -> auth_authenticated
Feb 26 20:03:10.703: dot1x-sm:[685b.35ab.ac5f, Gi0/9] 0xDE000006:entering authenticated state
```



Verification Commands

- show access-session
- show access-session interface <interface name> [detail]

IBNS Debugging

```
switch# show access-session interface GigabitEthernet 0/9 details
         Interface:  GigabitEthernet0/9
         MAC Address:  685b.35ab.ac5f
        IPv6 Address:  Unknown
        IPv4 Address:  192.168.1.178
          User-Name:  sam
             Status:  Authorized
             Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  3600s (local), Remaining: 2940s
      Timeout action:  Reauthenticate
     Restart timeout:  N/A
Periodic Acct timeout:  N/A
      Session Uptime:  661s
   Common Session ID:  C0A80182000008BC3F196453
     Acct Session ID:  0x000008B0
              Handle:  0x81000006
      Current Policy:  POLICY

Server Policies:
     Security Policy:  None
     Security Status:  Link Unsecure

Method status list:
     Method          State

     dot1x           Authc Success
```

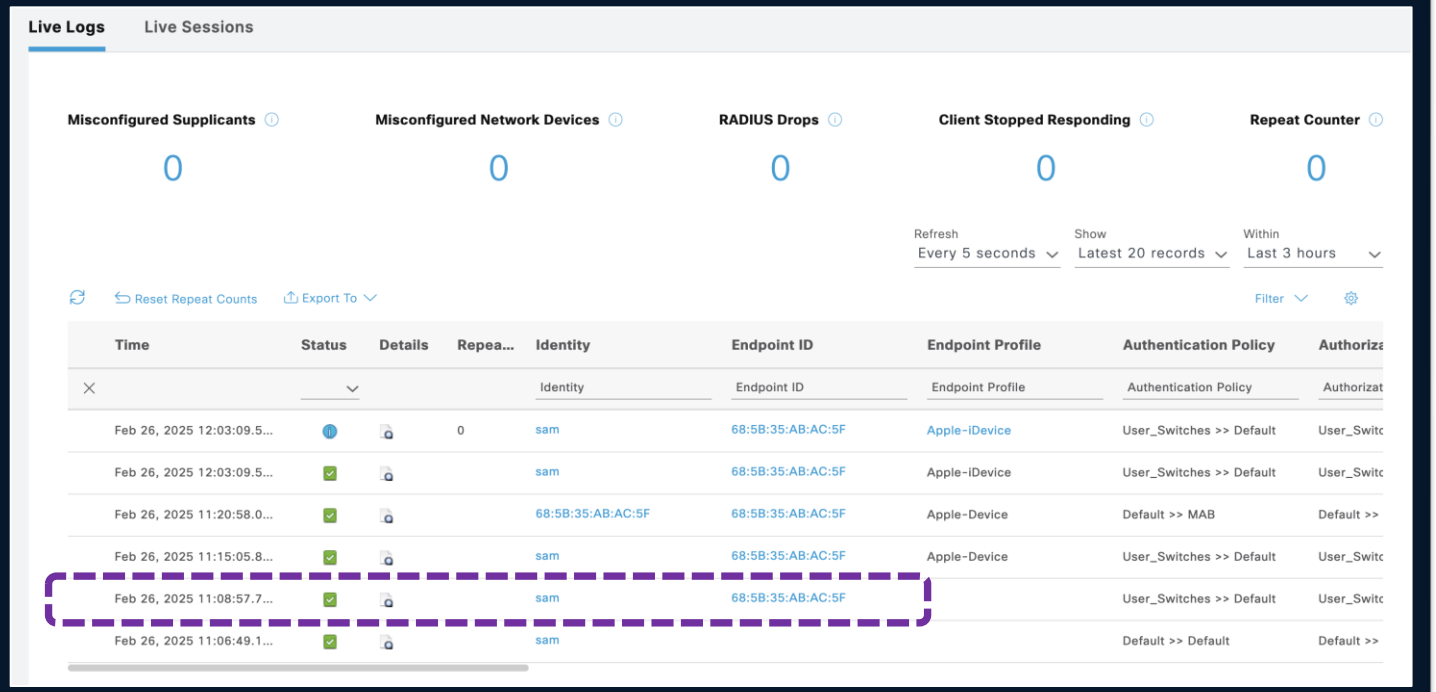
Dot1x events:

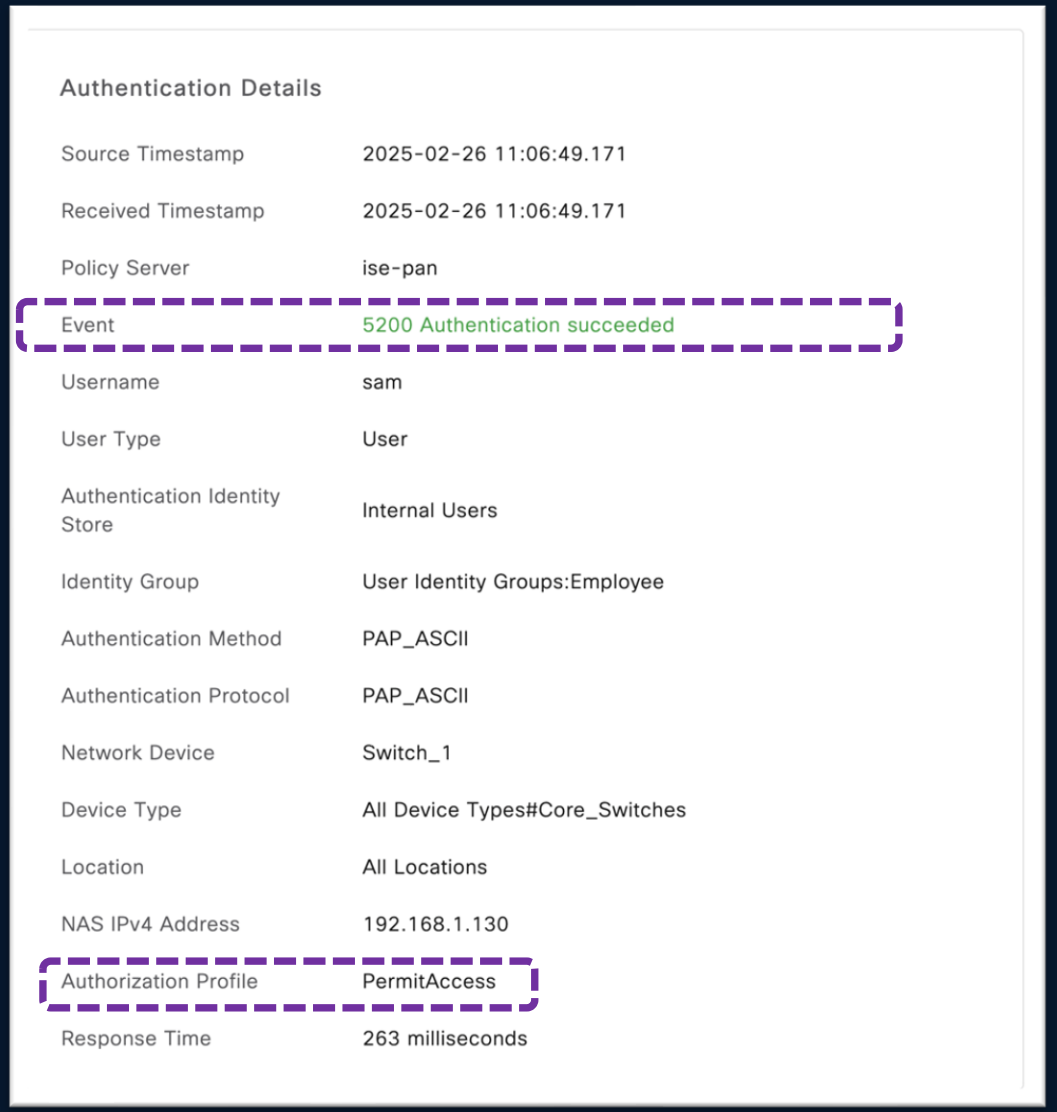
```
dot1x-ev:[685b.35ab.ac5f, Gi0/9]
```

Interface Template:

```
switch(config-template)# access-session host-mode multi-domain
switch(config-template)# service-policy type control subscriber POLICY
```

ISE Server Output





Automated Deployment Plans

Ansible Automation

- Ansible is an easy-to-use tool that allows the administrator to utilize YAML formatted ”playbook” files to apply configuration changes to Cisco IOS devices.

Ansible: Cisco ios_config module

/ Collection Index / Collections in the Cisco Namespace / Cisco.Ios / cisco.ios.ios_config module – Module to manage configuration sections.

This is the **latest** (stable) Ansible community documentation. For Red Hat Ansible Automation Platform subscriptions, see Life Cycle for version details.

cisco.ios.ios_config module – Module to manage configuration sections.

Note

This module is part of the cisco.ios collection (version 9.1.0).

You might already have this collection installed if you are using the `ansible` package. It is not included in `ansible-core`. To check whether it is installed, run `ansible-galaxy collection list`.

To install it, use: `ansible-galaxy collection install cisco.ios`.

To use it in a playbook, specify: `cisco.ios.ios_config`.

New in cisco.ios 1.0.0

- Synopsis
- Parameters
- Notes
- Examples
- Return Values

Synopsis

- Cisco IOS configurations use a simple block indent file syntax for segmenting configuration into sections. This module provides an implementation for working with IOS configuration sections in a deterministic way.

- Works on IOS, and IOS XE
- Main parameters are **lines**, and **parents**.
- Can be applied to many devices at once.

Ansible: Cisco ios_config module (cont.)

```
- name: enable 802.1x Engine
  cisco.ios.ios_config:
   lines:
      - dot1x system-auth-control
```

```
- name: class-map AAA_SVR_DOWN_HOST
  cisco.ios.ios_config:
   lines:
        - match result-type aaa-timeout
        - match authorization-status authorized
    parents : class-map type control subscriber match-all AAA_SVR_DOWN_HOST
```

```
- name: policy-map
  cisco.ios.ios_config:
   lines:
        - class-map AAA_SVR_DOWN_HOST
    parents : policy-map type control subscriber POLICY
```

Ansible jinja2 Template

```
! Basic configuration template for Cisco IOS

! Enable dot1x
dot1x system-auth-control

! Service Template
service-template {{ guest_data_segment }}
 description Enter a description
 vlan {{ restricted_VLAN }}
service-template {{ guest_voice_segment}}
 voice vlan
....
```


```
.....
! Interface Template
template {{ template_name_corp }}
 dot1x pae authenticator
 switchport mode access
 mab
 access-session host-mode {{ host_mode }}
 access-session port-control auto
 authentication periodic
 service-policy type control subscriber {{ policy_name }}
.....
```

Ansible Jinja2 Template Class, and Policy Map

```
.....
! Class-maps Template
class-map type control subscriber match-all AAA_SVR_DOWN_HOST
 match result-type aaa-timeout
 match authorization-status authorized
class-map type control subscriber match-all DOT1X
 match method dot1x
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
class-map type control subscriber match-any IN_CRITICAL_VLAN
 match activated-service-template {{ guest_data_segment }}
 match activated-service-template {{ guest_voice_segment }}
....
```

```
.....
! Policy-maps Template
policy-map type control subscriber POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template {{ guest_data_segment }}
   20 activate service-template {{ guest_voice_segment }}
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_HOST do-until-failure
   10 pause reauthentication
   20 authorize
....
```

Ansible Jinja2 Template Statements

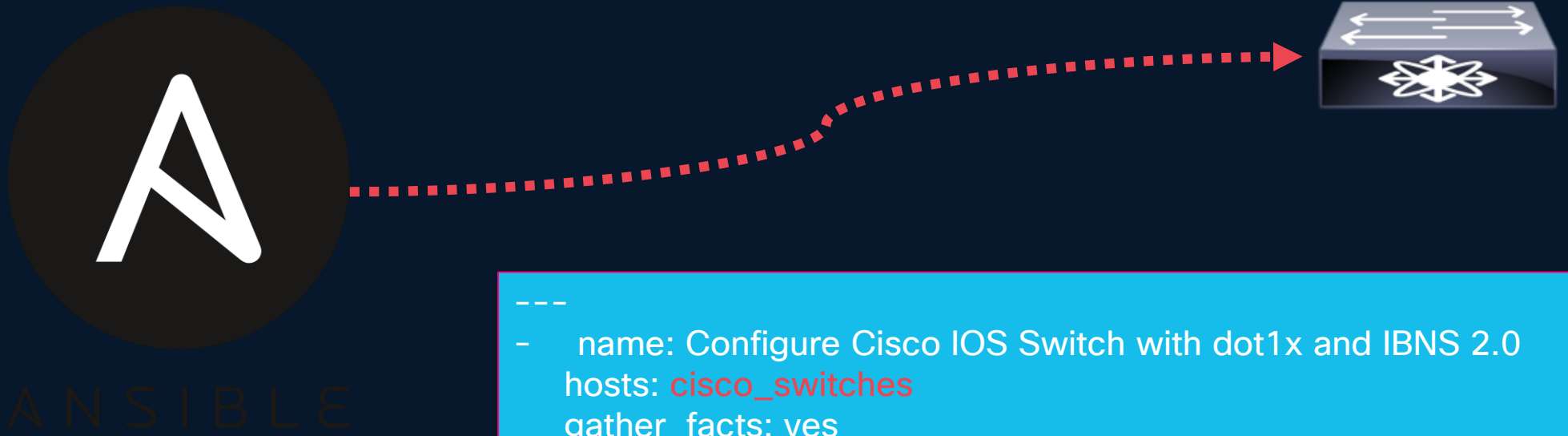
```
.....
! DOT1X Port Configuration for Range GigabitEthernet0/9 to GigabitEthernet0/12
{% for port in dot1x_ports %}
interface {{ port }}
source template {{ template_name_corp }}
{% endfor %}
....
```

- Jinja2 statements always start and end with:
  {% ... %}

- The **“set_fact”** Ansible module, allows setting variables associated to the current host(s).

```
tasks:
  - name: Generate list of interfaces
    set_fact:
      dot1x_ports:
        - "GigabitEthernet0/9"
        - "GigabitEthernet0/10"
        - "GigabitEthernet0/11”
        - "GigabitEthernet0/12"
```

Convert Jinia2 to Text file, and Apply



Make sure to apply “**set_fact**” as the first task.

```
---
-    name: Configure Cisco IOS Switch with dot1x and IBNS 2.0
     hosts: cisco_switches
     gather_facts: yes

     tasks:
       - name: Generate Cisco switch configuration from Jinja2 template
         template:
             src: "cisco_ios_switch_config.j2"
             dest: "/home/sam/{{ inventory_hostname }}_config.txt"

       - name: Apply configuration to Cisco IOS Switch
         ios_config:
             src: "/home/sam/{{ inventory_hostname }}_config.txt"
```

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: rleivaoc@cisco.com

Thank you


CISCO