Implementing Aruba Campus Access

LAB GUIDE

EDU-ICAC-RLABS-v23.11

Implementing Aruba Campus Access

Open Source Code
Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License ("GPL"),GNU Lesser General Public License ("LGPL"), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice
The use of Aruba Networks, Inc. switching platforms and software, by all individualsor corporations, to terminate other vendors' VPN client devices constitutes completeacceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty
This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORTTERMS AND CONDITIONS.
Altering this device (such as painting it) voids the warranty.

SKU: EDU-ICAC-RLABS-v23.11

January 2023

Implementing Aruba Campus Access

LAB GUIDE TABLE OF CONTENTS

Lab 01.01 Testing Remote Lab Connectivity

Overview

The Aruba Training Lab provides the equipment you need to complete several lab activities. You should know the purpose and access procedures for this equipment.

- **MGMT PC**: This client is used for remote lab management access, traffic analysis, and to access the switch's CLI via SSH.
- **PC-1:** This client is used connectivity testing. It has a wired and wireless NIC.
- **PC-4**: This client is used connectivity testing. It has a wired and wireless NIC.
- **Edge-1 switch**: This is one of your access switches, named sw-edge1.
- **Edge-2 switch**: This is one of your access switches, named sw-edge2.
- **Agg-1 switch**: This is the primary aggregation switch, named sw-agg1.
- **Agg-2 switch**: This is the secondary aggregation switch, named sw-agg2.
- **AP-1**: This is the first AP, connected to your sw-edge1 on port 2.
- **AP-2**: This is the second AP, connected to your sw-edge2 on port 2.
- **GW1**: This is the first gateway, connected to port 1/1/5 on the aggregation switches.
- **GW2**: This is the second gateway, connected to port 1/1/10 on the aggregation switches.
- **OOBM switch**: You have NO access to this switch, it connects the OOBM ports of the lab switches.
- **Core router**: Your aggregation switches connect with a routed connection to the Core router.
- **Windows Server**: This system will provide DHCP, DNS and NTP services for the lab devices. You have NO access to this server.
- **ClearPass server**: It is used as a AAA RADIUS server for your network environment.

Objectives

After completing this lab, you will have all needed information to support the hands-on labs in this course.

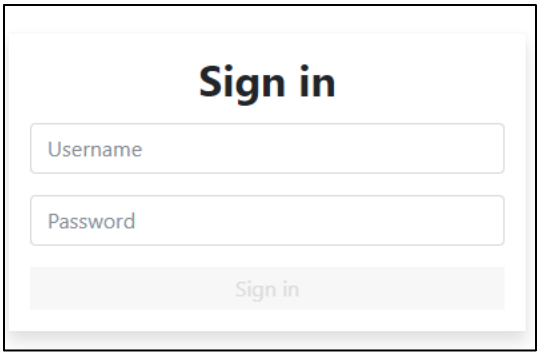
Task 1: Aruba Training Remote Lab Access

Objectives

- Validate remote lab connectivity and ability to log in.
- Ensure that you have remote lab access during this training.

Steps

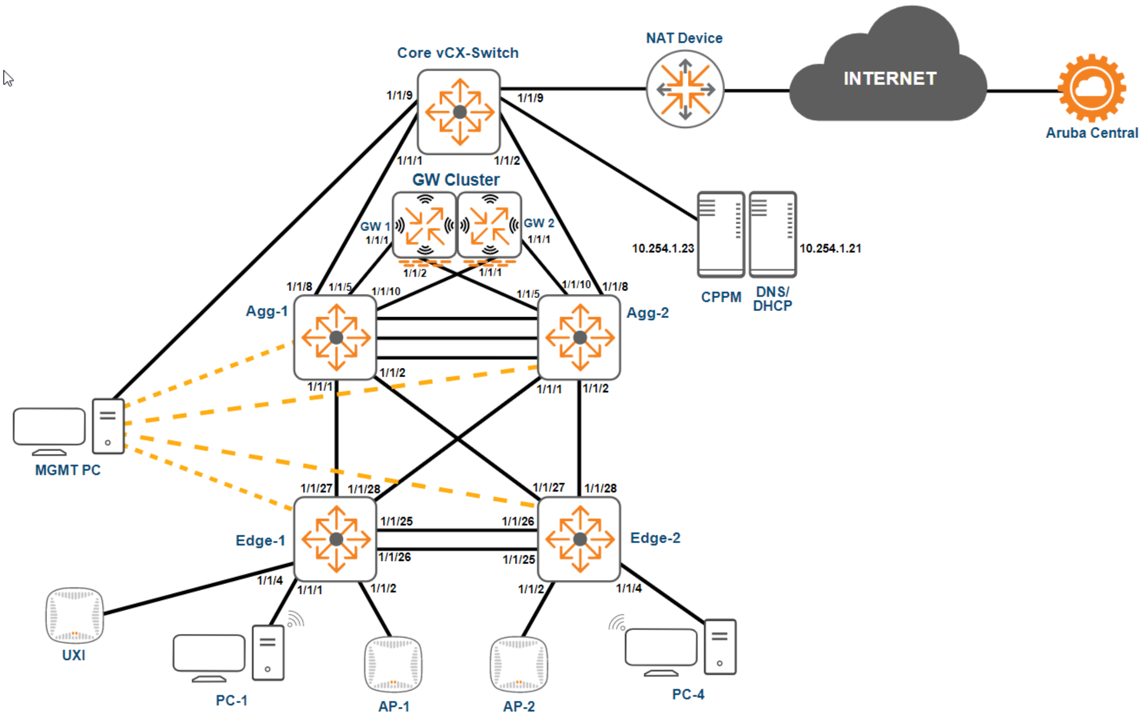
1. On your local computer, launch a web browser in Private or Incognito mode, and access the Aruba Training Lab web portal at the URL:https://arubatraininglab.computerdata.com.
2. Enter your **username** and **password** (if you do not have one, ask your instructor for the credentials), and click the **Sign in** button.



Task 2: Testing Connectivity

Objectives

- Test connectivity and authentication credentials for each of the devices.
- Working from the Aruba Training Lab diagram, connect and log into the lab devices and your client PCs.



sw-edge1 (Edge-1)

This device will be the first edge switch in your lab environment, to be named **sw-edge1**.

1. To connect to the console of the Edge-1 switch, right-click the icon in the lab diagram and select **Open Console.**
2. A new browser tab should open with a blank, black screen.
3. Press **[Enter]** a couple times, and you will see a user prompt.
4. Login using **admin** and no password.
5. It will ask you to define a new password, hit **[Enter]** twice.

NOTE: This switch is factory default at the start of the labs. A factory default switch prompts the administrator to change the password after the first login.

```
6300 login: admin
Password:


Please configure the 'admin' user account password.
Enter new password:
Confirm new password:
6300#
```

6. Take note of the switch sw-edge1 serial number and MAC address. You may also save this in a text file on your local system. When using Aruba Central, this information will be used to identify the devices.

```
show system
```

sw-edge1	
Serial Number	
MAC Address	

```
6300# show system
Hostname            : 6300
System Description  : FL.10.09.1040
System Contact      :
System Location     :

Vendor              : Aruba
Product Name        : JL666A 6300F 24G CL4 PoE 4SFP56 Sw
Chassis Serial Nbr  : SG00KN500Z
Base MAC Address    : 64e881-3f6540
ArubaOS-CX Version  : FL.10.09.1040

Time Zone           : UTC

Up Time             : 4 days, 20 hours, 29 minutes
CPU Util (%)        : 10
Memory Usage (%)    : 23
```

sw-edge2 (Edge-2)

This device will be the second edge switch in your lab environment, to be named **sw-edge2**.

7. To connect to the console of the Edge-2 switch, right-click the icon in the lab diagram and select **Open Console.**
8. A new browser tab should open with a blank, black screen.
9. Press **[Enter]** a couple times, and you will see a user prompt.

NOTE: This switch has been pre-configured in the remote lab environment;

you must connect using the correct credentials – see the next step.

10. Login using **admin** and password **Aruba123!**

IMPORTANT: For ease of use we use a simple password in the lab (Aruba123!), please **never** use a simple password in real life!

```
login: admin
Password:
```

11. Take note of the switch sw-edge2 serial number and MAC address. You may also save this in a text file on your local system.

```
show system
```

sw-edge2	
Serial Number	
MAC Address	

Aggregation Switches

These devices will be the primary and secondary aggregation switches in your campus lab environment. They will be named **sw-agg1** and **sw-agg2**.

12. To connect to the console of the **agg-1** switch, right-click the icon in the lab diagram and select **Open Console.**
13. Press **[Enter]** a couple times, login with username **admin**, password **Aruba123!**
14. This device has been pre-configured. Verify the prompt shows **sw-agg1**.

```
sw-agg1 login: admin
Password:

sw-agg1#
```

15. Repeat the previous 3 steps for the 8325-B, the hostname should be **sw-agg2**.

```
sw-agg2 login: admin
Password:

sw-agg2#
```

NOTE: You don't need to record the serial and MAC address of the aggregation switches - they will be automatically provisioned with the correct configuration.

GW1 and GW2

There are two gateways in your lab setup. The gateways are factory default at the start of the training labs.

16. To connect to the console of the GW1, right-click the icon in the lab diagram and select **Open Console.**
17. Press **[Enter]**, you should see the initial setup dialog menu.

```
Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...
    'enable-debug'      : Enable auto-provisioning debug logs
    'disable-debug'     : Disable auto-provisioning debug logs
    'full-setup'        : Start full setup dialog. Provides full customization
    'static-activate'   : Provides customization for static or PPPOE ip assignment.
Uses activate for master information

Enter Option (partial string is acceptable):
```

18. This confirms the gateway is in factory default state.
19. You may close the console connection.
20. Repeat the previous 4 steps for GW2.

AP1 and AP2

There are two APs in your lab setup. These APs are factory default at the start of the training labs. In the next steps you will make an inventory with the MAC address and serial number of both APs. This will make it easier in later labs to identify each AP either on the switch or in Aruba Central.

You will take note of the AP MAC using the console connection. Right after an AP starts to boot, you can press ENTER to access the **apboot** environment. In this apboot environment you can run the **mfginfo** (manufacturing information) command to see the AP MAC and serial number.

In the next procedure you will reboot the AP. Make sure to switch quickly to the AP console - you will need to press ENTER to access the apboot within a few seconds after the AP starts to boot.

21. To connect to the console of the AP1, right-click the icon in the lab diagram and select **Open Console.**
22. Press **[Enter]** a couple times, you should see a login prompt.
23. Return to the lab dashboard, right-click AP1 again and select **reboot**.
24. Quickly switch to the web page with the AP1 console access, press **[Enter]** when you see the option to access the apboot context.

```
APBoot 2.4.0.8 (build 64221)
Built: 2018-03-28 at 20:30:14

Model: AP-303H
DRAM:  512 MiB
Flash: Detected W25Q32FV_SPI: total 4 MiB
NAND:  Detected MX35LFxGE4AB: total 128 MiB
Power: 802.3af POE
Net:   eth0
Radio: ipq4029#0, ipq4029#1
Reset: warm
FIPS:  passed

Hit <Enter> to stop autoboot:  0
apboot>
```

25. In the *apboot* context, run the **mfginfo** command and press **[Enter]**.

```
mfginfo
```

Example output: your MAC and serial will likely be different from this output.

```
apboot> mfginfo
Inventory:
Card 0: System
        Wired MAC           : 20:4c:03:c5:fc:34
        Wired MAC Count     : 4
        Date Code           : 052520
        Serial              : CNKCK2R7R0
        Wireless MAC        : 24:62:ce:c5:b4:70
        Wireless MAC Count  : 2
        Country             : CCODE-US-b69c719895e67525a096729da53abcb37ee4b837
Card 1: CPU
        Assembly            : 2010258C
        Serial              : Y105810DA
        Date Code           : 051320
        Major Rev           : 02
        Minor Rev/Variant   : 00
Card 2: Power
        Assembly            : 2010259C
        Serial              : Y105803B8
        Date Code           : 051320
        Major Rev           : 02
        Minor Rev/Variant   : 00
apboot>
```

26. Take note of the serial number and MAC address:

AP1	
Serial Number	
MAC Address	

27. After you have noted the serial and MAC address, you can enter the **reset** command to reboot the AP.

```
reset
```

```
apboot> reset
resetting ...
```

NOTE: Even if you don't run any command, the AP will reboot automatically after a few minutes.

28. Repeat the previous procedure for AP2 and take note of the serial number and MAC address:

AP2	
Serial Number	
MAC Address	

MGMT PC, PC-1 and PC-4

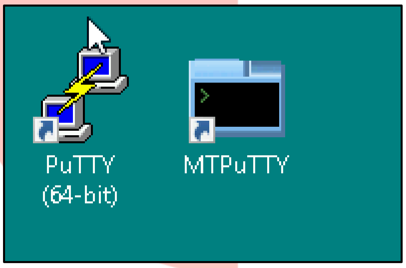
The MGMT PC is used for device management access. The PC1 and PC4 will be used as lab test-hosts for wired and wireless access.

29. To access the desktop MGMT PC, right-click the icon in the lab diagram and select **Open Desktop**.
30. A new browser tab will open with the remote desktop.
31. Repeat the previous 2 steps on **PC-1** and **PC-4**.

Core-router (via MGMT PC)

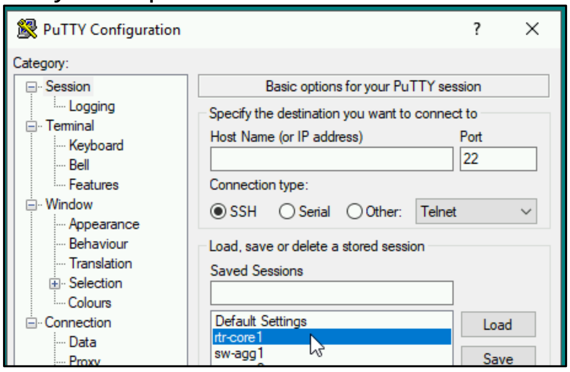
Unlike the access and aggregation switches, the core router in the remote lab is not a physical switch; it is running the AOS-CX simulator software.

32. Move back to the **MGMT PC**.
33. On the desktop, you can open Putty or MTPutty (multi-tab Putty). Either application is fine, use what works best for you (separate Putty windows or multiple tabs in MTPutty).

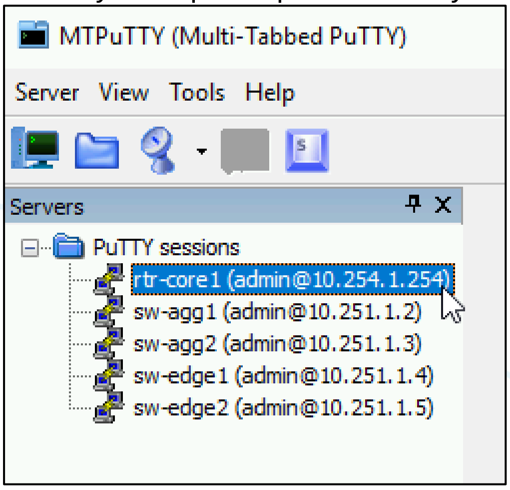


34. You will find saved sessions for **rtr-core1.**

Putty example:



MTPutty example: expand the Putty Sessions.



35. Double click the **rtr-core1** saved session to open the connection.

36. Log in using the username **admin** and password **Aruba123!**

ClearPass (via MGMT PC)

ClearPass is the AAA policy management solution in the Aruba lab environment.
The ClearPass admin Web UI can be accessed using the MGMT PC.

37. On the MGMT PC, open a web browser, Google Chrome for example, and navigate to:

https://10.254.1.23

38. You will be presented a security certificate warning.
39. Accept the warning. You will see the login page.
40. Click the **Policy Manager** icon.
41. Log in using the username **admin** and password **Aruba123!**

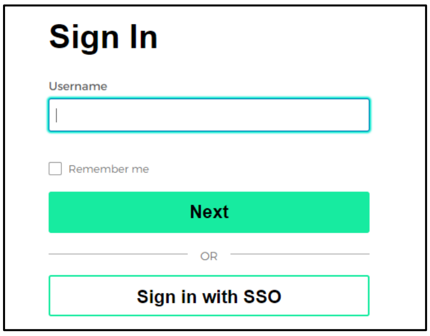
Aruba Central Access

Aruba Central is a cloud-based solution. It can be accessed with any system that has internet access.
You can access Aruba Central using your local PC internet connection.

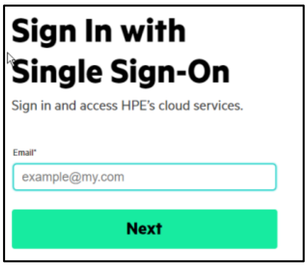
42. On your local PC, open a web browser and navigate to:

https://console.greenlake.hpe.com

43. Click Sign in with SSO.



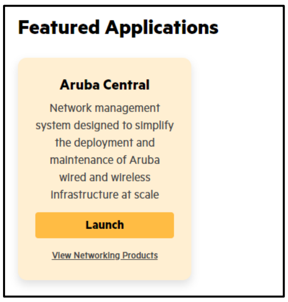
44. In the Sign In With Single Sign-On box, enter the ***username*** for HPGLCP (with the @arubatraininglabs.net suffix) and click **Next**.



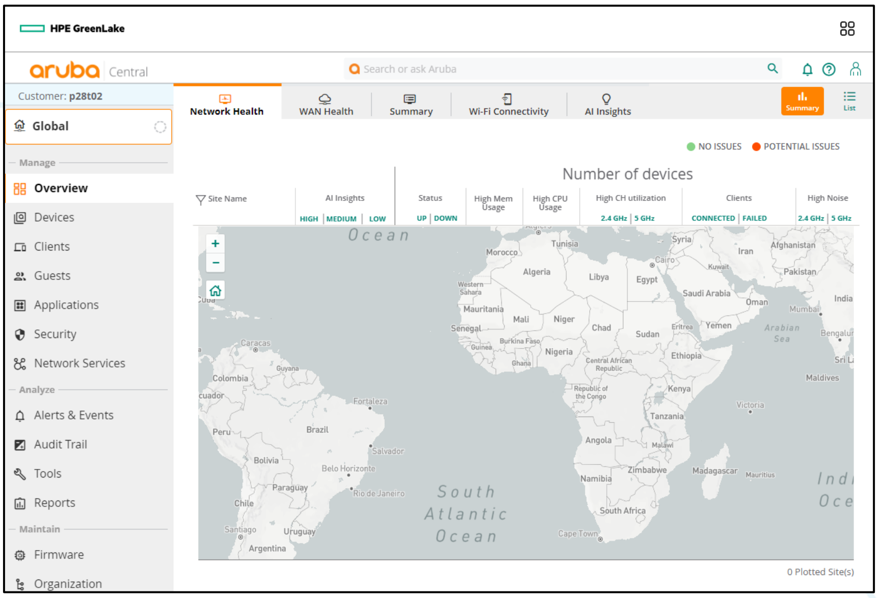
You will now be redirected to the Remote lab login page based on the arubatraininglabs.net domain name.

45. Enter the username and the password for HPE GLCP (@arubatraininglabs.net) as provided by your instructor and click **Login**.

46. After the login has completed successfully, the GLCP will present the Aruba Central application in the Featured Applications list. Click **Launch** for the Aruba Central tile.



47. This will take you to the Aruba Central **Global** > **Overview** page.



NOTE: In these steps you have seen how to access Aruba Central. In the remainder of the lab guide these steps will not be repeated. You will simply be instructed to access Aruba Central. Please refer to this task if you would need assistance with the login steps.

Review Central Device Inventory

In the next steps you will verify that your lab devices have been assigned to the current customer.

48. In Aruba Central, in the left navigation pane, click **Organization**.
49. Click **Device Preprovisioning**.
50. There should be 2 unprovisioned devices in the list, sw-agg1 and sw-agg2. The other devices will be added later.
51. This list can also be used to find the MAC address and serial information of your devices.

You have completed this lab!

Lab 02.01 Campus Wired Aggregation - VSX

Overview

In this lab you will configure the two aggregation switches with VSX.

The VSX configuration will start with the setup of the Inter Switch Link (ISL) and the VSX role configurations. Next you will explore how the VSX state and configuration synchronization works between the two VSX nodes.

To connect an edge switch with a LAG to the VSX system, you will then configure a VSX LAG.
The default gateway function will be configured using the VSX active gateway feature.

The last sections of this lab will explore the link up delay and split-brain detection configuration.

Objectives

After completing this lab, you will be able to:

- Configure the VSX ISL link.
- Configure and verify the VSX device roles and state.
- Configure and verify the VSX configuration synchronization.
- Configure the VSX LAG and active gateway.
- Review the VSX link up delay.
- Configure the VSX split brain detection.

Task 1: Review the Initial Configuration

In this task you will review the configuration that was loaded on the aggregation switches using the DHCP-based ZTP (zero touch provisioning) process.

The sw-agg1, sw-agg2 and sw-edge2 have received a configuration file from the MGMT PC.

The MGMT PC is running a TFTP and DHCP server on the OOBM (out-of-band management) network.

Sw-edge1 did not receive a ZTP configuration; you will configure sw-edge1 in these lab activities.

The OOBM network is using the IP prefix 10.251.1.0/24 and the MGMT PC has a static IP address of 10.251.1.90 in the OOBM network.

Objectives

Review the ZTP configuration.

Steps

1. Use the MGMT PC to open an SSH connection to sw-agg1 and sw-agg2.

> **NOTE:** All credentials in this training will be using **admin** / **Aruba123!** unless instructed otherwise. This will not be repeated in the remainder of the lab guide.

> **NOTE:** In some labs, Agg switches are model 8325 and Edge switches are model 6300. You may see these names in Webgate lab interface. This will not be repeated in the remainder of the lab guide.

> **NOTE:** On the MGMT PC, you can use either use Putty or MTPutty to connect to the devices.

2. On sw-agg1, review the running configuration.

```
show running-config
```

- **Question**: What is the configuration on port 1/1/8?
- **Answer**: Port 1/1/8 has a static IP address. It connects to the rtr-core1 device.
- **Question**: What is the destination for the default route configuration?
- **Answer**: IP 10.254.101.254, this is the IP address of the core-rtr1 device.

3. Attempt to ping an internet address: 8.8.8.8 for example. This should be successful.

```
ping 8.8.8.8
```

4. Repeat the previous 2 steps for sw-agg2. sw-agg2 has a default route to IP 10.254.102.254; this is the routed uplink between sw-agg2 and rtr-core1.

Task 2: VSX Basic Configuration

In this task you will configure VSX between the aggregation switches.

You will need to perform these steps:

- Prepare the ISL (Inter Switch Link)
  - Configure an LACP LAG with and ID of 256, using ports 1/1/46 and 1/1/47 between the aggregation switches
  - Allow all VLANs on LAG 256
  - Verify the LAG connection
- Configure the VSX roles
  - Set primary and secondary roles
  - Configure the system MAC address

Objectives

Perform the basic VSX Configuration

Steps

1. Using the MGMT PC, open an SSH connection to sw-agg1 and sw-agg2.
2. On both switches, enable ports 1/1/46 and 1/1/47.

```
interface 1/1/46,1/1/47
no shutdown
exit
```

3. Verify that they can see each other as LLDP neighbors.

```
show lldp neighbor-info
```

4. Configure the LAG that will be used as the ISL between sw-agg1 and sw-agg2. Try to configure this LAG by yourself. An example configuration is shown below if you are not sure.

   - Create and enable LAG256.
   - Enable LACP.
   - Configure the LAG as a switchport.
   - Configure the LAG as VLAN trunk and allow all the VLANs.
   - Assign ports 1/1/46 and 1/1/47.

```
# example configuration
interface lag 256
  no shutdown
  lacp mode active
  no routing
  vlan trunk allowed all
  exit
interface 1/1/46,1/1/47
  lag 256
  exit
```

5. Verify that the LAG members ports are in the up state.

```
show lacp interfaces
```

```
sw-agg1(config)# show lacp interfaces
State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State

1/1/46     lag256     47    1     ALFNCD  b8:d4:e7:d9:5e:00 65534  256  up
1/1/47     lag256     48    1     ALFNCD  b8:d4:e7:d9:5e:00 65534  256  up
```

Configure VSX

6. Review the default VSX status.

```
show vsx status
```

```
sw-agg1(config)# show vsx status
VSX is not configured
```

- **Question**: What is the default VSX status?
- **Answer**: VSX is disabled by default.

7. On sw-agg1, configure LAG 256 as the ISL under the VSX context.

```
vsx
 inter-switch-link lag 256
```

```
sw-agg1(config)# vsx
sw-agg1(config-vsx)# inter-switch-link lag 256
```

8. Review the VSX status.

```
show vsx status
```

```
sw-agg1(config-vsx)# show vsx status
VSX Operational State
---------------------
  ISL channel              : Init
  ISL mgmt channel         : inter_switch_link_down
  Config Sync Status       : Out-Of-Sync
  NAE                      : peer_unreachable
  HTTPS Server             : peer_unreachable

Attribute           Local               Peer
------------        --------            --------
ISL link            lag256
```

```
ISL version          2
system MAC           b8:d4:e7:d9:3d:00
Platform             8325
Software Version     GL.10.09.1040
Device Role                                     (Device roles inconsistent)
```

- **Question**: What is the status for device roles?
- **Answer**: Inconsistent. This occurs since you have not configured the primary and secondary roles.

9. On sw-agg1, under the vsx context, configure the VSX role as primary.

```
 role primary
 exit
```

```
sw-agg1(config-vsx)# role primary
sw-agg1(config-vsx)# exit
```

10. On sw-agg2, configure the ISL and role secondary.

```
vsx
 inter-switch-link lag 256
 role secondary
 exit
```

```
sw-agg2(config)# vsx
sw-agg2(config-vsx)# inter-switch-link lag 256
sw-agg2(config-vsx)# role secondary
sw-agg2(config-vsx)# exit
```

11. On sw-agg1, verify the VSX status.

```
show vsx status
```

```
sw-agg1(config-vsx)# show vsx status
VSX Operational State
---------------------
  ISL channel             : In-Sync
  ISL mgmt channel        : operational
  Config Sync Status      : In-Sync
  NAE                     : peer_unreachable
  HTTPS Server            : peer_reachable

Attribute            Local                Peer
------------         --------             --------
ISL link             lag256               lag256
ISL version          2                    2
system MAC           b8:d4:e7:d9:3d:00    b8:d4:e7:d9:ed:00
Platform             8325                 8325
Software Version     GL.10.09.1040        GL.10.09.1040
Device Role          primary              secondary
```

- **Question**: What is the status for the ISL channel?

- **Answer**: In-sync. This means the ISL protocol (ISLP) has an active connection between the primary and secondary systems.
- **Question**: What are the device roles for the local (sw-agg1) and the peer (sw-agg2)?
- **Answer**: primary and secondary.

Configure VSX System MAC

In the next steps you will configure the VSX system with a static system MAC address.

By default, VSX will use the MAC address of the primary switch. If this primary system would ever need to be replaced, the VSX MAC address would change at that time.

To prevent this and have a stable MAC address, the VSX system MAC address can be statically configured.

Typically, a MAC address from the private range is used for the VSX system MAC address.

12. On sw-agg1, configure the system MAC address.

```
vsx
 system-mac 02:01:00:00:01:00
 exit
```

```
sw-agg1(config)# vsx
sw-agg1(config-vsx)#  system-mac 02:01:00:00:01:00
sw-agg1(config-vsx)#  exit
```

13. Review the VSX status.

```
show vsx status
```

```
sw-agg1(config)# show vsx status
VSX Operational State
---------------------
  ISL channel             : In-Sync
  ISL mgmt channel        : operational
  Config Sync Status      : In-Sync
  NAE                     : peer_reachable
  HTTPS Server            : peer_reachable

Attribute           Local               Peer
------------        --------            --------
ISL link            lag256              lag256
ISL version         2                   2
system MAC          02:01:00:00:01:00   b8:d4:e7:d9:ed:00
Platform            8325                8325
Software Version    GL.10.09.1040       GL.10.09.1040
Device Role         primary             secondary
```

- **Question**: What is the system MAC for primary and secondary?
- **Answer**: Primary has the new system MAC address; the secondary is still shown with the original MAC.

14. Review the local VSX configuration in the running-config.

```
show running-config vsx
```

```
sw-agg1(config)# show running-config vsx
vsx
    system-mac 02:01:00:00:01:00
    inter-switch-link lag 256
    role primary
interface lag 256
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
interface 1/1/47
    no shutdown
    lag 256
interface 1/1/46
    no shutdown
    lag 256
```

15. When VSX is active, you can also execute **show** commands on the VSX peer device by adding the **vsx-peer** keyword to your command. Review the VSX configuration on the peer device.

```
show running-config vsx vsx-peer
```

```
sw-agg1(config)# show running-config vsx vsx-peer
vsx
    inter-switch-link lag 256
    role secondary
interface lag 256
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
interface 1/1/46
    no shutdown
    lag 256
interface 1/1/47
    no shutdown
    lag 256
```

- **Question**: What is the device role shown in this output?
- **Answer**: Secondary. Even though you are connected to sw-agg1, you received the output of the command form sw-agg2.
- **Question**: Do you see the **system-mac** command in the secondary VSX configuration?
- **Answer**: No, the command was only applied to the primary.

You will now fix this by enabling VSX configuration synchronization.

VSX Configuration Synchronization

VSX configuration synchronization can be very useful to assist in keeping the configuration of the two aggregation switches in sync.

The features that are enabled for synchronization will automatically be applied from the primary to the secondary switch.

IMPORTANT: When managing switches using Aruba Central templates, VSX sync should not be used. The template should contain the settings that need to be pushed to both VSX nodes.

IMPORTANT: Although both switch configurations are still fully accessible, you should configure the features that are enabled for VSX-sync only on the primary. Any config changes made on these synchronized features on the secondary will be lost since VSX sync will overwrite them.

16. On sw-agg1, enable **vsx-sync** for the **vsx-global** feature.

```
vsx
 vsx-sync vsx-global
 exit
```

```
sw-agg1(config)# vsx
sw-agg1(config-vsx)#  vsx-sync vsx-global
sw-agg1(config-vsx)#  exit
```

17. The VSX ISL will be re-established, use the **show vsx status** command to verify that the connection is *In-Sync* again after a few seconds.

```
show vsx status
```

```
sw-agg1(config)# show vsx status
VSX Operational State
---------------------
  ISL channel                : In-Sync
  ISL mgmt channel           : operational
  Config Sync Status         : In-Sync
  NAE                        : peer_reachable
  HTTPS Server               : peer_reachable

Attribute           Local               Peer
------------        --------            --------
ISL link            lag256              lag256
ISL version         2                   2
system MAC          02:01:00:00:01:00   02:01:00:00:01:00
Platform            8325                8325
Software Version    GL.10.09.1040       GL.10.09.1040
```

```
Device Role          primary              secondary
```

18. Review the VSX running-config on the vsx-peer.

```
show running-config vsx vsx-peer
```

```
sw-agg1(config)# show running-config vsx vsx-peer
vsx
    system-mac 02:01:00:00:01:00
    inter-switch-link lag 256
    role secondary
    vsx-sync vsx-global
interface lag 256
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
interface 1/1/46
    no shutdown
    lag 256
interface 1/1/47
    no shutdown
    lag 256
```

- **Question**: What changed in the peer configuration?
- **Answer**: The **system-mac** and **vsx-sync** commands were automatically added to the configuration on sw-agg2 as a result of the VSX sync.

Global and Context Synchronization

VSX sync can be used to selectively synchronize global features or context specific features.

Examples of a global features are STP and OSPF.

Examples of context specific features are a VLAN or ACL. Each VLAN or ACL can have the **vsx-sync** option enabled or disabled.

Example Global Feature: STP

19. On sw-agg1 and sw-agg2, review the default STP state.

```
show spanning-tree
```

```
sw-agg1(config)# show spanning-tree
Spanning-tree is disabled
```

```
sw-agg2(config)# show spanning-tree
Spanning-tree is disabled
```

- **Question**: What is the default STP state on both switches?

- **Answer**: STP is disabled.

20. On sw-agg1, enable the **stp-global** feature for VSX Synchronization.

```
vsx
 vsx-sync stp-global
 exit
```

```
sw-agg1(config)# vsx
sw-agg1(config-vsx)#  vsx-sync stp-global
sw-agg1(config-vsx)#  exit
```

21. Now define a STP root priority of 0 and enable STP.

```
spanning-tree priority 0
spanning-tree
```

```
sw-agg1(config)# spanning-tree priority 0
sw-agg1(config)# spanning-tree
```

22. Review the running configuration of the VSX peer; you should see the synchronized **spanning-tree** commands.

```
show running-config vsx-peer | include span
```

```
sw-agg1(config)# show running-config vsx-peer | include span
spanning-tree
spanning-tree priority 0
```

23. Review the STP status for both the local and peer system.

```
show spanning-tree
show spanning-tree vsx-peer
```

```
sw-agg1(config)# show spanning-tree
Spanning tree status      : Enabled Protocol: MSTP

MST0
  Root ID    Priority   : 0
             MAC-Address: 02:01:00:00:01:00
             This bridge is the root
             Hello time(in seconds):2  Max Age(in seconds):20
             Forward Delay(in seconds):15

  Bridge ID  Priority  : 0
             MAC-Address: 02:01:00:00:01:00
             Hello time(in seconds):2  Max Age(in seconds):20
             Forward Delay(in seconds):15

Port         Role           State      Cost           Priority   Type             BPDU-Tx
BPDU-Rx     TCN-Tx     TCN-Rx
------------ -------------- ---------- -------------- ---------- ---------------- --------
-- ---------- ---------- ----------
lag256       Designated     Forwarding 1              64         P2P              24
22          2          0
```

```
Number of topology changes    : 1
Last topology change occurred : 43 seconds ago
```

```
sw-agg1(config)# show spanning-tree vsx-peer
Spanning tree status      : Enabled Protocol: MSTP

MST0
  Root ID    Priority   : 0
             MAC-Address: 02:01:00:00:01:00
             This bridge is the root
             Hello time(in seconds):2  Max Age(in seconds):20
             Forward Delay(in seconds):15

  Bridge ID  Priority  : 0
             MAC-Address: 02:01:00:00:01:00
             Hello time(in seconds):2  Max Age(in seconds):20
             Forward Delay(in seconds):15

Port         Role           State      Cost           Priority   Type             BPDU-Tx
BPDU-Rx     TCN-Tx     TCN-Rx
------------ ------------- ---------- -------------- ---------- ---------------- --------
-- ---------- ---------- ----------
lag256       Designated     Forwarding 1              64         P2P              22
19         0          1

Number of topology changes    : 1
Last topology change occurred : 40 seconds ago
```

- **Question**: Is STP enabled on both switches?
- **Answer**: Yes, the config was synchronized and STP was enabled on both switches.

Example Context Feature: Enable VLAN for VSX sync

In the next steps you will enable VSX sync in a single VLAN context. You will use VLAN2 for this example.

24. On sw-agg1, create VLAN2 and enable it for VSX-sync.

```
vlan 2
name v2-vsx-routed-link
vsx-sync
exit
```

```
sw-agg1(config)# vlan 2
sw-agg1(config-vlan-2)# name v2-vsx-routed-link
sw-agg1(config-vlan-2)# vsx-sync
sw-agg1(config-vlan-2)# exit
```

25. Review the VLAN list on the local and peer systems. VLAN2 should have been synchronized with the name.

```
show vlan
show vlan vsx-peer
```

```
sw-agg1(config)# show vlan

--------------------------------------------------------------------------------
VLAN  Name                              Status  Reason   Type        Interfaces
--------------------------------------------------------------------------------
1     DEFAULT_VLAN_1                    up      ok       default     lag256
2     v2-vsx-routed-link                up      ok       static      lag256
```

```
sw-agg1(config)# show vlan vsx-peer

--------------------------------------------------------------------------------
VLAN  Name                              Status  Reason   Type        Interfaces
------------------------------------------------------------------------------------------
------------------------
1     DEFAULT_VLAN_1                    up      ok       default     lag256
2     v2-vsx-routed-link                up      ok       static      lag256
```

Attempt Local Configuration Change on Sw-agg2

You have seen that VLAN 2 has been created in the sw-agg2 configuration by VSX sync.

Now you will attempt to remove VLAN 2 on the sw-agg2.

26. On sw-agg2, remove VLAN2.

```
no vlan 2
```

```
sw-agg2(config)# no vlan 2
```

- **Question**: Did you receive an error when executing this command?
- **Answer**: No, the switch accepted the command just fine.

27. Review the VLAN list.

```
show vlan
```

```
sw-agg2(config)# show vlan

--------------------------------------------------------------------------------
VLAN  Name                              Status  Reason   Type        Interfaces
------------------------------------------------------------------------------------------
------------------------
1     DEFAULT_VLAN_1                    up      ok       default     lag256
2     v2-vsx-routed-link                up      ok       static      lag256
```

- **Question**: What do you observe?
- **Answer**: VLAN2 is still in the VLAN list.

28. Now review the last 5 entries in the event log.

```
show event -r -n 5
```

```
sw-agg2(config)# show event -r -n 5
---------------------------------------------------
Event logs from current boot
---------------------------------------------------
2022-12-18T12:31:30.162875+00:00 sw-agg2 ops-switchd[3264]:
Event|2101|LOG_INFO|AMM|1/1|VLAN 2 created in hardware
2022-12-18T12:31:30.157897+00:00 sw-agg2 vsx-syncd[3529]: Event|7602|LOG_INFO|AMM|-
|Configuration sync update : VSX configuration-sync updated database
2022-12-18T12:31:30.046992+00:00 sw-agg2 ops-switchd[3264]:
Event|2103|LOG_INFO|AMM|1/1|VLAN 2 removed from hardware
2022-12-18T12:29:43.417814+00:00 sw-agg2 ops-switchd[3264]:
Event|2101|LOG_INFO|AMM|1/1|VLAN 2 created in hardware
2022-12-18T12:29:43.412416+00:00 sw-agg2 vsx-syncd[3529]: Event|7602|LOG_INFO|AMM|-
|Configuration sync update : VSX configuration-sync updated database
```

- **Question**: What do you observe?
- **Answer**: VLAN 2 was removed from the switch, but VSX sync immediately re-created the entry.

29. On sw-agg2, attempt to change the name of VLAN2.

```
vlan 2
name test
exit
```

```
sw-agg2(config)# vlan 2
sw-agg2(config-vlan-2)# name test
sw-agg2(config-vlan-2)# exit
```

30. Review the VLAN list.

```
show vlan
```

```
sw-agg2(config)# show vlan

-------------------------------------------------------------------------------
VLAN  Name                                Status  Reason    Type         Interfaces
-------------------------------------------------------------------------------------------
------------------------
1     DEFAULT_VLAN_1                      up      ok        default      lag256
2     v2-vsx-routed-link                  up      ok        static       lag256
```

- **Question**: Did the VLAN name change?
- **Answer**: No, the name was immediately re-synchronized from the primary.

NOTE: If this would have been an ACL rule, you may believe that the switch has a defect since it accepted your commands, but the ACL did not get updated. If you notice such behavior, make sure to check if VSX sync is enabled for the object.

31. On sw-agg1, create VLANs 3-4,11-15 and 21-25 and enable **vsx-sync**.

```
vlan 3,4,11-15,21-25
vsx-sync
exit
```

```
sw-agg1(config)# vlan 3,4,11-15,21-25
sw-agg1(config-vlan-<3,4,11-15,21-25>)# vsx-sync
sw-agg1(config-vlan-<3,4,11-15,21-25>)# exit
```

Config Sync Errors

Sometimes configuration elements depend on other elements. VSX sync attempts to sync the feature that you have enabled for sync, but it will not automatically fix dependencies.

In the next steps you will see an example of a failed VSX configuration synchronization.

32. On sw-agg1, create a new class with name **any**.

```
class ip any
 match ip any any
 exit
```

```
sw-agg1(config)# class ip any
sw-agg1(config-class-ip)#  match ip any any
sw-agg1(config-class-ip)#  exit
```

33. Now use it in a policy with name **mirror**. This command will only work when the class with name *any* exists; the command refers to the class (reference).

```
policy mirror
 class ip any
```

```
sw-agg1(config)# policy mirror
sw-agg1(config-policy)#  class ip any
```

34. Now enable VSX configuration synchronization for the policy.

```
vsx-sync
exit
```

```
sw-agg1(config-policy)#  vsx-sync
sw-agg1(config-policy)#  exit
```

VSX sync will now attempt to push the policy commands to the sw-agg2; but since the class does not exist, this will fail.

35. Review the VSX status.

```
show vsx status
```

```
sw-agg1(config)# show vsx status
VSX Operational State
```

```
---------------------
  ISL channel              : In-Sync
  ISL mgmt channel         : operational
  Config Sync Status       : configuration_sync_missing_reference
  NAE                      : peer_reachable
  HTTPS Server             : peer_reachable

Attribute           Local               Peer
------------        --------            --------
ISL link            lag256              lag256
ISL version         2                   2
system MAC          02:01:00:00:01:00   02:01:00:00:01:00
Platform            8325                8325
Software Version    GL.10.09.1040       GL.10.09.1040
Device Role         primary             secondary
```

- **Question**: What is the Config sync status?
- **Answer**: The status reports a missing reference. This is a generic error, when you see this status, you will need to review the configurations to detect what configuration that is missing in the peer configuration.

The first useful command is **show running-config vsx-sync**. This output will show all the configuration items that are enabled for VSX synchronization.

36. On sw-agg1, review the configuration items that are marked for synchronization.

```
show running-config vsx-sync
```

```
sw-agg1(config)# show running-config vsx-sync
Current vsx-sync configuration:
!
!Version ArubaOS-CX GL.10.09.1040
!export-password: default
policy mirror
    vsx-sync
    !
    10 class ip any
vlan 2
    name v2-vsx-routed-link
    vsx-sync
vlan 3
    vsx-sync
...
```

- **Question**: Is the policy named “mirror” you just configured part of the config that is synchronized by VSX?
- **Answer**: Yes.
- **Question**: Is the class named “any” part of the synced config?
- **Answer**: No, it was not enabled for vsx-sync.

37. Now review the differences between the local switch configuration and the peer VSX switch.

```
show running-config vsx-sync peer-diff
```

```
sw-agg1(config)# show running-config vsx-sync peer-diff
--- /tmp/running-config-vsx.276e
+++ /tmp/peer-running-config-vsx.276e
@@ -5,7 +5,6 @@
 policy mirror
     vsx-sync
     !
-    10 class ip any
 vlan 2
     name v2-vsx-routed-link
     vsx-sync
```

- **Question**: What do you observe in the output?

- **Answer**: There is one line marked with a minus sign under the policy: *class ip any*. This indicates that there was a problem to execute this command on the peer switch. Note that only the lines with + or – signs are different in the configurations. The lines displayed before and after are only intended to give you context around the different command.

38. On sw-agg2, configure the policy *mirror* and attempt to execute the missing command manually.

```
policy mirror
 class ip any
 exit
```

```
sw-agg2(config)# policy mirror
sw-agg2(config-policy)#  class ip any
% Class does not exist.
sw-agg2(config-policy)#  exit
```

- **Question**: What is the reported error message?

- **Answer**: The switch reports that the class does not exist. This tells you that the class still needs to be created locally or enabled for VSX sync.

39. On sw-agg1, enable VSX sync for the *class ip any*.

```
class ip any
vsx-sync
exit
```

```
sw-agg1(config)# class ip any
sw-agg1(config-class-ip)# vsx-sync
sw-agg1(config-class-ip)# exit
```

40. Review the VSX status

```
show vsx status
```

```
sw-agg1(config)# show vsx status
VSX Operational State
```

```
---------------------
  ISL channel                : In-Sync
  ISL mgmt channel           : operational
  Config Sync Status         : In-Sync
  NAE                        : peer_reachable
  HTTPS Server               : peer_reachable

Attribute           Local               Peer
------------        --------            --------
ISL link            lag256              lag256
ISL version         2                   2
system MAC          02:01:00:00:01:00   02:01:00:00:01:00
Platform            8325                8325
Software Version    GL.10.09.1040       GL.10.09.1040
Device Role         primary             secondary
```

- **Question**: What is the reported config-sync status?
- **Answer**: In-Sync.

41. Review the running configuration vsx-sync peer-diff.

```
show running-config vsx-sync peer-diff
```

```
sw-agg1(config)# show running-config vsx-sync peer-diff
--- /tmp/running-config-vsx.276e
+++ /tmp/peer-running-config-vsx.276e
@@ -6,6 +6,8 @@
     vsx-sync
     !
     10 match any any any
+! policy mirror user configuration does not match active configuration.
+! run 'policy NAME reset' to reset policy to match active configuration.
 policy mirror
     vsx-sync
     !
```

- **Question**: What do you observe?
- **Answer**: There are no configuration commands missing, but there is a note (!) about the difference between the actual state and the configuration.

  +! policy mirror user configuration does not match active configuration.

  +! run ‘policy NAME reset’ to reset policy to match active configuration.

42. On sw-agg2, review that this note is also shown in the running-configuration.

```
show running-config
```

```
...
class ip any
    vsx-sync
    !
    10 match any any any
! policy mirror user configuration does not match active configuration.
```

```
! run 'policy NAME reset' to reset policy to match active configuration.
policy mirror
    vsx-sync
    !
    10 class ip any
...
```

43. Reset the policy *mirror*. This command will initiate the application of the policy in hardware again. Note that this command must be entered in configuration mode!

```
policy mirror reset
```

```
sw-agg2(config)# policy mirror reset
```

44. On sw-agg1, check the peer differences again.

```
show running-config vsx-sync peer-diff
```

```
sw-agg1(config)# show running-config vsx-sync peer-diff
No difference in configs.
```

- **Question**: What is the current diff status?
- **Answer**: There are no more differences between the 2 switches.

Task 3: Configure a VSX LAG

In this task you will configure a layer 2 multi-chassis LAG (MC-LAG) between the VSX switches and the edge switches. This is known as a VSX LAG in an Aruba AOS-CX setup. The configuration is performed using MC-LAG commands, and the terms MC-LAG and VSX LAG refer to the same feature.

The VSX system will assume the same LACP system ID for the primary and secondary VSX systems. This ensures that the peer device believes it is connected to the same neighbor switch and it will have active-active layer 2 links in the LAG.

VSX will use the VSX system MAC address as the LACP system ID.

In this task you will define a new VSX LAG to sw-edge2. This switch has been configured already by the ZTP initial setup.

Objectives

- Configure a VSX LAG.

Steps

1. Access the MGMT PC and open an SSH connection to both sw-agg1 and sw-agg2.
2. On sw-agg1, create a new LAG with and ID of 2; make sure to use the **multi-chassis** keyword.

```
interface lag 2 multi-chassis
```

```
sw-agg1(config)# interface lag 2 multi-chassis
sw-agg1(config-lag-if)#
```

- **Question**: What would happen if you did not include the **multi-chassis** keyword?
- **Answer**: A local LAG would be created on sw-agg1, but the status of the member ports would not be synchronized with the VSX peer. An example of a local LAG is LAG 256. Each VSX switch will locally handle the two member ports for LAG 256.

3. Review the current configuration of the LAG.

```
show running-config current-context
```

```
sw-agg1(config-lag-if)# show running-config current-context
interface lag 2 multi-chassis
    no routing
    vlan access 1
    lacp mode active
```

- **Question**: What do you observe?
- **Answer**: When creating an MC-LAG, the LAG is automatically a switched port (no routing) and by default it is active for LACP.
- **Question**: Does this mean you cannot configure a non-LACP (static) MC-LAG?
- **Answer**: No. A static MC-LAG can be configured using the command **interface lag 2 multi-chassis static**. However, the Aruba best practice is to configure LACP enabled LAGs.

4. Configure the LAG as VLAN trunk and allow VLANs 1,3-4,11-15,21-25.

```
 vlan trunk allowed 1,3-4,11-15,21-25
```

```
sw-agg1(config-lag-if)# vlan trunk allowed 1,3-4,11-15,21-25
```

NOTE: Do not configure VLAN allow all on the LAG to the edge switches. VLAN 2 is intended as routed VLAN between the primary and secondary and should only exist on the LAG256 between the 2 switches.

5. Enable the LAG.

```
 no shutdown
 exit
```

```
sw-agg1(config-lag-if)# no shutdown
```

6. Assign port 1/1/2 to LAG2, enable the port.

```
interface 1/1/2
 lag 2
 no shutdown
 exit
```

```
sw-agg1(config)# interface 1/1/2
sw-agg1(config-if)#  lag 2
sw-agg1(config-if)#  no shutdown
sw-agg1(config-if)#  exit
```

7. Use the MGMT PC to open an SSH connection to sw-edge2.

Sw-edge2 has been pre-configured with an LACP LAG on ports 1/1/27 and 1/1/28.

8. Review the LAG configuration and the member ports.

```
show running-config interface lag 256
```

```
sw-edge2# show running-config interface lag 256
interface lag 256
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 1,3-4,11-15,21-25
    lacp mode active
    exit
```

```
show running-config interface 1/1/27,1/1/28
```

```
sw-edge2# show running-config interface 1/1/27,1/1/28
interface 1/1/27
    no shutdown
    description sw-agg1
```

```
    lag 256
    exit
interface 1/1/28
    no shutdown
    description sw-agg2
    lag 256
    exit
```

9. Review the LACP status.

```
show lacp interfaces
```

```
sw-edge2# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
-------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
-------------------------------------------------------------------------------
1/1/27     lag256     28    1     ALFNCD  64:e8:81:3f:b5:00 65534  256  up
1/1/28     lag256                                                       down


Partner details of all interfaces:
-------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
-------------------------------------------------------------------------------
1/1/27     lag256     2     1     ALFNCD  02:01:00:00:01:00 65534  2
```

- **Question**: What is the status of the interfaces 1/1/27 and 1/1/28?
- **Answer**: Port 1/1/27 is connected to port 1/1/2 on sw-agg1. The status is up.
- **Question**: What is the LACP Partner System ID?
- **Answer**: The LACP partner System ID is the system MAC of the VSX system.

10. Review the LLDP neighbors

```
show lldp neighbor-info
```

```
sw-edge2# show lldp neighbor-info

LLDP Neighbor Information
=========================

Total Neighbor Entries          : 3
Total Neighbor Entries Deleted  : 4
```

```
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 4

LOCAL-PORT  CHASSIS-ID         PORT-ID       PORT-DESC     TTL      SYS-NAME
-------------------------------------------------------------------------------
...
1/1/27      b8:d4:e7:d9:3d:00  1/1/2         1/1/2         120      sw-agg1
...
```

- **Question**: What is the Chassis-id on the port 1/1/27?
- **Answer**: The base system MAC of sw-agg1 is reported as the Chassis ID.
- **Question**: Why is the VSX system MAC address not used for the Chassis ID?
- **Answer**: The VSX system MAC address is only used for services that are shared between the VSX switches, such as STP state and VSX LAG states. LLDP is a local protocol and will use the base system MAC address.

Configure the VSX LAG on sw-agg2

In the next steps you will configure the same VSX LAG on sw-agg2. The result will be that sw-edge2 has both links in the LAG active and believes it is connected to the same LACP peer.

11. On sw-agg2, create the MC-LAG LAG2.

```
interface lag 2 multi-chassis
```

```
sw-agg2(config)# interface lag 2 multi-chassis
```

12. Review the current port configuration.

```
show running-config current
```

```
sw-agg2(config-lag-if)# show running-config current
interface lag 2 multi-chassis
    no routing
    vlan access 1
    lacp mode active
```

- **Question**: On sw-agg1, you have configured the LAG as a VLAN trunk. Why are these commands not shown on the sw-agg2?
- **Answer**: MC-LAG configuration synchronization is not enabled yet.

13. On sw-agg1, enable vsx-sync for mclag-interfaces.

```
vsx
 vsx-sync mclag-interfaces
 exit
```

```
sw-agg1(config)# vsx
sw-agg1(config-vsx)#  vsx-sync mclag-interfaces
```

```
sw-agg1(config-vsx)#  exit
```

14. On sw-agg2, review the current port configuration again.

```
show running-config current
exit
```

```
sw-agg2(config-lag-if)# show running-config current
interface lag 2 multi-chassis
    no routing
    vlan trunk native 1
    vlan trunk allowed 1,3-4,11-15,21-25
    lacp mode active
sw-agg2(config-lag-if)# exit
```

- **Question**: Is the port configured as VLAN trunk now?
- **Answer**: Yes, the VSX sync has pushed the VLAN commands to the sw-agg2.

15. On sw-agg2, assign port 1/1/2 to lag 2 and enable the port.

```
interface 1/1/2
 lag 2
 no shutdown
 exit
```

```
sw-agg2(config)# interface 1/1/2
sw-agg2(config-if)#  lag 2
sw-agg2(config-if)#  no shutdown
sw-agg2(config-if)#  exit
```

- **Question**: Why is the physical port membership not synchronized by VSX sync?
- **Answer**: While it is a best practice to use the same physical ports on both VSX members for a VSX LAG, each member can be configured with a unique local set of physical ports. The physical port(s) must be manually assigned to the VSX LAG on each member.

16. On sw-agg2, review the LACP interface status.

```
show lacp interfaces
```

```
sw-agg2(config)# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
---------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
---------------------------------------------------------------------------------
1/1/2      lag2(mc)                                                     down
```

```
1/1/46     lag256     47    1     ALFNCD  b8:d4:e7:d9:ed:00 65534  256  up
1/1/47     lag256     48    1     ALFNCD  b8:d4:e7:d9:ed:00 65534  256  up


Partner details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
------------------------------------------------------------------------------
1/1/2      lag2(mc)
1/1/46     lag256     47    1     ALFNCD  b8:d4:e7:d9:3d:00 65534  256
1/1/47     lag256     48    1     ALFNCD  b8:d4:e7:d9:3d:00 65534  256
```

- **Question**: What is the lag2 status?
- **Answer**: The status is *down*. In the next steps you will investigate this.

Attempt to Troubleshoot Why the Port is Down

Attempt by yourself to discover why the LAG2 is currently down.

Command hints in case you are not sure where to start:

```
show interface brief
show interface 1/1/2
show interface lag2
```

```
sw-agg2(config)# show interface brief
------------------------------------------------------------------------------------------
--------------------
Port   Native Mode   Type     Enabled Status  Reason          Speed   Description
       VLAN                                                   (Mb/s)
------------------------------------------------------------------------------
...
1/1/2  1      trunk  SFP+DAC1 yes     down   Administratively down  --    --
...
lag2   1      trunk  --       no      down                          auto  --
...
```

```
sw-agg2(config)#    show interface 1/1/2

Interface 1/1/2 is down
 Admin state is up
 State information: Administratively down
...
```

```
sw-agg2(config)# show interface lag2

Aggregate lag2 is down
 Admin state is down
 State information : Admin state is down
```

```
...
```

- **Question**: What do you observe?
- **Answer**: The LAG interface was still administratively down. This results in the member port status of *admin down*.

Adjust the Configuration

17. On sw-agg2, enable the LAG2.

```
interface lag 2
 no shutdown
 exit
```

```
sw-agg2(config)# interface lag 2
sw-agg2(config-lag-if)#  no shutdown
sw-agg2(config-lag-if)#  exit
```

- **Question**: Didn't you enable VSX sync for the LAG?
- **Answer**: Yes, VSX sync will synchronize the VLAN and other configuration items on the VSX LAG, but the port status is always controlled locally on each member. This allows for troubleshooting connections without having to break the VSX sync.

18. Verify the LACP status. Port 1/1/2 should be in the up state now.

```
show lacp interfaces
```

```
sw-agg2(config)# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
------------------------------------------------------------------------------
1/1/2      lag2(mc)   1002  1     ALFNCD  02:01:00:00:01:00 65534  2    up
1/1/46     lag256     47    1     ALFNCD  b8:d4:e7:d9:ed:00 65534  256  up
1/1/47     lag256     48    1     ALFNCD  b8:d4:e7:d9:ed:00 65534  256  up


Partner details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
------------------------------------------------------------------------------
1/1/2      lag2(mc)   29    1     ALFNCD  64:e8:81:3f:b5:00 65534  256
1/1/46     lag256     47    1     ALFNCD  b8:d4:e7:d9:3d:00 65534  256
```

```
1/1/47      lag256      48     1      ALFNCD   b8:d4:e7:d9:3d:00 65534   256
```

Verify on sw-edge2

19. On sw-edge2, review the LLDP peers.

```
show lldp neighbor-info
```

```
sw-edge2# show lldp neighbor-info

LLDP Neighbor Information
=========================

Total Neighbor Entries          : 4
Total Neighbor Entries Deleted  : 4
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 4

LOCAL-PORT  CHASSIS-ID         PORT-ID       PORT-DESC     TTL      SYS-NAME
------------------------------------------------------------------------------------------
-----------------
...
1/1/27      b8:d4:e7:d9:3d:00  1/1/2         1/1/2         120      sw-agg1
1/1/28      b8:d4:e7:d9:ed:00  1/1/2         1/1/2         120      sw-agg2
...
```

- **Question**: Do you see neighbors on ports 1/1/27 and 1/1/28, with unique Chassis Ids?
- **Answer**: Yes, sw-agg1 and sw-agg2 are listed as LLDP neighbors, each with their own Chassis ID and not the VSX system MAC address.

20. Review the LACP interface state.

```
show lacp interfaces
```

```
sw-edge2# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
---------------------------------------------------------------------------------
Intf        Aggr        Port  Port  State   System-ID         System Aggr Forwarding
            Name        Id    Pri                             Pri    Key  State
---------------------------------------------------------------------------------
1/1/27      lag256      28    1     ALFNCD  64:e8:81:3f:b5:00 65534  256  up
1/1/28      lag256      29    1     ALFNCD  64:e8:81:3f:b5:00 65534  256  up


Partner details of all interfaces:
---------------------------------------------------------------------------------
Intf        Aggr        Port  Port  State   System-ID         System Aggr
            Name        Id    Pri                             Pri    Key
```

```
--------------------------------------------------------------------------------
1/1/27      lag256     2      1      ALFNCD  02:01:00:00:01:00 65534  2
1/1/28      lag256     1002   1      ALFNCD  02:01:00:00:01:00 65534  2
```

- **Question**: What is the status of ports 1/1/27 and 1/1/28?
- **Answer**: Both ports now in the up state.
- **Question**: What is the LACP system ID listed in the Partner details?
- **Answer**: The VSX system MAC address is used as the LACP system ID. This ensures the edge switch believes that it is connected to the same LACP peer with both links.
- **Question**: What is the partner port ID reported on ports 1/1/27 and 1/1/28?
- **Answer**: Port ID 2 and 1002. The ports 1/1/27 is connected to sw-agg1 port 1/1/2, while 1/1/28 is connected to sw-agg2 port 1/1/2. To be able to distinguish the same ports on the two aggregation switches, the ports of the secondary VSX are incremented by 1,000.

As an example: If you would see an access switch port is connected to LACP peer with port ID 1008, you know the port is connected to the secondary VSX switch, to the port ID 8 locally on the secondary.

Task 4: Configure VSX L3 SVI with Active Gateway

In the previous task you have configured an active-active layer 2 LAG between the edge switch sw-edge2 and the VSX system.

Now you will configure the VSX system as the default gateway for your clients, making sure the default gateway is redundant.

This could be achieved using VRRP, but only *one* system is active with a VRRP setup.

On a VSX system, you can configure active gateway. This ensures both VSX systems are active as the default gateway. In this task you will configure active gateway for an SVI.

Objectives

Configure active gateway on VSX

Steps

1. Open an SSH connection to sw-agg1 and sw-agg2.
2. On sw-agg1, create SVI 21. VLAN 21 is used for wired employees in the example lab environment.

```
interface vlan 21
```

```
sw-agg1(config)# interface vlan 21
sw-agg1(config-if-vlan)#
```

3. Configure IP address 10.1.21.2/24 on your new SVI.

```
ip address 10.1.21.2/24
```

```
sw-agg1(config-if-vlan)# ip address 10.1.21.2/24
```

NOTE: In the lab IP scheme, the same host IPs are used in all VLANs:
.1 is reserved for the default gateway.

.2 sw-agg1
.3 sw-agg2
.4 sw-edge1
.5 sw-edge2

4. Configure DHCP relay. Use 10.254.1.21 as the IP helper address.

```
ip helper-address 10.254.1.21
```

```
sw-agg1(config-if-vlan)# ip helper-address 10.254.1.21
```

Configure Active Gateway

Active gateway requires the configuration of a virtual IP (VIP) and virtual MAC (VMAC). The same VMAC and VIP will be configured on both aggregation switches. There is no protocol between the aggregation switches to check the status, since both switches are active with this IP. The peer LACP link aggregation hashing will distribute client traffic to both aggregation switches. The aggregation switch that happens to receive the traffic first will also perform the forwarding for the traffic.

A private MAC address will be used for the VSX VMAC. Check the Aruba VSX Best Practice Guide for suggested values:

https://asp.arubanetworks.com/downloads;search=vsx%20best%20practices;fileTypes=DOCUMENT;products=Aruba%20Switches.

Since a MAC address only requires to be unique within a VLAN, the same VMAC can be used on all SVI interfaces.

5. Configure the active gateway VIP and VMAC.

```
active-gateway ip mac 12:01:00:00:01:00
active-gateway ip 10.1.21.1
```

```
sw-agg1(config-if-vlan)# active-gateway ip mac 12:01:00:00:01:00
sw-agg1(config-if-vlan)# active-gateway ip 10.1.21.1
```

6. Review the current SVI configuration.

```
show running-config current
exit
```

```
sw-agg1(config-if-vlan)# show running-config current
interface vlan 21
    ip address 10.1.21.2/24
    active-gateway ip mac 12:01:00:00:01:00
    active-gateway ip 10.1.21.1
    ip helper-address 10.254.1.21
sw-agg1(config-if-vlan)# exit
```

Configure sw-agg2

In the next steps you will repeat this configuration on sw-agg2.

7. On sw-agg2, create SVI21 and assign IP 10.1.21.3/24.

```
interface vlan 21
 ip address 10.1.21.3/24
```

```
sw-agg2(config)# interface vlan 21
sw-agg2(config-if-vlan)#  ip address 10.1.21.3/24
```

8. Review the current SVI configuration.

```
show running-config current
```

```
sw-agg2(config-if-vlan)# show running-config current
interface vlan 21
    ip address 10.1.21.3/24
```

- **Question**: Do you see an IP helper and active gateway configuration?
- **Answer**: No, these features have not been enabled for VSX sync.

9. On sw-agg1, enable global DHCP VSX sync.

```
vsx
 vsx-sync dhcp-relay
 exit
```

```
sw-agg1(config)# vsx
sw-agg1(config-vsx)#  vsx-sync dhcp-relay
sw-agg1(config-vsx)#  exit
```

10. Enable the SVI 21 active gateway VSX sync.

```
interface vlan 21
vsx-sync active-gateways
exit
```

```
sw-agg1(config)# interface vlan 21
sw-agg1(config-if-vlan)#  vsx-sync active-gateways
sw-agg1(config-if-vlan)#  exit
```

11. On sw-agg2, review the SVI 21 current config again. The active gateway and IP helper should be in the list now.

```
show running-config current
```

```
sw-agg2(config-if-vlan)# show running-config current
interface vlan 21
    vsx-sync active-gateways
    ip address 10.1.21.3/24
    active-gateway ip mac 12:01:00:00:01:00
    active-gateway ip 10.1.21.1
    ip helper-address 10.254.1.21
```

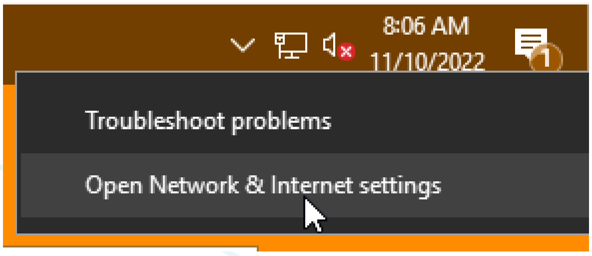
Verify IP Access on PC4

In the next steps you will use PC4 to test the SVI21 active gateway and IP helper configuration.

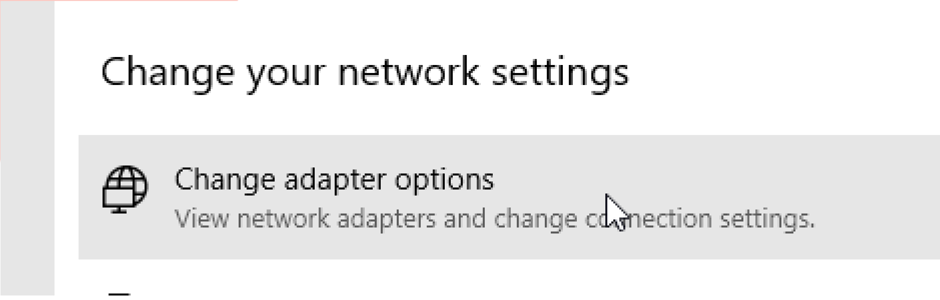
PC4 is connected to sw-edge2 port 1/1/4. This port is assigned to VLAN21.

12. Use the lab dashboard to open a connection to PC4.

13. Open the network connections. In the notification area, right-click the **Network** icon and click **Open Network & Internet Settings**.



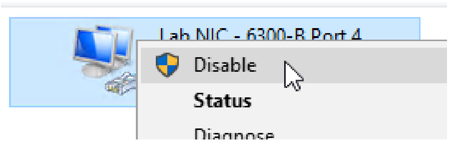
14. Click Change adapter options.

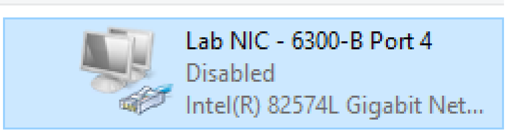


15. The WIFI NIC must be disabled. Disable it if it is enabled.
16. Bounce the LAB NIC (disable and enable). This will trigger the DHCP client process.

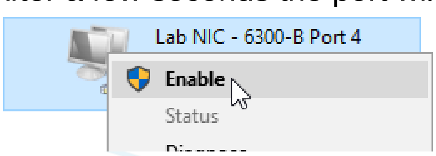
NOTE: Bouncing a port means you disable it and enable it again.
For example, on a switch this would mean ‘shutdown’ and ‘no shutdown’ in the port configuration.

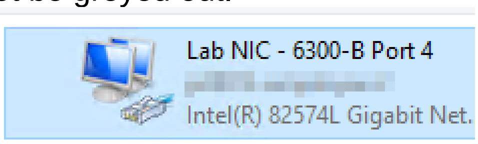
In this case, on a Window endpoint, this can be done by right-click the interface and click **Disable**. After a few seconds, the NIC will be disabled (greyed out).





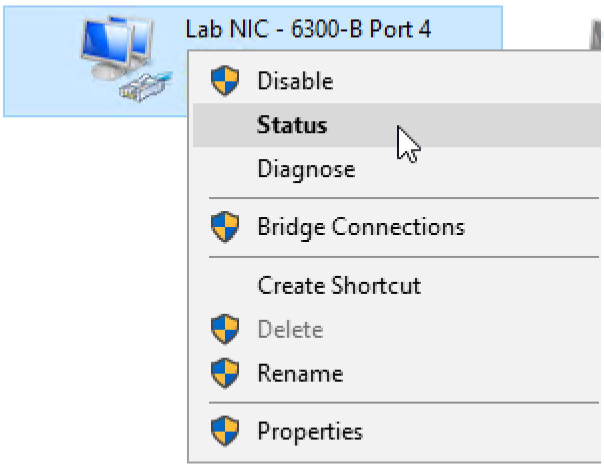
Then you can right-click the NIC again and click **Enable**.
After a few seconds the port will not be greyed out.





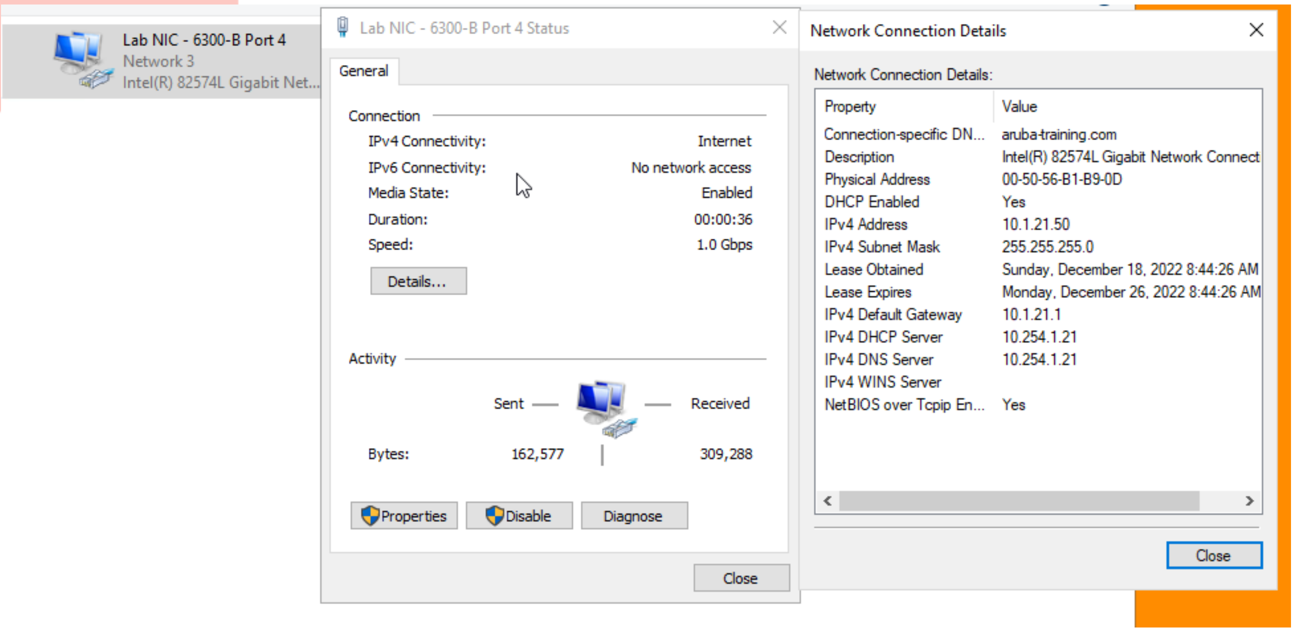
---

17. Right-click the LAB NIC to check the status (click **Status**).



18. Click **Details**.

19. Verify that the IPv4 address is in the 10.1.21.0/24 subnet.



- **Question**: What is the default gateway address?
- **Answer**: The DHCP scope assigned IP 10.1.21.1 as the default gateway.

20. Open a Windows command prompt (**cmd.exe**).

```
cmd.exe
```

21. In the prompt, review the ARP entry for the default gateway IP.

```
arp -a 10.1.21.1
```

```
C:\Users\student>arp -a 10.1.21.1

Interface: 10.1.21.50 --- 0xc
  Internet Address      Physical Address      Type
  10.1.21.1             12-01-00-00-01-00     dynamic
```

- **Question**: What is the MAC address for this IP?
- **Answer**: This is the virtual MAC address you configured on the active gateway for IP 10.1.21.1. Since the same VMAC is set on both VSX members, the endpoint does not need to learn another default gateway MAC in case of a failover.

Task 5: VSX Link Up delay

When a VSX member reboots, the ISLP needs some time to perform the initial synchronization of the MAC, ARP, STP and LACP tables. Routing protocols may also require some time to learn routes from their peers.

During this period, the booting member will keep its VSX LAG member ports down. Once the tables have been synced, the ports will be enabled automatically.

This ensures that the booting member does not drop any traffic nor floods unknown traffic when joining the VSX system.

This delay is achieved with the VSX link up delay feature.

In this task you will review the link up delay behavior.

Objectives

- Understand the VSX link up delay.

Steps

1. Use the lab dashboard to open a console connection to sw-agg1.

   NOTE: Make sure to use the console. You need to review the port status right after the reboot; this may take too much time if you try using SSH.

2. Save the configuration.

```
write mem
```

3. On PC4, open a command prompt and start a continuous ping to the default gateway IP.

```
cmd.exe
ping 10.1.21.1 -t
```

```
C:\Users\student>ping 10.1.21.1 -t

Pinging 10.1.21.1 with 32 bytes of datAnswer:
Reply from 10.1.21.1: bytes=32 time=10ms TTL=64
Reply from 10.1.21.1: bytes=32 time<1ms TTL=64
Reply from 10.1.21.1: bytes=32 time<1ms TTL=64
...
```

4. On sw-agg1 initiate the reboot.

```
boot system
```

```
sw-agg1# boot system
Checking if the configuration needs to be saved...

Checking for updates needed to programmable devices...

Done checking for updates.
```

```
1 non-failsafe device(s) also need to be updated.
Please run the 'allow-unsafe-updates' command to enable these updates.


This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.

 Dec 18 13:55:46 hpe-mgmtmd[31562]: RebootLibPh1: Reboot reason: Reboot requested by user
```

5. Keep monitoring the reboot process; this takes about 2 minutes. Log in immediately after you see the login prompt. Make sure to run the next two steps *immediately* after the reboot.
6. Execute the **show interface brief** command. Do not check the output yet; continue with the next step!

```
show interface brief
```

7. Check the VSX status linkup delay status.

```
show vsx status linkup-delay
```

```
sw-agg1#    show vsx status linkup-delay
Configured linkup delay-timer                             : 180 seconds
Initial sync status                                       : Completed
Delay timer status                                        : Running
Linkup Delay time left                                    : 2 minutes 28 seconds
Interfaces that will be brought up after delay timer expires : lag2
Interfaces enabled for shutdown-on-split that will be brought
up after the delay timer expires                          :
Interfaces that are excluded from delay timer             :
```

8. Now take a moment to review the interface brief status.

```
sw-agg1# show interface brief
Port      Native  Mode   Type           Enabled Status  Reason                  Speed
Description
          VLAN                                                                  (Mb/s)


...
1/1/2     1       trunk  SFP+DAC1       yes     down    Disabled by VSX         --      --
1/1/3     --      routed --             no      down    No XCVR installed       --      --
1/1/4     --      routed --             no      down    No XCVR installed       --      --
1/1/5     --      routed SFP-BT         no      down    Administratively down   --      --
1/1/6     --      routed --             no      down    No XCVR installed       --      --
1/1/7     --      routed SFP-BT         no      down    Administratively down   --      --
1/1/8     --      routed SFP+DAC3       yes     up                              10000
rtr-core1-1/1/1
1/1/9     --      routed --             no      down    No XCVR installed       --      --
1/1/10    --      routed SFP-BT         no      down    Administratively down   --      --
1/1/11    --      routed --             no      down    No XCVR installed       --      --
...
1/1/44    --      routed --             no      down    No XCVR installed       --      --
1/1/45    --      routed SFP28DAC0.65   no      down    Administratively down   --      --
1/1/46    1       trunk  SFP28DAC0.65   yes     up                              25000   --
1/1/47    1       trunk  SFP28DAC0.65   yes     up                              25000   --
```

```
1/1/48     --      routed --           no     down    No XCVR installed      --     --
1/1/49     --      routed --           no     down    No XCVR installed      --     --
1/1/50     --      routed --           no     down    No XCVR installed      --     --
1/1/51     --      routed --           no     down    No XCVR installed      --     --
1/1/52     --      routed --           no     down    No XCVR installed      --     --
1/1/53     --      routed --           no     down    No XCVR installed      --     --
1/1/54     --      routed --           no     down    No XCVR installed      --     --
1/1/55     --      routed --           no     down    No XCVR installed      --     --
1/1/56     --      routed --           no     down    No XCVR installed      --     --
vlan21     --             --           yes    down    Disabled by VSX        --     --
lag2       1       trunk  --           yes    down    --                     auto   --
lag256     1       trunk  --           yes    up      --                     50000  --
```

- **Question**: What was the status for ports 1/1/2 and 1/1/8?
- **Answer**: 1/1/2 was disabled by VSX, while port 1/1/8 was up.
- **Question**: Why was port 1/1/2 disabled by VSX, while port 1/1/8 was up?
- **Answer**: Port 1/1/2 belongs to a VSX LAG (MC-LAG), so the VSX wants to sync the VSX state first before this interface is enabled. Port 1/1/8 is just a local routed port; its status is not relevant to the peer VSX device.
- **Question**: What was the status of the VLAN21 (SVI)?
- **Answer**: SVI21 was also disabled by VSX. Any SVI on a VLAN that is allowed on the MC-LAGs of the system will also be kept disabled until the VSX sync has completed.

9. Review the events in reverse order, filtering on the **vsx** keyword.

```
show event -r | include vsx
```

```
sw-agg1# show event -r | include vsx
2022-11-10T15:45:57.394810+00:00 sw-agg1 hpe-vsxd[1689]: Event|7013|LOG_INFO|AMM|1/1|VSX 2
state local up, remote up
2022-11-10T15:45:54.073689+00:00 sw-agg1 hpe-vsxd[1689]:
Event|7028|LOG_INFO|AMM|1/1|Linkup-delay timer stopped
2022-11-10T15:45:53.089535+00:00 sw-agg1 hpe-vsxd[1689]:
Event|7034|LOG_INFO|AMM|1/1|Netdev 015120100000100 configured with ipv4 address 10.1.21.1
2022-11-10T15:45:17.554288+00:00 8325 hpe-vsxd[1689]: Event|7022|LOG_INFO|AMM|1/1|Linkup
delay timer started
2022-11-10T15:45:17.554195+00:00 8325 hpe-vsxd[1689]: Event|7027|LOG_INFO|AMM|1/1|Bailout
timer stopped
2022-11-10T15:45:13.230647+00:00 8325 hpe-vsxd[1689]: Event|7025|LOG_INFO|AMM|1/1|Bailout
timer started
2022-11-10T15:45:13.230205+00:00 8325 hpe-vsxd[1689]: Event|7012|LOG_INFO|AMM|1/1|VSX 2
state local down, remote up
2022-11-10T15:45:12.230006+00:00 8325 hpe-vsxd[1689]: Event|7015|LOG_INFO|AMM|1/1|VSX ISL
sliding window parameters are reset.
2022-11-10T15:45:12.229684+00:00 8325 hpe-vsxd[1689]: Event|7015|LOG_INFO|AMM|1/1|VSX ISL
sliding window parameters are reset.
2022-11-10T15:45:12.229574+00:00 8325 hpe-vsxd[1689]: Event|7003|LOG_INFO|AMM|1/1|VSX ISL
port lag256 is In-Sync with the peer.
```

```
2022-11-10T15:45:11.774045+00:00 8325 hpe-vsxd[1689]: Event|7002|LOG_INFO|AMM|1/1|VSX ISL
port lag256 is up
2022-11-10T15:44:58.238792+00:00 8325 hpe-vsxd[1689]: Event|7007|LOG_INFO|AMM|1/1|VSX role
is primary
```

10. After about one minute, check the status of the interfaces again. the *Delay timer status* should be completed. If the status is not completed yet, repeat the command after a few moments until it is completed.

```
show vsx status linkup-delay
```

```
sw-agg1#    show vsx status linkup-delay
Configured linkup delay-timer                                 : 180 seconds
Initial sync status                                           : Completed
Delay timer status                                            : Completed
Linkup Delay time left                                        :
Interfaces that will be brought up after delay timer expires :
Interfaces enabled for shutdown-on-split that will be brought
up after the delay timer expires                              :
Interfaces that are excluded from delay timer                 :
```

11. Review the interface brief status and pay attention to the port 1/1/2.

```
show interface brief
```

```
sw-agg1# show interface brief
------------------------------------------------------------------------------------------
--------------------
Port       Native  Mode   Type           Enabled Status  Reason                 Speed
Description
           VLAN                                                                 (Mb/s)
------------------------------------------------------------------------------------------
--------------------
1/1/1      --      routed SFP+DAC1       no      down    Administratively down  --      --
1/1/2      1       trunk  SFP+DAC1       yes     up                             10000   --
...
```

- **Question**: What is the status of the port 1/1/2?
- **Answer**: After the VSX sync has completed, the port is moved to the up state.

Task 6: VSX Split-brain detection

The ISL between the primary and secondary VSX systems should contain a redundant link(s).

Objectives

Steps

12. Review default keepalive status on sw-agg1.

```
show vsx status keepalive
```

```
sw-agg1# show vsx status keepalive
Keepalive State          : Keepalive-Init
Last Established         :
Last Failed              :
Peer System Id           :
Peer Device Role         : secondary

Keepalive Counters
Keepalive Packets Tx     : 0
Keepalive Packets Rx     : 0
Keepalive Timeouts       : 0
Keepalive Packets Dropped : 0
```

1. Configure sw-agg1. The keepalive link will be placed in its own VRF, which is a best practice recommendation from Aruba. Create a KA VRF and associate this with interface 1/1/45. Assign and IP address of 192.168.0.0/31.

```
vrf KA
 exit

interface 1/1/45
 vrf attach KA
 ip address 192.168.0.0/31
 no shutdown
 exit
```

```
sw-agg1(config)# vrf KA
sw-agg1(config-vrf)#  exit
sw-agg1(config)#
sw-agg1(config)# interface 1/1/45
sw-agg1(config-if)#  vrf attach KA
sw-agg1(config-if)#  ip address 192.168.0.0/31
sw-agg1(config-if)#  no shutdown
sw-agg1(config-if)#  exit
```

2. Configure sw-agg2 using the same configuration for the keepalive VRF. Assign an IP address of 192.168.0.1/31 to the 1/1/45 interface..

```
vrf KA
 exit

interface 1/1/45
 vrf attach KA
 ip address 192.168.0.1/31
```

```
 no shutdown
 exit
```

```
sw-agg2(config)# vrf KA
sw-agg2(config-vrf)#  exit
sw-agg2(config)#
sw-agg2(config)# interface 1/1/45
sw-agg2(config-if)#  vrf attach KA
sw-agg2(config-if)#  ip address 192.168.0.1/31
sw-agg2(config-if)#  no shutdown
sw-agg2(config-if)#  exit
sw-agg2(config)#
```

3. On sw-agg2, verify that you can reach sw-agg1 in the VRF KA.

```
ping 192.168.0.0 vrf KA
```

```
sw-agg2(config)# ping 192.168.0.0 vrf KA
PING 192.168.0.0 (192.168.0.0) 100(128) bytes of data.
108 bytes from 192.168.0.0: icmp_seq=1 ttl=64 time=12.7 ms
108 bytes from 192.168.0.0: icmp_seq=2 ttl=64 time=0.143 ms
108 bytes from 192.168.0.0: icmp_seq=3 ttl=64 time=0.159 ms
108 bytes from 192.168.0.0: icmp_seq=4 ttl=64 time=0.151 ms
108 bytes from 192.168.0.0: icmp_seq=5 ttl=64 time=0.135 ms

--- 192.168.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4109ms
rtt min/avg/max/mdev = 0.135/2.659/12.711/5.025 ms
```

Configure VSX Keepalive

4. On sw-agg1, define the destination of the keepalives as sw-agg2 and the source as the IP address on 1/1/45, using the VRF KA.

```
vsx
 keepalive peer 192.168.0.1 source 192.168.0.0 vrf KA
 exit
```

```
sw-agg1(config)# vsx
sw-agg1(config-vsx)#  keepalive peer 192.168.0.1 source 192.168.0.0 vrf KA
sw-agg1(config-vsx)#  exit
```

5. On sw-agg2, define the destination of the keepalives as sw-agg1 and the source as the IP address on 1/1/45, using the VRF KA.

```
vsx
 keepalive peer 192.168.0.0 source 192.168.0.1 vrf KA
 exit
```

```
sw-agg2(config)# vsx
sw-agg2(config-vsx)#  keepalive peer 192.168.0.0 source 192.168.0.1 vrf KA
sw-agg2(config-vsx)#  exit
```

6. On sw-agg1, verify the updated keepalive status.

```
show vsx status keepalive
```

```
sw-agg1(config)# show vsx status keepalive
Keepalive State           : Keepalive-Established
Last Established          : Sun Dec 18 14:18:08 2022
Last Failed               : Sun Dec 18 14:17:56 2022
Peer System Id            : 02:01:00:00:01:00
Peer Device Role          : secondary

Keepalive Counters
Keepalive Packets Tx      : 31
Keepalive Packets Rx      : 18
Keepalive Timeouts        : 0
Keepalive Packets Dropped : 0
```

- **Question**: What is the *Keepalive State*?
- **Answer**: The *Keepalive State* has changed to Keepalive-Established. This means the two VSX members have an active TCP connection to each other using the keepalive VRF.

Test Split Brain Detection

In the next steps you will introduce a VSX ISL failure by manually shutting down the ISL LAG.

7. On sw-agg2, disable the ISL by shutting down LAG 256.

```
interface lag 256
 shutdown
 exit
```

```
sw-agg2(config)# interface lag 256
sw-agg2(config-lag-if)#  shutdown
sw-agg2(config-lag-if)#  exit
```

8. Review the status of the VSX keepalive.

```
show vsx status keepalive
```

```
sw-agg2(config)# show vsx status keepalive
Keepalive State           : Keepalive-Established
Last Established          : Sun Dec 18 14:20:52 2022
Last Failed               :
Peer System Id            : 02:01:00:00:01:00
Peer Device Role          :

Keepalive Counters
Keepalive Packets Tx      : 189
Keepalive Packets Rx      : 190
Keepalive Timeouts        : 0
Keepalive Packets Dropped : 0
```

9. Review the status of the interfaces.

```
show interface brief
```

```
sw-agg2(config)# show interface brief
Port      Native  Mode   Type          Enabled Status  Reason                 Speed
Description
          VLAN                                                                (Mb/s)

1/1/1     --      routed SFP+DAC1      no      down    Administratively down  --       --
1/1/2     1       trunk  SFP+DAC1      yes     down    Disabled by VSX        --       --
1/1/3     --      routed --            no      down    No XCVR installed      --       --
1/1/4     --      routed --            no      down    No XCVR installed      --       --
1/1/5     --      routed SFP-BT        no      down    Administratively down  --       --
1/1/6     --      routed --            no      down    No XCVR installed      --       --
1/1/7     --      routed SFP-BT        no      down    Administratively down  --       --
1/1/8     --      routed SFP+DAC3      yes     up                             10000
rtr-core1-1/1/2
1/1/9     --      routed --            no      down    No XCVR installed      --       --
1/1/10    --      routed SFP-BT        no      down    Administratively down  --       --
1/1/11    --      routed --            no      down    No XCVR installed      --       --
```

- **Question**: What is the status of interface 1/1/2?
- **Answer**: Disabled by VSX.
- Question: What is the status of interface 1/1/8?
- **Answer**: Interface 1/1/8 is still enabled since it is not part of a VSX LAG (MC-LAG).

10. Review the VSX status.

```
show vsx status
```

```
sw-agg2(config)# show vsx status
VSX Operational State
---------------------
  ISL channel              : Out-Of-Sync
  ISL mgmt channel         : inter_switch_link_down
  Config Sync Status       : Out-Of-Sync
  NAE                      : peer_unreachable
  HTTPS Server             : peer_unreachable

Attribute           Local               Peer
------------        --------            --------
ISL link            lag256
ISL version         2
system MAC          02:01:00:00:01:00   02:01:00:00:01:00
Platform            8325
Software Version    GL.10.09.1040
Device Role         secondary
```

- **Question**: What is the status of the ISL channel?
- **Answer**: Since the ISL LAG256 is down, the ISL channel is shown as Out-Of-Sync.

11. Review the events in reverse order, filter on the vsx text.

```
show event -r -n 50 | include vsx
```

```
sw-agg2(config-lag-if)# show event -r -n 50 | include vsx
2022-11-10T16:04:31.412888+00:00 sw-agg2 hpe-vsxd[1699]: Event|7014|LOG_INFO|AMM|1/1|VSX 2
state local down, remote down
2022-11-10T16:04:31.405679+00:00 sw-agg2 hpe-vsxd[1699]: Event|7020|LOG_INFO|AMM|1/1|ISL
out-of-sync and keepalive is in established
2022-11-10T16:04:31.402633+00:00 sw-agg2 hpe-vsxkad[2657]: Event|7006|LOG_INFO|AMM|1/1|VSX
Keepalive succeeded
2022-11-10T16:04:31.281264+00:00 sw-agg2 vsx-syncd[3549]: Event|7602|LOG_INFO|AMM|-
|Configuration sync update : VSX Inter-Switch-Link is down.
2022-11-10T16:04:31.095718+00:00 sw-agg2 hpe-vsxd[1699]: Event|7011|LOG_INFO|AMM|1/1|VSX 2
state local up, remote down
2022-11-10T16:04:31.095645+00:00 sw-agg2 hpe-vsxd[1699]: Event|7004|LOG_ERR|AMM|1/1|VSX
ISL port lag256 is Out-Of-Sync with the peer: link is down
2022-11-10T16:04:31.095550+00:00 sw-agg2 hpe-vsxd[1699]: Event|7015|LOG_INFO|AMM|1/1|VSX
ISL sliding window parameters are reset.
2022-11-10T16:04:31.095453+00:00 sw-agg2 hpe-vsxd[1699]: Event|7001|LOG_INFO|AMM|1/1|VSX
ISL port lag256 is down
2022-11-10T16:03:53.423843+00:00 sw-agg2 hpe-vsxkad[2657]: Event|7006|LOG_INFO|AMM|1/1|VSX
Keepalive succeeded
```

This demonstrates how the secondary removes itself from the network by shutting down the VSX-related interfaces.

Restore the Connection

12. On sw-agg2, restore LAG 256.

```
interface lag 256
 no shutdown
 exit
```

```
sw-agg2(config)# interface lag 256
sw-agg2(config-lag-if)#  no shutdown
sw-agg2(config-lag-if)#  exit
```

13. Verify VSX status returns to *In-Sync*. You may need to repeat this command.

```
show vsx status
```

```
sw-agg2(config)# show vsx status
VSX Operational State
---------------------
  ISL channel               : In-Sync
  ISL mgmt channel          : operational
  Config Sync Status        : In-Sync
  NAE                       : peer_reachable
  HTTPS Server              : peer_reachable

Attribute           Local               Peer
------------        --------            --------
```

```
ISL link            lag256              lag256
ISL version         2                   2
system MAC          02:01:00:00:01:00   02:01:00:00:01:00
Platform            8325                8325
Software Version    GL.10.09.1040       GL.10.09.1040
Device Role         secondary           primary
```

14. Verify that port 1/1/2 is *up* again after the linkup delay phase completes. This may take about a minute in this lab environment.

```
show interface brief
```

```
sw-agg2(config)# show interface brief
------------------------------------------------------------------------------------------
--------------------
Port       Native  Mode   Type           Enabled Status  Reason                  Speed
Description
           VLAN                                                                  (Mb/s)
------------------------------------------------------------------------------------------
--------------------
1/1/1      --      routed SFP+DAC1       no      down    Administratively down   --      --
1/1/2      1       trunk  SFP+DAC1       yes     up                              10000   --
...
```

Save Configurations and Create Checkpoints

15. On sw-agg1 and sw-agg2, save the configurations.

```
write mem
```

16. On sw-agg1 and sw-agg2, copy the running config to a checkpoint named **iaca-lab0201-done**.

```
copy running-config checkpoint iaca-lab0201-done
```

```
sw-agg1(config)# copy running-config checkpoint iaca-lab0201-done
Copying configuration: [Success]
```

```
sw-agg2(config)# copy running-config checkpoint iaca-lab0201-done
Copying configuration: [Success]
```

You have completed this lab!

Lab 02.02 Wired Routing

Overview

In this lab you will configure routing on the aggregation switches.

The first section in this lab is a review of the single area OSPF configuration. This will be configured between the aggregation switches and the core router device.

Then you will learn how to perform route redistribution and tune the redistribution using route maps.

The lab will then continue with the configuration of multi-area OSPF.

In the last section you will explore how BFD can be used in an OSPF environment as a keepalive protocol.

Objectives

After completing this lab, you will be able to:

- Configure and verify single area OSPF.
- Configure and verify route redistribution.
- Configure and verify multi-area OSPF.
- Use BFD as a keep alive protocol for OSPF neighbors.

Task 1: Basic OSPF Configuration

In this task you will apply a basic OSPF configuration to the aggregation switches. This lab assumes you have basic knowledge to setup a single area OSPF network.

You should configure the network based on the following requirements. If you are unsure, the next pages contain the configuration commands that should be applied to each device.

Avoid using the solution, attempt to configure this by yourself! You should be familiar on how to configure this based on completing the *Aruba Campus Access Fundamentals* course.

Requirements:

- Configure loopback0 interfaces on the 2 aggregation switches.
  - sw-agg1: 10.1.0.2/32
  - sw-agg2: 10.1.0.3/32
- Configure SVI 2 on sw-agg1 and sw-agg2: This will act as a layer 3 transit VLAN between the aggregation switches.
  - sw-agg1: 10.1.2.2/24
  - sw-agg2: 10.1.2.3/24
- Configure OSPF area 1 on the 2 switches.
  - Configure loopback 0 IP as the router id.
- Enable OSPF on all the routed links between the devices
  - sw-agg1 to rtr-core1: port 1/1/8
  - sw-agg2 to rtr-core1: port 1/1/8
  - sw-agg1 to sw-agg2: svi2 on both switches
- Optimize the transit links:
  - Configure all transit links as OSPF Point to Point interfaces.
- Make sure all loopback interfaces are reachable through OSPF as well.
- On both aggregation switches, enable OSPF on SVI 21.
- Make all the interfaces passive by default and make sure the OSPF transit interfaces are enabled.

You may attempt to configure the above setup yourself. If you are unsure, use the configuration snippets on the next pages to complete the configuration on sw-agg1 and sw-agg2.

These snippets can also be found on the MGMT PC PC in the Student files IACA folder.

After you have completed the configuration, you should be able to verify the OSPF setup:

1. On all 3 systems, confirm 2 OSPF neighbors are in FULL state.

```
show ip ospf neighbors
```

2. On sw-agg1/2, check the flags active/passive for each of the interfaces.

```
show ip ospf interface brief
```

3. On sw-agg1/2, check that the LSDB does not contain any network LSAs. This confirms all transit links have been set to point-to-point.

```
show ip ospf lsdb
```

4. On rtr-core1, verify that the route 10.1.21.0/24 is listed via *two* ECMP paths (sw-agg1 and sw-agg2) in the routing table.

```
show ip route
```

Basic OSPF Solution

sw-agg1

```
interface loopback 0
 ip address 10.1.0.2/32
 exit
interface vlan 2
 ip address 10.1.2.2/24
 exit
router ospf 1
 router-id 10.1.0.2
 area 1
interface 1/1/8
 ip ospf 1 area 1
exit
interface vlan 2
 ip ospf 1 area 1
exit

interface 1/1/8
 ip ospf network point-to-point
 exit
interface vlan 2
 ip ospf network point-to-point
 exit
interface loopback 0
 ip ospf 1 area 1
 exit

interface vlan 21
 ip ospf 1 area 1
 exit

router ospf 1
 passive-interface default
 exit
interface 1/1/8
 no ip ospf passive
 exit
interface vlan2
 no ip ospf passive
 exit
```

sw-agg2

```
interface loopback 0
 ip address 10.1.0.3/32
 exit
interface vlan 2
 ip address 10.1.2.3/24
 exit
router ospf 1
 router-id 10.1.0.3
 area 1
interface 1/1/8
 ip ospf 1 area 1
 exit
interface vlan 2
 ip ospf 1 area 1
 exit

interface 1/1/8
 ip ospf network point-to-point
 exit
interface vlan 2
 ip ospf network point-to-point
 exit

interface loopback 0
 ip ospf 1 area 1
 exit

interface vlan 21
 ip ospf 1 area 1


router ospf 1
 passive-interface default
 exit
interface 1/1/8
 no ip ospf passive
 exit
interface vlan2
 no ip ospf passive
 exit
```

Optional Troubleshooting: OSPF Network Type Mismatch

This is a broadcast to p2p example.

5. On rtr-core1, review the available paths for the 10.1.21.0/24 subnet.

```
show ip route | begin 3 10.1.21.0
```

```
rtr-core1-IACA(config)# show ip route | begin 3 10.1.21.0
10.1.21.0/24          10.254.102.3      1/1/2         -              O          [110/200]
00h:02m:14s
                      10.254.101.2      1/1/1         -                         [110/200]
00h:02m:14s
10.2.0.1/32           -                 blackhole     -              S          [1/0]
05h:49m:24s
10.2.0.2/32           -                 blackhole     -              S          [1/0]
05h:49m:24s
```

- **Question**: How many paths are listed in the rtr-core1 routing table for the 10.1.21.0 subnet?
- **Answer**: 2—one path via sw-agg1 and one path via sw-agg2.

Introduce the Network Type Mismatch

6. On sw-agg1, configure port 1/1/8 (to rtr-core1) as OSPF broadcast.

```
interface 1/1/8
 ip ospf network broadcast
 exit
```

```
sw-agg1(config)# interface 1/1/8
sw-agg1(config-if)# ip ospf network broadcast
sw-agg1(config-if)# exit
```

7. Review that the adjacency to rtr-core1 is still FULL.

```
show ip ospf neighbors
```

```
sw-agg1(config)# show ip ospf neighbors
VRF : default                              Process : 1
===================================================

Total Number of Neighbors : 2

Neighbor ID      Priority  State              Nbr Address        Interface
-------------------------------------------------------------------------
10.1.0.254       1         FULL/DR            10.254.101.254      1/1/8

10.1.0.3         n/a       FULL               10.1.2.3            vlan2
```

NOTE: If the connection state with the rtr-core1 is listed as 2WAY-DROTHER, repeat the previous step after about 30 seconds.

- **Question**: What is the OSPF neighbor state for the rtr-core1?
- **Answer**: The rtr-core1 is listed with a FULL state again.

Review the Problem

8. On rtr-core1, check the IP routing table.

```
show ip route | begin 3 10.1.21.0
```

```
rtr-core1-IACA(config)# show ip route | begin 3 10.1.21.0
10.1.21.0/24        10.254.102.3      1/1/2         -                 O         [110/200]
00h:04m:11s
10.2.0.1/32         -                 blackhole     -                 S         [1/0]
05h:56m:51s
10.2.0.2/32         -                 blackhole     -                 S         [1/0]
05h:56m:51s
10.2.0.3/32         -                 blackhole     -                 S         [1/0]
05h:56m:51s
```

- **Question**: What happened with the 10.1.21.0/24 route?
- **Answer**: Previously there were 2 paths:
  - 1 via sw-agg1 (nexthop 10.254.101.2) and
  - 1 via sw-agg2 (nexthop 10.254.102.3)

  Now only the path via sw-agg2 (10.254.102.3) is available.

9. Review the OSPF routing table.

```
show ip ospf route
```

```
rtr-core1-IACA(config)# show ip ospf route
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPF Process ID 1 VRF default, Routing Table
---------------------------------------------

Total Number of Routes : 6

10.1.0.2/32        (i) areAnswer: 0.0.0.1
     via 10.254.102.3 interface 1/1/2, cost 200 distance 110
10.1.0.3/32        (i) areAnswer: 0.0.0.1
     via 10.254.102.3 interface 1/1/2, cost 100 distance 110
10.1.2.0/24        (i) areAnswer: 0.0.0.1
     via 10.254.102.3 interface 1/1/2, cost 200 distance 110
10.1.21.0/24       (i) areAnswer: 0.0.0.1
     via 10.254.102.3 interface 1/1/2, cost 200 distance 110
10.254.101.0/24    (i) areAnswer: 0.0.0.1
     directly attached to interface 1/1/1, cost 100 distance 110
10.254.102.0/24    (i) areAnswer: 0.0.0.1
     directly attached to interface 1/1/2, cost 100 distance 110
```

- **Question**: Do you see any routes with next hop 10.254.101.2?
- **Answer**: No. Sw-agg1 believes it is connected to the 'network' LSA for the 10.254.101.0 subnet. Rtr-core1 believes it is directly connected to sw-agg1. Therefor there is no 'active' path that can be calculated in the topology between these 2 systems. This is the result of an OSPF network type mismatch.

Restore the configuration

10. On sw-agg1, change the port 1/1/8 network type back to **point-to-point**.

```
interface 1/1/8
 ip ospf network point-to-point
 exit
```

```
sw-agg1(config)# interface 1/1/8
sw-agg1(config-if)# ip ospf network point-to-point
sw-agg1(config-if)# exit
```

11. On rtr-core1, verify that routes exist with 10.254.101.2 as next hop IP.

```
show ip ospf route
```

```
rtr-core1-IACA(config)# show ip ospf route
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPF Process ID 1 VRF default, Routing Table
---------------------------------------------

Total Number of Routes : 8

10.1.0.2/32        (i) areAnswer: 0.0.0.1
     via 10.254.101.2 interface 1/1/1, cost 100 distance 110
10.1.0.3/32        (i) areAnswer: 0.0.0.1
     via 10.254.102.3 interface 1/1/2, cost 100 distance 110
10.1.2.0/24        (i) areAnswer: 0.0.0.1
     via 10.254.101.2 interface 1/1/1, cost 200 distance 110
10.1.2.0/24        (i) areAnswer: 0.0.0.1
     via 10.254.102.3 interface 1/1/2, cost 200 distance 110
10.1.21.0/24       (i) areAnswer: 0.0.0.1
     via 10.254.101.2 interface 1/1/1, cost 200 distance 110
10.1.21.0/24       (i) areAnswer: 0.0.0.1
     via 10.254.102.3 interface 1/1/2, cost 200 distance 110
10.254.101.0/24    (i) areAnswer: 0.0.0.1
     directly attached to interface 1/1/1, cost 100 distance 110
10.254.102.0/24    (i) areAnswer: 0.0.0.1
     directly attached to interface 1/1/2, cost 100 distance 110
```

12. On rtr-core1, verify in the IP routing table that 2 ECMP routes exist for 10.1.21.0/24.

```
show ip route | begin 3 10.1.21.0
```

```
rtr-core1-IACA(config)# show ip route | begin 3 10.1.21.0
```

```
10.1.21.0/24        10.254.102.3      1/1/2          -                  O          [110/200]
00h:01m:37s
                    10.254.101.2      1/1/1          -                             [110/200]
00h:01m:37s
10.2.0.1/32         -                 blackhole      -                  S          [1/0]
06h:00m:36s
10.2.0.2/32         -                 blackhole      -                  S          [1/0]
06h:00m:36s
```

Task 2: Route Redistribution and Filtering Using Route Maps

In this task you will use OSPF to redistribute routes from an external system.

First you will use OSPF to redistribute the default route to the Campus network. The advantage is that traffic to the internet will also be able to failover.

Objectives

- Advertise a default route using OSPF.
- Redistribute routes.
- Tune route redistribution using a route map.

Steps

Remove the Static Default Route

1. On sw-agg1, remove the static default route.

```
no ip route 0.0.0.0/0 10.254.101.254
```

```
sw-agg1(config)# no ip route 0.0.0.0/0 10.254.101.254
```

2. Verify there is no default route anymore in the IP routing table.

```
show ip route 0.0.0.0
```

```
sw-agg1(config)# show ip route 0.0.0.0

No ipv4 routes configured
```

3. On sw-agg2, remove the static default route as well and verify the removal.

```
no ip route 0.0.0.0/0 10.254.102.254
```

```
sw-agg2(config)# no ip route 0.0.0.0/0 10.254.102.254
```

4. On sw-agg2, check if there is a default route in the IP routing table.

```
show ip route 0.0.0.0
```

```
sw-agg2(config)# show ip route 0.0.0.0

No ipv4 routes configured
```

OSPF Default Information Originate

5. On rtr-core1, review the IP Routing table.

```
show ip route 0.0.0.0
```

```
rtr-core1-IACA(config)# show ip route 0.0.0.0

VRF: default

   Prefix            : 0.0.0.0/0                                 VRF(egress)         : -
   Nexthop           : 10.254.1.253                              Interface           : 1/1/9
   Origin            : static                                    Type                : -
   Distance          : 1                                         Metric              : 0
   Age               : 06h:07m:17s                               Tag                 : 0
   Encap Type        : -                                         Encap Details       : -
```

- **Question**: Do you have a default route on rtr-core1?
- **Answer**: Yes, rtr-core1 still has a static, default route in the routing table. By default, this is verified by OSPF before a default route is advertised into the OSPF AS.

6. On rtr-core1, configure OSPF to advertise the default route.

```
router ospf 1
 default-information originate
 exit
```

```
rtr-core1-IACA(config)# router ospf 1
rtr-core1-IACA(config-ospf-1)# default-information originate
rtr-core1-IACA(config-ospf-1)# exit
```

7. On sw-agg1, review the IP routing table.

```
show ip route 0.0.0.0
```

```
sw-agg1(config)# show ip route 0.0.0.0

VRF: default

   Prefix            : 0.0.0.0/0                         VRF(egress)         : -
   Nexthop           : 10.254.101.254                    Interface           : 1/1/8
   Origin            : ospf                              Type                : ospf_type2_ext
   Distance          : 110                               Metric              : 1
   Age               : 00h:00m:32s                       Tag                 : 0
   Encap Type        : -                                 Encap Details       : -
```

- **Question**: Do you see a default route?
- **Answer**: Yes.
- **Question**: What is the Origin/Type?
- **Answer**: OSPF External Type 2.
- **Question**: What is the next-hop IP for this default route?
- **Answer**: The next hop IP will point to rtr-core1, 10.254.101.254.

Verify Default Route Failover Based on OSPF

In the next steps you will verify that OSPF failover also applies to the default route now.

8. On sw-agg1, disable the port 1/1/8.

```
interface 1/1/8
 shutdown
 exit
```

```
sw-agg1(config)# interface 1/1/8
sw-agg1(config-if)# shutdown
sw-agg1(config-if)# exit
```

9. Review the IP routing table again, looking for the 0.0.0.0/0 route.

```
show ip route 0.0.0.0
```

```
sw-agg1(config)# show ip route 0.0.0.0

VRF: default

   Prefix            : 0.0.0.0/0                              VRF(egress)       : -
   Nexthop           : 10.1.2.3                               Interface         :
vlan2
   Origin            : ospf                                   Type              :
ospf_type2_ext
   Distance          : 110                                    Metric            : 1
   Age               : 00h:00m:03s                            Tag               : 0
   Encap Type        : -                                      Encap Details     : -
```

- **Question**: Do you still have a default route in the routing table?
- **Answer**: Yes, OSPF calculated an alternative path to the rtr-core1.
- **Question**: What is the next hop IP for the default route?
- **Answer**: The next hop now points to sw-agg2 SVI 2: 10.1.2.3. This demonstrates how the default route failed over to an alternate path.

10. On sw-agg1, enable port 1/1/8 again.

```
interface 1/1/8
 no shutdown
 exit
```

```
sw-agg1(config)# interface 1/1/8
sw-agg1(config-if)# no shutdown
sw-agg1(config-if)# exit
```

Static Route Redistribution

On the rtr-core1 switch, several static routes exist that point to some partner networks. Some of these networks should be advertised into the campus network.

In this section you will first redistribute all static routes into the campus network. Next you will limit the redistribution to a subset of the static routes using a route-map.

11. On sw-agg1, verify that you currently don't have a route for the 10.2.1.0/24 network. The current routing table is using the default route to handle this traffic.

```
show ip route 10.2.1.0
```

```
sw-agg1(config)# show ip route 10.2.1.0

VRF: default

   Prefix          : 0.0.0.0/0                                  VRF(egress)        : -
   Nexthop         : 10.254.101.254                             Interface          :
1/1/8
   Origin          : ospf                                       Type               :
ospf_type2_ext
   Distance        : 110                                        Metric             : 1
   Age             : 00h:01m:06s                                Tag                : 0
   Encap Type      : -                                          Encap Details      : -
```

12. On rtr-core1, review the IP routing table for static routes. Your campus lab environment is using the 10.1.0.0/16 address block. The rtr-core1 has been configured with some static routes in the 10.2.0.0/16 and 10.3.0.0/16 address blocks. These are static routes with a blackhole destination, so any traffic matching these routes will be dropped. These static routes are only used to practice the control of route redistribution in this lab environment.

```
show ip route static
```

```
rtr-core1-IACA# show ip route static

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2

VRF: default

Prefix                 Nexthop      Interface  VRF(egress)   Origin/  Distance/    Age
                                                                       Type      Metric
------------------------------------------------------------------------------------------
----
0.0.0.0/0             10.254.1.253     1/1/9          -     S         [1/0]        17h:37m:02s
10.0.0.0/8            -                blackhole      -     S         [1/0]        17h:37m:02s
10.1.0.0/16           10.254.101.2     1/1/1          -     S         [1/0]        17h:37m:02s
```

```
10.1.3.0/24      10.254.101.2    1/1/1         -    S        [255/0]      17h:37m:02s
10.1.11.0/24     10.254.101.2    1/1/1         -    S        [255/0]      17h:37m:02s
10.1.12.0/24     10.254.101.2    1/1/1         -    S        [255/0]      17h:37m:02s
10.2.0.1/32      -               blackhole     -    S        [1/0]        17h:37m:02s
10.2.0.2/32      -               blackhole     -    S        [1/0]        17h:37m:02s
10.2.0.3/32      -               blackhole     -    S        [1/0]        17h:37m:02s
10.2.1.0/24      -               blackhole     -    S        [1/0]        17h:37m:03s
10.2.1.0/25      -               blackhole     -    S        [1/0]        17h:37m:04s
10.2.1.128/25    -               blackhole     -    S        [1/0]        17h:37m:04s
10.2.2.0/24      -               blackhole     -    S        [1/0]        17h:37m:04s
10.2.4.0/22      -               blackhole     -    S        [1/0]        17h:37m:04s
10.2.8.0/22      -               blackhole     -    S        [1/0]        17h:37m:04s
10.3.0.1/32      -               blackhole     -    S        [1/0]        17h:37m:04s
10.3.0.2/32      -               blackhole     -    S        [1/0]        17h:37m:04s
10.3.0.3/32      -               blackhole     -    S        [1/0]        17h:37m:04s
10.3.1.0/24      -               blackhole     -    S        [1/0]        17h:37m:04s
10.3.1.0/25      -               blackhole     -    S        [1/0]        17h:37m:04s
10.3.1.128/25    -               blackhole     -    S        [1/0]        17h:37m:04s
10.3.2.0/24      -               blackhole     -    S        [1/0]        17h:37m:04s
10.3.4.0/22      -               blackhole     -    S        [1/0]        17h:37m:04s
10.3.8.0/22      -               blackhole     -    S        [1/0]        17h:37m:04s
```

13. On rtr-core1, redistribute all static routes.

```
router ospf 1
 redistribute static
 exit
```

```
rtr-core1-IACA(config)# router ospf 1
rtr-core1-IACA(config-ospf-1)# redistribute static
rtr-core1-IACA(config-ospf-1)# exit
```

14. On sw-agg1, verify in the OSPF LSDB that external LSAs were received.

```
show ip ospf lsdb external
```

```
sw-agg1(config)# show ip ospf lsdb external
OSPF Router with ID (10.1.0.2) (Process ID 1 VRF default)
==========================================================

AS External Link State Advertisements
--------------------------------------

LSID            ADV Router      Age       Seq#       Checksum
--------------------------------------------------------------
0.0.0.0         10.1.0.254      726       0x80000018 0x0000624e
10.0.0.0        10.1.0.254      153       0x80000001 0x0000fea6
10.1.0.0        10.1.0.254      153       0x80000001 0x0000f2b1
10.1.3.0        10.1.0.254      153       0x80000001 0x0000d1cf
10.1.11.0       10.1.0.254      153       0x80000001 0x00007920
10.1.12.0       10.1.0.254      153       0x80000001 0x00006e2a
10.2.0.1        10.1.0.254      153       0x80000001 0x0000dcc5
10.2.0.2        10.1.0.254      153       0x80000001 0x0000d2ce
10.2.0.3        10.1.0.254      153       0x80000001 0x0000c8d7
10.2.1.0        10.1.0.254      153       0x80000001 0x0000dbc6
```

```
10.2.1.127      10.1.0.254      153        0x80000001 0x0000e3be
10.2.1.128      10.1.0.254      153        0x80000001 0x0000d9c7
10.2.2.0        10.1.0.254      153        0x80000001 0x0000d0d0
10.2.4.0        10.1.0.254      153        0x80000001 0x0000abf6
10.2.8.0        10.1.0.254      153        0x80000001 0x00007f1f
10.3.0.1        10.1.0.254      153        0x80000001 0x0000d0d0
10.3.0.2        10.1.0.254      153        0x80000001 0x0000c6d9
10.3.0.3        10.1.0.254      153        0x80000001 0x0000bce2
10.3.1.0        10.1.0.254      153        0x80000001 0x0000cfd1
10.3.1.127      10.1.0.254      153        0x80000001 0x0000d7c9
10.3.1.128      10.1.0.254      153        0x80000001 0x0000cdd2
10.3.2.0        10.1.0.254      153        0x80000001 0x0000c4db
10.3.4.0        10.1.0.254      153        0x80000001 0x00009f02
10.3.8.0        10.1.0.254      153        0x80000001 0x0000732a
```

15. On sw-agg1, verify in the IP routing table that the routes now exist as OSPF external (O/E2) routes.

```
show ip route
```

```
sw-agg1(config)# show ip route ospf

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2

VRF: default

Prefix              Nexthop       Interface  VRF(egress) Origin/   Distance/    Age
                                                         Type      Metric
------------------------------------------------------------------------------------------
0.0.0.0/0           10.254.101.254   1/1/8         -     O/E2      [110/1]      00h:23m:44s
10.0.0.0/8          10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.1.0.0/16         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.1.0.3/32         10.1.2.3         vlan2         -     O         [110/100]    12h:21m:08s
10.1.0.254/32       10.254.101.254   1/1/8         -     O         [110/100]    00h:23m:44s
10.1.3.0/24         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.1.11.0/24        10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.1.12.0/24        10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.2.0.1/32         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.2.0.2/32         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.2.0.3/32         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.2.1.0/24         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.2.1.0/25         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.2.1.128/25       10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.2.2.0/24         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.2.4.0/22         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.2.8.0/22         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.3.0.1/32         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.3.0.2/32         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
10.3.0.3/32         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:06m:52s
```

```
10.3.1.0/24        10.254.101.254   1/1/8         -    O/E2      [110/25]     00h:06m:52s
10.3.1.0/25        10.254.101.254   1/1/8         -    O/E2      [110/25]     00h:06m:52s
10.3.1.128/25      10.254.101.254   1/1/8         -    O/E2      [110/25]     00h:06m:52s
10.3.2.0/24        10.254.101.254   1/1/8         -    O/E2      [110/25]     00h:06m:52s
10.3.4.0/22        10.254.101.254   1/1/8         -    O/E2      [110/25]     00h:06m:52s
10.3.8.0/22        10.254.101.254   1/1/8         -    O/E2      [110/25]     00h:06m:52s
10.254.102.0/24    10.254.101.254   1/1/8         -    O         [110/200]    00h:23m:44s
                   10.1.2.3         vlan2         -              [110/200]    00h:23m:44s
```

This shows that rtr-core1 has redistributed all the static routes into the OSPF network.
While this works, the network administrator may want to have additional control over the routes that are redistributed, you will explore this in the next section by using a route map.

Route-map

In the next steps you will create a route-map so that only a subset of these routes is distributed into OSPF.

The customer wants to ensure that only routes that belong to 10.2.0.0/16 are advertised.

First you will create an IP prefix list to match on the routes that should be controlled.
Next this IP prefix list will be used in the route-map to allow these routes for redistribution.

16. On rtr-core1, create a new IP prefix list.

```
ip prefix-list static-2-ospf permit 10.2.0.0/16 ge 16
```

```
rtr-core1-IACA(config)# ip prefix-list static-2-ospf permit 10.2.0.0/16 ge 16
```

17. Next create a new route-map with a permit entry that matches routes in the IP prefix list.

```
route-map static-2-ospf permit
 match ip address prefix-list static-2-ospf
 exit
```

```
rtr-core1-IACA(config)# route-map static-2-ospf permit
rtr-core1-IACA(config-route-map-static-2-ospf-10)# match ip address prefix-list
rtr-core1-IACA(config-route-map-static-2-ospf-10)# exit
```

18. Now apply the route-map to the OSPF static route redistribution.

```
router ospf 1
 redistribute static route-map static-2-ospf
 exit
```

```
rtr-core1-IACA(config)# router ospf 1
rtr-core1-IACA(config-ospf-1)# redistribute static route-map static-2-ospf
rtr-core1-IACA(config-ospf-1)# exit
```

19. On rtr-core1, verify in the OSPF LSDB External LSAs that fewer LSAs are advertised.

```
show ip ospf lsdb external
```

```
rtr-core1-IACA(config)# show ip ospf lsdb external
OSPF Router with ID (10.1.0.254) (Process ID 1 VRF default)
============================================================

AS External Link State Advertisements
--------------------------------------

LSID            ADV Router      Age       Seq#       Checksum
--------------------------------------------------------------
0.0.0.0         10.1.0.254      252       0x80000019 0x0000604f
10.2.0.1        10.1.0.254      1479      0x80000001 0x0000dcc5
10.2.0.2        10.1.0.254      1479      0x80000001 0x0000d2ce
10.2.0.3        10.1.0.254      1479      0x80000001 0x0000c8d7
10.2.1.0        10.1.0.254      1479      0x80000001 0x0000dbc6
10.2.1.127      10.1.0.254      1479      0x80000001 0x0000e3be
10.2.1.128      10.1.0.254      1479      0x80000001 0x0000d9c7
10.2.2.0        10.1.0.254      1479      0x80000001 0x0000d0d0
10.2.4.0        10.1.0.254      1479      0x80000001 0x0000abf6
10.2.8.0        10.1.0.254      1479      0x80000001 0x00007f1f
```

20. On sw-agg1, verify that the OSPF LSDB has also been updated.

```
show ip ospf lsdb external
```

```
sw-agg1(config)# show ip ospf lsdb external
OSPF Router with ID (10.1.0.2) (Process ID 1 VRF default)
==========================================================

AS External Link State Advertisements
--------------------------------------

LSID            ADV Router      Age       Seq#       Checksum
--------------------------------------------------------------
0.0.0.0         10.1.0.254      176       0x80000019 0x0000604f
10.2.0.1        10.1.0.254      1403      0x80000001 0x0000dcc5
10.2.0.2        10.1.0.254      1403      0x80000001 0x0000d2ce
10.2.0.3        10.1.0.254      1403      0x80000001 0x0000c8d7
10.2.1.0        10.1.0.254      1403      0x80000001 0x0000dbc6
10.2.1.127      10.1.0.254      1403      0x80000001 0x0000e3be
10.2.1.128      10.1.0.254      1403      0x80000001 0x0000d9c7
10.2.2.0        10.1.0.254      1403      0x80000001 0x0000d0d0
10.2.4.0        10.1.0.254      1403      0x80000001 0x0000abf6
10.2.8.0        10.1.0.254      1403      0x80000001 0x00007f1f
```

21. On sw-agg1, verify in the IP routing table that only the required routes are in the list.

```
show ip route ospf
```

```
sw-agg1(config)# show ip route ospf

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
```

```
                IA - OSPF internal area, E1 - OSPF external type 1
                E2 - OSPF external type 2

VRF: default

Prefix              Nexthop           Interface     VRF(egress)       Origin/   Distance/
Age
                                                                       Type      Metric
---------------------------------------------------------------------------------------
--------------
0.0.0.0/0           10.254.101.254    1/1/8         -    O/E2      [110/1]      00h:42m:11s
10.1.0.3/32         10.1.2.3          vlan2         -    O         [110/100]    12h:39m:35s
10.1.0.254/32       10.254.101.254    1/1/8         -    O         [110/100]    00h:42m:11s
10.2.0.1/32         10.254.101.254    1/1/8         -    O/E2      [110/25]     00h:25m:19s
10.2.0.2/32         10.254.101.254    1/1/8         -    O/E2      [110/25]     00h:25m:19s
10.2.0.3/32         10.254.101.254    1/1/8         -    O/E2      [110/25]     00h:25m:19s
10.2.1.0/24         10.254.101.254    1/1/8         -    O/E2      [110/25]     00h:25m:19s
10.2.1.0/25         10.254.101.254    1/1/8         -    O/E2      [110/25]     00h:25m:19s
10.2.1.128/25       10.254.101.254    1/1/8         -    O/E2      [110/25]     00h:25m:19s
10.2.2.0/24         10.254.101.254    1/1/8         -    O/E2      [110/25]     00h:25m:19s
10.2.4.0/22         10.254.101.254    1/1/8         -    O/E2      [110/25]     00h:25m:19s
10.2.8.0/22         10.254.101.254    1/1/8         -    O/E2      [110/25]     00h:25m:19s
10.254.102.0/24     10.254.101.254    1/1/8         -    O         [110/200]    00h:42m:11s
                    10.1.2.3          vlan2         -              [110/200]    00h:42m:11s
```

Optional Practice

In this optional section, you may practice the configuration of the route map by yourself.

Update the existing route map based on these requirements:

- The customer wants to prevent any host prefixes (/32 mask) from being advertised
- The customer wants to include prefixes that belong to 10.3.0.0/16 with a mask of /24 or lower.

Try configuring this on your own. The answer is shown on the following page.

Solution

22. On rtr-core1, check the existing IP prefix List and adjust the existing line.

```
show ip prefix-list
ip prefix-list static-2-ospf seq 10 permit 10.2.0.0/16 ge 16 le 31
ip prefix-list static-2-ospf seq 20 permit 10.3.0.0/16 ge 16 le 24
show ip prefix-list
```

```
rtr-core1-IACA(config)# show ip prefix-list
ip prefix-list static-2-ospf: 1 entries
   seq 10 permit 10.2.0.0/16 ge 16
```

```
rtr-core1-IACA(config)# ip prefix-list static-2-ospf seq 10 permit 10.2.0.0/16 ge 16 le 31
rtr-core1-IACA(config)# ip prefix-list static-2-ospf seq 20 permit 10.3.0.0/16 ge 16 le 24
```

```
rtr-core1-IACA(config)# show ip prefix-list
ip prefix-list static-2-ospf: 2 entries
   seq 10 permit 10.2.0.0/16 ge 16 le 31
   seq 20 permit 10.3.0.0/16 ge 16 le 24
```

23. On sw-agg1, verify the result in the IP routing table.

```
show ip route ospf
```

```
sw-agg1(config)# show ip route ospf
...

Prefix              Nexthop       Interface     VRF(egress)  Origin/   Distance/    Age
                                                             Type      Metric
------------------------------------------------------------------------------------
--------------
0.0.0.0/0           10.254.101.254   1/1/8         -     O/E2      [110/1]      00h:58m:31s
10.1.0.3/32         10.1.2.3         vlan2         -     O         [110/100]    12h:55m:55s
10.1.0.254/32       10.254.101.254   1/1/8         -     O         [110/100]    00h:58m:31s
10.2.1.0/24         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:41m:39s
10.2.1.0/25         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:41m:39s
10.2.1.128/25       10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:41m:39s
10.2.2.0/24         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:41m:39s
10.2.4.0/22         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:41m:39s
10.2.8.0/22         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:41m:39s
10.3.1.0/24         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:04m:16s
10.3.2.0/24         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:04m:16s
10.3.4.0/22         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:04m:16s
10.3.8.0/22         10.254.101.254   1/1/8         -     O/E2      [110/25]     00h:04m:16s
10.254.102.0/24     10.254.101.254   1/1/8         -     O         [110/200]    00h:58m:31s
                    10.1.2.3         vlan2         -               [110/200]    00h:58m:31s
```

Task 3: Multi-Area OSPF and Route Aggregation between Areas

In this task you will configure multi-area OSPF.

In the previous task, the rtr-core1, sw-agg1 and sw-agg2 have been configured in OSPF area 1.

In this task, you will connect the rtr-core1 to a backbone router that has already been configured in OSPF area 0.

The rtr-core1 will become the area border router (ABR) between the backbone area 0 and the campus area 1.

After you have completed and verified this configuration, you will be able to perform route aggregation between these two areas.

Objectives

- Configure multi-area OSPF.
- Monitor multi-area OSPF routes.
- Configure route aggregation on the area border router (ABR).

Steps

1. On rtr-core1:

   - Create OSPF area 0.
   - Enable port 1/1/9 for OSPF area 0.
   - Set the port 1/1/9 as P2P (Point to Point) with these timers: hello 1 second and dead interval 4 seconds.

```
router ospf 1
 area 0
 exit
interface 1/1/9
 ip ospf 1 area 0
 ip ospf network point-to-point
 ip ospf hello 1
 ip ospf dead 4
 exit
```

```
rtr-core1-IACA(config)# router ospf 1
rtr-core1-IACA(config-ospf-1)# area 0
rtr-core1-IACA(config-ospf-1)# exit
rtr-core1-IACA(config)# interface 1/1/9
rtr-core1-IACA(config-if)# ip ospf 1 area 0
rtr-core1-IACA(config-if)# ip ospf network point-to-point
rtr-core1-IACA(config-if)# ip ospf hello 1
rtr-core1-IACA(config-if)# ip ospf dead 4
rtr-core1-IACA(config-if)# exit
```

2. Verify the OSPF neighbors of rtr-core1. The backbone router should be in the list.

```
show ip ospf neighbors
```

```
rtr-core1-IACA(config)# show ip ospf neighbors
VRF : default                              Process : 1
===================================================

Total Number of Neighbors : 3

Neighbor ID      Priority  State              Nbr Address       Interface
-------------------------------------------------------------------------
10.254.0.253     n/a       FULL               10.254.1.253       1/1/9

10.1.0.2         n/a       FULL               10.254.101.2       1/1/1

10.1.0.3         n/a       FULL               10.254.102.3       1/1/2
```

3. Review the OSPF LSDB. It will now contain entries in the area 0.0.0.1 LSDB and the area 0.0.0.0 LSDB.

```
show ip ospf lsdb
```

```
rtr-core1-IACA(config)# show ip ospf lsdb
OSPF Router with ID (10.1.0.254) (Process ID 1 VRF default)
=============================================================

Router Link State Advertisements (Area 0.0.0.0)
------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum       Link Count
-------------------------------------------------------------------------------
10.1.0.254      10.1.0.254      46         0x80000002 0x000060e9     2
10.254.0.253    10.254.0.253    52         0x80000150 0x00002ca7    15

Inter-area Summary Link State Advertisements (Area 0.0.0.0)
------------------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum
--------------------------------------------------------------
10.1.0.2        10.1.0.254      51         0x80000001 0x00005889
10.1.0.3        10.1.0.254      51         0x80000001 0x00004e92
10.1.0.254      10.1.0.254      51         0x80000001 0x00008abe
10.1.2.0        10.1.0.254      51         0x80000001 0x0000423b
10.1.21.0       10.1.0.254      51         0x80000001 0x000070f9
10.254.101.0    10.1.0.254      51         0x80000001 0x00002957
10.254.102.0    10.1.0.254      51         0x80000001 0x00001e61

Router Link State Advertisements (Area 0.0.0.1)
------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum       Link Count
-------------------------------------------------------------------------------
10.1.0.2        10.1.0.2        176        0x80000032 0x0000077e     6
10.1.0.3        10.1.0.3        25         0x8000001d 0x00001480     6
10.1.0.254      10.1.0.254      54         0x80000036 0x00000852     5

Inter-area Summary Link State Advertisements (Area 0.0.0.1)
```

```
------------------------------------------------------------

LSID             ADV Router       Age        Seq#       Checksum
--------------------------------------------------------------
10.254.0.253     10.1.0.254       46         0x80000001 0x0000984f
10.254.1.0       10.1.0.254       55         0x80000001 0x0000796b
10.254.3.0       10.1.0.254       46         0x80000001 0x0000637f
10.254.4.0       10.1.0.254       46         0x80000001 0x00005889
10.254.6.0       10.1.0.254       46         0x80000001 0x0000429d
10.254.7.0       10.1.0.254       46         0x80000001 0x000037a7
10.254.8.0       10.1.0.254       46         0x80000001 0x00002cb1
10.254.9.0       10.1.0.254       46         0x80000001 0x000021bb
10.254.10.0      10.1.0.254       46         0x80000001 0x000016c5
10.254.11.0      10.1.0.254       46         0x80000001 0x00000bcf
10.254.12.0      10.1.0.254       46         0x80000001 0x0000ffd9
10.254.13.0      10.1.0.254       46         0x80000001 0x0000f4e3
10.254.14.0      10.1.0.254       46         0x80000001 0x0000e9ed
10.254.15.0      10.1.0.254       46         0x80000001 0x0000def7

AS External Link State Advertisements
--------------------------------------

LSID             ADV Router       Age        Seq#       Checksum
--------------------------------------------------------------
0.0.0.0          10.1.0.254       1541       0x80000019 0x0000604f
10.2.1.0         10.1.0.254       968        0x80000002 0x0000d9c7
10.2.1.127       10.1.0.254       968        0x80000002 0x0000e1bf
10.2.1.128       10.1.0.254       968        0x80000002 0x0000d7c8
10.2.2.0         10.1.0.254       968        0x80000002 0x0000ced1
10.2.4.0         10.1.0.254       968        0x80000002 0x0000a9f7
10.2.8.0         10.1.0.254       968        0x80000002 0x00007d20
10.3.1.0         10.1.0.254       525        0x80000001 0x0000cfd1
10.3.2.0         10.1.0.254       525        0x80000001 0x0000c4db
10.3.4.0         10.1.0.254       525        0x80000001 0x00009f02
10.3.8.0         10.1.0.254       525        0x80000001 0x0000732a
```

Analyze a Multi-Area Route

You will now focus on one of the routes you learned from the backbone router.

4. On rtr-core1, check the number of router LSAs in the area0.

```
show ip ospf lsdb area 0
```

```
rtr-core1-IACA(config)# show ip ospf lsdb area 0
OSPF Router with ID (10.1.0.254) (Process ID 1 VRF default)
============================================================

Router Link State Advertisements (Area 0.0.0.0)
------------------------------------------------

LSID             ADV Router       Age        Seq#       Checksum        Link Count
-------------------------------------------------------------------------------
10.1.0.254       10.1.0.254       150        0x80000002 0x000060e9       2
10.254.0.253     10.254.0.253     156        0x80000150 0x00002ca7      15
```

```
Inter-area Summary Link State Advertisements (Area 0.0.0.0)
------------------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum
--------------------------------------------------------------
10.1.0.2        10.1.0.254      155        0x80000001 0x00005889
10.1.0.3        10.1.0.254      155        0x80000001 0x00004e92
10.1.0.254      10.1.0.254      155        0x80000001 0x00008abe
10.1.2.0        10.1.0.254      155        0x80000001 0x0000423b
10.1.21.0       10.1.0.254      155        0x80000001 0x000070f9
10.254.101.0    10.1.0.254      155        0x80000001 0x00002957
10.254.102.0    10.1.0.254      155        0x80000001 0x00001e61
```

- **Question**: How many router LSAs do you observe in area 0?
- **Answer**: 2: one for the rtr-core1 and one for the backbone router.
- **Question**: How many links are advertised by the backbone router (10.254.0.253) using its router LSA?
- **Answer**: The backbone router has more than 10 connected networks. These links are reported in the backbone router LSA. rtr-core1 learns these routes as being attached to the backbone router.
- **Question**: What LSA type will these routes be advertised in the area 1?
- **Answer**: Each of these routes will be advertised as an LSA type 3 (summary LSA) into area 1.

5. On rtr-core1, check the number of summary LSAs in area 1.

```
show ip ospf lsdb area 1
```

```
rtr-core1-IACA(config)# show ip ospf lsdb area 1
OSPF Router with ID (10.1.0.254) (Process ID 1 VRF default)
============================================================

Router Link State Advertisements (Area 0.0.0.1)
------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum       Link Count
-------------------------------------------------------------------------------
10.1.0.2        10.1.0.2        365        0x80000032 0x0000077e     6
10.1.0.3        10.1.0.3        214        0x8000001d 0x00001480     6
10.1.0.254      10.1.0.254      243        0x80000036 0x00000852     5

Inter-area Summary Link State Advertisements (Area 0.0.0.1)
------------------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum
--------------------------------------------------------------
10.254.0.253    10.1.0.254      234        0x80000001 0x0000984f
10.254.1.0      10.1.0.254      243        0x80000001 0x0000796b
10.254.3.0      10.1.0.254      234        0x80000001 0x0000637f
```

```
10.254.4.0       10.1.0.254       234        0x80000001 0x00005889
10.254.6.0       10.1.0.254       234        0x80000001 0x0000429d
10.254.7.0       10.1.0.254       234        0x80000001 0x000037a7
10.254.8.0       10.1.0.254       235        0x80000001 0x00002cb1
10.254.9.0       10.1.0.254       235        0x80000001 0x000021bb
10.254.10.0      10.1.0.254       235        0x80000001 0x000016c5
10.254.11.0      10.1.0.254       235        0x80000001 0x00000bcf
10.254.12.0      10.1.0.254       235        0x80000001 0x0000ffd9
10.254.13.0      10.1.0.254       235        0x80000001 0x0000f4e3
10.254.14.0      10.1.0.254       235        0x80000001 0x0000e9ed
10.254.15.0      10.1.0.254       235        0x80000001 0x0000def7
```

- **Question**: How many summary LSAs do you count?
- **Answer**: More than 10. For each prefix that is learned from the backbone router, a summary LSA will be generated in the area 1 by the area border.

Review the LSDB on Intra-Area Router

6. On sw-agg1, review the LSDB.

```
show ip ospf lsdb
```

```
sw-agg1(config)# show ip ospf lsdb
OSPF Router with ID (10.1.0.2) (Process ID 1 VRF default)
==========================================================

Router Link State Advertisements (Area 0.0.0.1)
------------------------------------------------

LSID             ADV Router       Age        Seq#       Checksum       Link Count
------------------------------------------------------------------------------
10.1.0.2         10.1.0.2         199        0x80000036 0x0000fe82     6
10.1.0.3         10.1.0.3         198        0x80000021 0x00000c84     6
10.1.0.254       10.1.0.254       198        0x8000003c 0x0000fb58     5

Inter-area Summary Link State Advertisements (Area 0.0.0.1)
------------------------------------------------------------

LSID             ADV Router       Age        Seq#       Checksum
--------------------------------------------------------------
10.254.0.253     10.1.0.254       203        0x80000001 0x0000984f
10.254.1.0       10.1.0.254       209        0x80000001 0x0000796b
10.254.3.0       10.1.0.254       203        0x80000001 0x0000637f
10.254.4.0       10.1.0.254       203        0x80000001 0x00005889
10.254.6.0       10.1.0.254       203        0x80000001 0x0000429d
10.254.7.0       10.1.0.254       203        0x80000001 0x000037a7
10.254.8.0       10.1.0.254       203        0x80000001 0x00002cb1
10.254.9.0       10.1.0.254       203        0x80000001 0x000021bb
10.254.10.0      10.1.0.254       203        0x80000001 0x000016c5
10.254.11.0      10.1.0.254       203        0x80000001 0x00000bcf
10.254.12.0      10.1.0.254       203        0x80000001 0x0000ffd9
10.254.13.0      10.1.0.254       203        0x80000001 0x0000f4e3
10.254.14.0      10.1.0.254       203        0x80000001 0x0000e9ed
10.254.15.0      10.1.0.254       203        0x80000001 0x0000def7
```

```
AS External Link State Advertisements
-------------------------------------

LSID            ADV Router      Age        Seq#       Checksum
-----------------------------------------------------------------
0.0.0.0         10.1.0.254      209        0x8000001b 0x00005c51
10.2.1.0        10.1.0.254      209        0x80000004 0x0000d5c9
10.2.1.127      10.1.0.254      209        0x80000004 0x0000ddc1
10.2.1.128      10.1.0.254      209        0x80000004 0x0000d3ca
10.2.2.0        10.1.0.254      209        0x80000004 0x0000cad3
10.2.4.0        10.1.0.254      209        0x80000004 0x0000a5f9
10.2.8.0        10.1.0.254      209        0x80000004 0x00007922
10.3.1.0        10.1.0.254      209        0x80000003 0x0000cbd3
10.3.2.0        10.1.0.254      211        0x80000003 0x0000c0dd
10.3.4.0        10.1.0.254      211        0x80000003 0x00009b04
10.3.8.0        10.1.0.254      211        0x80000003 0x00006f2c
```

- **Question**: Did you receive any new router (LSA Type1) or network (LSA Type2) LSAs?
- **Answer**: No, the topology inside area 1 did not change; there are no new router or network LSAs.
- **Question**: Do you see the summary (LSA Type3) LSAs in the LSDB?
- **Answer**: Yes, the summary LSAs are also replicated across all routers in the area.

7. Review the OSPF routing table.

```
show ip ospf route
```

```
sw-agg1(config)# show ip ospf route
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPF Process ID 1 VRF default, Routing Table
---------------------------------------------

Total Number of Routes : 32

0.0.0.0/0          (E2)
     via 10.254.101.254 interface 1/1/8, cost 1 distance 110
10.1.0.3/32        (i) areAnswer: 0.0.0.1
     via 10.1.2.3 interface vlan2, cost 100 distance 110
10.1.0.254/32      (i) areAnswer: 0.0.0.1
     via 10.254.101.254 interface 1/1/8, cost 100 distance 110
10.1.2.0/24        (i) areAnswer: 0.0.0.1
     directly attached to interface vlan2, cost 100 distance 110
10.1.21.0/24       (i) areAnswer: 0.0.0.1
     directly attached to interface vlan21, cost 100 distance 110
10.2.1.0/24        (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
10.2.1.0/25        (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
```

```
10.2.1.128/25      (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
10.2.2.0/24        (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
10.2.4.0/22        (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
10.2.8.0/22        (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
10.3.1.0/24        (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
10.3.2.0/24        (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
10.3.4.0/22        (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
10.3.8.0/22        (E2)
     via 10.254.101.254 interface 1/1/8, cost 25 distance 110
10.254.0.253/32    (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.1.0/24      (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.3.0/24      (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.4.0/24      (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.6.0/24      (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.7.0/24      (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.8.0/24      (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.9.0/24      (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.10.0/24     (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.11.0/24     (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.12.0/24     (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.13.0/24     (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.14.0/24     (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.15.0/24     (I)
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
10.254.101.0/24    (i) areAnswer: 0.0.0.1
     directly attached to interface 1/1/8, cost 100 distance 110
10.254.102.0/24    (i) areAnswer: 0.0.0.1
     via 10.1.2.3 interface vlan2, cost 200 distance 110
10.254.102.0/24    (i) areAnswer: 0.0.0.1
     via 10.254.101.254 interface 1/1/8, cost 200 distance 110
```

- **Question**: Did OSPF calculate a path for the new routes?
- **Answer**: Yes, the path to the ABR that advertised the summary LSA was calculated and the cost of the summary LSA was added. This is the resulting route for the inter-area routes.

- **Question**: What code is used for the inter-area routes?
- **Answer**: In the OSPF routing table, the code *I* is used for the inter-area OSPF routes.

8. Check the IP routing table.

```
show ip route
```

```
sw-agg1(config)# show ip route ospf

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2

VRF: default

Prefix              Nexthop          Interface     VRF(egress)       Origin/   Distance/
Age
                                                                      Type      Metric
------------------------------------------------------------------------------------------
0.0.0.0/0           10.254.101.254   1/1/8         -     O/E2       [110/1]       00h:07m:06s
10.1.0.3/32         10.1.2.3         vlan2         -     O          [110/100]     13h:34m:51s
10.1.0.254/32       10.254.101.254   1/1/8         -     O          [110/100]     00h:07m:06s
10.2.1.0/24         10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.2.1.0/25         10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.2.1.128/25       10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.2.2.0/24         10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.2.4.0/22         10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.2.8.0/22         10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.3.1.0/24         10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.3.2.0/24         10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.3.4.0/22         10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.3.8.0/22         10.254.101.254   1/1/8         -     O/E2       [110/25]      00h:07m:06s
10.254.0.253/32     10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.1.0/24       10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.3.0/24       10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.4.0/24       10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.6.0/24       10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.7.0/24       10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.8.0/24       10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.9.0/24       10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.10.0/24      10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.11.0/24      10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.12.0/24      10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.13.0/24      10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.14.0/24      10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.15.0/24      10.254.101.254   1/1/8         -     O/IA       [110/200]     00h:07m:06s
10.254.102.0/24     10.254.101.254   1/1/8         -     O          [110/200]     00h:07m:06s
                    10.1.2.3         vlan2         -                [110/200]     00h:07m:06s
```

```
Total Route Count : 28
```

- **Question**: How can you distinguish the intra and inter-area OSPF routes?
- **Answer**: Based on the origin (*O* for OSPF) and type *IA* (inter-area).

Route Summarization of Backbone Routes

Currently all the individual routes can be observed. Using route summarization, it is possible to aggregate matching routes into an aggregate route.

This aggregation is performed by the ABR; therefore it must be configured on the ABR.

9. On the rtr-core1, configure route aggregation for 10.254.0.0/16 for area 0.

```
router ospf 1
 area 0 range 10.254.0.0/16 type inter-area
 exit
```

```
rtr-core1-IACA(config)# router ospf 1
rtr-core1-IACA(config-ospf-1)# area 0 range 10.254.0.0/16 type inter-area
rtr-core1-IACA(config-ospf-1)# exit
```

10. Review the LSDB for area 1.

```
show ip ospf lsdb area 1
```

```
rtr-core1-IACA(config)# show ip ospf lsdb area 1
OSPF Router with ID (10.1.0.254) (Process ID 1 VRF default)
============================================================

Router Link State Advertisements (Area 0.0.0.1)
------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum       Link Count
-------------------------------------------------------------------------------
10.1.0.2        10.1.0.2        1491       0x80000036 0x0000fe82     6
10.1.0.3        10.1.0.3        1490       0x80000021 0x00000c84     6
10.1.0.254      10.1.0.254      1489       0x8000003c 0x0000fb58     5

Inter-area Summary Link State Advertisements (Area 0.0.0.1)
------------------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum
--------------------------------------------------------------
10.254.0.0      10.1.0.254      20         0x80000001 0x00008461
```

- **Question**: How many summary LSAs do you count for area 1?
- **Answer**: 1, the summary entry for the aggregate route you have just created.

11. On sw-agg1, review the updated routing table. The detailed routes have been removed and only the aggregate route 10.254.0.0/16 is listed in the routing table.

```
show ip ospf lsdb summary
```

```
sw-agg1(config)# show ip ospf lsdb summary
OSPF Router with ID (10.1.0.2) (Process ID 1 VRF default)
==========================================================

Inter-area Summary Link State Advertisements (Area 0.0.0.1)
------------------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum
--------------------------------------------------------------
10.254.0.0      10.1.0.254      168        0x80000001 0x00008461
```

```
show ip route
```

```
sw-agg1(config)# show ip route ospf

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2

VRF: default

Prefix              Nexthop           Interface     VRF(egress)       Origin/   Distance/
Age
                                                                       Type      Metric
-----------------------------------------------------------------------------------------
--------------
0.0.0.0/0           10.254.101.254    1/1/8         -     O/E2      [110/1]     00h:27m:49s
10.1.0.3/32         10.1.2.3          vlan2         -     O         [110/100]   13h:55m:34s
10.1.0.254/32       10.254.101.254    1/1/8         -     O         [110/100]   00h:27m:49s
10.2.1.0/24         10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.2.1.0/25         10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.2.1.128/25       10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.2.2.0/24         10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.2.4.0/22         10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.2.8.0/22         10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.3.1.0/24         10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.3.2.0/24         10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.3.4.0/22         10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.3.8.0/22         10.254.101.254    1/1/8         -     O/E2      [110/25]    00h:27m:49s
10.254.0.0/16       10.254.101.254    1/1/8         -     O/IA      [110/200]   00h:03m:21s
10.254.102.0/24     10.254.101.254    1/1/8         -     O         [110/200]   00h:27m:49s
                    10.1.2.3          vlan2         -               [110/200]   00h:27m:49s
```

Route Summarization of Campus Routes

In the same way, all the specific routes from the campus environment can be summarized into an aggregate route.

Since all the campus routes are in the 10.1.0.0/16 range, it is a good candidate as an aggregate route.

12. On rtr-core1, check the Summary LSA count in the backbone area.

```
show ip ospf lsdb area 0
show ip ospf lsdb database-summary
```

```
rtr-core1-IACA(config)# show ip ospf lsdb area 0
OSPF Router with ID (10.1.0.254) (Process ID 1 VRF default)
============================================================

Router Link State Advertisements (Area 0.0.0.0)
------------------------------------------------

LSID            ADV Router      Age       Seq#       Checksum       Link Count
-------------------------------------------------------------------------------
10.1.0.254      10.1.0.254      1766      0x80000006 0x000058ed      2
10.254.0.253    10.254.0.253    67        0x80000155 0x000022ac     15

Inter-area Summary Link State Advertisements (Area 0.0.0.0)
------------------------------------------------------------

LSID            ADV Router      Age       Seq#       Checksum
--------------------------------------------------------------
10.1.0.2        10.1.0.254      1755      0x80000001 0x00005889
10.1.0.3        10.1.0.254      1750      0x80000002 0x00004c93
10.1.0.254      10.1.0.254      1766      0x80000002 0x000088bf
10.1.2.0        10.1.0.254      1755      0x80000001 0x0000423b
10.1.21.0       10.1.0.254      1755      0x80000001 0x000070f9
10.254.101.0    10.1.0.254      1766      0x80000002 0x00002758
10.254.102.0    10.1.0.254      1766      0x80000002 0x00001c62
```

```
rtr-core1-IACA(config)# show ip ospf lsdb database-summary
OSPF Router with ID (10.1.0.254) (Process ID 1 VRF default)
============================================================

Area 0.0.0.0 database summary
------------------------------

LSA Type                Count
---------------------------
Router                  2
Network                 0
Inter-area Summary      7
ASBR Summary            0
NSSA External           0
Subtotal                9
...
```

- **Question**: How many summary LSAs (OSPF routes from other areas, in this lab these are routes from area 1) do you count in the backbone area?
- **Answer**: In the example output, there are 7 inter-area entries.

13. On rtr-core1, apply the aggregate route for the Campus area 1.

```
router ospf 1
 area 1 range 10.1.0.0/16 type inter-area
 exit
```

```
rtr-core1-IACA(config)# router ospf 1
rtr-core1-IACA(config-ospf-1)# area 1 range 10.1.0.0/16 type inter-area
rtr-core1-IACA(config-ospf-1)# exit
```

14. On rtr-core1, review the summary LSA count again for the backbone area.

```
show ip ospf lsdb summary area 0
show ip ospf lsdb database-summary
```

```
rtr-core1-IACA(config)# show ip ospf lsdb summary area 0
OSPF Router with ID (10.1.0.254) (Process ID 1 VRF default)
============================================================

Inter-area Summary Link State Advertisements (Area 0.0.0.0)
------------------------------------------------------------

LSID            ADV Router      Age        Seq#       Checksum
--------------------------------------------------------------
10.1.0.0        10.1.0.254      57         0x80000001 0x00005827
10.254.101.0    10.1.0.254      251        0x80000003 0x00002559
10.254.102.0    10.1.0.254      251        0x80000003 0x00001a63
```

```
rtr-core1-IACA(config)# show ip ospf lsdb database-summary
OSPF Router with ID (10.1.0.254) (Process ID 1 VRF default)
============================================================

Area 0.0.0.0 database summary
------------------------------

LSA Type             Count
---------------------------
Router               2
Network              0
Inter-area Summary   3
ASBR Summary         0
NSSA External        0
Subtotal             5
...
```

- **Question**: Did the summary LSA count change?
- **Answer**: Yes, the routes matching 10.1.0.0/16 are now aggregated.

Task 4: Enhance OSPF Neighbor State Detection with BFD

When OSPF routers are not physically directly connected, a link failure on one side cannot be detected by the peer router immediately.

This can happen when two routers are connected via other switches, for example.

In this case, OSPF needs to rely on hello and dead timers to detect if the peer is alive or not. Unfortunately, the most realistic time period before something is done is based on the dead interval, which is 40 seconds, by default. And since the recommendation is to have the dead interval set to 4x the hello interval, the lowest you could set the dead interval to, realistically, is 4 seconds. Another method is needed if you need faster convergence than this.

To solve this, Bi-directional Forward Detection (BFD) can be used as a fast keepalive protocol. BFD is be used by many different protocols (not just OSPF or even routing protocols in general). In this lab you will use it in combination with OSPF.

The rtr-core1 in the lab is a virtual router that runs on a VMware hypervisor. It is connected via lab switches to your aggregation switches on their port 1/1/8.

This means that shutting down the port 1/1/8 on the aggregation switch will not be seen by the rtr-core1. The rtr-core1 would still see its port as UP, and only when the hello timers expire, OSPF would report the neighbor as down. This will take up to 40 seconds with the default timers. Using BFD, this can be detected in less than one second, if required.

Objectives

- Configure and monitor BFD.

Steps

Review the Problem

1. Use the MGMT PC and open an SSH connection to sw-agg1.

> **NOTE:** Do not use a console connection. An SSH connection is required to use the **terminal-monitor** command. Use **logging console** if using a console connection.

2. Enable **Terminal-monitor** in SSH to see live event messages.

```
terminal-monitor
```

```
sw-agg1(config)# terminal-monitor
Terminal-monitor is enabled successfully
```

3. Review the OSPF neighbor details.

```
show ip ospf neighbors detail
```

```
sw-agg1(config)# show ip ospf neighbors detail
VRF   : default                               Process : 1
---------------------------------------------------------

Router-Id       : 10.1.0.254        Area Id            : 0.0.0.1
Interface       : 1/1/8             Address            : 10.254.101.254
State           : FULL              Neighbor Priority  : n/a
DR              : No                BDR                : No
Dead Timer Due  : 00:00:32          Options            : 0x42
Retransmission Queue Length  : 1
Time Since Last State Change : 00h:03m:08s
...
```

- **Question**: What is the current dead time?

- **Answer**: The dead timer counts down from 40 to 0. The rtr-core1 is using the default OSPF hello timer of 10 seconds. This means that the dead timer will be reset every 10 seconds when it receives a hello message. In your output, the dead timers should be anywhere between 30 and 40 seconds.

4. On rtr-core1, disable the port 1/1/1. Since the link is not directly connected to sw-agg1,

```
interface 1/1/1
 shutdown
 exit
```

```
rtr-core1-IACA(config)# interface 1/1/1
rtr-core1-IACA(config-if)# shutdown
rtr-core1-IACA(config-if)# exit
```

5. On sw-agg1, verify the OSPF neighbor details again. You should see the dead timer is no longer reset and will become lower than 30.

```
show ip ospf neighbors detail
```

```
sw-agg1(config)# show ip ospf neighbors detail
VRF   : default                               Process : 1
---------------------------------------------------------

Router-Id       : 10.1.0.254        Area Id            : 0.0.0.1
Interface       : 1/1/8             Address            : 10.254.101.254
State           : FULL              Neighbor Priority  : n/a
DR              : No                BDR                : No
Dead Timer Due  : 00:00:08          Options            : 0x42
Retransmission Queue Length  : 1
Time Since Last State Change : 00h:03m:08s
```

6. On sw-agg1, verify that the port 1/1/8 is still *up*. This is because the rtr-core1 and the sw-agg1 are not physically connected.

```
show interface brief
```

```
sw-agg1(config)# show interface brief
```

```
--------------------------------------------------------------------------------------------------------
Port      Native  Mode   Type           Enabled Status  Reason                 Speed
Description
          VLAN                                                                 (Mb/s)
------------------------------------------------------------------------------------------
...
1/1/7     --      routed SFP-BT         no      down    Administratively down  --      --
1/1/8     --      routed SFP-BT         yes     up                             1000
rtr-core1-1/1/1
1/1/9     --      routed --             no      down    No XCVR installed      --      --
...
```

7. Once the dead timer expires, an event will also show up.

```
2022-12-19T13:00:53.110341+0000 hpe-routing[7805] <INFO>
Event|2401|LOG_INFO|AMM|1/1|AdjChg: Nbr  rtr ID 10.1.0.254 on IP addr 10.254.101.2( area
ID 0.0.0.1): Full -> Down
```

8. On rtr-core1, restore the link.

```
interface 1/1/1
 no shutdown
 exit
```

```
rtr-core1-IACA(config)# interface 1/1/1
rtr-core1-IACA(config-if)# no shutdown
rtr-core1-IACA(config-if)# exit
```

Enable BFD

In the next steps, you will enable BFD. When enabled for OSPF, BFD will use a dedicated keepalive, via UDP messages, between the OSPF routers on the link. You will use the default timers for BFD. If you want convergence faster than one second, you would need to tune the BFD hello and dead interval timers.

9. On sw-agg1, enable global BFD.

```
bfd
```

```
sw-agg1(config)# bfd
```

10. On sw-agg1, enable BFD on OSPF interface 1/1/8.

```
interface 1/1/8
 ip ospf bfd
 exit
```

```
sw-agg1(config)# interface 1/1/8
sw-agg1(config-if)# ip ospf bfd
sw-agg1(config-if)# exit
```

11. On rtr-core1, enable BFD globally.

```
bfd
```

```
rtr-core1-IACA(config)# bfd
```

12. On rtr-core1, enable BFD on the OSPF interface 1/1/1.

```
interface 1/1/1
 ip ospf bfd
 exit
```

```
rtr-core1-IACA(config)# interface 1/1/1
rtr-core1-IACA(config-if)# ip ospf bfd
rtr-core1-IACA(config-if)# exit
```

13. Verify that the BFD session is *up*.

```
show bfd
```

```
rtr-core1-IACA(config)# show bfd

Admin status: enabled
Echo source IP: N/A
Statistics:
Total number of control packets transmitted: 6
Total number of control packets received: 6
Total number of control packets dropped: 0
Session Interface VRF       Source IP       Destination IP    Echo     State    Protocol
------- --------- --------- ------------------------------------- ----------------------
1       1/1/1     default   10.254.101.254  10.254.101.2      N/A      up           ospf
```

14. On sw-agg1, an event will be displayed with the up BFD session.

```
2022-12-19T13:14:02.998869+0000 ops-switchd[3384] <INFO> Event|7307|LOG_INFO|AMM|1/1|BFD
session is up. session_id=1, vrf=0, op_mode=async_and_echo, src_port=1/1/8,
dest_ip=10.254.101.254, local_state=up, local_diag=no_diagnostic, remote_state=up,
remote_diag=no_diagnostic
```

Repeat the Link Failure Test

15. On rtr-core1, shutdown the port 1/1/1.

```
interface 1/1/1
 shutdown
 exit
```

```
rtr-core1-IACA(config)# interface 1/1/1
rtr-core1-IACA(config-if)# shutdown
rtr-core1-IACA(config-if)# exit
```

16. On sw-agg1, review the events. Immediately after the BFD session is reported as down, the OSPF adjacency will be down as well. This demonstrates how BFD can assist with the neighbor state detection when two routers are connected via indirect links.

```
2022-12-19T13:16:03.256821+0000 ops-switchd[3384] <INFO> Event|7308|LOG_INFO|AMM|1/1|BFD
session is down. session_id=1, vrf=0, op_mode=async_and_echo, src_port=1/1/8,
dest_ip=10.254.101.254, local_state=down, local_diag=control_detection_time_expired,
remote_state=up, remote_diag=no_diagnostic

2022-12-19T13:16:03.257177+0000 ops-switchd[3384] <ERR> Event|7315|LOG_ERR|AMM|1/1|BFD
session is unidirectional. session_id=1, vrf=0, op_mode=async_and_echo, src_port=1/1/8,
dest_ip=10.254.101.254, local_state=down, local_diag=control_detection_time_expired,
remote_state=up, remote_diag=no_diagnostic

2022-12-19T13:16:03.263600+0000 hpe-routing[7805] <INFO>
Event|2401|LOG_INFO|AMM|1/1|AdjChg: Nbr  rtr ID 10.1.0.254 on IP addr 10.254.101.2( area
ID 0.0.0.1): Full -> Down
```

Restore the Link

17. On rtr-core1, enable the port 1/1/1 again.

```
interface 1/1/1
 no shutdown
 exit
```

```
rtr-core1-IACA(config)# interface 1/1/1
rtr-core1-IACA(config-if)# no shutdown
rtr-core1-IACA(config-if)# exit
```

18. On sw-agg1, disable terminal monitor (or logging console)

```
no terminal-monitor
```

```
sw-agg1(config)# no terminal-monitor
```

Save Configurations and Create Checkpoint

1. On sw-agg1, sw-agg2 and rtr-core1, save the configurations.

```
write mem
```

2. On sw-agg1 and sw-agg2, copy the running-config to a checkpoint named **iaca-lab0202-done**.

```
copy running-config checkpoint iaca-lab0202-done
```

```
sw-agg1(config)# copy running-config checkpoint iaca-lab0202-done
Copying configuration: [Success]
```

```
sw-agg2(config)# copy running-config checkpoint iaca-lab0202-done
Copying configuration: [Success]
```

You have completed this Lab!

Lab 02.03 Campus Wired with Central

Overview

In this lab you will connect the switches to Aruba Central.

The edge switches will be configured using ZTP (zero touch provisioning). This will allow them to connect in a factory default state to Aruba Central.

In Aruba Central you will configure the physical locations; these are referred to as sites.

The edge switches will be configured using a template group. You will learn how to import and build your own template and apply logic in the template using device variables.

In the last section of the lab, you will connect and configure the aggregation switches with Aruba Central as well, using a pre-defined template.

Objectives

After completing this lab, you will be able to:

- Understand and prepare ZTP.
- Configure Aruba Central sites and groups.
- Configure and build templates for switch management.
- Configure conditional logic in a template using variables.

Task 1: Onboard a switch to Central with ZTP

In this task you will first prepare the aggregation switches to support ZTP on the edge switch sw-edge1.

A new VSX LAG will be created to connect to sw-edge1 and VLAN 3 (with SVI 3) will be configured to support the management IP addresses of the edge switches.

To support ZTP, IP helper (DHCP relay) is configured on the SVI 3.

The next section in the lab will have you test how a factory default switch can be connected to an LACP VSX LAG using the LACP fallback feature.

Objectives

- Configure aggregation VSX LAG to support ZTP.
- Understand the LACP fallback feature.
- Verify switch connectivity to Aruba Central.

Steps

Prepare the Environment

In this section you will configure SVI1 and SVI3 on the aggregation switches.

The sw-edge2 will be configured with a static management IP and Aruba Central support will be enabled.

> **TIP:** On the MGMT PC, in the IACA Student Files folder (on the desktop), you can find these configuration snippets. You can use them to easily copy and paste the configurations to the devices.

On sw-agg1, apply the SVI 1 and SVI 3 configuration.

```
interface lag 1 multi-chassis
 no shutdown
 vlan trunk allowed 1,3-4,11-15,21-25
 exit

interface 1/1/1
 lag 1
 no shutdown

interface vlan 1
 ip address 10.1.1.2/24
 active-gateway ip mac 12:01:00:00:01:00
 active-gateway ip 10.1.1.1
 ip helper-address 10.254.1.21
 ip ospf 1 area 0.0.0.1
 exit

interface vlan 3
 ip address 10.1.3.2/24
```

```
 active-gateway ip mac 12:01:00:00:01:00
 active-gateway ip 10.1.3.1
 ip helper-address 10.254.1.21
 ip ospf 1 area 0.0.0.1
 exit
```

On sw-agg2, apply the SVI 1 and SVI 3 configuration.

```
interface lag 1 multi-chassis
 no shutdown
 vlan trunk allowed 1,3-4,11-15,21-25
 exit

interface 1/1/1
 lag 1
 no shutdown

interface vlan 1
 ip address 10.1.1.3/24
 active-gateway ip mac 12:01:00:00:01:00
 active-gateway ip 10.1.1.1
 ip helper-address 10.254.1.21
 ip ospf 1 area 0.0.0.1
 exit

interface vlan 3
 ip address 10.1.3.3/24
 active-gateway ip mac 12:01:00:00:01:00
 active-gateway ip 10.1.3.1
 ip helper-address 10.254.1.21
 ip ospf 1 area 0.0.0.1
 exit
```

On sw-edge2, apply a static mgmt IP address and default gateway

```
interface vlan 3
 ip address 10.1.3.5/24
 exit
ip route 0.0.0.0/0 10.1.3.1
```

Enable Aruba Central support: this was disabled by the ZTP script.

```
aruba-central
 enable
 exit
```

Onboard switch sw-edge1 to Central with ZTP

On sw-edge1, review the SVI 1 DHCP client.

```
show ip dhcp
```

```
6300# show ip dhcp
INTERFACE-NAME        ADDRESS  DEFAULT_GATEWAY    DOMAIN_NAME      VRF        DNS-SERVERS
-----------------------------------------------------------------------------------------
```

```
vlan1
default
```

- **Question**: Did the sw-edge1 switch receive a DHCP address?
- **Answer**: No. Without a DHCP address, the ZTP process cannot start and the switch will not be able to access Aruba Central.

Let's investigate on the aggregation switches.

On sw-agg1, review the LACP status.

```
show lacp interfaces
```

```
sw-agg1(config)# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
---------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
---------------------------------------------------------------------------------
1/1/1      lag1(mc)   1     1     ALFOE   02:01:00:00:01:00 65534  1    lacp-block
1/1/2      lag2(mc)   2     1     ALFNCD  02:01:00:00:01:00 65534  2    up
1/1/46     lag256     47    1     ALFNCD  b8:d4:e7:d9:3d:00 65534  256  up
1/1/47     lag256     48    1     ALFNCD  b8:d4:e7:d9:3d:00 65534  256  up


Partner details of all interfaces:
---------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
---------------------------------------------------------------------------------
1/1/1      lag1(mc)   0     0     PLFOEX  00:00:00:00:00:00 0      0
1/1/2      lag2(mc)   28    1     ALFNCD  64:e8:81:3f:b5:00 65534  256
1/1/46     lag256     47    1     ALFNCD  b8:d4:e7:d9:ed:00 65534  256
1/1/47     lag256     48    1     ALFNCD  b8:d4:e7:d9:ed:00 65534  256
```

- **Question**: What is the status for port 1/1/1 (LAG1)?
- **Answer**: The status is lacp-blocked.
- **Question**: Why?
- **Answer**: The sw-edge1 peer does not have LACP configured since it is factory default.
- **Question**: How can you solve this?

- **Answer**: LACP fallback mode must be enabled in the LAG context on the aggregation switches. When the aggregation switches don't receive any LACP messages, the LAG will be set to forwarding when fallback mode is enabled.

On sw-agg1, enable LACP fallback on the LAGs to the edge switches.

```
interface lag 1
 lacp fallback
 exit

interface lag 2
 lacp fallback
 exit
```

```
sw-agg1(config)# interface lag 1
sw-agg1(config-lag-if)# lacp fallback
sw-agg1(config-lag-if)# exit
sw-agg1(config)#
sw-agg1(config)# interface lag 2
sw-agg1(config-lag-if)# lacp fallback
sw-agg1(config-lag-if)# exit
```

NOTE: Make sure to apply fallback to LAG 2 as well! sw-edge2 is currently statically configured, but in next task you will apply configuration templates. When you would make an error in the configuration, the sw-edge2 could use the DHCP/ZTP process to check in to Central again when fallback mode is configured on a LAG(s).

Review the LAG status.

```
show lacp interfaces
```

```
sw-agg1(config)# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
----------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
----------------------------------------------------------------------------
1/1/1      lag1(mc)   1     1     IE      02:01:00:00:01:00 65534  1    up
1/1/2      lag2(mc)   2     1     ALFNCD  02:01:00:00:01:00 65534  2    up
1/1/46     lag256     47    1     ALFNCD  b8:d4:e7:d9:3d:00 65534  256  up
1/1/47     lag256     48    1     ALFNCD  b8:d4:e7:d9:3d:00 65534  256  up
```

```
Partner details of all interfaces:
---------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
---------------------------------------------------------------------------------
1/1/1      lag1(mc)   0     0     IE      00:00:00:00:00:00 0      0
1/1/2      lag2(mc)   28    1     ALFNCD  64:e8:81:3f:b5:00 65534  256
1/1/46     lag256     47    1     ALFNCD  b8:d4:e7:d9:ed:00 65534  256
1/1/47     lag256     48    1     ALFNCD  b8:d4:e7:d9:ed:00 65534  256
```

- **Question**: What is the status of the port 1/1/1 after enabling LACP fallback?
- **Answer**: The port is now in an up state. The flags *IE* indicate that this happened because there is no LACP partner.
- **Question**: In the Partner details output, what is the system ID reported for port 1/1/1?
- **Answer**: Since there are no LACP messages, there is no LACP system ID. This is shown in the output as System ID 00:00:00:00:00:00.

Bounce sw-edge1 SVI1

While the aggregation switches now support traffic on their LAG, the sw-edge1 DHCP client is not aware of this, so you can bounce the SVI 1 to restart the DHCP client. A switch reboot could also be used.

On sw-edge1, bounce the SVI 1 interface to trigger the DHCP client.

```
config
interface vlan 1
shutdown
no shutdown
exit
```

```
6300# config
6300(config)# interface vlan 1
6300(config-if-vlan)# shutdown
6300(config-if-vlan)# no shutdown
6300(config-if-vlan)# exit
```

On sw-edge1, review DHCP client status.

```
show ip dhcp
```

```
6300(config)# show ip dhcp
INTERFACE-NAME  ADDRESS        DEFAULT_GATEWAY  DOMAIN_NAME         VRF      DNS-SERVERS
------------------------------------------------------------------------------------------
vlan1           10.1.1.52/24   10.1.1.1         aruba-training.com  default  10.254.1.21
```

Review the Aruba Central status.

```
show aruba-central
```

```
6300(config)# show aruba-central
Central admin state                      : enabled
```

```
Central location                        : device-uswest4-d2.central.arubanetworks.com
VRF for connection                      : default
Shared Token                            : N/A
Central connection status               : connected

Central source                          : activate
Central source connection status        : connected
Central source last connected on        : Mon Dec 19 14:46:23 UTC 2022
System time synchronized from Activate  : False

Activate Server URL                     : devices-v2.arubanetworks.com
CLI location                            : N/A
CLI VRF                                 : N/A

Source IP                               : 10.1.1.52
Source IP Overridden                    : False

Central support mode                    : disabled
```

Task 2: Aruba Central Initial Access

In this task you will explore some initial steps when connecting to an Aruba Central environment for the first time.

Objectives

- Access Aruba Central using HPE GLCP.
- Understand the core navigation flow in Aruba Central.
- Configure sites and labels in Aruba Central.

Steps

Access HPE GreenLake Cloud Platform (GLCP)

On your local system, use a browser to open a connection to the HPE GreenLake Cloud Platform: https://common.cloud.hpe.com.

Click **Sign In with SSO**. Enter the email address provided by your instructor and click **Next**.

You are now redirected to the Aruba Training Labs SAML host.

Enter the email address and password provided by your instructor and click **Login**.

You are now logged in to HPE GreenLake Cloud Platform.

Launch Aruba Central Application

From the Aruba Central tile, click **Launch**.

Aruba Central UI Navigation Instructions

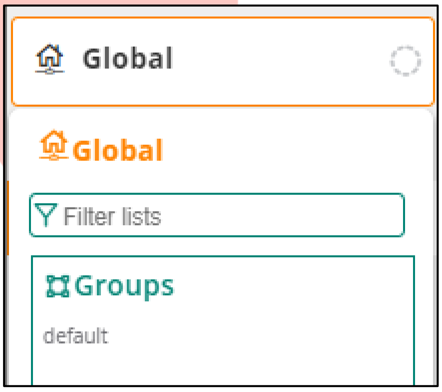
In the next steps you will be introduced to the core navigation structure in Aruba Central: using the context, navigation, and top areas. This will be used in the remainder of the labs to guide you to the correct Aruba Central screen.

Context Filter

The context filter is used to narrow the scope of the Aruba Central UI.

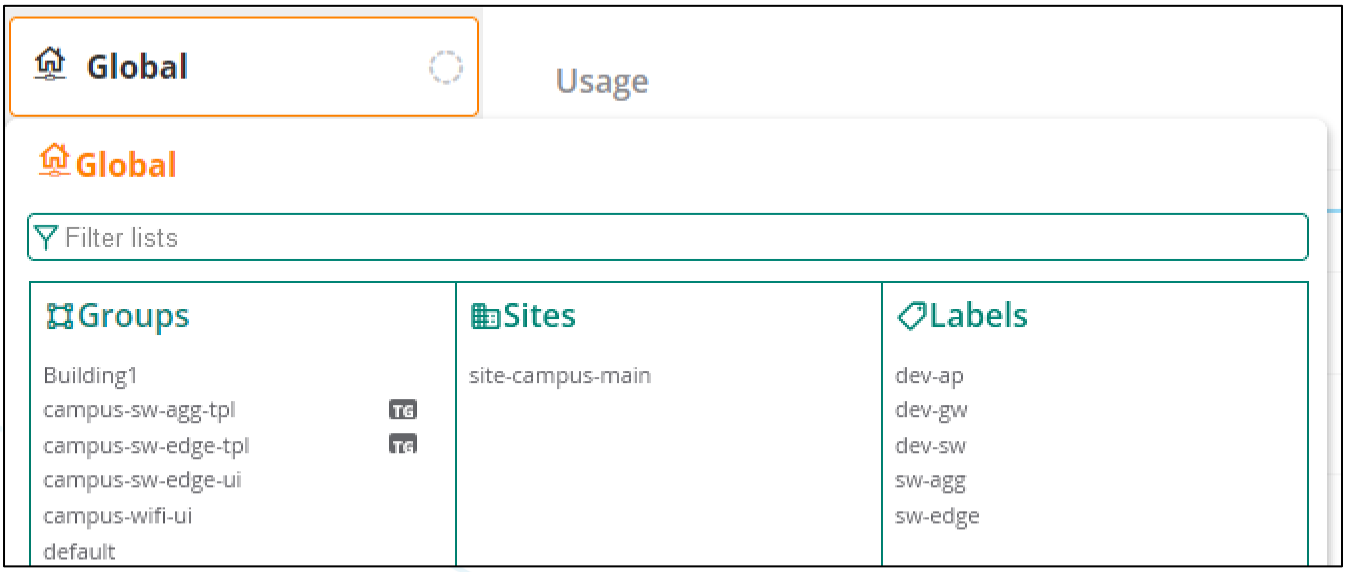
By default, the *Global* context is selected.

Click the context area to see a pop-up with context options. Currently, only the default group is listed in the context filter.



As you progress with the lab activities, additional groups, sites, and labels will show up in this context selection list.

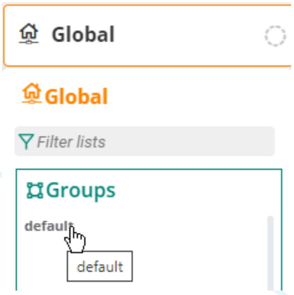
Example: Context filter with Groups, Sites and Labels:

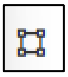


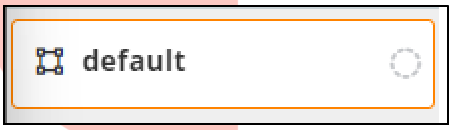
In the lab guide, you will find instructions such as:

Navigate to Context: **Groups / default**

You should now click the **Context** button, under the Groups heading, then click **default**.



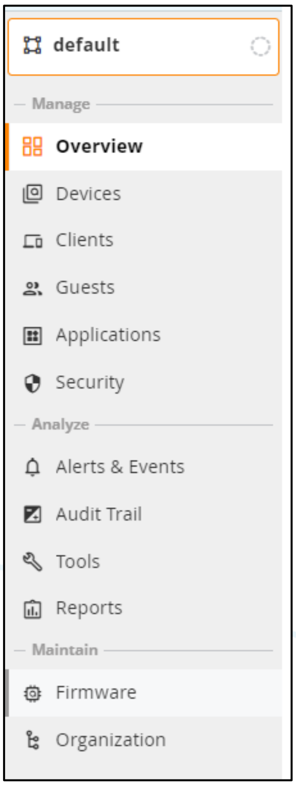
The context filter will now show the *group* icon  and the name of the group: *default*.



Navigation Menu

On the left side of the UI, you see the navigation menu. This menu provides access to various status and configuration screens for a given context.

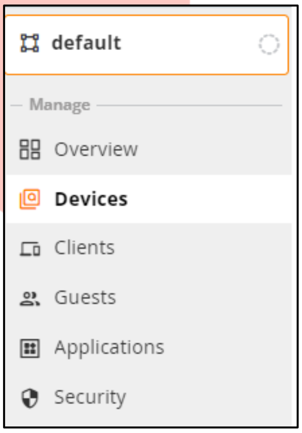
This is an example of the navigation menu with the *Manage*, *Analyze*, and *Maintain* sections:



You may see an instruction such as:

Navigate to: Context: **Groups / default** > Navigation: **Devices**.

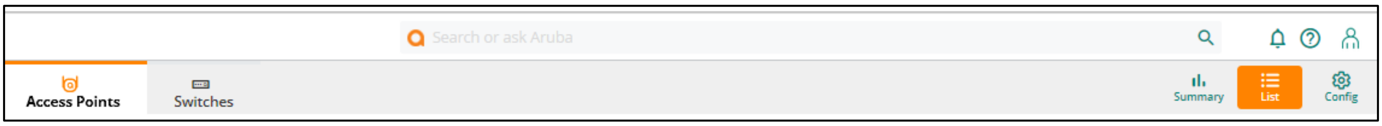
You should first verify that you are at the correct context filter level (or change the context filter), then use the Navigation menu on the left side and click **Devices.** Here is an example:



Top Menu

Each of the navigation menu's Aruba Central screens have one or more tabs at the top of the screen.

In this example (Context: **Group / default** > Navigation: **Devices**), the top options are *Access Points* and *Switches*.



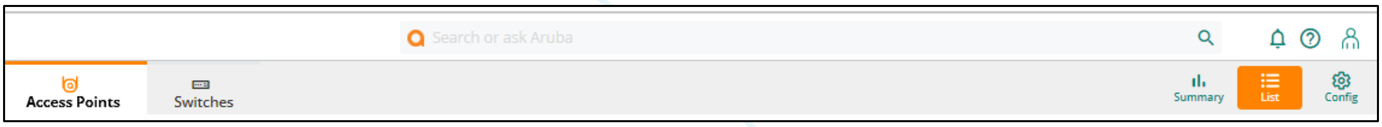
The example instruction to reach this page would be:

Context: **Groups / default** > Navigation: **Devices** > Top: **Access Points**.

Top Right

Many of the Aruba Central pages will have similar options at the top right of the screen.

In this example (Context: **Group / default** > Navigation: **Devices** > Top: **Access Points**), the top right options (icons) are *Summary*, *List* and *Config*.



To access this example page, the instruction would be:

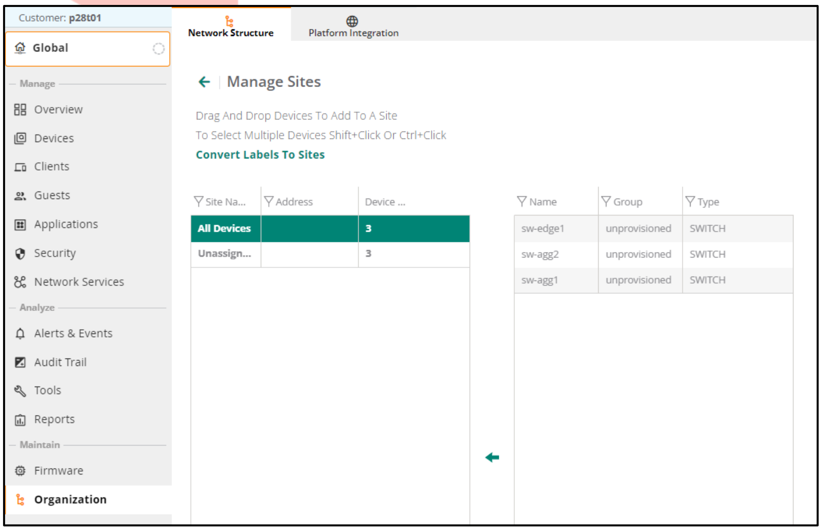
Context: **Group / default** > Navigation: **Devices** > Top: **Access Points** > Top right: **List**

This concludes the introduction to the Aruba Central navigation.

Sites

Aruba Central uses sites to map devices to their physical locations. In Aruba Central, all devices in the same location should be mapped to the same site. A device can only belong to one site.

In Aruba Central, navigate to: Context: **Global** > Navigation: **Organization** > Top: **Network Structure > Sites**. Here is an example screenshot:



At the bottom of the page, click the plus (**+**) sign to create a **New Site**.

NOTE: This guide uses a fictitious example site address. Feel free to enter your own site address information, but please use the site name **site-campus-main**.

Field	Value
Name	**site-campus-main**
Street address	**Main Street**
City	**Oranjestad**
Country	**Aruba**
State	**Aruba**
ZIP	**0000**

Click **Add** to save the site.

Assign the Switches to the Site

Now that the switches are connected to Central, you can assign them to a site. A device can only belong to a single site.

In Aruba Central, navigate to Context: **Global** > Navigation: **Organization** Top: **Network** Structure > Sites.

In the left pane, select **Unassigned**. The four switches should be listed in the pane on the right side.

Select all four switches (you can use the control or command key to select multiple entries), then drag them to the site named **site-campus-main**.

Confirm the action with **Yes**.

Task 3: Managing Edge Switches using a Template Group

In this task you will configure the edge switches using an Aruba Central Template group.

First you will configure a new group. A new template group does have a configuration template by default; therefore, it will not push a configuration to the device in the group.

You will then move the sw-edge2 device to this group. This will allow you to import the existing configuration of sw-edge2 as a template configuration for the group.

Next you will update this template to include some conditional logic and you will learn to use device variables in the template.

In the last section, you will test the configuration template by deploying sw-edge1 using this template group and variables.

Objectives

- Import a template in Aruba Central.
- Understand the conditional logic in a template.
- Understand the use of variables in the template.
- Deploy a device using ZTP and a template group.

Steps

Configure the Template Group and Move sw-edge2

In the next steps, you will create a template group in Aruba Central and move sw-edge2 to it.
Sw-edge1 will not be moved yet: it will be moved later on in this lab.

In Aruba Central, navigate to: Context: **Global**, Navigation: **Organization** Top: **Network Structure > Groups**.

At the right-top, click the **plus** sign to add a New Group.

For the name, enter '**campus-sw-edge-tpl**'.

For the value "Group will contain", only select **switches**.

Configure using **templates**: move the slider to the right (**enabled**). The checkbox for switches is automatically selected.

Click **Next**.

Types of switches used: Select **AOS-CX only**.

> **NOTE:** You don't need to select 'Make these the preferred settings'. This would make the current selection the default selection for future group additions.

Click **Add**.

Verify that the group *campus-sw-edge-tpl* is now listed.

Move sw-edge2 to the New Group

In the next steps you will start by moving *only* sw-edge2 to the target group.

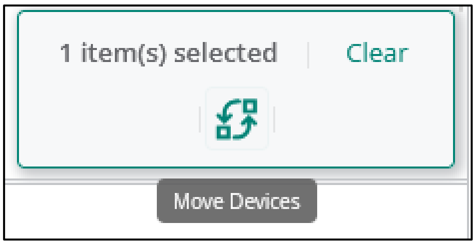
In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Groups.**

Expand *All connected devices* by clicking the the **>** icon.

Under *All connected devices*, select sw-edge2.

NOTE: Pay attention. This screen is multi-select enabled by default; clicking on multiple devices will select *all* of them. To un-select, click on the device again.

On the right-hand side, a popup will be displayed with the Move Devices action button.



Click the **Move Devices** button.

Click the **Destination Group** field.

You can either select the group **campus-sw-edge-tpl** *or* start typing a substring of the group name, such as **edge**, then select the group from the filtered list. This can be convenient when a lot of groups exist in Central.

Click the **Move** button to continue. With this action, Aruba Central will be in control of the sw-edge1 configuration (once you have configured a template in the group).

Import Template from Existing Switch

You will now import the existing configuration of the sw-edge2 as a template to this group.

Navigate to Context: **Groups / campus-sw-edge-tpl** > Navigation: **Devices**> Top: **Switches** > **Config** (gear icon).

The Top navigation shows *Templates*, *Variables*, and *Configuration Audit*.

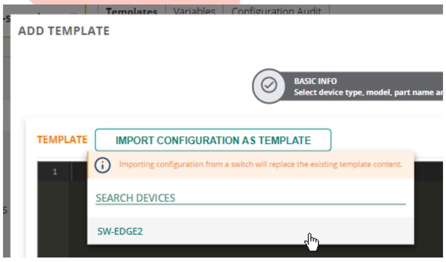
Under **Templates**, at the right-top, click the **+** icon to add a template. The Add Template window appears.

For template name, enter **sw-edge**.

For device type, verify that **Aruba CX** is selected. (This is the default based on the group settings).

You can leave the other fields at default and click **Next**.

Click Import Configuration as Template, then select sw-edge2.



Review the imported configuration. You should see around line 6 that the **hostname** command has been changed to use a variable. Each switch in the group can be configured with its own set of variables, resulting in a unique device configuration.

```
hostname %_sys_hostname%
```

Click **Save**.

Verify Template Application

In this section, you will discover how to make a local config change (for troubleshooting or testing) and how to force a template push from the device.

Use the MGMT PC to open an SSH connection to sw-edge2.

Create a new VLAN.

```
vlan 1000
exit
```

```
sw-edge2(config)# vlan 1000
sw-edge2(config-vlan-1000)# exit
```

Enable terminal monitor or logging console

```
terminal-monitor
```

```
sw-edge2(config)# terminal-monitor
Terminal-monitor is enabled successfully
```

NOTE: Terminal monitor is only supported in an SSH connection to the switch. Use `logging console` if you are connected to the console.

Disable and enable Aruba Central to force the check in and trigger the template push.

```
aruba-central
 disable
```

```
enable
exit
```

```
sw-edge2(config)# aruba-central
sw-edge2(config-aruba-central)# disable
sw-edge2(config-aruba-central)# enable
sw-edge2(config-aruba-central)# exit
```

Change template to trigger push from Central.

About 1 minute after the connection to Central is established, the template will be applied again. You should notice some events about the VLAN 1000 removal.

```
2022-12-19T15:25:44.034947+0000 ops-switchd[684] <INFO> Event|2103|LOG_INFO|CDTR|1|VLAN
1000 removed from hardware
2022-12-19T15:25:44.582928+0000 hpe-restd[988] <INFO> Event|4613|LOG_INFO|AMM|-|admin has
written a new switch configuration to running-config
2022-12-19T15:25:45.085703+0000 hpe-restd[988] <INFO> Event|6801|LOG_INFO|AMM|-|Copying
configs from: running-config to: startup-config
2022-12-19T15:25:46.932903+0000 hpe-restd[988] <INFO> Event|4614|LOG_INFO|AMM|-|admin has
copied switch configuration running-config to startup-config
```

Confirm the VLAN has been removed from the VLAN list

```
show vlan
```

```
sw-edge2(config)# show vlan

-----------------------------------------------------------------------------------------
------------------------
VLAN  Name                Status  Reason     Type        Interfaces
-----------------------------------------------------------------------------------------
------------------------
1     DEFAULT_VLAN_1      up      ok         default     1/1/1-1/1/3,1/1/5-1/1/26,lag256
3     VLAN3               up      ok         static      lag256
...
25    VLAN25              up      ok         static      lag256
```

Configuration Lockout Central Managed

In this section you will enable the Aruba Central lockout feature. This ensures that the configuration will be read-only on the device when the connection to Aruba Central is active.

In Aruba Central, navigate to Context: Groups / campus-sw-edge-tpl > Navigation: Devices > Top: Switches > Config (gear icon).

Under Templates, edit the **sw-edge** template using the **pencil** icon.

At the end of the template text, add a new line with this text:

```
configuration-lockout central managed
```

```
https-server vrf default
https-server vrf mgmt
configuration-lockout central managed
```

Click **Save**.

Use the MGMT PC to open an SSH connection to sw-edge2.

Check the list of available configuration commands

```
sw-edge2(config)# ?
  aruba-central  Configure Aruba-Central
  debug          Configure debug logging
  end            End current mode and change to enable mode
  exit           Exit current mode and change to previous mode
  list           Print command list
  no             Negate a command or set its defaults
sw-edge2(config)#
```

When the connection to Aruba Central is lost, local configuration changes can be made. These changes will be lost when the connection is restored.

In this lab environment, you want to be able to apply local changes while testing. Therefore, you will disable the configuration lockout in these labs.

In Aruba Central, edit the template **sw-edge** in the group **sw-edge-tpl**.

Remove the line with the configuration lockout and save the template.

On the SSH connection with sw-edge2, confirm all configuration commands are available again.

```
sw-edge2(config)# ?
  aaa                           Configure Authentication, Authorization and
                                Accounting feature
  access-list                   Access control list (ACL)
  alias                         Create a short name for the specified
                                command(s).
...
```

Update Template

In this section you will remove the static IP address of SVI3 and you will insert a conditional logic using variables in the template.

In Aruba Central, navigate to

Context: **Groups / campus-sw-edge-tpl >** Navigation: **Devices** > Top: **Switches > Config (gear icon)**.

Under Templates, edit the **sw-edge** template using the **pencil** icon.

Remove these 3 lines with the current, static management VLAN and IP:

```
interface vlan 3
```

```
    ip address 10.1.3.5/24
ip route 0.0.0.0/0 10.1.3.1
```

Replace with this snippet. Note that there is a typo in the snippet, this is on *purpose* to show the error message.

NOTE: The snippet can be copied from the file in the IACA Student Folder on MGMT PC:

iaca - lab 02.03 - task3 - snippet - mgmt-ip.txt

The logic of this snippet is:

Lines starting with "!" can be used for comments

If a variable exists with the name **mgmt_vlan**
    if a variable exists with the name **mgmt_ip**
        if a variable exists with the name **mgmt_gw**
            create the vlan with id **mgmt_vlan** (e.g. vlan 3)
            assign the vlan a name based on the variable (e.g. v3-mgmt)

            create an SVI for the VLAN id **mgmt_vlan**
                set IP address on the SVI based on variable **mgmt_ip**

            create a default route with next hop to variable **mgmt_gw**

```
! ####### start mgmt config
%if mgmt_vlan%
%if mgmt_ip%
%if mgmt_gw%
vlan %mgmt_vlan%
 name v%mgmt_vlan%-mgmt
interface vlan %mgmt_vlan%
    ip address %mgmt_ip%
ip route 0.0.0.0/0 %mgmt_gw%
%endif%
%endif%
%endif%%
! ####### end mgmt config
```

Click **Save**. An error should be displayed showing there is a syntax error and the line number.

Correct the error in the template by removing the extra % sign.

```
%endif%%
```

This must be changed to:

```
%endif%
```

On the MGMT PC, open an SSH connection to sw-edge2 to verify the current IP address.

```
show ip interface brief
```

```
sw-edge2(config)# show ip interface brief
Interface          IP Address             Interface Status
                                            link/admin
vlan1             10.1.1.53/24              up/up
```

NOTE: It may take 1-2 minutes for the template to get pushed and the switch to request a DHCP based IP address.

- **Question**: What do you notice?
- **Answer**: After the template push has completed, the switch no longer has an SVI3 IP address. This happened because you have not applied the per-device variables yet. In the lab environment, the DHCP based VLAN 1 will still have an IP address; this is how the switch can still reach Aruba Central to receive the correct the configuration.

Update Device Variables

Now you will apply the device level variables for sw-edge2. Note that your initial variable configuration in the next section will contain an error that you will troubleshoot later in the section.

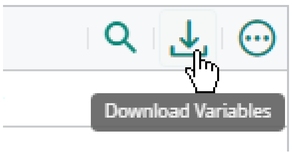
In Aruba Central, navigate to

Context: **Groups / campus-sw-edge-tpl** > Navigation: **Devices** > Top: **Switches > Config (gear icon).**

Click Variables.

For Upload/Download File Format, click **JSON**.

Download variables to your local system using the **Download** button.



Important: Make sure you *don't* use the Download Sample Variable file button!

Edit the JSON File to Add the Three Variables

Open the JSON file with a local text editor.

NOTE: Use VisualStudio Code, Notepad++ or similar tools to verify the JSON. You can also use online tools, for example www.jsoneditoronline.com, to verify the JSON syntax.

Add a comma after the “_sys_serial” line, then add these 3 variables, and make sure that the format should like this (every line ends with a comma, *except* the last one)

```
    "mgmt_vlan" : "3",
    "mgmt_ip" : "10.1.3.5",
    "mgmt_gw" : "10.1.3.1"
```

Here is an example result file

```
{
  "SG00KN5019": {
    "_sys_hostname": "sw-edge2",
    "_sys_lan_mac": "64:e8:81:3f:b5:40",
    "_sys_serial": "SG00KN5019" ,
    "mgmt_vlan" : "3",
    "mgmt_ip" : "10.1.3.5",
    "mgmt_gw" : "10.1.3.1"
  }
}
```

Save the file on your local system.

In Aruba Central, click **Upload Variables file** to upload your JSON file.

IMPORTANT: Make sure the file format option is still set to *JSON*!

NOTE: After the upload, a success message will be displayed. This success upload message only means the file was uploaded. It *does not* mean the JSON syntax was correct!

TIP: It takes a few seconds after the upload to process the new variables. You can refresh the webpage to see the updated list of variables.

Here is an example variable list:

Variables

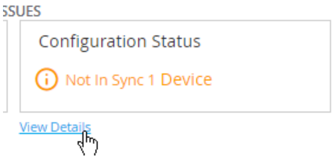
Device MAC Address	Device Serial Number	Variable Name	Variable Value
64:e8:81:3f:b5:00	SG00KN501B	_sys_hostname	sw-edge2
64:e8:81:3f:b5:00	SG00KN501B	_sys_lan_mac	64:e8:81:3f:b5:00
64:e8:81:3f:b5:00	SG00KN501B	_sys_serial	SG00KN501B
64:e8:81:3f:b5:00	SG00KN501B	mgmt_gw	10.1.3.1
64:e8:81:3f:b5:00	SG00KN501B	mgmt_ip	10.1.3.5
64:e8:81:3f:b5:00	SG00KN501B	mgmt_vlan	3

Troubleshoot CLI Syntax Errors

In the previous section, an error was introduced. In this section you will explore how you can troubleshoot issues with a template configuration.

In Aruba Central, click **Configuration Audit.**

Under the *Not in Sync* tile, click **View Details**.



- **Question**: What is the error message shown?
- **Answer**: The message states:

```
Note: Config push failed.
    ip address 10.1.3.5 #% Command incomplete.
```

- **Question**: Why does the system state command incomplete?
- **Answer**: There is only the IP address, while both IP and subnet mask are required. You should use the value **10.1.3.5/24** in the variable file instead of only **10.1.3.5**.

Explore the Device Level Configuration Audit

On the top right, click **List view**.

Click the switch **sw-edge2**.

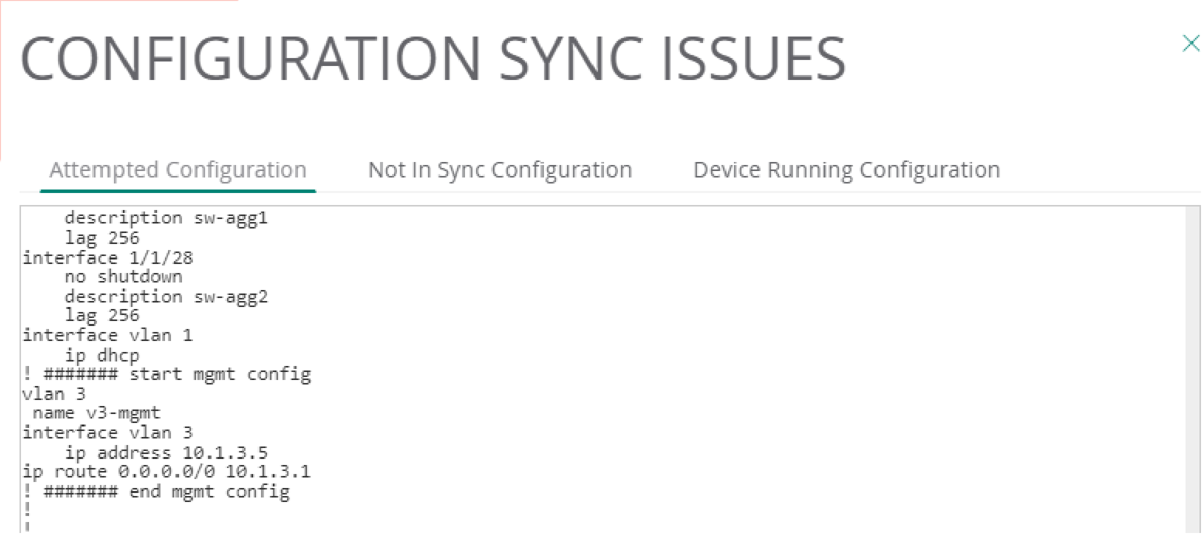
Click **Device**.

Click Configuration Audit.

Under the Configuration Status - Config Not In Sync, click **View**.

Click **Attempted Configuration**. This allows you to see the *merged* configuration of the template text with the configured variables for this device.

- **Question**: What is the attempted command under **interface vlan 3**?
- **Answer**: The attempted command is **ip address 10.1.3.5**.



This is the line that is missing the subnet mask. Now you can correct the configuration by setting the correct variable.

Adjust your local JSON variable file. Update the mgmt_ip value to **10.1.3.5/24**.

```
  "mgmt_ip" : "10.1.3.5/24"
```

Save the file.

In Aruba Central, navigate to

Context: **Groups / campus-sw-edge-tpl** > Navigation: **Devices** > Top: **Switches > Config (gear icon).**

Click Variables.

For Upload/Download File Format, click **JSON**.

Upload your local variables file again.

Refresh the page after about 10 seconds. Verify the mgmt_ip now includes the /24 mask.

Now the configuration should be pushed successfully to the switch.

On MGMT PC, open an SSH connection to sw-edge2 to verify the SVI 3 IP address has been successfully applied.

```
show ip interface brief
```

```
sw-edge2(config)# show ip interface brief
Interface          IP Address              Interface Status
                                             link/admin
vlan1             10.1.1.53/24               up/up

vlan3             10.1.3.5/24                up/up
```

Practice

Now try to practice customization a template to push a static AP port configuration.

If you are unsure, the solution is provided on the next page. However, attempt to build this template by yourself.

Add your configuration to the end of the template.
The template should have these items:

- if variable vlan_ap exists
  - Create VLAN vlan_ap
  - Give it the name v***vlan_ap***-ap-mgmt (e.g. v**4**-ap-mgmt if vlan_ap would be value 4)
- if variable port_ap exists:
  - Enter interface port_ap (e.g. interface 1/1/2,1/1/6 if port_ap would be value 1/1/2,1/1/6).
  - Enable the ports
  - Set port Description "ap"
  - if variable vlan_ap exists
    - configure port as vlan TRUNK and set vlan_ap as native vlan
    - add vlan_ap as allowed VLANs on the trunk.
  - if variable vlan_ap_trunk_list exists
    - add vlan_ap_trunk_list as allowed VLANs on the trunk

To test, add these variables to the JSON file, making sure to leave the existing mgmt variables in place. Upload the variable file.

```
    "vlan_ap" : "4",
    "port_ap" : "1/1/2,1/1/10-1/1/12",
    "vlan_ap_trunk_list" : "11-15"
```

Example file.

```
{
  "SG00KN5019": {
    "_sys_hostname": "sw-edge2",
    "_sys_lan_mac": "64:e8:81:3f:b5:40",
    "_sys_serial": "SG00KN5019",
    "mgmt_vlan" : "3",
    "mgmt_ip" : "10.1.3.5",
    "mgmt_gw" : "10.1.3.1",
    "vlan_ap" : "4",
    "port_ap" : "1/1/2,1/1/10-1/1/12",
    "vlan_ap_trunk_list" : "11-15"
  }
}
```

To verify, open an SSH connection to sw-edge2 and check the running config for 1/1/2.

```
sw-edge2(config)# show running-config interface 1/1/2
interface 1/1/2
    no shutdown
    description ap
    no routing
    vlan trunk native 4
    vlan trunk allowed 4,11-15
    exit
```

Template Solution

In Aruba Central, edit the template and add this config snippet to the end of the file.

NOTE: The snippet can be copied from the file in the IACA Student Folder on MGMT PC:

iaca - lab 02.03 - task3 - snippet ap-port.txt

```
! ####### example static AP vlan and port configuration
%if vlan_ap%
vlan %vlan_ap%
 name v%vlan_ap%-ap-mgmt
 exit
%endif%


%if port_ap%
interface %port_ap%
 no shutdown
 description ap
%if vlan_ap%
 vlan trunk allowed %vlan_ap%
 vlan trunk native %vlan_ap%
%endif%
%if vlan_ap_trunk_list%
 vlan trunk allowed %vlan_ap_trunk_list%
%endif%
!
%endif%
! ####### end of example ap and port configuration
```

Practice Deploy sw-edge1

Now you will practice by deploying sw-edge1 in the same group. The goal is to have the same configuration on sw-edge1, with minimal configuration differences, such as the hostname.

Move sw-edge1 to the New Group

Move sw-edge1 to the campus-sw-edge-tpl group.

In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Groups**

Expand *All connected devices* by clicking the **>** icon.

Under *All connected devices*, select **sw-edge1**.

On the right-hand side, a popup will be displayed with the Move Devices action button.

Click the **Move Devices** button.

Click the **Destination Group** field.

Select the group **campus-sw-edge-tpl**.

Click **Move**.

> **TIP:** You can use this screen to find the devices serial number and MAC address information.

Prepare the sw-edge1 Variable File

On your local system, copy the existing JSON file to a new file for sw-edge1.

Adjust the **new** JSON file with these settings for sw-edge1:

> **NOTE:** Pay attention, the serial number is configured **two** times in the file!

> **NOTE:** Make sure to use the xx:xx:xx:xx:xx:xx format with colons (:) for the MAC address! Please avoid any extra white (extra) spaces when you are adding the values. You can use the **show system** command from the sw-edge CLI to identify the serial and MAC values.

SERIAL	
_sys_serial	*serial number*
_sys_lan_mac	*MAC address*
_sys_hostname	**sw-edge1**
mgmt_ip	**10.1.3.4/24**

The other values can remain the same.
Here is an example file:

```
{
    "SG00KN500Z": {
       "_sys_hostname": "sw-edge1",
       "_sys_lan_mac": "64:e8:81:3f:65:40",
       "_sys_serial": "SG00KN500Z",
       "mgmt_vlan" : "3",
       "mgmt_ip" : "10.1.3.4/24",
       "mgmt_gw" : "10.1.3.1",
       "vlan_ap" : "4",
       "port_ap" : "1/1/2,1/1/10-1/1/12",
       "vlan_ap_trunk_list" : "11-15"
         }
}
```

Important: Double-check your JSON file!
- serial number (two times!)
- MAC address
- hostname (should now be **sw-edge1**!)
- IP address (should now be **10.1.3.4/24**)

Save and upload the JSON file to Aruba Central.

Use MGMT PC to open an SSH connection to sw-edge1.

Verify the running-configuration.

Use the troubleshooting options you have learned earlier if there are any errors.

Optional Step: Test Complete ZTP Deployment

On sw-edge1, perform a factory reset.

```
erase all zeroize
```

After a few minutes, sw-edge1 should have connected to Aruba Central and received the complete configuration based on the template and the device-specific variables for sw-edge1.

End of the optional step. Make sure to continue

Upload Final Template for the Edge Switches

In the next section, you will upload a prepared template to the *campus-sw-edge-tpl* group. This will ensure that any previous template or variable errors in your lab setup are corrected, if any exist.

In Aruba Central, navigate to

Context: **Groups / campus-sw-edge-tpl** > Navigation: **Devices** > Top: **Switches > Config (gear icon)**.

Under Templates, edit the **sw-edge** template using the **pencil** icon.

Remove the contents of the template.

On the MGMT PC, navigate to *the IACA Student Files* folder on the desktop.

Open the file iaca - lab 02.03 - task3 - template - sw-edge lab complete.txt and copy the contents.

Paste the text in the template in Aruba Central.

Click **Save**.

Click **Configuration Audit**. Verify the Configuration Status tile. It should eventually report *Not in Sync 0 Devices*.

Processing the new template may take 1-2 minutes. You can refresh the page to update the status.

Verify the Configuration on the Edge Switches

Use the MGMT PC to open an SSH connection to sw-edge1.

Review the interface list and the port descriptions for ports 1/1/1,1/1/2 and 1/1/4.

```
show interface brief
```

```
sw-edge1# show interface brief
------------------------------------------------------------------------------------------
--------------------
Port      Native  Mode   Type  Enabled Status  Reason                  Speed   Description
          VLAN                                                                 (Mb/s)
------------------------------------------------------------------------------------------
1/1/1     21      access 1GbT   yes     up                              1000    pc1
1/1/2     4       trunk  1GbT   yes     up                              1000    ap1
1/1/3     1       access 1GbT   no      down    Administratively down   --      --
1/1/4     24      access 1GbT   yes     up                              1000    uxi-sensor1
1/1/5     1       access 1GbT   no      down    Administratively down   --      --
```

Use the MGMT PC to open an SSH connection to sw-edge2.

Review the interface list and the port descriptions for ports 1/1/2 and 1/1/4.

```
show interface brief
```

```
sw-edge2(config)# show interface brief
------------------------------------------------------------------------------------------
--------------------
Port      Native  Mode   Type  Enabled Status  Reason                  Speed   Description
          VLAN                                                                 (Mb/s)
------------------------------------------------------------------------------------------
1/1/1     1       access 1GbT  no      down    Administratively down   --      --
1/1/2     4       trunk  1GbT  yes     up                              1000    ap2
1/1/3     1       access 1GbT  no      down    Administratively down   --      --
1/1/4     21      access 1GbT  yes     up                              1000    pc4
1/1/5     1       access 1GbT  no      down    Administratively down   --      --
```

This concludes the Edge Switch configuration.

Task 4: Migrate Aggregation Switches to Aruba Central

In this task, you will migrate the aggregation switches to Aruba Central.

You will import a prepared template and you will need to verify the aggregation switches have synchronized their configuration.

Objectives

- Import a predefined template in Aruba Central.

Steps

In Aruba Central, navigate to

Context: **Global** > Navigation: **Organization**> Top: **Network Structure** > **Groups**

At the right-top, click the **+** sign to add a New Group.

For the name, enter **campus-sw-agg-tpl**.

For the value *Group will contain*, only select **switches**.

Configure using **templates**: move the slider to the right (**enabled**). The checkbox for switches is automatically selected.

Click **Next**.

Types of switches used: Select **AOS-CX only**.

Click **Add**.

Verify that the group *campus-sw-agg-tpl* is now listed.

Upload the Aggregation Switch Template

In Aruba Central, navigate to

Context: **Groups / campus-sw-agg-tpl** > Navigation: **Devices** > Top: **Switches > Config (gear icon)**.

Under Templates, add a new template.

For the template name, enter **sw-agg**.

Click **Next**. This will take you to the template content page.

On the MGMT PC, navigate to *the IACA Student Files* folder on the desktop.

Open the file: iaca - lab 02.03 - task4 - template - sw-agg.txt

Review the Contents of the Template

The template contains conditional logic for the aggregation switches based on the hostname.

It will assign the primary and secondary VSX roles to sw-agg1 and sw-agg2.

```
vsx
```

```
    inter-switch-link lag 256
   system-mac 02:01:00:00:01:00
%if _sys_hostname=sw-agg1%
    role primary
    %endif%
%if _sys_hostname=sw-agg2%
    role secondary
    %endif%
```

It will also ensure that all SVIs are configured with a unique IP address for each aggregation switch, and with a shared active gateway IP address.

```
interface vlan 3
    description v03-mgmt
%if _sys_hostname=sw-agg1%
    ip address 10.1.3.2/24
    %endif%
%if _sys_hostname=sw-agg2%
    ip address 10.1.3.3/24
    %endif%
    active-gateway ip mac 12:01:00:00:01:00
    active-gateway ip 10.1.3.1
    ip helper-address 10.254.1.21
    ip ospf 1 area 0.0.0.1
    no ip ospf passive
```

Upload the Template

Copy the contents of the file.

Paste the text in the template in Aruba Central.

Click **Save**.

Move both Aggregation Switches to the New Group

In the next steps you will move both aggregation switches to the new group.

In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Groups**.

Expand *All connected devices* by clicking on the **>** icon.

Under *All connected devices*, select **sw-agg1** and **sw-agg2**.

On the right-hand side, a popup will be displayed with the Move Devices action button.

Click the **Move Devices** button.

Click the **Destination Group** field.

Select the group **campus-sw-agg-tpl**.

Click the **Move** button to continue.

Click **Configuration Audit**. Verify the *Configuration Status* tile. It should report *Not in Sync 0 Devices*.

Processing the new template may take 1-2 minutes. You can refresh the page to update the status.

Bounce the AP power

The APs are connected to the sw-edge1 and sw-edge2 ports 1/1/2. These ports have moved from VLAN 1 to VLAN 4 during this lab.

In the remote lab, the APs are not directly connected to the edge switches, therefore they still have their original VLAN 1 IP address.

You will now power cycle the APs. During the reboot they will get a VLAN 4 IP address.

Verify VLAN 4 on sw-agg-1 and sw-agg-2.

```
show interface vlan 4
```

```
sw-agg1# show int vlan 4

Interface vlan4 is up
 Admin state is up
 Description: v04-ap-mgmt
 Hardware: Ethernet, MAC Address: 44:5b:ed:64:8e:00
 IPv4 address 10.1.4.2/24
    active-gateway L3 source mac 44:5b:ed:64:8e:00
    active-gateway ip mac 12:01:00:00:01:00
    active-gateway ip 10.1.4.1
 L3 Counters: Rx Disabled, Tx Disabled
```

Note: Verify the list of Variables for sw-agg-1 and sw-agg-2 has been properly created when the switches were moved into the group. You can check it under Context: campus-sw-agg-tpl > Navigation: Devices> Top: Config, then examine the Variables tab.

Use the lab dashboard to power cycle AP1.

Next power cycle AP2.

You have completed this Lab!

Lab 03.01 – Deploying APs

Overview

In this lab you will assign the APs to a group in Aruba Central and apply the initial AP configuration.

Objectives

After completing this lab, you will be able to:

- Create an AP group in Aruba Central
- Assign APs to a group.
- Apply the initial configuration to the AP group.

Task 1: Deploying APs

In this task you will create a new group in Aruba Central to support the AOS 10 APs.

The existing APs will be moved to this group, and you will apply the initial group configuration, such as configuring the group password.

In the last steps you will assign the APs to the correct site in Aruba Central.

Objectives

- Create an AOS 10 UI group in Aruba Central.
- Apply the initial configuration to the AP group.
- Assign APs to a site in Aruba Central.

Steps

1. In Aruba Central, verify that two APs are online under context **Global > Devices > Access Points**.

> **NOTE:** If you have just completed lab 02.03, the APs may still be booting. Please wait a few minutes for the APs to connect to Aruba Central.

- **Question**: What is the IP address for the APs?
- **Answer**: The IP address should be in the VLAN4 subnet (10.1.4.0/24). VLAN 4 was assigned as the trunk native VLAN on the AP port 1/1/2 on the edge switches.

Create the UI Group for APs

In the next steps, you will create a User Interface (UI) group in Aruba Central.

2. In Aruba Central, navigate to

Context: **Global** > Navigation: **Organization**> Top: **Network Structure > Groups**

3. At the right-top, click the **+** sign to add a new group.
4. For the name, enter **campus-wifi-ui**.
5. For the value *Group will contain*, only select **Access Points**.
6. Do ***not*** configure using templates.
7. Click **Next**.
8. For *Architecture*, select **ArubaOS 10**.
9. For *Network Role*, select **Campus/Branch**.
10. Click **Add**.
11. Verify that the group **campus-wifi-ui** is now listed.

Move the APs to the Group

In the next steps you will move the APs to the new group.

12. In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Groups**.
13. Expand *All connected devices* by clicking on the **>** icon.
14. Under *All connected devices*, select both APs.
15. On the right-hand side, a popup will be displayed with the Move Devices action button.
16. Click the **Move Devices** button.
17. Click the **Destination Group** field.
18. Select the group **campus-wifi-ui.**
19. Click the **Move** button to continue.

Initial AP Group Configuration

In the next steps, you will apply the initial group password and country code information. The initial group password will be used to set the built-in admin account password of the APs of this group.

20. Navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points > Config** (gear icon).

For a new AP UI group, Aruba Central requires the group password to be configured. A window will appear to set the password.

21. Set the initial group password to **Aruba123!**
22. Click **Show Advanced** to enable the advanced view.
23. Under *System* > set *Country Code* to **US** and click **Save Settings**.

> **NOTE:** The remote lab is based in the US. Make sure to use the correct country code for this lab!

24. Under *Access Points*, use **pencil** to edit the APs and set the name for the APs to **ap1** and **ap2**.

> **NOTE:** The AP on sw-edge1 should be named *ap1*, the AP on sw-edge2 should be named *ap2*. Check the switches MAC address table on port 1/1/2 to find the MAC addresses.

Access Points (2)

Name	Status	IP Address	WLANs	Radio Profile	Type
ap2	• Online	10.1.4.51	All SSIDs selected	default	AP-303H
ap1	• Online	10.1.4.50	All SSIDs selected	default	AP-303H

Assign the Access Points to the Site campus-site-main

25. In Aruba Central, navigate to

Context: **Global** > Navigation: **Organization**> Top: **Network Structure** > **Sites**

26. In the left pane, select **Unassigned**. The two APs should be listed in the pane on the right side.
27. Select *both* access points. (You can use the control or command key to select multiple entries), then drag them to the site named **site-campus-main**.
28. Confirm the action with **Yes**.

You have completed this Lab!

Lab 03.02 Deploying Gateways

Overview

In this lab you will perform the initial configuration of the gateways.

The gateways will be configured using the console connection to complete the setup dialog wizard.

This will apply the initial IP address and VLAN to the gateways and provide the gateways with internet access to Aruba Activate and Aruba Central.

In Aruba Central you will configure a group for the gateway configuration and complete the initial guided setup of a gateway group.

Once the gateway has been moved to the correct Central configuration group, you will complete the device level guided setup wizard.

In the last section of this lab, you will review how configuration changes are pushed to the gateways. You will also explore the differences between the group level and the device level configuration.

Objectives

After completing this lab, you will be able to:

- Complete the initial setup of a gateway.
- Verify the gateway access to Aruba Central.
- Complete the gateway group configuration.
- Complete the gateway device level configuration.
- Verify the gateway configuration deployment.

Task 1: Configure Gateway1 using the Setup Dialog

In this task you will complete the first gateway (gw1) initial configuration using the console setup dialog. In this lab environment, the gateways are factory default.

The gw1 port GE0/0/1 is connected to sw-agg1 port 1/1/5, therefore you will use the port GE0/0/1 during the setup wizard.

Using the setup dialog, you will configure port GE0/0/1 as a VLAN trunk with native VLAN 1 and configure the gateway with VLAN 3 as the management VLAN with a static IP address.

With this setup, the gateway will have internet access and it will contact Aruba Activate. Aruba Activate will then provide the gateway with the correct Aruba Central device URL.

Objectives

- Complete the gateway initial setup dialog.
- Verify the gateway connection to Aruba Central.
- Review the setup dialog configuration on the gateway.

Steps

1. Open gw1 console, press **<Enter>**. The initial deployment options will be shown.

```
Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...
    'enable-debug'      : Enable auto-provisioning debug logs
    'disable-debug'     : Disable auto-provisioning debug logs
    'full-setup'        : Start full setup dialog. Provides full customization
    'static-activate'   : Provides customization for static or PPPOE ip assignment. Uses
activate for master information

Enter Option (partial string is acceptable):
```

2. Enter static activate.

```
static-activate
```

```
Enter Option (partial string is acceptable): static-activate
```

3. In the wizard, use these values:

- Controller VLAN ID **3**
- Uplink port **GE 0/0/1** (*important*: do ***not*** use the default GE 0/0/0!)
- Port mode **trunk**
- Native VLAN id **1**
- IP assignment method **static**
- Static IP address **10.1.3.21**
- IP netmask **255.255.255.0**
- Default Gateway **10.1.3.1**
- DNS **10.254.1.21**
- IPv6 **no**
- Disable spanning tree **yes**

- Configure Port Channel **no** (**Important**: the port channel will be configured later in the lab!)

```
Enter Controller VLAN ID [1]: 3
Enter Uplink port [GE 0/0/0]: ge 0/0/1
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]:
Enter Uplink Vlan IP assignment method (static|pppoe) [static]:
Enter Uplink Vlan Static IP address [192.168.1.1]: 10.1.3.21
Enter Uplink Vlan Static IP netmask [255.255.255.0]:
Enter IP default gateway [none]: 10.1.3.1
Enter DNS IP address [none]: 10.254.1.21
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to disable spanning tree (yes|no)? [no]: yes
Do you want to configure dynamic port-channel (yes|no) [no]:
```

4. Confirm the options with **yes**.

```
Current choices are:

Controller VLAN id: 3
Uplink port: ge 0/0/1
Uplink port mode: trunk
Native VLAN id: 1
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 10.1.3.21
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 10.1.3.1
Domain Name Server to resolve FQDN: 10.254.1.21
Option to configure VLAN interface IPV6 address: no
Spanning-tree is disabled: yes

Do you wish to accept the changes (yes|no) yes
```

5. The gw1 will contact Aruba Activate to obtain the Aruba Central URL. With that information, it will make a connection to Aruba Central.

```
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2764  100   134  100  2630    199   3919 --:--:-- --:--:-- --:--:--  4113
Received Activate response, Central = device-uswest4.central.arubanetworks.com
Master =  auto-discovered from Activate

INFO: Backing up existing configuration directory.

Country code is restricted to US
Uplink Port : gigabitethernet 0/0/3
Sent ztp message successfully for addr type :1
Sent ztp message successfully for addr type :2
Processes will restart now
Restarting ntpwrap...
Restarting cert_dwnld...
Processes restarted successfully!


[09:56:52]:Initializing GSM                                      [ DONE ]
```

```
[09:56:52]:Initializing CCM                                    [ DONE ]
[09:56:52]:Initializing FPAPPs                                 [ DONE ]
[09:56:52]:Initializing CFGM                                   [ DONE ]
[09:57:09]:Waiting for Controller IP                           [ DONE ]
[09:57:13]:Initializing AAA                                    [ DONE ]
[09:57:13]:Initializing Controller management                  [ DONE ]
In process of syncing configuration with Central. User login configured from Central will
be enabled after the sync. It may take some time.

User:
```

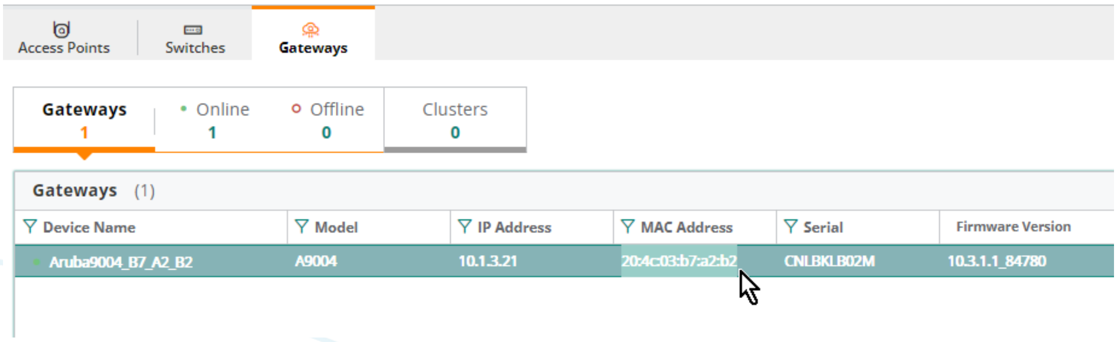
- **Question**: What is the Aruba Central URL received by the gateway?
- **Answer**: In this lab environment, the URL is device-uswest4.central.arubanetworks.com.

Verify the Gateway Setup Dialog Configuration

6. In Aruba Central, navigate to

Context: **Global** > Navigation: D**evices**> Top: **Gateways**

7. Verify that the gateway is online with the correct IP address (10.1.3.21).
8. Copy the MAC address of the gw1 as shown in Aruba Central.



9. Use the lab dashboard to open a console connection to the gateway **gw1**.
10. Login with username **branchsupport**; the password is the gateway MAC address, lowercase with a colon delimiter. For example 20:4c:03:b7:a2:2a

> **NOTE:** Login for this account will be automatically disabled when an admin account is pushed to the gateway by Aruba Central.

11. Review configuration made by setup-dialog wizard

```
show configuration setup-dialog
```

```
(Aruba9004_B7_A2_B2) *# show configuration setup-dialog
country US
hostname Aruba9004_B7_A2_B2
vlan 3
interface gigabitethernet 0/0/0
!
```

```
interface gigabitethernet 0/0/1
  trusted
  trusted vlan 1-4094
  switchport mode trunk
  switchport trunk native vlan
!
interface gigabitethernet 0/0/2
!
interface gigabitethernet 0/0/3
!
interface vlan 3
  ip address 10.1.3.21 255.255.255.0
!
ip default-gateway 10.1.3.1
ip name-server 10.254.1.21
controller-ip vlan 3
!
masterip device-uswest4.central.arubanetworks.com web-socket-acp
firewall
  dpi
!
(Aruba9004_B7_A2_B2) *#
```

- **Question**: What is the VLAN and IP address that were created in the gateway configuration by the setup dialog?
- **Answer**: VLAN 3, the IP address is 10.1.3.21/24
- **Question**: What port is configured as VLAN trunk?
- **Answer**: GE 0/0/1
- **Question**: What is the master IP? How was this learned?
- **Answer**: Based on Aruba Activate. After enabling the subscription for the gateway, Aruba Activate will provide the correct Aruba Central URL to the device when it checks in to Activate.
- **Question**: Why is the setup-dialog config important?
- **Answer**: When a gateway is moved to another group in Aruba Central, it will clear its configuration and revert to the setup-dialog configuration. Once the connection with Aruba Central is re-established, the new group configuration will be pushed by Aruba Central.

Task 2: Configuring the Gateway in Aruba Central

In this task you will complete the initial configuration of the gateway in Aruba Central.

In the first section of this task, you will assign the gateways to the correct site in Aruba Central.

You will then configure a new group to support the gateways and move the gateway to this new group.

You will complete the initial setup by configuring a port-channel (LAG) on the gateway, this will connect to the VSX LAG on the aggregation switches.

In the last section of this task, you will practice this configuration by configuring gw2.

Objectives

- Complete the initial setup dialog of the gateway.
- Verify the Gateway connection to Aruba Central.
- Complete the Aruba Central gateway group setup guide.
- Complete the Aruba Central gateway device level setup guide.

Steps

Assign the Gateway to the Site campus-site-main

1. In Aruba Central, navigate to

Context: **Global** > Navigation: **Organization**> Top: **Network Structure** > **Sites**

2. In the left pane, select **Unassigned**. The gateway should be listed in the pane on the right side.
3. Select the gateway, then drag it to the site named **site-campus-main**.
4. Confirm the action with **Yes**.

Create the UI Group for Gateways

In the next steps, you will create a User Interface (UI) group in Aruba Central for the Gateways.

12. In Aruba Central, navigate to

Context: **Global** > Navigation: **Organization** > Top: **Network Structure > Groups**

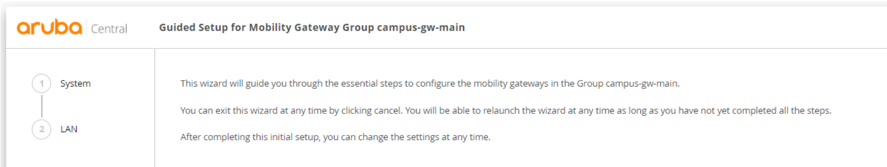
13. At the right-top, click the **+** sign to add a **New Group**.
14. For the name, enter **campus-gw-main**.
15. For the value *Group will contain*, only select **Gateways**.
16. Do ***not*** configure using templates.
17. Click **Next**.
18. For the *Architecture*, select **ArubaOS 10**.
19. For the *Network Role*, select **Mobility**.

20. Click **Add**.
21. Verify that the group *campus-gw-main* is now listed.

Initial Group Wizard

22. Navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices** > Top: **Gateways > Config** (gear icon).

For a new Gateway UI group, Aruba Central will start a Guided Setup wizard that will take you through some basic configuration options.



23. Complete the Guided Setup initial wizard with these settings:

System
- Platform
  - Platform: **A9004**
  - Auto-Cluster mode: **Group based** (default)
- Time
  - NTP IPv4: **10.254.1.21**
  - Burst Mode: **enabled**
  - Timezone: **America/Detroit** (UTC-04:00)
- DNS
  - Leave default (you have set the DNS server already in the setup wizard)
- Management User
  - Leave default

NOTE: You will set the admin account at the device level configuration. In a production deployment you may set the admin password at the group level. However, in these labs, you will move the gateways between groups, therefore it is more convenient to set these values at the device level.

24. Click **Finish**.
25. Click **Continue** to start the next page of the guided setup.

LAN
- VLAN
  - Use **+** to Add a new VLAN
  - ID: **3**
  - Name: **v3-mgmt**
- LAN Ports
  - leave default

NOTE: You will be configuring a port-channel for the gateways, but this will be done at the device level. Do not configure the port-channel in this step, this will cause issues if the gateway would be moved to a different group!

26. Click **Finish**.
27. Click **Continue** to complete the guided setup.

Move gw1 to a Group

In the next steps you will move the gw1 to the new group.

28. In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Groups**
29. Expand All connected devices by clicking the **>** icon.
30. Under *All connected devices*, select the gateway.
31. On the right-hand side, a popup will be displayed with the **Move Devices** action button.
32. Click the **Move Devices** button.
33. Click the **Destination Group** field.
34. Select the group **campus-gw-main.**
35. Click the **Move** button to continue.

Central Device Level Gateway Configuration

Aruba Central provides a group level configuration and device level configuration. The device level configuration overrides the settings applied at the group level.

For Gateways, the device level configuration is kept when the gateway is moved to a new group.

In these training labs, you will be moving the gateways to different groups to test different deployment options. This is why some configuration options, such as the port-channel, are configured at the device level rather than the group level.

In the next section you will configure the device level for gw1.

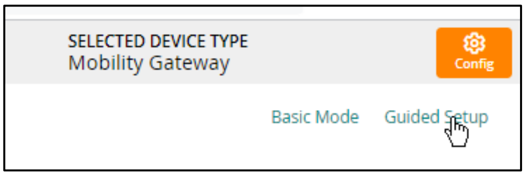
36. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways**
37. At the top right, click **List**.
38. Click the **gateway** in the list to move to the device context.

NOTE: The gateway may show as offline. After moving the gateway to the group, the gateway will be rebooted to apply the new configuration. If your gateway is still online, the reboot may still be pending. You do not need to wait for the reboot to continue the lab.

39. Click **Device.** This will open the device level configuration.
40. The device-level initial wizard will be launched.

Device level wizard
System
System IP — Select **vlan 3** from the dropdown list. (should be default).
hostname — **gw1**

NOTE: If the System IP dropdown list does not contain VLAN 3, Central is still importing the device level configuration. You may exit the guided setup. In the device configuration screen, you can then re-launch the guided setup.



41. Click **Finish** and **Continue**.
42. Complete the LAN settings of the guided setup:

LAN
VLANs
no change (v3 present and configured)
LAN Ports
no change

43. Click **Finish** and **Continue** to complete the guided setup.

Post Wizard Device Level Configuration

In this section you will complete the *device-level* configuration, make sure you are still connected to the device context, and *not* the group context in Aruba Central.

The Aruba context will show either the setup hostname or the updated gw1 hostname, either is fine.

Define Local admin Account

The local admin account can be inherited from the group. In the lab environment you did not configure it at the group level.

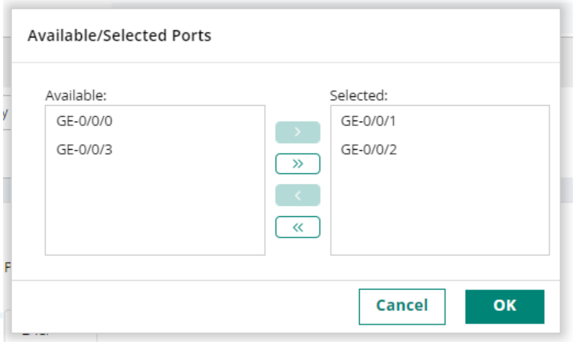
You will be moving the device several times between groups; therefore, it is easier to save the admin account at the device level, since you don't have to create a new admin on the target group.

44. Navigate to **Device** to access the device configuration.(you should still be at this page).
45. Enable **Advanced Mode** view.
46. Navigate to **System > General > Basic**.
47. Set the password for admin to **Aruba123!**
48. Click **Save Settings**.

Port-Channel Configuration

49. Navigate to **Interfaces > Ports**. You will see a Ports list and Port Channel list.
50. In the Port Channel list (at the bottom), click the **+** sign to add a new Port Channel.
51. In the ID list, select **PC-0**.
52. Click Save Settings.
53. At the bottom of the screen, you will see the Port Channel configuration options.

- Protocol **LACP**
- LACP Mode **active**
- Port Members **GE 0/0/1** and **GE 0/0/2** (double check the ports! Do not select GE 0/0/0!)



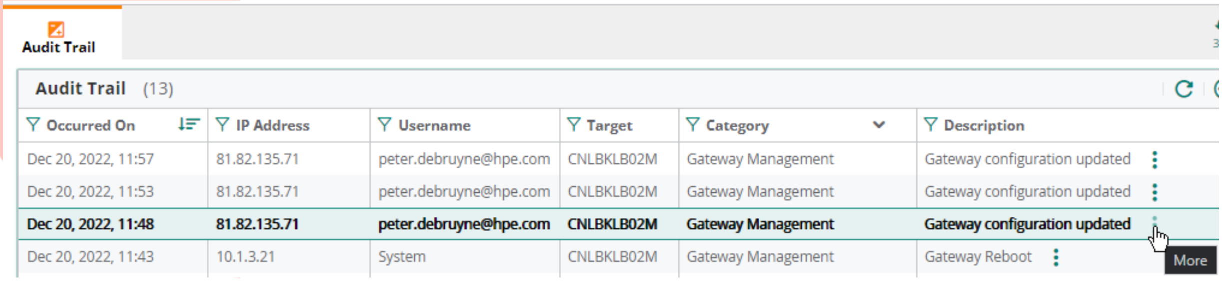
- Admin State **Checked** (enabled)
- Trust **Checked** (enabled)
- Mode **Trunk**
- Native **1**
- Allowed VLANs **1,3,31-35,41-45**

54. Click **Save Settings**.

Review the Generated Configuration in the Audit Trail

The configuration you have just completed at the device level will be logged in the audit trail. In the next steps you will review this audit trail. It provides an easy way to learn the CLI commands that are generated based on your UI configuration steps.

55. In Aruba Central, click **Audit Trail**. If you followed the lab steps, the last 3 records include the configuration that was generated by the guided setup and your device level configuration of the admin password and port-channel.



56. Review the last 3 records details to see the CLI configuration.

Hostname changed

```
Transaction ID: cfbe0608-8053-11ed-8cd7-721b03eb85cf

Config Id updated to: 142.

hostname gw1
```

Management user admin password example

```
mgmt-user admin root 32506a5f011161b63222d2b4615b8ee1f66046eb7eb851d1c9
```

Port-Channel0 Configuration

```
interface port-channel 0
 no shutdown
 switchport mode trunk
 switchport trunk allowed vlan 1,3,31-35,41-45
 switchport trunk native vlan 1
 trusted
 trusted vlan 1,3,31-35,41-45

interface gigabitethernet 0/0/1
 lacp group 0 mode active

interface gigabitethernet 0/0/2
 lacp group 0 mode active
```

Verify the Applied Configuration on the GW

57. Use the MGMT PC to open an SSH connection to gw1 (10.1.3.21). Login with **admin** / **Aruba123!**.

```
login as: admin
admin@10.1.3.21's password:
(gw1) *#
```

58. Check the port status.

```
show port status
```

```
(gw1) *# show port status
```

```
Port Status
-----------
Slot-Port  PortType  AdminState  OperState  PoE  Trusted  SpanningTree  PortMode  Speed
Duplex  PortError
---------  --------  ----------  ---------  ---  -------  ------------  --------  -----
------  ---------
0/0/0      GE        Enabled     Down       N/A  No       Disabled      Access    Auto
Auto      -
0/0/1      GE        Enabled     Up         N/A  N/A      N/A           PC0       1 Gbps
Full      -
0/0/2      GE        Enabled     Up         N/A  N/A      N/A           PC0       1 Gbps
Full      -
0/0/3      GE        Enabled     Down       N/A  No       Disabled      Access    Auto
Auto      -
PC0        PC        Enabled     Up         N/A  Yes      Forwarding    Trunk     N/A
N/A       -
```

- **Question**: Do you see PC0?
- **Answer**: Yes, the port channel (LAG) with ID 0 was created on the gateway.
- **Question**: What is the Trusted status for the PC0?
- **Answer**: Trusted.

59. Review the Port-Channel 0 status and LACP state.

```
show interface port-channel 0
```

```
(gw1) *# show interface port-channel 0


Port-Channel 0 is administratively up, Link is up, Line protocol is up
Hardware is Port-Channel, address is 20:4C:03:B7:A2:2A (bia 20:4C:03:B7:A2:2A)
Description: Link Aggregate (LACP)
Spanning Tree is Forwarding
Switchport priority: 0
MTU: 1500 bytes
Member port(s):
    GE 0/0/1, Admin is up, Link is up, Line protocol is up
    GE 0/0/2, Admin is up, Link is up, Line protocol is up
Speed :2 Gbps
Interface index: 8193
Last clearing of "show interface" counters 0 day 22 hr 44 min 3 sec
link status last changed 0 day 0 hr 25 min 26 sec
    80508 packets input, 43754161 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input error bytes, 0 CRC, 0 frame
    0 multicast, 80508 unicast
    66834 packets output, 11556467 bytes
    0 output errors bytes, 0 deferred
    0 collisions, 0 late collisions, 0 throttles
```

```
Port-Channel 0 is TRUSTED

Statistics for member port: GE 0/0/1
    54715 packets input, 15810910 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input error bytes, 0 CRC, 0 frame
    0 multicast, 54715 unicast
    65326 packets output, 11296808 bytes
    0 output errors bytes, 0 deferred
    0 collisions, 0 late collisions, 0 throttles
Statistics for member port: GE 0/0/2
    25793 packets input, 27943251 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input error bytes, 0 CRC, 0 frame
    0 multicast, 25793 unicast
    1508 packets output, 259659 bytes
    0 output errors bytes, 0 deferred
    0 collisions, 0 late collisions, 0 throttles
```

- **Question**: What is the description of the port-channel?
- **Answer**: Description: Link Aggregate (LACP)

60. Check the LACP status on the Gateway side.

```
show lacp 0 neighbor
```

```
(gw1) *# show lacp 0 neighbor

Flags: S - Device is requesting slow LACPDUs
       F - Device is requesting fast LACPDUs
       A - Device is in Active mode P - Device is in Passive mode
LACP Neighbor Table
-------------------
Port      Flags  Pri  OperKey  State  Num    Dev Id
----      -----  ---  -------  -----  ---    ------
GE 0/0/1  SA     1    0x5      0x3d   0x5    02:01:00:00:01:00
GE 0/0/2  SA     1    0x5      0x3d   0x3ed  02:01:00:00:01:00
```

Question: What is the neighbor Dev ID?

Answer: This is the Neighbor LACP system ID. In this setup, it is the VSX system MAC that is used on a VSX LAG.

Practice with Gateway2

In the next section you will deploy gateway 2.

The initial setup dialog configuration steps are included, the other steps can be used to practice the configuration.

Configure gw2 using the Setup Dialog

61. Use the lab dashboard to open the gw2 console, start the static activate option:

```
static-activate
```

```
Enter Option (partial string is acceptable): static-activate
```

62. In the wizard, use these values:

• Controller VLAN ID	**3**
• Uplink port	**GE 0/0/1** (**important:** do *not* use the default GE 0/0/0!)
• Port mode	**trunk**
• Native VLAN id	**1**
• IP assignment method	**static**
• Static IP address	**10.1.3.22**
• IP netmask	**255.255.255.0**
• Default Gateway	**10.1.3.1**
• DNS	**10.254.1.21**
• IPv6	**no**
• Disable spanning tree	**yes**
• Configure Port Channel	**no** (**important**: port-channel will be configured later!)

63. gw2 will now contact Aruba Activate to learn the Aruba Central URL. With that information, it will make a connection to Aruba Central.

Configure gw2 in Aruba Central

The next section only shows the high-level steps to complete. You can refer to the previous section for the detailed steps.

These are the steps to complete in Aruba Central:

- Move the second gw to the group campus-gw-main
- Assign the second gw to the site site-campus-main.
- At the device level gw2 config, complete the Guided Setup
    - Hostname **gw2**
    - No other changes in the wizard
- Complete the **Device** level configuration
    - Set local admin password to **Aruba123!**
    - Create **PortChannel0**
    - Configure the PortChannel0
        - Protocol: **LACP**
        - mode: **active**
        - Ports **GE 0/0/1** and **GE 0/0/2** (make sure you do not select GE 0/0/0!)
        - Admin State: **enabled**
        - Trust: **enabled**
        - VLAN trunk with native **VLAN 1**
        - Allowed VLANs **1,3,31-35,41-45**

Task 3: Monitor Gateway Configuration Changes from Central

In this task you will monitor the configuration changes that Central pushes to the gateway.

In Aruba Central you will see how the Audit Trail can be used to track the generated configuration commands.

On the gateways, you can use the configuration ID and status to verify the current state of the configuration synchronization.

You will also explore the difference between the group and the device level configuration in Aruba Central.

Objectives

- Review the gateway configuration version.
- Understand the difference between the group and device level configuration.
- Understand how the device level overrides can be seen in Aruba Central.

Steps

1. Use the MGMT PC to open an SSH connection to gw1 (10.1.3.21).
2. Review the current configuration version.

```
show switches
```

Example output:

```
(gw1) *# show switches

All Switches
------------
IP Address  IPv6 Address  Name  Location          Type  Model     Version         Status
Configuration State  Config Sync Time (sec)  Config ID
----------  ------------  ----  --------          ----  -----     -------         ------
-------------------  ----------------------  ---------
10.1.3.21   None          gw1   Building1.floor1  MD    Aruba9004  10.3.1.1_84780  up
UPDATE SUCCESSFUL    0                       149

Total Switches:1
```

- **Question**: What is the config id?
- **Answer**: In the example output, this is 149 (this will probably be different in your lab environment). For each configuration change in Aruba Central, the version number is incremented with 1.

3. Use the MGMT PC to open an SSH connection to gw2.
4. Review the current configuration version.

```
show switches
```

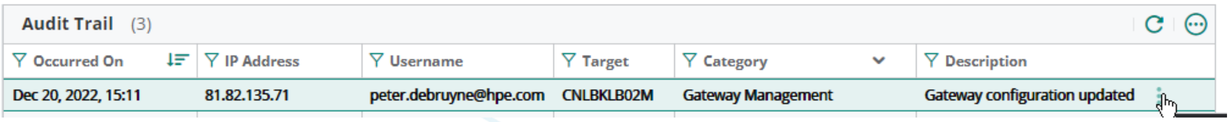
```
(gw2) # show switches

All Switches
------------
IP Address   IPv6 Address  Name  Location           Type  Model      Version         Status
Configuration State  Config Sync Time (sec)  Config ID
----------   ------------  ----  --------           ----  -----      -------         ------
-------------------  ----------------------  ---------
10.1.3.22    None          gw2   Building1.floor1   MD    Aruba9004  10.3.1.1_84780  up
UPDATE SUCCESSFUL    0                       149

Total Switches:1
```

- **Question**: What is the configuration version number?
- **Answer**: The same number as gw1.

Make a Configuration Change in Aruba Central

In the next steps you will make a configuration change in Aruba Central. This will allow you to track the configuration sync on the gateways.

5. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
6. Under Interface > VLANs, create a new VLAN
   - VLAN name **employee**
   - VLAN id/Range **31**
7. Click **Audit-trail** to see the latest audit events.
8. Use the **3 dots** to open the details of the latest event.



NOTE: Verify the timestamp of the latest event. You may need to refresh the page to see the latest audit event.

```
vlan-name employee
vlan range 31
vlan employee 31
```

9. Use MGMT PC to open an SSH connection to gw1.
10. Check the VLANs and the config id.

```
show vlan
show switches
```

```
(gw1) *# show vlan
```

```
VLAN CONFIGURATION
------------------
VLAN  Description  Ports                   AAA Profile  Option-82
----  -----------  -----                   -----------  ---------
1     Default      GE0/0/0 GE0/0/3 Pc0-7   N/A          Disabled
3     VLAN0003     Pc0                     N/A          Disabled
31    VLAN0031     Pc0                     N/A          Disabled
```

```
(gw1) *# show switches

All Switches
------------
IP Address  IPv6 Address  Name  Location          Type  Model     Version         Status
Configuration State  Config Sync Time (sec)  Config ID
----------  ------------  ----  --------          ----  -----     -------         ------
-------------------  ----------------------  ---------
10.1.3.21   None          gw1   Building1.floor1  MD    Aruba9004  10.3.1.1_84780  up
UPDATE SUCCESSFUL    0                       150

Total Switches:1
```

11. On gw2, check the VLANs and the config id.

```
show vlan
show switches
```

```
(gw2) *# show vlan

VLAN CONFIGURATION
------------------
VLAN  Description  Ports                   AAA Profile  Option-82
----  -----------  -----                   -----------  ---------
1     Default      GE0/0/0 GE0/0/3 Pc0-7   N/A          Disabled
3     VLAN0003     Pc0                     N/A          Disabled
31    VLAN0031     Pc0                     N/A          Disabled
```

```
(gw2) *# show switches

All Switches
------------
IP Address  IPv6 Address  Name  Location          Type  Model     Version         Status
Configuration State  Config Sync Time (sec)  Config ID
----------  ------------  ----  --------          ----  -----     -------         ------
-------------------  ----------------------  ---------
10.1.3.22   None          gw2   Building1.floor1  MD    Aruba9004  10.3.1.1_84780  up
UPDATE SUCCESSFUL    0                       150

Total Switches:1
```

12. On gw1, check the log for received commands. You should notice the commands that were pushed by Aruba Central to the gateway.

```
show log all 6 | include fpapps
```

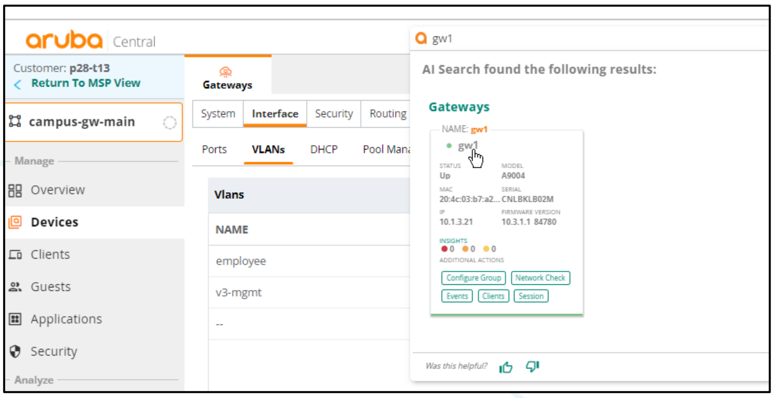
```
(gw1) *# show log all 6 | include fpapps
Dec 20 09:18:29 2022  fpapps[6133]:  executeCommandObject: Received response for
command[vlan 31 ] optype[6] AMAPI flag[0] errorno[0]
Dec 20 09:18:29 2022  fpapps[6133]:  executeCommandObject: Received response for
command[vlan employee 31 ] optype[2] AMAPI flag[0] errorno[0]
Dec 20 09:18:29 2022  fpapps[6133]:  executeCommandObject: Received response for
command[vlan-name employee ] optype[2] AMAPI flag[0] errorno[0]
Dec 20 09:18:29 2022  fpapps[6133]:  executeCommandObject: Sending command request[vlan
31 ] optype[6]
Dec 20 09:18:29 2022  fpapps[6133]:  executeCommandObject: Sending command request[vlan
employee 31 ] optype[2]
Dec 20 09:18:29 2022  fpapps[6133]:  executeCommandObject: Sending command request[vlan-
name employee ] optype[2]
```

Device Level Overrride

In this section, you will explore the difference between the group and device level configuration.

13. In Aruba Central, navigate to the **gw1** device level context.

TIP: You can enter the text gw1 in the AI Search bar to quickly access the gw1 device context.



14. Click **Device** to access the device level configuration.
15. Under **Interfaces > VLANs**, add a new Named VLAN

- VLAN Name **guest**
- VLAN ID/Range **35**

16. Click **Audit Trail** to review the generated configuration. Open the details of the latest entry.

NOTE: You may need to refresh the list to see the latest entry.

```
vlan-name guest
vlan range 35
vlan guest 35
```

17. Switch to the SSH session of gw1, review the status

```
show vlan
show switches
show log all 6 | include fpapps
```

```
(gw1) *# show vlan

VLAN CONFIGURATION
------------------
VLAN  Description  Ports                  AAA Profile  Option-82
----  -----------  -----                  -----------  ---------
1     Default      GE0/0/0 GE0/0/3 Pc0-7  N/A          Disabled
3     VLAN0003     Pc0                    N/A          Disabled
31    VLAN0031     Pc0                    N/A          Disabled
35    VLAN0035     Pc0                    N/A          Disabled
```

```
(gw1) *# show switches

All Switches
------------
IP Address  IPv6 Address  Name  Location          Type  Model      Version        Status
Configuration State  Config Sync Time (sec)  Config ID
----------  ------------  ----  --------          ----  -----      -------        ------
-------------------  ----------------------  ---------
10.1.3.21   None          gw1   Building1.floor1  MD    Aruba9004  10.3.1.1_84780 up
UPDATE SUCCESSFUL    0                       151

Total Switches:1
```

```
(gw1) *# show log all 6 | include fpapps
Dec 20 09:28:49 2022  fpapps[6133]:  executeCommandObject: Received response for
command[vlan 35 ] optype[6] AMAPI flag[0] errorno[0]
Dec 20 09:28:49 2022  fpapps[6133]:  executeCommandObject: Received response for
command[vlan guest 35 ] optype[2] AMAPI flag[0] errorno[0]
Dec 20 09:28:49 2022  fpapps[6133]:  executeCommandObject: Received response for
command[vlan-name guest ] optype[2] AMAPI flag[0] errorno[0]
Dec 20 09:28:49 2022  fpapps[6133]:  executeCommandObject: Sending command request[vlan
35 ] optype[6]
Dec 20 09:28:49 2022  fpapps[6133]:  executeCommandObject: Sending command request[vlan
guest 35 ] optype[2]
Dec 20 09:28:49 2022  fpapps[6133]:  executeCommandObject: Sending command request[vlan-
name guest ] optype[2]
```

18. On the SSH connection to gw2, review the status.

```
show vlan
show switches
show log all 6 | include fpapps
```

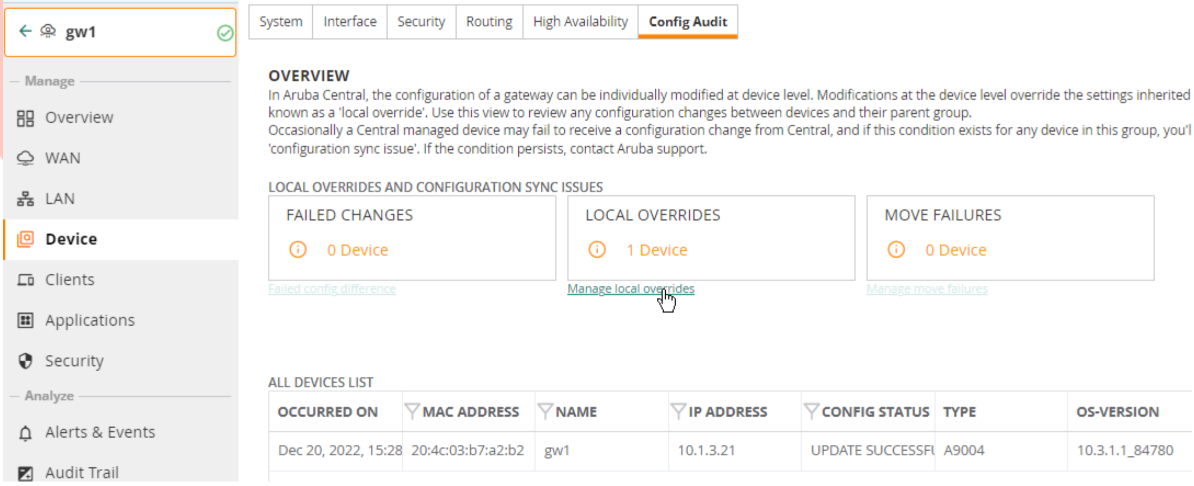
```
(gw2) # show vlan

VLAN CONFIGURATION
------------------
VLAN  Description  Ports                   AAA Profile  Option-82
----  -----------  -----                   -----------  ---------
1     Default      GE0/0/0 GE0/0/3 Pc0-7   N/A          Disabled
3     VLAN0003     Pc0                     N/A          Disabled
31    VLAN0031     Pc0                     N/A          Disabled
```

```
(gw2) # show switches

All Switches
------------
IP Address  IPv6 Address  Name  Location         Type  Model      Version         Status
Configuration State  Config Sync Time (sec)  Config ID
----------  ------------  ----  --------         ----  -----      -------         ------
-------------------  ----------------------  ---------
10.1.3.22   None          gw2   Building1.floor1  MD   Aruba9004  10.3.1.1_84780  up
UPDATE SUCCESSFUL    0                       151

Total Switches:1
```

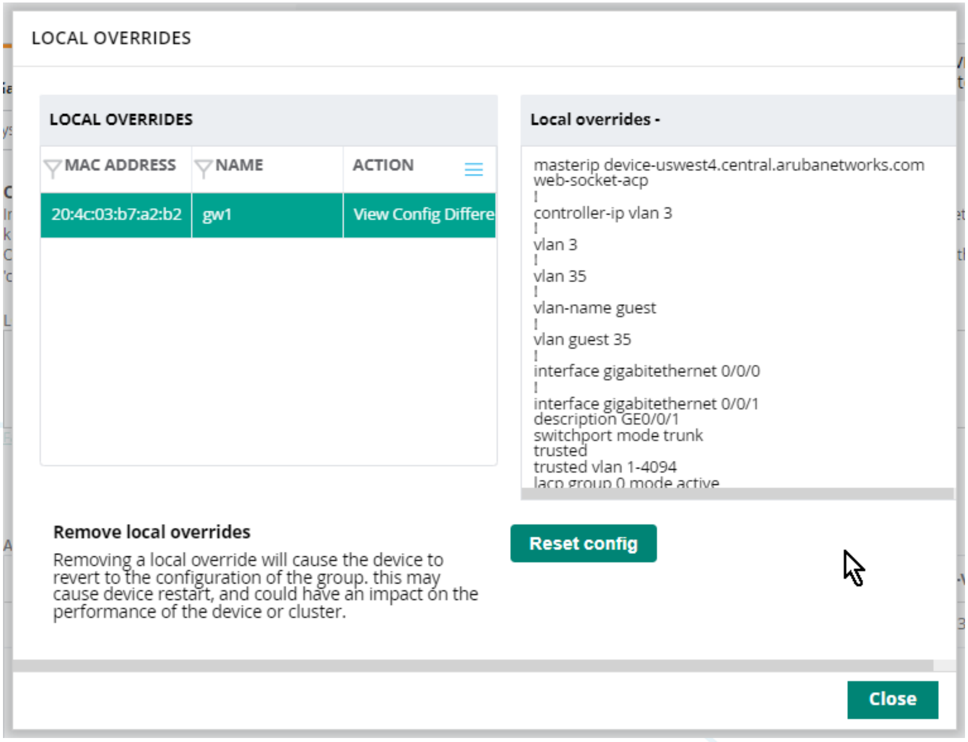
```
(gw2) #show log all 6 | include fpapps
Dec 20 09:18:33 2022  fpapps[6077]:  executeCommandObject: Received response for
command[vlan-name employee ] optype[2] AMAPI flag[0] errorno[0]
Dec 20 09:18:33 2022  fpapps[6077]:  executeCommandObject: Sending command request[vlan
31 ] optype[6]
Dec 20 09:18:33 2022  fpapps[6077]:  executeCommandObject: Sending command request[vlan
employee 31 ] optype[2]
Dec 20 09:18:33 2022  fpapps[6077]:  executeCommandObject: Sending command request[vlan-
name employee ] optype[2]
Dec 20 09:28:54 2022  fpapps[6077]:  PortFirewall: Duplicate update drop flag 0, return.
Dec 20 09:28:54 2022  fpapps[6077]:  PortFirewall: Received pubsub message type
PUBSUB_SERVICE_CFGID_CHANGE_INFO role 3, factory false, rollback false(0), ID 154.
(gw2) #
```

- **Question**: What do you observe?
- **Answer**: The named VLAN guest is only created on gw1. This is because the guest VLAN was only created at the gw1 device level.
- **Question**: What do you notice about the Config ID?
- **Answer**: The Config ID was incremented on both gw1 and gw2. Even though there were no configuration changes for gw2, the ID was incremented.

19. In Aruba Central, on the gw1 device level, navigate **to Device > Config Audit**.



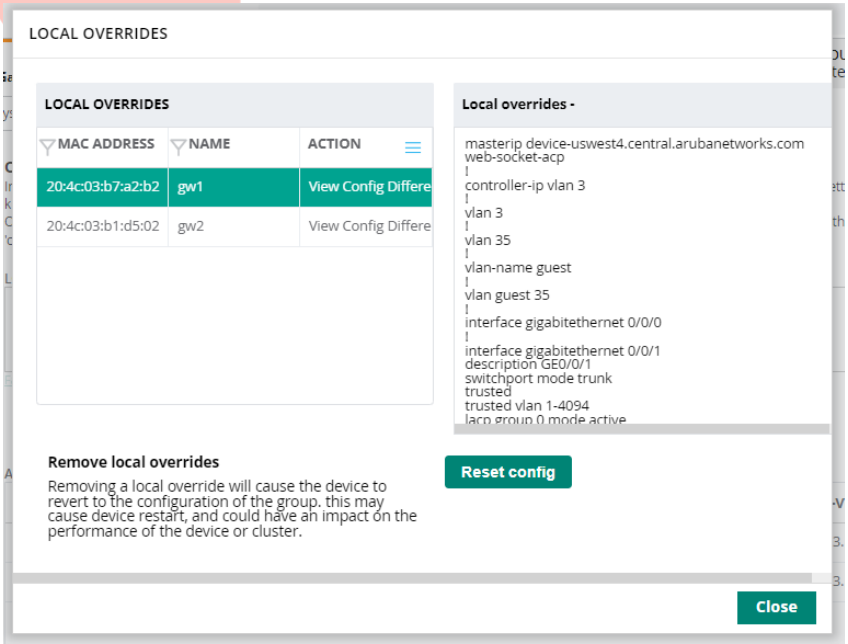
20. Click **Manage Local** overrides.

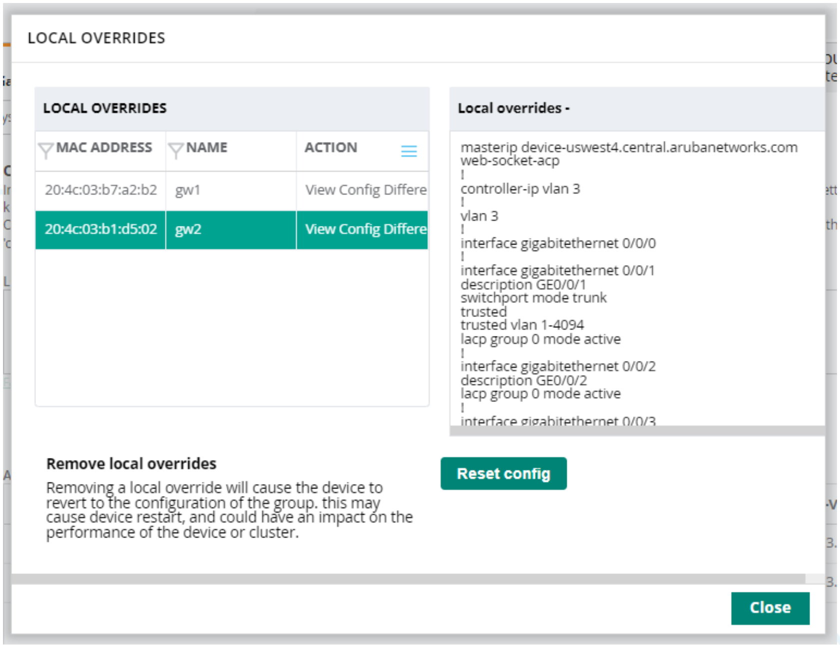


- **Question**: What are the VLANs that are defined in the local config?
- **Answer**: 3,35.
- **Question**: Why is VLAN 31 not defined in the local config?
- **Answer**: VLAN31 is defined at the group level and inherited by the device.

21. In Aruba Central, navigate to the **campus-gw-main** group context.
22. Click **Devices > Config Audit**.

23. Click **Manage Local** overrides.
24. Click **gw1** and **gw2** to compare the local configurations.





- **Question**: What VLAN differences do you see?
- **Answer**: VLAN 35 exists only on gw1.

This concludes the group and device level configuration and overrides.

Cleanup

In the next steps you will remove the named VLAN guest and the VLAN id 35 from the gw1 device level.

25. In Aruba Central, navigate to the device level **gw1** context.
26. Click **Device**.
27. Under *Interfaces* > *VLANs*, remove the named VLAN guest.

NOTE: This will only remove the named VLAN guest, not the member VLANs.

28. Click the named VLAN **“—"** and remove the VLAN id 35.

You have completed this Lab!

Lab 03.03 Automatic Gateway Clustering

Overview

In this lab you will review how gateways in the same group can automatically form a gateway cluster.

You will only explore the basic monitoring of the cluster feature; the detailed cluster operation will be covered in lab 04.02.

Objectives

After completing this lab, you will be able to:

- Monitor a gateway cluster in Aruba Central.
- Review the gateway cluster configuration.

Task 1: Review the Existing Auto Cluster

In this task you will review how the gateways in the same group can automatically form a gateway cluster. Aruba Central will automatically update the configuration of the existing gateways when a new gateway is added to the group.

Objectives

- Review the group automatic cluster configuration.
- Review the cluster configuration on the gateways.

Steps

1. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways > Config (gear icon).**
2. Click **High Availability**.
   - **Question**: What is the cluster mode?
   - **Answer**: Automatic.
   - **Question**: What auto mode is selected?
   - **Answer**: Auto Group. You have selected this "Auto Group" option during the initial setup wizard of the group.
   - **Question**: What is the name of the cluster?
   - **Answer**: The cluster name will start with **auto_gwcluster**_xyz_0. This number xyz is based on the internal group ID of the group campus-gw-main. This means that every group that is set to auto-group cluster in Aruba Central will have its own, unique cluster name.
3. Use the MGMT PC to open an SSH connection to gw1.
4. Review the lc-cluster group profiles.

```
show lc-cluster group-profile
```

```
(gw1) *# show lc-cluster group-profile

Classic Controller Cluster Profile List
---------------------------------------
Name                      Profile Status
----                      --------------
auto_gwcluster_125_0
```

5. Review the content of your cluster group profile. Make sure to adjust the command with your own group profile name. In the example command, xyz is used.

```
show lc-cluster group-profile auto_gwcluster_xyz_0
```

Example output:

```
(gw1) *# show lc-cluster group-profile auto_gwcluster_125_0

IPv4 Cluster Members
--------------------
CONTROLLER-MAC     CONTROLLER-IP  PRIORITY  VRRP-IP  RAP-PUBLIC-IP
--------------     -------------  --------  -------  -------------
20:4c:03:b7:a2:b2  10.1.3.21      128       0.0.0.0  0.0.0.0
20:4c:03:b1:d5:02  10.1.3.22      128       0.0.0.0  0.0.0.0


Starting VRRP ID:220

VRRP Passphrase:********
```

- **Question**: How does the gateway know that the 10.1.3.22 is another member in the cluster?

- **Answer**: This is automatically handled by Aruba Central. When the group is set to auto cluster, a new gateway that is added to the group will automatically result in an updated cluster group-profile configuration. This will include the IP address of the new gateway. Since the configuration is generated at the group level, all the member controllers will be aware of the updated cluster profile configuration.

6. Review the current cluster membership.

```
show lc-cluster group-membership
```

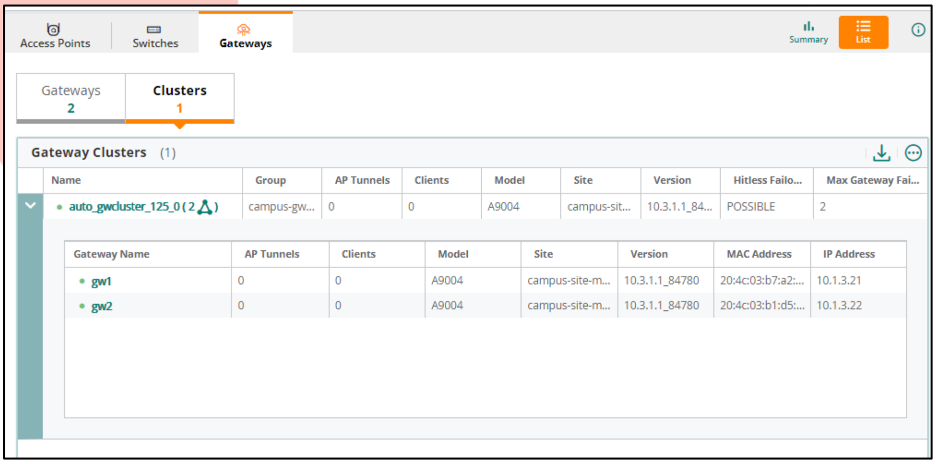
```
(gw1) *# show lc-cluster group-membership

Cluster Enabled, Profile Name = "auto_gwcluster_125_0"
Heartbeat Threshold = 900 msec (default)
Cluster Info Table
------------------
Type IPv4 Address    Priority Connection-Type STATUS
---- --------------- -------- --------------- ------
self       10.1.3.21      128             N/A CONNECTED (Leader)
peer       10.1.3.22      128    L2-Connected CONNECTED (Member)
```

- **Question**: What is the status of the other member of the cluster?

- **Answer**: gw1 and gw2 are CONNECTED, this indicates they have an active IPsec connection and can exchange user information to support stateful failover.

Review the Cluster in Aruba Central

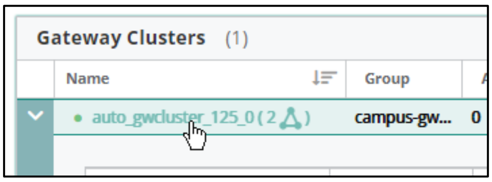
7. In Aruba Central, navigate to context **Global** > **Devices** > **Gateways**
8. Click **Clusters**. The current clusters should be listed.
9. Expand your cluster.



- **Question**: What are the Gateways that belong to this cluster?

- **Answer**: gw1 and gw2 both belong to the current group. Based on the auto-group cluster, they have automatically been assigned to the auto_gwcluster for this group. Any future gateway that would be added to this group will automatically be added to this cluster as well.

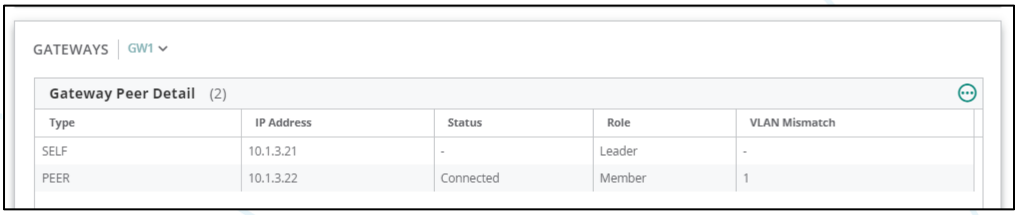
10. Click the name of your cluster.



Notice how the Aruba Central Device Context now shows the cluster as the device.

11. Navigate to **Overview > Summary**.
    - **Question**: What is the cluster client capacity?
    - **Answer**: 8192. This is the combined values of both gateways without failover consideration.

12. Navigate to **Overview > Gateways**.



- **Question**: With gw1 selected, what is the status of the peer 10.1.3.22?

- **Answer**: The status is connected. This means there is an active connection between GW1 and GW2.

You have completed this Lab!

Lab 04.01 Deploy Tunnel WLAN

Overview

In this lab you will configure a tunnel WLAN to explore the AP and gateway tunnel operation.

To keep the setup simple, a pre-shared key (PSK) WLAN will be configured.

Once the WLAN is configured, you will explore the configuration that is applied to the AP, the gateways, and the Overlay Tunnel Orchestrator (OTO).

You will also verify the status of the WLAN and the GRE tunnel on the APs and the gateways.

In the last section, you will see how to configure datapath security by enabling GRE over IPsec between the AP and the gateways.

Objectives

After completing this lab, you will be able to:

- Configure an AOS 10 tunnel WLAN.
- Understand the components in an AOS 10 tunnel WLAN.
- Verify the status of a tunnel WLAN.
- Configure a data plane security between the AP and the gateway.

Task 1: Review the Wired Network

In the next task you will deploy an open WLAN to explore the Tunnel WLAN operation.

This tunnel WLAN will be bound to VLAN 34.

A VLAN that is used in a tunnel WLAN should not be available on the AP switch port (if that would be a VLAN trunk port).

In this task you will verify that VLAN 34:

- Is allowed on the gateway VLAN trunk ports. This applies to the sw-agg1 and sw-agg2. They have a VSX LAG 5 for gw1 and a VSX LAG10 for gw2.
- Is not allowed on the AP switch VLAN trunk ports. This applies to the sw-edge1 and sw-edge2. They have the AP1 and AP2 connected on their port 1/1/2.

Objectives

Review the wired network for a tunneled VLAN.

Steps

1. Use the MGMT PC to open an SSH connection to sw-agg1.
2. Review the VLANs on port LAG 5 (to gw1) and LAG 10 (to gw2).

```
show vlan port lag5
```

```
sw-agg1(config)# show vlan port lag5

-------------------------------------------------------------------------------
VLAN  Name                                Mode            Mapping
-------------------------------------------------------------------------------
3     VLAN3                               trunk           port
31    VLAN31                              trunk           port
32    VLAN32                              trunk           port
33    VLAN33                              trunk           port
34    VLAN34                              trunk           port
35    VLAN35                              trunk           port
41    VLAN41                              trunk           port
...
45    VLAN45                              trunk           port
```

```
show vlan port lag10
```

```
sw-agg1(config)# show vlan port lag10

-------------------------------------------------------------------------------
VLAN  Name                                Mode            Mapping
-------------------------------------------------------------------------------
3     VLAN3                               trunk           port
31    VLAN31                              trunk           port
32    VLAN32                              trunk           port
33    VLAN33                              trunk           port
```

```
34     VLAN34                              trunk           port
35     VLAN35                              trunk           port
41     VLAN41                              trunk           port
...
45     VLAN45                              trunk           port
```

- **Question**: Is VLAN 34 allowed?
- **Answer**: Yes.

3. Use the MGMT PC to open an SSH connection to sw-edge1 to review the AP port VLAN membership.

```
show vlan port 1/1/2
```

```
sw-edge1(config)# show vlan port 1/1/2

-------------------------------------------------------------------------------
VLAN   Name                                Mode            Mapping
-------------------------------------------------------------------------------
4      v4-ap-mgmt                          native-untagged port
11     VLAN11                              trunk           port
12     VLAN12                              trunk           port
13     VLAN13                              trunk           port
14     VLAN14                              trunk           port
15     VLAN15                              trunk           port
```

- **Question**: Is VLAN 34 allowed?
- **Answer**: No. Tunnel VLANs should only be allowed on the gateway VLAN trunk ports. In the VLAN plan, a customer should have a dedicated set of bridged VLAN IDs and tunnel VLAN IDs. A VLAN that is used for tunnel forwarding on one WLAN should *not* be used for bridge forwarding on another WLAN. The VLAN used for tunnel forwarding should never be allowed on the AP VLAN trunk ports.

In the training lab, VLANs 11-15 are used for bridged WLAN, VLANs 31-35 are used for tunnel WLANs.

Task 2: Create PSK Tunnel WLAN with the GW cluster

In this task you will setup a tunnel WLAN and explore the operation. For this example, you will create a PSK WLAN.

During the creation of a new tunnel WLAN, you will be able to select the gateway cluster that will handle the client traffic. The WLAN wizard will automatically present the list of VLANs that exist on the selected gateway cluster.

Objectives

- Configure a tunnel WLAN.
- Understand the VLAN list in the WLAN workflow.

Steps

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points**> **Config (gear icon)**.
2. On the WLANs page, click **add SSID** to create a new WLAN.
    - Name (SSID) p#tx-psk

NOTE: Make sure to replace the # value with your pod number and **x** with your table number.

For example, if you are using table 07 in pod 28, your WLAN name would be

p28t07-psk

This represents p(od) 28 and t(able) 07.

Check with your instructor if you are not sure about the pod and table number.

---

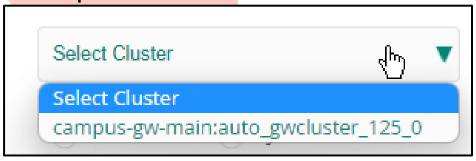
3. Click **Next**.
4. On the VLAN page, configure:
    - Traffic forwarding mode **Tunnel**
5. Review the VLAN dropdown list when **no** cluster is selected.

- **Question**: What VLANs are shown in the list?
- **Answer**: VLAN 1 is selected by default. No other VLANs are shown in the list. (no data)

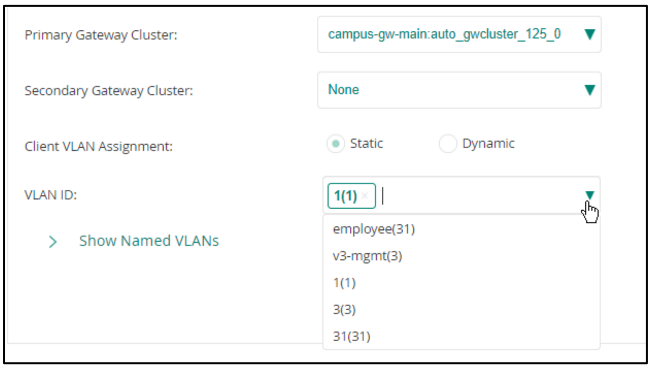
6. Click the **Primary Gateway Cluster** dropdown list. Review the list of clusters.

- **Question**: What are the names in the cluster list?
- **Answer**: The cluster name list is based on the group name and the cluster name.

Example:



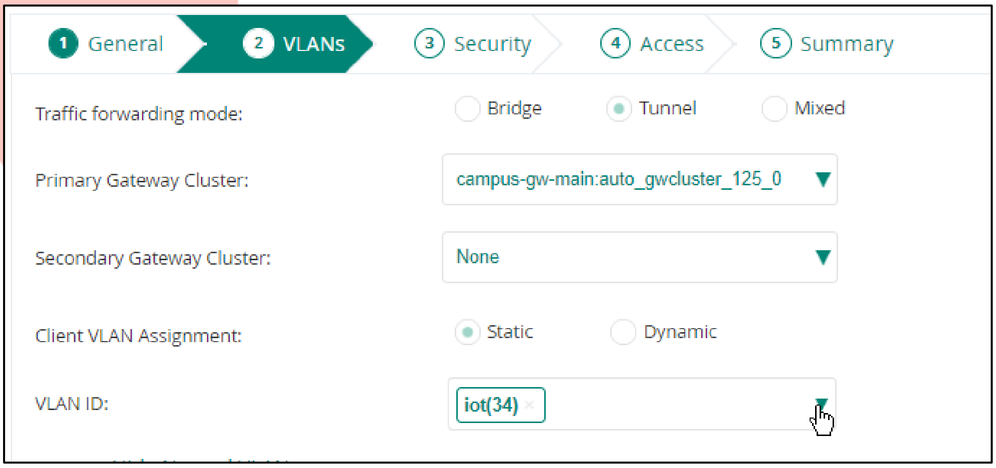
7. Select *your* cluster from the list.
8. Now review the dropdown list of VLANs again.



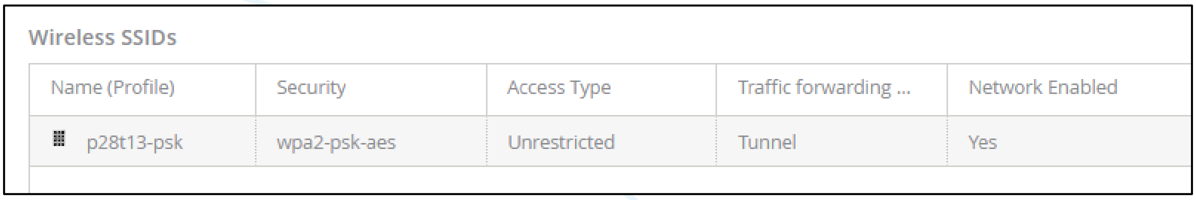
- **Question**: What happened with the VLAN list?
- **Answer**: When a cluster was selected, Aruba Central updated the list of VLANs.
- **Question**: Do you recognize any VLANs in the list?
- **Answer**: The named VLAN employee is listed. This is a VLAN that you have created on the gateway group. The list of VLANs is populated based on the selected cluster group configuration.

Create New Named VLAN

9. Click **Show Named VLANs**.
10. Click **Add Named VLAN** to create a new named VLAN.
    - VLAN Name **iot**
    - VLAN Id **34**
11. Click **OK**.
12. In the VLAN list, select the named VLAN **iot**.



13. Click **Next**.
14. On the Security page, set the option to **Personal**.
15. For Key Management, select **WPA2-Personal**.
16. Set Passphrase to **Aruba123!**.
17. Confirm the Passphrase.
18. Click **Next**.
19. Leave the Access page to **Unrestricted**.
20. Click **Next**, review the summary page.
21. Click **Finish** to complete the WLAN wizard.
22. Wait for the wizard to complete, click **OK**.
23. Verify the *p#tx-psk* WLAN is in the WLAN list.


Wireless SSIDs

Name (Profile)	Security	Access Type	Traffic forwarding ...	Network Enabled
p28t13-psk	wpa2-psk-aes	Unrestricted	Tunnel	Yes

Task 3: Review the Configuration

In this task you will review the configuration that was generated by the WLAN wizard.

The WLAN wizard has processed your changes and pushed the configuration to *three* places:

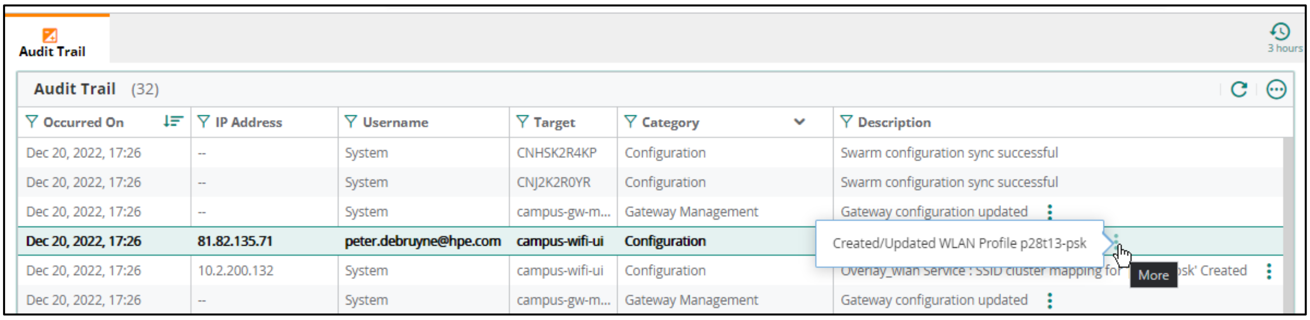
- APs
- Overlay Tunnel Orchestrator (OTO)
- Gateways

Objectives

- Understand the different configuration elements for a tunnel WLAN.
- Learn to use the Audit Trail to review the configuration changes.

Steps

1. In Aruba Central, select the **Global** context, navigate to **Audit Trail.**
2. Review the list of the latest entries.



- **Question**: What are the targets for the latest configuration change?

- **Answer**: The groups *campus-wifi-ui* and *campus-gw-main*, as well as both serial numbers of the APs.

3. Open the details (using the three dots …) of the entry of the target campus-wifi-ui with the description **Created/Updated WLAN Profile...**.

   Here is an example output. The following output is the same as the audit entry, but it has been organized by wlan access-rule and wlan ssid-profile:

```
wlan access-rule p28t13-psk
 utf8
 rule any any match any any any permit
 exit
```

```
wlan access-rule logon
 captive-portal external
 rule any any match udp 500 500 permit
 rule any any match esp any any permit
 rule any any match tcp 1723 1723 permit
 rule any any match udp 1701 1701 permit
 rule any any match any any any deny
```

```
 exit
```

```
wlan ssid-profile p28t13-psk
 essid p28t13-psk
 opmode wpa3-sae-aes
 wpa-passphrase ********
 type employee
 captive-portal disable
 dtim-period 1
 broadcast-filter none
 radius-accounting
 radius-interim-accounting-interval 1
 inactivity-timeout 1000
 max-authentication-failures 0
 blacklist
 dmo-channel-utilization-threshold 90
 max-clients-threshold 64
 enable
 dot11r
 utf8
 out-of-service vpn-down disable
 openflow-enable
 gw-profile p28t13-psk_#1669019213728_45#_
 gw-auth-server default
 forward-mode l2
 cluster-name auto_gwcluster_125_0
 cluster-group-name campus-gw-main
 mac-authentication
 exit
```

```
wlan gw-auth-server default
 key ********
 rfc3576
 exit
```

- **Question**: What is the WLAN ESSID name and opmode?
- **Answer**: Under the WLAN ssid-profile, the essid command shows *p#tx-tsk* and opmode *wpa3-sae-aes***.**
- **Question**: What is the cluster-name this WLAN ssid-profile is bound to?
- **Answer**: This is the cluster name of the auto-cluster that was formed on the gateways. In the example it shows *auto_gwcluster_125_0*.

4. Open the details for the **campus-gw-main entry**.

Here is an example output:

```
Config Id updated to: 292.

aaa authentication captive-portal p28t13-psk_#1669019213728_45#_
```

```
 default-role p28t13-psk
```

```
aaa profile p28t13-psk_#1669019213728_45#_
 no dl3-radius-proxy-mode
 no enforce-dhcp
 no radius-accounting
 no l2-auth-fail-through
 no download-role
 initial-role p28t13-psk
 default-vlan iot
 authentication-captive-portal p28t13-psk_#1669019213728_45#_
```

```
vlan-name iot
vlan 34
vlan iot 34
```

```
ip access-list session p28t13-psk
 any any any permit position 1
```

```
user-role p28t13-psk
 access-list session p28t13-psk
```

- **Question**: What VLAN is created in this command set?
- **Answer**: The named VLAN iot with VLAN 34.
- **Question**: Did you see this VLAN 34 in the AP configuration?
- **Answer: No.** Since you have created a tunnel WLAN, the VLANs you create during the WLAN wizard are created in the gateway group configuration, *not* in the AP group!

5. Open the details for the Overlay WLAN Service audit entry.

Here is an example output (output aligned to make it easier to read).

```
Overlay_wlan ssid_cluster Created

{
"aruba-overlay-wlan:config": {
"ssid_cluster": [
+ {
+  "profile": "p28t13-psk"
+  "gw_cluster_list": [
+   {
+   "cluster_redundancy_type": "PRIMARY"
+   "cluster": "auto_gwcluster_125_0"
+   "cluster_group_name": "campus-gw-main"
+   "tunnel_type": "GRE"
+   "cluster_type": "CLUSTER_ID"
+   }
+  ]
+ "profile_type": "WIRELESS_PROFILE"
+ }
```

```
]
}
}
```

- **Question**: What is the name of the WLAN profile that will be tunneled?
- **Answer**: p#tx-psk.
- **Question**: What is the primary cluster?
- **Answer**: The primary cluster points to the name of your gateway cluster. In the example the name is *auto_gwcluster_125_0*.
- **Question**: What is the tunnel type?
- **Answer**: The OTO builds GRE tunnels between the APs and the gateways by default. Later in this lab, you will configure GRE over IPsec as the tunnel type.

Review the Gateway Group Applied VLAN Configuration

In the next steps, you will review the settings that were applied by the WLAN wizard to the gateway group.

6. In Aruba Central, select the context group **campus-gw-main**.
7. Navigate to **Devices > Configuration**.
8. Open **Interface > VLANs**.
   - **Question**: Do you see the iot VLAN in the named VLAN list? What is the bound VLAN id?
   - **Answer**: Yes, the named VLAN iot was created with member VLAN id 34 on the gateway group. While you started the WLAN wizard on the AP group, the VLAN configuration was applied to the gateway group since you have selected tunnel forwarding mode.

Task 4: Verify the Operation of the Tunnel WLAN

In this task you will test the operation of the tunnel WLAN using a wireless client.

Objectives

Verify the tunnel WLAN operation.

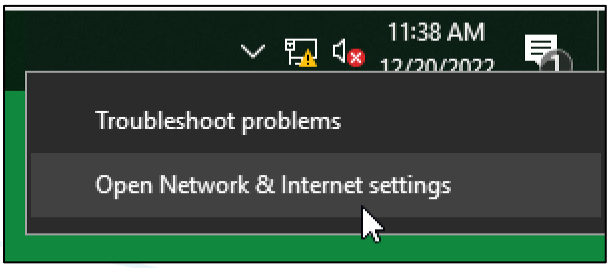
Steps

Verify the PC1 Network Interfaces

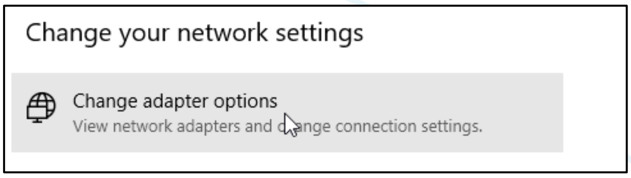
In the next steps, you will open a connection to PC1 and review the network connections.
You will:

- Verify the WLAN NIC is enabled.
- Verify the OOBM and Lab NIC are disabled.
- Do not touch the DO NOT TOUCH interface (required for the remote lab access).

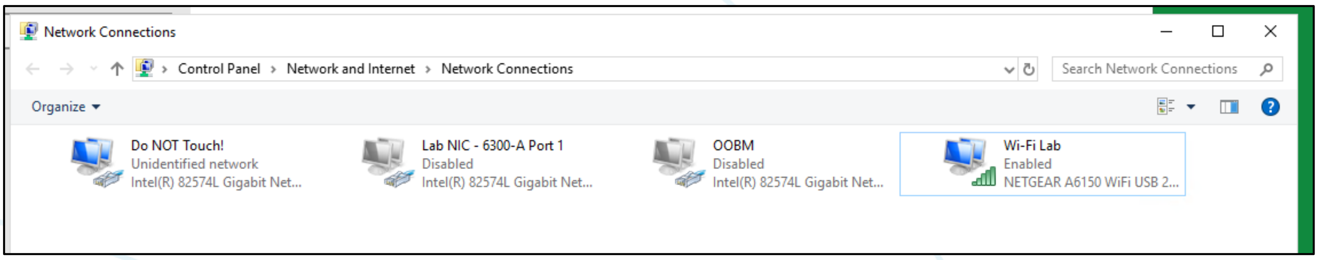
1. Use the lab dashboard to open a connection to **PC1**.
2. In the status bar, right-click the **Network** icon and click **Open Network & Internet Settings**.



3. Click **Change Adapter Options**.



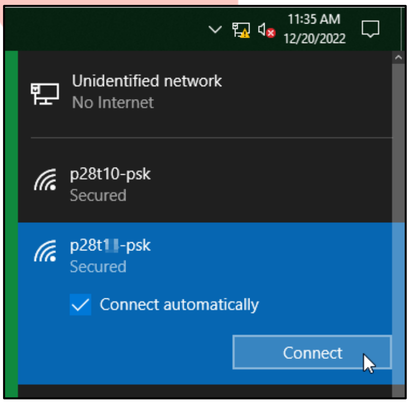
4. Verify the OOBM and Lab NIC are *disabled*. The **WLAN NIC** should be *enabled*.



IMPORTANT: Do not change the *Do NOT Touch* interface. It is used in the remote lab to make an RDP connection to the PC.

Connect with a Client to the PSK network

5. Connect to the WLAN **p#tx-psk** using the key **Aruba123!**



6. Open a command prompt (**cmd.exe**)

7. Run **ipconfig** to show your IP address.

```
C:\Users\student> ipconfig

Windows IP Configuration

...

Wireless LAN adapter Wi-Fi Lab:

   Connection-specific DNS Suffix  . : aruba-training.com
   Link-local IPv6 Address . . . . . : fe80::f56c:996b:bcc7:fb18%9
   IPv4 Address. . . . . . . . . . . : 10.1.34.50
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.34.1
```

8. Verify you have received an IP address in the 10.1.34.0/24 subnet.

Verify the Client Status in Aruba Central

9. In Aruba Central, open context Group: **campus-wifi-ui**, click **Clients**.

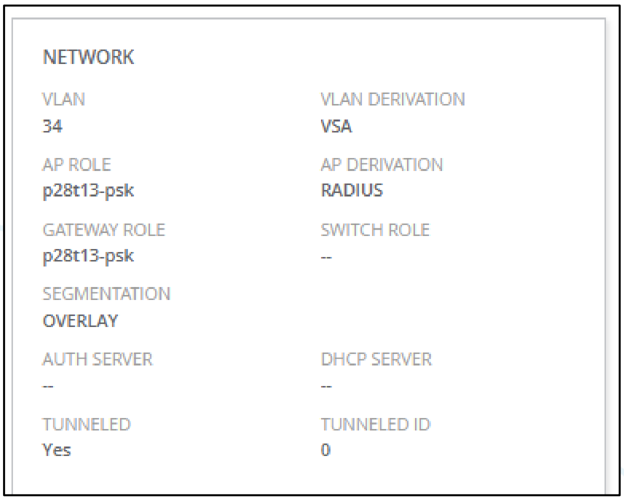
NOTE: Even though the client is tunneled to the gateway, Aruba Central will only show the client in the AP group, not the gateway group!

10. Verify your client is displayed in the client list.
11. Click the *client name* to open the client details.

12. The datapath tile will show the AP and GW that are used by the client connection.

Example:

- **Question**: To what AP is the client connected?
- **Answer**: This will be either ap1 or ap2.
- **Question**: To what gateway is the client connected?
- **Answer**: Based on the client MAC address, the client will be assigned to one of the gateways in the cluster, this will be either gw1 or gw2.
- **Question**: What is the connection between the AP and the gateway?
- **Answer**: Overlay. This represents the tunnel used between the AP and the gateway to transport the client traffic.



- **Question**: In the network tile, what is the segmentation and tunnel status?
- **Answer**: The client is tunneled, and the segmentation is overlay.

Verify the Client Status on the AP and GW CLI

13. Use the lab dashboard to open a console connection to the AP that your client is connected to.
14. Login using **admin** / **Aruba123!**.
15. Review the connected clients.

```
show clients
```

Here is an example output:

```
ap2# show clients

Client List
-----------
Name          IP Address  MAC Address        OS      ESSID       Access Point  Channel
Type  Role        IPv6 Address               Signal    Speed (mbps)
----          ----------  -----------        --      -----       ------------  -------  --
--  ----        ------------              ------    ------------
3c3786d49142  10.1.34.50  3c:37:86:d4:91:42  Win 10  p28t13-psk  ap2           52E      AC
p28t13-psk  fe80::f56c:996b:bcc7:fb18  62(good)  650(good)
Number of Clients   :1
Info timestamp      :756825
```

Review the Client Status on the Gateway

16. Use the MGMT PC to open an SSH connection to your client gateway.
17. Login using **admin** / **Aruba123!**.
18. Review the connected clients.

```
show user-table
```

```
(gw1) *# show user-table

Users
-----
    IP           MAC              Name          Role        Age(d:h:m)  Auth  VPN link
Connected To     Roaming   Essid/Bssid/Phy  Profile                          Forward mode
Type  Host Name  User Type
----------  ------------       ------        ----        ----------  ----  --------  -----
10.1.34.50  3c:37:86:d4:91:42  3c3786d49142  p28t13-psk  00:00:17
20:4c:03:5b:27:e2   Wireless  p28t13-psk       p28t13-psk_#1671553563764_37#_  dtunnel
WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/1 Free:0/0 Dyn:1 AllocErr:0 FreeErr:0
```

19. Review the assigned VLAN for the client.

```
show user-table verbose
```

```
(gw1) *# show user-table verbose

Users
-----
    IP           MAC              Name          Role        Age(d:h:m)  Auth  VPN link
Connected To     Roaming   Essid/Bssid/Phy  Profile                          Forward mode
Type  Host Name  User Type  Server  Vlan     Bwm  UaStr:ParseDisable/Flag/ShortIndex
----------  ------------       ------        ----        ----------  ----  --------  -----
10.1.34.50  3c:37:86:d4:91:42  3c3786d49142  p28t13-psk  00:00:17
20:4c:03:5b:27:e2   Wireless  p28t13-psk       p28t13-psk_#1671553563764_37#_  dtunnel
WIRELESS             34 (34)       OFF/0/0
```

```
User Entries: 1/1
 Curr/Cum Alloc:1/1 Free:0/0 Dyn:1 AllocErr:0 FreeErr:0
```

- **Question**: What is the VLAN the client is assigned to?
- **Answer**: The client is assigned to VLAN 34.

Review Tunnel Orchestration and Status

20. On the AP console, review the IPsec connections.

```
show crypto ipsec stats
```

```
ap2# show crypto ipsec stats

IPSEC STATS
-----------
MAP NAME                      IP ADDR    DEVNAME  TX/RX PACKETS  TX/RX BYTES    TX/RX
DROPS  TX/RX ERRORS
--------                      -------    -------  -------------  -----------    ---------
--  ------------
gw-ipsecmap-20:4c:03:b7:a2:b2  10.1.3.21  tun0     2940/2765      332684/304384  0/0
0/0
gw-ipsecmap-20:4c:03:b1:d5:02  10.1.3.22  tun1     2922/2741      327123/299563  0/0
0/0
Total IPSEC Count: 2
```

- **Question**: How many IPsec connections do you have in the list?
- **Answer**: 2, one for each gateway in the connected cluster.

21. Review the AP Tunnel Agent (ata) current endpoint (tunnel endpoints) configuration.

```
show ata current-cfg
```

```
ap2# show ata current-cfg

Current Central is Up
Microbranch AP is Disabled
Microbranch System IP is 0.0.0.0/::
[Current Configuration For cluster(auto_gwcluster_125_0)]
<Tunnel list>
-----pub_ip=10.1.3.21, local_ip=10.1.3.21, vlan=1,3,31,34, mcast=0, Tun_Type=GRE,
peer_device_type=Gateway
     key_exp=129600, dstNatt=4500, HBT_interval=3, HBT_Threshold=10
-----pub_ip=10.1.3.22, local_ip=10.1.3.22, vlan=1,3,31,34, mcast=0, Tun_Type=GRE,
peer_device_type=Gateway
     key_exp=129600, dstNatt=4500, HBT_interval=3, HBT_Threshold=10
<SSID list for primary>
-----ssid=p28t13-psk, type=0
```

- **Question**: What is the current Central status?

- **Answer**: The current central status is up. This is the tunnel agent connection to Central.
- **Question**: What is the cluster name?
- **Answer**: This should match the cluster name you have seen on the gateway group. If multiple cluster connections would be established, each cluster entry shows its own tunnel endpoints.
- **Question**: What SSIDs are bound to this cluster?
- **Answer**: Only one SSID is bound to this cluster connection: The SSID p#tx-psk.
- **Question**: Can you see in this output if the tunnels are currently up?
- **Answer**: No, this command output shows the configuration as received from the tunnel orchestrator. The status can be seen in the output of the **show ata endpoint** command.

22. Check the ata tunnel endpoint output.

```
show ata endpoint
```

```
ap2# show ata endpoint

ATA Endpoint Status
-------------------
UUID                                  IP ADDR    STATE                TUN DEV  TUN
SPI(OUT/IN)     LINK TAG  VALID TIME(s)  TUNNEL TYPE  GRE VLANs  HBT(Jiff/Missed/Sent/Rcv)
INNER IP    UP TIME(s)
----                                  -------    -----                -------  ------------
---    --------  -------------  -----------  ---------  ------------------------  -------
-   ----------
2424a9e8-0520-417e-bd2a-1b4007599672  10.1.3.21  SM_STATE_CONNECTED  tun0
1ef12800/7ab2e800  inet      127601         GRE          1,3,31,34  757225/0/2040/1990
10.1.4.51  2022-12-20 16:26:53
5d1ecf65-caef-4f7e-bfad-1207034b79ac  10.1.3.22  SM_STATE_CONNECTED  tun1
a6eab000/61a57000  inet      127603         GRE          1,3,31,34  757225/0/2039/1989
10.1.4.51  2022-12-20 16:26:53
Total Endpoints Count: 2
```

- **Question**: What is the state of the tunnels?
- **Answer**: Connected.
- **Question**: What does the TUN SPI OUT/IN indicate?
- **Answer**: These are the IPsec SAs that have been orchestrated by the tunnel orchestrator. These will match the SPI IN/OUT on the gateway side.

Review Tunnel Status on the GW

23. Switch to the gateway SSH connection associated with the AP (the example shows gw1, but it might be gw2 in your topology). Review the status of the connection to the Overlay Tunnel Orchestrator.

```
show crypto oto
```

```
(gw1) *# show crypto oto

OTO Status
Channel state:            CONNECTED
Channel UP since:         Tue Dec 20 08:31:11 2022
Channel Up count:         1
Channel Down count:       0
Keepalive Interval:       25
#Create Channel:          7
#Delete Channel:          6
#KeepAlive Sent:          532
#KeepAlive Received:      510
#KeepAlive Pending:       0
Create Spec:              5
Update Spec Sent/Recv:    0/0
Delete Spec:              2
Device Spec:              3
Resync Event Sent:        18
Ike Event Sent:           4
Peer Down DPD/HCM/OTO:    0/0/0
BG-SRC Learn/OnRekey:     4/0
BG-SRC Err SPI/Map/Vlan/B-Mesh:  0/0/0/0
Rekey Request/Done/Abort/Fake: 0/0/0/0
State Update Event Sent:  1
Down Event Sent:          0/0
HCM Message Lookup (Success/Fail): 0/0
HCM Message Drops No(VpnIP/ProbeIP): 0/0
Tunnel State Trigger: HCM
```

24. Review the active IPsec security associations.

```
show crypto ipsec sa
```

```
(gw1) *# show crypto ipsec sa


IPSEC SA (V2) Active Session Information
-----------------------------------
Initiator IP                            Responder IP
SPI(IN/OUT)        Flags   Start Time      Tunnel Type   Inner IP
------------                            ------------                            ------
----------   ------  ---------------   ------------  ----------
10.1.3.22                               10.1.3.21
fea4e400/9a8f0100  T2      Dec 20 10:28:38   N/A            -

Tunnel Service SA Information
-----------------------------------
```

```
Initiator IP                                Responder IP
SPI(IN/OUT)         Flags   Start Time         Tunnel Type   Inner IP
------------                                ------------                                          ------
----------   ------  ---------------   ------------  ----------
10.1.4.50                                   10.1.3.21
5f199000/5caa2000  UTlt    Dec 20 11:26:49   N/A           10.1.4.50
10.1.4.51                                   10.1.3.21
1ef12800/7ab2e800  UTlt    Dec 20 11:26:49   N/A           10.1.4.51

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
       L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
       l = uplink load-balance; t = Tunnel Service; P = Reverse-Pinning Enabled

Total IPSEC SAs: 3
```

- **Question**: How many IPsec sessions are there in the list?
- **Answer**: 3.
- **Question**: What are the destination systems of these IPsec sessions?
- **Answer**: One session to the other gateway in the cluster, two IPsec sessions for the APs.

25. Review the ISAKMP security associations.

```
show crypto isakmp sa
```

```
(gw1) *# show crypto isakmp sa

ISAKMP SA Active Session Information
------------------------------------
Initiator IP                              Responder IP                          Flags
Start Time         Private IP                               Peer ID
------------                              ------------                          -----
10.1.3.22                                 10.1.3.21                             r-v2-c
Dec 20 08:33:36     -                                  CN=CNJJKLB09H::20:4c:03:b1:d5:02
L=SW

Flags: i = Initiator; r = Responder
       m = Main Mode; a = Agressive Mode; v2 = IKEv2
       p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature
       x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
       3 = 3rd party AP; C = Campus AP; R = Microbranch AP;  Ru = Custom Certificate RAP;
I = IAP
       V = VIA; S = VIA over TCP; l = uplink load-balance; P = Reverse-Pinning Enabled

Total ISAKMP SAs: 1
```

- **Question**: How many ISAKMP SAs are there in the list?
- **Answer**: There is 1 ISAKMP SA between the two gateway IP addresses.
- **Question**: Why are there no ISAKMP Security Associations for the APs?

- **Answer**: The IPsec session keys between the gateways and the APs are orchestrated by the cloud-based Overlay Tunnel Orchestrator. ISAKMP is not used in this process under normal conditions. During the availability chapter you will learn that local tunnel survivability is available when the APs or gateways cannot reach the cloud OTO.

26. Review the tunnels that have been provisioned by the OTO.

```
show tunnelmgr tunnel-list
```

```
(gw1) *# show tunnelmgr tunnel-list

Tunnelmgr Table Dump
--------------------
Tunnel ID                             Map ID  Peer IP    Peer MAC           Device-Type
Secure-Mode   Status  GRE ID  Mtu
---------                             ------  -------    --------           -----------  -
63acc9b0-c92a-4145-a9e3-0e5b29e61ea6  327682  10.1.4.50  20:4c:03:8c:27:42  AP
No            UP      13      1500
c317426d-ccb5-46a6-a412-f54feebeac1c  327681  10.1.4.51  20:4c:03:5b:27:e2  AP
No            UP      10      1500

Total Entries:  2 Up: 2
```

- **Question**: How many tunnels are provisioned by the OTO?
- **Answer**: 1 for each AP.
- **Question**: What is the status of secure-mode?
- **Answer**: No. This indicates that an unencrypted GRE tunnel is used for the connection. In the next task you will see that you can also establish GRE over IPsec tunnels. By default, a standard, unencrypted GRE tunnel is used.

27. Review the active tunnels.

```
show datapath tunnel
```

Example screenshot:

```
#       Source          Destination     Prt  Type  MTU   VLAN  Acls                              BSSID              Decaps     Encaps     Heartbeats  Flags            EncapKBytes   DecapKBytes
------  --------------  --------------  ---  ----  ----  ----  --------------------------------  -----------------  ---------- ---------- ----------  ---------------  ------------  -----------
13      10.1.3.21       10.1.4.50       47   0     1500  0     0    0    0    0     0     0      00:00:00:00:00:00        7116       8365       2643 EMSPDt
14      SPI7AB2E800out  10.1.4.51       50   IPSE  1450  0     routeDest 0003     0     0                                    0       4021             TN               0             0
12      SPIFEA4E400 in  10.1.3.21       50   IPSE  1500  0     routeDest 0000     0     0                                 1208          0             TF               0             0
9       SPI1EF12800 in  10.1.3.21       50   IPSE  1450  0     routeDest 0003     0     0                                 4278          0             TN               0             0
10      10.1.3.21       10.1.4.51       47   0     1500  0     0    0    0    0     0     0      00:00:00:00:00:00        5775       2367       2643 EMSPDb
15      SPI5F199000 in  10.1.3.21       50   IPSE  1450  0     routeDest 0000     0     0                                 4282          0             TN               0             0
17      SPI5CAA2000out  10.1.4.50       50   IPSE  1450  0     routeDest 0003     0     0                                    0       4021             TN               0             0
11      SPI9A8F0100out  10.1.3.22       50   IPSE  1500  0     routeDest 0003     0     0                                    0       1212             TF               0             0
```

- **Question**: What are the two types of tunnels in the list based on the Protocol (Prt)?
- **Answer**: IPsec (IP protocol 50) and GRE (IP protocol 47).
- **Question**: What are these tunnels used for between the AP and the gateway?

- **Answer**: The IPsec tunnel is, by default used, to transport and secure the control plane communication between the AP and the gateway. The GRE tunnel is used to transport the user data frames between the AP and the gateway.

Review the GRE Tunnel Heartbeats

28. Take note of the value in the GRE heartbeats column for one of your APs.
29. Run the **show datapath tunnel** command again.

```
show datapath tunnel
```

- **Question**: Did the value change in the GRE heartbeat column?
- **Answer**: Yes. The GRE heartbeat is exchanged once every second.

Tunnel VLANs

In this section you will review the VLANs that are enabled on the GRE tunnel.

30. On the AP console connection, review the ata current-cfg.

```
show ata current-cfg
```

```
ap2# show ata current-cfg

Current Central is Up
Microbranch AP is Disabled
Microbranch System IP is 0.0.0.0/::
[Current Configuration For cluster(auto_gwcluster_125_0)]
<Tunnel list>
-----pub_ip=10.1.3.21, local_ip=10.1.3.21, vlan=1,3,31,34, mcast=0, Tun_Type=GRE,
peer_device_type=Gateway
     key_exp=129600, dstNatt=4500, HBT_interval=3, HBT_Threshold=10
-----pub_ip=10.1.3.22, local_ip=10.1.3.22, vlan=1,3,31,34, mcast=0, Tun_Type=GRE,
peer_device_type=Gateway
     key_exp=129600, dstNatt=4500, HBT_interval=3, HBT_Threshold=10
<SSID list for primary>
-----ssid=p28t13-psk, type=0
```

- **Question**: What VLANs are provisioned by the OTO on the gateway tunnels?
- **Answer**: The tunnel orchestrator lists VLANs 1,3,31,34 to be provisioned on the data plane tunnels.

31. Review the active tunnels and the list of active VLANs.

```
show ata endpoint
```

```
ap2# show ata endpoint

ATA Endpoint Status
-------------------
```

```
UUID                                  IP ADDR    STATE              TUN DEV  TUN
SPI(OUT/IN)    LINK TAG  VALID TIME(s)  TUNNEL TYPE  GRE VLANs  HBT(Jiff/Missed/Sent/Rcv)
INNER IP   UP TIME(s)
----                                  -------    -----              -------  ------------
---    --------  ------------  -----------  ---------  ------------------------  -------
-   ----------
2424a9e8-0520-417e-bd2a-1b4007599672  10.1.3.21  SM_STATE_CONNECTED  tun0
1ef12800/7ab2e800  inet      126605         GRE          1,3,31,34  758221/0/3058/2984
10.1.4.51  2022-12-20 16:26:53
5d1ecf65-caef-4f7e-bfad-1207034b79ac  10.1.3.22  SM_STATE_CONNECTED  tun1
a6eab000/61a57000  inet      126607         GRE          1,3,31,34  758221/0/3057/2983
10.1.4.51  2022-12-20 16:26:53
Total Endpoints Count: 2
```

- **Question**: Does the GRE VLANs list match the provisioned VLANs?
- **Answer**: Yes, VLANs 1,3,31,34 are provisioned on the GRE tunnels.
- **Question**: You configured the WLAN with VLAN 34. Why are VLANs 1,3 and 31 are also provisioned in the list?
- **Answer**: The orchestrator will provision *all* VLANs that are defined on the gateway, independent of the configured VLAN on the WLAN profile. Whenever a client is assigned to any of these VLANs, the traffic will be tunneled.
- **Question**: Your WLAN operates on 2.4 GHz and 5 GHz bands. In AOS 8, this would result in *two* GRE tunnels between the AP and the gateway. What do you notice on AOS 10?
- **Answer**: In AOS 10, only *one* GRE tunnel is used between the AP and the gateway. All WLANs and bands will use the same GRE tunnel and their traffic will be forwarded with a VLAN tag inside of the GRE tunnel. This is how multiple WLANs and VLANs can be transported over a single tunnel in AOS 10.

This is the reason that a VLAN used for a tunnel WLAN should *not* be enabled on the AP switch VLAN trunk port. If that tunneled VLAN would be enabled on the AP trunk port, the AP may see the same MAC addresses on both the wired port and the GRE tunnel.

Task 5: Configure GRE over IPsec

In this task you will change the default GRE tunnel forwarding mode between the AP and the gateway to GRE over IPsec.

This provides data plane encryption on the path between the AP and the gateway.

Objectives

- Understand the default data plane security between AP and gateway.
- Configure GRE over IPsec for the data plane traffic.

Steps

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config (gear icon)**.
2. Navigate to **Security > Expand Data Handling**.
3. Set the option Data Encryption to **enabled**.
4. Click **Save Settings**.

> **NOTE:** Although this option shows under the AP group configuration, this setting is not saved in the AP config. This setting configures the cloud Overlay Tunnel Orchestrator. The OTO will now instruct the APs and gateways to establish GRE over IPsec tunnels instead of GRE tunnels.

5. In Aruba Central, click **Audit Trail** to review the changed configuration.
   - **Question**: What is the description of the latest audit entry? (You may need to refresh the audit trail to see the latest entry)
   - **Answer**: Overlay_wlan Service : config Updated.
   - **Question**: Did the configuration on the AP itself change because of your change?
   - **Answer**: No. Only the Overlay Tunnel Orchestrator in Aruba Central was updated.

6. Use the **3 dots** to check the details of the audit trail entry.

```
Overlay_wlan config Updated

"aruba-overlay-wlan:config": {
"ssid_cluster": [
{
"profile": "p28t13-psk"
"gw_cluster_list": [
{
"cluster_redundancy_type": "PRIMARY"
"cluster_group_name": "campus-gw-main"
! "tunnel_type": "GREOIPSEC"
```

```
}
]
"profile_type": "WIRELESS_PROFILE"
}
]
}
}
```


- **Question**: What is the tunnel type that is now set on the OTO profile?
- **Answer**: *GREOIPSEC*—this is GRE over IPSEC.

7. On the console of the AP, review the ata current configuration.

```
show ata current-cfg
```

```
ap2# show ata current-cfg

Current Central is Up
Microbranch AP is Disabled
Microbranch System IP is 0.0.0.0/::
[Current Configuration For cluster(auto_gwcluster_125_0)]
<Tunnel list>
-----pub_ip=10.1.3.22, local_ip=10.1.3.22, vlan=1,3,31,34, mcast=0, Tun_Type=GREoIPsec,
peer_device_type=Gateway
     key_exp=129600, dstNatt=4500, HBT_interval=3, HBT_Threshold=10
-----pub_ip=10.1.3.21, local_ip=10.1.3.21, vlan=1,3,31,34, mcast=0, Tun_Type=GREoIPsec,
peer_device_type=Gateway
     key_exp=129600, dstNatt=4500, HBT_interval=3, HBT_Threshold=10
<SSID list for primary>
-----ssid=p28t13-psk, type=0
```

- **Question**: What is the tunnel type that the AP received from the Overlay Tunnel Orchestrator?
- **Answer**: GREoIPsec.

8. On the AP, review the active tunnels.

```
show ata endpoint
```

```
ap2# show ata endpoint

ATA Endpoint Status
-------------------
UUID                                      IP ADDR    STATE                TUN DEV  TUN
SPI(OUT/IN)    LINK TAG  VALID TIME(s)  TUNNEL TYPE  GRE VLANs  HBT(Jiff/Missed/Sent/Rcv)
INNER IP   UP TIME(s)
----                                      -------    -----                -------  ------------
---    --------  ------------  -----------  ---------  -------------------------  -------
-   ----------
```

```
2de6f27f-06fe-4a73-bedb-ceee2db49c87  10.1.3.21  SM_STATE_CONNECTED  tun0
f7d0a400/a416bc00  inet      129270        GREoIPsec    1,3,31,34  1855/0/326/326
10.1.4.50  2022-11-21 07:33:41
7f0f139e-de82-4bb2-b281-3520c26d33bb  10.1.3.22  SM_STATE_CONNECTED  tun1
34e4a400/d893e400  inet      129267        GREoIPsec    1,3,31,34  1855/0/327/327
10.1.4.50  2022-11-21 07:33:39
Total Endpoints Count: 2
```

- **Question**: What is the tunnel type?
- **Answer**: GREoIPsec.

9. Open a session to the gateway.
10. Review the active tunnels provisioned by the Overlay Tunnel Orchestrator.

```
show tunnelmgr tunnel-list
```

```
(gw2) #show tunnelmgr tunnel-list

Tunnelmgr Table Dump
--------------------
Tunnel ID                             Map ID  Peer IP    Peer MAC          Device-Type
Secure-Mode  Status  GRE ID  Mtu
---------                             ------  -------    --------          -----------  -
----------  ------  ------  ---
2409738b-43a9-4f65-b83a-3e8c439920b8  327681  10.1.4.51  20:4c:03:c5:e4:48  AP
Yes          UP      16      1200
74733718-7748-4677-9c6f-741459b47fe0  327682  10.1.4.50  20:4c:03:8c:28:26  AP
Yes          UP      13      1200

Total Entries:  2 Up: 2
```

- **Question**: What is the status of the Secure-mode column?
- **Answer**: Yes, for both AP tunnels.

11. In Aruba Central, in the AP group, on the security page, disable the data encryption option.
12. Click **Save Settings**.
13. On the AP console, verify the tunnel type has reverted to GRE.

```
show ata endpoint
```

```
ap2# show ata endpoint

ATA Endpoint Status
-------------------
UUID                                  IP ADDR    STATE                TUN DEV  TUN
SPI(OUT/IN)    LINK TAG  VALID TIME(s)  TUNNEL TYPE  GRE VLANs  HBT(Jiff/Missed/Sent/Rcv)
INNER IP   UP TIME(s)
```

```
----                                 -------    -----                -------  -----------
----    --------  ------------  -----------  ---------  ------------------------  ------
--   ----------
2424a9e8-0520-417e-bd2a-1b4007599672  10.1.3.21  SM_STATE_CONNECTED   tun0
1ef12a00/7ab2ea00  inet      129594         GRE         1,3,31,34  0/3/0/0
10.1.4.51  2022-12-21 08:24:54
5d1ecf65-caef-4f7e-bfad-1207034b79ac  10.1.3.22  SM_STATE_CONNECTING  tun1
a6eab200/61a57200  inet      129597         GRE         1,3,31,34  0/0/0/0
10.1.4.51  1970-01-01 00:00:00
Total Endpoints Count: 2
```

You have completed this Lab!

Lab 04.02 Tunneled WLAN Cluster Operation

Overview

In this lab you will explore how the gateway cluster operates with a tunnel WLAN.

You will see how the APs establish a tunnel to each of the cluster members, and clients are assigned to a gateway based on a hashing algorithm and the bucket map.

The last section of the lab will demonstrate what happens in case of a gateway failure.

Objectives

After completing this lab, you will be able to:

- Understand the gateway cluster operation.
- Understand how clients are assigned to a gateway in the cluster.
- Understand the cluster bucket map.
- Verify the client distribution and failover operation of a gateway cluster.

Task 1: Review the Cluster Status

In this task you will review the cluster status on the gateways.

Objectives

- Review the cluster status on the gateways.
- Review the cluster heartbeat.

Steps

Review the Gateway Cluster Status

1. Use the MGMT PC to open an SSH connection to the gateway used by your wireless client.
2. Review the cluster configuration. Remember that Aruba Central will automatically include all the gateways in the group as cluster members when the auto-group cluster mode is selected.

```
show lc-cluster group-profile
```

```
(gw1) *# show lc-cluster group-profile

Classic Controller Cluster Profile List
---------------------------------------
Name                  Profile Status
----                  --------------
auto_gwcluster_125_0

Total:1
```

3. Review the currently applied profile on the GW1.

```
show lc-cluster group-membership
```

```
(gw1) *# show lc-cluster group-membership

Cluster Enabled, Profile Name = "auto_gwcluster_125_0"
Heartbeat Threshold = 900 msec (default)
Cluster Info Table
------------------
Type IPv4 Address    Priority Connection-Type STATUS
---- --------------- -------- --------------- ------
self       10.1.3.21      128             N/A CONNECTED (Leader)
peer       10.1.3.22      128    L2-Connected CONNECTED (Member)
```

4. Review the active IPsec connections.

```
show crypto ipsec sa
```

```
(gw1) *# show crypto ipsec sa


IPSEC SA (V2) Active Session Information
-----------------------------------
```

```
Initiator IP                              Responder IP                              SPI(IN/OUT)        Flags   Start Time
Tunnel Type   Inner IP
------------                              ------------                              ----------------   ------  ---------------
------------  ----------
10.1.3.22                                 10.1.3.21                                 e6337800/eaa53e00  T2      Dec 21 03:43:41
N/A                -

Tunnel Service SA Information
-----------------------------------
Initiator IP                              Responder IP                              SPI(IN/OUT)        Flags   Start Time
Tunnel Type   Inner IP
------------                              ------------                              ----------------   ------  ---------------
------------  ----------
10.1.4.50                                 10.1.3.21                                 5f199200/5caa2200  UTlt    Dec 21 03:24:47
N/A           10.1.4.50
10.1.4.51                                 10.1.3.21                                 1ef12a00/7ab2ea00  UTlt    Dec 21 03:24:47
N/A           10.1.4.51

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
       L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
       l = uplink load-balance; t = Tunnel Service; P = Reverse-Pinning Enabled

Total IPSEC SAs: 3
```

- **Question**: Do you have an IPsec session to the gw2 (10.1.3.22)?
- **Answer**: Yes, all members of a cluster establish full-mesh IPsec tunnels between each other.
- **Question**: What does the *2* flag indicate for the IPsec SA?
- **Answer**: The IPsec sessions is established using IKEv2.

5. Review the ISAKMP SAs between the cluster members.

```
show crypto isakmp sa
```

```
(gw1) *#  show crypto isakmp sa

ISAKMP SA Active Session Information
------------------------------------
Initiator IP                             Responder IP                            Flags       Start Time         Private IP
Peer ID
------------                             ------------                            -----       ----------         ----------
-------------
10.1.3.22                                10.1.3.21                               r-v2-c      Dec 21 00:09:37     -
CN=CNJJKLB09H::20:4c:03:b1:d5:02 L=SW

Flags: i = Initiator; r = Responder
       m = Main Mode; a = Agressive Mode; v2 = IKEv2
       p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature
       x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
       3 = 3rd party AP; C = Campus AP; R = Microbranch AP;  Ru = Custom Certificate RAP; I = IAP
       V = VIA; S = VIA over TCP; l = uplink load-balance; P = Reverse-Pinning Enabled

Total ISAKMP SAs: 1
```

- **Question**: What does the *c* flag indicate?
- **Answer**: The *c* flag indicates certificate-based authentication. The gateway uses the factory certificate that is installed in the TPM chip for the IPsec IKEv2 authentication.

6. Review the active firewall sessions to the peer gateway. You can filter on the peer gateway IP address and use “Port” to get the header line in the output.

```
show datapath session | include 10.1.3.22,Port
```

a Hewlett Packard Enterprise company

```
(gw1) *# show datapath session | include 10.1.3.22,Port
Source IP or MAC  Destination IP  Prot SPort DPort Cntr     Prio ToS Age Destination TAge Packets    Bytes      Flags
CPU ID
10.1.3.21         10.1.3.22       50   0     0     0/0      0    0   117 pc0         ece4 0          0          FY              1
10.1.3.22         10.1.3.21       6    9190  9199  0/0      0    0   1   tunnel 10   18c2 4922       256073     C               1
10.1.3.22         10.1.3.21       6    9199  9190  0/0      0    0   1   local       18bd 4650       242038                     1
10.1.3.22         10.1.3.21       17   8211  8211  0/0      0    46  0   pc0         18cc 1502609    170048347  FCI             1
10.1.3.21         10.1.3.22       17   8498  8211  0/0      0    0   0   pc0         1c   2          493        FI              1
10.1.3.21         10.1.3.22       6    9199  9190  0/0      0    0   1   tunnel 10   18c2 4924       619988                     1
10.1.3.21         10.1.3.22       17   8211  8211  0/0      0    0   35  pc0         18cc 0          0          FYI             1
10.1.3.22         10.1.3.21       50   0     0     0/0      0    0   0   pc0         ece4 11880      1745648    FC              1
10.1.3.22         10.1.3.21       17   8211  8498  0/0      0    0   1   pc0         1c   0          0          FYCI            1
10.1.3.21         10.1.3.22       6    9190  9199  0/0      0    0   1   local       18bd 4652       242033     C               1
```

- **Question**: What is the Prot 50 session?
- **Answer**: This is the IPsec connection between the 2 gateways.
- **Question**: What is the Prot 17 (UDP) Port 8211 session?
- **Answer**: This is the Aruba PAPI control plane protocol. The gateways use PAPI to exchange cluster and client information to each other.

Cluster Heartbeat Counters

The cluster members will use a heartbeat mechanism to verify they are still connected to each other.

7. Review the cluster heartbeat counters.

```
show datapath cluster heartbeat counters
```

```
(gw1) *# show datapath cluster heartbeat counters

Cluster Heartbeat Counters
--------------------------
IPv4 Address         RES        RSR         MIS        TOTRES     TOTRSR     TOTMIS    HMPD
--------------- ---------- ---------- ---------- ---------- ---------- ---------- ------
      10.1.3.22     751448     751448          0     751448     751448          0      0

-----------PREAMBLE----------------
RES    - REQ SENT
RSR    - RSP RCVD
MIS    - MISSES
TOTRES - TOTAL REQ SENT
TOTRSR - TOTAL RSP RCVD
TOTMIS - TOTAL MISSES
HMPD   - HBT MISS PEER DEAD
```

VLAN Probing

To ensure connected clients can successfully failover to another cluster member, the gateways will test if the connected VLANs are actually reachable between each other.

In case the switch administrator would have forgotten to enable a VLAN on the switch VLAN trunk port, this mechanism will detect that there is a problem with the VLAN connectivity.

8. On the SSH connection to gw1, review the cluster VLAN probe status.

```
show lc-cluster vlan-probe status
```

```
(gw1) *# show lc-cluster vlan-probe status

Cluster VLAN Probe Status
-------------------------
Type IPv4 Address    REQ-SENT REQ-FAIL ACK-SENT ACK-FAIL REQ-RCVD ACK-RCVD VLAN_FAIL CONN-
TYPE START/STOP
---- --------------- -------- -------- -------- -------- -------- -------- --------- -----
peer       10.1.3.22     4599        0        5        0        5        4         1   L3
Conn      0/    2
```

- **Question**: What VLAN is listed as failed for the probing test?
- **Answer**: VLAN 1. This is expected since the VLAN 1 is not enabled on the aggregation switches trunk port.
- **Question**: What does the Connection Type L3 Connected mean?
- **Answer**: It means that for clients connected to the VLAN 1 (the failed probe), the cluster will not perform a stateful failover (Stateful failover requires access to the same VLAN for both gateways).

Task 2: Cluster Bucket Map

The bucket map is used by the cluster to distribute the clients to the cluster members in order to distribute the load.

The bucket map is a table of 256 records.

A hashing algorithm is used to assign the client MAC address to a bucket map entry. This hashing system is predictable, meaning that if a client MAC A1 would be hashed to bucket ID 20, it will always be mapped to bucket ID 20. Multiple clients can be hashed to the same bucket ID. MAC A2 could be hashed to the same bucket ID 20, for example, or a different bucket.

Each of the 256 bucket IDs is handled by one of the gateways in the cluster. These gateways are referred to as UAC, or user anchor controllers. If there are two gateways in the cluster, there will be a UAC0 and UAC1.

By changing the active UAC for a bucket map entry, the cluster can change the load distribution of the clients. This system will not directly move clients to another member of the cluster, but it changes the bucket ID UAC; therefore, all the clients that happen to be hashed to these bucket IDs are moved to the new UAC (gateway).

The AP will perform the hashing and forward the client traffic to the assigned UAC. This requires the AP to have the active bucket map of the cluster. Each AP will be assigned a DDG (Device Designated Gateway); that cluster member will provide the active bucket map to the AP using the PAPI protocol. This bucket map update does not rely on a cloud connection: it is updated directly between the AP and the GW cluster.

The concept of the DDG ensures that the load of updating the maps to the APs is distributed over the members of the cluster.

Objectives

- Understand the bucket map.
- Review the bucket map on the AP and the gateway.
- Verify the client assignment to a bucket ID.

Steps

Explore the Bucket Map

In the next steps, you will explore the bucket map on the gateway.

1. Use the MGMT PC to open an SSH connection to the gateway that your wireless client is connected to.
2. Review the current bucket map.

```
show aaa cluster bucketmap
```

```
(gw1) *# show aaa cluster bucketmap


Bucket map for auto_gwcluster_125_0, Rcvd at : Tue Dec 20 08:36:29 2022
```

```
---------------------------------------------------------------------------
Item                  Value
----                  -----
Essid                 auto_gwcluster_125_0
UAC0                  10.1.3.21
UAC1                  10.1.3.22
Active Map[0-31]      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Active Map[32-63]     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Active Map[64-95]     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Active Map[96-127]    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Active Map[128-159]   01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Active Map[160-191]   01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Active Map[192-223]   01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Active Map[224-255]   01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01

Standby Map[0-31]     01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Standby Map[32-63]    01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Standby Map[64-95]    01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Standby Map[96-127]   01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Standby Map[128-159]  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Standby Map[160-191]  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Standby Map[192-223]  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Standby Map[224-255]  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

L2connect[0-31]       1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2connect[32-63]      1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2connect[64-95]      1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2connect[96-127]     1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2connect[128-159]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2connect[160-191]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2connect[192-223]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2connect[224-255]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

IsActive[0-31]        1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
IsActive[32-63]       1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
IsActive[64-95]       1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
IsActive[96-127]      1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
IsActive[128-159]     0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
IsActive[160-191]     0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
IsActive[192-223]     0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
IsActive[224-255]     0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

- **Question**: How many UAC entries do you see?
- **Answer**: 2: UAC0 and UAC1.
- **Question**: What are the IP addresses of these gateways?
- **Answer**: In the example output, UAC0 is mapped to 10.1.3.21, UAC1 is mapped to 10.1.3.22. The line Active Map [0-31] shows the first 32 bucket ids and the number in each field indicates the active UAC.
- **Question**: In the Active Map, what is the UAC that is used for bucket id 0 and 1?
- **Answer**: The values show *00*, this represents the UAC0. In the example output, this is the 10.1.3.21 gateway.
- **Question**: In the Active Map, what is the UAC that is used for bucket id 128 and 129?
- **Answer**: The values show *01*, this represents the UAC1. In the example output, this is the 10.1.3.22 gateway.
- **Question**: How are the bucket IDs assigned to the UAC?

- **Answer**: Half of the bucket IDs are assigned to the UAC0, the other half to the UAC1. This will result in a fair, hash-based distribution of the clients over the two gateways.

Review the Bucket Map on the AP

3. Use the lab dashboard to open a console connection to the AP used by your wireless client.
4. Review the bucket map that was received using PAPI from the DDG

```
show overlay bucketmap status
```

```
ap1# show overlay bucketmap status

Cluster auto_gwcluster_125_0 radio=0 zone=0 - Num UACs 2
--------------------------------------------------------
Index  ArrayIdx  UAC IP     Num STAs
-----  --------  ------     --------
0      0         10.1.3.21  1
1      1         10.1.3.22  0
Station List
------------
UAC Index  Station Mac        BSSID
---------  -----------        -----
0          3C:37:86:D4:91:42  F4:2E:7F:7B:15:F0
Bucket Map
----------
Bucket Idx Range  Bucket Map
----------------  ----------
[0-31]            0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[32-63]           0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[64-95]           0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[96-127]          0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[128-159]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[160-191]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[192-223]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[224-255]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-                 Standby Map
[0-31]            1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[32-63]           1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[64-95]           1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[96-127]          1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[128-159]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[160-191]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[192-223]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[224-255]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Statistics:Bmap Updates=0; UAC:Adds=2 Deletes=0; STAnswer:Adds=0 Deletes=1 moves=0 errs=0
copies=0
```

5. Review station manager bucket map. This output includes the active client MAC addresses and the bucket ID that was calculated for that MAC.

```
show ap debug stm-bucketmap
```

```
ap1#      show ap debug stm-bucketmap

Bucket map for cluster auto_gwcluster_125_0
```

```
-------------------------------------------
Item                        Value
----                        -----
Cluster                     auto_gwcluster_125_0
UAC 0                       10.1.3.21 (N/A)
UAC 1                       10.1.3.22 (N/A)
Current Map [0-31]          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Current Map [32-63]         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Current Map [64-95]         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Current Map [96-127]        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Current Map [128-159]       01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Current Map [160-191]       01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Current Map [192-223]       01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Current Map [224-255]       01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01

Active Map [0-31]           00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Active Map [32-63]          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Active Map [64-95]          00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Active Map [96-127]         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Active Map [128-159]        01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Active Map [160-191]        01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Active Map [192-223]        01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Active Map [224-255]        01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01

Standby Map [0-31]          01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Standby Map [32-63]         01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Standby Map [64-95]         01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Standby Map [96-127]        01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
Standby Map [128-159]       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Standby Map [160-191]       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Standby Map [192-223]       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Standby Map [224-255]       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

L2 Connectedness [0-31]     1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [32-63]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [64-95]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [96-127]   1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [128-159]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [160-191]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [192-223]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [224-255]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Current Map Timestamp Wed Dec 21 08:24:54 2022 (1h:21m:1s ago); gen_num=1 Reason=Bmap Message Trigger=Normal Bmap
Bucket Map Rcvd Timestamp Wed Dec 21 08:24:54 2022 (1h:21m:1s ago)
Cluster auth-surv status 0 (up)

Mappings
--------
Type   Name
----   ----
ESSID  p28t13-psk

Bucket Index 7:
        stAnswer:3c:37:86:d4:91:42
```

- **Question**: Do you see your station (sta) at the bottom of the output?
- **Answer**: Yes, the active clients will be listed.
- **Question**: What is the bucket index for your client?
- **Answer**: This depends on your client MAC address. In the example output, the MAC is assigned to index 7.

Review the Client to Bucketmap Mapping

6. Switch to the gateway and review the client to bucket map entry.

```
show aaa cluster users
```

Example

```
(gw1) *# show aaa cluster users


Active Users for ESSID : auto_gwcluster_125_0
---------------------------------------------
BUCKET  MAC                IP          Active UAC  Standby UAC
------  ---                --          ----------  -----------
7       3c:37:86:d4:91:42  10.1.34.50  10.1.3.21   10.1.3.22
```

- **Question**: What is the bucket for the client MAC?
- **Answer**: Since the hash algorithm has a predictable result, the gateway shows the same bucket index as the AP. In the example output, this is 7.

7. Take note of the current active gateway for the client. In the example output, this is gw1.

Task 3: Load Distribution and Failover

In this task you will test the failover of the gateway cluster. First you will review the active load and active gateway of the client.

The next step will be to reboot the gateway that is used by the client and verify the impact on the client traffic flow.

Objectives

- Verify the cluster load distribution for clients and APs.
- Verify the failover of a cluster member.

Steps

Review the Current Load Distribution

In these steps you will review the active load of the DDG (Device Designated Gateway – AP load) and the client load.

1. On the gateway, review the current load distribution of the APs.

```
show lc-cluster load distribution ap
```

```
(gw1) *# show lc-cluster load distribution ap

Cluster Load Distribution for APs
---------------------------------
Type IPv4 Address    Active APs     Standby APs
---- --------------- -------------- ---------------
self       10.1.3.21              1               1
peer       10.1.3.22              1               1
Total: Active APs 2 Standby APs 2
```

2. Review the current load distribution of the clients.

```
show lc-cluster load distribution client
```

```
(gw1) *# show lc-cluster load distribution client

Cluster Load Distribution for Clients
-------------------------------------
Type IPv4 Address    Active Clients Standby Clients
---- --------------- -------------- ---------------
self       10.1.3.21              1               0
peer       10.1.3.22              0               1
Total: Active Clients 1 Standby Clients 1
```

Prepare the Failover

3. On the AP, review the currently used gateway for the client.

```
show overlay bucketmap status
```

```
ap1# show overlay bucketmap status

Cluster auto_gwcluster_125_0 radio=0 zone=0 - Num UACs 2
--------------------------------------------------------
Index  ArrayIdx  UAC IP     Num STAs
-----  --------  ------     --------
0      0         10.1.3.21  1
1      1         10.1.3.22  0
Station List
------------
UAC Index  Station Mac        BSSID
---------  -----------        -----
0          3C:37:86:D4:91:42  F4:2E:7F:7B:15:F0
Bucket Map
----------
Bucket Idx Range  Bucket Map
----------------  ----------
[0-31]            0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
...
```

4. Use the MGMT PC to open an SSH connection to the standby gateway (the gateway that is currently not active for the client). In the example output, this is gw2.
5. Review the user-table. There should be no active users at this point.

```
show user-table
```

Example output.

```
(gw2) # show user-table

Users
-----
    IP            MAC        Name    Role   Age(d:h:m)   Auth   VPN link     Connected To
Roaming  Essid/Bssid/Phy  Profile  Forward mode  Type  Host Name  User Type
----------  ------------  ------  ----  ----------  ----  --------  ------------------  --

User Entries: 0/0
 Curr/Cum Alloc:0/0 Free:0/0 Dyn:0 AllocErr:0 FreeErr:0
```

6. Review the standby user table.

```
show user-table standby
```

```
(gw2) # show user-table standby

Dormant Mac Hash Table
----------------------
 IP          MAC                l2role      l3role     vlan    ua_done
Essid/Bssid/Tunnelid                  Counts(User/PTK)    UUID                      Active
UAC IP
---         -----              --------     --------   ------  ---------  ------------------
----                -----------------  ------                   ---------------
```

```
10.1.34.50  3c:37:86:d4:91:42  p28t13-psk            34      1          p28t13-
psk/20:4c:03:8c:27:42/0x1000a  8/0                 204c03b7a2b2000000a80000  10.1.3.21

Total Entries    : 1
```

Reboot the Gateway of the Client

You are now ready to test the failover.

7. On the wireless client, perform a continuous ping to **10.254.1.21**.

```
ping 10.254.1.21 -t
```

8. Reboot the gateway that is currently used for your client.

```
reload
```

Example output. In the example, GW1 is the active gateway for the client.

```
(gw1) *# reload
Do you really want to restart the system(y/n): y

System will now restart!
Log infrastructure ended gracefully.
```

9. On the wireless client, verify the ping continues.

```
Reply from 10.254.1.21: bytes=32 time=41ms TTL=126
Reply from 10.254.1.21: bytes=32 time=8ms TTL=126
Reply from 10.254.1.21: bytes=32 time=22ms TTL=126
Request timed out.
Reply from 10.254.1.21: bytes=32 time=26ms TTL=126
Reply from 10.254.1.21: bytes=32 time=11ms TTL=126
Reply from 10.254.1.21: bytes=32 time=79ms TTL=126
```

10. On the AP, verify that the updated client to UAC mapping.

NOTE: The client is immediately assigned to the standby gateway. The bucket map itself will be updated a few moments later. You may repeat the command until you see all the bucket ids mapped to one UAC.

```
ap1# show overlay bucketmap status

Cluster auto_gwcluster_125_0 radio=0 zone=0 - Num UACs 1
--------------------------------------------------------
Index  ArrayIdx  UAC IP     Num STAs
-----  --------  ------     --------
0      0         10.1.3.22  1
Station List
------------
UAC Index  Station Mac        BSSID
---------  -----------        -----
0          3C:37:86:D4:91:42  F4:2E:7F:7B:15:F0
Bucket Map
----------
Bucket Idx Range  Bucket Map
```

```
----------------  ----------
[0-31]            0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[32-63]           0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[64-95]           0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[96-127]          0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[128-159]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[160-191]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[192-223]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[224-255]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
-                 Standby Map
[0-31]            X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X
[32-63]           X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X
[64-95]           X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X
[96-127]          X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X
[128-159]         X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X
[160-191]         X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X
[192-223]         X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X
[224-255]         X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X
Statistics:Bmap Updates=1; UAC:Adds=2 Deletes=0; STAnswer:Adds=0 Deletes=1 moves=1 errs=0
copies=1
```

Verify the Status on the New Gateway

11. Switch to the standby gateway (the gateway that has now become the active gateway for the client).
12. Review the cluster heartbeat counters.

```
show datapath cluster heartbeat counters
```

```
(gw2) #show datapath cluster heartbeat counters

Cluster Heartbeat Counters
--------------------------
IPv4 Address        RES        RSR         MIS        TOTRES     TOTRSR      TOTMIS     HMPD
--------------- ---------- ---------- ---------- ---------- ---------- ---------- ------
      10.1.3.21          0          0          0     789706     789686          20       1

-----------PREAMBLE----------------
RES     - REQ SENT
RSR     - RSP RCVD
MIS     - MISSES
TOTRES - TOTAL REQ SENT
TOTRSR - TOTAL RSP RCVD
TOTMIS - TOTAL MISSES
HMPD    - HBT MISS PEER DEAD
------------------------------------
```

- **Question**: How many missed heartbeats do you see?
- **Answer**: This depends on your setup. In the example output, 20 missed heartbeats were reported.

13. Review the user table. This table was empty before the failover.

```
show user-table
```

```
(gw2) # show user-table

Users
-----
    IP          MAC            Name         Role        Age(d:h:m)  Auth  VPN link
Connected To     Roaming   Essid/Bssid/Phy  Profile                         Forward mode
Type    Host Name  User Type
----------  ------------      ------       ----        ----------  ----  --------  -----
-------------  -------   ---------------  -------                        ------------  --
--    ---------  ---------
10.1.34.50  3c:37:86:d4:91:42  3c3786d49142  p28t13-psk  00:17:33
20:4c:03:8c:27:42   Wireless  p28t13-psk       p28t13-psk_#1671553563764_37#_  dtunnel
Win 10             WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/1 Free:0/0 Dyn:1 AllocErr:0 FreeErr:0
```

14. On the AP, review the tunnel status history.

```
show ap debug stm-cluster node-msg-history
```

```
 ...
2022-12-21 08:24:54  10.1.3.22  auto_gwcluster_125_0  NODE READY
2022-12-21 08:24:54  10.1.3.21  auto_gwcluster_125_0  NODE ADD
2022-12-21 08:24:54  10.1.3.21  auto_gwcluster_125_0  NODE READY
2022-12-21 10:07:39  10.1.3.21  auto_gwcluster_125_0  NODE DEL
...
```

```
show ap debug sapd-cluster tun-status-history 10
```

```
ap1# show ap debug sapd-cluster tun-status-history 10

Tun Status History
----------------
Timestamp             Node IP           Status
---------             -------           ------
2022-11-21 10:38:41  10.1.3.22         UNREACHABLE
2022-11-21 10:38:45  10.1.3.22         TUN_ADD
2022-11-21 10:40:45  10.1.3.22         TUN_DOWN
2022-11-21 10:40:45  10.1.3.22         UNREACHABLE
2022-11-21 10:40:57  10.1.3.22         TUN_ADD
...
```

15. On the AP, review the current tunnel status.

```
show ata endpoint
```

```
ap1# show ata endpoint

ATA Endpoint Status
-------------------
```

```
UUID                                  IP ADDR    STATE                TUN DEV  TUN
SPI(OUT/IN)    LINK TAG  VALID TIME(s)  TUNNEL TYPE  GRE VLANs  HBT(Jiff/Missed/Sent/Rcv)
INNER IP   UP TIME(s)
----                                  -------    -----                -------  -----------
----    --------  -------------  -----------  ---------  ------------------------  ------
--   ----------
0175b356-478e-4874-9844-223d4e0350e2  10.1.3.21  SM_STATE_CONNECTING  tun0
5f199500/5caa2500  inet      129571        GRE         1,3,31,34  819370/31/6539/6313
10.1.4.50  2022-12-21 10:12:34
2dc45464-1c66-4855-a305-5b4540fa6955  10.1.3.22  SM_STATE_CONNECTED   tun1
f9c42200/26496200  inet      122901        GRE         1,3,31,34  819443/0/6849/6682
10.1.4.50  2022-12-21 08:24:54
Total Endpoints Count: 2
```

- **Question**: What is the State for the tunnel to 10.1.3.21?
- **Answer**: The AP is attempting to reach the gateway and the state is *Connecting*.

16. On the sw-agg1, review the MAC address table of VLAN 34. The LAG 5 connects to the gw1 and LAG 10 connects to gw2.

```
show mac-address-table vlan 34
```

In the example output, the client is now connected to gw2.

```
sw-agg1(config)# show mac-address-table vlan 34
MAC age-time            : 300 seconds
Number of MAC addresses : 2

MAC Address          VLAN     Type                      Port
--------------------------------------------------------------
3c:37:86:d4:91:42    34       dynamic                   lag10
b8:d4:e7:d9:ed:00    34       dynamic                   lag256
```

- **Question**: What happened with the MAC address of the wireless client?
- **Answer**: As the traffic is now tunneled to the other gateway, the aggregation switches will receive traffic from the wireless client on the LAG of the other Gateway.

About 5 minutes after the reload, the original Gateway will join the cluster again.

17. On the AP, review the bucket map until you see the bucket map with half of the IDs mapped to each gateway.

```
show overlay bucketmap status
```

Here is an example of the final bucket map status.

```
ap1# show overlay bucketmap status

Cluster auto_gwcluster_125_0 radio=0 zone=0 - Num UACs 2
-------------------------------------------------------
Index  ArrayIdx  UAC IP     Num STAs
-----  --------  ------     --------
0      0         10.1.3.21  1
1      1         10.1.3.22  0
Station List
```

```
------------
UAC Index  Station Mac        BSSID
---------  -----------        -----
0          3C:37:86:D4:91:42  F4:2E:7F:7B:15:F0
Bucket Map
----------
Bucket Idx Range  Bucket Map
----------------  ----------
[0-31]            0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[32-63]           0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[64-95]           0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[96-127]          0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[128-159]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[160-191]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[192-223]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[224-255]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-                 Standby Map
[0-31]            1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[32-63]           1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[64-95]           1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[96-127]          1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[128-159]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[160-191]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[192-223]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[224-255]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Statistics:Bmap Updates=7; UAC:Adds=2 Deletes=0; STAnswer:Adds=0 Deletes=1 moves=4 errs=0
copies=7
```

NOTE: You may see an interim version of the bucket map; check again after a few moments to see the final map.

- **Question**: What happened with the client to gateway assignment after the original gateway completed the reboot?

- **Answer**: The cluster updated the bucket map, and the client is tunneled back to the original gateway.

18. On the sw-agg1, review the VLAN 34 MAC address table.

NOTE: gw1 connects to LAG 5 and gw2 connects to LAG 10.

```
show mac-address-table vlan 34
```

Here is an example output.

```
sw-agg1(config)# show mac-address-table vlan 34
MAC age-time            : 300 seconds
Number of MAC addresses : 4

MAC Address          VLAN     Type                      Port
--------------------------------------------------------------
```

```
b8:d4:e7:d9:ed:00    34      dynamic                    lag256
3c:37:86:d4:91:42    34      dynamic                    lag5
20:4c:03:b1:d5:02    34      dynamic                    lag10
20:4c:03:b7:a2:b2    34      dynamic                    lag5
```

- **Question**: What happened with the client MAC address?
- **Answer**: The client station is tunneled back to the original gateway. The aggregation switches will see that the MAC address has moved to the original gateway LAG.

You have completed this Lab!

Lab 05.01 Deploy Tunnel Corporate WLAN

Overview

You will first explore how a AAA profile is used between the AP and the gateway to control the access to a WLAN.

You will then deploy a tunnel corporate WLAN and verify the operation with a wireless client.

The wireless client will be configured with a certificate to connect to the corporate WLAN using EAP-TLS.

In the last section you will review how AOS 10 performs distribution of the authentication keys to neighboring APs to support fast roaming.

Objectives

After completing this lab, you will be able to:

- Understand the AAA profile logic on the gateway.
- Configure an Enterprise tunnel WLAN using AOS 10.
- Verify the key roaming for a tunneled employee WLAN.

Task 1: Understanding the AAA Profile on PSK WLAN

In this task you will review the RADIUS communication between the AP and the gateway on a tunnel WLAN. In this example, a PSK tunnel WLAN will be used.

Objectives

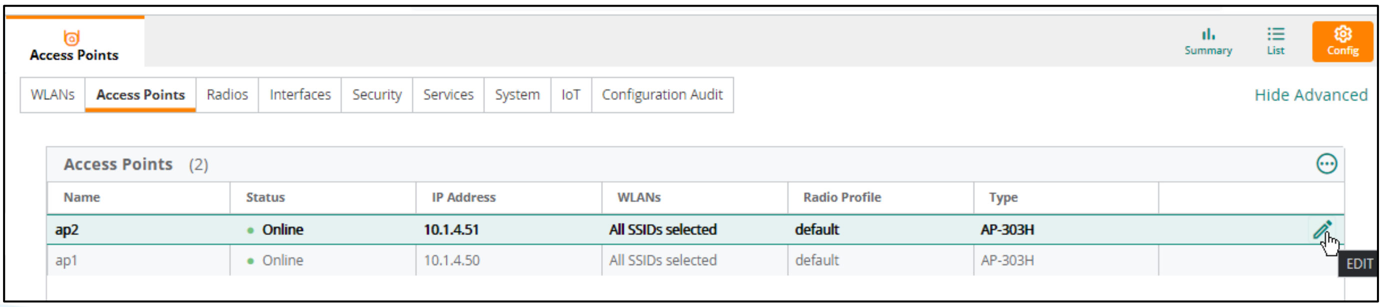
- Understand the RADIUS communication between the AP and the gateway.
- Understand the AAA profile on the gateway.

Steps

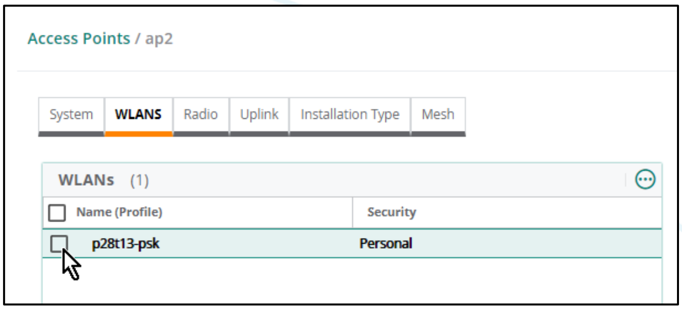
Disable the PSK WLAN on AP2

First you will disable the PSK WLAN on ap2. This makes it easier to test and troubleshoot the connection on ap1.

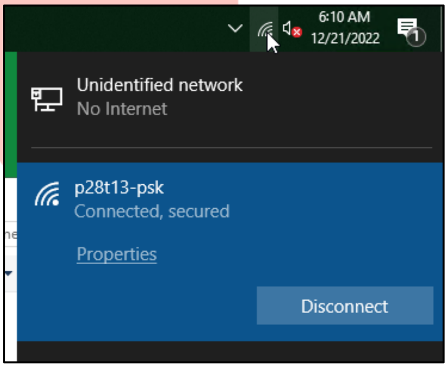
1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config (gear icon)**.
2. On the Access Points page, use the **pencil** icon to edit **ap2**.



3. Under WLANs, *uncheck* the PSK WLAN.



4. Click **Save Settings**.
5. Use the lab dashboard to open a connection to PC1.
6. Verify you are still connected to the PSK WLAN.



Review the AP Configuration for a Tunnel WLAN

You will now review the existing running configuration of the AP.

7. Use the lab dashboard to open a console connection to ap1. This AP still broadcasts the PSK WLAN.
8. Review the running-configuration.

```
show running-config
```

9. In the running-config, review the WLAN SSID-profile for the PSK WLAN.

Here is an example output:

```
wlan ssid-profile p28t13-psk
 enable
 out-of-service vpn-down disable
 index 0
 type employee
 essid p28t13-psk
 utf8
 wpa-passphrase 661a904c88604e46b787c233780c9215abc5b26982ba8fbc
 opmode wpa3-sae-aes
 gw-profile p28t13-psk_#1671553563764_37#_
 gw-auth-server default
 max-authentication-failures 0
 rf-band all
 captive-portal disable
 mac-authentication
 dtim-period 1
 broadcast-filter none
 radius-accounting
 radius-interim-accounting-interval 1
 blacklist
 dmo-channel-utilization-threshold 90
 local-probe-req-thresh 0
 max-clients-threshold 64
 dot11r
 forward-mode l2
```

- **Question**: What type of authentication do you see in the WLAN SSID-profile?
- **Answer**: mac-authentication.

- **Question**: Did you enable MAC-auth during the WLAN setup?
- **Answer**: No. This is automatically enabled when a tunnel WLAN is configured.
- **Question**: What is the authentication server?
- **Answer**: gw-auth-server default.

10. Check the running-config for a gw-auth server

```
wlan gw-auth-server default
 key
815676a258d795628c150951846bb6e9b5dc8f644373319172a4dc868fb9265b30a351b808ee74acec07b0ed7a
c70cca
 rfc3576
```

- **Question**: Did you configure this server?
- **Answer**: No. The gateway is automatically defined on the AP as a RADIUS server. All connections on the AP WLAN will be authenticated using MAC-auth to the gateway.

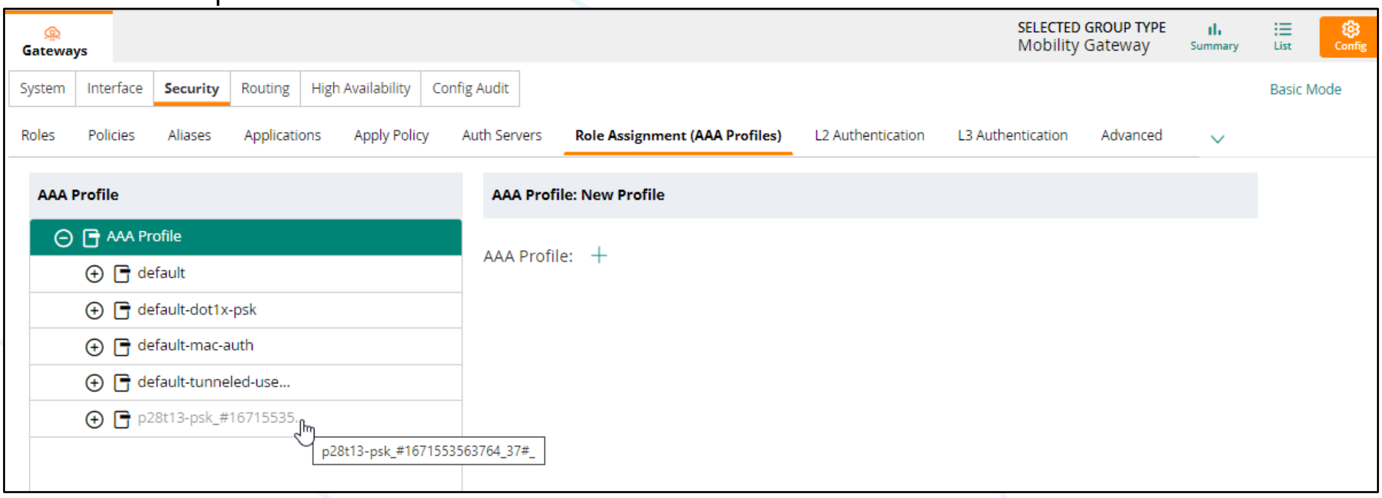
11. Take note of the gateway profile name. You will see this profile name again in the next steps.

- gateway profile name: ______________________

Review the Gateway Configuration for a Tunnel WLAN

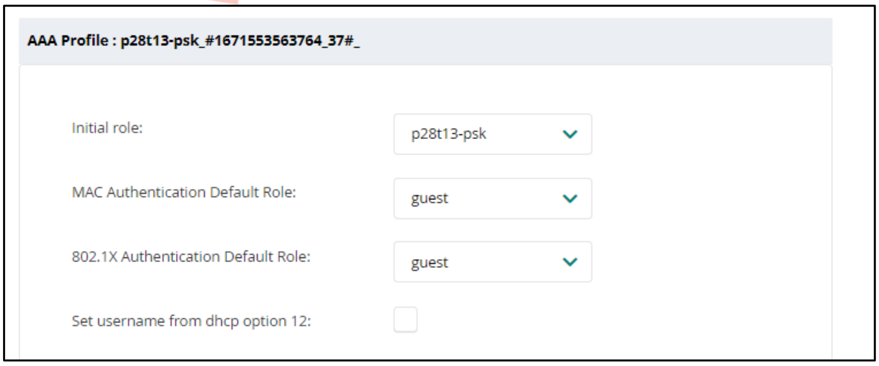
12. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config (gear icon)**.
13. Open Security > Role Assignment (AAA Profiles).
14. Expand AAA Profiles.

Here is an example screenshot:



- **Question**: Do you recognize the profile name?
- **Answer**: Yes. The AP will use RADIUS authentication requests to the gateway and include the AAA profile name in the RADIUS request in an Aruba VSA. On the gateway, this RADIUS attribute will be used for the authentication and role mapping derivation.

15. Click the **p#tx-psk** AAA profile.



- **Question**: What is the initial role on this AAA profile?
- **Answer**: The initial role is applied to any device when it initially authenticates against this AAA profile. All clients that connect on the AP WLAN will be authenticated using RADIUS to the gateway and will be assigned this initial role by default.
- **Question**: Do you need to use an external RADIUS server for this process to work?
- **Answer**: No. This process works even without external RADIUS server. Of course, it is possible to add an external RADIUS server; in that case the gateway will start to act as a RADIUS proxy. The external RADIUS server can return a different Aruba-User-Role value and override the AAA initial role assignment.

16. On the AP console, check the last 15 lines of the authentication trace buffer.

```
show ap debug auth-trace-buf 15
```

```
ap1# show ap debug auth-trace-buf 15

Auth Trace Buffer
-----------------


Nov 21 13:36:59  rad-acct-int-update   ->  78:d2:94:37:c1:61  24:62:ce:dc:2b:e0
Nov 21 13:37:59  rad-acct-int-update   ->  78:d2:94:37:c1:61  24:62:ce:dc:2b:e0
Nov 21 13:38:59  rad-acct-int-update   ->  78:d2:94:37:c1:61  24:62:ce:dc:2b:e0
Nov 21 13:39:59  rad-acct-int-update   ->  78:d2:94:37:c1:61  24:62:ce:dc:2b:e0
Nov 21 13:41:00  rad-acct-int-update   ->  78:d2:94:37:c1:61  24:62:ce:dc:2b:e0
Nov 21 13:42:00  rad-acct-int-update   ->  78:d2:94:37:c1:61  24:62:ce:dc:2b:e0
Nov 21 13:43:00  rad-acct-int-update   ->  78:d2:94:37:c1:61  24:62:ce:dc:2b:e0
Nov 21 13:44:00  rad-acct-int-update   ->  78:d2:94:37:c1:61  24:62:ce:dc:2b:e0
Nov 21 13:45:00  rad-acct-int-update   ->  78:d2:94:37:c1:61  24:62:ce:dc:2b:e0
```

- **Question**: What type of RADIUS messages do you see in the list?
- **Answer**: The AP sends RADIUS interim accounting messages for the connected client.

You will now disconnect the wireless client and review the authentication buffer on the AP.

17. Open an SSH connection to the gateway that is handling your wireless client.
18. On the gateway, use the **aaa user delete all** command to disconnect the user. This will send a RADIUS CoA message to the AP. The client will be disconnected, but it should immediately reconnect to the network.

```
aaa user delete all
```

19. On PC1, verify that you are still connected to the *p#tx-psk* WLAN. Connect to it if you are disconnected.
20. On the AP, review the auth-trace-buffer again.

```
show ap debug auth-trace-buf 15
```

```
ap1# show ap debug auth-trace-buf 15

Auth Trace Buffer
-----------------


Dec 21 11:43:35  rad-acct-int-update-> 3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:44:35  rad-acct-int-update->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:45:35  rad-acct-int-update->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:46:15  rad-acct-stop      ->  3c:37:86:d4:91:42 f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:15  rad-acct-start     ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:15  rad-acct-stop      ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:16  mac-auth-req       ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:16  mac-auth-success   <-  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:16  station-up         *  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0 - -wpa2 psk aes
Dec 21 11:46:16  wpa2-key1          <-  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:46:16  wpa2-key2          ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:46:16  wpa2-key3          <-  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:46:16  wpa2-key4          ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:46:17  rad-acct-start     ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:35  rad-acct-int-update->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
```

- **Question**: Do you see a MAC authentication request?
- **Answer**: Yes, when a station connects to the WLAN, the AP sends a MAC-auth request to the gateway. The gateway replies with a MAC-auth RADIUS success and assigns the Aruba-User-Role value to the AP.

21. Request an update of the auth-trace-buffer.

```
show ap debug auth-trace-buf 15
```

```
ap1# show ap debug auth-trace-buf 15

Auth Trace Buffer
-----------------


Dec 21 11:46:15  rad-acct-start  ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:15  rad-acct-stop   ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:16  mac-auth-req    ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:16  mac-auth-success<-  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:16  station-up      *  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0 -  - wpa2 psk aes
Dec 21 11:46:16  wpa2-key1       <-  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:46:16  wpa2-key2       ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:46:16  wpa2-key3       <-  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:46:16  wpa2-key4       ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:46:17  rad-acct-start  ->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0/__gw_10.1.3.21
Dec 21 11:46:35  rad-acct-int-update->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:47:35  rad-acct-int-update->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:48:35  rad-acct-int-update->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:49:36  rad-acct-int-update->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
Dec 21 11:50:36  rad-acct-int-update->  3c:37:86:d4:91:42  f4:2e:7f:7b:15:f0
```

- **Question**: What messages do you see after the 4 WPA2 keys?
- **Answer**: RADIUS accounting interim updates. This is how the AP informs the gateway that the wireless client is still connected. The AP will send RADIUS interim accounting packets every minute to update the gateway.

22. On the gateway, review the user table.

```
show user-table
```

```
(gw1) *# show user-table

Users
-----
    IP          MAC             Name         Role        Age(d:h:m)  Auth  VPN link
Connected To     Roaming   Essid/Bssid/Phy  Profile                          Forward mode
Type  Host Name  User Type
----------  ------------      ------       ----        ----------  ----  --------  -----
-------------  -------   ---------------  -------                          ------------  --
--  ---------  ---------
10.1.34.50  3c:37:86:d4:91:42  3c3786d49142  p28t13-psk  00:00:09
20:4c:03:8c:27:42   Wireless  p28t13-psk       p28t13-psk_#1671553563764_37#_  dtunnel
WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/2 Free:0/1 Dyn:1 AllocErr:0 FreeErr:0
```

23. On the gateway, review the user details by adding the IP address of your client.

```
show user ip 10.1.34.xyz
```

Since this command provide extensive output for the client, you can use some filters to make it easier to collect the AAA information.

NOTE: Pay attention! The filters used in the **include** lines below are *case-sensitive*!

```
show user ip 10.1.34.xyz | include AAA
```

```
(gw1) *# show user ip 10.1.34.50 | include AAA
This operation can take a while depending on number of users. Please be patient ....
Profiles AAAnswer:p28t13-psk_#1671553563764_37#_, dot1x:, mac: CP:n/a def-role:'p28t13-psk' via-auth-profile:''
```

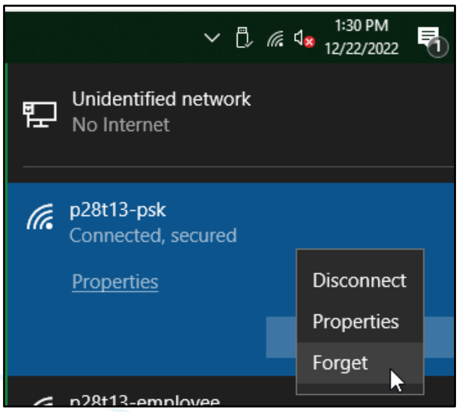
- **Question**: What is the AAA profile that was used to authenticate the client?
- **Answer**: This will be the name of the gateway profile, as included by the AP in the MAC-auth RADIUS request.

```
show user ip 10.1.34.xyz | include Role
```

```
(gw1) *# show user ip 10.1.34.50 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: p28t13-psk (how: ROLE_DERIVATION_INITIAL_ROLE), ACL: 88/0
Role Derivation: ROLE_DERIVATION_INITIAL_ROLE
```

- **Question**: What is the assigned user role?
- **Answer**: Since there is no external RADIUS server or other role derivation configuration, the client is assigned the INITIAL ROLE, this is the p#tx-psk role. This shows how the AP informs the gateway about the connected client using RADIUS access request, and how the gateway uses the AAA profile to process the authentication request and informs the AP about the result using a RADIUS access accept.

24. On PC1, **forget** the *p#tx-psk* network.



NOTE: Make sure you use the forget option, otherwise the client will automatically reconnect to this PSK WLAN in the next lab activities when a disconnect of the client would be performed.

Task 2: Configure Corporate 802.1X Tunnel WLAN

In this task you will configure a new corporate WLAN and verify the configuration deployment.

Objectives

- Configure a corporate tunnel WLAN.
- Understand the generated configuration on the AP and the gateway.

Steps

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config (gear icon)**.
2. On the WLAN page, add a new SSID.
   - name p**#**t**x**-employee

NOTE: Make sure to replace the **#** value with your pod number and **x** with your table number.

For example, if you are using table 07 in pod 28, your WLAN name would be

p28t07-employee

This represents p(od) 28 and t(able) 07.

Check with your instructor if you are not sure about the pod and table number.

---

3. Click **Next**.
4. On the VLAN page:
   - Forwarding mode **Tunnel**
   - Primary Gateway Cluster select ***your*** cluster from the list

The VLAN ID dropdown will now be populated with the VLANs from your gateway.

5. For VLAN ID, select **employee (31).**
6. Click **Next**.
7. On the Security page, move the slider to **Enterprise**.
8. Click **+** to add the primary server. A new window will show up to add the RADIUS server.
   - Name **cppm1**
   - IP Address **10.254.1.23**
   - Shared Key **Aruba123!**

9. Click **OK** to add the server. The server *cppm1* will now be selected as the primary server.

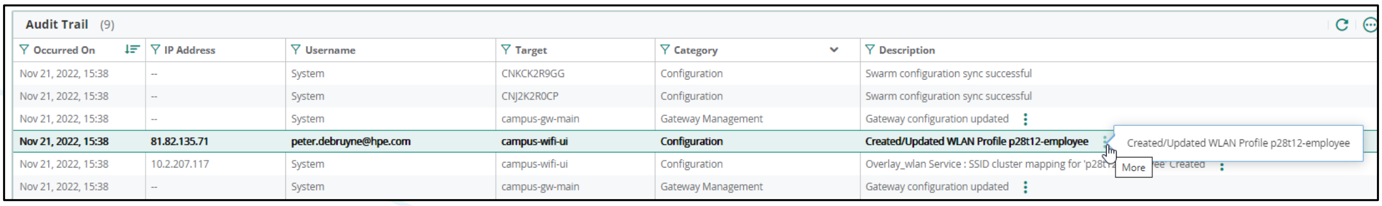
NOTE: Some browsers may automatically fill in the CPPM Username field for you (auto-fill). In that case you will see an error that a password is required in the Password field. By clearing the CPPM Username field you will be able click OK without error messages..

10. Expand Advanced Settings, expand Accounting, select Use Authentication Servers.
11. Click **Next**.
12. Under the Access page, you may leave the access as **Unrestricted**.
13. Click **Next**.
14. On the Summary page, click **Finish**.
15. Once the wizard completes, click **OK** to confirm.

Review the Generated Configuration

In the next steps you will use the audit trail to review the generated configuration.

16. In Aruba Central, navigate to the **Global** context.
17. Click **Audit Trail** to see the audit change entries.
18. Look for the entry with the description Created/Updated WLAN Profile p#tx-employee.
19. Use the **three dots** to open the details of the entry.




```
wlan access-rule p28t13-employee
 utf8
 rule any any match any any any permit
 exit
```

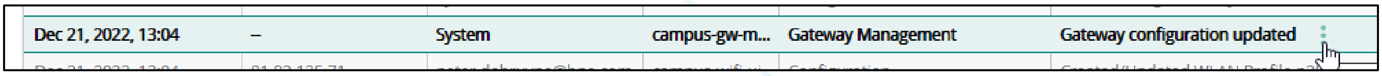
```
wlan ssid-profile p28t13-employee
 essid p28t13-employee
 opmode wpa3-aes-ccm-128
 type employee
 captive-portal disable
 dtim-period 1
 broadcast-filter none
 radius-accounting
 radius-interim-accounting-interval 1
 inactivity-timeout 1000
 max-authentication-failures 0
 blacklist
 dmo-channel-utilization-threshold 90
```

```
max-clients-threshold 64
enable
dot11r
utf8
okc
out-of-service vpn-down disable
openflow-enable
gw-profile p28t13-employee_#1671624128149_37#_
gw-auth-server default
forward-mode l2
cluster-name auto_gwcluster_125_0
cluster-group-name campus-gw-main
exit
```

- **Question**: Do you still see MAC-auth enabled on this WLAN?
- **Answer**: No. Since this WLAN uses WPA3-Enterprise (opmode wpa3-aes-ccm-128), it automatically means a RADIUS server is used for authentication.
- **Question**: What is the configured RADIUS server on the AP?
- **Answer**: The gw-auth-server with name **default** is used. There is no reference to the external RADIUS server 10.254.1.23 on the AP. The AP will use the gateway as the RADIUS server; the gateway will act as a RADIUS proxy and forward the requests to the external RADIUS server.
- **Question**: Is the gateway profile the same as the PSK WLAN?
- **Answer**: No, each WLAN profile will receive a unique gateway profile. The name is based on the original WLAN object name, the epoch timestamp and the AP group ID where the WLAN was created. This ensures that AAA profile names are always unique, and they can still be backtracked on the gateway to the original AP group based on the group ID when needed.

NOTE: You can enter the epoch time value (e.g. 1671624128149) on a time conversion website, such as https://epochtimestamp.com/ to convert the epoch time to a human-readable time. This represents the creation time of the WLAN object.

20. In the audit trail, open the details of the latest entry under *Gateway Management*.



NOTE: In the audit trail, the commands are not properly indented. To make it easier for you, the snippets below have been applied with proper indentation.

21. The details show the AAA profile configuration.

```
aaa profile p28t13-employee_#1671624128149_37#_
 no dl3-radius-proxy-mode
 no enforce-dhcp
 no l2-auth-fail-through
 no download-role
```

```
 default-vlan employee
 authentication-dot1x p28t13-employee_#1671624128149_37#_
 dot1x-default-role p28t13-employee
 dot1x-server-group p28t13-employee_#1671624128149_37#__auth_svg
 authentication-captive-portal p28t13-employee_#1671624128149_37#_
 radius-accounting p28t13-employee_#1671624128149_37#__acct_svg
 radius-interim-accounting
```

- **Question**: What is the default VLAN under the AAA profile?
- **Answer**: The default VLAN is set to the named VLAN employee. This is based on the default VLAN you have set during the WLAN wizard.
- **Question**: What is the dot1x-default-role set to?
- **Answer**: All clients that successfully authenticate will by default be assigned the 802.1X Authentication default role. This can be overruled by the RADIUS server or other rules, but this is the authentication default role.

22. Scroll down to the end to see the RADIUS server definition.

```
...

aaa authentication-server radius cppm1
 no enable-radsec
 no service-type-framed-user
 no nas-ip
 no nas-identifier
 no radsec-port
 host 10.254.1.23
 key 8ff5f219cec07a2861375dc01addde1e7e1ea909d0ccc9fc
 authport 1812
 retransmit 3
 timeout 5
```

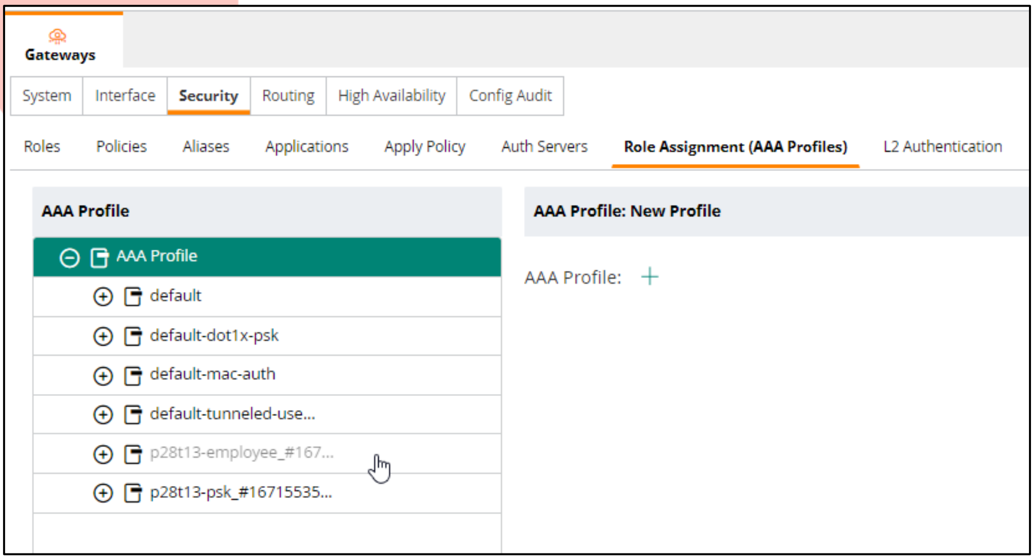
- **Question**: Does this mean that only the gateway will be able to contact the RADIUS server?
- **Answer**: Yes, in a tunnel or mixed mode WLAN, the AP will always use the gateway as the authentication server. The gateway will forward the authentication requests to the external RADIUS server, as it acts as the RADIUS proxy.
- **Question**: What would happen when the gateway fails? Will the AP be able to contact the external RADIUS server?
- **Answer**: No. The AP will always require a gateway for a tunnel or mixed WLAN authentication. Therefore, a cluster of gateways is recommended to provide redundancy.

Review the Gateway AAA Profile Settings in the UI

In the next steps, you will review the generated AAA profile in the Central UI.

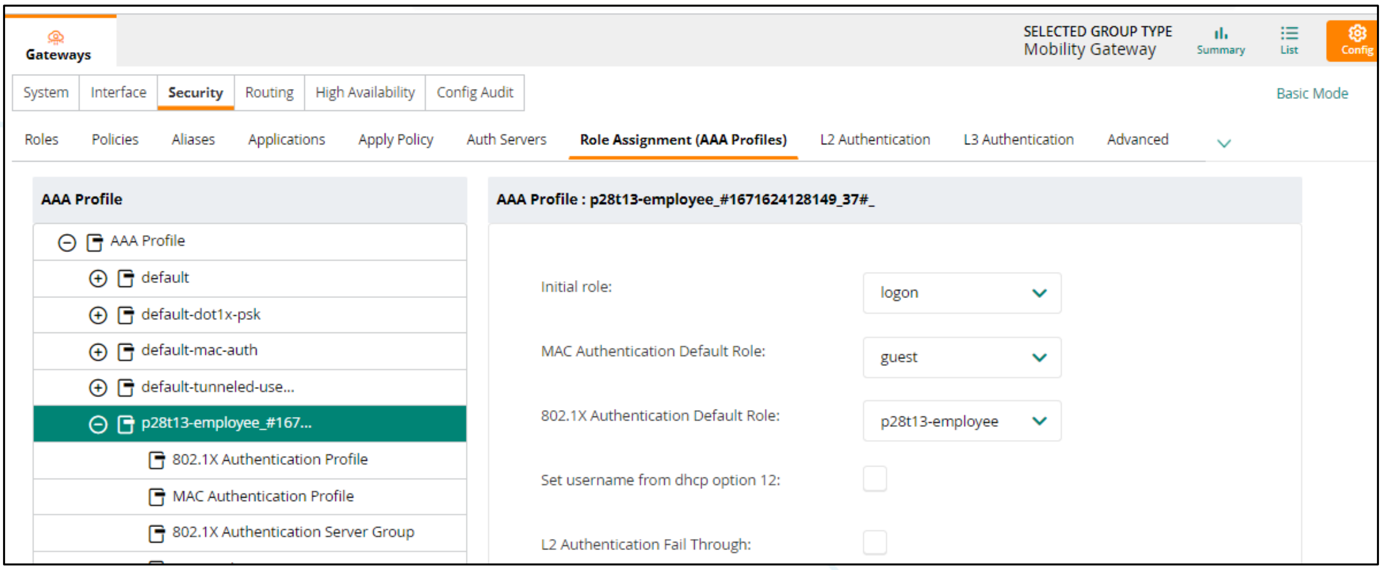
23. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config (gear icon)**.
24. Click Security > Role Assignment (AAA Profiles).

25. Expand the **AAA Profile**.



- **Question**: Do you see a new AAA Profile?
- **Answer**: Yes, there is a new profile for p#tx-employee. The name matches the gateway profile name you have seen in the AP WLAN configuration.

26. Expand the AAA profile **p#tx-employee**.



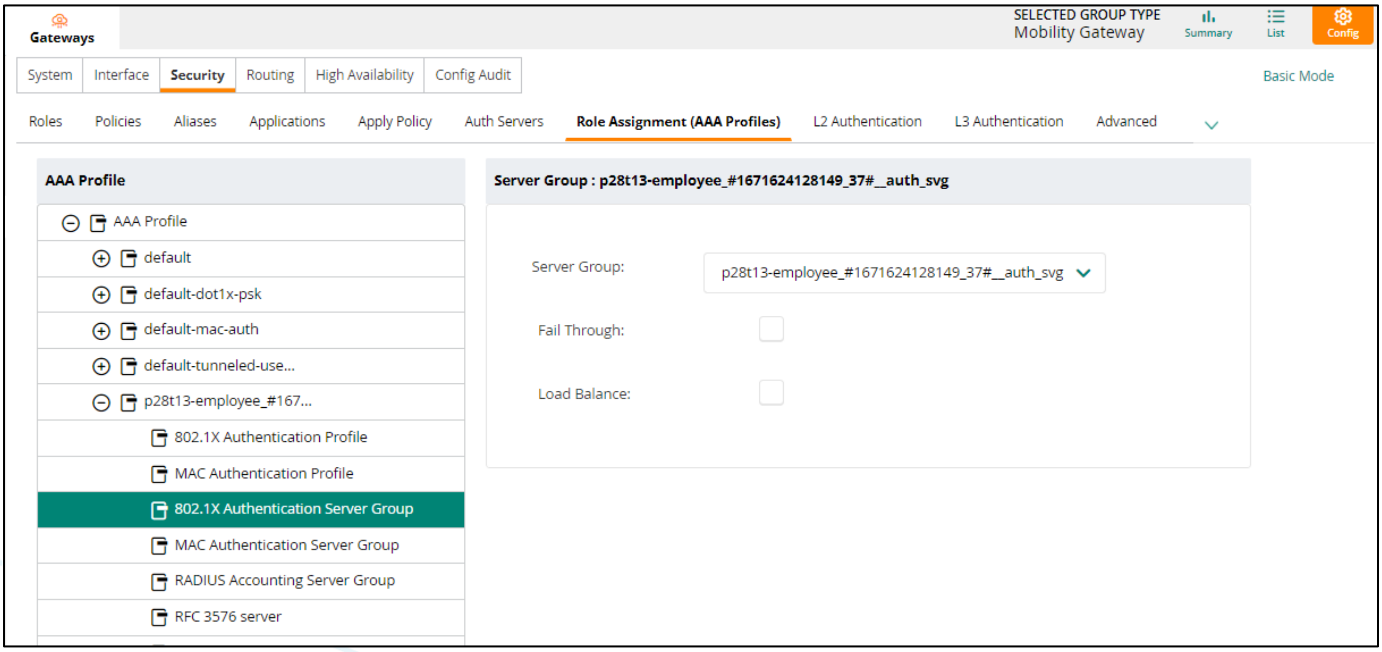
- **Question**: What is the initial role for this AAA profile?
- **Answer**: The initial role is *logon*.
- **Question**: Isn't this the wrong role? Shouldn't authenticated clients receive the role based on the WLAN name, in this example p#tx-employee?

- **Answer**: While it is true that all connecting clients will initially get the logon role, they must complete 802.1X authentication to access the network.
  - **1**: Without successful 802.1X authentication, there are no WPA keys exchanged, and the client cannot access the network.
  - **2**: With a successful 802.1X authentication, the AAA profile will assign the authentication default role, in this example this is the 802.1X authentication default role.

- **Question**: What role is set as the 802.1X authentication default role?

- **Answer**: The default role of the WLAN: p#tx-employee.

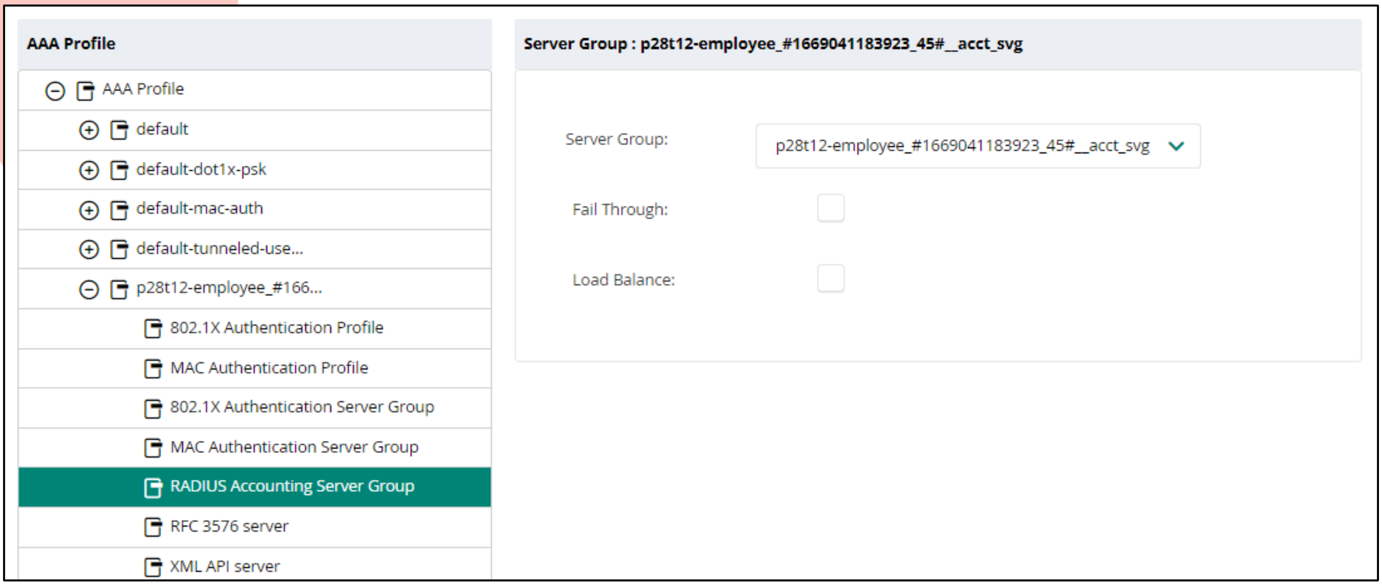
27. Click 802.1X Authentication Server Group.



- **Question**: What is the configured authentication server group?

- **Answer**: The WLAN wizard has automatically created a new authentication server group (auth_svg) on the gateway, based on the same unique profile ID (epoch time and group ID).

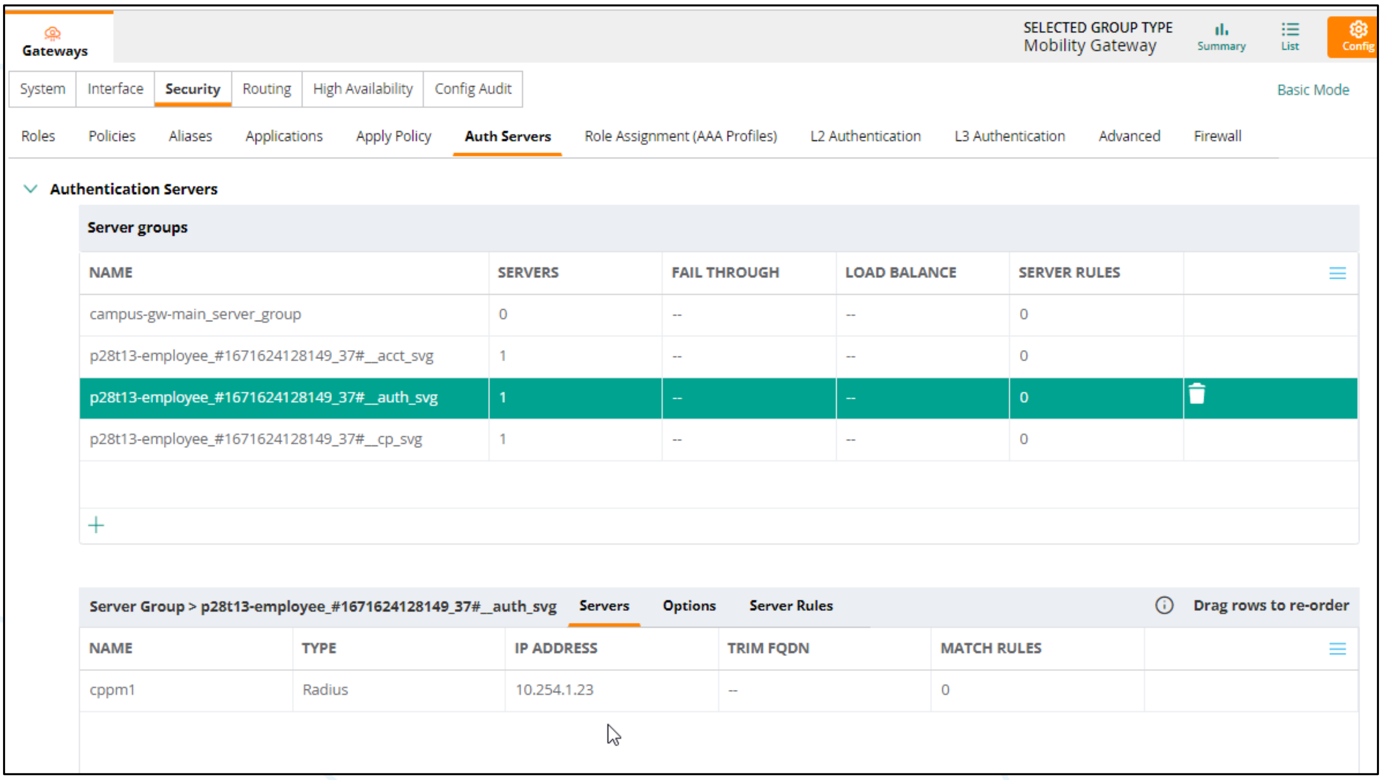
28. Click RADIUS Accounting Server Group.



- **Question**: What is the configured accounting server group?
- **Answer**: Just like the authentication server group, the WLAN wizard has automatically created an accounting (acct_svg) server group based on the same unique profile ID.

Now you will explore the authentication server group.

29. Click Security > Auth Servers.
30. Click the **p#tx-employee….auth_svg** (Authentication Server Group)



- **Question**: What is this group used for?
- **Answer**: Any MAC-auth or 802.1X authentication requests in the AAA profile are sent to this generated authentication server group.
- **Question**: What server is assigned to this server group?
- **Answer**: The RADIUS cppm1 server belongs to this group. This is the server you have created during the WLAN wizard. Since you have selected to create a tunnel WLAN, the wizard has created the RADIUS server on the gateway group. In case you would have added a primary and secondary RADIUS server, they would both be listed, in the correct order, in this list.

Task 3: Connect with a WLAN Client

In this task you will test the corporate 802.1X WLAN connection with your PC1 client.

In the lab environment, EAP-TLS will be used for the client authentication.

Before you can make the connection, you will need to install a certificate on the client.

You will enroll for a new certificate using ClearPass Onboard.

ClearPass has been preconfigured for you.

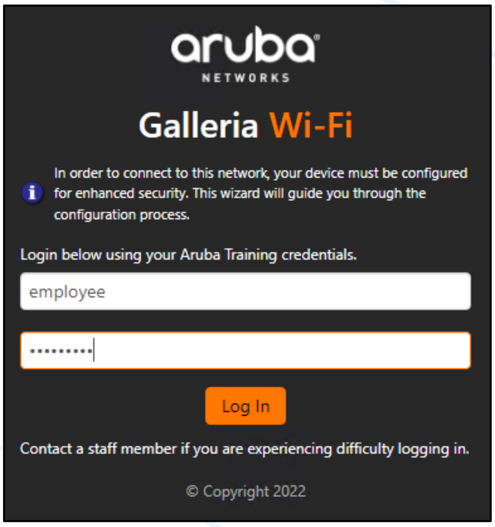
Objectives

- Verify the tunnel WLAN operation.
- Install a certificate on the client system.

Steps

Install the Client Certificate

1. On PC1 and make sure you are connected to the **p#tx-psk** WLAN. This WLAN provides access the ClearPass server in your lab.
2. On PC1, open a browser, such as Google Chrome, and navigate to:
   - **https://10.254.1.23/onboard/cert-iaca.php**
3. Accept the certificate warning and continue. (**Advanced > Proceed**).
4. You should be presented with the Onboard Portal page. Enter the employee credentials.
   - Username **employee**
   - Password **Aruba123!**



5. Click **Login**.

6. Click **Start QuickConnect.** This will download the Aruba QuickConnect application.

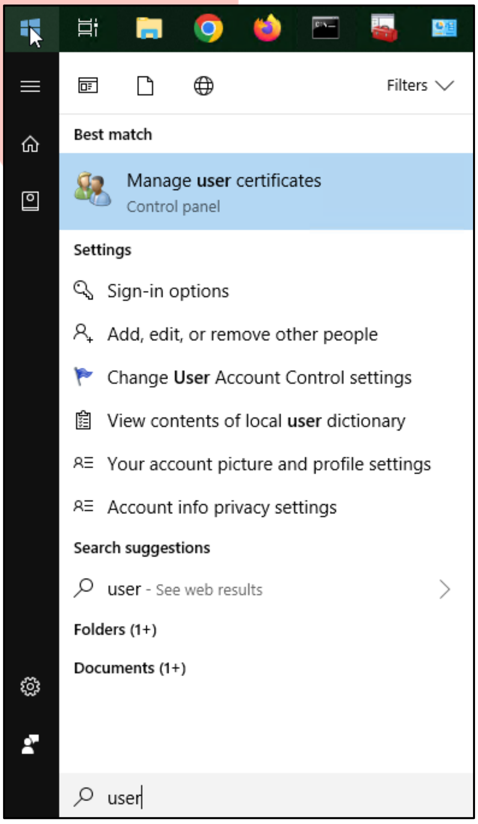
7. Wait for the download to complete.
8. In the downloads, click the **QuickConnect** app.

9. Microsoft Windows will prompt you to search the App Store, click **No**.
10. Click **Yes** for the administrator prompt.
11. You will now be presented with the ClearPass Onboard Wizard.
12. Click **Next**.
13. Accept any warning messages about certificate installations if applicable.
14. Click **Finish** to complete the wizard.

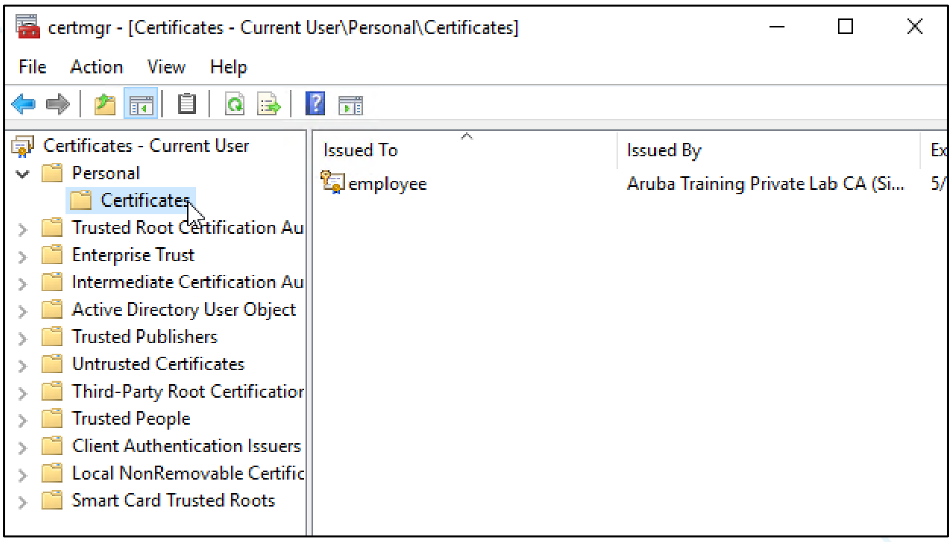
NOTE: The onboard wizard in this lab is only intended to deploy a certificate. A dummy WLAN client profile will be created *training-network-dummy*: this can be ignored.

Verify the Installation of the Client Certificate

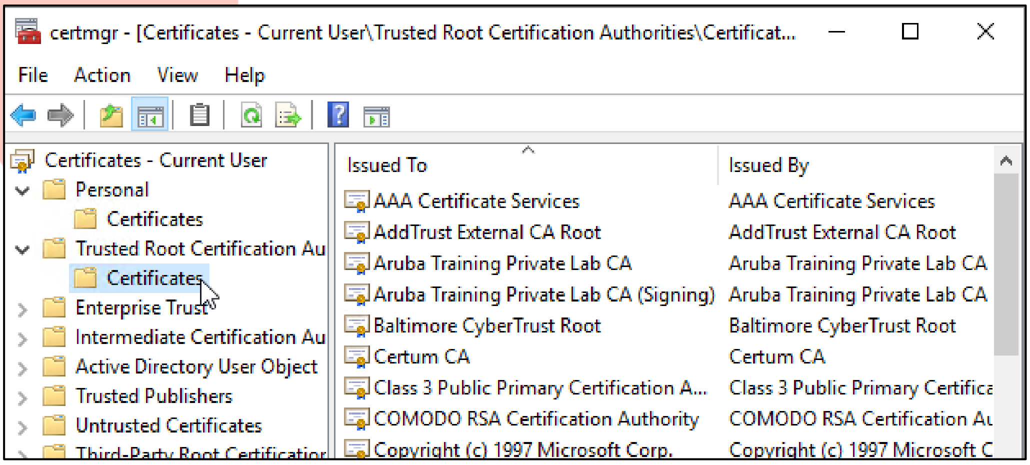
15. On PC1, click the **Start** button and type **user**.



16. In the list of options, click **Manage User Certificates**. This will open the User Certificate store manager.
17. Expand **Personal > Certificates**. You should see the employee certificate.



18. Expand Trusted Root Certificate Authorities > Certificates.



- **Question**: Do you see the **Aruba Training Private Lab CA** in the list?

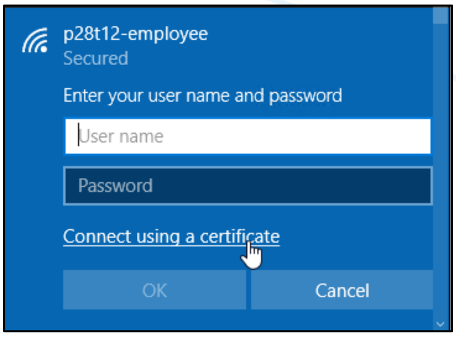
- **Answer**: Yes, the ClearPass Onboard tool has automatically updated the client Root Certificates.

NOTE: You may see the certificates two times in the list since the lab PC were preconfigured with these lab certificates.

19. Close the client certificate manager window.

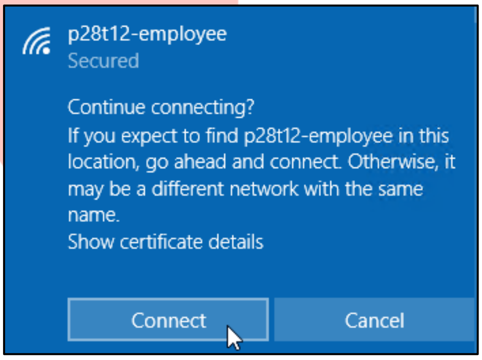
Connect the Client to the Employee WLAN

20. Disconnect from the PSK WLAN.
21. Connect to your **p#tx-employee** WLAN.
22. When prompted, click Connect using a certificate.

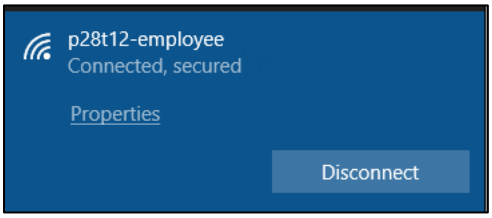


NOTE: If you do not see the *Connect using a certificate* option, the time of the PC1 may be different from the CPPM time. In this case, it is possible that the installed certificate is not yet valid from the client time perspective. Verify the time on the PC1 or adjust it to 1 day in the past/future.

23. Click **Connect** to confirm the RADIUS EAP Certificate on this location.

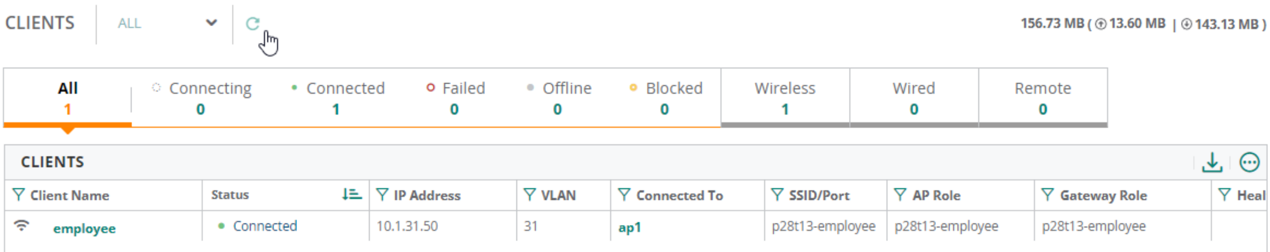


24. The client should now be connected to the employee WLAN.



Verify the Client Status in Aruba Central

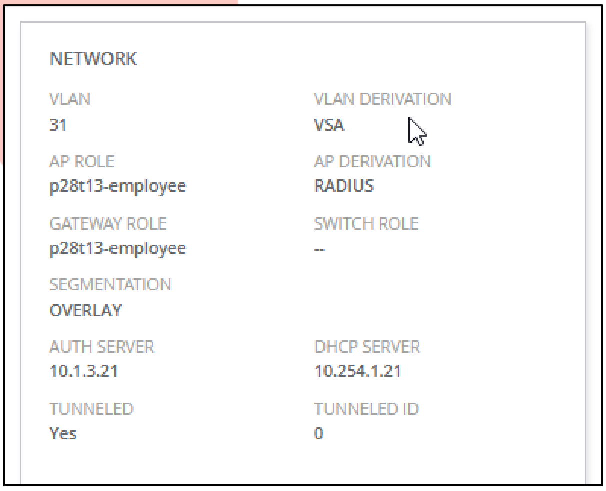
25. In Aruba Central, navigate to the group **campus-wifi-ui** > **Clients**.



NOTE: It may take a minute for the client to appear with the updated client name and IP address. Use the refresh button to see the latest client list.

- **Question**: What is the IP address and VLAN assignment for the client?
- **Answer**: You have configured the default WLAN VLAN as employee (31). The client is assigned to this VLAN.

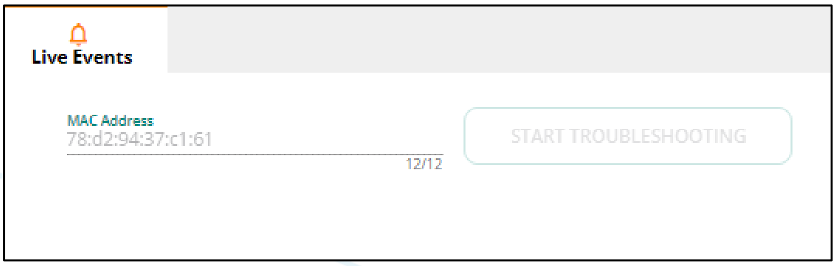
26. Click your *client name* to access the client details page.



- **Question**: What is the VLAN derivation method?
- **Answer**: VSA. This is based on the Aruba-User-Vlan VSA. The gateway will include this attribute as part of the RADIUS access accept to the AP.

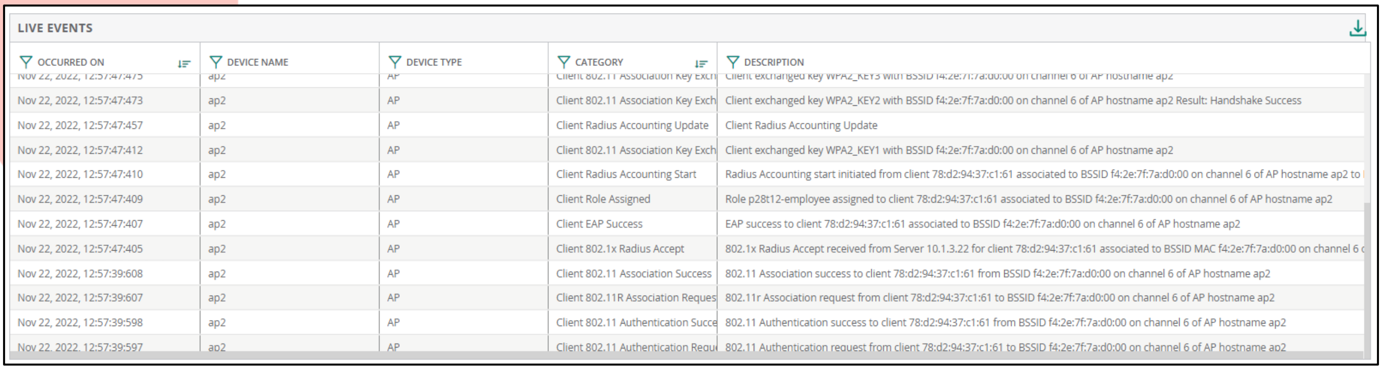
Review Live Events for the Client Connection

27. While on the client details page, navigate to **Live Events**. Aruba Central will now receive a live feed of events about the client MAC address.



NOTE: The Live Events troubleshooting will start automatically when you access this page.

28. On the PC1, disconnect from the WLAN and reconnect. You should see a list of live events passing on the screen.
29. Click **Stop Troubleshooting** once the client is connected.
30. Here is an example of the Live Events:



LIVE EVENTS

OCCURRED ON	DEVICE NAME	DEVICE TYPE	CATEGORY	DESCRIPTION
Nov 22, 2022, 12:57:47:475	ap2	AP	Client 802.11 Association Key Exch	Client exchanged key WPA2_KEY3 with BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2
Nov 22, 2022, 12:57:47:473	ap2	AP	Client 802.11 Association Key Exch	Client exchanged key WPA2_KEY2 with BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2 Result: Handshake Success
Nov 22, 2022, 12:57:47:457	ap2	AP	Client Radius Accounting Update	Client Radius Accounting Update
Nov 22, 2022, 12:57:47:412	ap2	AP	Client 802.11 Association Key Exch	Client exchanged key WPA2_KEY1 with BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2
Nov 22, 2022, 12:57:47:410	ap2	AP	Client Radius Accounting Start	Radius Accounting start initiated from client 78:d2:94:37:c1:61 associated to BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2 to
Nov 22, 2022, 12:57:47:409	ap2	AP	Client Role Assigned	Role p28t12-employee assigned to client 78:d2:94:37:c1:61 associated to BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2
Nov 22, 2022, 12:57:47:407	ap2	AP	Client EAP Success	EAP success to client 78:d2:94:37:c1:61 associated to BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2
Nov 22, 2022, 12:57:47:405	ap2	AP	Client 802.1x Radius Accept	802.1x Radius Accept received from Server 10.1.3.22 for client 78:d2:94:37:c1:61 associated to BSSID MAC f4:2e:7f:7a:d0:00 on channel 6 c
Nov 22, 2022, 12:57:39:608	ap2	AP	Client 802.11 Association Success	802.11 Association success to client 78:d2:94:37:c1:61 from BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2
Nov 22, 2022, 12:57:39:607	ap2	AP	Client 802.11R Association Reques	802.11r Association request from client 78:d2:94:37:c1:61 to BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2
Nov 22, 2022, 12:57:39:598	ap2	AP	Client 802.11 Authentication Succe	802.11 Authentication success to client 78:d2:94:37:c1:61 from BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2
Nov 22, 2022, 12:57:39:597	ap2	AP	Client 802.11 Authentication Requ	802.11 Authentication request from client 78:d2:94:37:c1:61 to BSSID f4:2e:7f:7a:d0:00 on channel 6 of AP hostname ap2

- **Question**: Do you see the authentication and association phases of the connecting client?
- **Answer**: Yes, each phase is shown in the event list.

Task 4: Monitoring and Roaming Key Distribution

In this task you will review how key client information is shared between APs to facilitate a smooth roaming experience.

Currently only AP1 is configured with the employee WLAN, you will enable AP2 for this WLAN as well.

Next you will review that key client information is shared between neighboring APs.

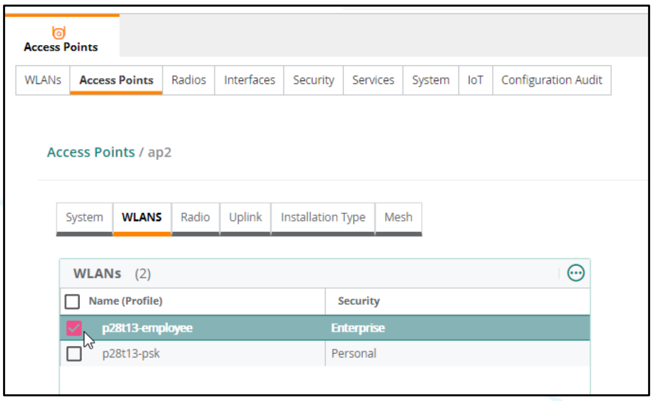
Objectives

- Understand the client key distribution process.
- Review the distributed keys on the APs.

Steps

Enable Employee WLAN on AP2

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config (gear icon)**.
2. On the Access Points page, use the **pencil** icon to edit **ap2**.
3. On the WLANs page, enable the **p#tx-employee** WLAN.



4. Click **Save Settings**.

Review AP DTLS and PMKCache

5. Use the lab dashboard to open a console connection to both AP1 and AP2.
6. On AP1, review the current client list. Make sure PC1 is connected using the *employee* role.

```
show clients
```

```
ap1# show clients

Client List
-----------
Name      IP Address  MAC Address       OS      ESSID            Access Point  Channel
Type  Role             IPv6 Address              Signal     Speed (mbps)
```

```
----     ----------  -----------      --     -----         ------------  -------  -
---  ----            ------------            ------    ------------
employee  10.1.31.50  3c:37:86:d4:91:42  Win 10  p28t13-employee  ap1          11
GN    p28t13-employee  fe80::f56c:996b:bcc7:fb18  44(good)  144(good)
Number of Clients   :1
Info timestamp      :831568
```

7. On AP1, review the PMK Cache information.

```
show ap pmkcache
```

```
ap1# show ap pmkcache

PMK Cache Table
---------------
Client MAC          Key                         OKC/11r  Expiry      Role              VLAN
ESSID             ualg/malg  R1Key List (BSSID : R1name : R1Key)  Seqno  IP
----------          ---                         -------  ------      ----              ----
-----             ---------  -----------------------------------  -----  --
3c:37:86:d4:91:42  (6): 07 ff 63 34 56 77 ...  11r      7h:55m:22s  p28t13-employee  31
p28t13-employee  64 64                                            45809  10.1.31.50
PMK Cache Count:1
```

- **Question**: What information is stored in the pmkcache?
- **Answer**: The PMK key, whether the client supports OKC or 802.11r, the key expiration time, the user role and VLAN, the ESSID information, and the client IP address.

AP DTLS Neighbors

DTLS provides TLS security for datagram (UDP) exchange. The APs can use their built-in factory certificate to establish secure DTLS based sessions with each other to share information.

Aruba Central will provide each AP a list of neighbor AP MAC addresses. This list will be used by the AP to verify that the subject of the certificate used in the DTLS session setup appears in this list.

8. On AP1, review the APs that are allowed to establish a DTLS session with the local AP.

```
show ap dtls allowed-aps
```

```
ap1# show ap dtls allowed-aps

DTLS Allowed APs
----------------
AP Serial   MAC Address        IP Address
---------   -----------        ----------
CNHSK2R4KP  20:4c:03:5b:27:e2  10.1.4.51
```

- **Question**: How does the AP learns from what other APs a connection could be expected?
- **Answer**: In Aruba Central, the AirMatch service stores information about the surrounding APs and this neighbor information (the base MAC and IP addresses) is shared with the individual APs.

9. On AP1, review the currently active DTLS sessions.

```
show ap dtls provisioned-neighlist
```

Here is an example output.

```
ap1# show ap dtls provisioned-neighlist

AP Neighbour list
-----------------
AP Serial   MAC Address        IP Address  Conn Status
---------   -----------        ----------  -----------
CNHSK2R4KP  20:4c:03:5b:27:e2  10.1.4.51   Connected
```

Take note of the IP address of the neighbor I: in the example this is 10.1.4.51.

10. You can also find the DTLS session in the AP firewall session table. Use the neighbor AP IP Address for the **include** filter.

```
show datapath session | include 10.1.4.xyz
```

```
ap1# show datapath session | include 10.1.4.51
10.1.4.50         10.1.4.51       17    4434  4434  0    0    0   0    dev8        26a  12
d92   F
10.1.4.51         10.1.4.50       17    4434  4434  0    0    0   0    dev8        26a  12
d92   FC
```

11. On AP2, verify that it AP1 is in the allow list and it also has the active DTLS session to AP1.

```
show ap dtls allowed-aps
show ap dtls provisioned-neighlist
```

```
ap2# show ap dtls allowed-aps

DTLS Allowed APs
----------------
AP Serial   MAC Address        IP Address
---------   -----------        ----------
CNJ2K2R0YR  20:4c:03:8c:27:42  10.1.4.50
```

```
ap2# show ap dtls provisioned-neighlist

AP Neighbour list
-----------------
AP Serial   MAC Address        IP Address  Conn Status
---------   -----------        ----------  -----------
CNJ2K2R0YR  20:4c:03:8c:27:42  10.1.4.50   Connected
```

Verify the PMK Cache on AP2

12. On AP2, review the client list. This is expected to be empty since the client connected to AP1 while AP2 was still offline for this WLAN.

NOTE: Sometimes the lab wireless client may get disconnected from the WLAN. You may have to manually reconnect to the wireless network if the client was disconnected.

NOTE: If you manually reconnect, the client may connect to AP2 instead of the AP1. If that happens in your lab, just inverse the AP1/AP2 instructions in the next steps.

```
show client
```

```
ap2# show client

Client List
-----------
Name  IP Address  MAC Address  OS  ESSID  Access Point  Channel  Type  Role  IPv6 Address
Signal  Speed (mbps)
----  ----------  -----------  --  -----  ------------  -------  ----  ----  ------------
------  ------------
Number of Clients   :0
Info timestamp      :102471
```

13. On AP2, review the PMK Cache.

```
show ap pmkcache
```

```
ap2# show ap pmkcache

PMK Cache Table
---------------
Client MAC         Key                         OKC/11r  Expiry      Role             VLAN
ESSID            ualg/malg  R1Key List (BSSID : R1name : R1Key)
Seqno  IP
----------         ---                         -------  ------      ----             ----
3c:37:86:d4:91:42  (6): 07 ff 63 34 56 77 ...  11r      7h:56m:32s  p28t13-employee  31
p28t13-employee  64 64      (6): f4 2e 7f 7b 15 f1  : (6): c0 d3 f9 a5 e7 e9  : (6): 7b d9
a6 f5 34 48  ;(6): f4 2e 7f 7b 15 e1  : (6): f3 4f 33 ea 9b 60  : (6): 6b 20 5b 33 3d f3
45809  0.0.0.0
PMK Cache Count:1
```

NOTE: If you don't see the entry in the PMK Cache yet, you might need to reconnect the PC1 client to the WLAN. AP2 was only recently enabled for the employee WLAN.

- **Question**: Do you see any records?
- **Answer**: Yes, AP2 is a neighbor AP of AP1 and has received the PMK information.
- **Question**: Does the key match the key on the AP1 output?

- **Answer**: Yes, the same key information is shared between the APs as part of the cache.

14. On AP1, you can review the PMK Synchronization Statistics.

```
ap1# show ap debug pmk-sync-statistics
```

```
ap1# show ap debug pmk-sync-statistics

STM Module Roaming PMK Sync Stats
---------------------------------
Description                             Value
-----------                             -----
PMK update to central                   5
PMK update to central fail              2
PMK update from central                 3
PMK update from central fail            0
PMK delete from central count           0
PMK key deleted event sent to central   0
PMK Key found in DT cache               0
PMK Key not found DT in cache           0
PMK Key found in R1 lcoal cache         0

STM module Neighbor update Stats
--------------------------------
Description                             Value
-----------                             -----
Neighbor update to central              0
Neighbor update to central fail         0

STM module FT/11r Authentication Stats
--------------------------------------
Description                             Value
-----------                             -----
FT Auth Requests pkt Count              0
FT Auth Success Responses Count         0
FT Auth Error R0KHUNREACHABLE Count     0
FT Auth Error invalid MDID IE           0
FT Auth Error MDID mismatch Count       0
FT Auth Error Invalid FT IE Count       0
FT Auth Error Invalid RSN IE Count      0
FT Auth Failed Count                    0

STM module OKC Authentication Stats
-----------------------------------
Description                             Value
-----------                             -----
OKC Auth Requests pkt Count             5
OKC Auth Success Responses Count        0
OKC Auth Failed Count                   0
OKC Key found in DT cache               3
OKC Key not found DT in cache           2

STM module PMK keycache latency Stats
-------------------------------------
Description      Value
```

```
-----------       -----
Maximum latency   2457
Median latency    835
Average latency   931


CLI module Encryption key Stats
-------------------------------
Description                                  Value
-----------                                  -----
Enc key req to central                       1
Enc key req to central fail                  0
Enc key resp from central                    1
Enc key resp from central invalid            0

CLI module Neighbor update Stats
--------------------------------
Description                                  Value
-----------                                  -----
Send neighbor update to central              0
Send neighbor update to central fail         0
```

15. And the PMK mobility statistics when stations have roamed. Note that none of the clients in the lab environment have roamed.

```
show ap debug pmk-mobility-statistics
```

```
ap1# show ap debug pmk-mobility-statistics

 STM Module Mobility debug Stats
--------------------------------
Description                              Value
-----------                              -----
Mobility session req sent                0
Mobility session req sent failed         0
Mobility session resp timeout            0
Mobility session clfl resp timeout       0

CLI module STA move and MOB session debug Stats
-----------------------------------------------
Description                                  Value
-----------                                  -----
STA Move req sent to ngbr AP                 4
STA Move req sending failed to ngbr AP       0
STA Move resp sent to ngbr AP                1
STA Move resp sending failed to ngbr AP      0
STA Move Cloud Fallback response timeout     0
STA Move request retries                     3
STA Move response received                   0
MOB Session response received                1
STA Move Cloud Fallback req to cloud         0
MOB Session Cloud Fallback req to cloud      0
```

You have completed this Lab!

Lab 05.02 Roles and Access Control

Overview

In this lab you will explore network access control options.

You will start the lab with the configuration of user roles and review the client role derivation process of the AAA profile.

Next you will see that the user role can also be assigned using the RADIUS VSA attribute Aruba-User-Role.

After you have seen how the role can be assigned, you will configure differentiated access controls for the employee and contractor user roles.

These configurations will be reviewed in the AP and the gateway configurations. You will also configure a role directly in the gateway configuration.

The next section of the lab will show how dynamic authorization (CoA or RFC3576) can be configured and used on the gateways.

In the last section, you will see how a custom server derivation rule can be configured to map a standard RADIUS attribute to a user role on the AOS 10 solution.

Objectives

After completing this lab, you will be able to:

- Understand the role assignment of a AAA profile.
- Configure new user roles on the AP and gateway.
- Configure access control using an Aruba user role.
- Configure dynamic authorization (CoA).
- Create custom server derivation rules for user role assignments.

Task 1: User Role Derivation

In this task you will review the user role derivation process that is performed by the gateway. Based on the AAA profile configuration, the GW will first assign the initial role.

When a form of authentication is used, such as 802.1X or MAC authentication, and this authentication is successful, the client will be assigned the authentication *default* role.

This Authentication default role can be overruled by a server-assigned (or server-derived) role, such as the RADIUS assigned Aruba-User-Role VSA.

Objectives

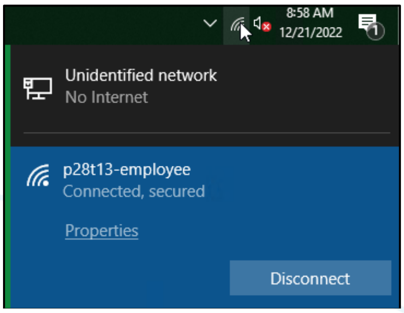
- Understand the default authentication role in the AAA profile.
- Understand how roles can be assigned using the RADIUS Aruba-User-Role VSA.

Steps

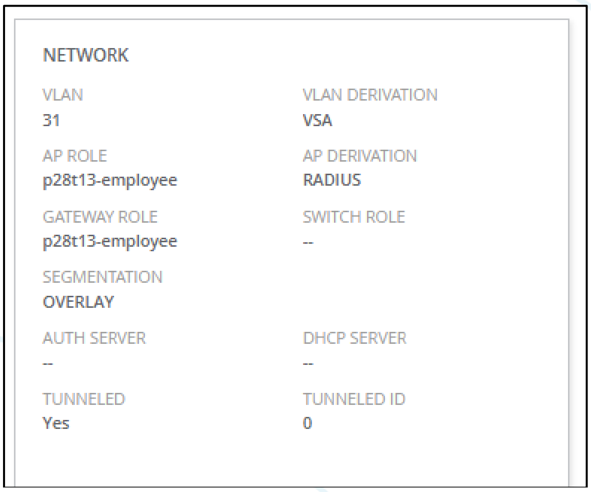
Review the Default Authentication Role

Your PC1 is connected as employee to the employee WLAN. You will first review the currently assigned role and how it was assigned.

1. On PC1, verify you are still connected to the **p#tx-employee** WLAN.



2. In Aruba Central, open the client details page for your client. Check the *NETWORK* tile on the details page.

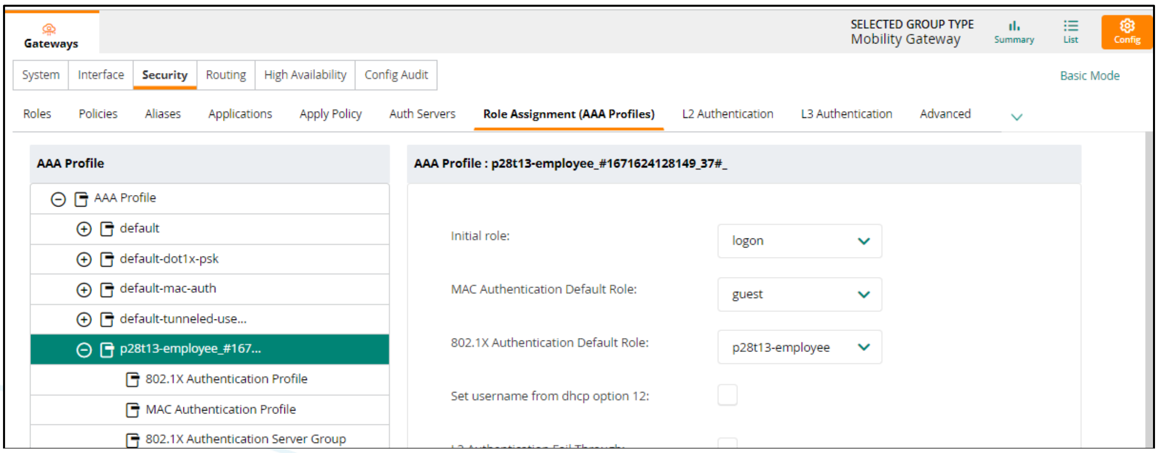


NOTE: It may take a minute for the details of both AP and GW to be present. This is because both AP and GW update Aruba Central independent of each other with their client authentication details. You may use the refresh button to get the latest status.

- **Question**: What is the AP role and the gateway role for the client?
- **Answer**: The client is assigned the role p#tx-employee on both the AP and the GW.

Review the AAA Profile on the GW

3. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config (gear icon)**.
4. Navigate to **Security > Role Assignment (AAA Profiles)**.
5. Expand the AAA profile for **p#tx-employee-#...#**.



- **Question**: What is the 802.1X authentication default role?
- **Answer**: This role is created by default based on the WLAN object name. Any device that successfully authenticates using 802.1X will be assigned this role. This assignment can be overruled by server rules or RADIUS based Aruba-User-Role attribute.

Review the Current Client Role Derivation

6. Use the MGMT PC to open an SSH session to the gateway that is used by the wireless client.
7. Review the user table and check the client details using the client IP address.

```
show user-table
```

```
(gw1) *# show user-table
Users
```

```
    IP          MAC            Name      Role            Age(d:h:m)  Auth    VPN
link     Connected To     Roaming   Essid/Bssid/Phy  Profile
Forward mode  Type  Host Name  User Type
----------  ------------      ------    ----            ----------  ----    -------
-  ------------------  -------   ---------------  -------
------------  ----  ---------  ---------
10.1.31.50  3c:37:86:d4:91:42  employee  p28t13-employee  00:00:37    802.1x
20:4c:03:8c:27:42   Wireless  p28t13-employee  p28t13-employee_#1671624128149_37#_
dtunnel                       WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/4 Free:0/3 Dyn:1 AllocErr:0 FreeErr:0
```

- **Question**: What is the assigned role for the client?
- **Answer**: The client is assigned the default 802.1X authentication role.

8. Review the client details based on the client IP; you can filter using the **Role** string.

```
show user ip 10.1.31.xyz | include Role
```

```
(gw1) *# show user ip 10.1.31.50 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: p28t13-employee (how: ROLE_DERIVATION_DOT1X), ACL: 92/0
Role Derivation: ROLE_DERIVATION_DOT1X
```

Server Assigned Role

In the next steps you will see how a server assigned role is applied.

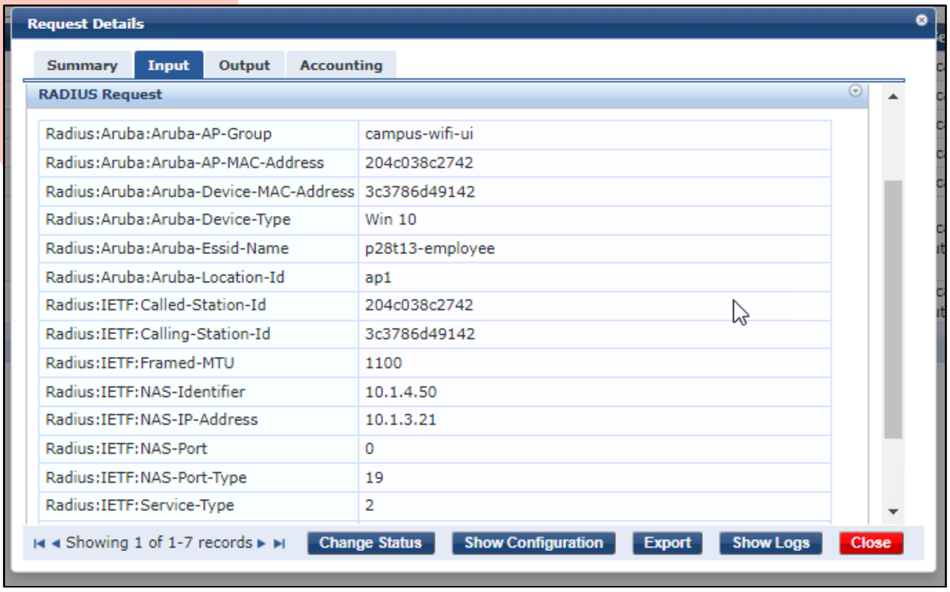
9. Use the MGMT PC to open a connection to ClearPass, login with admin / Aruba123!

```
https://10.254.1.23/tips
```

10. Navigate to **Monitoring > Live Monitoring > Access Tracker**.
11. Review the latest entry for **employee** user.

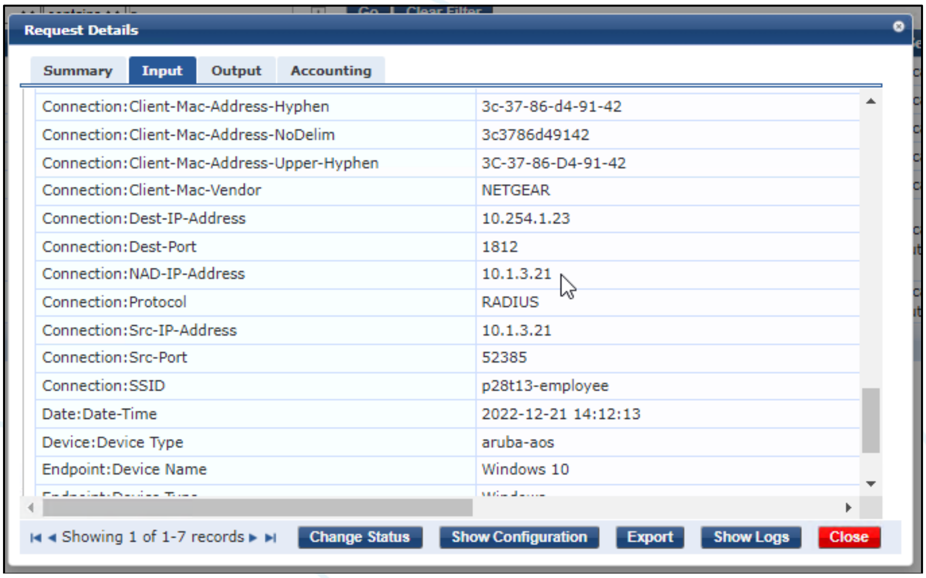
#	Server Name	Source	NAS IP Address	NAS Port	Host MAC Addres	Username	Service	Login Status	Request Timestar	Enforcement Pro
1.	P58-T01-CPPM	RADIUS	10.1.3.22	0	78-D2-94-37-C1-61	employee	acap - wireless - dot1x	ACCEPT	2022/11/21 14:37:17	aruba-role-employee

12. Click the entry to open it.
13. Click the **Input** tab. Expand RADIUS Request.



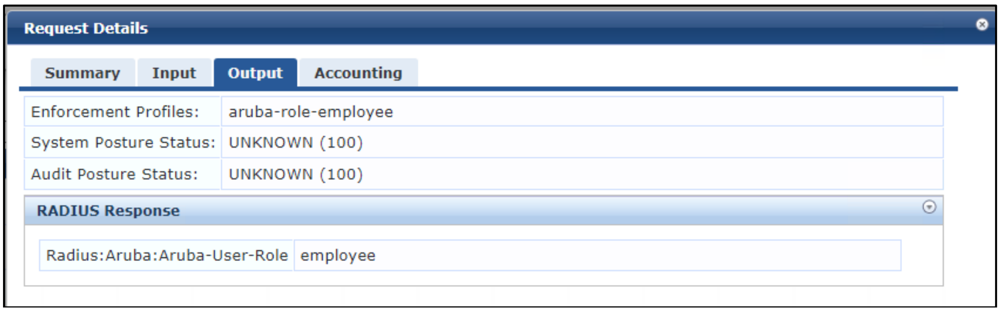
- **Question**: What is the NAS IP address?
- **Answer**: The IP address of the gateway, as reported inside the RADIUS header using the NAS-IP-Address attribute.
- **Question**: What is the NAS Identifier?
- **Answer**: The IP Address of the AP.
- **Question**: What do you notice?
- **Answer**: NAS-ID is the original AP IP address, while NAS-IP is the GW acting as RADIUS proxy.

14. Scroll down and expand **Computed Attributes**.



- **Question**: What is the Connection Src IP address?
- **Answer**: This value is based on the IP source address of the RADIUS packet. It will be the GW IP address.
- **Question**: What is the Connection NAD-IP-Address?
- **Answer**: This value is based on the RADIUS NAS IP address attribute in the RADIUS packet. it will also show the GW IP address.
- **Question**: What is the difference between these two?
- **Answer**: The Connection Source IP is the layer 3 source IP address, while the NAS IP address is the IP address reported by the GW inside the RADIUS attribute value pairs. The NAS-IP-Address will be used by ClearPass to record on what NAS this session is active.

15. Click the **Output** tab to review the Attributes returned by ClearPass to the Gateway. Expand **RADIUS Response**.



- **Question**: What value is returned by ClearPass to the gateway?
- **Answer**: ClearPass returns the Aruba VSA Aruba-User-Role with a value of employee.
- **Question**: Do you need to configure anything on the gateway to process this value?
- **Answer**: No. There is no configuration required on the gateway to process this VSA; this works by default. You only need to ensure that the user role exists on the gateway, otherwise the authenticated client will still have the 802.1X authentication default role from the AAA profile.

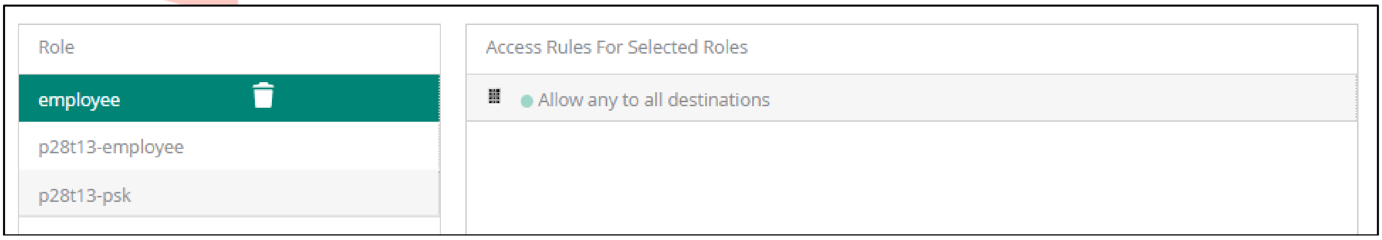
Create Employee User Role

In these steps you will create a new user role using the WLAN wizard.

When using the WLAN wizard, the user role is automatically created in the AP configuration and the GW configuration.

16. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
17. Under WLAN, edit the **p#tx-employee** WLAN.

18. On the **Access** page, change the slider to **Role Based**.
19. In the Role list, add a **new role**.
20. For the name, use **employee**.
21. Click **OK**.
22. Review the access control of the new role.



- **Question**: What is the default access for a new role created using the wizard?
- **Answer**: Allow any to all destinations.

23. Click **Save Settings**.
24. Wait for the wizard to complete, click **OK** to confirm.

Review the AP Configuration

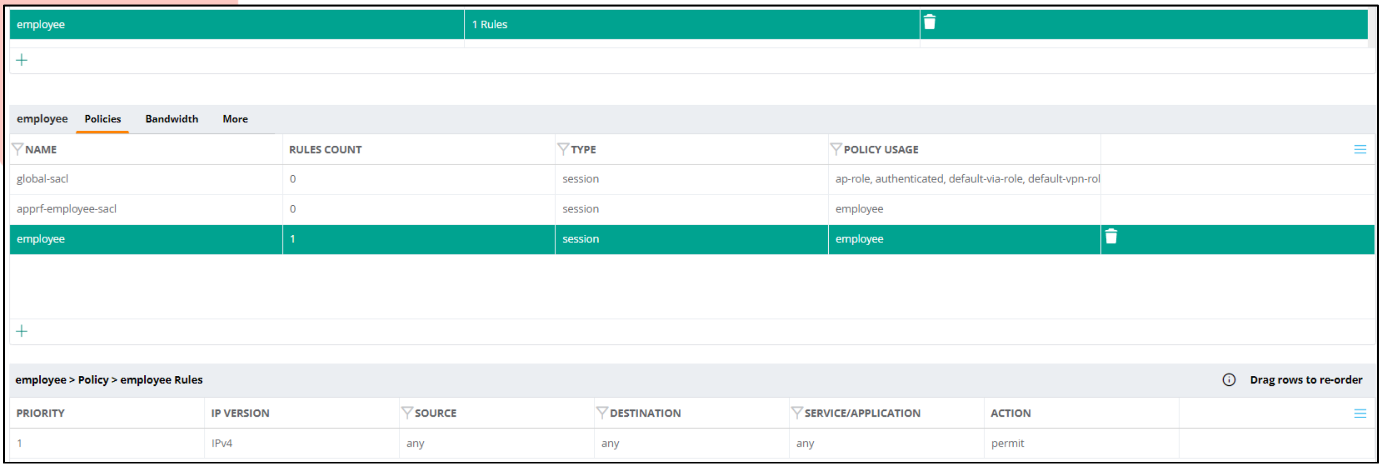
In the next steps, you will review the configuration that was applied by the WLAN wizard.

25. Navigate to **Security** page, expand **Roles**.
26. Click **employee** role.
27. Review the rules of the employee role.
    - **Question**: What access rules do you see?
    - **Answer**: Allow any to all destinations.

Review the GW Configuration

28. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
29. Under **Security** > **Roles**, click the **employee** role.
    - **Question**: Did this role exist by default?
    - **Answer**: No, it was created when you used the WLAN wizard on the AP group.

30. The window under the user role will show the active policies for the selected role.
31. In the policy list, click the policy **employee**. The rules for that policy will appear in a new window under the policy list.



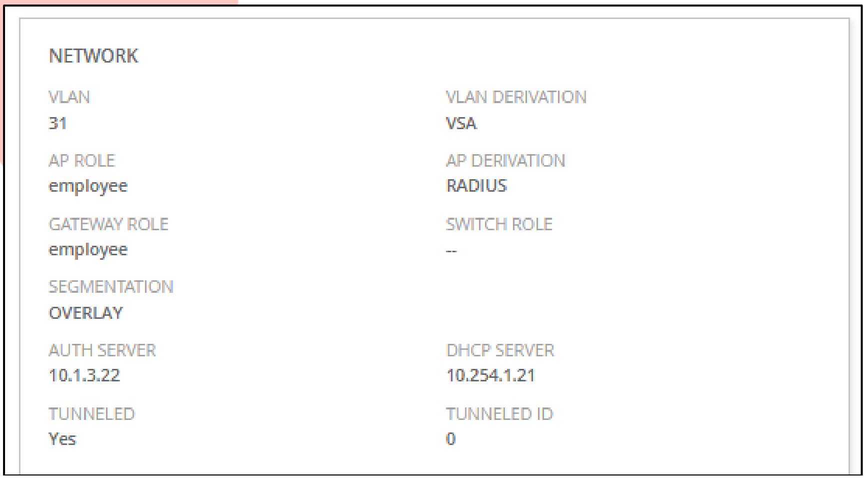
- **Question**: What rule do you see in the policy employee?
- **Answer**: IPv4 any any permit. This is the same as the WLAN wizard 'allow any to all destinations'. The rules set in the WLAN wizard were applied in a role on the AP and in a role on the GW.

Test with the Employee Client

In the next steps you will re-connect with the employee user to verify the updated role assignment.

32. On PC1, disconnect and reconnect to the **p#tx-employee** WLAN.
33. In Aruba Central, open the PC1 client details page, check the Network tile.

TIP: You can enter the text employee in the AI Search bar and click the employee entry. This will take you directly to the client details page.



- **Question**: What is the GW role and the AP Role?
- **Answer**: The GW role is employee and the AP role is also employee. The GW received the RADIUS access-accept from ClearPass that contains the Aruba-User-Role VSA for the role employee, and since the role exists on the GW, this became the active role. This access-accept was forwarded by the GW to the AP (the RADIUS proxy function), therefore the AP also received the Aruba-User-Role VSA and applied the employee role as well.

34. On the GW console/SSH session, review the client details, use the IP address of your client.

```
show user ip 10.1.31.xyz | include Role

(gw1) *# show user ip 10.1.31.50 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: employee (how: ROLE_DERIVATION_DOT1X_VSA), ACL: 95/0
Role Derivation: ROLE_DERIVATION_DOT1X_VSA
```

- **Question**: What is the role derivation method?
- **Answer**: ROLE_DERIVATION_DOT1X_VSA. This indicates that the GW received a RADIUS VSA for the Aruba-User-Role.

Task 2: Use the WLAN Workflow to Apply Access Control

In this task you will use the WLAN wizard to apply access control for the employee user.

Objectives

- Use the WLAN wizard to create access control rules.
- Verify the access control.

Steps

Update Access Control for the Role employee

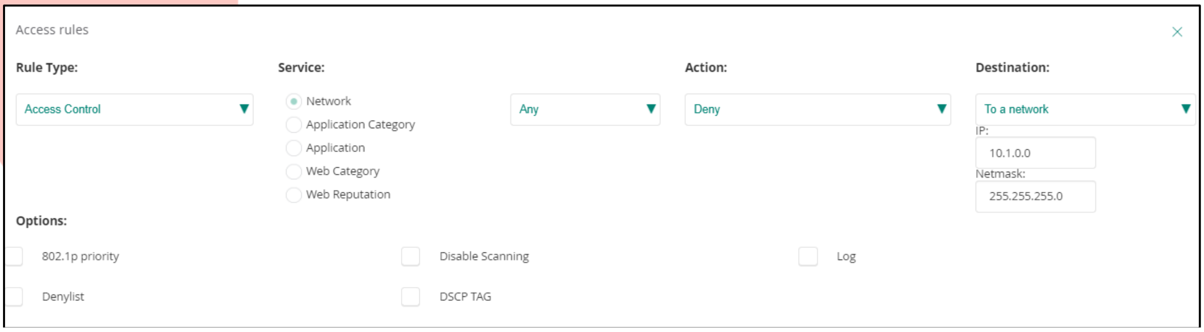
1. On PC1, you are currently connected as employee. Start a continuous ping to an IP address that will be blocked in this task. The ping should be successful.

```
ping 10.1.0.2 -t
```

2. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
3. On the WLAN page, edit the **p#tx-employee** WLAN.
4. Open the **Access** page.
5. Move the slider to **Role-based**.

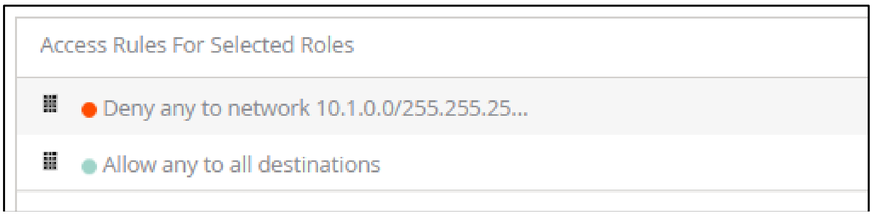
> **NOTE:** As you can see, the slider only remains selected if custom role assignment rules are defined. Since you are using the Aruba-User-Role VSA RADIUS attribute to assign the role, the slider does not remain enabled. This only applies to the UI and does not mean you cannot use the Aruba-User-Role VSA.

6. Select the role **employee**.
7. Click **Add rule** to block any protocol access to the network 10.1.0.0/24.
8. Configure the rule with the following settings:
   - Rule Type **Access Control**
   - Service **Network - any**
   - Action **Deny**
   - Destination To a network:
     - IP **10.1.0.0**
     - Netmask **255.255.255.0**



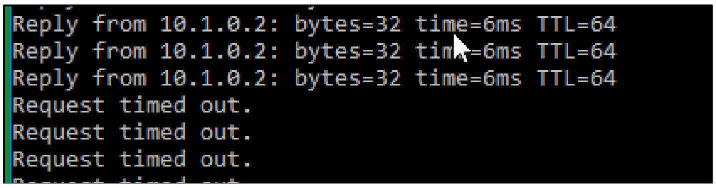
9. Click **OK** to add the rule.

10. Verify the rules are in the correct order. Traffic is processed in order, with the first rule as the top rule.



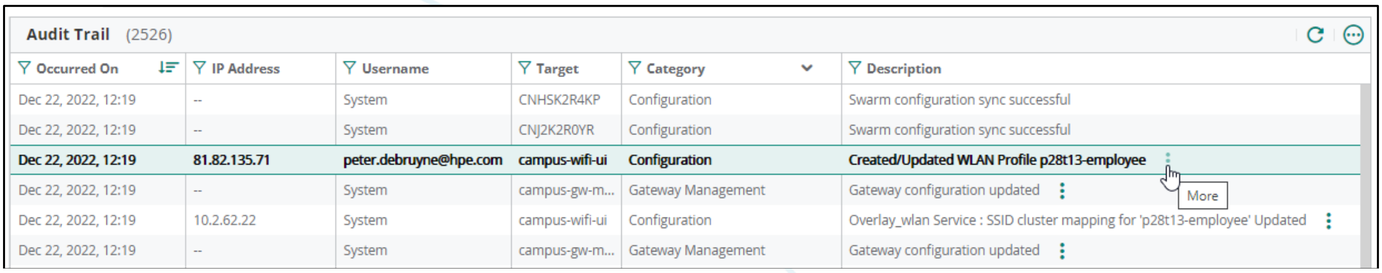
11. Click **Save Settings**.

12. On the PC1, verify that the ping responses have stopped.



Review the Applied Configuration in the Audit Trail

13. In Aruba Central, navigate to Context: **Global** > Navigation: **Audit Trail**.


Audit Trail (2526)

Occurred On	IP Address	Username	Target	Category	Description
Dec 22, 2022, 12:19	--	System	CNHSK2R4KP	Configuration	Swarm configuration sync successful
Dec 22, 2022, 12:19	--	System	CNJ2K2R0YR	Configuration	Swarm configuration sync successful
Dec 22, 2022, 12:19	81.82.135.71	peter.debruyne@hpe.com	campus-wifi-ui	Configuration	Created/Updated WLAN Profile p28t13-employee
Dec 22, 2022, 12:19	--	System	campus-gw-m...	Gateway Management	Gateway configuration updated
Dec 22, 2022, 12:19	10.2.62.22	System	campus-wifi-ui	Configuration	Overlay_wlan Service : SSID cluster mapping for 'p28t13-employee' Updated
Dec 22, 2022, 12:19	--	System	campus-gw-m...	Gateway Management	Gateway configuration updated

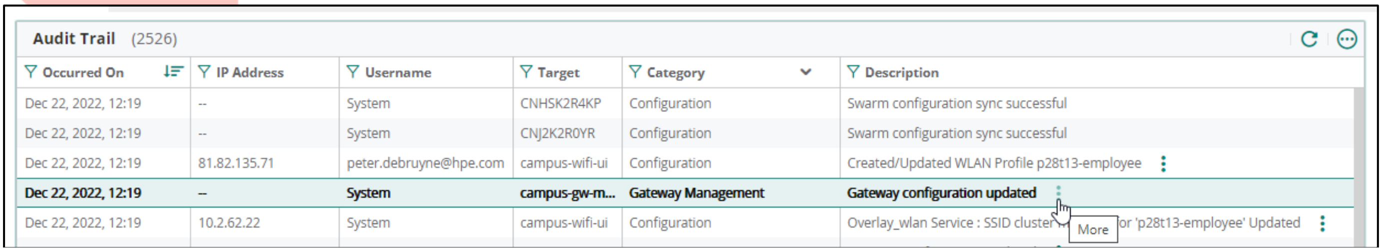
14. Open the details of the **Created/Updated WLAN Profile** p#tx-employee entry using the **three dots**.

```
wlan access-rule employee
no rule
rule 10.1.0.0 255.255.255.0 match any any any deny
rule any any match any any any permit
exit
```

- **Question**: Do you see the blocked network rule?

- **Answer**: Yes, the first rule blocks access to the 10.1.0.0/24 network.

15. Open the details of the last **Gateway Configuration Updated** entry.

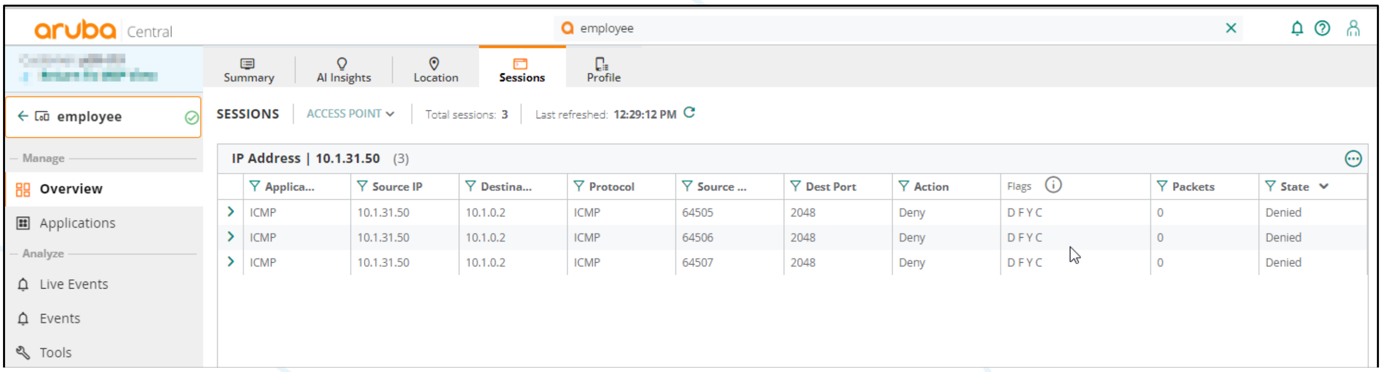


16. Scroll down to the bottom to see the configuration for the policy employee (ip access-list) and the user-role employee.

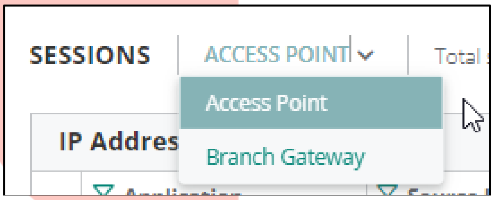
```
...
ip access-list session employee
any network 10.1.0.0 255.255.255.0 any deny position 1
any any any permit position 2

user-role employee
access-list session employee
...
```

- **Question**: Do you see the blocked network 10.1.0.0/24?
- **Answer**: Yes, on the GW, the same access control is applied by the WLAN wizard. The first rule blocks access to the 10.1.0.0/24 network.
- **Question**: If both AP and GW apply the same rules, which of these 2 devices will block the traffic from the user?
- **Answer**: The first device that receives the client traffic is the AP, the AP will be blocking the traffic in this example.

17. In Aruba Central, open the PC1 Client details page via the AI Search: **employee**.
18. Navigate to **Overview > Sessions**.

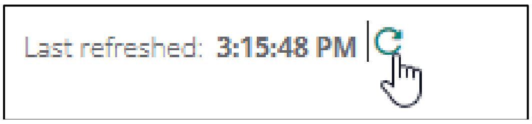


19. Click the dropdown list next to SESSIONS.

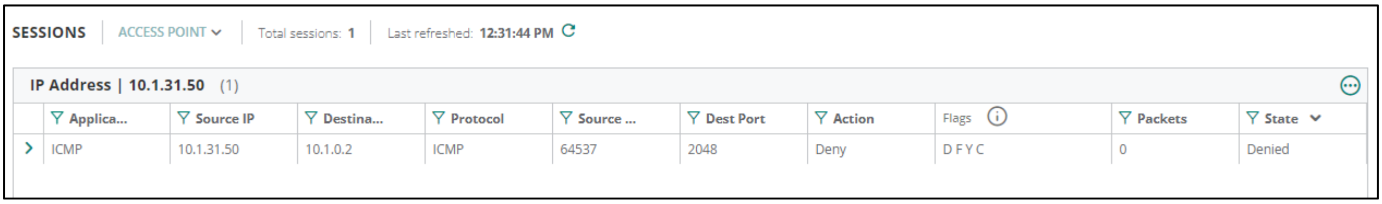


- **Question**: What options do you see in the Sessions dropdown list?
- **Answer**: Access Point and Branch Gateway. This allows you to query the client AP or the client gateway for their current firewall sessions for this client.

20. Leave **Access Point** as the selected entry for SESSIONS.
21. Use the **refresh** button to query the Access Point session list.



22. Review the list of active Sessions.



NOTE: You may see more sessions in your output, this depends on the traffic that is generated by the PC1 Windows client.

- **Question**: Do you see any ICMP Denied sessions?
- **Answer**: Yes, the Access Point blocks access to the 10.1.0.2 host.

Task 3: Gateway Controlled Access Control

In this task you will use the firewall of the gateway to control the access for the contractor user to the network.

You will connect PC4 with contractor credentials to the employee WLAN and use the gateway group to configure the gateway firewall rule set.

Objectives

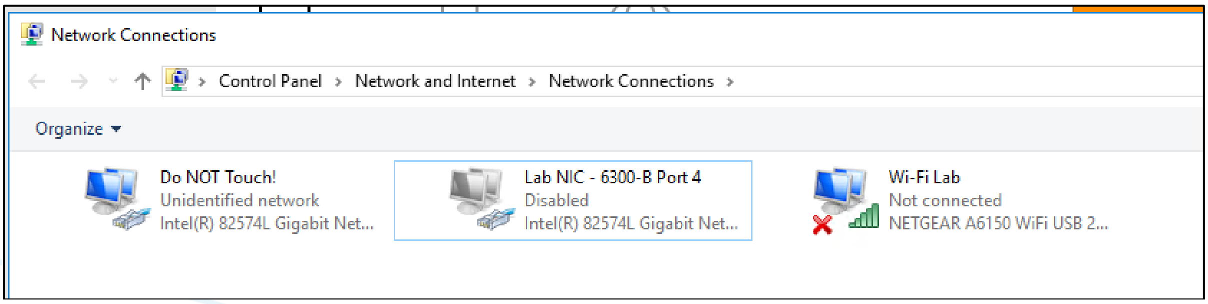
- Configure a user role on the gateway group.
- Apply access control using the gateway configuration.

Steps

Connect PC4 as Contractor to the employee WLAN

On PC4, you will enroll for a certificate using the PSK WLAN; then you will connect to the employee WLAN using EAP-TLS with the contractor certificate.

1. Use the lab dashboard to open a connection to PC4.
2. Using PC4, verify the Wi-Fi NIC is enabled and the wired LAB NIC is disabled.



IMPORTANT: Do not change the Do Not Touch interface.

3. On the PC4, connect to the **p#tx-psk** WLAN (PSK Aruba123!). This WLAN provides access the ClearPass server in your lab.
4. On the PC4, open a browser, such as Google Chrome, and navigate to

```
https://10.254.1.23/onboard/cert-iaca.php
```

5. Accept the certificate warning and continue. (**Advanced > Proceed**).
6. You will be presented with the Onboard Portal page. Enter the contractor credentials.
   - Username: **contractor**
   - Password: **Aruba123!**
7. Download and Run the QuickConnect app to install the certificate. Accept the notification messages.

NOTE: If you are unsure about the steps, refer to the previous lab activity to see the detailed steps.

8. Once the certificate has been installed, connect to the **p#tx-employee** WLAN using the certificate.

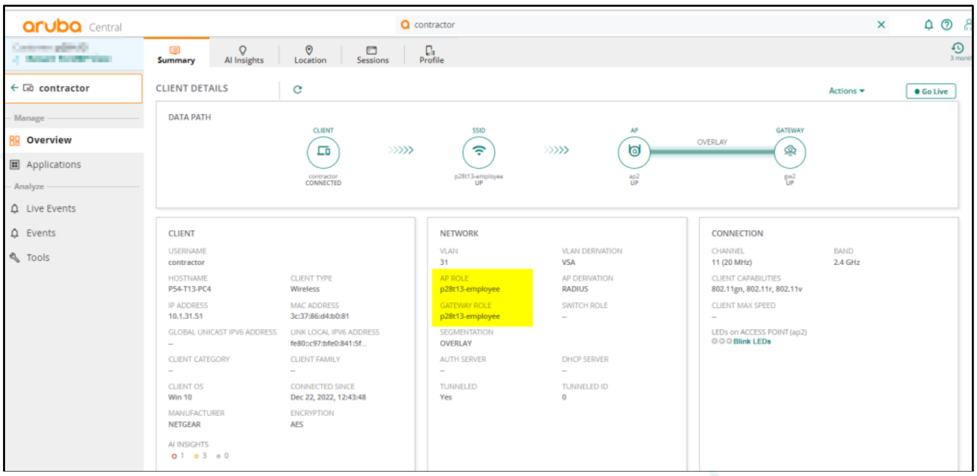
> **NOTE:** If you don't see the option to connect with the certificate, the time on PC4 may be different from the ClearPass server.

9. On PC4, verify that you can successfully ping 10.1.0.2. Access to this host will be controlled through the gateway policy.

```
ping 10.1.0.2
```

```
C:\Users\student> ping 10.1.0.2
Pinging 10.1.0.2 with 32 bytes of datAnswer:
Reply from 10.1.0.2: bytes=32 time=4ms TTL=64
Reply from 10.1.0.2: bytes=32 time=6ms TTL=64
Reply from 10.1.0.2: bytes=32 time=7ms TTL=64
Reply from 10.1.0.2: bytes=32 time=5ms TTL=64
```

10. In Aruba Central, use the AI Search and enter **contractor** to access the client details page for PC4.
11. Verify the contractor is connected and has been assigned the 802.1X default Authentication role (p#tx-employee) on both the AP and the GW.



Create the Contractor Role

In the next steps, you will use the WLAN wizard on the AP group to create the user-role for contractor.

12. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
13. **Edit** the WLAN p#tx-employee.
14. Navigate to the **Access** page.

15. Add a new role with name **contractor**. You don't need to change the default access rule.
16. Click **Save Settings**.

Configure the Contractor Role on the Gateway

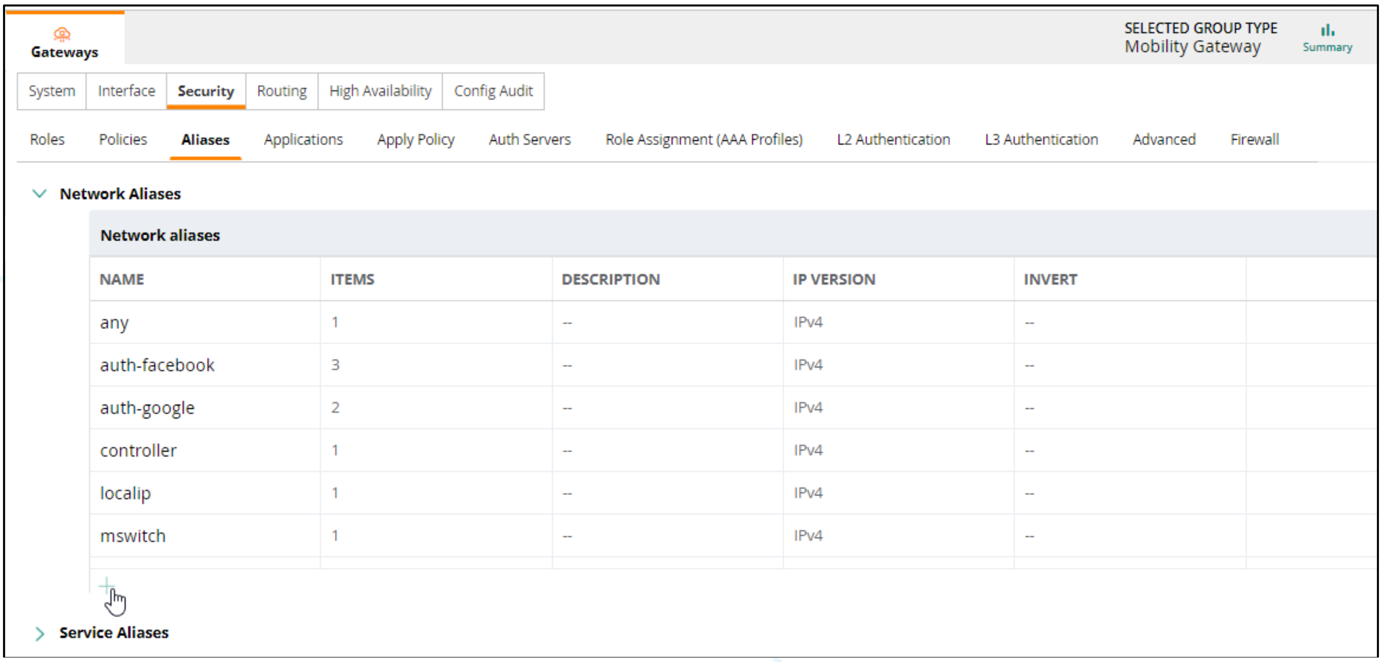
In this section, you will apply the firewall rules on the gateway group.

You want block access to some critical servers. Since the subnets of these critical servers could change at a later moment, you will create an alias.

The alias can then be used in the access policies.

Create Alias

17. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
18. Navigate to Security > Aliases.
19. Under Network aliases, click the **+** button to add a new alias.
    - Name: **critical-servers**



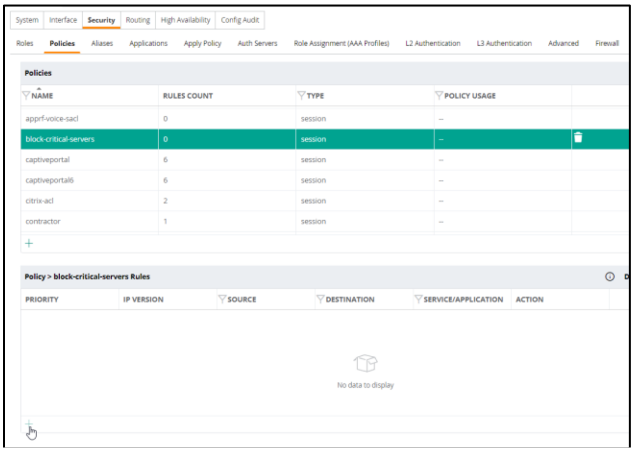
20. In the items list, click the **+** button to add a new item to the alias.
    - Rule type **network**
    - IP address **10.1.0.0**
    - Netmask/wildcard **255.255.255.0**

21. Click **OK** to add the item.
22. Click **Save Settings** to add the alias.

Configure New Policy to Block Access to Critical Servers

On the gateway, a user-role consists of 1 or more policies. The policy contains the individual rules that allow or deny the traffic.

23. Navigate to Security > Policies.
24. Use the **+** button to add a new Policy.
    - Type **Session**
    - Name **block-critical-servers**
25. Click Save Settings.
26. In the policy list, select the policy **block-critical-servers**.
27. At the bottom of the page, click the **+** button to **add a new rule**.

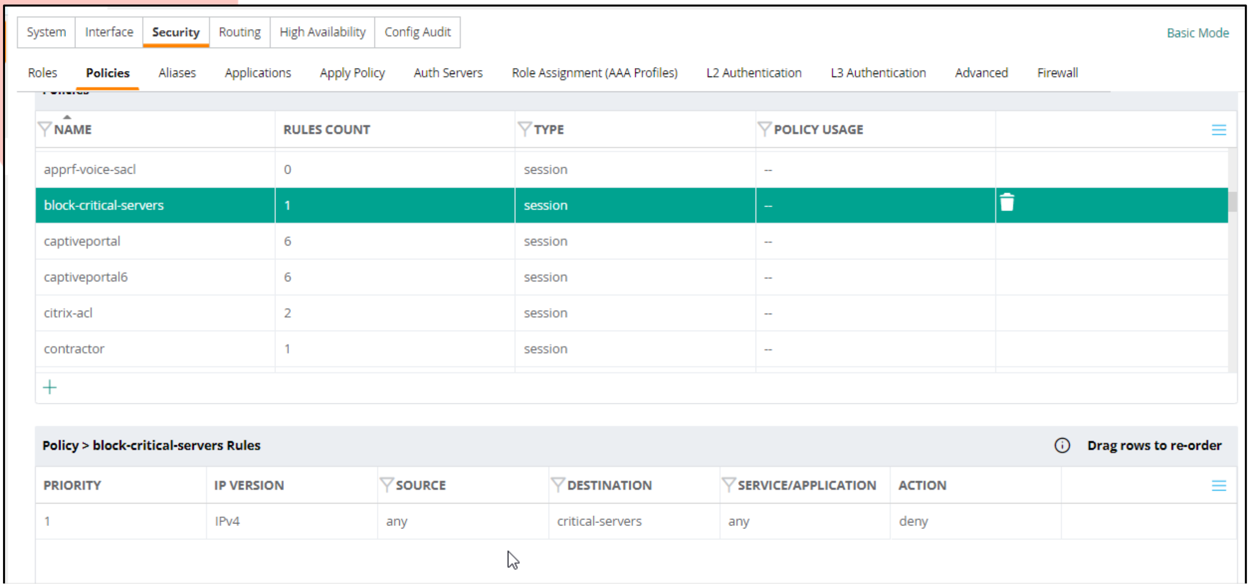


The new rule screen will appear under the policy rule list.

28. Scroll down to enter the rule details.

- **Destination:** **Alias**
- **Destination alias:** **critical-servers**
- **Action:** **Deny**

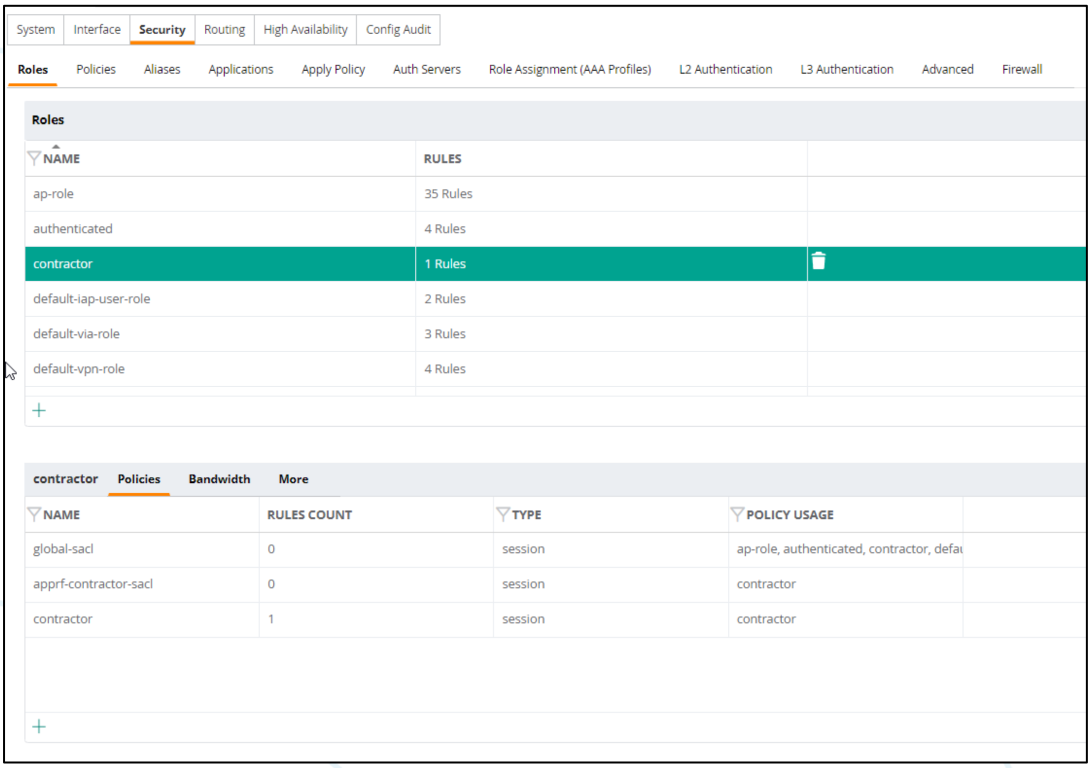
29. Click **Save Settings** to save the rule.
30. Verify the new rule is displayed in the policy rule list.



Update the Contractor User Role to add the new Policy

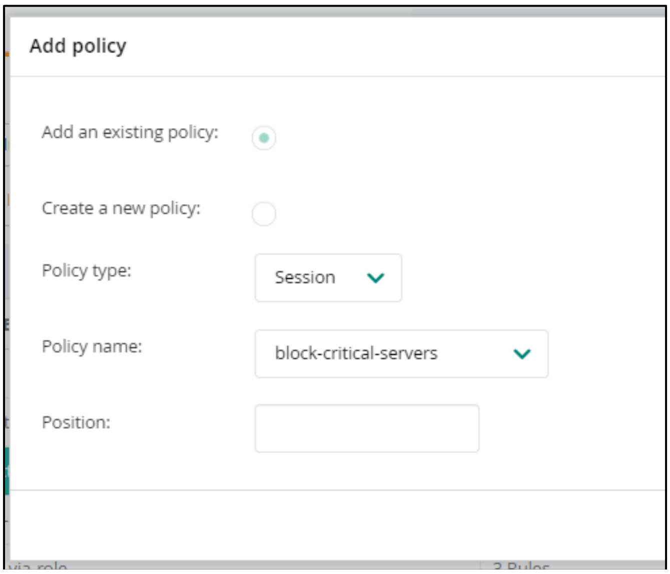
31. Navigate to **Security > Roles**.
32. Select the **contractor** role from the list.
33. At the bottom of the screen, the policies will be listed. These include:

- the global session ACL: global-sacl
- the role-based apprf-sacl: apprf-contractor-sacl
- the role-based policy: contractor

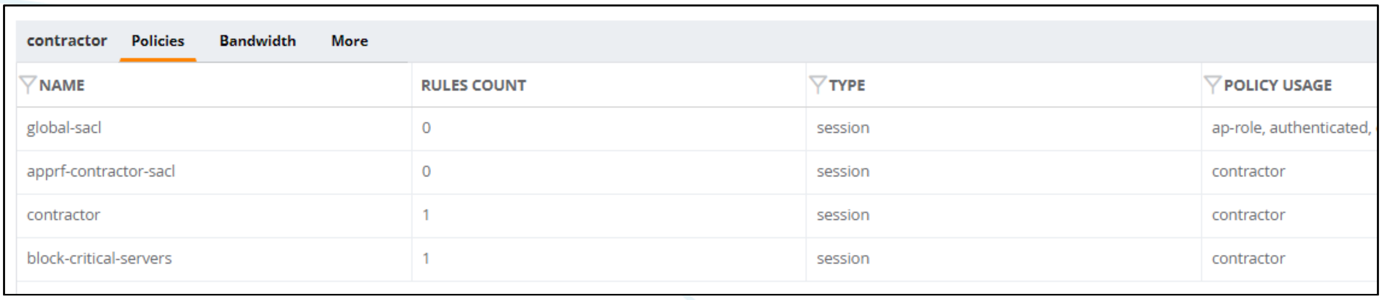


NOTE: The first two policies are system defined, they should not be used to configure custom rules.

34. Click the **+** button to add a new policy to the role.
35. Select **Add an existing policy** and select the **block-critical-servers** policy. This is the policy you have created in the previous steps.



36. Click **Save Settings**.
37. Review the list of policies.



NAME	RULES COUNT	TYPE	POLICY USAGE
global-sacl	0	session	ap-role, authenticated,
apprf-contractor-sacl	0	session	contractor
contractor	1	session	contractor
block-critical-servers	1	session	contractor

- **Question**: Will access to the critical servers be blocked with this configuration?
- **Answer**: No. The default contractor policy contains a default rule with ‘permit any to all destinations’. When this rule set is applied before the critical-servers policy, the rules of the critical-servers will never be used.

38. Change the order of the policies. **Move** the **block-critical-servers** *before* the contractor policy using drag and drop.

NOTE: After the drag and drop, it takes a few moments for the UI to update.

contractor | Policies | Bandwidth | More

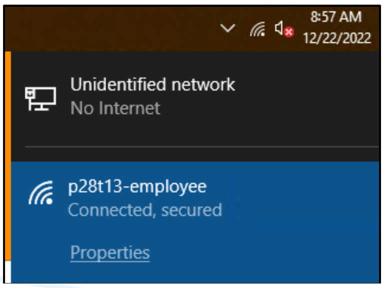
NAME	RULES COUNT	TYPE	POLICY USAGE
global-sacl	0	session	ap-role, authenticated, co
apprf-contractor-sacl	0	session	contractor
block-critical-servers	1	session	contractor
contractor	1	session	contractor

Verify the updated Contractor Access Control

In the next steps, you will use the PC4 (connected as contractor user) to verify that the new access control was configured for the gateway user role.

39. On PC4, disconnect and reconnect to the **p#tx-employee** WLAN.

IMPORTANT: The PC4 may attempt to reconnect to the p#tx-psk WLAN. Make sure to double-check it is connected to the p#tx-employee WLAN!

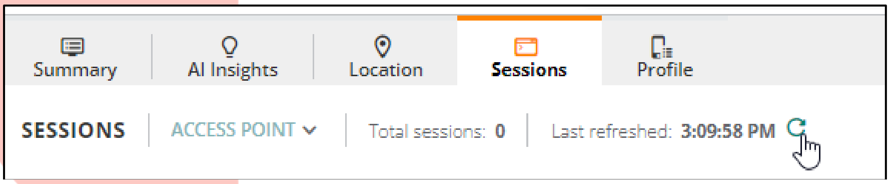


40. In Aruba Central, use the AI Seach: **contractor** to open the contractor client details page.
41. On the client details page, navigate to **Overview > Sessions** page.
42. On PC4, attempt to ping to 10.1.0.2, there should be no response.

```
ping 10.1.0.2
```

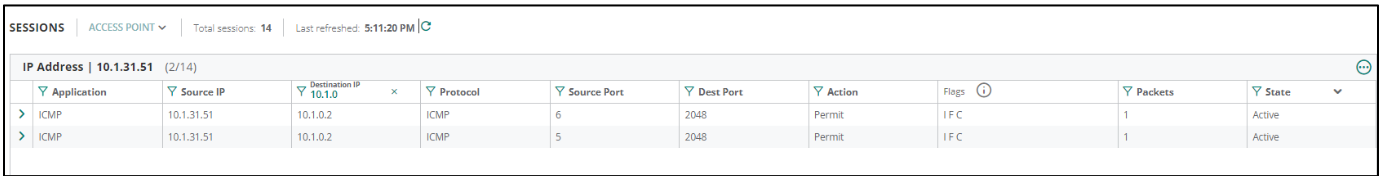
NOTE: If you do get a response, check these items:
- Is PC4 connected to the correct p#tx-employee WLAN?
- Did the client get the correct role contractor assigned?
- Check the order of the policies on the contractor user role.
- Check if the policy block-critical-servers contains the deny list.
- Check if the alias critical-servers contains the correct subnet.

43. In Aruba Central, on the Sessions page, use the refresh button to get the latest session list. You should see an ICMP session.



TIP: You can filter the sessions using the column filters. You can enter 10.1.0 in the destination column filter for example.

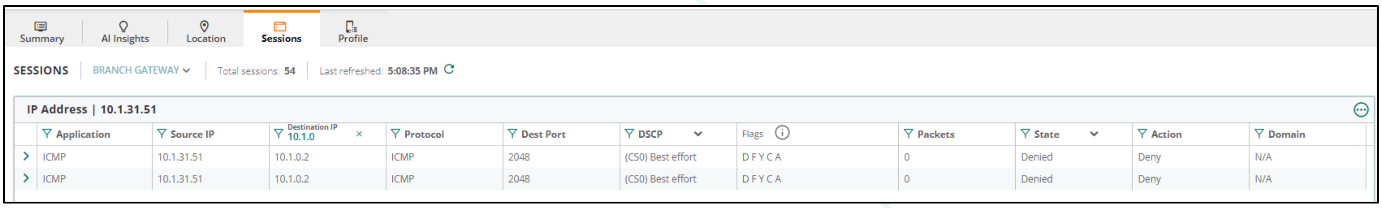
NOTE: The ICMP sessions age out quickly. If you don't see the ICMP session, you can repeat the ping on the client.



- **Question**: Do you see the ICMP session to 10.1.0.2?
- **Answer**: Yes.
- **Question**: What is the Action based on the AP firewall?
- **Answer**: Permit. This is correct since the AP role configuration allows all traffic for the contractor role.

44. In the SESSIONS dropdown list, select **Gateway**. Review the gateway firewall sessions.

TIP: Remember you can enter 10.1.0 in the Destination IP column filter.



- **Question**: Do you see the ICMP session to 10.1.0.2?
- **Answer**: Yes. Since the AP is passing the traffic to the gateway, the traffic arrives at the gateway and will be processed by the gateway firewall.
- **Question**: What is the action for the ICMP session to 10.1.0.2?

- **Answer**: Denied. This is correct based on the gateway contractor user role configuration.

Task 4: Gateway Controlled Access Control using the User Alias

In this task you will explore a feature that is specific to the identity-based firewall on the gateway.

The gateway can apply a unique, per-client rule set by using the special alias *user* in an access rule.

This alias *user* will be replaced by the actual client IP address in the firewall policies for the client. The result is that each user will have a unique rule set, based on the actual IP address of the system.

By using the *user* alias as the source or destination in a rule set, the administrator can choose whether the traffic should be controlled from the client (use *user* as source in a rule) or controlled to the client (use *user* as the destination alias in a rule).

In this task you will configure the contractor so only a limited set of internal IP addresses is allowed to connect to the contractor.

Objectives

- Understand the gateway firewall user alias.
- Implement the user alias in a user role to control inbound or outbound traffic.

Steps

Verify Internal Network Access to Contractor

In these steps you will first verify that several IP addresses on the internal network can access the contractor system. One of these subnets will be blocked access to the contractor in the upcoming section.

1. In Aruba Central, take note of the contractor client IP address.
2. Open a connection to the **sw-agg1** and attempt to ping to the contractor using 2 different **source** IP addresses (10.1.**31**.2 and 10.1.**11**.2)

```
ping 10.1.31.<contractor-ip> source 10.1.31.2
```

Here is an example output:

```
sw-agg1(config)# ping 10.1.31.51 source 10.1.31.2
PING 10.1.31.51 (10.1.31.51) from 10.1.31.2 : 100(128) bytes of data.
108 bytes from 10.1.31.51: icmp_seq=1 ttl=128 time=15.6 ms
```

```
ping 10.1.31.<contractor-ip> source 10.1.11.2
```

Here is an example output:

```
sw-agg1(config)# ping 10.1.31.51 source 10.1.11.2
PING 10.1.31.51 (10.1.31.51) from 10.1.11.2 : 100(128) bytes of data.
108 bytes from 10.1.31.51: icmp_seq=1 ttl=128 time=6.88 ms
```

NOTE: Make sure both pings are successful. If these pings would fail, check the Windows firewall on the PC4.

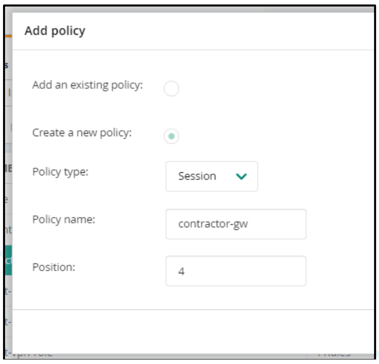
Update the Contractor Role on the Gateway Group

In these steps you will update the contractor user role on the gateway.

You will ensure that systems in the 10.1.11.0/24 subnet cannot initiate connections to the contractor system.

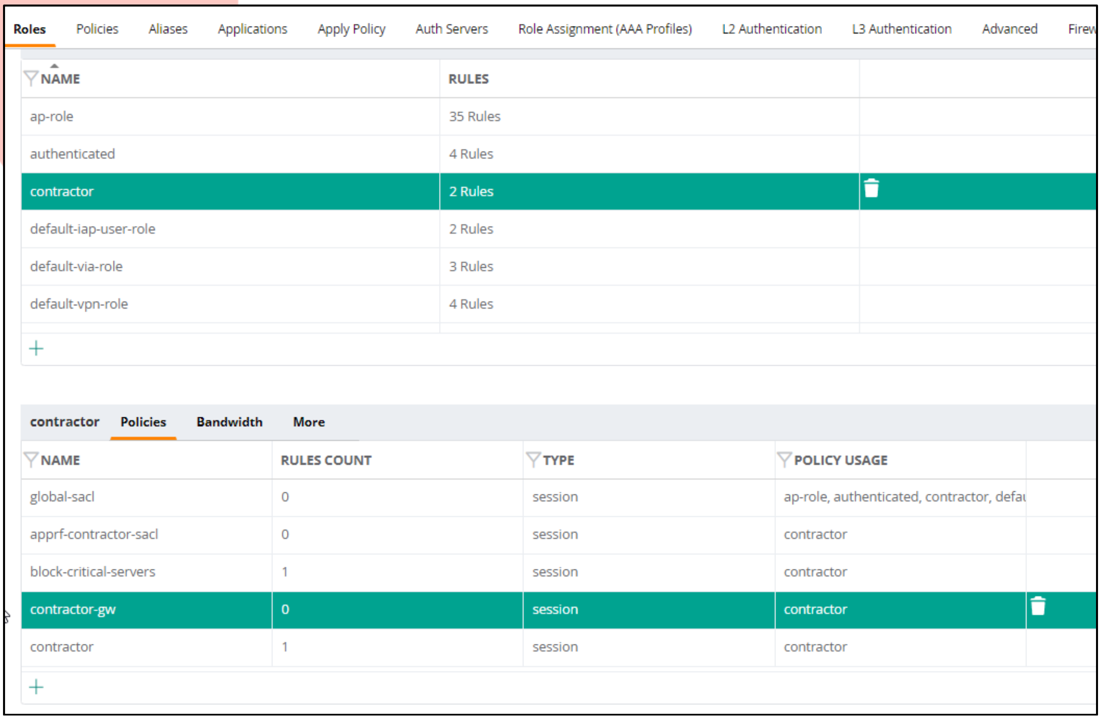
You will also see that this configuration still allows the contractor to initiate sessions to that subnet. The initial connection is checked by the firewall rules, the return traffic is automatically allowed.

3. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
4. Navigate to **Security > Roles**.
5. Select the role **contractor**. You will now add the new policy:
   - after the existing block-critical-servers
   - before the existing contractor policy
6. This can be achieved by using position 4 for the new policy.
7. In the Policy list, click **+** button to add a new policy.
8. Select **Create New Policy**.
   - Type: **Session**
   - Name: **contractor-gw**
   - Position: **4**



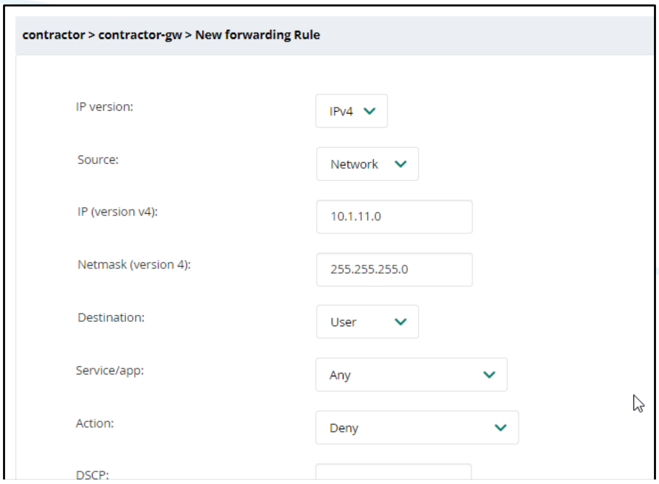
NOTE: The default **contractor** policy is the ruleset that will be edited by the WLAN wizard, therefore you are creating a *new* policy. This new policy will not be affected by any changes made in the WLAN Wizard.

9. In the policy list, select the **contractor-gw** policy.



10. Scroll down to see the contractor-gw policy rules.
11. Click the **+** button to add a new rule to the policy.

- Source: Network **10.1.11.0**
  Mask **255.255.255.0**
- Destination: **User**
- Action: **Deny**



12. Click **Save Settings**.

NOTE: Changes to the gateway role do not require a reconnect of the client. Existing sessions would require a reconnect, but the ICMP test pings are considered new sessions with every ping attempt.

Verify the Access Control based on the User IP Address

13. On the sw-agg1 session, attempt to ping the contractor PC using both source IP addresses.

> **TIP:** Each ping is displayed as 1 session. To simplify the firewall session view, limit the pings to 1 by using the repetitions 1 option.

The ping from source IP 10.1.31.2 should be successful.

```
ping 10.1.31.<contractor-ip> source 10.1.31.2 repetitions 1
```

Here is an example output

```
sw-agg1(config)# ping 10.1.31.51 source 10.1.31.2 repetitions 1
PING 10.1.31.51 (10.1.31.51) from 10.1.31.2 : 100(128) bytes of data.
108 bytes from 10.1.31.51: icmp_seq=1 ttl=128 time=7.06 ms
--- 10.1.31.51 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 7.061/7.061/7.061/0.000 ms
```

The ping from the source IP 10.1.11.2 should fail.

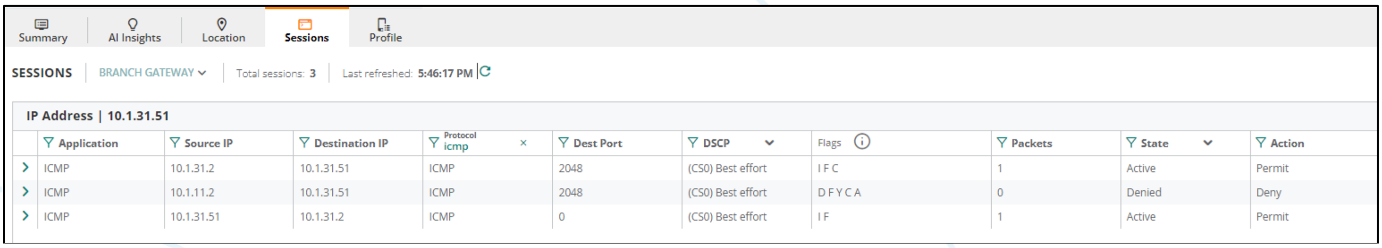
```
ping 10.1.31.<contractor-ip> source 10.1.11.2 repetitions 1
```

Here is an example output

```
sw-agg1(config)# ping 10.1.31.51 source 10.1.11.2 repetitions 1
PING 10.1.31.51 (10.1.31.51) from 10.1.11.2 : 100(128) bytes of data.
--- 10.1.31.51 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

14. In Aruba Central, open the client details page for the contractor.
15. Navigate to **Overview > Sessions**.
16. In the SESSIONS dropdown list, click **Gateway**.
17. Enter **icmp** in the protocol filter. This filter is not case-sensitive.

18. Review the allowed and denied sessions.



Summary | AI Insights | Location | Sessions | Profile

SESSIONS | BRANCH GATEWAY | Total sessions: 3 | Last refreshed: 5:46:17 PM

IP Address | 10.1.31.51

Application	Source IP	Destination IP	Protocol icmp	Dest Port	DSCP	Flags	Packets	State	Action
ICMP	10.1.31.2	10.1.31.51	ICMP	2048	(CS0) Best effort	I F C	1	Active	Permit
ICMP	10.1.11.2	10.1.31.51	ICMP	2048	(CS0) Best effort	D F Y C A	0	Denied	Deny
ICMP	10.1.31.51	10.1.31.2	ICMP	0	(CS0) Best effort	I F	1	Active	Permit

> **NOTE:** The ICMP sessions age out quickly, you can repeat the ping test if needed.

- **Question**: For the denied session, what is the destination IP?
- **Answer**: The destination IP address is the IP address of the contractor client. The **user** keyword in the rule was replaced with the active user IP address in the firewall rule.

Test the direction from Contractor to the Blocked Subnet

The ArubaOS firewall is stateful: this means only sessions initiated from the blocked subnet to the contractor are blocked.

You will now verify that the contractor user can still initiate sessions *to* the blocked subnet.

19. On the PC4, attempt to ping **10.1.11.2** with a count of **1**.

```
C:\Users\student>ping 10.1.11.2 -n 1
Pinging 10.1.11.2 with 32 bytes of datAnswer:
Reply from 10.1.11.2: bytes=32 time=6ms TTL=64
Ping statistics for 10.1.11.2:
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

This confirms that you have control about the direction of the session filtering by placing the user alias as either source or destination in a rule.

Task 5: Configure Dynamic Authorization with the Gateway Cluster

In this task you will first explore how to enable support RADIUS dynamic authorization on the gateway. RADIUS dynamic authorization allows the RADIUS server to send a message to the NAS to update the authorization or re-authenticate the client.

The NAS (the gateway in this lab environment) must be configured to support these messages from the RADIUS servers.

In the first part of the lab, you will confirm that by default, the dynamic authorization messages are rejected by the gateways.

Next you will configure the gateways to support the dynamic authorization messages by adding the ClearPass servers as an RFC3576 host, which is the RFC that covers the RADIUS Dynamic Authorization messages.

In the last section of this task, you will see how a gateway cluster can be configured with a VRRP address as the NAS IP. This will ensure that the RADIUS server can still send a dynamic authorization message to the cluster even when a cluster member might have failed. Thanks to the VRRP address, the other cluster members can ensure the original NAS IP address is still active on the network. Therefore, the RADIUS server can still send a Dynamic Authorization message for a user that has failed over to another cluster member because of a gateway failure.

Objectives

- Configure dynamic authorization support on the AOS 10 solution.
- Configure the gateway cluster with support for dynamic authorization.

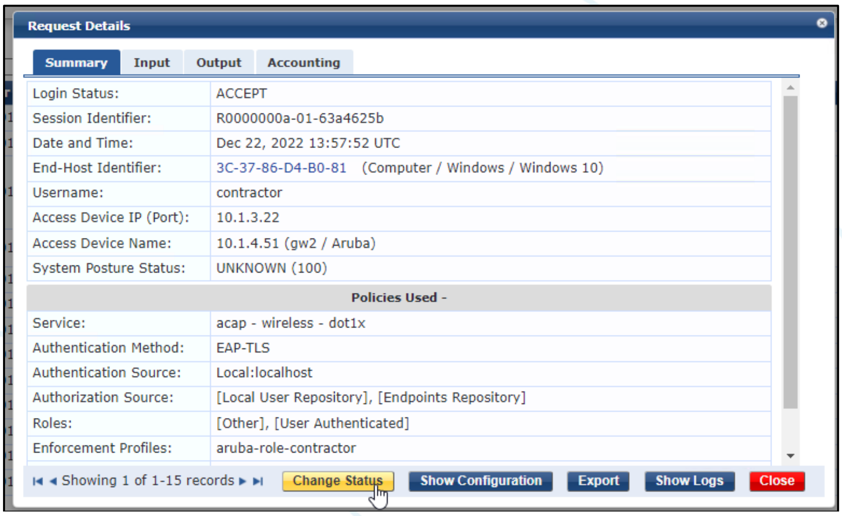
Steps

Verify the Dynamic Authorization is Rejected by Default

1. Use MGMT PC to connect to ClearPass using **admin** / **Aruba123!**.

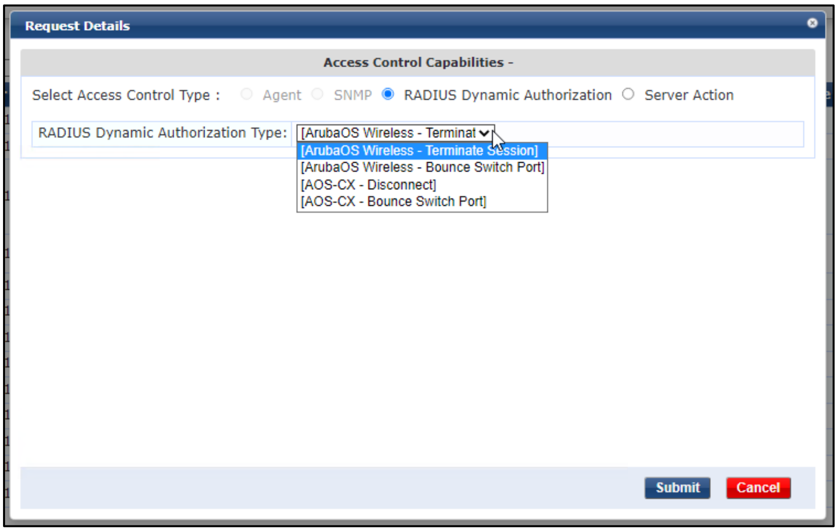
```
https://10.254.1.23/tips
```

2. Navigate to **Monitoring > Live Monitoring > Access Tracker**.
3. Click the latest authentication event for the user contractor.
4. Click **Change Status** at the bottom of the window.



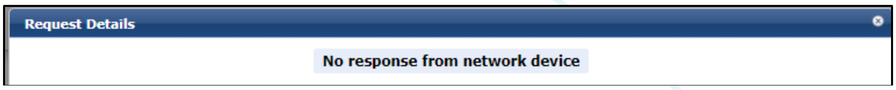
NOTE: If you don't see the Change Status option, the client is offline for ClearPass. Make sure:
1. The contractor wireless client (PC4) is connected.
2. Accounting is enabled on the WLAN (This was done in the previous lab as part of the p#tx-employee WLAN setup).

5. Verify that the Type is set to **ArubaOS Wireless – Terminate Session** and click **Submit**.



NOTE: Both AOS (AOS 8/AOS1 0/InstantOS) on the APs/gateways and AOS-CX on the switches use the Aruba RADIUS dictionary. Since the CoA instruction is slightly different between the wireless and wired platforms, you will see separate disconnect options.

6. After a few moments, the action will stop with the message:



This happened because the gateways are not configured to allow dynamic authorization (CoA/Disconnect Messages) from the ClearPass RADIUS system.

Review the Default NAS IP Address

7. On the **Input** tab of the authentication entry, expand the **RADIUS Request** section.

- Take note of the value of **RADIUS:IETF:NAS-IP-Address**:________________________
- This will be either 10.1.3.21 or 10.1.3.22 with the current setup.

8. Scroll down and expand the **Computed Attributes** section.

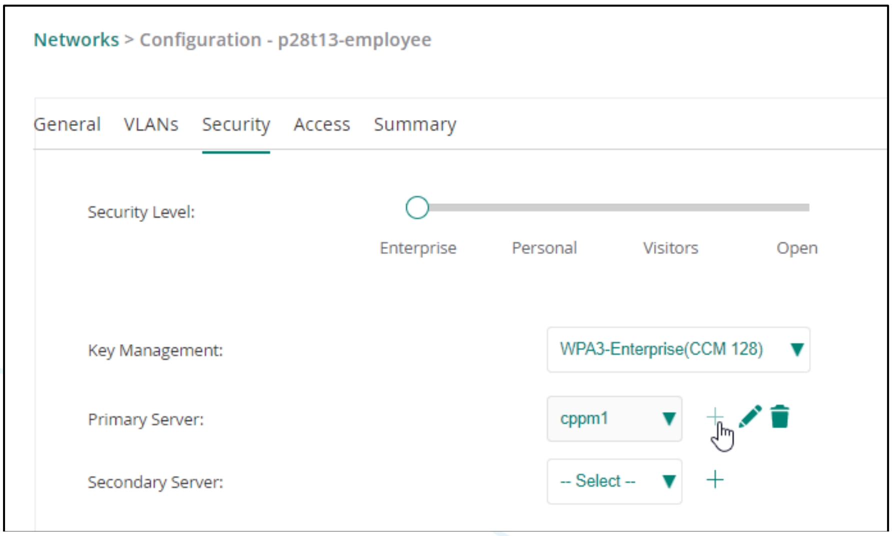
- Take note of the value of **Connection:Src-IP-Address** :________________________
- **Question**: What do you observe?
- **Answer**: Both values are the same and point to the controller IP address of the gateway. When the Dynamic Authorization is sent by ClearPass, the NAS-IP-Address value is used as the destination IP. The Connection:Src-IP-Address is not used in this process.

Configure the Gateways to Support RFC 3576 Dynamic Authorization

In these steps you will allow the ClearPass IP address (10.254.1.23) to send the RADIUS CoA messages to the gateways.

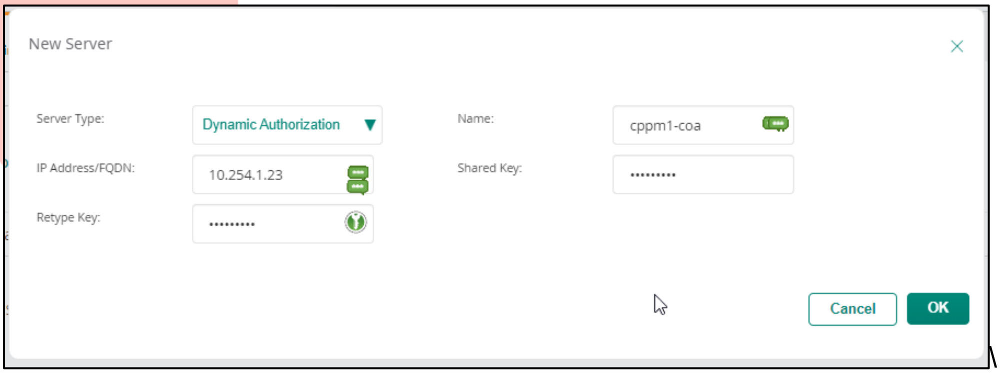
Support for RFC3576 servers can be added through the WLAN wizard.

9. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
10. On the WLAN page, edit the **p#tx-employee** SSID.
11. On the Security page, click the **+** button next to the Primary server.



12. Enter these values

- Server type: **Dynamic Authorization**
- Name: **cppm1-coa**
- IP address: **10.254.1.23**
- Shared key: **Aruba123!**
- Confirm the key



13. Click **OK**.
14. Set the Primary Server to **cppm1**.

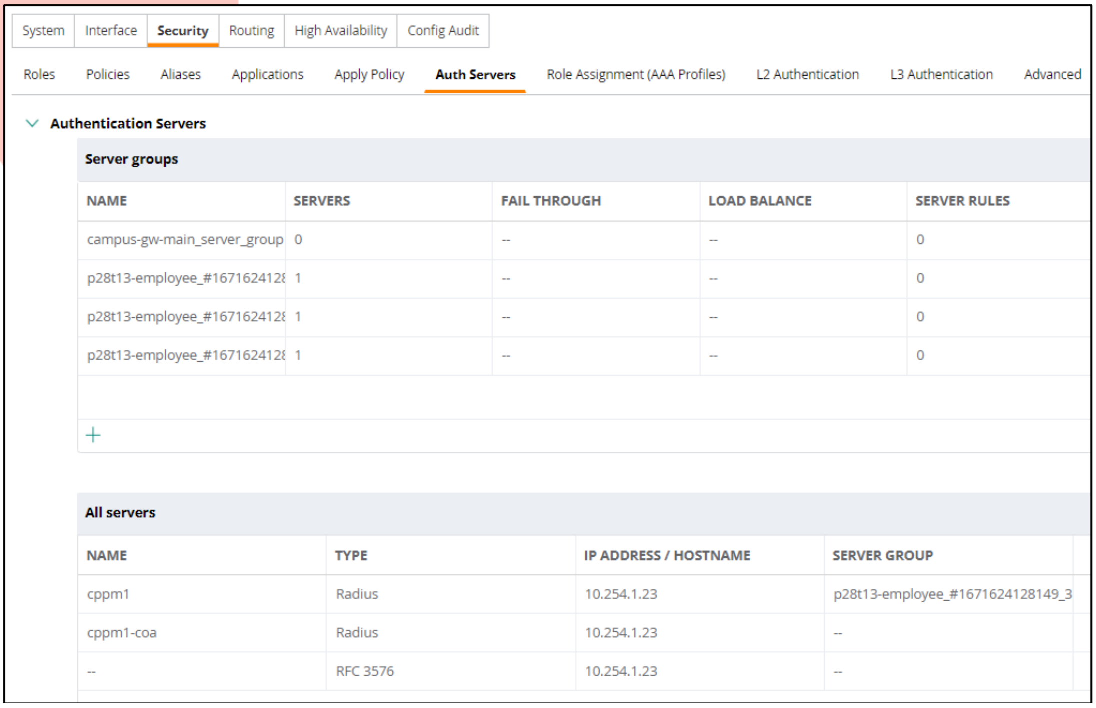
NOTE: When adding the Dynamic Authorization server, the wizard assigns it as the primary server by default. Revert the primary server to **cppm1**.

15. Click **Save Settings**.
16. Wait for the wizard to complete, then click **OK**.

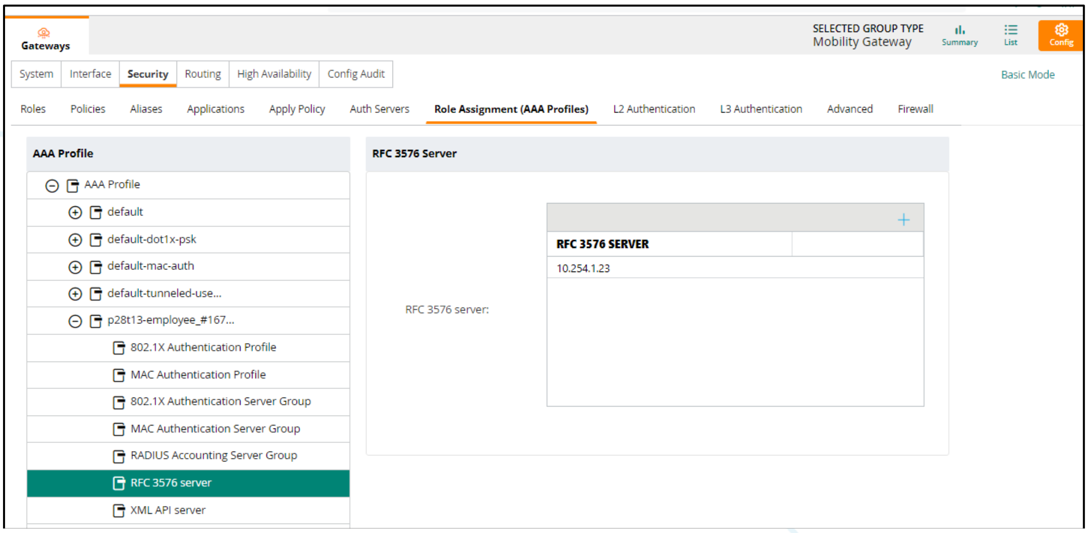
Review the RFC3576 Configuration on the Gateway Group

In the previous steps, you used the WLAN wizard to add the RFC3576 servers. In the next steps you will confirm that this RFC3576 was created in the gateway configuration.

17. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config (gear icon)**.
18. Navigate to **Security > Auth Servers**.
19. Under **All Servers**, review the RFC3576 server is in the list.



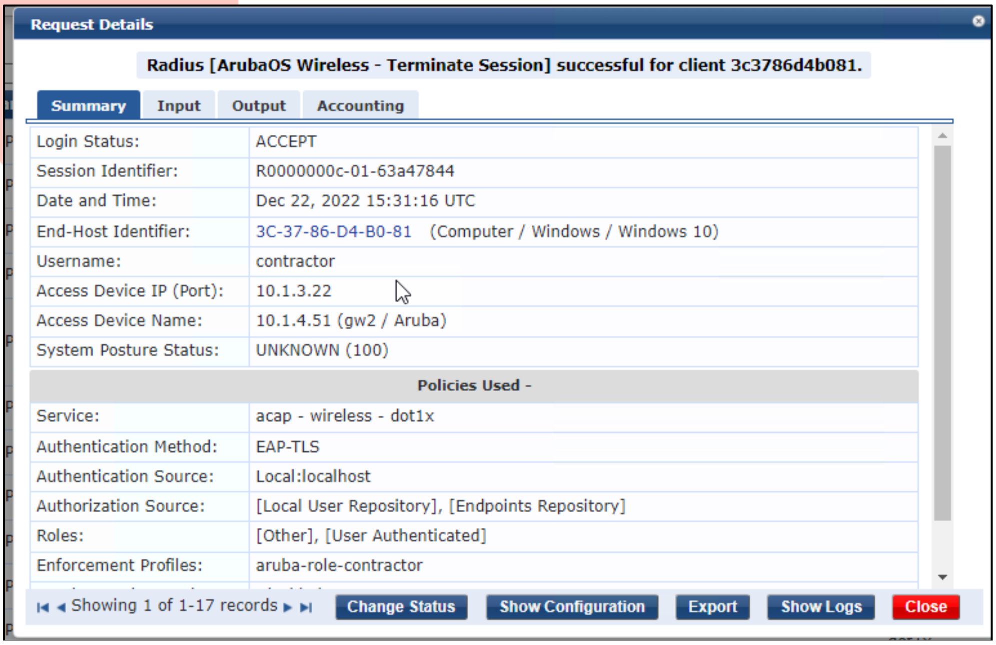
20. Navigate to **Security > Role Assignment (AAA Profiles)**.
21. Expand the AAA profile that begins with **p#tx-employee-…**
22. Expand the **RFC3576 Server** section.



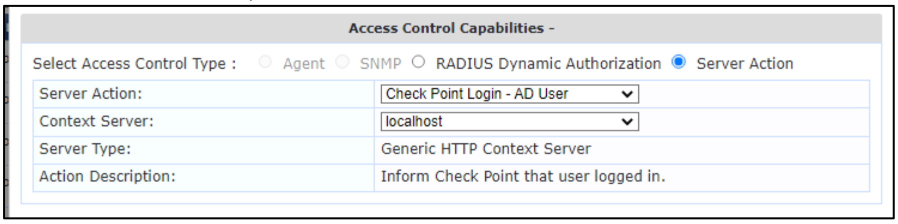
23. Confirm that the server 10.254.1.23 is in the list.

Verify the Dynamic Authorization from ClearPass

24. Switch to the ClearPass session on MGMT PC.
25. Attempt to **Change Status** of the contractor user again.



NOTE: If you do not have the RADIUS Dynamic Authorization option, but only the Server Action, like this:



You may reconnect the PC4 to get a new session in ClearPass.

- **Question**: Was the disconnect successful?
- **Answer**: Yes, the gateways now accept the Dynamic Authorization message from ClearPass.

Gateway Cluster CoA Support

In the previous section you have verified that the gateway cluster now supports the CoA messages for the connected clients.

In case CoA support is critical in a deployment, you may need to enhance the dynamic authorization configuration.

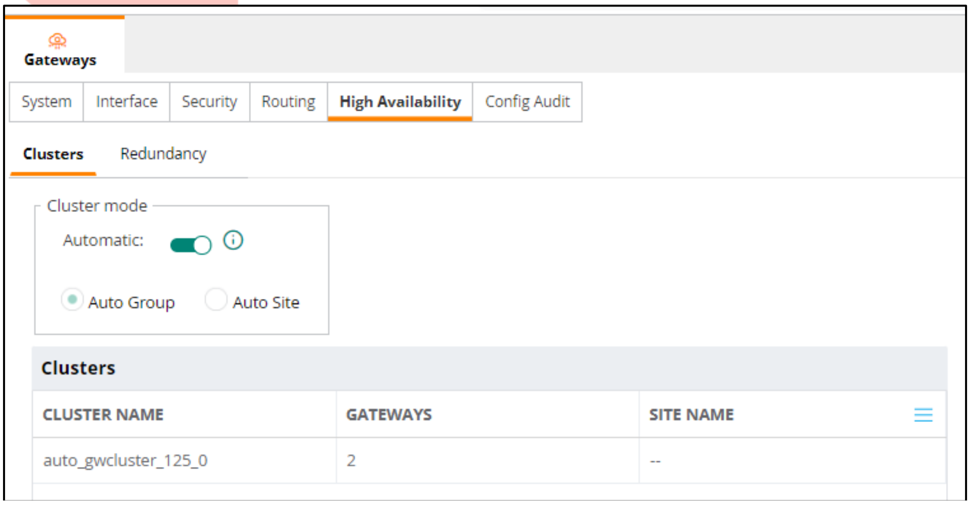
ClearPass will send the dynamic authorization message to the NAS IP address as reported by the gateway in the accounting packets.

When a gateway would go offline, the clients will move to another gateway in the cluster. However, ClearPass would attempt to send the CoA messages to an IP address that is no longer reachable (the original gateway), therefore the dynamic authorization will fail for the moved clients.

In the next steps you will enable dynamic authorization to use a VRRP IP address as the NAS IP address. When a gateway fails, another gateway will take control of the VRRP IP and it will be able to respond to the ClearPass dynamic authorization messages.

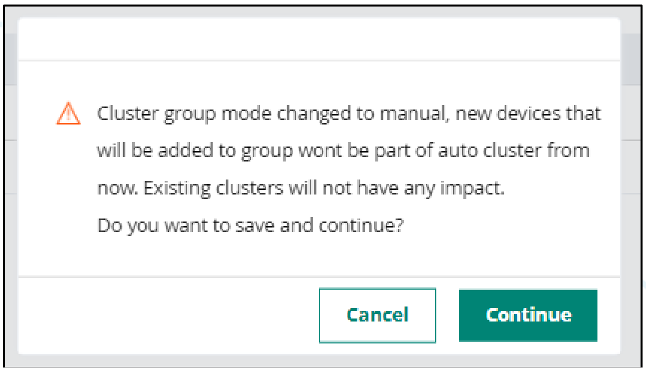
To configure VRRP IP addresses, a manual cluster setup must be used.

26. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config (gear icon)**.
27. Navigate to the **High Availability** page.



- **Question**: What is the current cluster mode?
- **Answer**: The default cluster mode has automatic enabled.

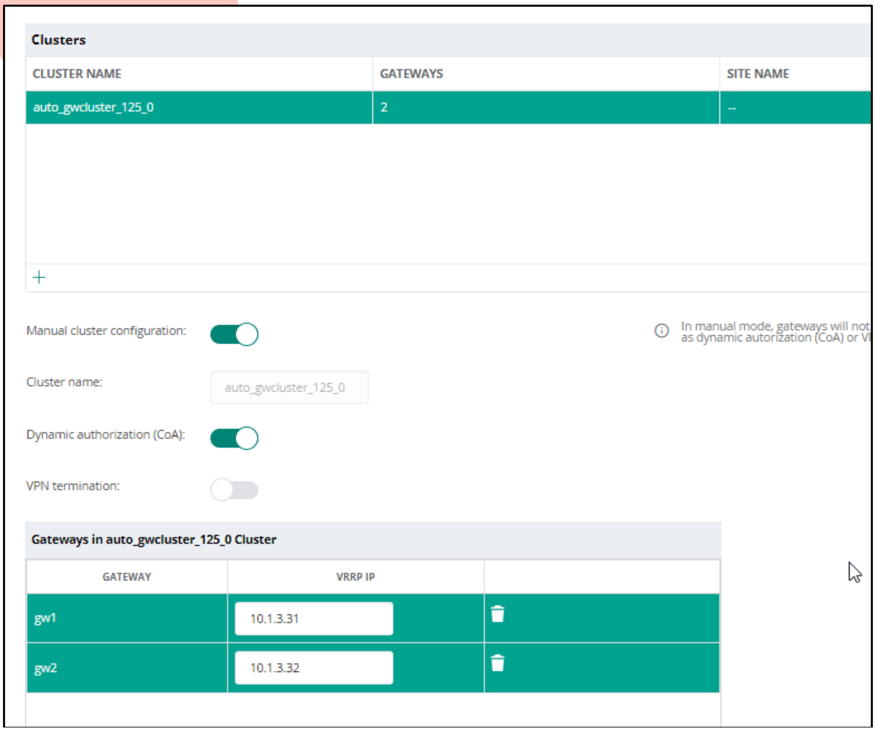
28. Move the slider for Automatic setting to **Disabled**.
29. Read the warning messages and confirm.



IMPORTANT: Make sure you realize that any gateways that are added to this group in the future will not be automatically part of this cluster. You must manually add them to the cluster configuration on this page!

30. Select the **auto_gwcluster_#...#** in the list.
31. Enable the **Manual cluster** configuration slider.
32. Enable Dynamic Authorization (CoA).
33. Set the VRRP IP address in the table.

- gw1: **10.1.3.31**
- gw2: **10.1.3.32**



IMPORTANT: Pay attention, the order of the gateways in the list may be reversed! Enter the correct VRRP IP for each GW!

34. Set **VRRP VLAN** to **3**.
35. Leave the VRRP ID at its default.

NOTE: The default VRID starting range is 220. If this would conflict with your existing network setup, you can manually enter a VRID start ID. You will need as many VRIDs as you have gateways in your cluster.

36. Click **Save Settings**.

Verify the Virtual NAS IP Address

Once the configuration has been pushed to the gateways, they will automatically enable the VRRP process and each become conductor for their VRRP address.

37. Use MGMT PC to open an SSH session to the gateway your contractor user is tunneled to.

TIP: In Aruba Central you can use the client details page to see on which gateway the client is connected.

38. Review the VRRP status.

```
show vrrp
```

NOTE: After the configuration has been pushed from Aruba Central, the gateway will need some time to process and activate the VRRP changes. If you don't see any VRRP instances yes, try again after about 1 minute.

Example output:

```
(gw2) # show vrrp
Virtual Router 220:
Description
Admin State UP, VR State BACKUP
IP Address 10.1.3.31, MAC Address 00:00:5e:00:01:dc, vlan 3
Priority 235, Advertisement 1 sec, Preemption Enable Delay 0
Auth type NONE ********
tracking is not enabled

Virtual Router 221:
Description
Admin State UP, VR State MASTER
IP Address 10.1.3.32, MAC Address 00:00:5e:00:01:dd, vlan 3
Priority 255, Advertisement 1 sec, Preemption Enable Delay 0
Auth type NONE ********
tracking is not enabled
```

39. You can also review the VRRP address in the IP interface brief list.

```
show ip interface brief
```

```
(gw2) # show ip interface brief
Interface                   IP Address / IP Netmask        Admin    Protocol   VRRP-IP
vlan 3                       10.1.3.22 / 255.255.255.0     up       up
10.1.3.31

10.1.3.32
loopback                    unassigned / unassigned        up       up
```

The gateways will now use their active VRRP address as the NAS IP for any new client authentication sessions.

Test the Cluster VRRP NAS IP

40. On PC4, disconnect and reconnect the contractor client to the p#tx-employee WLAN.

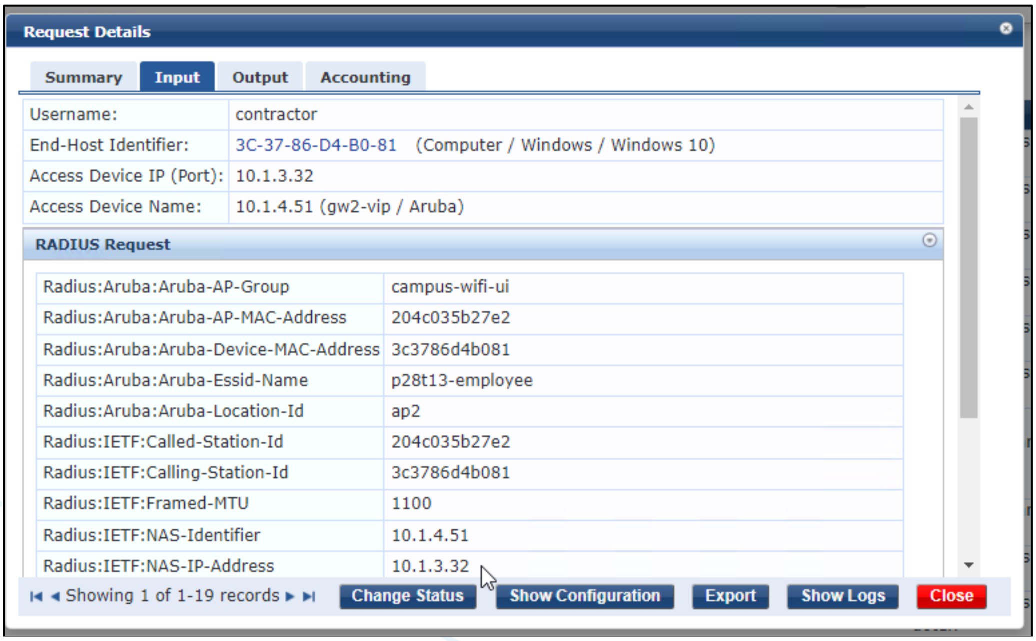
NOTE: You could also use a disconnect using ClearPass, but the Wireless client in the lab does not always respect the 'automatically reconnect' option.

Therefore, the manual disconnect and reconnect is recommended here.

41. On MGMT PC, use the ClearPass session to review the NAS IP address in the latest session.

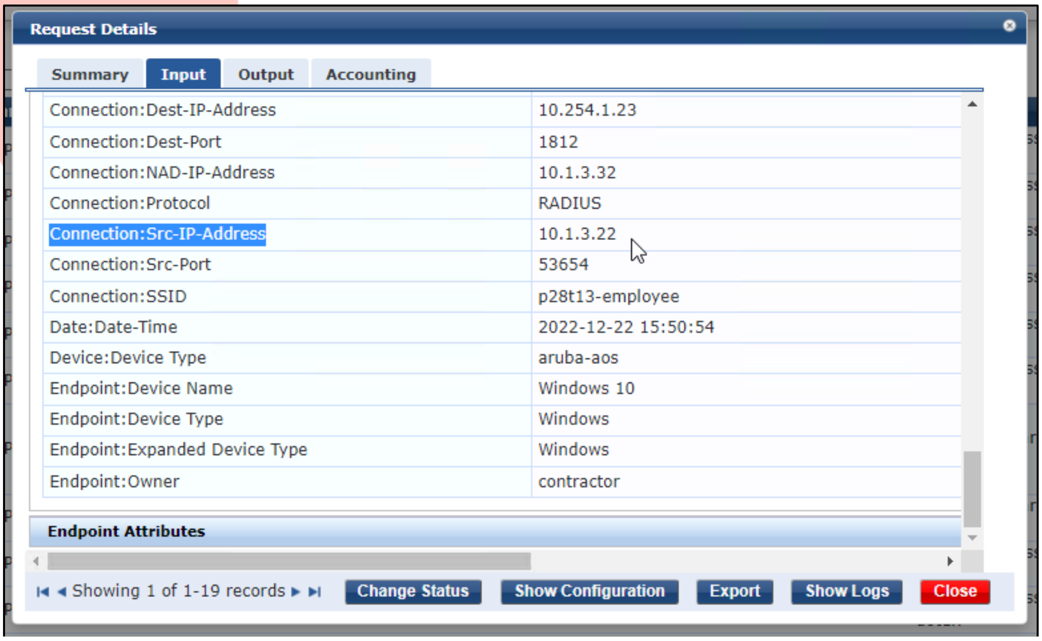
#	Server Name	Source	NAS IP Address	NAS Port	Host MAC Address	Username
1.	P58-T01-CPPM	RADIUS	10.1.3.32	0	3C-37-86-D4-B0-81	contractor
2.	P58-T01-CPPM	RADIUS	10.1.3.22	0	3C-37-86-D4-B0-81	contractor

42. Click the latest entry to open it.
43. On the Input page, expand the **RADIUS Request** section.



- **Question**: What is the NAS IP address as reported by the gateway?
- **Answer**: The VRRP Address is now used as the NAS IP address.

44. Scroll down and expand the **Computed Attributes** section.



- **Question**: What is the Connection Src-IP-Address as seen by ClearPass?
- **Answer**: The RADIUS packet is still sent with the original GW source IP address. Only the NAS-IP-Address attribute in the RADIUS header is changed to the VRRP address.

45. This completes the cluster dynamic authorization configuration support.

Optional Test of the Dynamic Authorization

You may optionally test the CoA:

46. Open a console session to both gateways
47. Reboot the gateway that is currently used by the contractor client.

```
reload
```

TIP: Use **show user** on each gateway to check the user table.

48. While that gateway is rebooting, switch to the console of the other gateway.
49. Verify the client is connected to this gateway now.

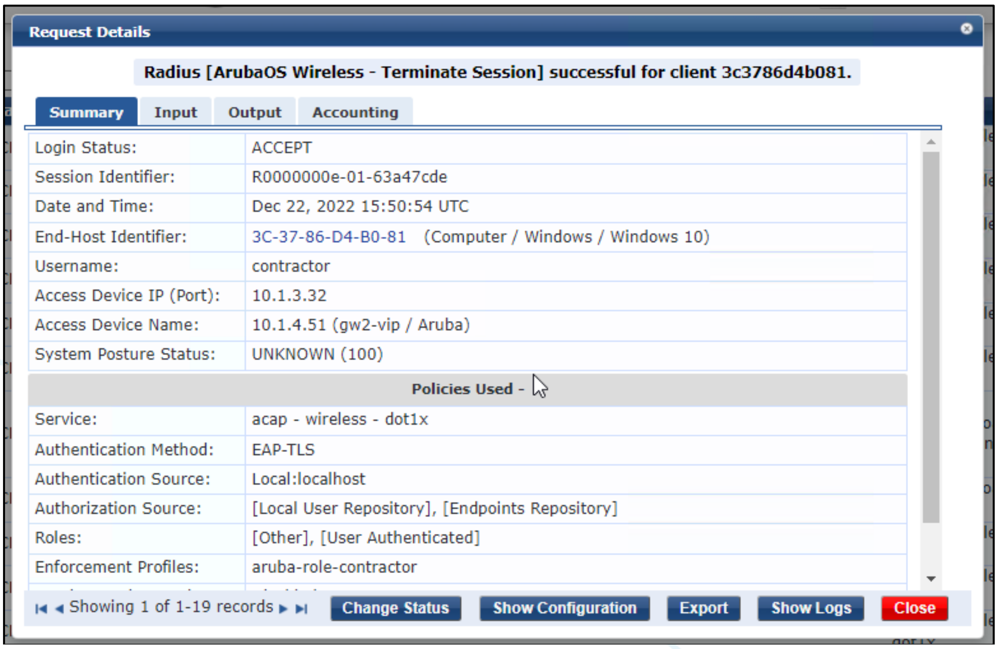
```
show user
```

50. It may take some time for the other gateway to initiate the reboot. Wait until the user shows in the user table.
51. Verify the VRRP IP is now active on this gateway.

```
show vrrp
(gw1) *# show vrrp
```

```
Virtual Router 220:
Description
Admin State UP, VR State MASTER
IP Address 10.1.3.31, MAC Address 00:00:5e:00:01:dc, vlan 3
Priority 255, Advertisement 1 sec, Preemption Enable Delay 0
Auth type NONE ********
tracking is not enabled

Virtual Router 221:
Description
Admin State UP, VR State MASTER
IP Address 10.1.3.32, MAC Address 00:00:5e:00:01:dd, vlan 3
Priority 235, Advertisement 1 sec, Preemption Enable Delay 0
Auth type NONE ********
tracking is not enabled
```

52. While the original gateway is rebooting, use ClearPass to send the Dynamic Authorization message for the contractor client. Even though the original gateway is offline, the message should still succeed.



End of the optional test section.

Optional Task 6: Server Rule based Role Derivation

In some customer environments, the RADIUS server may be managed by a different team, and it may be difficult to configure the Aruba-User-Role on the RADIUS server.

In this case you may need to adjust the Aruba gateway configuration to map a RADIUS attribute from the existing setup to an Aruba-User-Role.

This is known as server-based rule derivation.

In this task, you will create a new rule to map the RADIUS standard Filter-ID attribute to an Aruba-User-Role.

Objectives

- Configure server rules for role derivation

Steps

ClearPass Configuration

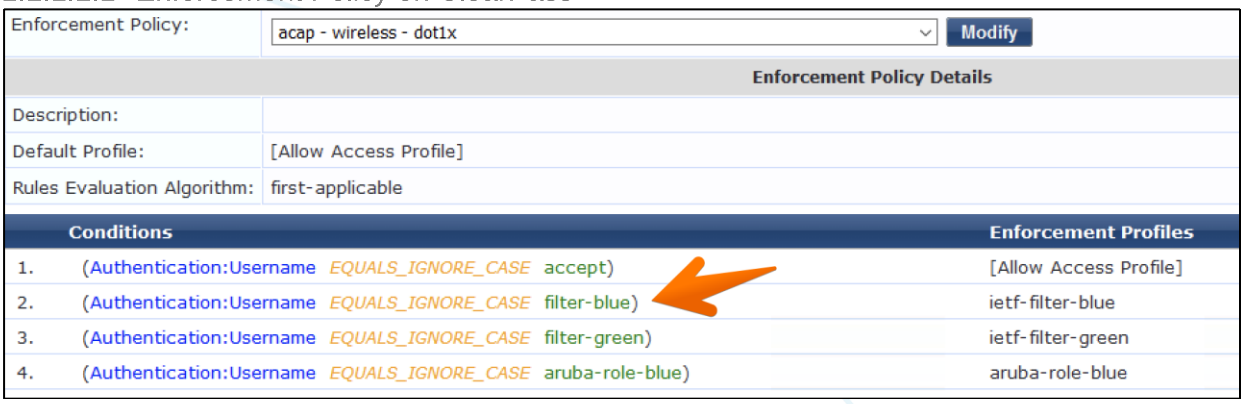
This section simply shows the prepared ClearPass configuration, there are no action steps in this section.

You will be testing the server rules using a new test user account:

- Username **filter-blue**
- Password **Aruba123!**

The ClearPass server has been configured with an enforcement policy to return the RADIUS IETF attribute Filter-Id with a value of blue for this test user account.

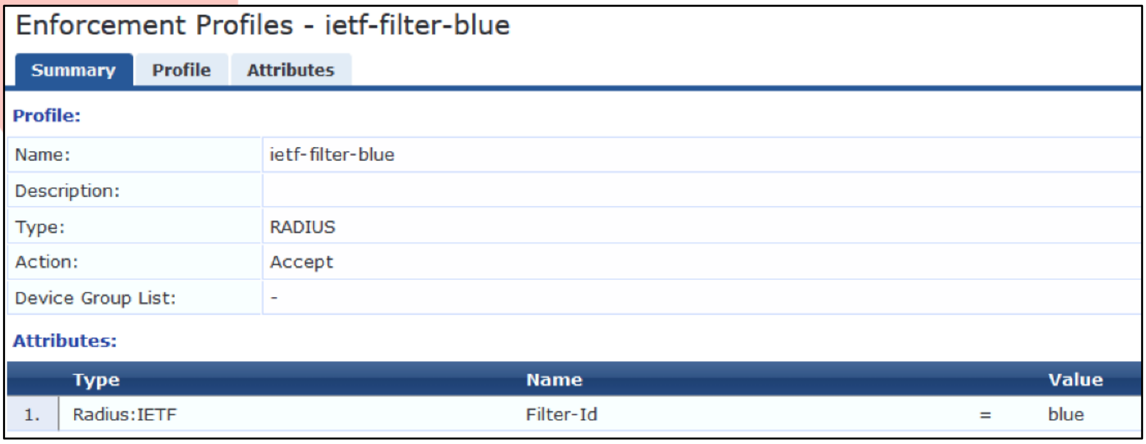
1.1.1.1.1 Enforcement Policy on ClearPass



Enforcement Policy:	acap - wireless - dot1x (Modify)
Enforcement Policy Details	
Description:	
Default Profile:	[Allow Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authentication:Username EQUALS_IGNORE_CASE accept)	[Allow Access Profile]
2.	(Authentication:Username EQUALS_IGNORE_CASE filter-blue)	ietf-filter-blue
3.	(Authentication:Username EQUALS_IGNORE_CASE filter-green)	ietf-filter-green
4.	(Authentication:Username EQUALS_IGNORE_CASE aruba-role-blue)	aruba-role-blue

1.1.1.1.2 Enforcement Profile on ClearPass



Enforcement Profiles - ietf-filter-blue

Summary | Profile | Attributes

Profile:

Name:	ietf-filter-blue
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

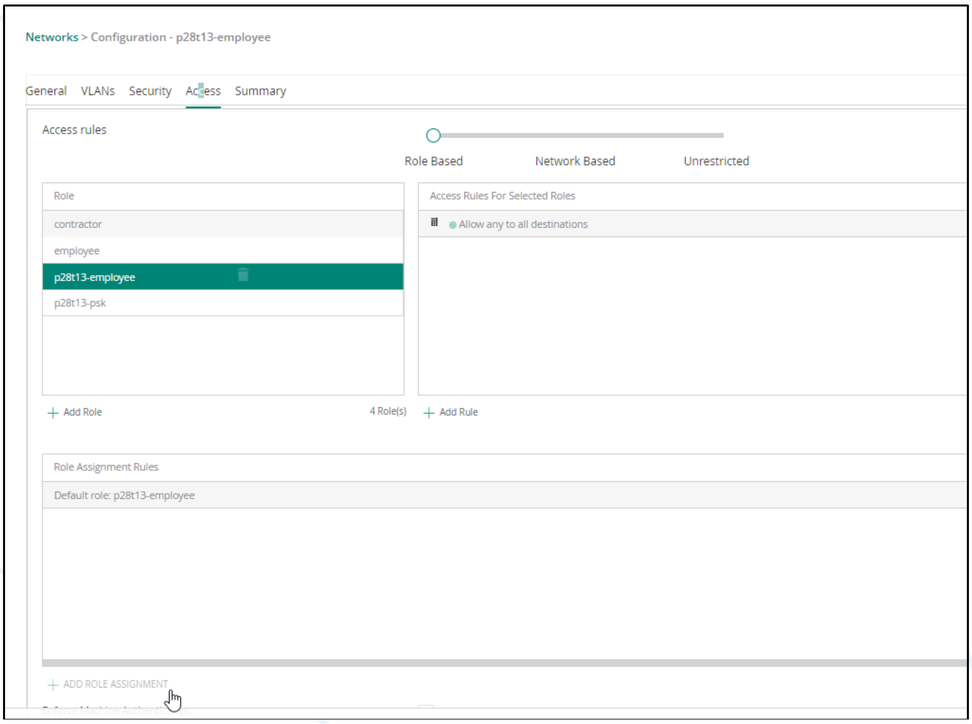
	Type	Name		Value
1.	Radius:IETF	Filter-Id	=	blue

Configure a Custom Role Derivation Based on a Filter-id

In this section, you will configure the p#tx-employee WLAN make a new role assignment rule.

When the **filter-id** has a value of **blue**, the user role **contractor** will be assigned.

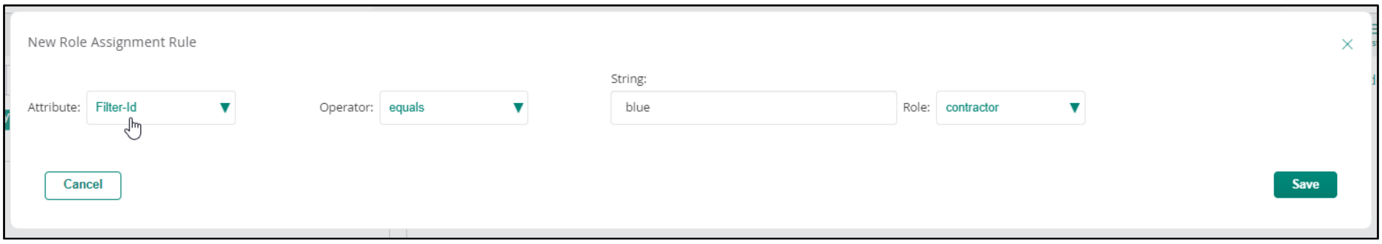
1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
2. Edit the WLAN **p#tx-employee**.
3. Navigate to the **Access** page.
4. Change the slider to **Role Based**.
5. Click **Add Role Assignment**.



6. Configure the rule with these settings:

- **If:**
    - Attribute: **filter-id**
    - Operator: **equals**
    - String: **blue**

- **Then assign**
    - Role: **contractor**



7. Click **Save**.

> **TIP:** Remember a role assignment rule is not required to use the Aruba-User-Role VSA. This is the typical and recommended method to assign the user roles in an Aruba solution.

8. Click **Save Settings**.
9. Wait for the wizard to complete, then click **OK**.

Verify Gateway Configuration

First you will check the audit trail to see the generated configuration.

10. In Aruba Central, navigate to Context: **Global** > Navigation: **Audit Trail**.
11. Click the **three dots** to see the generated configuration for the latest gateway Configuration entry.

In the generated configuration, this snippet applies the server rule in the gateway configuration:

```
aaa server-group p28t13-employee_#1671624128149_37#__auth_svg
no load-balance
auth-server cppm1 position 1
set role condition Filter-Id equals blue set-value contractor
```

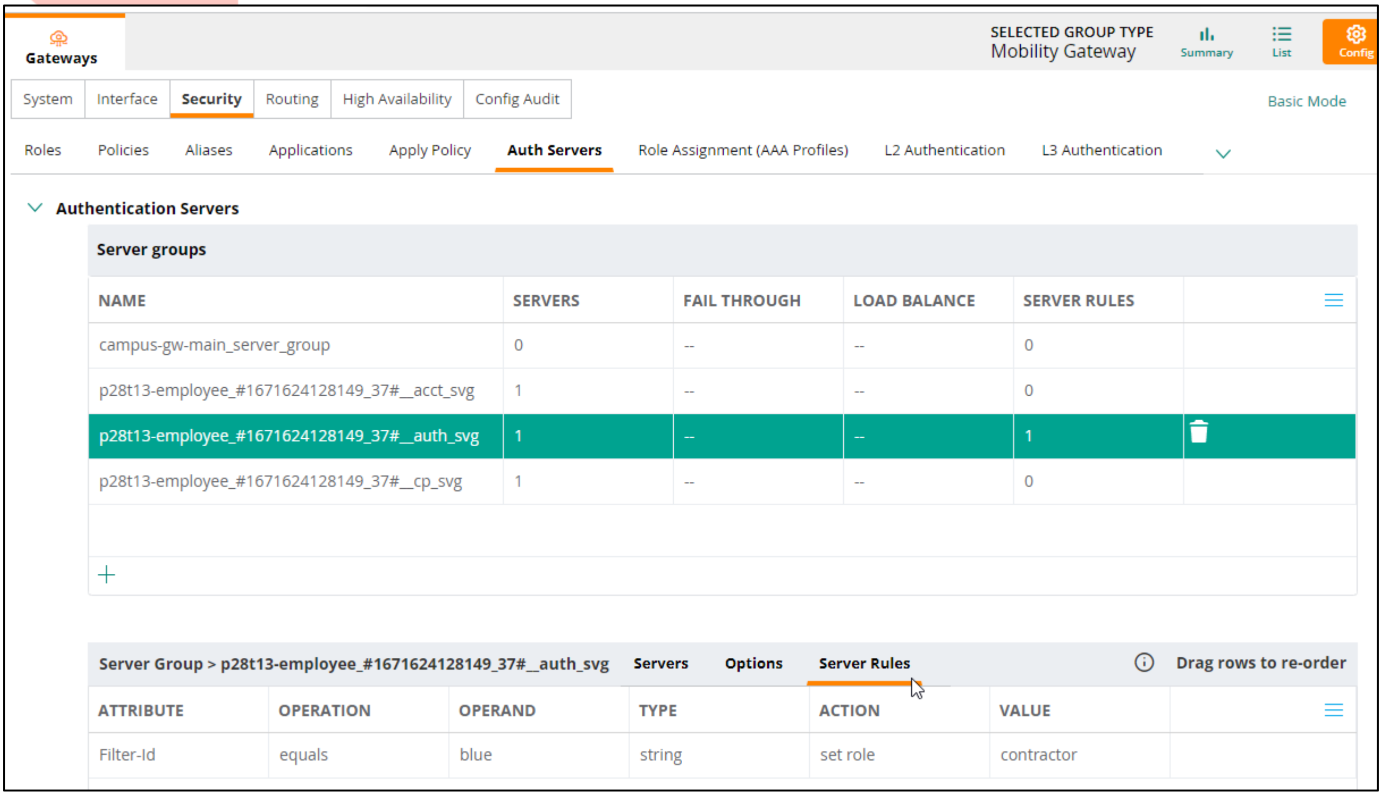
12. **Close** the audit entry.

Now you can verify the UI configuration of the gateways.

13. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config (gear icon)**.
14. Navigate to **Security > Auth Servers**.
15. Click **p#tx-employee…auth_svg** (Authentication Server Group).

TIP: You may need to resize the Name column or hoover with the mouse over the name to see the full name.

16. Click **Server Rules**.

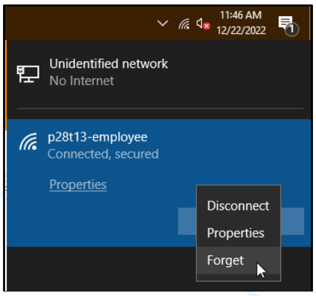


- **Question**: Do you see any rules?
- **Answer**: Yes, the WLAN wizard applied the custom role assignment rule on the gateway as a server rule on the authentication server group.

Verify the Configuration

To test the configuration, you can connect with PC4 with a user account filter-blue / Aruba123!

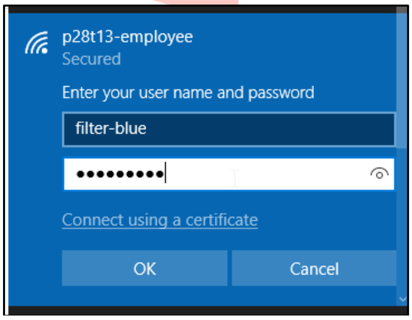
17. Open PC4, use the option to **Forget** the wireless network, this ensures the existing access credentials are cleared.



NOTE: The client certificate is still installed on the client.

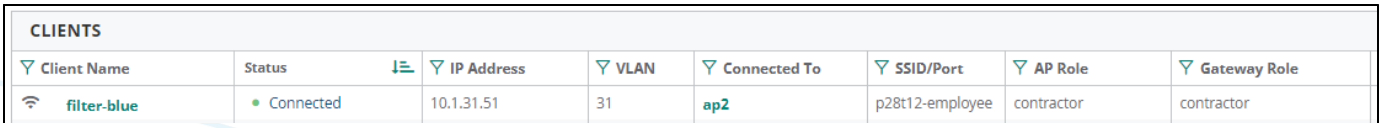
18. Use PC4 to connect to the p#**tx-employee** WLAN.
19. When prompted for credentials, use these credentials:

- Username: **filter-blue**
- Password: **Aruba123!**



NOTE: Do *not* use the certificate option for this test.

20. Accept the warning for the certificate.
21. Verify the client is connected.
22. In Aruba Central, navigate to Context: **Global** > Navigation: **Clients**.
23. Verify the client named *filter-blue* is connected and has the role *contractor* assigned.



CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role
filter-blue	Connected	10.1.31.51	31	ap2	p28t12-employee	contractor	contractor

24. Open a console/SSH connection to the gateway that is used by the client PC4.
25. On the GW, review the PC4 client IP address (user filter-blue).

```
show user
```

26. Review the user details, use the include filter to limit the output to only Role.

```
show user ip 10.1.31.xyz | include Role
```

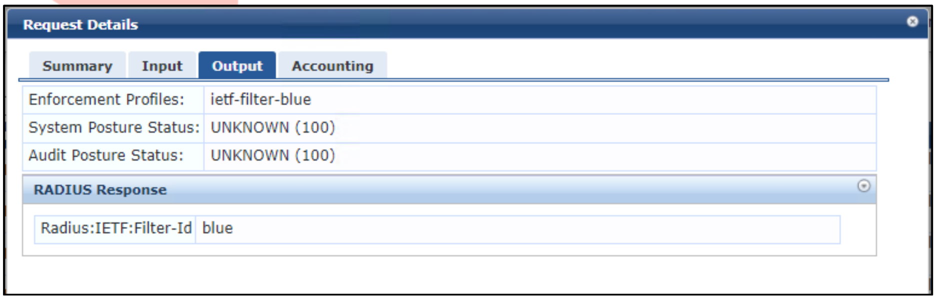
```
(gw2) # show user ip 10.1.31.51 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: contractor (how: ROLE_DERIVATION_DOT1X_VSA), ACL: 103/0
Role Derivation: ROLE_DERIVATION_DOT1X_VSA
```

- **Question**: What is the role derivation method?
- **Answer**: The derivation method is ROLE_DERIVATION_DOT1X_VSA. This is the same method as the Aruba-User-Role VSA, since it is based on an authentication server attribute.

27. Use MGMT PC to connect to ClearPass with admin / Aruba123!

https://10.254.1.23/tips

28. Navigate to **Monitoring > Live Monitoring > Access Tracker**.
29. Open the latest authentication event with username **filter-blue**.
30. Open the **Output** tab and expand the **RADIUS Response**.



- **Question**: Did ClearPass return any Aruba VSA?
- **Answer**: No, only the IETF standard attribute of Filter-id was used. The gateway server rule translated this to the correct user role when the client was authenticated.

Cleanup

31. On PC4, **forget** the p#tx-employee WLAN.
32. Connect again to the **p#tx-employee** WLAN using the already installed contractor certificate.

You have completed this Lab!

Lab 06.01 Overlay Guest WLAN with ClearPass Guest

Overview

In this lab you will create a tunnel guest WLAN with an external captive portal page. A captive portal page is also referred to as the splash page.

The ClearPass captive portal page has been preconfigured in this lab environment, in the first task you will review the configuration that was applied to this captive portal page.

Then you will configure a new AOS 10 tunnel WLAN and enable the captive portal function using the ClearPass external captive portal page.

When you connect with the client to this guest WLAN, you will explore the different user roles that are used for the pre- and post-authentication access.

In the last section, you will enable MAC authentication on the guest WLAN. This will enable support for MAC caching and ensures guest devices can be allowed to bypass the captive portal after they have completed the initial captive portal authentication.

Objectives

After completing this lab, you will be able to:

- Verify the ClearPass captive portal page configuration.
- Create an AOS 10 WLAN with external captive portal.
- Understand the different roles used for captive portal
- Integrate the guest WLAN with ClearPass MAC caching.

Task 1: Verify a ClearPass Guest page

In this task you will review the existing guest page configuration on the ClearPass Guest server.

Objectives

- Understand the URL of a ClearPass guest page.
- Understand the NAS Vendor Settings on the ClearPass guest page for a default AOS 10 AP.

Steps

Review the ClearPass Guest Page

In these steps you will connect to ClearPass and review the preconfigured guest captive portal page.

1. On the MGMT PC, open a command prompt and ping to cppm.aruba-training.com

```
ping cppm.aruba-training.com
```

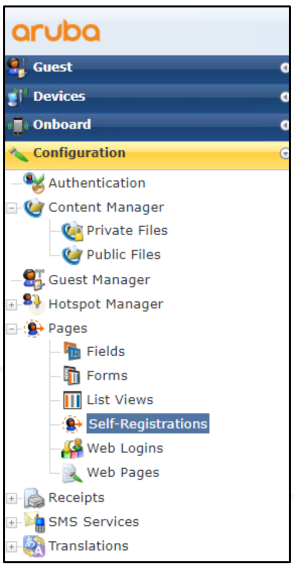
- **Question**: What is the IP address for this host?
- **Answer**: The name resolves to IP address 10.254.1.23. This is the IP address of the ClearPass server.

2. On the MGMT PC, open a browser to ClearPass to:

https://cppm.aruba-training.com/guest

> **NOTE:** The FQDN cppm.aruba-training.com is only available inside the remote lab environment.

3. Login with username **admin** / password **Aruba123!**
4. On the left side, open the section **Configuration** > **Pages** > **Self-Registrations**.



- **Question**: What are the page names you see in the list?
- **Answer**: There is a **Guest Self-Registration** and **acaa-wifi** page. The **acaa-wifi** was created for this training lab.

5. Click the **acaa-wifi** entry. Some action buttons will appear under the line.

6. Click **Launch** to see an example of the self-registration page. Pay attention to click *Launch*, **<u>not</u>** *Launch Self-Service* or *Launch Login*.

NOTE: You should ***not*** enter any credentials in the web form at this point, since you are connected using the MGMT PC; you are not using a guest client PC now!

- **Question**: What is the full URL of the page?
- **Answer**: The full URL is https://cppm.aruba-training.com/guest/acaa-wifi.php. Take note of this URL, you will need this URL for the Guest WLAN redirect page configuration.

NOTE: ClearPass is using a server certificate that was signed by a private lab CA in this lab environment.

- **Question**: What is the FQDN used to reach the ClearPass Guest URL?
- **Answer**: The FQDN is cppm.aruba-training.com.

7. After the preview, you may **Close** the preview web page.

NAS Vendor Settings

On the external captive portal server (ClearPass), the administrator needs to provide the hostname to which the guest browser will submit the guest credentials.

The AOS 10 APs are by default configured with a public signed certificate with subject name of *securelogin.hpe.com*.

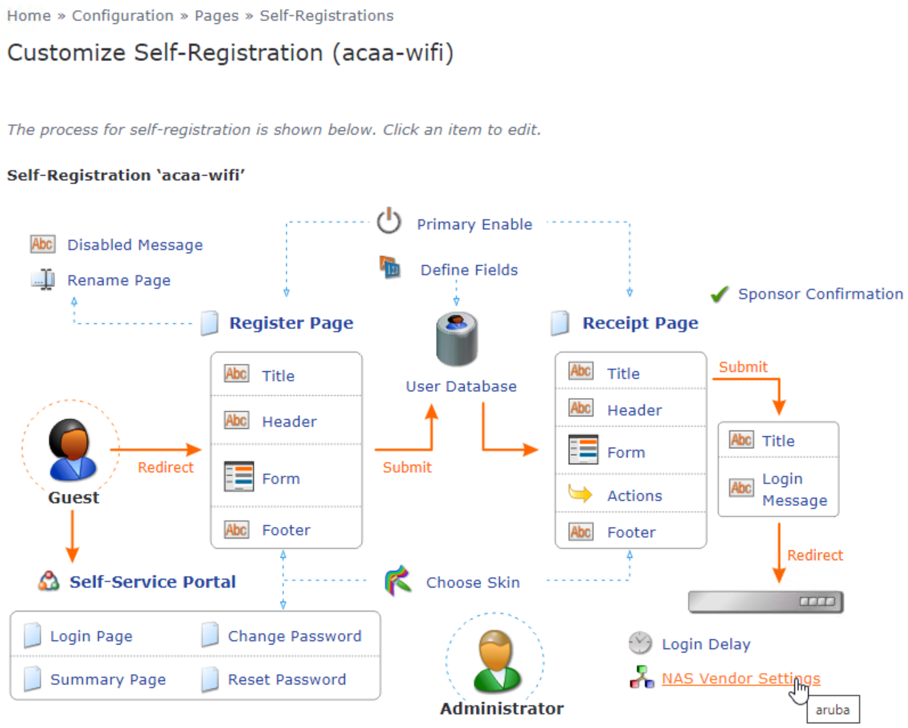
This is automatically installed and configured by Aruba Central on the AOS 10 APs, no user action is required.

The captive portal administrator only needs to refer to this name in the captive portal configuration.

In the next steps you will review that this information has been configured on the guest captive portal page.

8. In the Self-Registrations list, click **Edit** for the *acaa-wifi* page.

9. On the customize self-registration page, click **NAS Vendor Settings**.



10. Review the value that has been set in the *Address* field.

This value must match the captive portal certificate name that has been installed on the APs. In this lab setup, it matches the AOS 10 default - the public certificate with subject name of *securelogin.hpe.com*.

This concludes the ClearPass page review. You may close the web browser on MGMT PC.

Task 2: Configure WLAN Profile with ClearPass Guest Splash Page

In this task you will configure the APs with a guest tunnel WLAN profile. This WLAN will use the ClearPass splash page that you have just reviewed in the previous task.

Objectives

- Enable guest captive portal on a WLAN.
- Configure the external splash page with a ClearPass guest page.

Steps

Create the Guest CPPM WLAN

1. In Aruba Central, navigate to

Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > Right top: **Config**

2. On the WLAN page, click **Add SSID**.
3. On the **General** page, in the **Name** field, enter **p#tx-guest-cppm**.

NOTE: Make sure to replace the # value with your Pod number and x with your table number.
For example, if you are using table 07 in pod 28, your WLAN name will be

p28t07-guest-cppm

This represents p(od) 28 and t(able) 07.

Check with your instructor if you are not sure about the Pod and Table number.

4. Click **Next.**
5. On the **VLANs** page, select **Tunnel**.
6. For **Primary Gateway Cluster**, select your cluster from the list.
7. Click **Show Named VLANs**.
8. Click **Add Named VLAN**.
   - Name: **guests**
   - ID: **35**
9. Verify that the Client VLAN Assignment is set to **Static**.
10. Set the VLAN ID to **guests(35)**.
11. Click **Next** to move to the Security page.

Configure the External Captive Portal

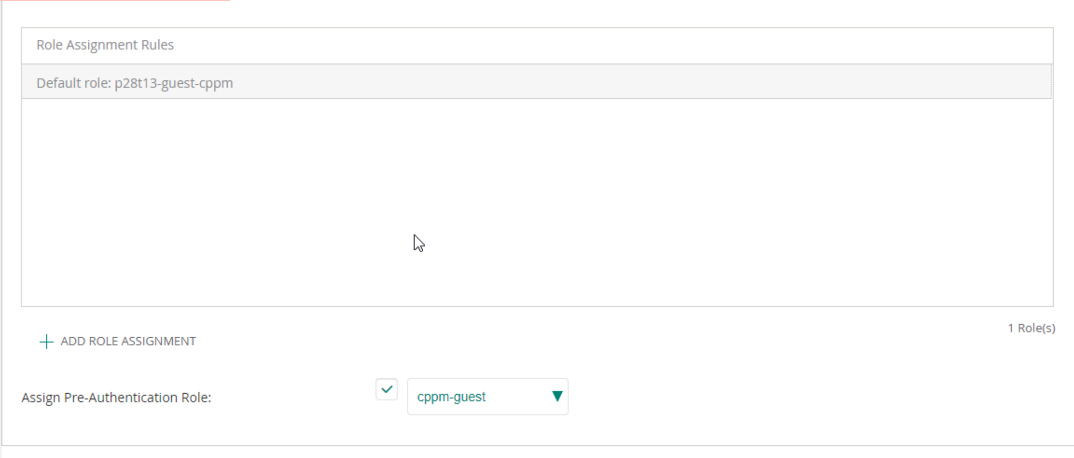
In the next steps you will define the ClearPass guest page as an external captive portal.

12. On the *Security* page, move the **Security Level** slider to **Visitors**.
13. Set the *Type* to **External Captive Portal**.
14. For the *Captive Portal Profile*, use the **+** button to add a new profile.
15. In the **External Captive Portal New** window enter these settings:
    - Name: **cppm-guest**
    - IP or hostname: **cppm.aruba-training.com**
    - URL: **/guest/acaa-wifi.php**
    - Port" leave the default as **443**
16. Click **OK** to save the profile.
    - **Question**: Why did you configure cppm.aruba-training.com as the hostname?
    - **Answer**: This is the DNS name that was registered in the lab environment for the ClearPass guest server.
    - **Question**: Why are you using /guest/acaa-wifi.php as the URL name?
    - **Answer**: You have reviewed on ClearPass guest the Splash Page. Based on the launch example, you have seen that the page name was /guest/acaa-wifi.php. You need to update this field to match the page name of the ClearPass system.
17. In the **Captive Portal Profile** field, verify **cppm-guest** is now selected.
18. For Primary server, select **cppm1**.
    - **Question**: When was this RADIUS server created?
    - **Answer**: You created the cppm1 RADIUS server during the Employee WLAN lab activity.
19. Open **Advanced Settings** > **Accounting**.
20. Set the **Accounting** to **Use Authentication Servers**.
21. Click **Next** to continue to the Access page.

Authenticated Guest Access Control

Using the Access Control, you can control the level of network access that the guest users will have on the network. In this example, some basic restrictions will be applied.

22. On the *Access* page, make sure the slider is set to **Role Based**.



- **Question**: What is the default role that will be assigned to authenticated clients?
- **Answer**: The default role is based on the SSID name: p#tx-guest-cppm. This is, by default, the post-authentication role for the guest users.
- **Question**: What is the role assigned for pre-authentication role?
- **Answer**: The role name is cppm-guest. This is based on the external captive portal name you have used during the wizard.
- Make sure authenticated guests can only reach the host 10.254.1.21 (for any service) and block traffic to all other 10.0.0.0/8 IP addresses.

You can do this by modifying the post-authentication role, this is the SSID default role p#tx-guest-cppm.

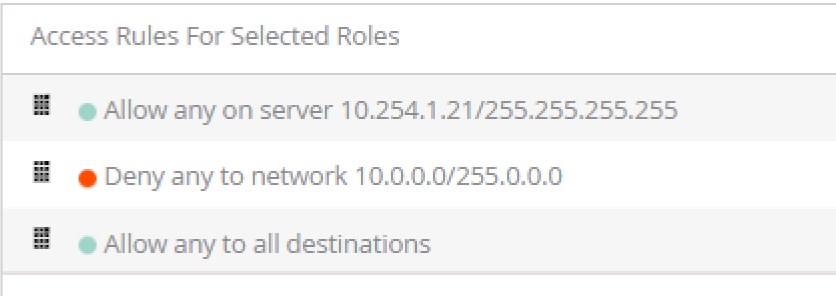
23. Select the **p#tx-guest-cppm** user role.

> **IMPORTANT:** This is **not** the *cppm-guest* role, but **p#tx**-guest-cppm (based on the WLAN name).

24. Click **Add rule** and create a rule with these settings:
    - Type: **Access Control**
    - Services: **Any (default)**
    - Action: **Deny**
    - Destination: **network** IP: **10.0.0.0** netmask: **255.0.0.0**
25. Click **OK** to save the rule.
26. Click **Add rule** and create a rule with these settings:
    - Type: **Access Control**
    - Services: **Any** (default)

- Action: **Allow** (default)
- Destination: Particular server **10.254.1.21**

27. Click **OK** to save the rule.
28. Verify the allow access to 10.254.1.21 is listed before the deny to the 10.0.0.0/8 network.



29. Click **Next** to move to the Summary page.
30. On the *Summary* page, click **Finish**.
31. After a few moments, click **OK** to confirm the success configuration message.

Task 3: Test ClearPass Guest access

In this task you will use a wireless client to test the guest access. You will review the user roles that are used for the pre-authentication and post-authentication and explore the status of the client in Aruba Central and on the gateway.

Objectives

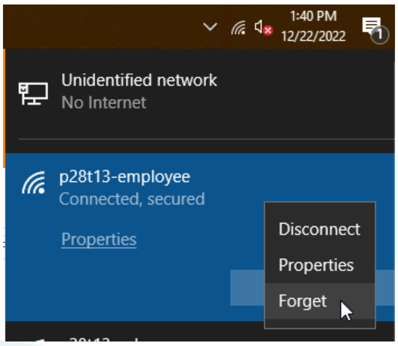
- Test the access to a guest WLAN with external captive portal.
- Review the user roles used by the guest clients.
- Review the user table on the gateway and the AP.

Steps

Make the WLAN Connection

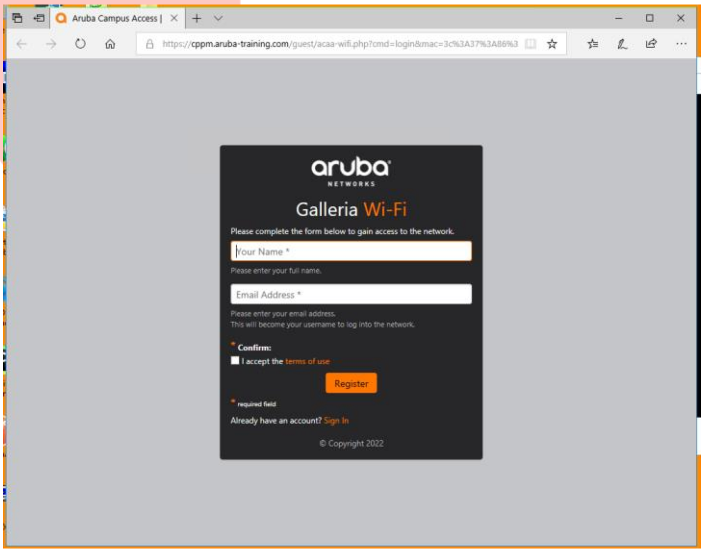
In these steps you will connect to the guest-cppm WLAN, but you will ***not login*** yet.

1. Open a connection to PC4.
2. On PC4, **forget** the p#tx-employee network.



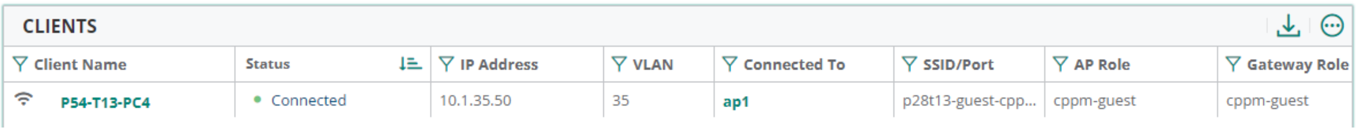
3. Make a connection to your guest CPPM WLAN: p**#**t**x**-guest-cppm.

> **NOTE:** A Microsoft Edge browser page will pop up at this point, **do not log in** at this point. You will first explore the status of the client during the pre-authentication phase.



4. In Aruba Central, navigate to

Context: **Groups / campus-wifi-ui** > Navigation: **Clients**



CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role
P54-T13-PC4	Connected	10.1.35.50	35	ap1	p28t13-guest-cpp...	cppm-guest	cppm-guest

NOTE: It may take 1-2 minutes to see the updated information in Central. Use the refresh button to see the latest status.

- **Question**: What is the status of the PC4 client?
- **Answer**: The client state is connected.
- **Question**: What is the assigned AP and gateway role?
- **Answer**: The role name is **cppm-guest**. This role was created during the WLAN wizard and was based on the external captive portal profile name you have used in the wizard. Since the client has not completed authentication yet, this is referred to as the pre-authentication role.

5. Click the *client name* to access the client details page.

Take note of the AP and GW your client is connected to.

- **AP:** ________________
- **GW:** ________________

6. On PC4, open a command prompt (**cmd.exe**) and verify the hostname **securelogin.hpe.com** is handled by the AP.

```
ping securelogin.hpe.com
```

```
C:\Users\student> ping securelogin.hpe.com

Pinging securelogin.hpe.com [172.31.98.1] with 32 bytes of datAnswer:
Reply from 172.31.98.1: bytes=32 time=6ms TTL=63
```

- **Question**: Did you have to register the hostname securelogin.hpe.com in a DNS server?
- **Answer**: No. This public certificate is by default installed when an AOS 10 AP is managed by Aruba Central and configured as the AP captive portal certificate. The AP will inspect all DNS requests and it will automatically spoof the response when it sees a DNS request with this name.
- **Question**: Did you have to configure the 172.31.98.1 IP address on the AP?
- **Answer**: No, this IP address is automatically configured on VLAN 3333 of every AP. This is an internal VLAN, sometimes referred to as the *magic* VLAN on the AP.

7. Open a console connection to the AP where the client is connected.
8. Review the IP interface brief output.

a Hewlett Packard Enterprise company

```
show ip interface brief
```

```
ap1# show ip interface brief
Interface                          IP Address / IP Netmask       Admin  Protocol
br0                                 10.1.4.50 / 255.255.255.0    up     up
br0.3333                          172.31.98.1 / 255.255.254.0    up     up
```

- **Question**: What are the two IP interfaces listed on the AP?
- **Answer**: The br0 and br0.3333. br0 is the interface used for the native VLAN uplink management IP address. br0.3333 is the internal VLAN 3333 that is used for the captive portal server IP address.

9. Use the MGMT PC to open an SSH connection to the gateway that PC4 is tunneled to.
10. Review the user table, take note of the PC4 guest IP address.

```
show user-table
```

```
(gw2) #show user-table

Users
-----
    IP           MAC              Name          Role         Age(d:h:m)  Auth  VPN link
Connected To      Roaming   Essid/Bssid/Phy    Profile
Forward mode   Type   Host Name   User Type
----------  ------------      ------        ----         ----------  ----  --------
-----
10.1.35.50  3c:37:86:d4:b0:81  3c3786d4b081  cppm-guest  00:00:19
20:4c:03:8c:27:42   Wireless  p28t13-guest-cppm  p28t13-guest-
cppm_#1671732616072_37#_  dtunnel                          WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/2 Free:0/1 Dyn:1 AllocErr:0 FreeErr:0
```

- **Question**: What is the listed for the Auth column?
- **Answer**: The Auth column is empty, since the client did not perform any authentication (not MAC, 802.1X or captive portal). The client will still be assigned the initial role based on this information.

11. Check the role derivation details and filter on the **Role** text, using the IP address of the client.

```
show user ip 10.1.35.xyz | include Role
```

```
(gw2) #show user ip 10.1.35.50 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: cppm-guest (how: ROLE_DERIVATION_INITIAL_ROLE), ACL: 111/0
```

```
Role Derivation: ROLE_DERIVATION_INITIAL_ROLE
```

- **Question**: What is the role derivation method for the guest user to receive the Pre-Authentication role?

- **Answer**: The method is ROLE_DERIVATION_INITIAL_ROLE. This is the initial role on the AAA profile.

Guest Login to the ClearPass Captive Portal

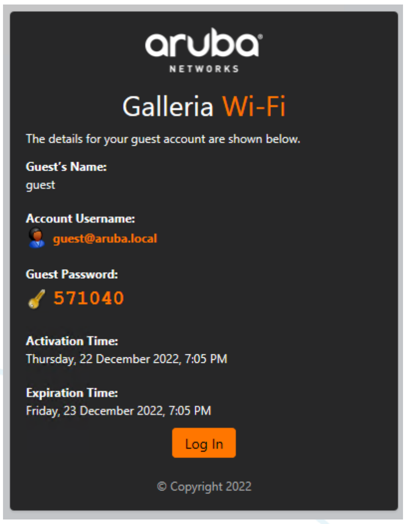
In these steps you will login to the captive portal page.

12. On the PC4, complete the guest self-registration form

- Full name: **guest**
- Email: **guest@aruba.local**

13. Click the **I accept** checkbox and click **Register** to create a new account.

14. A new guest account is now created, and the details will be displayed.



15. Click **Log In** to connect to the network.
16. You should now have access to the internet.

After the successful authentication, the browser will redirect you to the configured welcome page.

17. Switch to the SSH connection of the gateway.
18. Review the client and the role details.

```
show user-table
```

```
(gw2) # show user-table

Users
-----
    IP          MAC            Name              Role               Age(d:h:m)  Auth
VPN link     Connected To     Roaming   Essid/Bssid/Phy    Profile
Forward mode  Type  Host Name  User Type
----------  ------------      ------             ----               ----------  ----
--------  ------------------  -------  ---------------    -------
------------  ----  ---------  ---------
10.1.35.50  3c:37:86:d4:b0:81  guest@aruba.local  p28t13-guest-cppm  00:00:23    Web
20:4c:03:8c:27:42   Wireless  p28t13-guest-cppm  p28t13-guest-
cppm_#1671732616072_37#_  dtunnel                        WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/2 Free:0/1 Dyn:1 AllocErr:0 FreeErr:0
```

- **Question**: What is the listed as the Auth method for the client?
- **Answer**: Web. This indicates captive portal authentication.
- **Question**: Did the client submit its credentials to the web/captive portal on the Gateway?
- **Answer**: No, the guest credentials were posted to the AP captive portal. The AP then forwarded these guest credentials using a RADIUS access-request to the Gateway. The gateway knows this request is a web/captive portal request based on the RADIUS Service-Type that the AP has assigned in the Access Request.
- **Question**: What is the user role that was assigned to the authenticated guest?
- **Answer**: The role name is p#tx-guest-cppm, this is the default SSID role, the role name is based on the WLAN name. This role is assigned because it is the default role that is set on the captive portal profile of the Gateway. The RADIUS server can override this role, but in this lab setup, the RADIUS server returns a basic Access-Accept (without Aruba-User-Role authorization). Since the RADIUS server does not include a user role, the captive portal default role is applied.

19. Review the client details

```
show user ip 10.1.35.50 | include Role
```

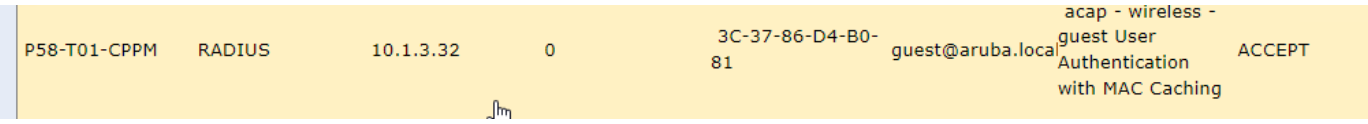
```
(gw2) # show user ip 10.1.35.50 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: p28t13-guest-cppm (how: ROLE_DERIVATION_CP), ACL: 105/0
Role Derivation: ROLE_DERIVATION_CP
```

- **Question**: What is the role derivation method for the post-authenticated client?
- **Answer**: ROLE_DERIVATION_CP. This is the default role that was set on the captive portal profile for the client.

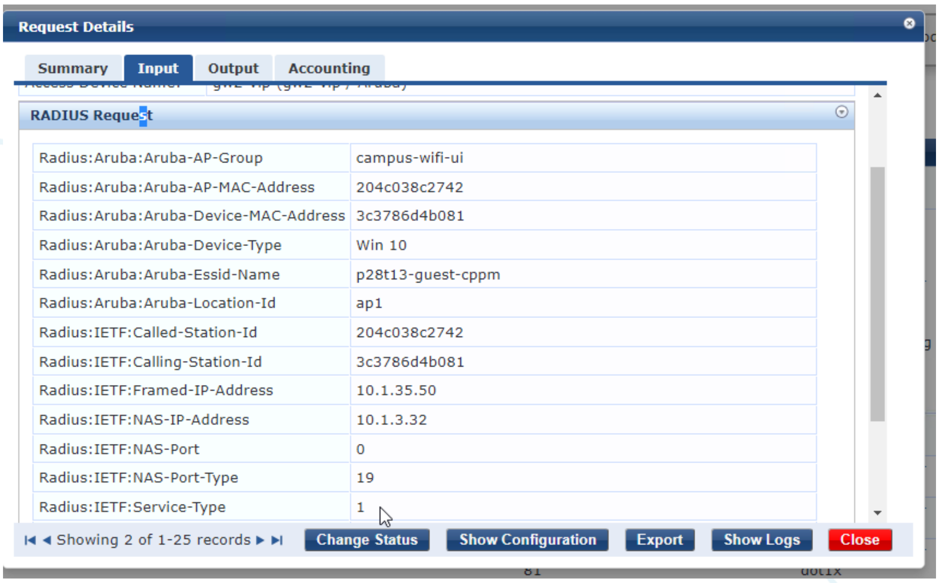
Review the Captive Portal User Login Service Type

In the next steps, you will review the service type that is used in the RADIUS Access-Request for the captive portal authentications.

20. Use the MGMT PC to access the ClearPass Access Tracker.
21. Click the latest guest login event and click the **Input** tab.



22. In the RADIUS Request section, look for the Service-Type value.



- **Question**: What is the value for the captive portal login service type?
- **Answer**: 1. This is the service type named *Login*. Based on this service type, the Gateway reports that a Web captive portal authentication is used.

Verify the Client Connection

In these steps you will check the updated client status in Aruba Central after the guest login has completed.

23. In Aruba Central, navigate to

Context: **Groups / campus-wifi-ui** > Navigation: **Clients**

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role
guest@aruba.local	Connected	10.1.35.50	35	ap1	p28t13-guest-cp...	p28t13-guest-cppm	p28t13-guest-cppm

NOTE: It may take a minute before you see the updated client information and username in Aruba Central. Use the refresh button to get the latest status.

- **Question**: What is the guest client name now?
- **Answer**: The client's name changed from the original hostname to the username that was entered during the self-registration. If you used guest@aruba.local, this will be shown as the Client name.
- **Question**: What is the AP role for this user?
- **Answer**: The AP user role is p#tx-guest-cppm. After ClearPass returns a RADIUS accept to the GW, the GW assigned the captive portal default role.

This completes the guest WLAN with ClearPass Guest configuration.

Task 4: Guest Authentication with ClearPass MAC Caching

Guest authentication enables the guest to login to the network, but the client will need to login on the portal again after an offline period.

Using MAC caching, the client MAC address can be cached by the RADIUS server. When the client returns after an offline period, it can be authorized on the network based on MAC authentication. This avoids a new captive portal login for the guest.

The ClearPass system has been configured to support MAC caching already. You need to configure the Gateway to use MAC authentication on the guest WLAN.

Objectives

- Enable MAC authentication on the guest WLAN.
- Verify the MAC caching function.
- Recognize the difference between web (captive portal) and MAC authentication in the user table.

Steps

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
2. Under the WLAN list, edit the **p#tx-guest-cppm** WLAN.
3. On the **Security** page, expand the **Advanced settings**.
4. Set *MAC Authentication* to **enabled**.

> **NOTE:** You don't have to select a separate RADIUS server, since you have selected the primary server already as cppm1 for the external captive portal user authentication.

5. Expand **Accounting**. Verify the *cppm1* server is listed as **Accounting Server 1**.
6. Click **Save Settings**.

> **NOTE:** Enabling MAC Authentication on the WLAN only changes the Gateway configuration. The AP was already using MAC Authentication to send client requests to the Gateway.

Review the Authentication on the Gateway

In the next steps you will connect to the gateway and review the authentication method in the user table.

7. Use the MGMT PC to open an SSH connection to the gateway associated with your PC4 client.
8. Review the active client authentication, the initial captive portal authentication will be reported as *Web*.

```
show user-table
```

```
(gw2) # show user-table

Users
-----
    IP            MAC              Name                Role                Age(d:h:m)  Auth
VPN link      Connected To      Roaming   Essid/Bssid/Phy     Profile
Forward mode  Type  Host Name  User Type
----------  ------------       ------              ----                ----------  ----
--------  ------------------  -------   ---------------    -------
------------  ----  ---------  ---------
10.1.35.50  3c:37:86:d4:b0:81  guest@aruba.local  p28t13-guest-cppm  00:00:31    Web
20:4c:03:8c:27:42   Wireless  p28t13-guest-cppm  p28t13-guest-
cppm_#1671732616072_37#_  dtunnel                        WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/2 Free:0/1 Dyn:1 AllocErr:0 FreeErr:0
```

9. Disconnect the user using the aaa user delete command.

```
aaa user delete all
```

```
(gw2) # aaa user delete all
```

10. On your PC4, verify you are still connected to the guest WLAN. You should not have to login again on the captive portal.

> **NOTE:** The lab wireless clients do not always reconnect automatically, therefore a manual check is included in the steps.

11. On the gateway session, review the active clients again.

```
show user-table
```

```
(gw2) # show user-table

Users
-----
    IP            MAC              Name          Role                Age(d:h:m)  Auth  VPN
link      Connected To      Roaming   Essid/Bssid/Phy     Profile
Forward mode  Type  Host Name  User Type
----------  ------------       ------        ----                ----------  ----  ---
-----  ------------------  -------   ---------------    -------
------------  ----  ---------  ---------
10.1.35.50  3c:37:86:d4:b0:81  3c3786d4b081  p28t13-guest-cppm  00:00:00    MAC
20:4c:03:8c:27:42   Wireless  p28t13-guest-cppm  p28t13-guest-
cppm_#1671732616072_37#_  dtunnel                        WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/3 Free:0/2 Dyn:1 AllocErr:0 FreeErr:0
```

- **Question**: What is the *Auth* method now?
- **Answer**: The client is authenticated with the MAC-auth method.

12. Review the client details for your client IP.

```
show user ip 10.1.35.xyz | include Role
```

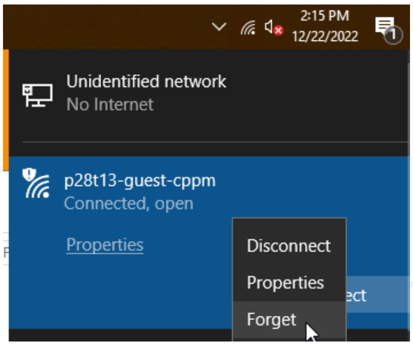
```
(gw2) # show user ip 10.1.35.50 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: p28t12-guest-cppm (how: ROLE_DERIVATION_MBA), ACL: 110/0
Role Derivation: ROLE_DERIVATION_MBA
```

- **Question**: What is the role derivation method now?
- **Answer**: The method is ROLE_DERIVATION_MBA. The role is derived from MAC-based authentication.

Cleanup

You have completed the guest access.

13. On PC4, **forget** the p#tx-guest-cppm network.



Optional Task 5: Web Redirect for a Corporate User

In some deployments, the network administrator wants to use the captive portal redirect function for other use cases than just guest access.

For example, a customer may have some 802.1X authenticated clients that need to be redirected to ClearPass OnGuard or Onboard or to perform device profiling.

In this task, you will configure the contractor role with a custom redirect page. When the contractor connects, it will be redirected to the ClearPass posture status page.

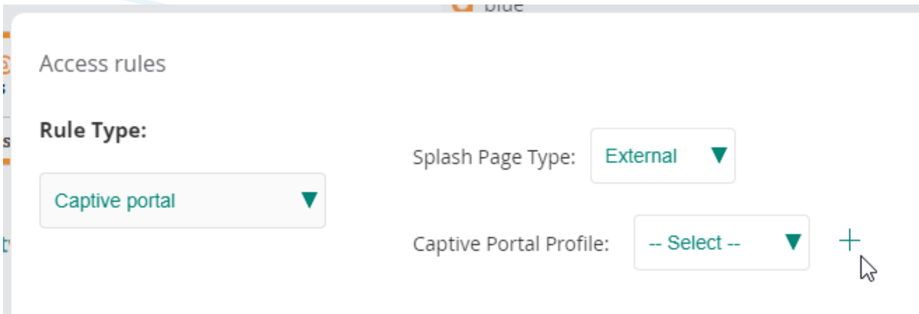
Objectives

- Configure web redirect for a role used in a corporate WLAN.
- Verify the redirect function.

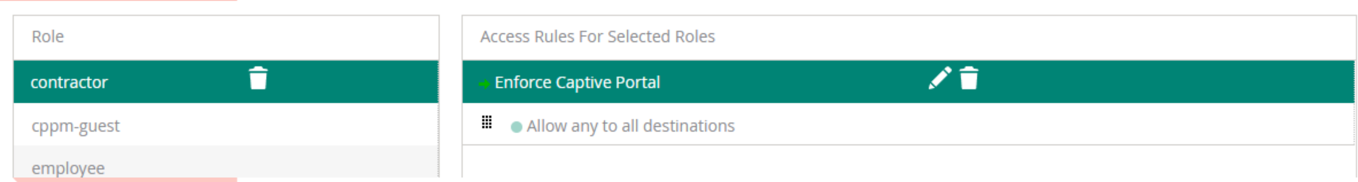
Steps

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
2. **Edit** the WLAN p#tx-employee.
3. Open the **Access** Page, make sure the slider is set to **Role Based**.
4. Select the role **contractor**.
5. Click **Add rule**.

- Type: **Captive Portal**
- Splash page: **External**



6. For the *Captive Portal Profile*, click the **+** button to create a new profile.
7. Use these settings for the new profile:
    - Name: **cppm-posture**
    - IP: **cppm.aruba-training.com**
    - URL: **/guest/posture_check.php**
8. Click **OK**.
9. Review contractor role rules. Verify that it contains the *Enforce Captive Portal* policy.



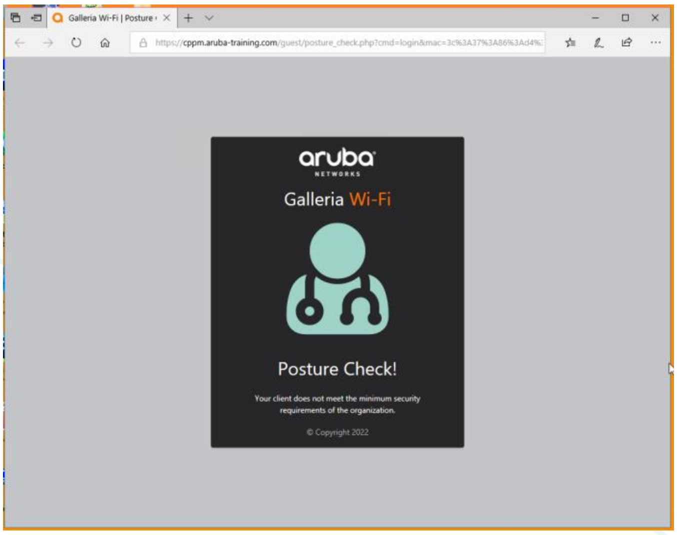
NOTE: The required ACLs to redirect the HTTP(S) traffic are automatically configured in the role for you.

10. Click **Save Settings**.
11. Click **OK** after the wizard has completed.

Verify the Configuration

You will verify the configuration using PC4.
It should use the installed contractor certificate to authenticate with EAP-TLS.

12. Use **PC4** to connect to your **p#tx-employee** WLAN.
13. Click **Connect using a certificate**.
14. Verify the PC is automatically redirected to the posture page.



Cleanup

Remove the Enforce Captive Portal rule from the contractor role.

15. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config (gear icon)**.
16. Edit the **p#tx-employee** WLAN.
17. Navigate to the **Access** page.
18. Open the Access page and make sure the slider is set to **Role Based**.
19. Select the role **contractor**.
20. Delete the rule **Enforce Captive Portal**.

21. Confirm with **Yes**.
22. Click **Save Settings**.
23. On PC4, **forget** the WLAN p#tx-employee.

You have completed this Lab!

Lab 07.01 PSK IOT WLAN

Overview

In this lab you will configure a tunnel WLAN with WPA2 multiple pre-shared key (MPSK) local feature.

The MPSK local feature allows you to configure multiple PSKs in the WLAN configuration, and each PSK can optionally be bound to a user role. This will be configured in the first task of this lab.

In the second task, you will explore how the MPSK key name can be sent to ClearPass and the role assignment (authorization) can be performed by ClearPass.

Objectives

After completing this lab, you will be able to:

- Configure a tunnel PSK WLAN.
- Configure MPSK local on a tunnel WLAN.
- Assign a user role to an MPSK entry.
- Understand how the MPSK key name can be sent to ClearPass for authorization purposes.

Task 1: Create MPSK Local Overlay WLAN

In a previous lab you have created the PSK WLAN.

In this task you will enable Multiple PSKs on the PSK WLAN:
- Default key: **Aruba123!**
- Key for iot-sensor-air devices: **Sensorair123!**

You want to ensure that any device that connects with the *Sensorair123!* PSK is assigned the user role *iot-sensor-air*.

This allows you to apply specific access controls to these devices by configuring this user role when needed.

In this task you will only apply the role assignment, the access control configuration of roles has been covered in the previous lab activities.

Objectives

- Create a MPSK tunnel WLAN.
- Create MPSK local list.
- Assign a user role to an MPSK role.

Steps

Create a New User Roles Called iot-sensor-air

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
2. On the WLAN page, edit the **p#tx-psk** WLAN.
3. On the *Access* page, make sure the slider is set to **Role Based**.
4. Click **Add Role** and assign it a name: **iot-sensor-air**.

> **NOTE:** The default rule set includes *Allow any* to all destinations. This is fine for the lab setup.

5. Click **OK**.
6. Click **Save Settings**.
7. Click **OK** when the wizard completes.

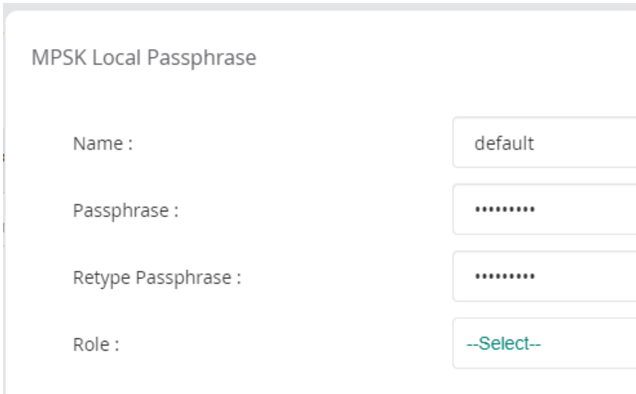
Define MPSK Local List

In the next steps you will configure an MPSK Local key list. This list will be bound to the p#tx-psk WLAN security.

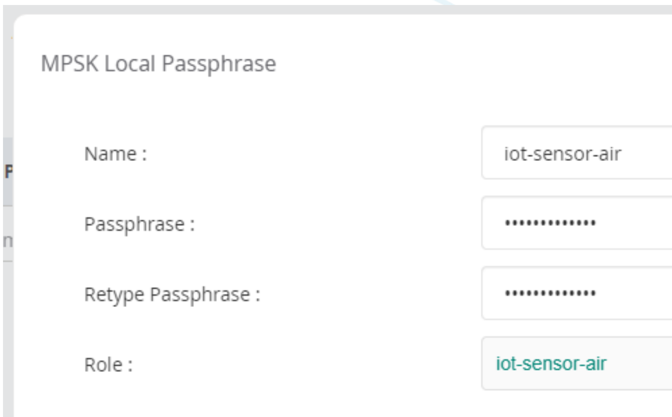
It will replace the existing PSK. If you have an existing key set on the PSK, you can include that existing key in the key list as well.

In this lab setup, you will add this existing PSK Aruba123! to the list to provide support for the existing clients.

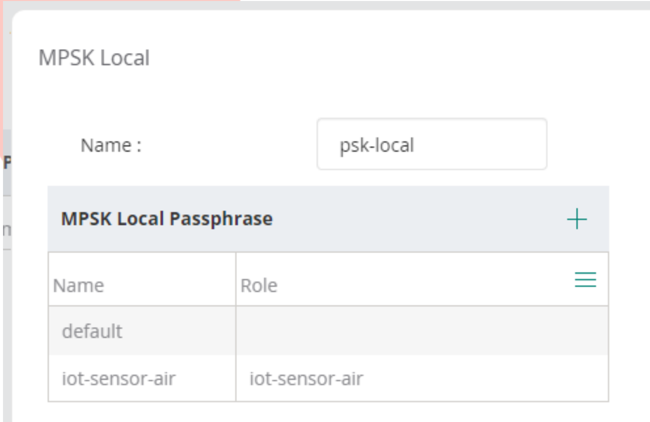
8. Under Security, expand **MPSK Local**.
9. Use the **+** button to add a new **MPSK Local** key list with a name of **psk-local**.
10. Use the **+** button to add a new PSK to the list.
    - Name: **default**
    - Passphrase: **Aruba123!**
    - Role: leave unselected (default).



11. Click **OK**.
12. Use the **+** button to add a new MPSK Local key list.
    - Name : **iot-sensor-air**
    - Passphrase : **Sensorair123!**
    - Role: **iot-sensor-air**



13. Click **OK**.
14. Review the MPSK local key list.



15. Click **OK**.
16. Click **Save Settings**.

Apply the MPSK Rule Set to the WLAN

In the next steps, you will assign the MPSK rule set to the PSK WLAN that was previously created.

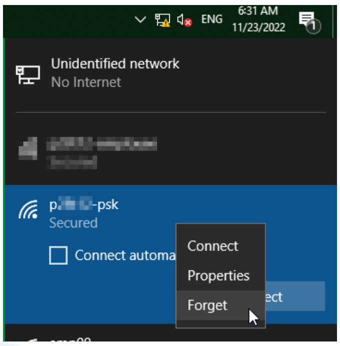
17. On the **WLAN** page, edit the **p#tx-psk** WLAN.
18. On the Security page, set *Key Management* to **MPSK Local**.

> **NOTE:** MPSK Local is only supported with WPA2.

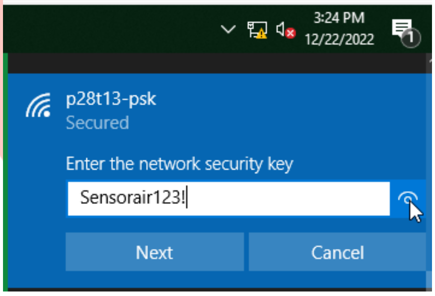
19. For the *MPSK Local* value, set it to **psk-local**. This is the name of the key list you have created.
20. Click **Save Settings**.

Test with PC1 and PC4

> **NOTE:** PC1 and PC4 may have connected previously to the PSK WLAN. Make sure to **forget** the network first, then you can connect with the new key.



21. Use *PC1* to connect to your **p#tx-psk** WLAN; use the key **Sensorair123!**



22. Use *PC4* to connect to your **p#tx-psk** WLAN; use the key **Aruba123!**
23. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > **Clients**

CLIENTS

	Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role
	P54-T13-PC4	Connected	10.1.34.51	34	ap1	p28t13-psk	p28t13-psk	p28t13-psk
	P54-T13-PC1	Connected	10.1.34.50	34	ap1	p28t13-psk	iot-sensor-air	iot-sensor-air

- **Question**: What user roles are assigned to the PC1 and PC4?
- **Answer**: PC1 is assigned the role iot-sensor-air as the gateway role *and* the AP role. PC4 is connected with a PSK (Aruba123!) that doesn't have a linked role. Therefore, it will use the *initial* role, which is the SSID default role, based on the name of the WLAN.

Review the Role Status on the Gateway

24. Use the MGMT PC to open an SSH session to the gateway of the client.

NOTE: PC1 and PC4 may be assigned to different gateways, you should make a connection to both in that case.

25. Review the user list to see the IP address.

```
show user-table
```

```
(gw2) # show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP          MAC            Name          Role        Age(d:h:m)  Auth  VPN link
Connected To     Roaming  Essid/Bssid/Phy  Profile                          Forward
mode  Type  Host Name  User Type
----------  ------------      ------        ----        ----------  ----  --------
------------------  -------   ---------------  -------                         ------
------  ----  ---------  ---------
10.1.34.51  3c:37:86:d4:b0:81  3c3786d4b081  p28t13-psk  00:00:02
20:4c:03:8c:27:42   Wireless  p28t13-psk      p28t13-psk_#1671553563764_37#_
dtunnel                          WIRELESS
```

```
(gw1) *# show user
This operation can take a while depending on number of users. Please be patient ....
```

```
Users
-----
    IP          MAC            Name          Role            Age(d:h:m)  Auth  VPN
link     Connected To     Roaming   Essid/Bssid/Phy  Profile
Forward mode  Type  Host Name  User Type
----------  ------------  ------        ----            ----------  ----  ------
--  ------------------  -------  ---------------  -------                       --
----------  ----  ---------  ---------
10.1.34.50  3c:37:86:d4:91:42  3c3786d49142  iot-sensor-air  00:00:02
20:4c:03:8c:27:42   Wireless  p28t13-psk      p28t13-psk_#1671553563764_37#_
dtunnel                       WIRELESS
```

26. Review the user role derivation based on the client IP.

```
show user ip 10.1.34.50 | include Role
```

```
(gw1) *# show user ip 10.1.34.50 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: iot-sensor-air (how: ROLE_DERIVATION_USER_RULE), ACL: 113/0
Role Derivation: ROLE_DERIVATION_USER_RULE
```

```
show user ip 10.1.34.51 | include Role
```

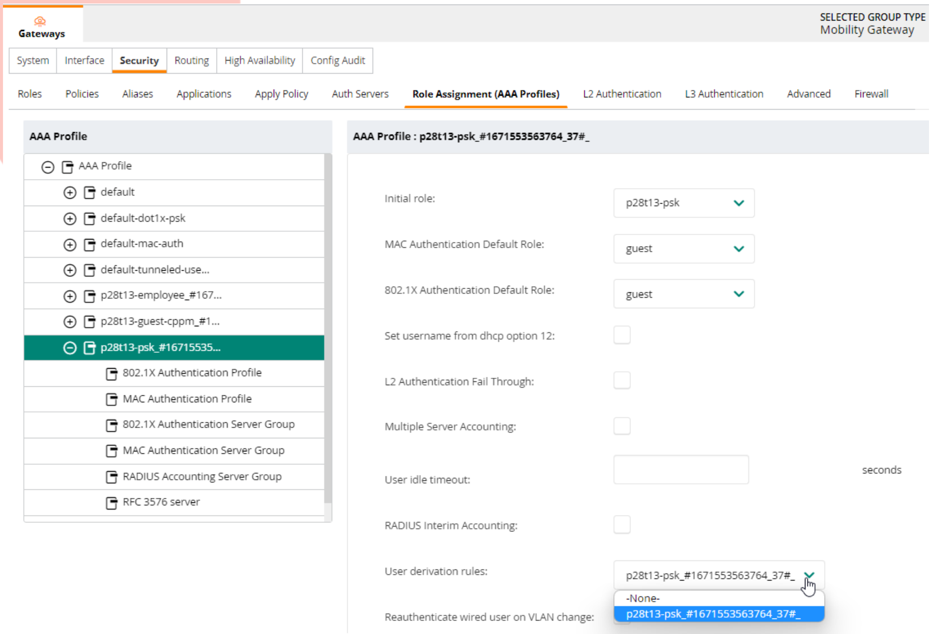
```
(gw2) # show user ip 10.1.34.51 | include Role
This operation can take a while depending on number of users. Please be patient ....
Role: p28t13-psk (how: ROLE_DERIVATION_INITIAL_ROLE), ACL: 99/0
Role Derivation: ROLE_DERIVATION_INITIAL_ROLE
```

- **Question**: What are the Role derivation methods used for these clients?
- **Answer**: PC1 is assigned the role iot-sensor-air based on the ROLE_DERIVATION_USER_RULE. This means a user derivation rule was used to apply the role. You will review this configuration in the next steps. PC4 is assigned the role p#tx-psk (default) based on the ROLE_DERIVATION_INITIAL_ROLE. This means the AAA profile initial role is applied.

Review the Gateway User Derivation Rules

In the next steps you will review the configuration that was applied to the gateways based on the MPSK Local rule set.

27. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
28. Navigate to **Security > Role Assignment (AAA Profiles)**.
29. Expand **AAA Profiles** and select the AAA Profile that begins with **p#tx-psk_#...**



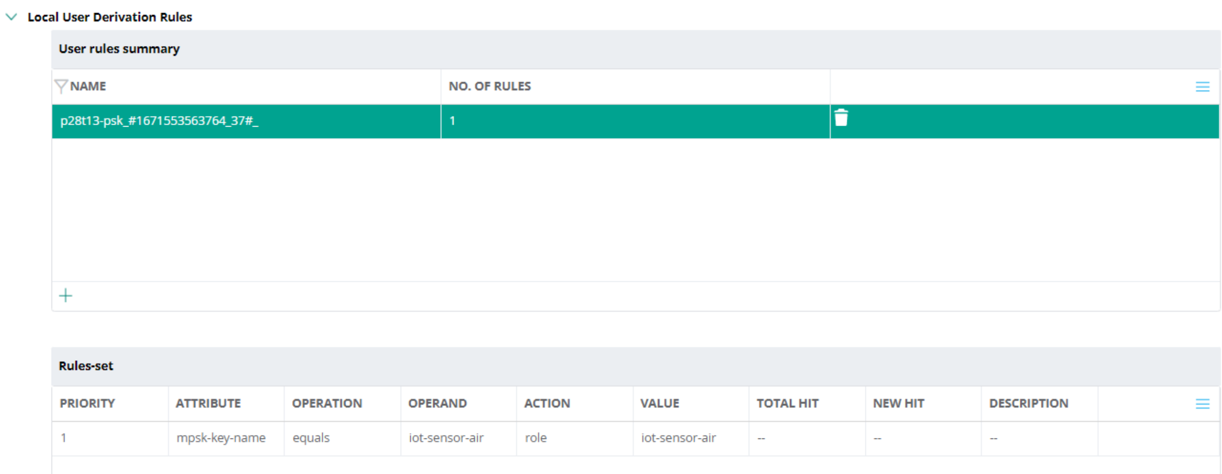
- **Question**: In the AAA profile, what is setting for user derivation rules (UDRs)?
- **Answer**: A UDR rule set is active. The name is based on the AAA profile name *p#tx-psk-#..#.*

Let's review this UDR.

30. Navigate to **Security > Advanced**.

NOTE: If the Security page would not be visible, click **Show Advanced** at the top right.

31. Expand **Local User Derivation Rules**.
32. Click the generated UDR to see the rules.



- **Question**: What is the configuration of the generated rule?

- **Answer**: If **mpsk-key-name equals iot-sensor-air**, then apply **role iot-sensor-air**. This is the translation of the MPSK Local entry that had a role mapping on the gateway side.

This concludes the MPSK local configuration with local role assignment task.

Task 2: Configure ClearPass-based Role Mapping for MPSK

In this task you want to use ClearPass to authorize the MAC addresses that connect to the PSK WLAN. Therefore, you will enable MAC authentication on the PSK WLAN.

You will configure a new PSK to support HVAC air conditioning IoT devices.

Using ClearPass, you want to make sure that any device that connects using the key **Airco123!** (the key with the name *iot-ac*), is automatically assigned the user role *iot-ac*.

While this looks like the previous task, the fact that ClearPass is involved means you can also check on the client MAC address or other endpoint attribute information. If some other (non-HVAC MAC address) device would connect using this PSK, ClearPass could assign a different user role, for example.

ClearPass has been preconfigured for this task:

- All MAC addresses that connect to the PSK will be accepted.
- Any connection that uses the PSK key name iot-ac will be assigned the user role iot-ac.

Objectives

- Understand how the MPSK key name can be sent to ClearPass for authorization purposes.

Steps

Update the MPSK Local List with the iot-ac

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
2. Navigate to the *Security* page, expand **MPSK Local**.
3. Edit the **psk-local** list.
4. Use the **+** button to add a new key.
5. Configure the new key with these settings:
   - Name: **iot-ac**
   - Passphrase: **Airco123!**
   - Role: Leave unselected (the role will be assigned by ClearPass based on the MAC-auth)

> **IMPORTANT:** Make sure the name is exactly **iot-ac**. The name of the key will be included in the RADIUS Access-Request to ClearPass. The ClearPass system in the lab environment has been configured to check for the key with name *iot-ac* and then return the Aruba-User-Role *iot-ac*.

6. Click **OK** to add the key.
7. Click **OK** to save the PSK local list.

8. Click **Save Settings**.

Create a New Role called iot-ac

9. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
10. In the WLAN List, edit your **p#tx-psk** WLAN.
11. On the **Access** page, make sure the slider is set to **Role Based**.
12. Click **Add Role**:
    - Name: **iot-ac**
13. Click **OK**.

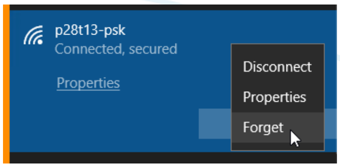
Enable the PSK WLAN with MAC Authentication to ClearPass

14. On the *Security* page, expand **Advanced Settings**.
15. Set *MAC Authentication* to **enabled**.
16. Set Primary Server to cppm1.
17. Expand *Accounting* and set *Accounting* to **Use Authentication Servers**.
18. Click **Save Settings**.
19. Click **OK** when the wizard completes.

Connect with Your Clients

In the next steps you will connect your two clients to see the updated role assignment.

20. On *PC1*, disconnect and reconnect to your PSK WLAN.
21. On *PC4*, **forget** the p#tx-psk WLAN.



22. On **PC4**, connect to your PSK WLAN with the key **Airco123!**.
23. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > **Clients**

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role	Health
P54-T13-PC4	Connected	10.1.34.51	34	ap1	p28t13-psk	iot-ac	iot-ac	Good
P54-T13-PC1	Connected	10.1.34.50	34	ap1	p28t13-psk	iot-sensor-air	p28t13-psk	

NOTE: It may take a minute before the AP role and gateway role are updated for both clients.

- **Question**: What do you observe for the PC4 role assignment?

- **Answer**: PC4 is assigned the role **iot-ac** as gateway role and AP role. The gateway has sent a MAC Auth RADIUS Access-Request to ClearPass that included the Aruba-MPSK-Key-Name VSA. Based on the key name in the MPSK configuration (iot-ac), ClearPass has assigned the Aruba-User-Role iot-ac. The gateway, acting as the RADIUS proxy, has forwarded the Aruba-User-Role information to the AP in the RADIUS Access-Accept. Therefore, both the AP and the rateway have assigned the iot-ac user role for the PC4.

- **Question**: What do you notice for the PC1 roles?

- **Answer**: Something happened with the MPSK local assignment for PC1. Before the MAC authentication was enabled, PC1 was using the iot-sensor-air role on both the AP and the GW. Now it is using the **p#tx-psk** (SSID default role) on the gateway, while it has the iot-sensor-air role on the AP. This happened because on the GW, the MAC authentication *default* role is now applied based on the successful MAC authentication. On the AP, the local MPSK rule configuration overrides the gateway role assignment.

NOTE: Since this is not convenient to work with, your setup may be better with either MPSK local role assignments *or* ClearPass-based role assignments.

Review the RADIUS Authentication Events

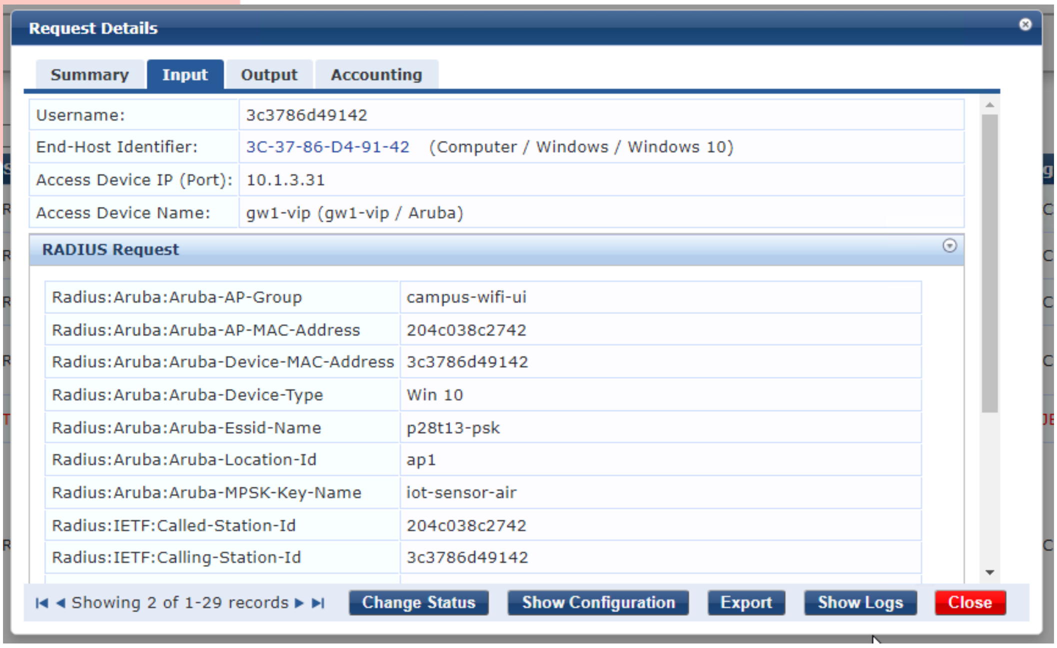
24. Use the MGMT PC to open a connection the ClearPass using admin / Aruba123!

```
https://10.254.1.23/tips
```

25. Navigate to **Monitoring > Live Monitoring > Access Tracke**r.
26. In the latest authentication events, you will see two authentications, one for PC1 and the other for PC4.

#	Server Name	Source	NAS IP Address	NAS Port	Host MAC Address	Username	Service	Login Status	Request Timestan	Enforcement Prof
1.	P58-T01-CPPM	RADIUS	10.1.3.32	0	3C-37-86-D4-B0-81	3c3786d4b081	acap - wireless - psk macauth	ACCEPT	2022/12/22 20:53:23	aruba-role-iot-ac
2.	P58-T01-CPPM	RADIUS	10.1.3.31	0	3C-37-86-D4-91-42	3c3786d49142	acap - wireless - psk macauth	ACCEPT	2022/12/22 20:52:45	[Allow Access Profile]

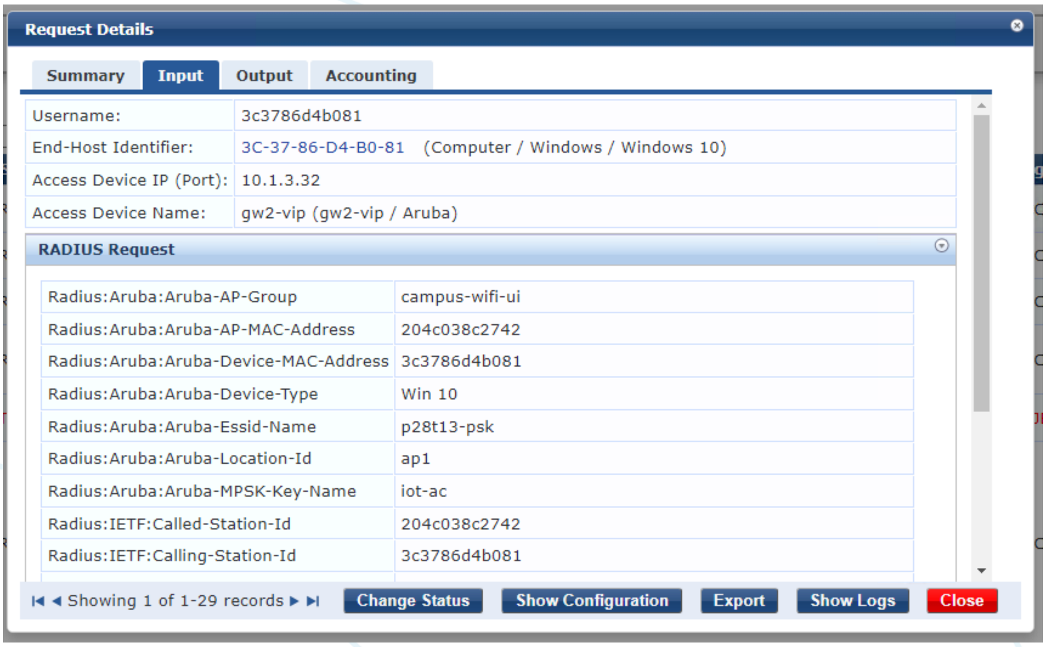
27. Open the entry with the MAC address of PC1 as the username.
28. Open the **Input** page and expand **RADIUS Request**.



- **Question**: Do you see an incoming RADIUS attribute Aruba-MPSK-Key-Name?
- **Answer**: Yes, it has a value of iot-sensor-air. This is the key name (not the actual PSK value) you have configured on the WLAN.

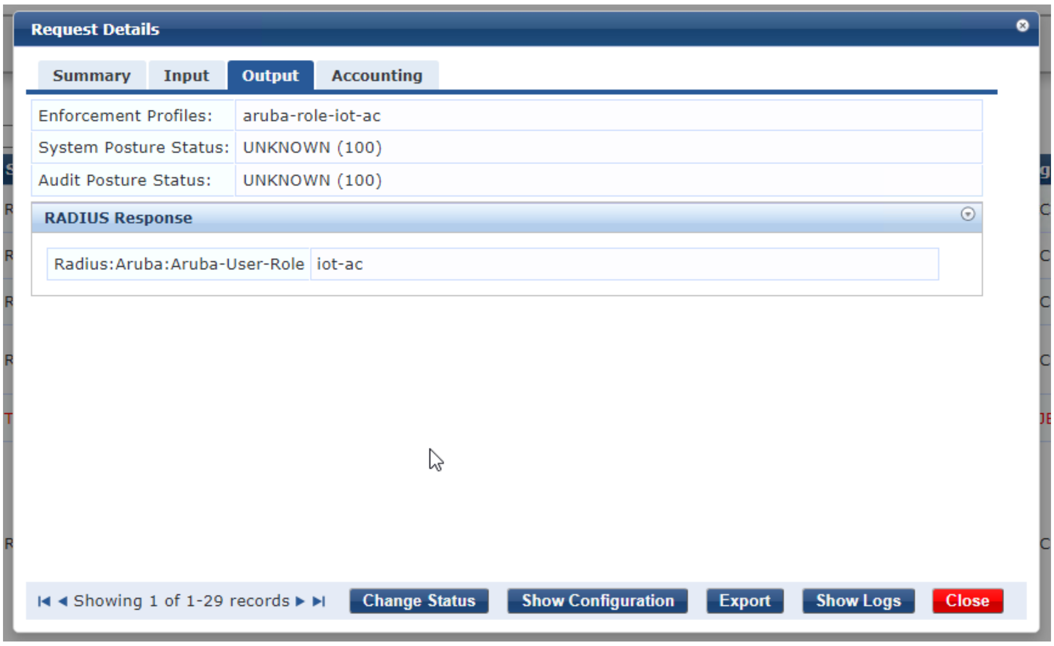
NOTE: The Aruba-MPSK-Key-Name is a new Aruba VSA that is included as of ClearPass release 6.11.

29. Close the entry and open the entry for PC4.
30. Open the **Input** page and expand **RADIUS Request**.



- **Question**: Do you see a different MPSK Key for this authentication?
- **Answer**: Yes, the MPSK key name is *iot-ac*. This allows ClearPass to take different decisions based on the key names.

31. To see an example of the decision, click the **Output** page and expand the **RADIUS Response**.



- **Question**: What role is returned by ClearPass to the gateway?
- **Answer**: ClearPass returns the role iot-ac to the gateway. The gateway applies this role and the RADIUS proxy on the gateway forwards this to the AP .

32. You may close the request details.
33. On PC1, **forget** the p#tx-psk WLAN.
34. On PC4, **forget** the p#tx-psk WLAN.

You have completed this Lab!

Lab 08.01 Configuring Mixed Forwarding WLAN

Overview

In this lab you will learn how to configure and use a mixed mode forwarding WLAN. While the intent of a tunnel WLAN is to tunnel all the traffic to a centralized gateway, the intend of a mixed mode WLAN is to give you the option to tunnel or bridge the client traffic based on the VLAN ID.

In a network with mixed forwarding, the bridged and tunneled VLANs should *not* overlap; therefore, make sure the switch limits the list of VLANs on the AP trunk to only the bridged VLANs.

If you plan to have two mixed forwarding WLAN for example, then you should not use the same VLAN ID for bridge forwarding in one WLAN and for tunnel forwarding in the other WLAN.

In the lab environment, the VLAN IDs for bridged and tunnel forwarding are:

- 11-15 AP bridged
- 31-35 GW tunneled

Therefore, the VLANs 11-15 are enabled on the AP switch trunk ports, but VLANs 31-35 are not enabled on these trunk ports. Instead, the VLANs 31-35 are only enabled on the gateway switch trunk ports.

In the first task of this lab, you will use the employee login to explore how traffic can be configured as bridged or tunneled. This will include the creation of custom VLAN assignment rules for bridge or tunneled forwarding.

In the second task, you will see that it is not required to create these VLAN rules. The ClearPass RADIUS server can assign a VLAN ID as part of the authentication and assign the client to that VLAN.

In the last task you will see that it is also possible to map a custom RADIUS attribute to the VLAN assignment. While not typical in a full Aruba deployment, this may be useful when you need to integrate with an existing RADIUS authentication infrastructure.

Objectives

After completing this lab, you will be able to:

- Understand when VLANs are bridged or tunneled in a mixed mode WLAN.
- Configure VLAN rules for a WLAN.
- Use RADIUS-assigned VLANs for authenticated clients.
- Use custom RADIUS attributes to assign a VLAN.

Task 1: Employee WLAN with Mixed Mode

In this task you will create a mixed mode WLAN. You will remove the existing corporate (employee) tunnel WLAN and create a new employee mixed mode WLAN.

Next you will review the VLANs that are enabled on the GRE tunnel, and you will see how a user role can be assigned a non-tunneled (bridged) VLAN.

In the last section of this task, you will see how to create VLAN assignment rules for both bridged and tunneled VLAN assignments.

Objectives

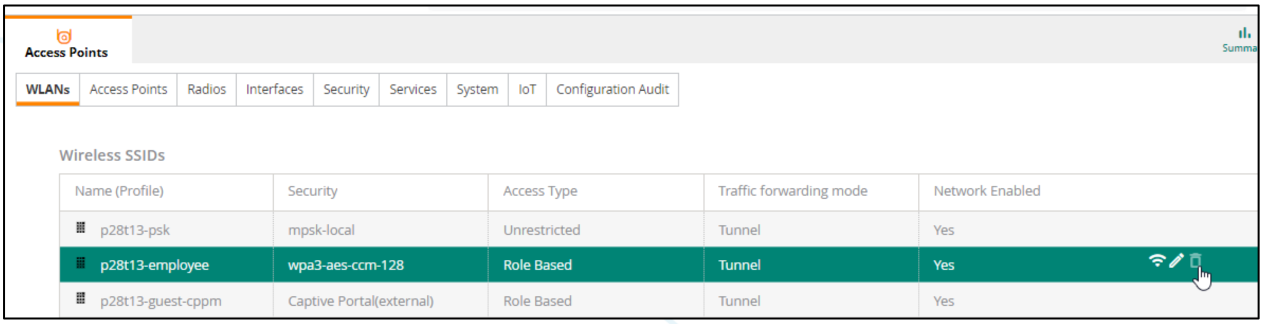
- Understand when VLANs are bridged or tunneled in a mixed mode WLAN.
- Configure VLAN rules for a WLAN.

Steps

Change the Employee WLAN to Mixed Mode

The forwarding mode for a configured WLAN *cannot* be changed after the WLAN is created. In the next steps, you will first delete the employee tunnel mode WLAN and then create the employee WLAN with mixed forwarding mode.

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
2. On the WLAN page, **delete** the p#tx-employee WLAN.



3. Confirm the delete with **Yes**.
4. Click **add SSID**.
5. On the **General** page, configure:
   - SSID: <u>**p#tx**</u>-employee

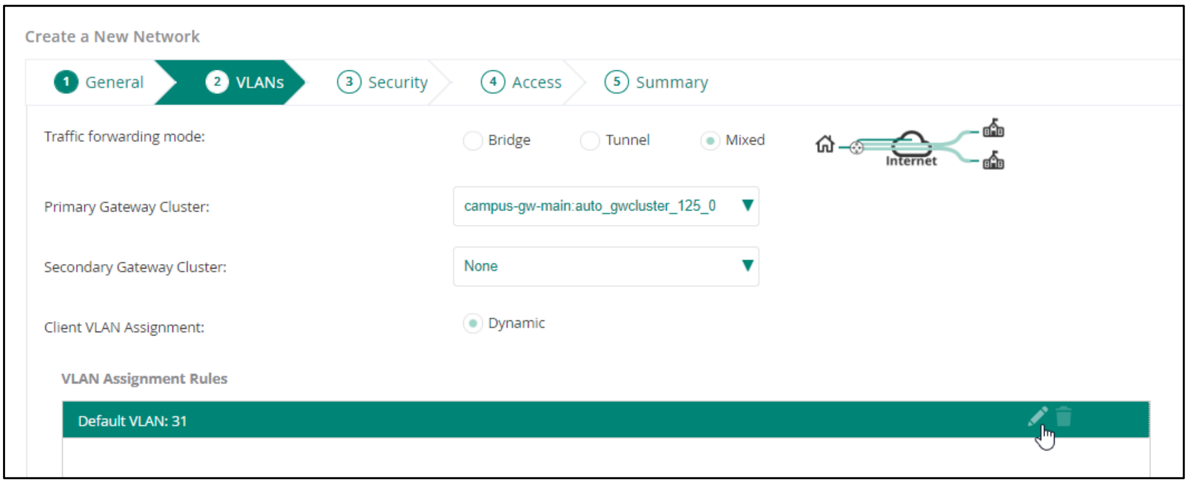
NOTE: Make sure to replace the # value with your Pod number and x with your table number. For example, if you are using table 07 in pod 28, your WLAN name will be:

p28t07-employee

This represents p(od) 28 and t(able) 07.

Check with your instructor if you are not sure about the Pod and Table number.

6. Click **Next**.
7. On the **VLAN** page, configure:
   - Forwarding mode: **Mixed**
   - Primary cluster: Select *your* gateway cluster
   - Default VLAN: Change to **31**



8. Click **Next**.
9. On the **Security** page, configure:
   - Security level: **Enterprise**
   - Primary server: **cppm1**

10. Under *Advanced Settings*, expand **Accounting**.
11. For *Accounting*, set **Use Authentication Servers**.
12. Click **Next**.
13. On the *Access* page, no changes are required.
14. Click **Next**.
15. Click **Finish** to complete WLAN wizard.
16. Click **OK** when the wizard completes.

Review the Tunneled VLANs on the AP

In the next section, you will review the VLANs that are enabled on the GRE tunnel between the AP and the gateway.

17. Use the MGMT PC to open an SSH connection to **gw1** and review the active VLANs

```
show vlan
```

```
(gw1) *# show vlan

VLAN CONFIGURATION
------------------
VLAN  Description  Ports                   AAA Profile  Option-82
----  -----------  -----                   -----------  ---------
1     Default      GE0/0/0 GE0/0/3 Pc0-7   N/A          Disabled
3     VLAN0003     Pc0                     N/A          Disabled
31    VLAN0031     Pc0                     N/A          Disabled
34    VLAN0034     Pc0                     N/A          Disabled
35    VLAN0035     Pc0                     N/A          Disabled
```

18. Use the lab dashboard to open a console session to AP1.
19. Review the VLANs on the GRE tunnel.

```
show overlay tunnel config
```

```
ap1# show overlay tunnel config

Overlay Tunnel Config
Cluster auto_gwcluster_125_0 - Zone 0
-------------------------------------
Index  UAC IP      Tunnel Type  Heartbeat  MTU   Vlan List
-----  ------      -----------  ---------  ---   ---------
0      10.1.3.21   GRE          Enabled    1500  1,3,31,34-35
1      10.1.3.22   GRE          Enabled    1500  1,3,31,34-35
```

- **Question**: What do you observe?
- **Answer**: All the VLANs that exist on the gateway are allowed on the GRE tunnel.
- **Question**: What is the VLAN you have configured for the p#tx-employee WLAN?
- **Answer**: 31.
- **Question**: Suppose a client would be assigned to VLAN 34 by the RADIUS server or a VLAN rule; would it be tunneled or bridged?
- **Answer**: Since the VLAN 34 is allowed on the GRE tunnel, the AP will tunnel the traffic.
- **Question**: Suppose a client would be assigned to VLAN 32 by the RADIUS server or a VLAN rule, would it be tunneled or bridged?
- **Answer**: Since the VLAN 32 is not defined for the GRE tunnel, the AP will bridge the client traffic.

Create new VLAN on the GW

20. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config (gear icon)**.
21. Navigate to **Interface** > **VLANs**.
22. Edit the **employee** VLAN.
23. Add VLAN 32 to the VLAN name employee as **31-32**.
24. Click **Save Settings**. The employee named VLAN list should contain both 31 and 32 now.
25. On the *ap1* console, review the allowed VLANs on the tunnel.

```
show overlay tunnel config
```

```
ap1# show overlay tunnel config

Overlay Tunnel Config
Cluster auto_gwcluster_127_0 - Zone 0
-------------------------------------
Index  UAC IP     Tunnel Type  Heartbeat  MTU   Vlan List
-----  ------     -----------  ---------  ---   ---------
0      10.1.3.21  GRE          Enabled    1500  1,3,31-32,34-35
1      10.1.3.22  GRE          Enabled    1500  1,3,31-32,34-35
```

NOTE: It may take a minute before the new VLAN is listed on the AP tunnel.

- **Question**: What do you notice?
- **Answer**: The cloud Overlay Tunnel Orchestrator has informed the APs that VLAN 32 now exists on the GW. The AP has added the VLAN 32 to the allowed VLANs on the tunnel.
- **Question**: What would happen with a client that was previously assigned to VLAN 32?
- **Answer**: Since the VLAN 32 is now allowed on the GRE tunnel, the client traffic will be tunneled.

IMPORTANT: The above scenario should never happen in a real deployment. You should have dedicated VLAN IDs in your VLAN plan for bridged and tunnel forwarding. When using dedicated VLAN IDs for bridge and tunnel forwarding, a VLAN that is used for bridging will never need to be created on the gateway.

NOTE: Remember, the creation/existence of a VLAN on the gateway is all you need in order to make it a tunneled VLAN for a mixed mode WLAN. Any VLAN that does not exist on the gateway (and as a result not on the tunnel) will be *bridged* by the AP.

Connect the Employee and Contractor Users

In this section, you will confirm the tunneled operation for the default VLAN.

You have selected VLAN 31 as the default VLAN. Since VLAN 31 exists on the GRE tunnel, the default VLAN will be tunneled to the gateway.

> **NOTE:** If you would have entered a VLAN ID that does not exist on the gateway, the default VLAN would be a bridged by the AP.

Connect both wireless clients PC1 and PC4 to the p#tx-employee WLAN using their certificate.

26. Use PC1 to connect to the employee WLAN using the certificate (*employee*).
27. Use PC4 to connect to the employee WLAN using the certificate (*contractor*).
28. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > **Clients**
29. Verify that both clients are assigned to VLAN 31 (a tunneled VLAN)

CLIENTS

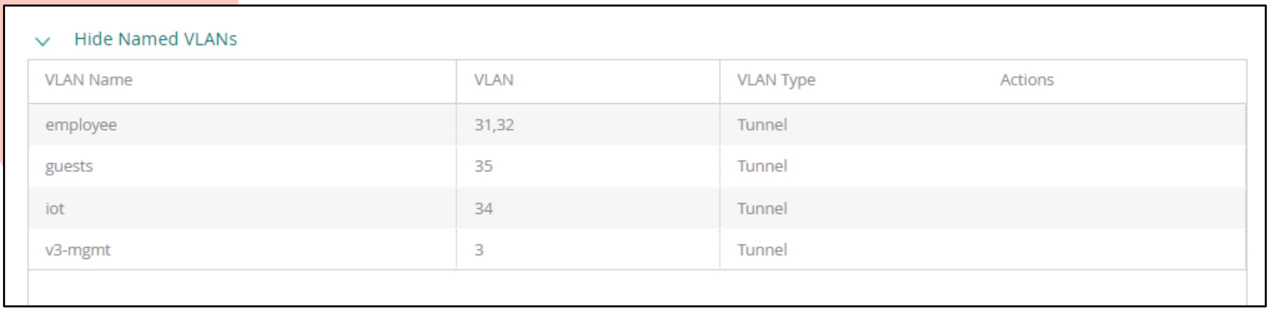
Client Name	Status	IP Address	VLAN
contractor	Connected	10.1.31.51	31
employee	Connected	10.1.31.50	31

> **NOTE:** It may take 1-2 minutes before the information in Central is updated. Use the refresh button to see the latest status.

Create VLAN Assignment Rule for Tunneled VLAN in WLAN Wizard

In the next steps you will configure the contractor user to be assigned to VLAN 32.
VLAN 32 exists on the gateway, which will result in that traffic being tunneled to the GW.

30. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
31. In the WLAN list, **edit** the p#tx-employee SSID.
32. On the VLANs page, click **Show named VLANs**.

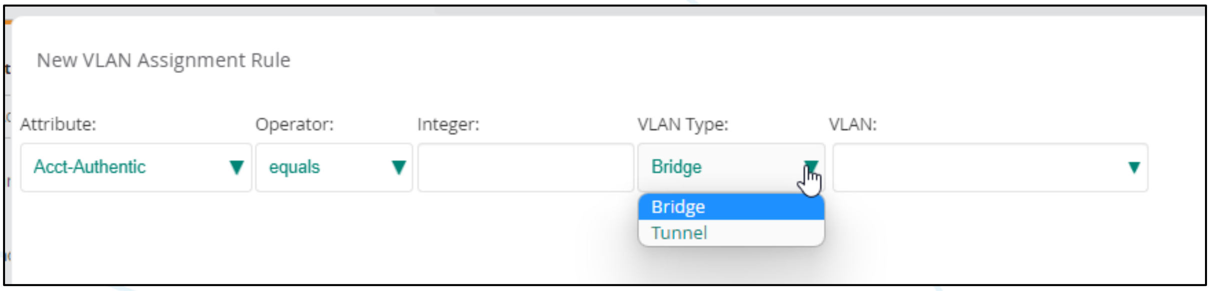


- **Question**: What is listed as the VLAN type for these VLANs?
- **Answer**: Tunnel. Note that there is no special tunnel configuration, this indicates that the VLAN exists on the gateway.

33. Review the list of VLAN Assignment Rules.

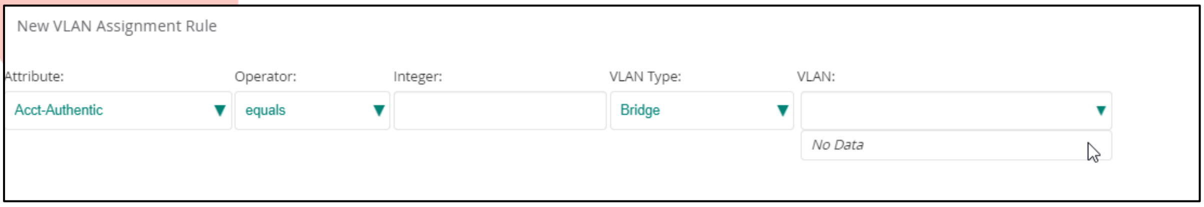
- **Question**: Are there any rules defined?
- **Answer**: Only the default VLAN rule exists.

34. Click **Add Rule** to create a new VLAN assignment rule.



- **Question**: What are the two VLAN types listed?
- **Answer**: Bridged and Tunneled.

35. With the default VLAN type *Bridge* selected, click the **VLAN** dropdown list.

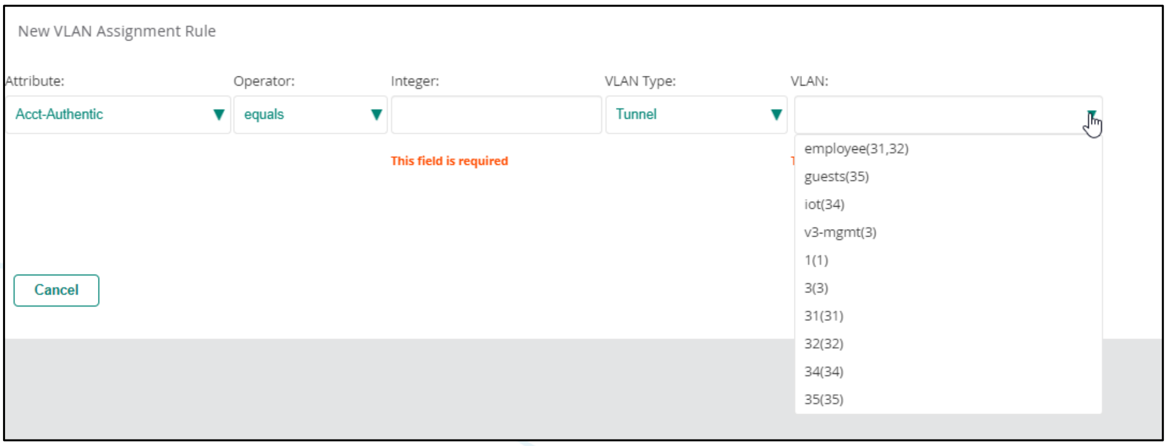


- **Question**: What VLANs do you see in the list?
- **Answer**: This list would show you any named VLANs that have been created locally on the AP. Currently, there are no named VLANs created locally on the AP.

NOTE: The fact that you don't see VLANs in the dropdown list does *not* mean you cannot assign a VLAN. You can manually enter a VLAN ID and that will be bridged by the AP! You will test this in the next section.

---

36. Change the VLAN type to **Tunnel**.

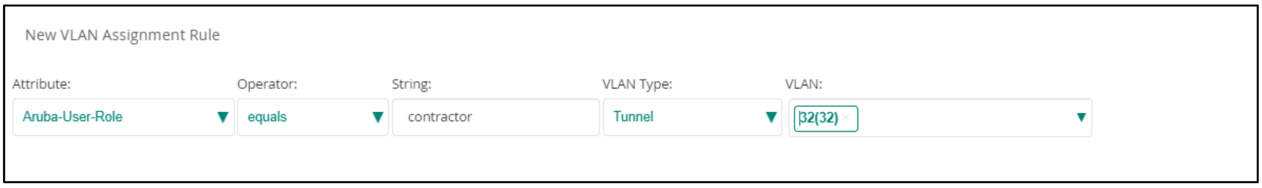


- **Question**: What VLANs do you see in the list?
- **Answer**: The list has now changed to a fixed dropdown list of the VLANs that exist on the selected gateway cluster for this SSID profile.
- **Question**: Can you manually enter some other value in the VLAN field?
- **Answer**: No. Since you have selected tunnel, you must select a VLAN that exists on the gateway. Therefor the rule does not allow you to enter some other VLAN (that does not exist on the gateway).
- **Question**: Suppose you want to assign contractor to a tunneled VLAN 33, would that be possible?
- **Answer**: Yes, this is possible when using these steps:

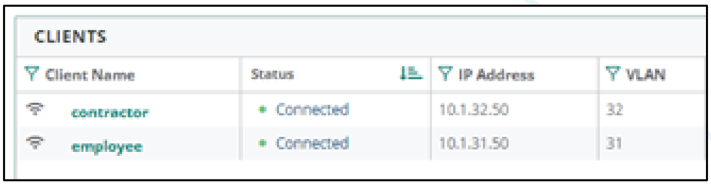
- First you need to create the VLAN first on the Gateway group (Interfaces > VLANs) and make sure it is allowed on the uplink VLAN trunk port.
- Then you can edit the WLAN VLAN rule and the new VLAN will be available in the list.
- Because the client is then assigned to a VLAN that exists on the gateway, the traffic will be tunneled.

In this lab you want to assign contractor users to VLAN32.

37. Configure the rule with these settings:
    - Attribute: **Aruba-User-Role** (You may start to type the attribute name to speed up the search)
    - Operator: **equals**
    - String: **contractor** (Pay attention this needs to match exactly!)
    - VLAN Type: **Tunnel**
    - VLAN: **32(32)**



38. Click **OK** to save the rule.
39. Click **Save Settings**.
40. Click **OK** when the WLAN wizard completes.
41. Wait about one minute for the changes to get pushed to the gateways.
42. On PC4 (contractor), disconnect and reconnect to your *employee* WLAN.
43. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > **Clients**.
44. Verify that PC4 (contractor) is now connected to VLAN 32.



CLIENTS

Client Name	Status	IP Address	VLAN
contractor	Connected	10.1.32.50	32
employee	Connected	10.1.31.50	31

45. Optional step: On the switch sw-agg1, you can confirm the operation by examining the MAC address table for VLAN 32 where the client is still tunneled. The client MAC should be learned on either *LAG 5* or *LAG 10* (These are the LAGs that connect to GW1 and the GW2).

```
show mac-address-table vlan 32
```

```
sw-agg1# show mac-address-table vlan 32
MAC age-time            : 300 seconds
```

```
Number of MAC addresses : 2

MAC Address          VLAN     Type                       Port
--------------------------------------------------------------
3c:37:86:d4:b0:81    32       dynamic                    lag10
b8:d4:e7:d9:ed:00    32       dynamic                    lag256
```

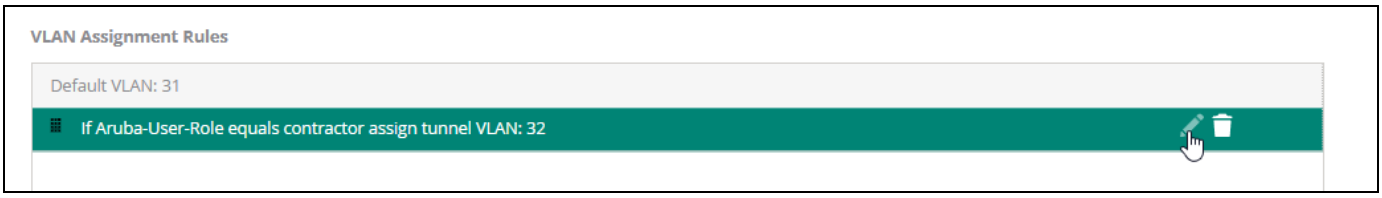
This shows how a custom tunneled VLAN assignment can be configured.

Create VLAN Assignment Rule for Bridged VLAN in WLAN Wizard

In the next steps you want to assign the contractor user to bridged VLAN 12 on the AP.

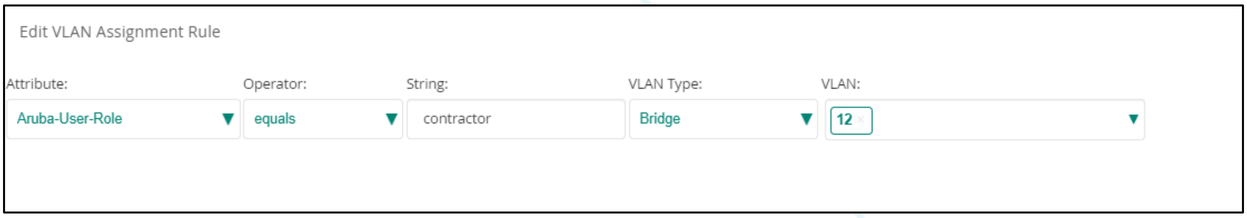
In the lab environment, the VLANs 11-15 are enabled on the AP trunk port and can be used for wireless bridge forwarding. These VLANs do **not** exist on the gateways, and they are **not** allowed by the aggregation switches on the LAG 5 or LAG 10.

46. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
47. In the WLAN list, **edit** the p#tx-employee SSID.
48. On the *VLAN* page, edit the existing VLAN assignment rule for the contractor.



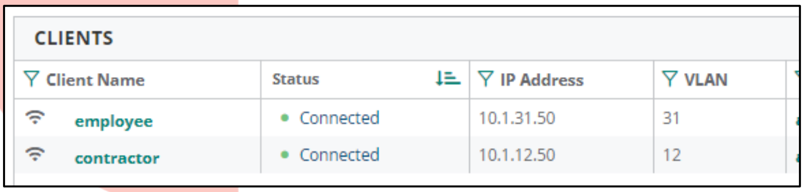
- VLAN type: **Bridge**
- VLAN: **12**

NOTE: You have not created any named VLANs on the AP; therefore, you need to enter the VLAN ID yourself.



49. Click **OK**.
50. Click **Save Settings**.
51. Click **OK** when the wizard completes.
52. Wait about one minute for the changes to get pushed to the gateways.
53. On PC4, disconnect and reconnect to your employee WLAN.

54. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > **Clients**



CLIENTS

Client Name	Status	IP Address	VLAN
employee	Connected	10.1.31.50	31
contractor	Connected	10.1.12.50	12

NOTE: It may take a minute to update the client view. Refresh the page after a few moments.

- **Question**: What is the VLAN for the contractor user?
- **Answer**: The contractor is now assigned to VLAN 12.

55. Optional step: On the switch sw-agg1, you can confirm, using the MAC address table for VLAN 12, that the client is now bridged. The client MAC should be learned on either *LAG1* **or** *LAG2*.

These are the LAGs that connect to the sw-edge1 (if client would be connected to AP1) and the sw-edge2 (for AP2).

```
show mac-address-table vlan 12
```

```
sw-agg1# show mac-address-table vlan 12
MAC age-time            : 300 seconds
Number of MAC addresses : 3

MAC Address          VLAN     Type                          Port
--------------------------------------------------------------
b8:d4:e7:d9:ed:00    12       dynamic                       lag256
20:4c:03:5b:27:e2    12       dynamic                       lag2
3c:37:86:d4:b0:81    12       dynamic                       lag2
```

This shows how a custom bridged VLAN assignment can be configured on a mixed mode WLAN.

Task 2: RADIUS-based VLAN Assignment

Instead of VLAN rules on the gateway, you can also use a RADIUS server to assign the VLAN. This requires no configuration on the gateways or the APs.

When the RADIUS server assigns a VLAN that exists on the gateway, the traffic will be tunneled.

When the RADIUS server assigns a VLAN that does not exist on the gateway, the traffic will be bridged by the AP.

There are no configuration steps in this task: you only need to test the operation since the configuration was already performed on the ClearPass server.

Objectives

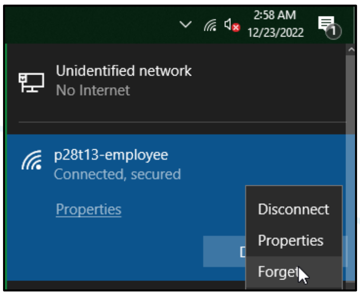
- Use RADIUS assigned VLANs for authenticated clients.

Steps

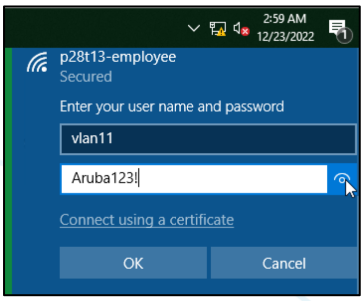
Review the RADIUS Assigned VLAN Not in Tunneled List > Bridged

The ClearPass RADIUS server has been configured with a user named *vlan11*. ClearPass will return the IETF Tunneled-Private-Group-Id 11 for this user.

1. On PC1, **forget** your employee WLAN.



2. On PC1, connect to your employee WLAN, but *do **not** connect with your certificate*.
3. Connect with these user credentials:
   - Username: **vlan11**
   - Password: **Aruba123!**



4. Click **Connect** when prompted for the network certificate.

5. In Aruba Central, verify the client with username *vlan11* is now assigned to VLAN 11.

CLIENTS

Client Name	Status	IP Address	VLAN
contractor	Connected	10.1.12.50	12
vlan11	Connected	10.1.11.50	11

Review the ClearPass Access Tracker

6. The Use MGMT PC to connect to ClearPass; login with **admin** / **Aruba123!**

```
https://10.254.1.23/tips
```

7. Navigate to **Monitoring > Live Monitoring > Access Tracker**.
8. Click the latest authentication event for the username *vlan11*.

P58-T01-CPPM	RADIUS	10.1.3.31	0	3C-37-86-D4-91-42	vlan11	acap - wireless - dot1x	ACCEPT	2022/12/23 08:01:03	ietf-vlan-11

9. Open the **Output** page and expand the **RADIUS Response**.

Request Details

Summary | Input | **Output**

Enforcement Profiles:	ietf-vlan-11
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:IETF:Tunnel-Medium-Type	6
Radius:IETF:Tunnel-Private-Group-Id	11
Radius:IETF:Tunnel-Type	13

- **Question**: What is the Tunnel-Private-Group-id?
- **Answer**: ClearPass returns a value of 11 for this client. This will assign the client to VLAN 11. Since this VLAN does not exist in the gateway, the AP will *bridge* the client.

10. Open the **Input** page.

Request Details

Summary | **Input** | Output

Username:	vlan11
End-Host Identifier:	78-D2-94-98-C5-A8 (Computer / Windows / Windows 10)
Access Device IP (Port):	10.1.3.32
Access Device Name:	10.1.4.51 (gw2-vip / Aruba)

RADIUS Request

- **Question**: What is the Access Device IP?

- **Answer**: The Access Device IP (NAS IP Address) is 10.1.3.31 or 10.1.3.32. This is the gateway IP Address. So even when the traffic is bridged, the authentication is still using the gateway as the RADIUS proxy.
- Take note of the gateway (gw1 or gw2) that is handling the PC1 authentication.
  - PC1 gateway: ________________

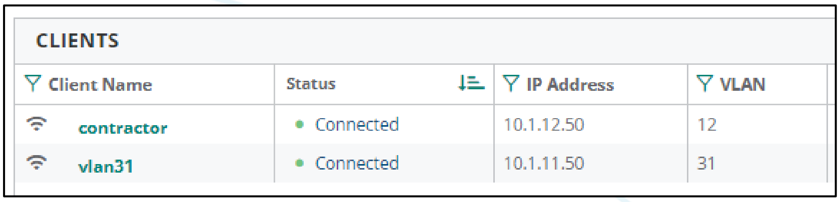
11. **Close** the request.

Review the RADIUS assigned VLAN in Tunneled List

The ClearPass RADIUS server has been configured with a user named *vlan31*. ClearPass will return the IETF Tunneled-Private-Group-Id 31 for this user.

Since this VLAN exists on the gateway, the client will be tunneled.

12. On PC1, **forget** for your employee WLAN.
13. On PC1, connect to your employee WLAN, but *do **not** connect with your certificate*.
14. Connect to the WLAN p#tx-employee with these credentials:
    - Username: **vlan31**
    - Password: **Aruba123!**
15. Click **Connect** when prompted for the network certificate.
16. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > **Clients**
17. Verify that the client is now assigned to VLAN 31.



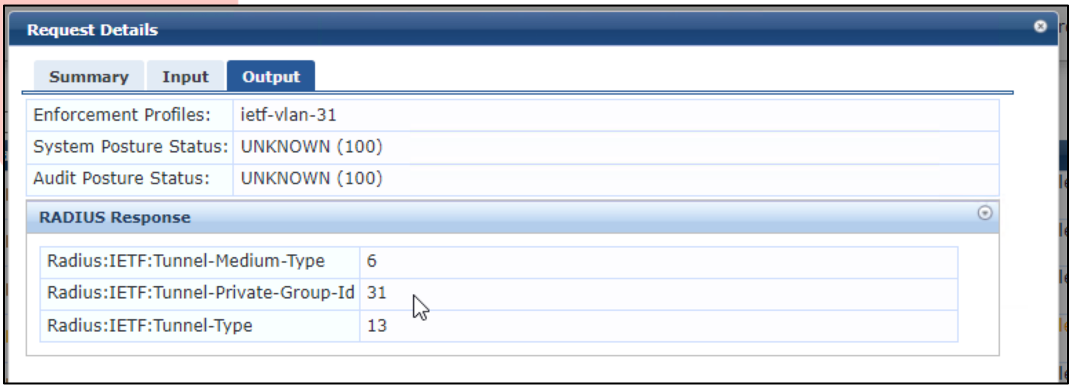
CLIENTS

Client Name	Status	IP Address	VLAN
contractor	Connected	10.1.12.50	12
vlan31	Connected	10.1.11.50	31

18. Use the MGMT PC to access ClearPass Access Tracker.
19. Click the latest authentication event for the username *vlan31*.

P58-T01-CPPM	RADIUS	10.1.3.31	0	3C-37-86-D4-91-42	vlan31	acap - wireless - dot1x	ACCEPT	2022/12/23 08:04:56	ietf-vlan-31

20. Open the **Output** page and expand the **RADIUS Response**.



Request Details

Summary | Input | Output

Enforcement Profiles:	ietf-vlan-31
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

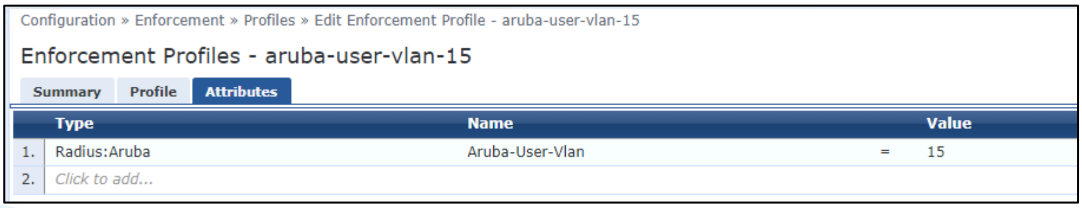
RADIUS Response

Radius:IETF:Tunnel-Medium-Type	6
Radius:IETF:Tunnel-Private-Group-Id	31
Radius:IETF:Tunnel-Type	13

- **Question**: What is the Tunnel-Private-Group-id?
- **Answer**: ClearPass returns a value of 31 for this client. This will assign the client to VLAN 31. Since VLAN 31 exists on the gateway, the AP will tunnel the client traffic.

NOTE: The RADIUS server may also return the VSA Aruba-User-VLAN to assign the VLAN to the client instead of the IETF Tunnel attributes.

Example enforcement profile in ClearPass:



Configuration » Enforcement » Profiles » Edit Enforcement Profile - aruba-user-vlan-15

Enforcement Profiles - aruba-user-vlan-15

Summary | Profile | Attributes

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Vlan	=	15
2.	Click to add...			

Cleanup

There is one optional task in this lab. If you want to complete the optional task, you may **skip** this cleanup section, it will be repeated after the optional task.

21. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
22. In the WLAN list, **edit** the p#tx-employee SSID.
23. On the *VLAN* page, **remove** the custom VLAN rule for contractor.
24. Click **OK**.
25. Click **Save Settings**.
26. Click **OK** when the wizard completes.
27. On both PC1 and PC4, **forget** your employee WLAN.

Optional Task 3: Custom RADIUS Attribute in a VLAN Rule

In some customer environments, the RADIUS server may be managed by a different team, and it may be difficult to get that team to configure the IETF VLAN attributes or the Aruba-User-Vlan on the RADIUS server.

In this case, you may need to adjust the Aruba gateway configuration to map a RADIUS attribute from the existing setup to a specified VLAN. This VLAN can be either:

- a VLAN that exists on the gateway: the result will be tunneled forwarding.
- a VLAN that does not exist on the gateway: the result will be bridged forwarding.

This can be achieved using the VLAN assignment rules and it uses server-based derivations on the gateways to solve this issue.

In this task, you will create a new rule to map the RADIUS standard filter-id attribute to a VLAN.

Objectives

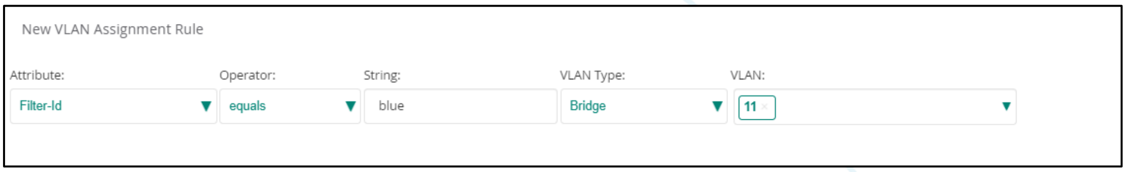
Use custom RADIUS attributes to assign a VLAN.

Steps

Apply VLAN Assignment Rule for VLAN not on Gateway > Bridged

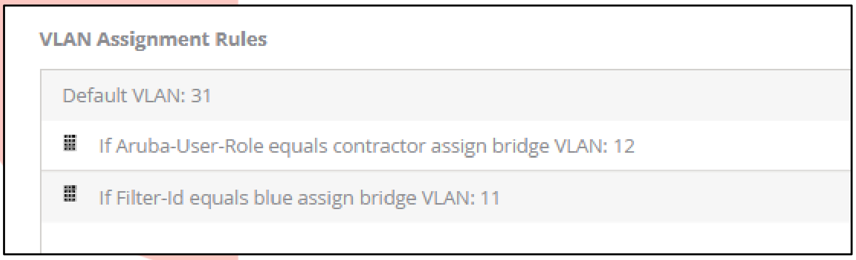
In the next steps, you will link the RADIUS attribute Filter-Id with a value of blue to the bridge VLAN 11.

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config (gear icon)**.
2. In the WLAN list, **edit** the p#tx-employee SSID.
3. On the **VLAN** page, create a new VLAN assignment rule.
    - Attribute: **Filter-id**
    - Operator: **equals**
    - String: **blue** (Pay attention: this needs to match *exactly*!)
    - VLAN type: **Bridge**
    - VLAN: **11**

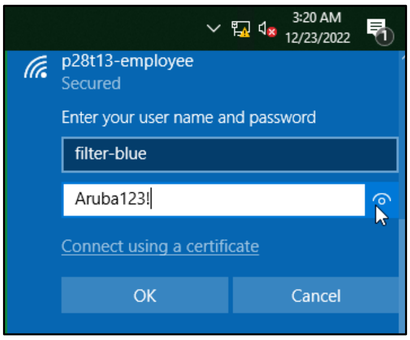


NOTE: Remember that selecting *bridge* will show you the AP named VLAN list (there are no named VLANs defined in the AP in this setup) and allows you to enter a VLAN manually. Since you enter a VLAN that does not exist on the gateway, the client traffic will be bridged.

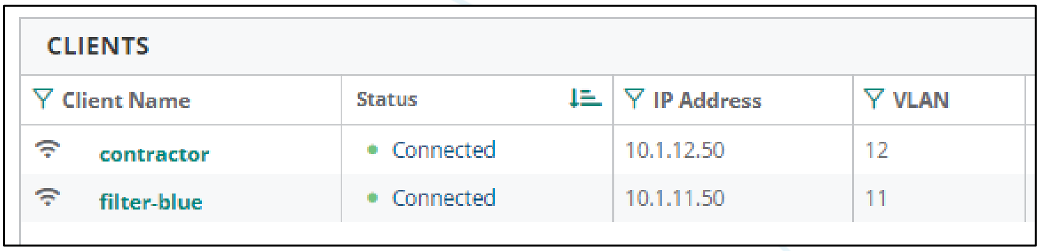
4. Click **OK**.



5. Click **Save Settings**.
6. Click **OK** when the wizard completes.
7. On PC1, **forget** your employee WLAN.
8. On PC1, connect to your employee WLAN, but *do **not** connect with your certificate.*
9. Connect with these credentials:
   - Username: **filter-blue**
   - Password: **Aruba123!**



10. Click **Connect** when prompted for the network certificate.
11. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > **Clients**
12. Verify that the client is now assigned to VLAN 11.



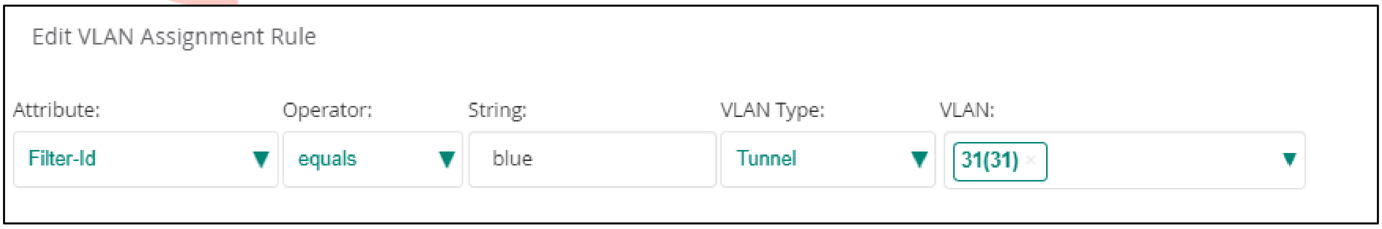
Apply VLAN Assignment Rule for VLAN on Gateway > Tunnel

In the next steps, you will link the RADIUS attribute Filter-Id with a value of *blue* to the tunnel VLAN 31.

13. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
14. In the WLAN list, **edit** the p#tx-employee SSID.

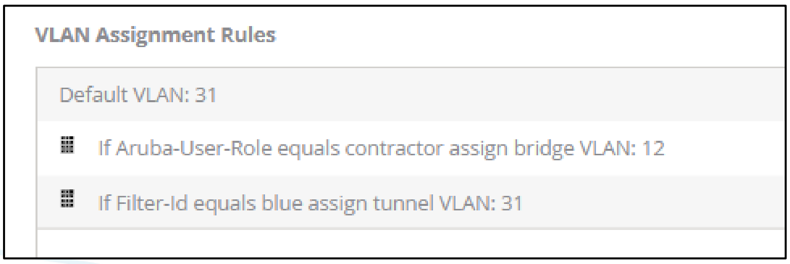
15. On the **VLAN** page, edit the existing VLAN assignment rule.

- Attribute: **Filter-id**
- Operator: **equals**
- String: **blue**
- VLAN type: **Tunnel**
- VLAN: select **31(31)**



> **NOTE:** Remember that selecting *Tunnel* will show you the *gateway* VLAN list. The UI will not allow you to enter a VLAN manually. Therefore, the selected VLAN does exist on the gateway and the traffic will be tunneled.

16. Click **OK**.



17. Click **Save Settings**.
18. Click **OK** when the wizard completes.

Disconnect User

The AP will cache the current authentication and VLAN settings for the client; therefore, you can use the **aaa user delete all** command on the gateway to force a new authentication.

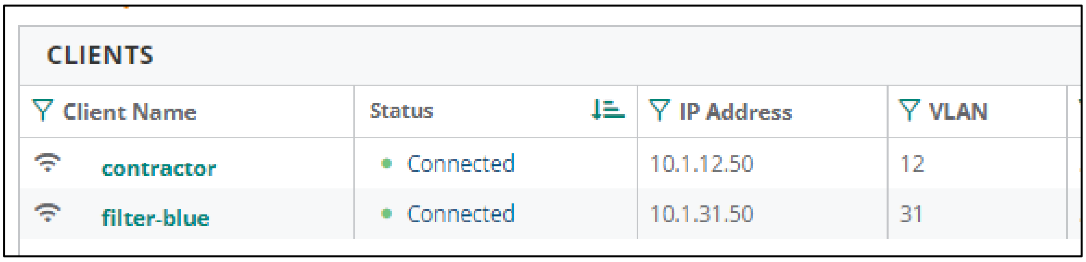
19. Use the MGMT PC to open an SSH connection to the GW that handles the authentication for PC1. (You have noted the authentication gateway for the PC1 in the previous task)
20. On the GW, disconnect all users:

```
aaa user delete all
```

> **NOTE:** Be careful when using this command in a production environment! All connected clients would need to reauthenticate. You selectively disconnect a single MAC using the command:

```
aaa user delete mac 3c:37:86:d4:91:42
```

21. On PC1, **reconnect** your employee WLAN, you should be able to use the previously saved credentials for the filter-blue user account.
22. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > **Clients**
23. Verify that the client is now assigned to VLAN 31.



CLIENTS

Client Name	Status	IP Address	VLAN
contractor	Connected	10.1.12.50	12
filter-blue	Connected	10.1.31.50	31

This task shows how a custom RADIUS attribute can be used to assign a client to a VLAN, which can be either bridged or tunneled.

Cleanup

24. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
25. In the WLAN list, **edit** the p#tx-employee SSID.
26. On the VLAN page, **delete** the custom VLAN assignment rules.
27. Confirm each removal with **OK**.
28. Click **Save Settings**.
29. Click **OK** when the wizard completes.
30. On both PC1 and PC4, **forget** your employee WLAN.

You have completed this Lab!

Lab 09.01 Gateway Cluster Deployments

Overview

In this lab you will explore different types of gateway cluster deployments.

In the first section, you will move gw2 to a new group. This will allow you to have a separate cluster on gw2.

In the next section, you will configure a new WLAN that will be tunneled to this new cluster. This was known as multi-zone in AOS 8.

After the auto-group cluster, you will configure an *auto-site* cluster. This can simplify the configuration when several sites are deployed, each with their own APs and gateways.

The last section of the lab will show how you can configure cluster redundancy. This allows you to configure a secondary cluster for a WLAN. You will configure the secondary cluster, test the failover, and verify how the service reverts to the original cluster.

Objectives

After completing this lab, you will be able to:

- Understand the configuration changes of a group move.
- Understand how to configure WLANs with different gateway clusters.
- Configure site based gateway clustering.
- Understand primary and secondary cluster configuration.

Task 1: Move Gateway gw2 to the Group campus-main-dmz

In this task you will review the process of moving a gateway to a new group. The new group will be used in the next task to apply a different configuration from the campus main gateway group.

These are the steps in the gateway group move process:

- The gateway clears the local configuration and reboots with the local setup-dialog config.
- Central keeps the device-level config when device is moved to another group.
- Central merges the new group config with the device level config.
- The merged config is pushed to the gateway when the gateway checks in with Central.

Objectives

- Understand the configuration changes of a group move.
- Verify the applied configuration after a group move.

Steps

Create new Group for campus-gw-dmz

1. In Aruba Central, navigate to Context: **Global**> Navigation: **Organization**> Top **Network Structure**> **Groups**.
2. At the right-top, click the **+** sign to add a **New Group**.
3. For the name, enter **campus-gw-dmz**.
4. For the value *Group will contain*, only select **Gateways**.
5. Do **not** configure using templates.
6. Click **Next**.
7. For Architecture, select **ArubaOS 10**.
8. For Network Role, select **Mobility**.
9. Click **Add**.
10. Verify that the group **campus-gw-dmz** is now listed.

Complete Guided Setup for the Group

11. In Aruba Central, navigate to Context: **Groups / campus-gw-dmz** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
12. The Guided Setup will be automatically launched.
13. Complete the initial setup wizard for the group using the following parameters:

System
- Platform
  - Platform **9004**
  - Clustering **Group based clustering** (default)
- Time
  - IPv4 **10.254.1.21**
  - burst **enabled**

Timezone **America/Detroit (UTC-05:00)**
DNS
Specify
Domain **aruba-training.com**
User Defined **10.254.1.21**
Management User
AAA authentication leave disabled
Local management users leave default

LAN
VLAN
id **3**
name **v3-mgmt**
LAN
leave default
Finish

Create Named VLAN Guests for the DMZ Group

14. Navigate to **Interface** > **VLANs**.
15. Add a new named VLAN.
    - VLAN Name: **guests**
    - VLAN ID/Range: **35**
16. Click **Save Settings**.

Move the gw2 to the New Group

In the next steps you will move the GW2 to the new DMZ group.

17. In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Groups**
18. Expand *All connected devices* by clicking the **>** icon.
19. Under *All connected devices*, select the gateway **gw2**.
20. On the right-hand side, a popup will be displayed with the **Move Devices** action button.
21. Click the **Move Devices** button.
22. Click the **Destination Group** field.
23. Select the group **campus-gw-dmz.**
24. Click the **Move** button to continue.

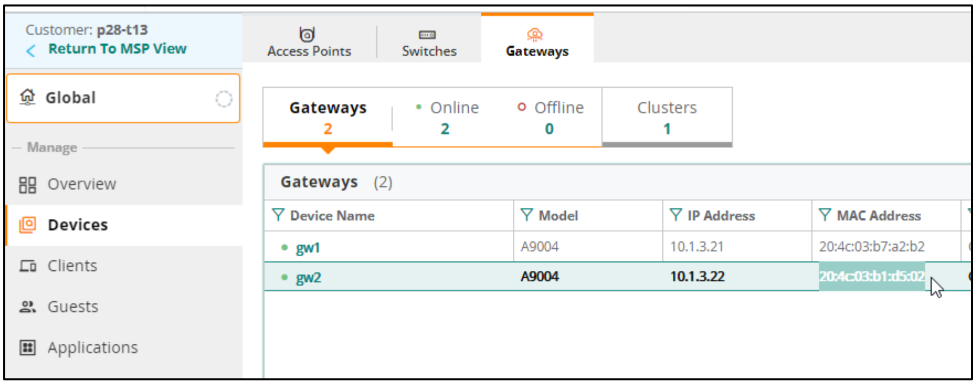
Verify the Initial Configuration after a Group Move

NOTE: You will need to login to the console of gw2 immediately after it completes the reboot. Make sure you don't waste time in the next section.

25. Use the lab dashboard to access the console of gw2.

You will need to login with the **branchsupport** user account, the password is the lower-case MAC address of the gateway. In the next steps, you will copy this password in Aruba Central.

26. In Aruba Central, navigate to Context: **Global**> Navigation: **Devices**> Top **Gateways**
27. Copy the lower-case MAC address of **gw2** (this is the password for the *branchsupport* account).



28. On the console of gw2, wait for the reboot to complete, then immediately login:

- Username: **branchsupport**
- Password: <the lowercase mac address you have copied>

NOTE: Make sure there are no leading or trailing spaces when you copy the MAC address.

NOTE: Once the gateway connects and syncs the config with Aruba Central, the branchsupport account will no longer work. Login immediately after the reload completes.

Example password format: 20:4c:03:b1:d5:02

```
User: branchsupport
Password:
(Aruba9004_B1_D5_02) #
```

29. Check the local VLAN list.

```
show vlan
```

```
(Aruba9004_B1_D5_02) # show vlan
```

```
VLAN CONFIGURATION
------------------
VLAN  Description  Ports                AAA Profile  Option-82
----  -----------  -----                -----------  ---------
1     Default      GE0/0/0-0/3 Pc0-7    N/A          Disabled
3     VLAN0003     GE0/0/1              N/A          Disabled
```

- **Question**: What happened with VLANs 31,32,34?
- **Answer**: Since the gateway rebooted with the setup-dialog configuration, only VLAN3 exists.

30. Review the current mgmt users

```
show mgmt-user
```

```
(Aruba9004_B1_D5_02) # show mgmt-user
No Users defined
```

- **Question**: Why is there no mgmt-user?
- **Answer**: After the setup-dialog was completed, the gateway did not have a local admin account. Therefore, you could login using the branchsupport account.

31. Check the configuration version

```
show switches
```

```
(Aruba9004_B1_D5_02) # show switches

All Switches
------------
IP Address  IPv6 Address  Name                Location          Type  Model
Version         Status  Configuration State  Config Sync Time (sec)  Config ID
----------  ------------  ----                --------          ----  -----      ----
---         ------  -------------------  ----------------------  ---------
10.1.3.22   None          Aruba9004_B1_D5_02  Building1.floor1  MD    Aruba9004
10.3.1.1_84780  up      UPDATE REQUIRED      0                       0

Total Switches:1
```

- **Question**: What is the Configuration State?
- **Answer**: UPDATE REQUIRED. The gateway has connected to Aruba Central and is waiting for the configuration from Aruba Central.

32. Wait a few minutes for the configuration sync to complete.

Once the config sync completes, you will be logged out of the gateway. The branchsupport account can no longer be used after a local management user has been created.

```
Management user configuration has changed. Please re-authenticate.
```

```
User:
```

33. Login again with **admin** / **Aruba123!**

```
User: admin
Password:
(gw2) #
```

- **Question**: Why can you login using these credentials now?
- **Answer**: You have previously applied the password at the device level. The device level configuration is maintained by Aruba Central when a gateway is moved to a different group. Therefore, the device level admin account admin / Aruba123! still works.

34. Review the Config Id.

```
show switches
```

```
(gw2) # show switches

All Switches
------------
IP Address  IPv6 Address  Name  Location          Type  Model      Version           --
Status  Configuration State  Config Sync Time (sec)  Config ID
----------  ------------  ----  --------          ----  -----      -------         --
----  -------------------  ----------------------  ---------
10.1.3.22   None          gw2   Building1.floor1  MD    Aruba9004  10.3.1.1_84780  up
UPDATE SUCCESSFUL    0                       211

Total Switches:1
```

35. Review the VLAN list.

```
show vlan
```

```
(gw2) # show vlan

VLAN CONFIGURATION
------------------
VLAN  Description  Ports                   AAA Profile  Option-82
----  -----------  -----                   -----------  ---------
1     Default      GE0/0/0 GE0/0/3 Pc0-7   N/A          Disabled
3     VLAN0003     Pc0                     N/A          Disabled
35    VLAN0035     Pc0                     N/A          Disabled
```

- **Question**: What happened with VLANs 31,32,34?
- **Answer**: On the DMZ group, only the guests VLAN with VLAN ID 35 was created. The VLANs 31,32 and 34 were not created at the device level but at the campus-gw-main **group level**. Therefore, they are not maintained when the gateway is moved to another group.

36. Review the port status

```
show port status
```

```
(gw2) # show port status

Port Status
-----------
Slot-Port  PortType  AdminState  OperState  PoE  Trusted  SpanningTree  PortMode     Speed   Duplex  PortError
---------  --------  ----------  ---------  ---  -------  ------------  --------  -----  ------  ---------
0/0/0      GE        Enabled     Down       N/A  No       Disabled      Access       Auto    Auto    -
0/0/1      GE        Enabled     Up         N/A  N/A      N/A           PC0       1 Gbps  Full    -
0/0/2      GE        Enabled     Up         N/A  N/A      N/A           PC0       1 Gbps  Full    -
0/0/3      GE        Enabled     Down       N/A  No       Disabled      Access       Auto    Auto    -
PC0        PC        Enabled     Up         N/A  Yes      Forwarding    Trunk     N/A  N/A     -
```

- **Question**: Did you define the Port Channel 0 on the new group?
- **Answer**: No.
- **Question**: Why is the Port Channel 0 in the list and trusted?
- **Answer**: You have previously applied the Port Channel 0 and the trust options at the **device level**. The device level configuration settings are maintained by Aruba Central when a gateway is moved.

Task 2: Multi-Zone

In this task you will use a separate cluster for the guest WLAN. This provides the option to have the guest traffic handled by a dedicated gateway cluster, separate from the corporate traffic cluster. The DMZ acts as a separate zone.

To create a DMZ cluster, you have moved the gw2 to the group campus-gw-dmz.
This results in *two* clusters, each consisting of a *single* gateway.

In this task you will create a new WLAN and use the DMZ cluster as the primary cluster.

Note that the multi-zone concept was introduced in AOS 8, but in AOS 10 there is no multizone configuration required. There is no longer a concept of primary and data zones since the AP is primarily managed by Aruba Central.

In AOS 10, you only need to setup multiple clusters and create WLANs that use those clusters.

Objectives

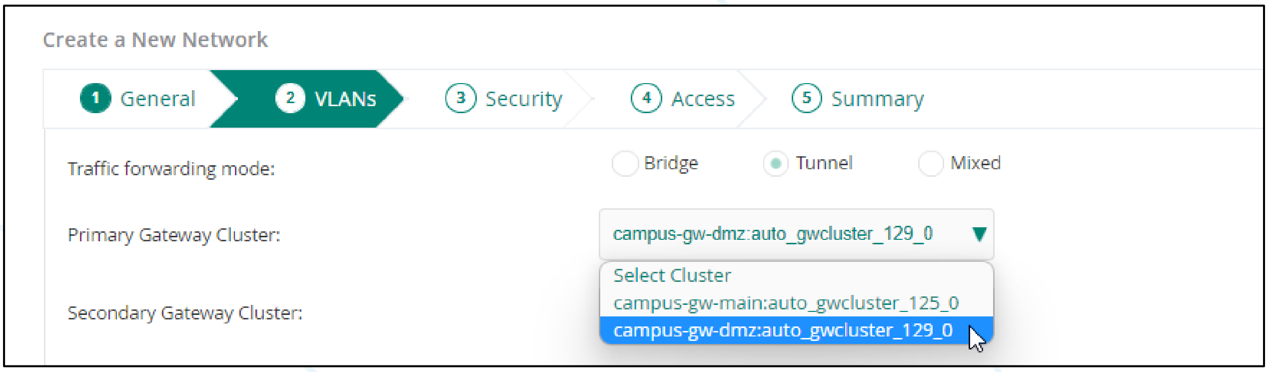
Understand how to configure WLANs with different gateway clusters.

Steps

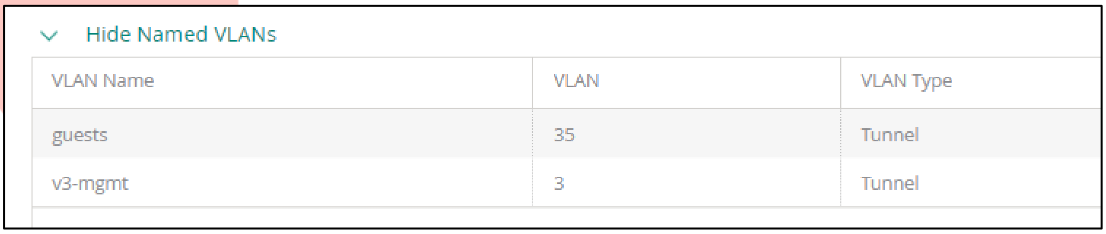
Create guest WLAN with a DMZ Cluster

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
2. On the WLAN page, click **add SSID**.
3. On the General page, configure your DMZ SSID (Remember that # is your pod number and *x* is your table number):
   - Name(SSID): **p#*tx*-guest-dmz**
4. Click **Next**.
5. On the **VLANs** page, configure:

Forwarding mode	Tunnel
Primary Gateway Cluster	Select the campus-gw-dmz:auto_gwcluster_xxxx



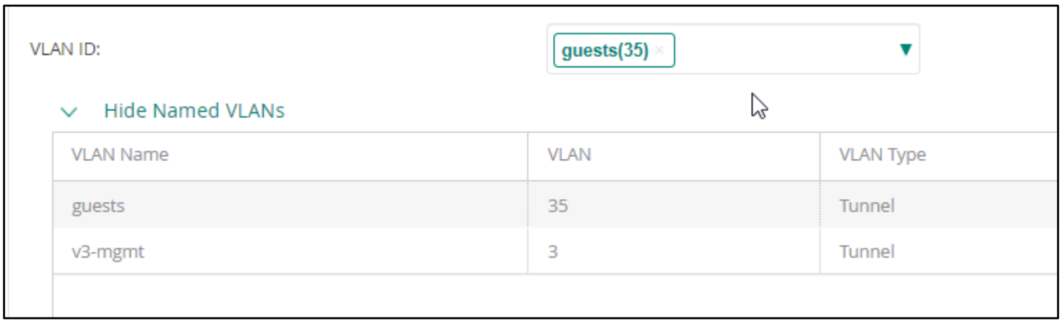
6. Click **Show named VLANs**.



VLAN Name	VLAN	VLAN Type
guests	35	Tunnel
v3-mgmt	3	Tunnel

- **Question**: Why don't you see the employee VLAN?
- **Answer**: After you have selected the primary gateway cluster, the wizard will retrieve the list of VLANs that exist on the selected cluster. On the campus-gw-dmz group, only the guests named VLAN was created.

7. Leave the Client VLAN Assignment as *Static*.
8. Set VLAN ID to **guests(35)**.



VLAN Name	VLAN	VLAN Type
guests	35	Tunnel
v3-mgmt	3	Tunnel

9. Click **Next**.
10. On the **Security** page, move the security to **Open**.

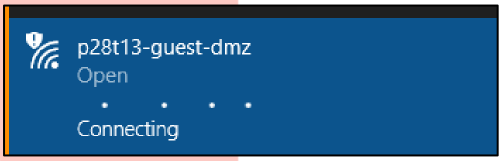
NOTE: The WLAN configuration is kept as simple as possible in this lab, since the focus is on different cluster tunnel termination, not security.

11. On the **Access** page, leave it as **Unrestricted**.
12. Click **Next**.
13. Click **Finish**.
14. Click **OK** when the wizard completes.

Test the DMZ Guest WLAN

In the next steps you will use PC4 to test the guest WLAN on the DMZ cluster.

15. On PC4, connect to the p#tx-guest-dmz WLAN.



16. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > **Clients**
17. Verify that PC4 has received an IP Address in the 10.1.35.0/24 subnet.

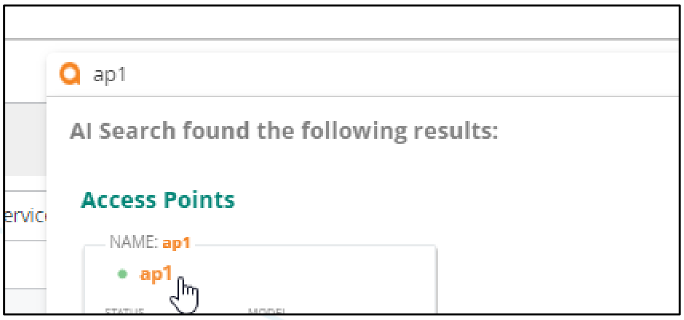
CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role
P54-T13-PC4	Connected	10.1.35.50	35	ap1	p28t13-guest-dmz	p28t13-guest-dmz	p28t13-guest-dmz

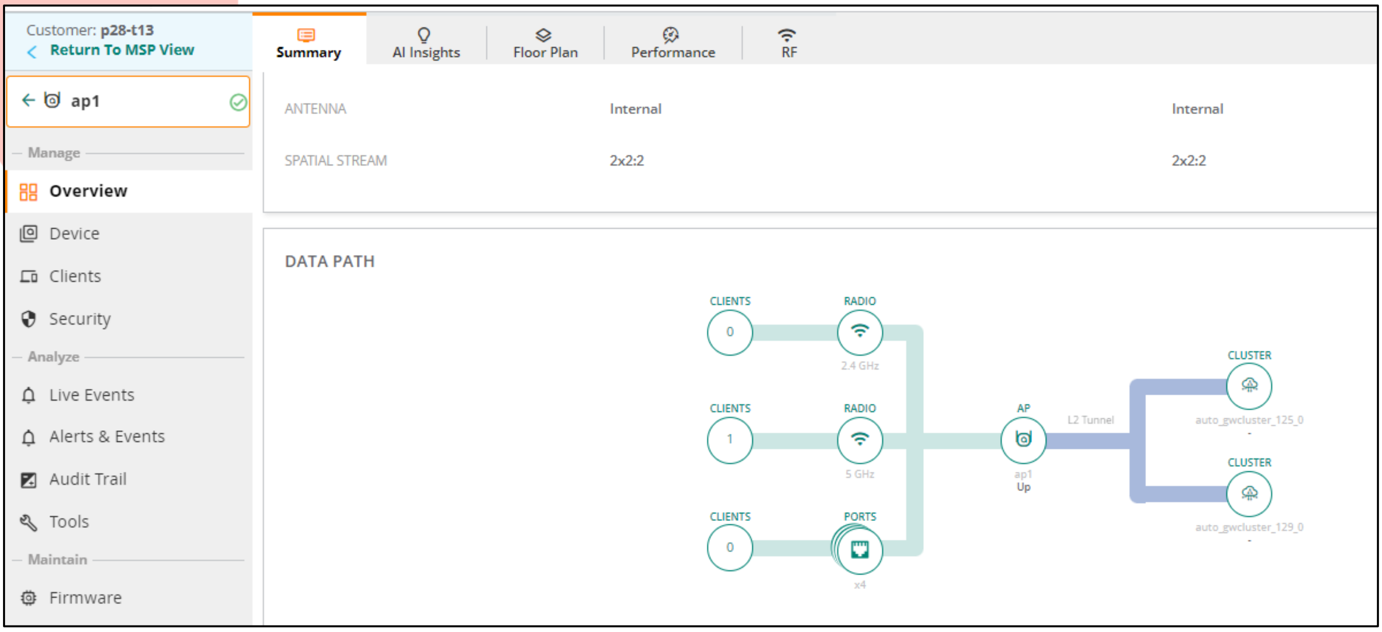
NOTE: It may take a minute for both AP and GW information to show. Use the refresh button to see the latest information.

18. In Aruba Central, open the AP1 details page.

TIP: You can use the AI Search bar to enter the ap1 name. In the search results, click ap1 to get to the AP details page.



19. On the **Overview > Summary** page, scroll down to see the datapath to the two clusters.



Verify on the AP

You can also verify the connections on the AP.

20. Use the lab dashboard to open a console connection to the AP1.
21. Check the overlay tunnel configurations. Notice the different VLAN lists for each zone.

```
show overlay tunnel
```

```
ap1# show overlay tunnel

Overlay Tunnel Config
Cluster auto_gwcluster_125_0 - Zone 0
-------------------------------------
Index  UAC IP     Tunnel Type  Heartbeat  MTU   Vlan List
-----  ------     -----------  ---------  ---   ---------
0      10.1.3.21  GRE          Enabled    1500  1,3,31-32,34-35
Cluster auto_gwcluster_129_0 - Zone 1
-------------------------------------
Index  UAC IP     Tunnel Type  Heartbeat  MTU   Vlan List
-----  ------     -----------  ---------  ---   ---------
0      10.1.3.22  GRE          Enabled    1500  1,3,35
```

22. Use the **show overlay cluster-info** command to see the tunnel heartbeat information.

```
show overlay cluster-info
```

```
ap1# show overlay cluster-info
```

```
Cluster auto_gwcluster_125_0 - Zone 0 Multicast-Vlan 0 bktmap_refs 1 uac_refs 1
-------------------------------------------------------------------------------
Index  Zone  UAC IP     HeartBeat  MTU   Refs  Odev  HeartBeat
Sequence/Send/Recv/Drop  Clients  Overlay-Vlans
-----  ----  ------     ---------  ---   ----  ----  --------------------------------
-  --
0      0     10.1.3.21  1          1500  1     tun0  50026/185051/180433/0
0        1,3,31-32,34-35
Cluster auto_gwcluster_129_0 - Zone 1 Multicast-Vlan 0 bktmap_refs 1 uac_refs 1
-------------------------------------------------------------------------------
Index  Zone  UAC IP     HeartBeat  MTU   Refs  Odev  HeartBeat
Sequence/Send/Recv/Drop  Clients  Overlay-Vlans
-----  ----  ------     ---------  ---   ----  ----  --------------------------------
-  --
0      1     10.1.3.22  1          1500  1     tun1  390/397/387/0
1        1,3,35
```

This concludes the guest DMZ configuration.

Task 3: Set up Site-Based Clustering Using a Single Site

Site based clustering is a convenient option when several sites will be deployed, each with a local gateway cluster.

If the group-based cluster would be used, each site would require its own group in Aruba Central, since the cluster should only consist of the two gateways within each site.

This makes it more difficult to keep the gateway configuration in sync between these groups.

When a group is created using a site-based cluster, many gateways can be added to the same group, therefore the configuration can be easily kept in sync.

When you assign multiple gateways to the same Central site, Aruba Central will automatically create a site-based cluster between them. This means that a lot of clusters could exist within the *same* group.

On the AP side, the WLAN can point to this primary site-based cluster. Automatically the AP will connect to the cluster that belongs to its own site.

The restriction is that each AP must belong to a site where a gateway exists.
In the case where an AP is assigned to a site that does not have a gateway, there will be no tunnels configured; which means no WLAN service will be available for that SSID.

In this first task, you will implement a site-based cluster and verify the operation with all Gateways and all APs in a single site.

Objectives

- Configure site based gateway clustering.
- Configure a WLAN with site based clustering.

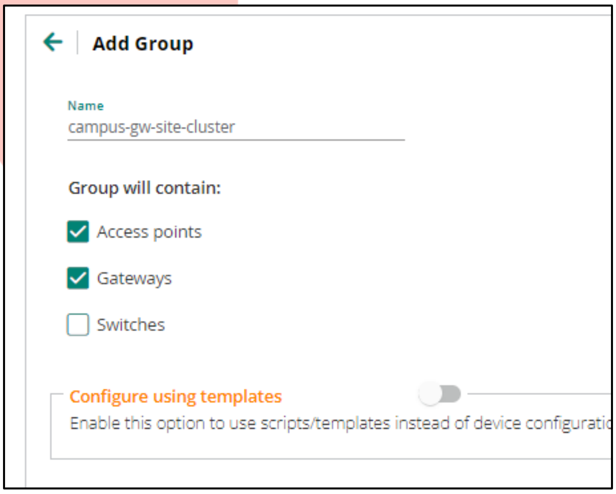
Steps

Gateway Group campus-gw-site-cluster

It is possible to change the cluster type of an existing group. However, to keep your existing lab setup in a working state, a new group will be created for your gateways and access points.

Create a New Group for campus-gw-dmz

1. In Aruba Central, navigate to Context: **Global**> Navigation: **Organization**> Top **Network Structure**> **Groups**.
2. At the right-top, click the Plus sign to add a **New Group**.
3. For the name, enter campus-gw-site-cluster.
4. For the value “Group will contain”, select **both** **Access Points** and **Gateways**.

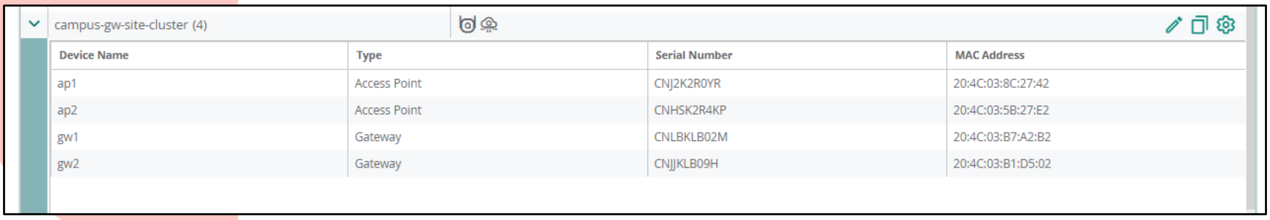


5. Do **<u>not</u>** configure using templates.
6. Click **Next**.
7. For Architecture, select **ArubaOS 10**.
8. For Network Role of the access points, select **Campus/Branch**.
9. For Network Role of the gateways, select **Mobility**.
10. Click **Add**.
11. Verify that the group **campus-gw-site-cluster** is now listed.

Move the Access Points and Gateways to the New Group

In the next steps you will move both APS and both GWs to the new DMZ group.

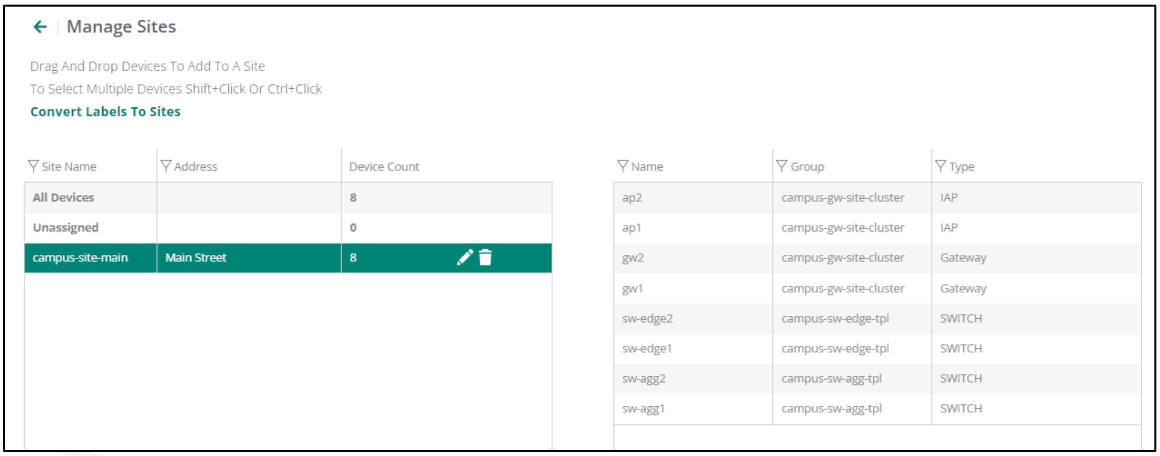
12. In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Groups**
13. Expand *All connected devices* by clicking the **>** icon.
14. Under All connected devices, select both APs (**ap1/ap2**) and both GWs (**gw1/gw2**).
15. On the right-hand side, a popup will be displayed with the **Move Devices** action button.
16. Click the **Move Devices** button.
17. Click the **Destination Group** field.
18. Select the group campus-gw-site-cluster.
19. Click the **Move** button to continue.
20. Click **OK** to confirm the move message.
21. Expand the group campus-gw-site-cluster and verify both APs and both GWs are listed.



Verify Site Assignment for Access Points and Gateways

In the next steps you will verify that both APS and both GWs belong to the same site.

22. In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Sites**.
23. Select the site campus-site-main, verify on the right side that your APs and GWs have been assigned to this site.

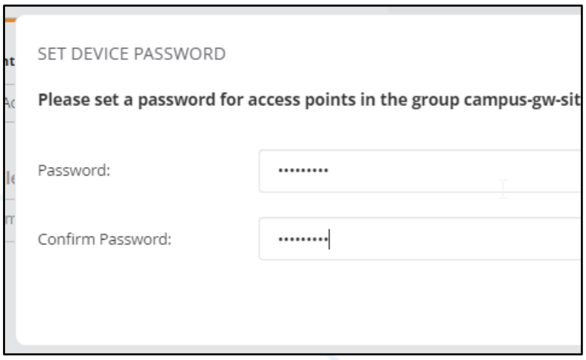


Complete Guided Setup for the Group

24. In Aruba Central, navigate to Context: **Groups / campus-gw-site-cluster** > Navigation: **Devices**> **Config** (gear icon).

This will take you to the Access Points page by default. Since this is the first time you access the configuration for this group, you are prompted to set the Access Point admin password.

25. Set the password to **Aruba123!**



26. Click **Gateways** at the top of the page, the Guided Setup will be launched.
27. Complete the Guided Setup wizard for the **group level**.

System
- Platform
  - Platform **A9004**
  - Clustering **Site based clustering**
- Time
  - IPv4 **10.254.1.21**
  - burst **enabled**
  - Timezone **America/Detroit (UTC-05:00)**
- DNS
  - Specify
  - domain **aruba-training.com**
  - User Defined **10.254.1.21**
- Management User
  - AAA authentication leave disabled
  - Local management users leave default

LAN
- VLAN
  - id **3**
  - name **v3-mgmt**

  - id **31**
  - name **employee**
- LAN
  - leave default
- Finish

Review the Cluster Operation with Both Gateways in the Same Site

Both gateways have been moved to a new group, but they are still assigned to the same site in Aruba Central at this point.

You will first verify that the site-based cluster has successfully formed for 2 gateways that belong to the same site.

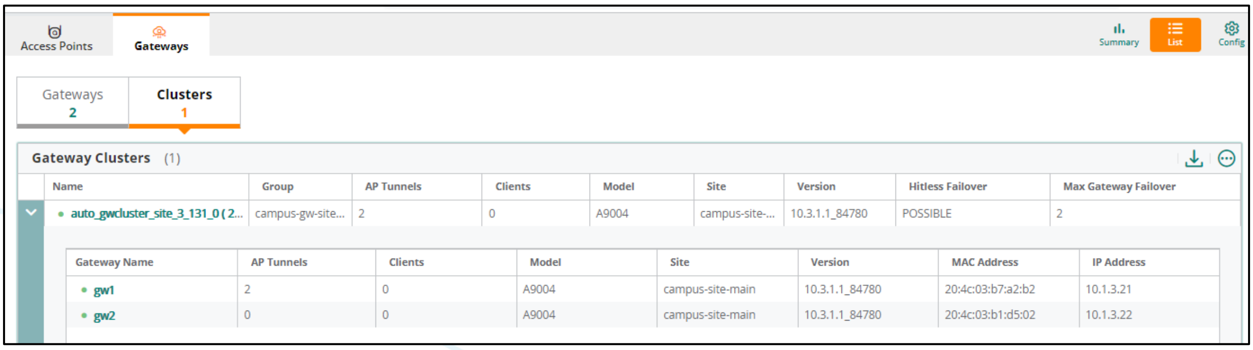
Verify the Site-Based Cluster

28. In Aruba Central, navigate to Context: **Groups / campus-gw-site-cluster** > Navigation: **Devices**> Top: **Gateways** > **List**.
29. Click the **Clusters** page.

- **Question**: How many clusters do you see?
- **Answer**: 1. Since you currently only have gateways in 1 site, only 1 site-based cluster is created.
- **Question**: What is the name of the cluster?
- **Answer**: You can recognize a site cluster based on the site text in the cluster name. Example name: auto_gwcluster_site_3_131_0.

  The first number (3 in the example) is the Central internal Site id, the second number (131 in the example) is the Central internal Group id.

30. Expand the **auto_gwcluster_site** to list the member gateways.



Create WLAN with the Site-Based Cluster

Now that the site-based cluster group was created and verified, you will create a WLAN on the Access Points that will point to the site-based cluster.

31. In Aruba Central, navigate to Context: **Groups / campus-gw-site-cluster** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
32. On the **System** page, set the **Country code** to **US**.

> **IMPORTANT:** This must be set to US, since the remote lab hardware is based in the US.

33. Set the Time zone to **Eastern-Time (UTC-05)**.
34. Click **Save Settings**.

35. On the WLAN page, click **Add SSID**.
36. On the General page, configure:
    - Name(SSID): **p#tx-employee**

NOTE: Make sure to replace the # value with your pod number and x with your table number. For example, if you are using table 07 in pod 28, your WLAN name will be

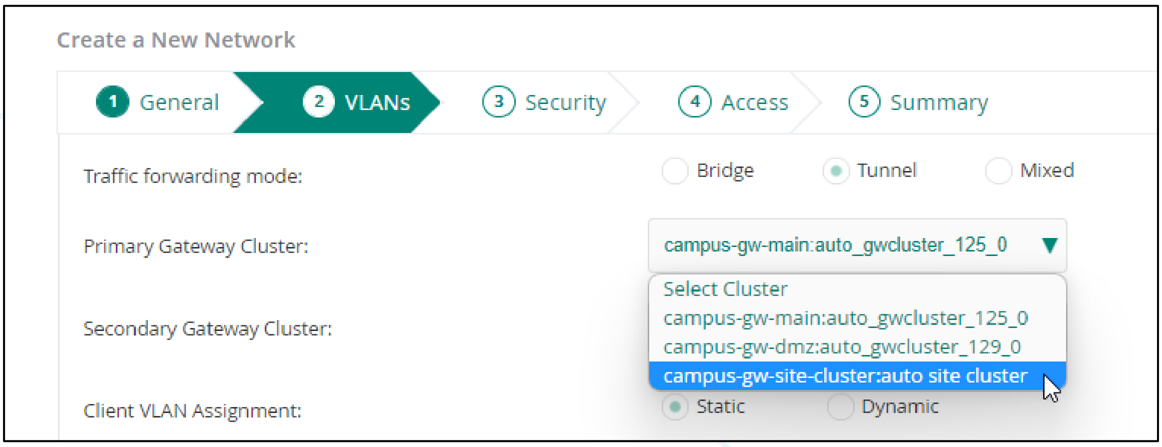
p28t07-employee

This represents p(od) 28 and t(able) 07.

Check with your instructor if you are not sure about the pod and table number.

---

37. Click **Next**.
38. On the VLAN page, configure:
    - Forwarding mode: **Tunnel**
    - Primary Cluster: Select the Site based cluster for group **campus-gw-site-cluster**
    - Client VLAN Assignment: **Static**
    - VLAN ID: **employee**



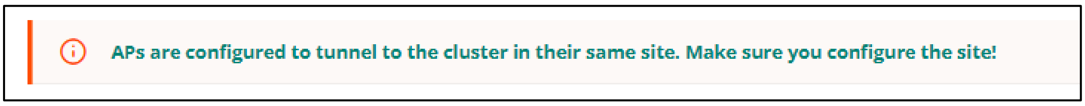
- **Question**: Does the cluster name match the name you reviewed in the previous section?
- **Answer**: No. In the previous section the cluster name contained the side id and group id. For example auto_gwcluster_site_3_131_0.
- **Question**: Why is this cluster name not shown in this list?
- **Answer**: A site cluster will build a cluster for each site. This means that a single group with 10 sites will result in 10 unique clusters to be build.

The goal is to simplify the configuration.

So instead of having to create 10 AP groups and point each AP group WLAN to a unique cluster for its own site, the new WLAN primary cluster will simply point to this placeholder auto site cluster object.

When an AP connects to Aruba Central, it will automatically be pointed to the correct, unique cluster for its own site. This means that a single group can be used to point APs in 10 different sites to their own clusters, each in their own site.

- **Question**: Why do you see this warning when selecting a site-based cluster?



- **Answer**: While the site-based cluster is very convenient, there is the risk that you may add an AP without a site assignment or an invalid site assignment. In that case, the AP would not get any instruction to setup a tunnel and the tunnel WLAN would not be functional on this AP.

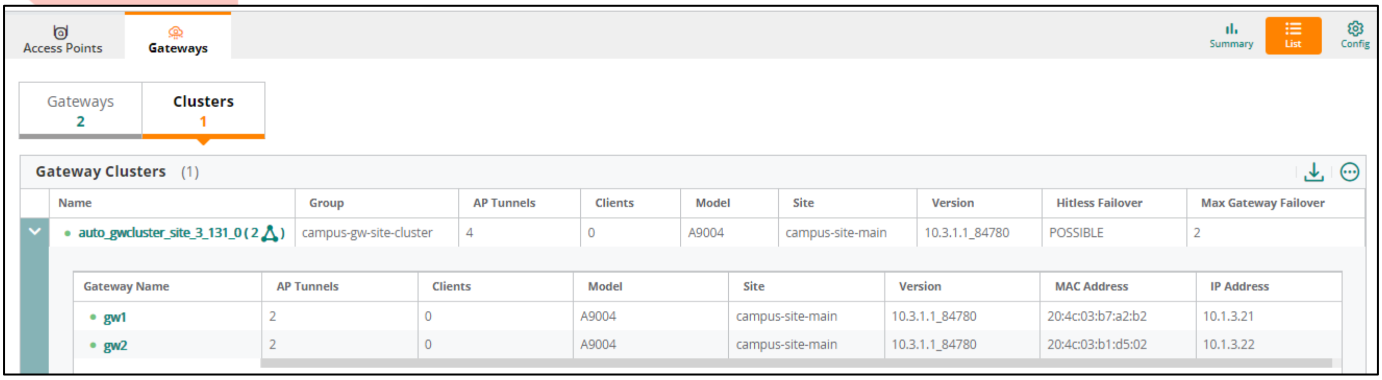
- **Question**: What are the available VLANs in the list?

- **Answer**: The VLAN list is derived from the selected primary cluster group campus-gw-site-cluster. During the Guided setup of the new group you have added the named VLAN employee(31).

39. Click **Next**.
40. On the **Security** page, move the slider to **Enterprise**.
41. For primary server, add:
    - Name: **cppm1**
    - IP: **10.254.1.23**
    - Shared key: **Aruba123!**
    - Retype key
42. Click **Advanced Settings**.
43. For Accounting, select **Use Authentication Servers**.
44. Click **Next**.
45. On the **Access** page, leave **Unrestricted**.
46. Click **Next**.
47. Click **Finish**.
48. Click **OK** when the wizard completes.

Verify AP to Gateway Tunnels are Established

49. In Aruba Central, navigate to Context: **Groups / campus-gw-site-cluster** > Navigation: **Devices**> Top: **Gateways** > **List**.
50. On the **Clusters** page, expand the **auto_gwcluster**.



- **Question**: How many AP tunnels are reported for the cluster?
- **Answer**: 4. Each AP establishes a tunnel to each GW in the cluster because they all belong to the same site.

Verify the Cluster Tunnel Status on the AP

51. Use the lab dashboard to open a console connection to your ap1.
52. Review the overlay cluster-info.

```
show overlay cluster-info
```

```
ap1# show overlay cluster-info

Cluster auto_gwcluster_site_3_131_0 - Zone 0 Multicast-Vlan 0 bktmap_refs 1 uac_refs
2
--------------------------------------------------------------------------------
-
Index  Zone  UAC IP     HeartBeat  MTU   Refs  Odev  HeartBeat
Sequence/Send/Recv/Drop  Clients  Overlay-Vlans
-----  ----  ------     ---------  ---   ----  ----  -------------------------------
-  -------  -------------
0      0     10.1.3.21  1          1500  1     tun0  91/89/88/0
0        1,3,31
1      0     10.1.3.22  1          1500  1     tun1  90/88/87/0
0        1,3,31
```

- **Question**: Do you see the actual cluster name in this output?
- **Answer**: Yes. The APs and Gateways belong to the same site. In the example output, this was site with internal ID 3.

53. Review the SSID to cluster mapping status.

```
show overlay ssid-cluster status
```

```
ap1# show overlay ssid-cluster status

[SSID(p28t13-employee) Information]
-----------------------------------
Parameter                Value
---------                -----
Type                     wireless
Primary cluster          auto_gwcluster_site_3_131_0
Backup cluster           N/A
Current cluster          auto_gwcluster_site_3_131_0
Preemption knob          Disable
Hold Time                300(s)
Preemption Create time   Null
Preemption Status        No
Map Create time          2022-12-23 06:33:10
```

- **Question**: To what cluster is the WLAN p#tx-employee connected?
- **Answer**: On this AP, the p#tx-employee WLAN is connected to the site-based cluster of the current AP site.

Task 4: Site-Based Clustering using Multiple Sites

In the previous task you have prepared the site-based cluster setup. All gateways and APs were still assigned to the same site **site-campus-main**.

In this task, you will assign GW2 and AP2 to a new site.

Aruba Central is aware that the group is set to site-based cluster, therefore, it will create a new cluster when it notices that the GW2 is assigned to a new site.

When the AP2 is moved to the new site, the overlay tunnel orchestrator will inform AP2 to establish its tunnels to the new site cluster (with GW2).

AP1 will still be connected to the cluster in the original site-campus-main, but that cluster will no longer have the GW2.

Objectives

- Understand process to assign devices to correct site for auto-site based clustering.
- Verify operation of auto-site clustering.

Steps

Create a new Site in Aruba Central.

Aruba Central uses sites to map devices to their physical locations. In Aruba Central, all devices in the same location should be mapped to the same site. A device can only belong to one site.

1. In Aruba Central, navigate to Context: **Global** > Navigation: **Organization** > Top: **Network Structure** > **Sites**
2. At the bottom of the page, click the plus sign to create a **New Site**.

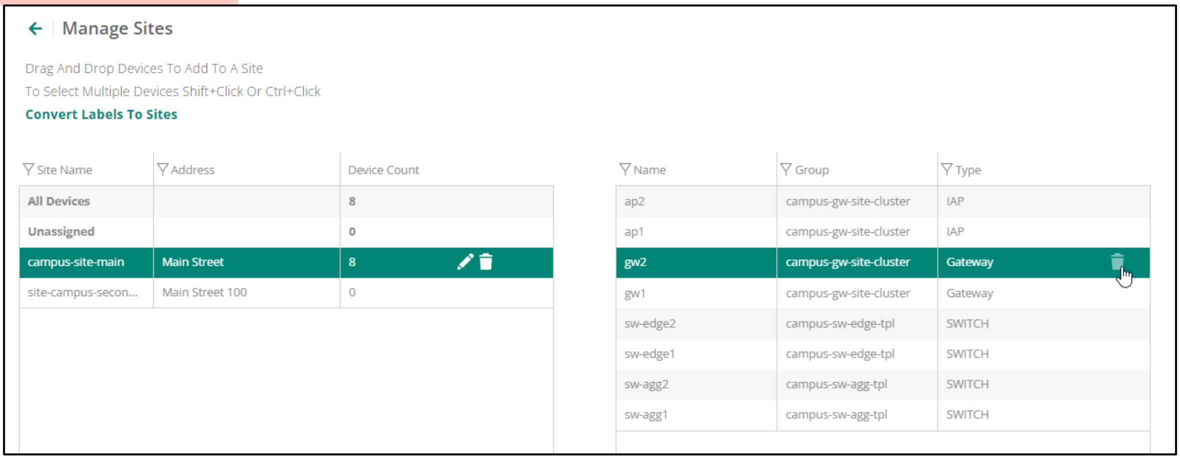
> **NOTE:** This guide uses a fictitious site, feel free to use your own location or site code.

Field	Value
Name	**site-campus-secondary**
Street Address	**Main Street 100**
City	**Oranjestad**
Country	**Aruba**
State	**Aruba**
ZIP	**0000**

3. Click **Add** to save the site.

Move AP2 and GW2 to the New Site

4. In the left pane, select **site-campus-main**.
5. On the right side, **remove gw2**. Confirm with **Yes**.

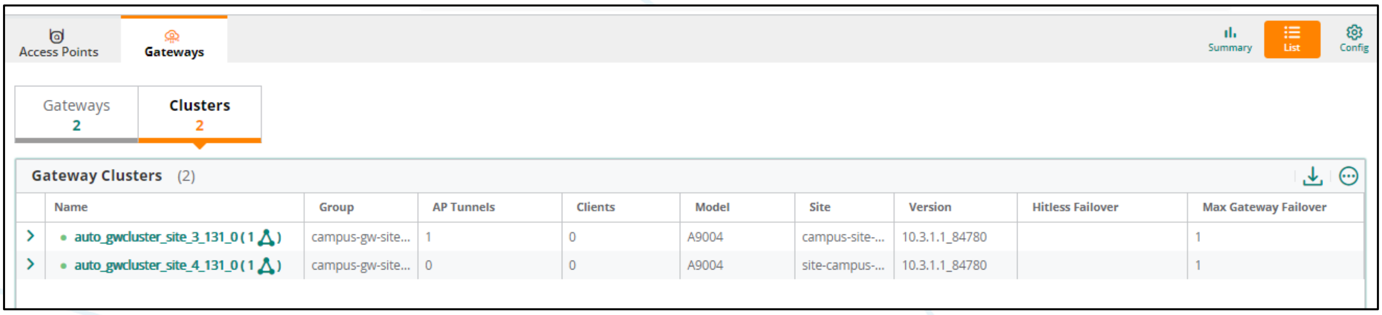


6. **Remove ap2**. Confirm with **Yes**.
7. In the left pane, select **Unassigned**.
8. Select **gw2** and drag it to the site named **site-campus-secondary**.
9. Confirm with **Yes**.

IMPORTANT: Do not move the ap2 to the new site yet! If you have assigned it to the new site, remove it again. You will first review the status with the site mismatch.

Verify the Site Cluster changes in Aruba Central

10. In Aruba Central, navigate to Context: **Groups / campus-gw-site-cluster** > Navigation: **Devices**> Top: **Gateways** > **List**.
11. Open the **Clusters** page.



- **Question**: How many clusters have been created in this group?
- **Answer**: Since there are 2 sites now, Central has created 2 clusters, each with the gateways of the respective sites.

- **Question**: What is the difference in the cluster names between the 2 sites?
- **Answer**: Both clusters are based in the same group, in the example output this is id 131. They have a unique site code based on the internal site id. In the example output, these are site ids 3 and 4.
- **Question**: How many AP tunnels do you see on the original auto_gwcluster?
- **Answer**: 1. Only 1 AP is currently assigned to the site-campus-main.
- **Question**: How many AP tunnels do you see on the new auto_gwcluster (for the site-campus-secondary)?
- **Answer**: 0. No AP has been assigned to this site yet.

Verify Status on AP1: site-campus-main

12. On the console connection of AP1, review the overlay tunnel configuration.

```
show overlay tunnel config
```

```
ap1# show overlay tunnel config

Overlay Tunnel Config
Cluster auto_gwcluster_site_3_131_0 - Zone 0
-------------------------------------------
Index  UAC IP     Tunnel Type  Heartbeat  MTU   Vlan List
-----  ------     -----------  ---------  ---   ---------
0      10.1.3.21  GRE          Enabled    1500  1,3,31
```

- **Question**: How many tunnels do you see on the AP1?
- **Answer**: AP1 is assigned to the same site as GW1. Since the cluster of the site only contains 1 gateway, only 1 tunnel is established.

13. Review the SSID to cluster mapping.

```
show overlay ssid-cluster status
```

```
ap1# show overlay ssid-cluster status

[SSID(p28t13-employee) Information]
-----------------------------------
Parameter                Value
---------                -----
Type                     wireless
Primary cluster          auto_gwcluster_site_3_131_0
Backup cluster           N/A
Current cluster          auto_gwcluster_site_3_131_0
Preemption knob          Disable
Hold Time                300(s)
```

```
Preemption Create time  Null
Preemption Status       No
Map Create time         2022-12-23 06:33:10
```

14. Review the AP BSS Table.

```
show ap bss-table
```

```
ap1# show ap bss-table

Aruba AP BSS Table
------------------
bss                ess              port  ip          phy    type  ch/EIRP/max-EIRP    
cur-cl  ap name  in-t(s)  tot-t      flags  mu-mimo
---                ---              ----  --          ---    ----  ----------------    -
-----  -------  -------  -----      -----  -------
f4:2e:7f:7b:15:f0  p28t13-employee  ?/?   10.1.4.50   a-VHT  ap    100E/15.0/25.5     0
ap1      0       1h:7m:24s  W3r     1
f4:2e:7f:7b:15:e0  p28t13-employee  ?/?   10.1.4.50   g-HT   ap    11/7.0/23.0        0
ap1      0       1h:7m:24s  W3r     0

Channel followed by "*" indicates channel selected due to unsupported configured
channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:2
Num Associations:0
```

- **Question**: Is the WLAN advertised by the AP?
- **Answer**: Yes, the AP has cluster information and active connections, therefore it will advertise the WLAN.

Verify Status on AP2: Unassigned Site

In the next steps you will verify the status on AP2. This AP currently does not have a site assigned.

15. Open a console connection to AP2.

```
show overlay tunnel config
```

```
ap2# show overlay tunnel config

Overlay Tunnel Config
```

- **Question**: What do you notice?
- **Answer**: AP2 did not receive any cluster information. This is expected, since it does not belong to a site that contains a GW cluster.

IMPORTANT: This shows that it is critical for the APs and GWs to have the same site assignment in a site-based cluster. An AP without site assignment will not have any tunnels and will not be able to provide WLAN service for the site-based tunnel WLAN.

16. Review the SSID to cluster mapping. There will be no mapping at this point.

```
show overlay ssid-cluster status
```

```
ap2# show overlay ssid-cluster status

ap2#
```

17. Review the current BSS table.

```
show ap bss-table
```

```
ap2# show ap bss-table

Aruba AP BSS Table
------------------
bss  ess  port  ip  phy  type  ch/EIRP/max-EIRP  cur-cl  ap name  in-t(s)  tot-t
flags  mu-mimo
---  ---  ----  --  ---  ----  ----------------  ------  -------  -------  -----  ---
--  -------

Channel followed by "*" indicates channel selected due to unsupported configured
channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:0
Num Associations:0
```

- **Question**: What do you observe?
- **Answer**: When there is no cluster information, the AP will not advertise the WLAN.

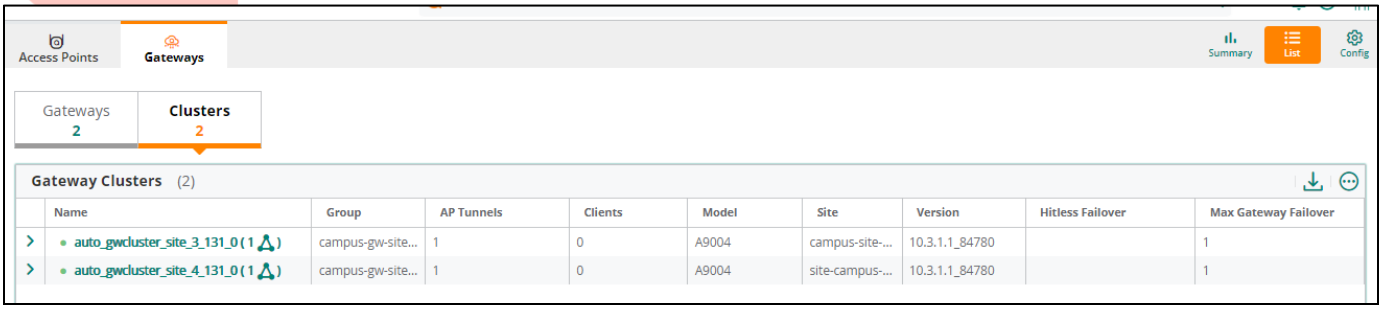
Assign AP2 to site-campus-secondary

You will now correct the configuration by assigning AP2 to the same site as GW2.

18. In Aruba Central, navigate to Context: **Global** > Navigation: **Organization** > Top: **Network Structure** > **Sites**.
19. Select **Unassigned**.
20. Assign ap2 to the site **site-campus-secondary**. Confirm with **Yes**.

Verify the Cluster in site-campus-secondary

21. In Aruba Central, navigate to Context: **Groups / campus-gw-site-cluster** > Navigation: **Devices**> Top: **Gateways** > **List**.
22. Click the **Clusters** page.



- **Question**: How many tunnels do you see for each cluster?
- **Answer**: Each cluster now has 1 AP tunnel.

23. On the console of AP2, review the overlay status.

```
show overlay tunnel config
```

```
ap2# show overlay tunnel config

Overlay Tunnel Config
Cluster auto_gwcluster_site_4_131_0 - Zone 0
--------------------------------------------
Index  UAC IP     Tunnel Type  Heartbeat  MTU   Vlan List
-----  ------     -----------  ---------  ---   ---------
0      10.1.3.22  GRE          Enabled    1500  1,3,31
```

- **Question**: What is the gateway IP address for the tunnel?
- **Answer**: 10.1.3.22. This is gateway 2, it belongs to the same site as the AP2.

24. Review the SSID to cluster mapping.

```
show overlay ssid-cluster status
```

```
ap2# show overlay ssid-cluster status

[SSID(p28t13-employee) Information]
-----------------------------------
Parameter               Value
---------               -----
Type                    wireless
Primary cluster         auto_gwcluster_site_4_131_0
Backup cluster          N/A
Current cluster         auto_gwcluster_site_4_131_0
```

```
Preemption knob         Disable
Hold Time               300(s)
Preemption Create time  Null
Preemption Status       No
Map Create time         2022-12-23 07:25:39
```

25. Review the active BSS table.

```
show ap bss-table
```

```
ap2# show ap bss-table

Aruba AP BSS Table
------------------
bss                ess            port  ip         phy    type  ch/EIRP/max-EIRP   cur-cl  ap name  in-t(s)  tot-t  flags  mu-mimo
---                ---            ----  --         ---    ----  ----------------   ------  -------  -------  -----  -----  -------
00:4e:35:75:ff:d0  p28t13-employee  ?/?   10.1.4.51  a-VHT  ap    56E/15.0/27.0     0 ap2      0        7s     W3r    1
00:4e:35:75:ff:c0  p28t13-employee  ?/?   10.1.4.51  g-HT   ap    6/7.0/23.0        0 ap2      0        7s     W3r    0

Channel followed by "*" indicates channel selected due to unsupported configured
channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:2
Num Associations:0
```

- **Question**: What do you observe?
- **Answer**: The AP now received the cluster information. With the tunnels established, it will advertise the WLAN.

This shows how AP1 automatically connects to the local site cluster with GW1 and AP2 automatically connects to its own local site cluster with GW2.

This concludes the site-based cluster setup.

Optional Task 5: Site-Based Cluster with Group-Based Backup Cluster

In this optional task, you can explore the cluster redundancy option.

The typical redundancy is provided by having multiple gateways in a single cluster.

It is possible to provide a secondary cluster in the WLAN configuration, this task will explore this configuration.

When the primary cluster of a WLAN is site-based, the secondary cluster must be group-based.

In this lab task, the existing site-based WLAN will be reconfigured with a group-based secondary cluster.

Objectives

- Configure cluster redundancy.
- Understand the failover between clusters.
- Understand the cluster pre-empt mechanism.

Steps

Move GW1 to a Group-Based Cluster Group

In the next steps you will move the GW1 back to the group campus-gw-main.

1. In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Groups**
2. Expand *All connected devices* by clicking the **>** icon.
3. Under All connected devices, select the gateway **gw1**.
4. On the right-hand side, a popup will be displayed with the **Move Devices** action button.
5. Click the **Move Devices** button.
6. Click the **Destination Group** field.
7. Select the group **campus-gw-main.**
8. Click the **Move** button to continue.
9. Click **OK** to confirm the move message.

Review the Group Cluster

You have previously changed the cluster mode on the group from automatic to manual to configure the Dynamic Authorization VRRP addresses.
After moving the gateway, it will no longer automatically be configured as a cluster in the group.

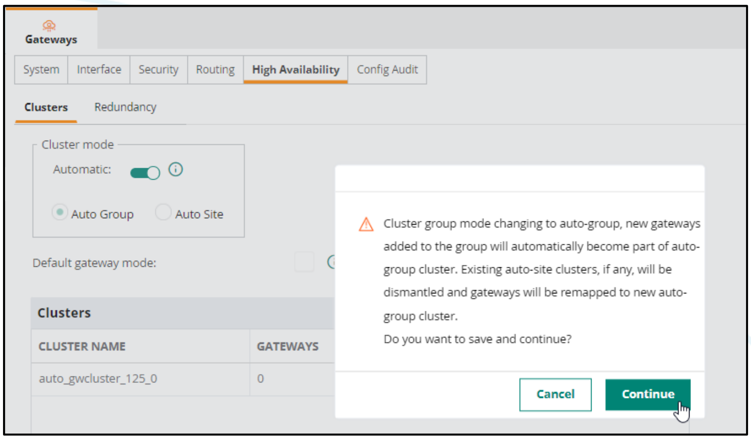
10. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **List**.
11. Open the **Clusters** page.

- **Question**: What do you observe?
- **Answer**: After the gateway move, the gateway still belongs to the site-based cluster.

NOTE: Central may also cleanup the site-based cluster after the gateway has completed the reboot, so you may also see 0 clusters.

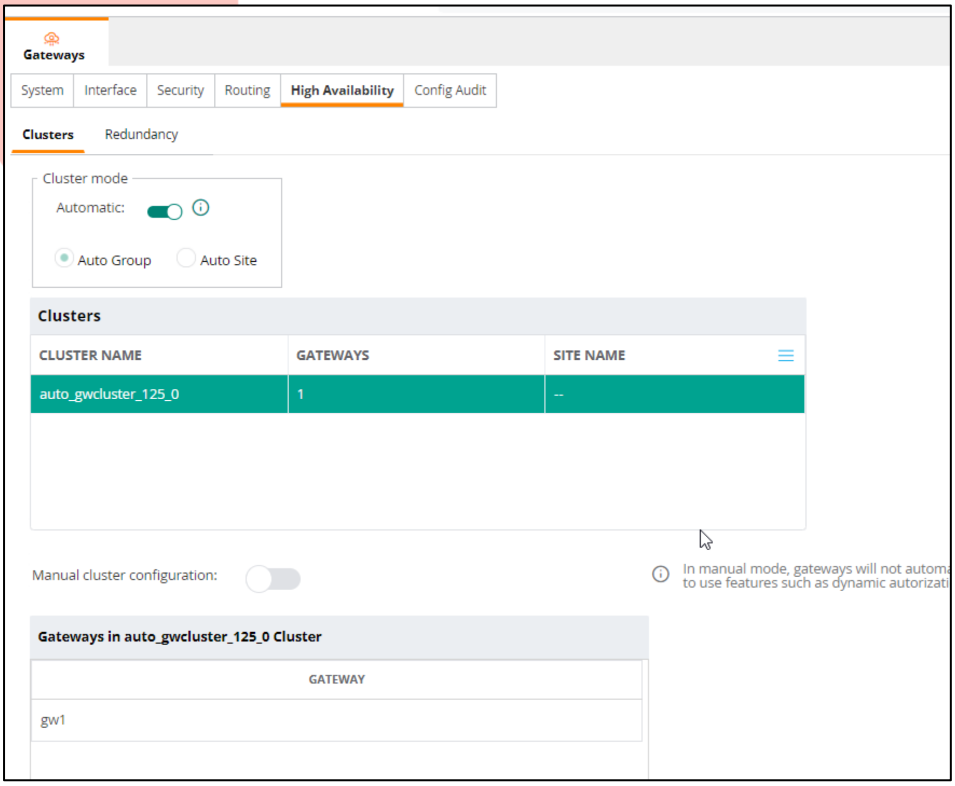
Reconfigure the Group Cluster

12. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
13. Click **High Availability**.
14. Set cluster mode to **Automatic**.
15. Select **Auto Group** and confirm the change

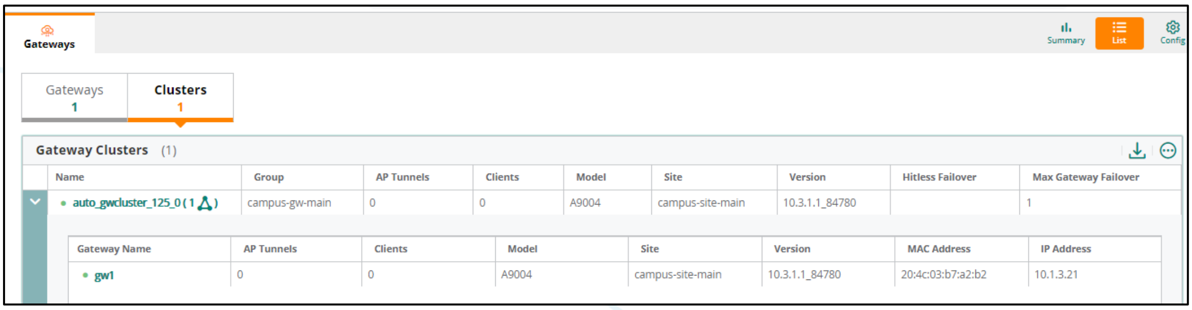


.

16. In the cluster list, select **auto_gwcluster**.
17. Set the Manual Cluster to **disabled** (this means automatic).
18. Confirm the message.
19. Select the **auto_gwcluster** and verify that gw1 is listed.



20. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **List**.
21. Click **Clusters**. gw1 should now belong to the original group based cluster again.



Reconfigure the Employee WLAN

Now you have a site-based cluster (with GW2) and a group-based cluster (with GW1). With these 2 clusters, you will be able to configure a WLAN with cluster redundancy.

22. In Aruba Central, navigate to Context: **Groups / campus-gw-site-cluster** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
23. Remove your **p#tx-employee** WLAN.
24. Click **Add SSID** to create a new p#tx-employee WLAN
25. On the General page:
    - Name(SSID): p#tx-employee

NOTE: Make sure to replace the # value with your Pod number and x with your table number.
For example, if you are using Table 07 in Pod 28, your WLAN name will be

p28t07-employee

This represents p(od) 28 and t(able) 07.

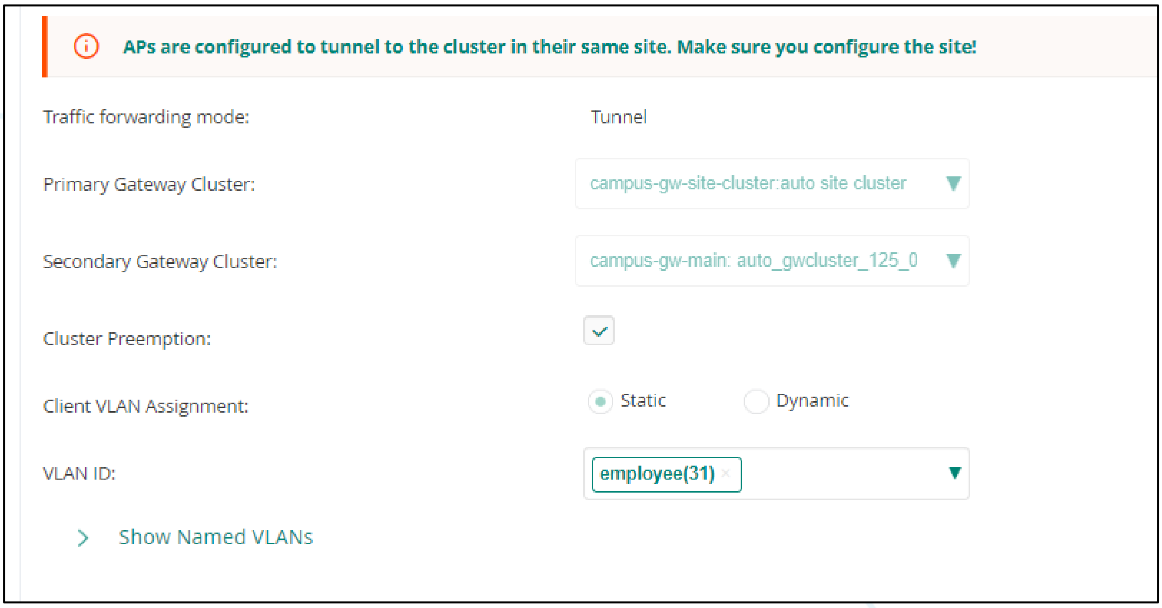
Check with your instructor if you are not sure about the Pod and Table number.

26. Click **Next**.
27. On the **VLAN** page, configure:

- Traffic forwarding mode: **Tunnel**
- Primary: **site cluster: campus-gw-site-cluster**
- Secondary: **group cluster: campus-gw-main**
- Cluster Preempt: **yes**
- VLAN: **employee**

- **Question**: What VLANs do you see in the VLAN ID list?

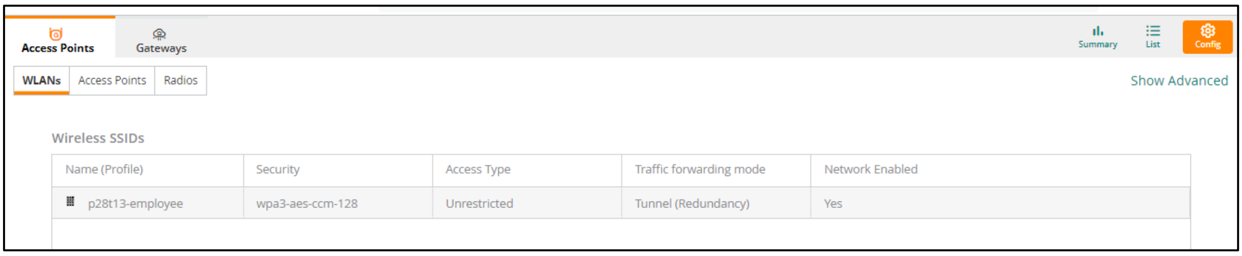
- **Answer**: The VLAN list is based on the Primary Gateway cluster.



28. Click **Next**.
29. On the **Security** page, configure:

- Mode: **Enterprise**
- Primary server: select **cppm1** (existing server)

30. Expand **Advanced Settings > Set Accounting to Use Authentication Servers**.
31. Click **Next**.
32. On the **Access** page, leave the default to unrestricted.
33. Click **Next**.
34. Click **Finish**.
35. Click **OK** when the wizard completes.
36. Verify the new WLAN in the list traffic forwarding mode shows Tunnel (Redundancy).



Test Cluster Failover and Preempt

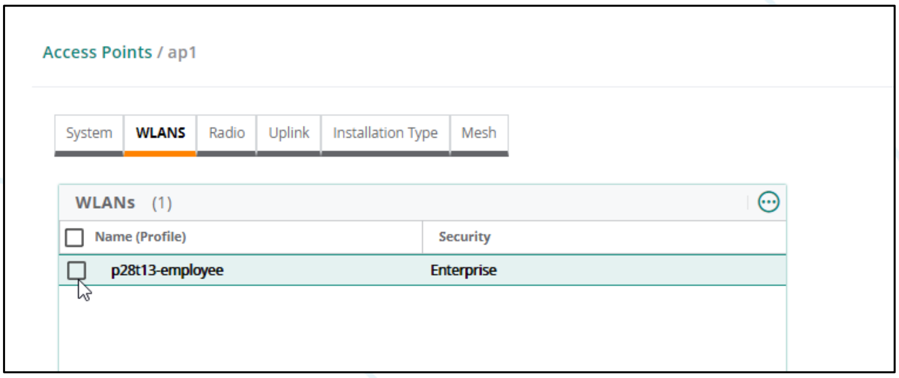
In the next section you will first test the cluster failover and then the preempt function when the original cluster comes back online.

Currently, only your AP2 is active in the site-cluster (GW1 was removed from the site-cluster and is now part of the campus-gw-main group-based cluster).

To simplify the testing with AP2, disable all WLANs on AP1. This will ensure the wireless client will connect to AP2.

AP1: Disable WLANs

37. In Aruba Central, navigate to Context: **Groups / campus-gw-site-cluster** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
38. Click **Access Points**.
39. Edit *ap1* using the **pencil** button.
40. On the WLANs page, disable all WLANs (unchecked).



41. Click **Save Settings**.
42. Verify in the AP list that:
    - ap1 does not have any entries in the WLANs column.
    - ap2 has ***All SSIDs selected***.

Access Points (2)

Name	Status	IP Address	WLANs	Radio Profile	Type
ap2	Online	10.1.4.51	All SSIDs selected	default	AP-303H
ap1	Online	10.1.4.50		default	AP-303H

Now you are sure that your wireless client will connect to the AP2. AP2 is primarily using the site cluster, with the group-based cluster as the secondary cluster.

Connect with PC4 to your employee-site WLAN

43. On PC4, connect to the p#tx-employee WLAN with EAP-TLS.
44. Click **Connect using a certificate** to connect to the WLAN.
45. Click **Connect** to accept the certificate warning.
46. On PC4, start a continuous ping to 10.254.1.21

```
ping 10.254.1.21 -t
```

```
C:\Users\student> ping 10.254.1.21 -t

Pinging 10.254.1.21 with 32 bytes of datAnswer:
Reply from 10.254.1.21: bytes=32 time=7ms TTL=126
Reply from 10.254.1.21: bytes=32 time=19ms TTL=126
Reply from 10.254.1.21: bytes=32 time=12ms TTL=126
...
```

Verify the Cluster Status on AP2

47. On the console of AP2

```
show overlay ssid-cluster status
```

```
ap2# show overlay ssid-cluster status

[SSID(p28t13-employee) Information]
-----------------------------------
Parameter                Value
---------                -----
Type                     wireless
Primary cluster          auto_gwcluster_site_4_131_0
Backup cluster           auto_gwcluster_125_0
Current cluster          auto_gwcluster_site_4_131_0
Preemption knob          Enable
Hold Time                300(s)
```

```
Preemption Create time  Null
Preemption Status       No
Map Create time         2022-12-23 08:22:15
```

- **Question**: What is the Primary and Backup cluster configuration for the p#tx-employee WLAN?
- **Answer**: This is based on the WLAN configuration. The Primary cluster points to the site cluster and the backup cluster points to the group-based cluster.
- **Question**: Is Preemption enabled?
- **Answer**: Yes, you have enabled this option during the WLAN wizard. This will ensure that the APs revert after 5 minutes to the original cluster when it is reachable again.

NOTE: The AP will only revert to the original cluster if it has equal or more gateway tunnels active to the original cluster. This is a safety check to ensure that the original cluster is at equal or better capacity than the current backup cluster.

IMPORTANT: Make sure you don't configure a WLAN with a primary cluster of 2 gateways to a backup cluster with 4 gateways, since the APs would never consider the original cluster of 2 gateways *good enough* to revert to when they are connected to the 4-node backup cluster.

48. Review the configured tunnels. Both primary and backup clusters should be listed.

```
show overlay tunnel
```

```
ap2# show overlay tunnel

Overlay Tunnel Config
Cluster auto_gwcluster_site_4_131_0 - Zone 0
--------------------------------------------
Index  UAC IP     Tunnel Type  Heartbeat  MTU   Vlan List
-----  ------     -----------  ---------  ---   ---------
0      10.1.3.22  GRE          Enabled    1500  1,3,31
Cluster auto_gwcluster_125_0 - Zone 1
-------------------------------------
Index  UAC IP     Tunnel Type  Heartbeat  MTU   Vlan List
-----  ------     -----------  ---------  ---   ---------
0      10.1.3.21  GRE          Enabled    1500  1,3,31-32,34-35
```

49. Review the current tunnel status.

```
show ata endpoint
```

```
ap2# show ata endpoint

ATA Endpoint Status
-------------------
UUID                                  IP ADDR    STATE              TUN DEV   TUN
SPI(OUT/IN)    LINK TAG  VALID TIME(s)  TUNNEL TYPE  GRE VLANs
HBT(Jiff/Missed/Sent/Rcv)  INNER IP   UP TIME(s)
----                                  -------    -----              -------   -------
--------    --------  -------------  -----------  ---------       ------------------
-------  --------   ----------
13aac1f1-9d70-45be-a30c-554bee010059  10.1.3.21  SM_STATE_CONNECTED  tun1
b39e5800/659b0000  inet      128316        GRE          1,3,31-32,34-35
1004639/0/1311/1279        10.1.4.51  2022-12-23 08:22:19
358957b8-336a-49ca-8a74-b6b182faad0d  10.1.3.22  SM_STATE_CONNECTED  tun0
7c9c9000/2dce4000  inet      128314        GRE          1,3,31
1004639/0/1312/1280        10.1.4.51  2022-12-23 08:22:18
Total Endpoints Count: 2
```

- **Question**: What is the current state for the tunnels?
- **Answer**: Both tunnels to the primary and backup are connected. The AP will not wait for a failure of the primary cluster before it establishes the tunnels to the backup cluster.

50. Review the active clients for each cluster.

```
show overlay cluster-info
```

```
ap2# show overlay cluster-info

Cluster auto_gwcluster_site_4_131_0 - Zone 0 Multicast-Vlan 0 bktmap_refs 1 uac_refs
1
------------------------------------------------------------------------------------
-
Index  Zone  UAC IP     HeartBeat  MTU   Refs  Odev  HeartBeat
Sequence/Send/Recv/Drop  Clients  Overlay-Vlans
-----  ----  ------     ---------  ---   ----  ----  -------------------------------
-  -------  -------------
0      0     10.1.3.22  1          1500  1     tun0  1462/1496/1459/0
1        1,3,31
Cluster auto_gwcluster_125_0 - Zone 1 Multicast-Vlan 0 bktmap_refs 1 uac_refs 1
------------------------------------------------------------------------------
Index  Zone  UAC IP     HeartBeat  MTU   Refs  Odev  HeartBeat
Sequence/Send/Recv/Drop  Clients  Overlay-Vlans
-----  ----  ------     ---------  ---   ----  ----  -------------------------------
-  -------  -------------
0      1     10.1.3.21  1          1500  1     tun1  1461/1495/1458/0
0        1,3,31-32,34-35
```

- **Question**: What is the client count for the site-based cluster versus the group-based cluster?

- **Answer**: Since the primary cluster is available, the client is currently active on the primary cluster.

Test the Cluster failover to the Secondary Cluster

In the next steps, you will test the cluster failover by rebooting gateway gw2. First you will review the user table on the gateway to confirm the client is currently active on this cluster.

51. Open a console/SSH connection to GW2.
52. Verify the client is in the user table.

```
show user-table
```

```
(gw2) # show user-table

Users
-----
    IP            MAC            Name       Role            Age(d:h:m)  Auth    VPN
link     Connected To     Roaming   Essid/Bssid/Phy  Profile
Forward mode  Type  Host Name  User Type
----------  ------------       ------      ----             ----------  ----    -----
---  ------------------  -------   ---------------  -------
------------  ----  ---------  ---------
10.1.31.51  3c:37:86:d4:b0:81  contractor  p28t13-employee  00:00:00    802.1x
20:4c:03:5b:27:e2   Wireless  p28t13-employee  p28t13-employee_#1671801529103_42#_
dtunnel                          WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/2 Free:0/1 Dyn:1 AllocErr:0 FreeErr:0
```

53. Next reboot the gateway.

```
reload
```

```
(gw2) # reload
Do you really want to restart the system(y/n): y

System will now restart!
Log infrastructure ended gracefully.
```

Verify Cluster Failover on the Client PC4

The client will be disconnected during a failover from the primary to the secondary cluster. Manually attempt to reconnect the client, since the Wireless client in the remote lab does not respect the automatically reconnect option for the Wi-Fi profile!

Example ping trace for a client with a functional automatic reconnect.

NOTE: Your lab client PC4 will need a manual reconnect!

```
Reply from 10.254.1.21: bytes=32 time=20ms TTL=126
Reply from 10.254.1.21: bytes=32 time=18ms TTL=126
Reply from 10.254.1.21: bytes=32 time=50ms TTL=126
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.1.33.50: Destination host unreachable.
Reply from 10.254.1.21: bytes=32 time=563ms TTL=126
Reply from 10.254.1.21: bytes=32 time=29ms TTL=126
Reply from 10.254.1.21: bytes=32 time=14ms TTL=126
Reply from 10.254.1.21: bytes=32 time=8ms TTL=126
```

Verify in Aruba Central

54. In Aruba Central, open the PC4 Client details page (AI Search: contractor).
55. The client PC4 should now show as connected on GW1 (the gateway of the backup cluster).

NOTE: It may take 1-2 minutes to see the updated information in Aruba Central.

Verify on AP2

56. On the console of AP2, review the SSID-to-cluster mapping.

```
show overlay ssid-cluster status
```

```
ap2# show overlay ssid-cluster status

[SSID(p28t13-employee) Information]
-----------------------------------
Parameter                Value
---------                -----
Type                     wireless
Primary cluster          auto_gwcluster_site_4_131_0
Backup cluster           auto_gwcluster_125_0
Current cluster          auto_gwcluster_125_0
Preemption knob          Enable
Hold Time                300(s)
Preemption Create time   2022-12-23 08:56:58
Preemption Status        Yes
Map Create time          2022-12-23 08:22:15
```

57. On the AP2 console, verify that the cluster failover was detected.

```
show ap debug sapd-cluster failover-history 10
```

```
ap2# show ap debug sapd-cluster failover-history 10

Cluster Failover History
----------------
Timestamp            ESSID                            ACTION       From/To
---------            -----                            ------       --------
2022-12-23 08:52:32  p28t13-employee                  Failover
auto_gwcluster_site_4_131_0/auto_gwcluster_125_0
```

Preemption of an Existing Cluster

Once the primary cluster tunnel is back online, a default timer of 5 min is used before the pre-empt occurs.

58. About 5 minutes after the GW2 has completed the reboot, the preempt message can be observed.

```
show ap debug sapd-cluster failover-history 10
```

```
ap2# show ap debug sapd-cluster failover-history 10

Cluster Failover History
----------------
Timestamp            ESSID                            ACTION       From/To
---------            -----                            ------       --------
2022-12-23 08:52:32  p28t13-employee                  Failover
auto_gwcluster_site_4_131_0/auto_gwcluster_125_0
2022-12-23 09:02:07  p28t13-employee                  Preempt Back
auto_gwcluster_125_0/auto_gwcluster_site_4_131_0
```

59. The client PC4 can now reconnect via the original cluster connection.

NOTE: The lab client requires a manual reconnect to the WLAN!

This concludes the cluster failover.

Cleanup

You will now restore the APs and GWs in their original groups.

In the next steps you will move GW2 back to the group *campus-gw-main*.

60. In Aruba Central, navigate to Context: **Global** > Navigation: **Organization**> Top: **Network Structure**> **Groups**
61. Expand *All connected devices* by clicking the **>** icon.
62. Under *All connected devices*, select the gateway **gw2**.
63. On the right-hand side, a popup will be displayed with the **Move Devices** action button.
64. Click the **Move Devices** button.
65. Click the **Destination Group** field.
66. Select the group **campus-gw-main.**
67. Click the **Move** button to continue.
68. Click **OK** to confirm the move message.

In the next steps you will move AP1 and AP2 back to the group *campus-wifi-ui*.

69. Expand *All connected devices* by clicking the **>** icon.
70. Under *All connected devices*, select the access points **ap1 and ap2**.
71. On the right-hand side, a popup will be displayed with the **Move Devices** action button.
72. Click the **Move Devices** button.
73. Click the **Destination Group** field.
74. Select the group **campus-wifi-ui**.
75. Click the **Move** button to continue.
76. Click **OK** to confirm the move message.

Wireless Client PC4 Cleanup

77. On PC4, forget the p#tx-employee WLAN.

You have completed this Lab!

Lab 10.01 Wired Access Control

Overview

In this lab you will configure wired access control. You will configure port access on sw-edge2 in this lab activity.

In the first task in this lab you will configure the RADIUS server and enable 802.1X authentication. PC4 will be configured to perform 802.1X authentication on the LAB NIC to authenticate to the network.

In the second task, you will enable MAC authentication. MAC authentication can be used for devices that do not support 802.1X authentication. You will enable both 802.1X and MAC authentication on the same port, concurrently, and explore how the client authentication is processed.

In the last task, you will explore the difference between client-mode and device-mode authentication.

Objectives

- Configure a RADIUS server.
- Configure 802.1X authentication at the global and port level.
- Configure MAC authentication at the global and port level.
- Understand concurrent authentication.
- Understand the difference between client-mode and device-mode port access.

Task 1: Configure sw-edge2 for Access Control and 802.1X

In this task you will configure 802.1X authentication on the sw-edge2 port 1/1/4. This is the port that connects the PC4.

First you will configure the RADIUS server and assign it to an authentication server group.
Next you will enable the 802.1X authenticator process on the switch and enable 802.1X on the port 1/1/4.

To test the authentication, you will configure PC4 to perform 802.1X authentication on the LAB NIC using the previously installed certificate.

After the basic 802.1X authentication has been tested, you will configure port access control for the wired client, by applying access control policies in the wired user role.

Objectives

- Configure a RADIUS server.
- Configure 802.1X authentication at global and port level.
- Verify 802.1X authentication.
- Configure wired port access control.

Steps

Disable Aruba Central in the Switch CLI

You will be making configuration changes on sw-edge2 outside of Aruba Central. To prevent Aruba Central from overwriting your local configuration changes, you will *disable* access to Aruba Central for now.

1. Use the MGMT PC to open an SSH connection to sw-edge2.
2. Disable the Aruba Central connection.

```
aruba-central
 disable
 exit
```

```
sw-edge2(config)# aruba-central
sw-edge2(config-aruba-central)# disable
sw-edge2(config-aruba-central)# exit
```

Configure the RADIUS Server

In the next steps you will configure the RADIUS server

3. Set SVI3 as the source interface for the RADIUS communication

```
ip source-interface all interface vlan3
```

```
sw-edge2(config)# ip source-interface all interface vlan3
```

4. Define the RADIUS server.

```
ip dns host cppm.aruba-training.com 10.254.1.23
radius-server host cppm.aruba-training.com key plaintext Aruba123!
```

```
sw-edge2(config)# ip dns host cppm.aruba-training.com 10.254.1.23
sw-edge2(config)# radius-server host cppm.aruba-training.com key plaintext Aruba123!
```

5. Create a RADIUS server group for port access named **pa**. Assign the server.

```
aaa group server radius pa
 server cppm.aruba-training.com
 exit
```

```
sw-edge2(config)# aaa group server radius pa
sw-edge2(config-sg)#   server cppm.aruba-training.com
sw-edge2(config-sg)# exit
```

6. Enable RADIUS accounting for port access and interim updates every 10 minutes.

```
aaa accounting port-access start-stop interim 10 group pa
```

```
sw-edge2(config)# aaa accounting port-access start-stop interim 10 group pa
```

Configure 802.1X

In the next steps you will set the global 802.1X authenticator process on the switch to use the RADIUS server group and enable the process.

On the port 1/1/4, you will enable 802.1X authentication.

7. Enable the 802.1X authenticator and set it to use the **pa** server group.

```
aaa authentication port-access dot1x authenticator
 radius server-group pa
 enable
 exit
```

```
sw-edge2(config)# aaa authentication port-access dot1x authenticator
sw-edge2(config-dot1x-auth)# radius server-group pa
sw-edge2(config-dot1x-auth)# enable
sw-edge2(config-dot1x-auth)# exit
```

8. Enable the 802.1X authenticator on the port 1/1/4 (connected to PC4). Apply 802.1X timeout settings based on the Aruba Validated Solution Guide.

NOTE: The client limit must be increased, since PC4 is connected via *transit* switches to your lab switch. These transit devices may generate some traffic and consume a client session.

```
interface 1/1/4
 aaa authentication port-access client-limit 4
 aaa authentication port-access dot1x authenticator
  eapol-timeout 30
  max-eapol-requests 1
  max-retries 1
  enable
  exit
 exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# aaa authentication port-access client-limit 4
sw-edge2(config-if)# aaa authentication port-access dot1x authenticator
sw-edge2(config-if-dot1x-auth)# eapol-timeout 30
sw-edge2(config-if-dot1x-auth)# max-eapol-requests 1
sw-edge2(config-if-dot1x-auth)# max-retries 1
sw-edge2(config-if-dot1x-auth)# enable
sw-edge2(config-if-dot1x-auth)# exit
sw-edge2(config-if)# exit
```

9. Define a new user role for contractor. Contractors will be assigned to VLAN 22.

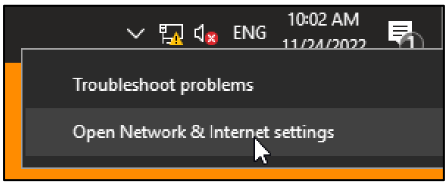
```
port-access role contractor
 vlan access 22
 exit
```

```
sw-edge2(config)# port-access role contractor
sw-edge2(config-pa-role)# vlan access 22
sw-edge2(config-pa-role)# exit
```

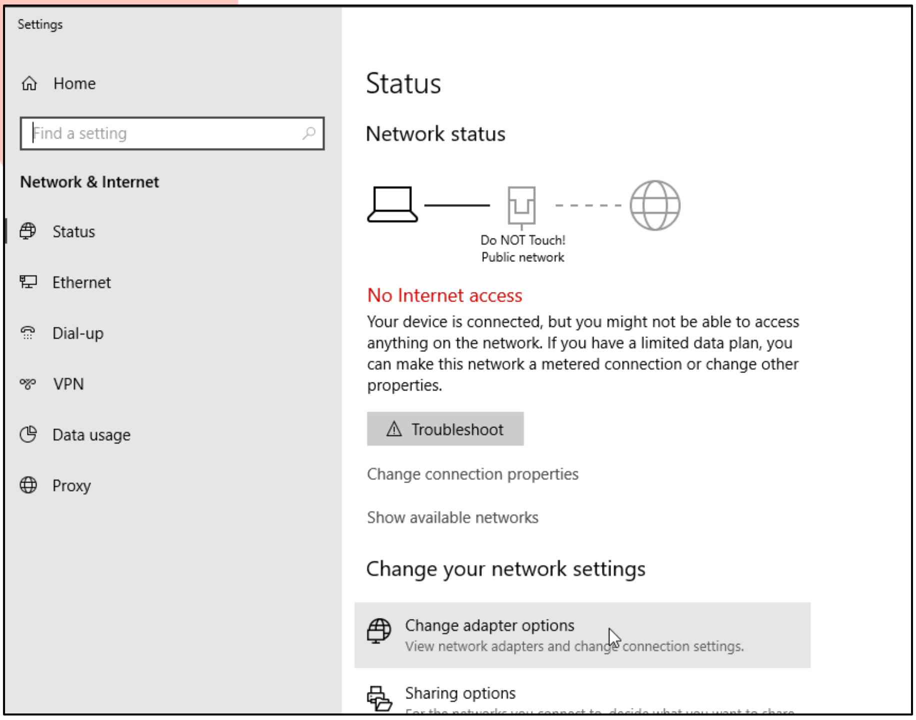
Prepare the PC4 Lab NIC Interface

In the next steps you will prepare the PC4 network interfaces to support wired access to the network.

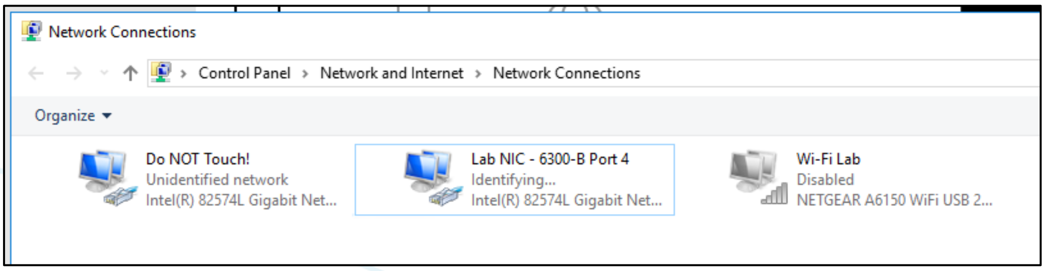
10. Use the lab dashboard to open a connection to PC4.
11. Open the **Network & Internet Settings** from the status bar.



12. Click **Change Adapter Options**.



13. In the NIC List, make sure the **Wifi NIC** is **disabled**.
14. Make sure the **Lab NIC** is **enabled**.



15. Switch to the MGMT PC and open an SSH session to sw-edge2.
16. Review the current VLAN assignment on the port 1/1/4. The port is currently an access port in VLAN 21.

```
show vlan port 1/1/4
```

```
sw-edge2(config)# show vlan port 1/1/4

-------------------------------------------------------------------------------
VLAN  Name                              Mode             Mapping
-------------------------------------------------------------------------------
21    VLAN21                            access           port
```

17. Review the MAC address table for port 1/1/4.

```
show mac-address-table port 1/1/4
```

```
sw-edge2(config)# show mac-address-table port 1/1/4
```

```
MAC age-time              : 300 seconds
Number of MAC addresses : 2

MAC Address          VLAN     Type                      Port
--------------------------------------------------------------
00:50:56:b1:b9:0d    21       port-access-security      1/1/4
ec:b1:d7:1b:07:00    21       port-access-security      1/1/4
```

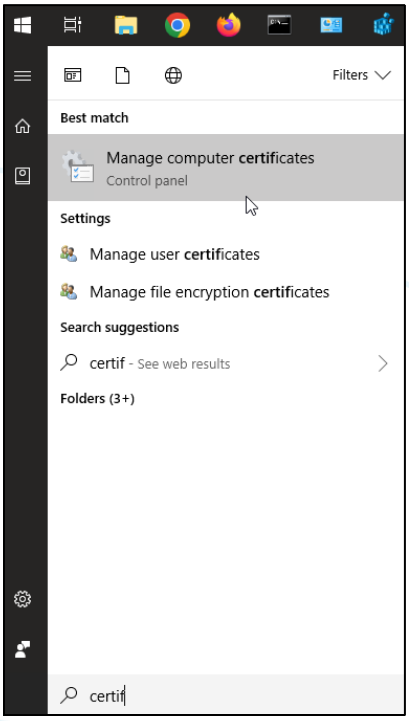
NOTE: In the topology, only PC4 is connected to the port 1/1/4, but you may see additional MAC addresses on the port because of the transit switches between the PC4 and your sw-edge2.

Prepare PC4 as an 802.1X Supplicant

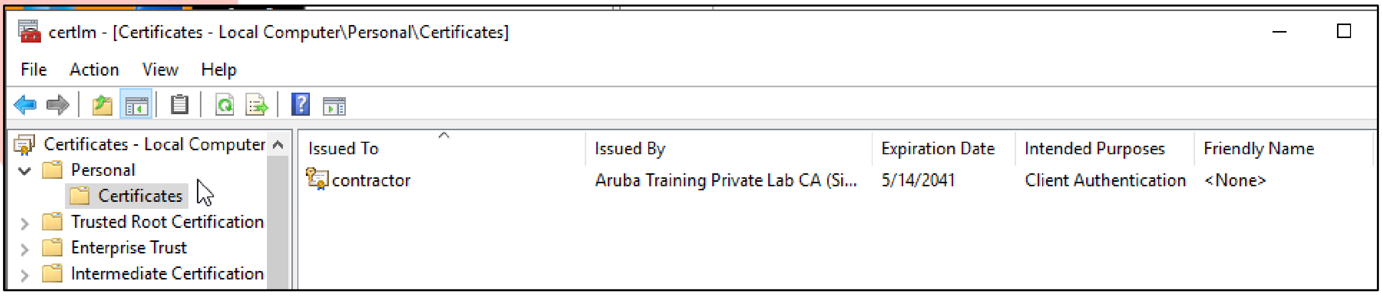
In the next steps you will prepare the 802.1X supplicant on PC4.

18. On PC4, click the **Start Button** and type **certif**.
19. An option should show to *Manage Computer Certificates*. Select it.

NOTE: Pay attention—you **don't** want to select *Manage User Certificates*!



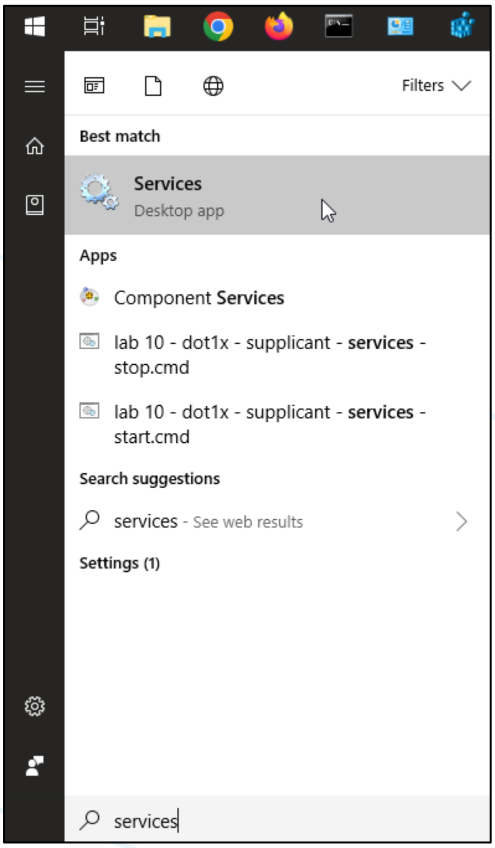
20. Click **Yes** for the admin prompt warning.
21. Expand **Personal > Certificates**.



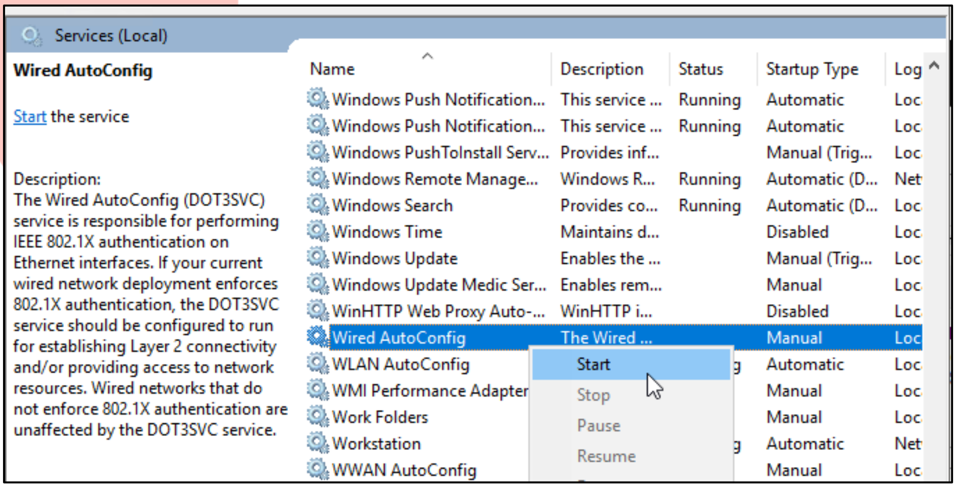
- **Question**: Do you see a machine(computer) certificate installed?
- **Answer**: Yes. This was installed during the ClearPass Onboard certificate enrollment.

NOTE: You are accessing the remote lab PC over RDP. Windows does not support the use of a user certificate for 802.1X when accessing the system over RDP.

22. **Close** the Certificates window.
23. Click Start and type **services**. Click the Services app in the list.



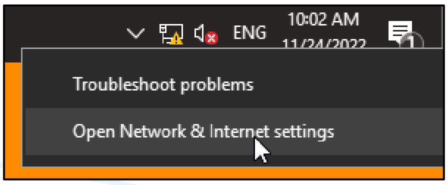
24. Look for the **Wired AutoConfig** service.
25. Right-click on the this line and select **Start**. This is the 802.1X supplicant software on the Windows client.



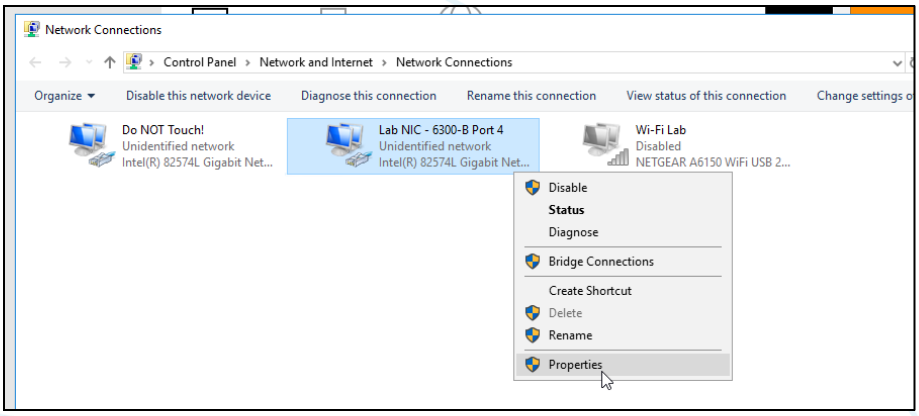
NOTE: In a production environment, you should set this service so start automatically. This is not required in this lab environment.

NOTE: You may leave the Services window open, you will use it later in the lab to stop and start the supplicant.

26. Open the **Network & Internet Settings** from the status bar.



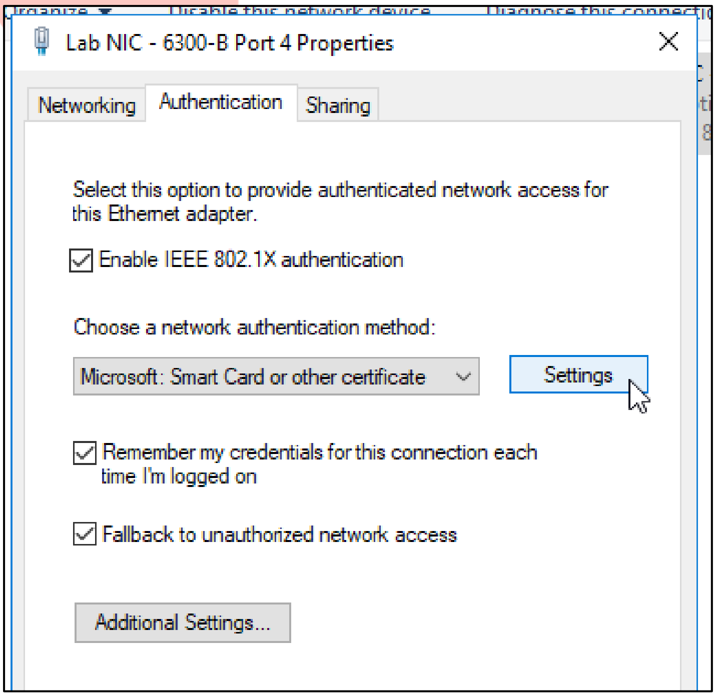
27. Click **Change Adapter Options**.
28. Right-click on the **Lab NIC > Properties**.



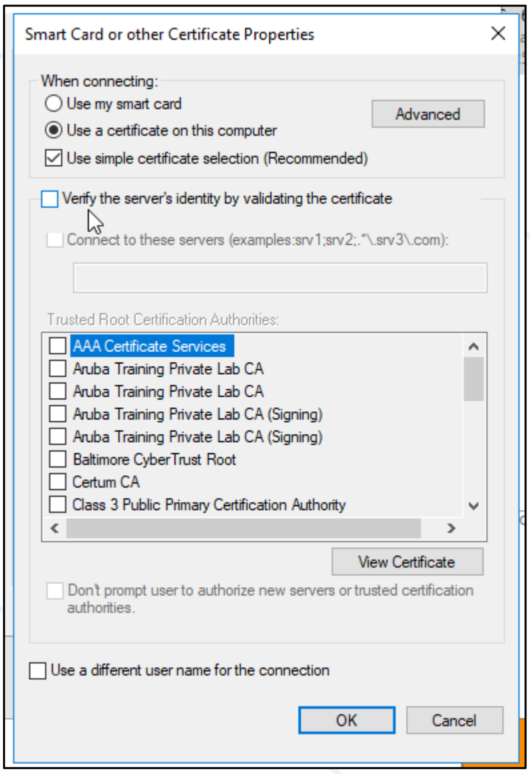
29. Click **Authentication**.

NOTE: If you don't see the authentication page, the Wired AutoConfig service was not started. Check the previous steps to start the service.

- Enable 802.1X authentication: **enabled**
- Method: **Smart Card or other certificate**



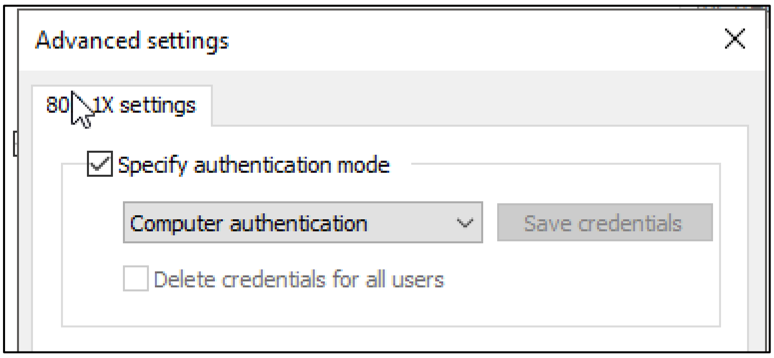
30. Click **Settings**.
31. Uncheck the **Verify the server identity** to simplify the lab testing



NOTE: In a production environment, you should always keep the certificate check enabled!

32. Click **OK**.
33. Click **Additional Settings**.

- Specify authentication mode: **enabled**
- Authentication mode: **Computer authentication** (required for remote lab RDP setup)



NOTE: As stated earlier, you are accessing the remote lab PC over RDP. Windows does not support the use of a user certificate for 802.1X when accessing the system over RDP. Therefore Computer authentication **must** be configured in this lab.

34. Click **OK** to close the Advanced Settings.
35. Click **OK** to close the NIC Properties. The supplicant on PC4 will now attempt to connect with the installed certificate.

NOTE: You may leave the **Network Connections** window open, you'll need it later in this lab.

36. PC4 should now have an IP address in VLAN22.
37. On PC4, open a command prompt (cmd.exe) and check the IP address of the Lab NIC using **ipconfig**.

```
ipconfig
```

```
C:\Users\student> ipconfig

Windows IP Configuration


Ethernet adapter Do NOT Touch!:
```

```
   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.16.28.83
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Lab NIC - 6300-B Port 4:

   Connection-specific DNS Suffix  . : aruba-training.com
   IPv4 Address. . . . . . . . . . . : 10.1.22.50
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.22.1
```

- **Question**: What IP Address did PC4 receive?
- **Answer**: PC4 should have received an IP address in VLAN 22 in the 10.1.22.0/24 subnet.

Verify the 802.1X Client Connection on the Switch

38. On the sw-edge2, review the port access clients.

```
show port-access clients
```

NOTE: You may see other MAC addresses on the port due to transit switches between the PC4 and your sw-edge switch.

```
sw-edge2(config)# show port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-------------------------------------------------------------------------------------
-------------------
  Port      MAC-Address       Onboarding     Status      Role
Device Type
                              Method
-------------------------------------------------------------------------------------
-------------------
c 1/1/4     ec:b1:d7:1b:07:00                Fail
c 1/1/4     00:50:56:b1:b9:0d dot1x          Success     contractor
```

39. Review the port access client details.

```
show port-access clients interface 1/1/4 detail
```

NOTE: Due to the other MAC address on the port, you may need to scroll down in the output to reach your PC4 MAC address.

Example output (filtered to show only the PC4 MAC address).

```
sw-edge2(config)# show port-access clients interface 1/1/4 detail

Port Access Client Status Details:

Client 00:50:56:b1:b9:0d, host/contractor
=========================================
  Session Details
  ---------------
    Port         : 1/1/4
    Session Time : 1123s
    IPv4 Address :
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 22
      Access          : 22
      Native Untagged :
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : dot1x Authenticated
    Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
    Auth History    : dot1x - Authenticated, 208s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 442s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 1062s ago

  Authorization Details
  ----------------------
    Role   : contractor
    Status : Applied


Role Information:

Name  : contractor
Type  : local
----------------------------------------------
    Reauthentication Period            :
    Cached Reauthentication Period     :
    Authentication Mode                :
    Session Timeout                    :
    Client Inactivity Timeout          :
    Description                        :
    Gateway Zone                       :
    UBT Gateway Role                   :
    UBT Gateway Clearpass Role         :
    Access VLAN                        : 22
    Native VLAN                        :
    Allowed Trunk VLANs                :
    Access VLAN Name                   :
    Native VLAN Name                   :
```

```
    Allowed Trunk VLAN Names                    :
    VLAN Group Name                             :
    MTU                                         :
    QOS Trust Mode                              :
    STP Administrative Edge Port                :
    PoE Priority                                :
    PVLAN Port Type                             :
    Captive Portal Profile                      :
    Policy                                      :
    GBP                                         :
    Device Type                                 :
```

- **Question**: What is the status of MAC-auth for the client?
- Answer: Not attempted. MAC-auth is not enabled yet, but even if you would enable MAC-auth, by default, the switch will perform 802.1X authentication first. You will change this in the next section.

40. Review the VLAN configuration of the port 1/1/4.

```
show vlan port 1/1/4
```

```
sw-edge2(config)# show vlan port 1/1/4

-------------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
-------------------------------------------------------------------------------
22    VLAN22                          access          mbv
```

- **Question**: What does the mapping mbv indicate?
- **Answer**: MAC based VLAN. This means that each MAC address that comes online on the port can be assigned its own VLAN. This is different from a port based VLAN, where all MAC addresses on the port will be assigned the same VLAN.

41. Compare this with the running configuration of the port 1/1/4.

```
show running-config interface 1/1/4
```

```
sw-edge2(config)# show running-config interface 1/1/4
interface 1/1/4
    no shutdown
    description pc4
    no routing
    vlan access 21
    aaa authentication port-access client-limit 4
    aaa authentication port-access dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
```

```
      enable
   exit
```

- **Question**: Do you see the active VLAN 22 in the running configuration?
- **Answer**: No, the port-access (authentication) based VLAN assignment is operational on the port, but not stored in the configuration of the switch.

Port Access Policy

In the next steps you will apply a traffic filter for the contractor role by configuring a port access policy.

Using the port access policy, you will filter access for the contractor role and block access to the 10.1.0.0/24 network.

42. On PC4, start a continuous ping to 10.1.0.2. The ping should be successful. This traffic will be blocked in the next steps using a port access policy.

```
ping 10.1.0.2 -t
```

```
C:\Users\student> ping 10.1.0.2 -t

Pinging 10.1.0.2 with 32 bytes of datAnswer:
Reply from 10.1.0.2: bytes=32 time<1ms TTL=64
Reply from 10.1.0.2: bytes=32 time<1ms TTL=64
Reply from 10.1.0.2: bytes=32 time<1ms TTL=64
...
```

43. Create a new IP Class named critical-servers, match on destination IP 10.1.0.0/24. Enable the count option, this will provide a counter that increases for any packet matching the class.

```
class ip critical-servers
 10 match any any 10.1.0.0/255.255.255.0 count
 exit
```

```
sw-edge2(config)# class ip critical-servers
sw-edge2(config-class-ip)# 10 match ip any 10.1.0.0/24 count
sw-edge2(config-class-ip)# exit
```

44. Create a new IP class named **any** and match on any IP traffic.

```
class ip any
 match any any any
 exit
```

```
sw-edge2(config)# class ip any
sw-edge2(config-class-ip)# match any any any
sw-edge2(config-class-ip)# exit
```

45. Create a new port access policy: drop the critical-servers class and allow the *any* class.

```
port-access policy contractor
 10 class ip critical-servers action drop
 20 class ip any
 exit
```

```
sw-edge2(config)# port-access policy contractor
sw-edge2(config-pa-policy)# 10 class ip critical-servers action drop
sw-edge2(config-pa-policy)# 20 class ip any
sw-edge2(config-pa-policy)# exit
```

46. For the user role contractor, associate the port access policy *contractor*. When the port access role changes, the updated role configuration will be immediately applied to the authenticated clients.

```
port-access role contractor
 associate policy contractor
 exit
```

```
sw-edge2(config)# port-access role contractor
sw-edge2(config-pa-role)# associate policy contractor
sw-edge2(config-pa-role)# exit
```

47. PC4 is still attempting to ping; this can now be seen with the hit counter.

```
show port-access policy contractor hitcounts client
```

```
sw-edge2(config)# show port-access policy contractor hitcounts client

Port Access Policy Hit-Counts Details:
======================================

Policy Name   : contractor
Policy Type   : local
Policy Status : applied

SEQUENCE CLASS            TYPE ACTION                            CUR-RATE(kbps)
-------- ---------------- ---- --------------------------------- --------------

Class Name : critical-servers
Class Type : ipv4

SEQUENCE    CLASS-ENTRY                                              HIT-COUNT
----------- -------------------------------------------------------- -----------
10          match any any 10.1.0.0/255.255.255.0 count                 6
```

48. After about 10 seconds, repeat the **show** command to verify hit count increase.

```
show port-access policy contractor hitcounts client
```

```
sw-edge2(config)# show port-access policy contractor hitcounts client
```

```
Port Access Policy Hit-Counts Details:
======================================
...

SEQUENCE CLASS            TYPE ACTION                           CUR-RATE(kbps)
-------- ---------------- ---- -------------------------------- --------------

Class Name : critical-servers
Class Type : ipv4

SEQUENCE    CLASS-ENTRY                                           HIT-COUNT
----------- ----------------------------------------------------- -----------
10          match any any 10.1.0.0/255.255.255.0 count                  8
```

49. On PC4, check that the ping is not working.

```
Request timed out.
Request timed out.
...
```

50. On PC4, you may stop the ping.

Task 2: Enable MAC Authentication

In this task you will configure MAC Authentication to support client devices that don't have an 802.1X supplicant.

Since you may not know in advance whether the connecting device support 802.1X or not, you will need to enable *both* MAC authentication and 802.1X authentication on the port.

This will require either an authentication order or a concurrent authentication system. In this lab, you will configure concurrent authentication for MAC authentication and 802.1X authentication.

Objectives

- Configure MAC authentication at the switch global and port level.
- Understand concurrent authentication (802.1X and MAC-auth).
- Verify MAC authentication.

Steps

Enable MAC Authentecation

In this task you will configure MAC authentication to support client devices that don't have an 802.1X supplicant.

1. Enable global MAC authentication using your RADIUS server group

```
aaa authentication port-access mac-auth
 radius server-group pa
 enable
 exit
```

```
sw-edge2(config)# aaa authentication port-access mac-auth
sw-edge2(config-macauth)# radius server-group pa
sw-edge2(config-macauth)# enable
sw-edge2(config-macauth)# exit
```

2. On port 1/1/4, enable concurrent onboarding. This means both 802.1X and MAC-auth will be attempted concurrently, without having to wait for 1 method to timeout first.

```
interface 1/1/4
 port-access onboarding-method concurrent enable
 exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# port-access onboarding-method concurrent enable
sw-edge2(config-if)# exit
```

3. On port 1/1/4, enable MAC authentication.

```
interface 1/1/4
 aaa authentication port-access mac-auth
```

```
  enable
  exit
 exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# aaa authentication port-access mac-auth
sw-edge2(config-if-macauth)# enable
sw-edge2(config-if-macauth)# exit
sw-edge2(config-if)# exit
```

Create a User Role for a Phone

4. Create a new user role with name *phone* and assign it to VLAN 23.

```
port-access role phone
 vlan access 23
 exit
```

```
sw-edge2(config)# port-access role phone
sw-edge2(config-pa-role)# vlan access 23
sw-edge2(config-pa-role)# exit
```

Verify MAC authentication

5. Use MGMT PC to access ClearPass using admin / Aruba123!

```
https://10.254.1.23/tips
```

6. Navigate to **Monitoring > Live Monitoring > Access Tracker**. Keep this screen open.
7. On sw-edge2, bounce port 1/1/4 and verify the result in ClearPass access tracker.

```
interface 1/1/4
 shutdown
 no shutdown
 exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# shutdown
sw-edge2(config-if)# no shutdown
sw-edge2(config-if)# exit
```

Server Name	Source	NAS IP Address	NAS Port	Host MAC Address	Username	Service	Login Status	Request Timestam	Enforcement Profil
P58-T01-CPPM	RADIUS	10.1.3.5	4	C6-00-00-28-12-04	host/contractor	acap - wired - dot1x	ACCEPT	2022/11/25 05:56:34	aruba-role-contractor
P58-T01-CPPM	RADIUS	10.1.3.5	4	C6-00-00-28-12-04	c60000281204	acap - wired - macauth	REJECT	2022/11/25 05:56:32	[Deny Access Profile]
P58-T01-CPPM	RADIUS	10.1.3.5	4	EC-B1-D7-1B-07-00	ecb1d71b0700	acap - wired - macauth	REJECT	2022/11/25 05:56:31	[Deny Access Profile]

- **Question**: Do you see a MAC Authentication event?

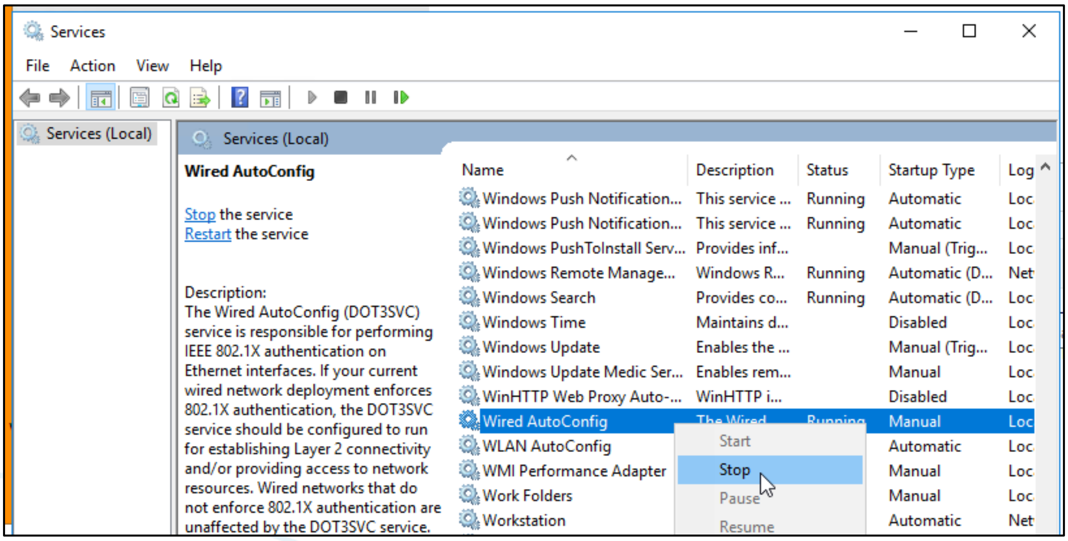
- **Answer**: Yes. MAC auth and 802.1X authentication are performed concurrent by the switch now. If 802.1X succeeds, it will have precedence over the success MAC-auth. In this example, the MAC Auth is rejected by ClearPass.

Attempt MAC Authenticaton with PC4

You will now change the MAC address on PC4 to make it appear with the MAC address of a phone in the lab.

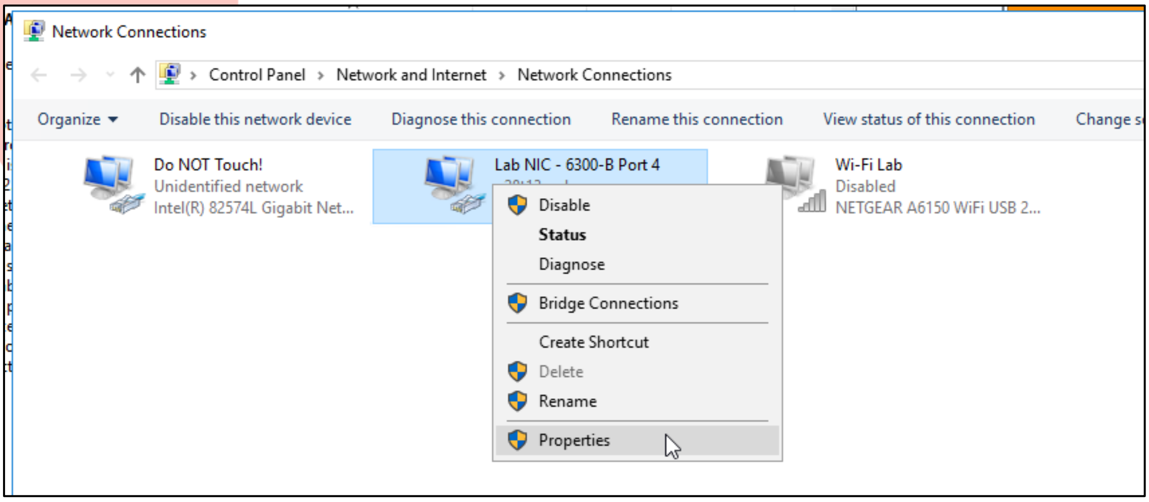
First you will disable the 802.1X supplicant on PC4.

8. On PC4, disable the 802.1X authentication.
9. Switch to the **Services** window.
10. Look for the **Wired AutoConfig** Service; right-click it and select **Stop**.

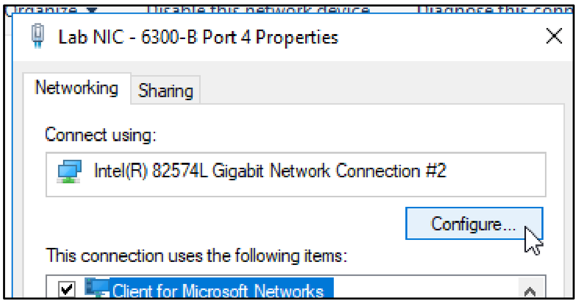


Now you can change the MAC Address of the PC4 Lab NIC.

11. Switch to the **Network Connections** window.
12. Right-click the LAB NIC and select **Properties**.



13. Click **Configure** for the Lab NIC.

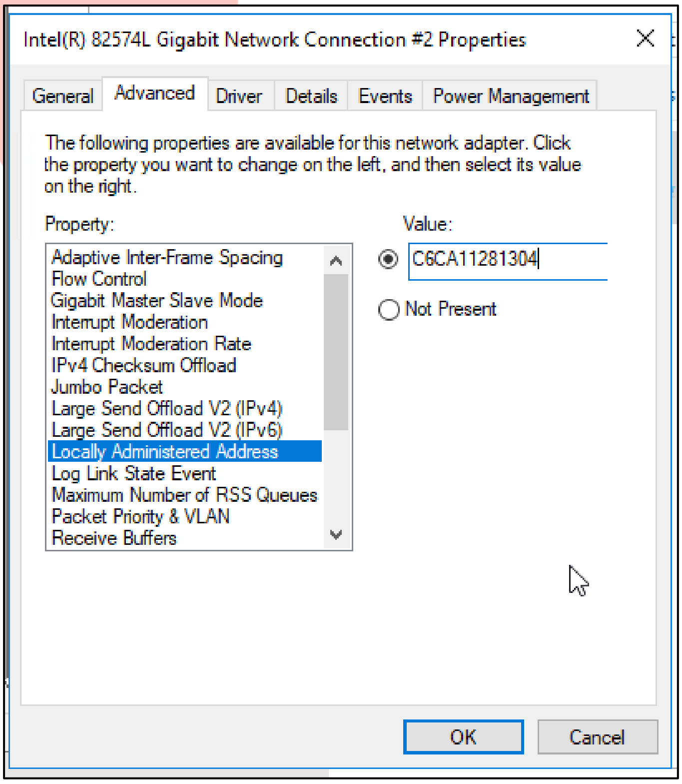


14. Click **Advanced**.
15. In the property list, look for the **Locally Administered Address**.
16. Click the radio button to enter a **Value**.
17. The MAC address for the lab phone will use the MAC range <u>**C6CA11**</u>xxyyzz. Replace the xx yy and zz in the address with:

- xx: Pod #
- yy: Table #
- zz: PC # > 04

IMPORTANT: The MAC address MUST start with **C6CA11.** ClearPass will return the phone role based on *this* MAC address.

For example if you are using Pod 28, Table 13, PC4: c6ca11<u>**281304**</u>



18. Click **OK**. The NIC in Windows will be disabled and enabled again.
19. On the sw-edge2, review the port access clients.

```
show port-access clients
```

```
sw-edge2(config)# show port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-------------------------------------------------------------------------------------
-------------------
  Port      MAC-Address        Onboarding     Status      Role
Device Type
                               Method
-------------------------------------------------------------------------------------
-------------------
c 1/1/4     00:50:56:b1:b9:0d dot1x           Success     contractor
c 1/1/4     c6:cAnswer:11:28:13:04 mac-auth        Success     phone
c 1/1/4     ec:b1:d7:1b:07:00                 Fail
```

- **Question**: Why did the MAC authentication occur?
- **Answer**: A new MAC address appeared on the port; this triggered the switch to initiate the authentication.

20. Review the active VLANs on port 1/1/4 with both contractor and phone connected.

```
show vlan port 1/1/4
```

```
sw-edge2(config-if)# show vlan port 1/1/4

-------------------------------------------------------------------------------
VLAN  Name                                Mode            Mapping
-------------------------------------------------------------------------------
22    VLAN22                              access          mbv
23    VLAN23                              access          mbv
```

21. In ClearPass Access tracker, review the success MAC-auth.

Server Name	Source	NAS IP Address	NAS Port	Host MAC Address	Username	Service	Login Status	Request Timestamp	Enforcement Profile
P58-T01-CPPM	RADIUS	10.1.3.5	4	C6-CA-11-28-13-04	c6ca11281304	acap - wired - macauth	ACCEPT	2022/12/23 15:42:06	aruba-role-phone

This concludes the MAC authentication and concurrent authentication task.

Cleanup

On PC4, remove the custom MAC address.

22. In the **Network Connections**, right-click on the **LAB Nic**, and click **Properties**.
23. Click **Configure**.
24. Click **Advanced**.
25. Select **Locally Administered Address**.
26. Click **Not Present**.
27. Click **OK**.

On PC4, start the Wired AutoConfig service again.

28. Switch to the **Services** window.
29. Right-click on the **Wired AutoConfig** service and click **Start**.

Task 3: User Roles with Device-Based Authentication

A deployment that requires bridged wireless functions will typically have the AP forward the wireless traffic with a VLAN tag. This requires the switch port to be configured as a VLAN trunk.

Bridged forwarding results in another challenge: The switch will see all the wireless client MAC addresses as new MAC clients and it will attempt to perform authentication for these MAC addresses.

This would result in double-authentication (Wireless client could be 802.1X authenticated by the AP and then MAC authenticated by the switch) and this could lead to a lot of confusion.

When the authentication is performed by the downstream device (in this example the AP), there is no more need for the switch to perform its own authentication.

This can be configured on a port using the device-based authentication feature.

When the switch authenticates an AP on a switch port, the user role for the AP can be set as device-based. The switch port will then become open for all MAC addresses, therefore eliminating the double-authentication problem.

Objectives

- Understand the difference between client-mode and device-mode port access.
- Configure a user role for device based port access.
- Verify device-mode access.

Steps

Configure a User Role for the AP

1. Configure a user role named *dev-ap* (the name must match exactly since this is the role name that ClearPass sends to the switch).

```
port-access role dev-ap
 vlan trunk native 4
 vlan trunk allowed 4,11-15
 exit
```

```
sw-edge2(config)# port-access role dev-ap
sw-edge2(config-pa-role)# vlan trunk native 4
sw-edge2(config-pa-role)# vlan trunk allowed 4,11-15
sw-edge2(config-pa-role)# exit
```

2. On port 1/1/2 (that connects to the AP) review the current, static VLAN configuration.

```
show running-config interface 1/1/2
```

```
sw-edge2(config)# show running-config interface 1/1/2
interface 1/1/2
```

```
    no shutdown
    description ap2
    no routing
    vlan trunk native 4
    vlan trunk allowed 4,11-15
    exit
```

3. Configure port 1/1/2 as access port in VLAN 21. This VLAN 21 acts as the default port VLAN.

```
interface 1/1/2
 vlan access 21
 exit
```

```
sw-edge2(config)# interface 1/1/2
sw-edge2(config-if)# vlan access 21
sw-edge2(config-if)# exit
```

4. Review the current interface configuration.

```
show running-config interface 1/1/2
```

```
sw-edge2(config)# show running-config interface 1/1/2
interface 1/1/2
    no shutdown
    description ap2
    no routing
    vlan access 21
    exit
```

5. Check the operational VLAN status.

```
show vlan port 1/1/2
```

```
sw-edge2(config)# show vlan port 1/1/2

-------------------------------------------------------------------------------
VLAN  Name                                Mode             Mapping
-------------------------------------------------------------------------------
21    VLAN21                              access           port
```

Enable MAC Authentication

6. Enable MAC authentication on the port.

```
interface 1/1/2
 aaa authentication port-access mac-auth
  enable
  exit
 exit
```

```
sw-edge2(config)# interface 1/1/2
sw-edge2(config-if)# aaa authentication port-access mac-auth
sw-edge2(config-if-macauth)# enable
```

```
sw-edge2(config-if-macauth)# exit
sw-edge2(config-if)# exit
```

Verify the MAC Authentication Results

7. Review the port-access clients on interface 1/1/2.

```
show port-access clients interface 1/1/2
```

```
sw-edge2(config)# show port-access clients interface 1/1/2

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-------------------------------------------------------------------------------------
-------------------
  Port     MAC-Address       Onboarding     Status      Role
Device Type
                             Method
-------------------------------------------------------------------------------------
-------------------
c 1/1/2    20:4c:03:5b:27:e2 mac-auth       Success     dev-ap
```

- **Question**: What is the status code for the connected AP client?
- **Answer**: *c*. This shows client-mode is used, therefor **only** the AP MAC address will be allowed access to the network.

8. Review the VLAN port status for the port 1/1/2. This will now include the VLAN trunk configuration based on the dev-ap user role.

```
show vlan port 1/1/2
```

```
sw-edge2(config)# show vlan port 1/1/2

-------------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
-------------------------------------------------------------------------------
4     v4-ap-mgmt                      native-untagged port-access
11    VLAN11                          trunk           port-access
12    VLAN12                          trunk           port-access
13    VLAN13                          trunk           port-access
14    VLAN14                          trunk           port-access
15    VLAN15                          trunk           port-access

Overridden VLAN list: 21
```

9. Update the port access role dev-ap to device mode.

```
port-access role dev-ap
 auth-mode device-mode
 exit
```

```
sw-edge2(config)# port-access role dev-ap
sw-edge2(config-pa-role)# auth-mode device-mode
sw-edge2(config-pa-role)# exit
```

10. Review the updated port access clients on interface 1/1/2.

```
show port-access clients interface 1/1/2
```

```
sw-edge2(config)# show port-access clients interface 1/1/2

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-----------------------------------------------------------------------------------
-------------------
  Port      MAC-Address       Onboarding     Status      Role
Device Type
                              Method
-----------------------------------------------------------------------------------
-------------------
d 1/1/2     20:4c:03:5b:27:e2 mac-auth       Success     dev-ap
```

- **Question**: What is the Status code for the client?
- **Answer**: The status code has now changed from **c (client mode) to d (device-mode).** Any clients that would be bridged by the AP will now be allowed access on the network without additional authentication by the switch.

You have completed this Lab!

Lab 10.02 Wired Access with Aruba Gateways

Overview

In this lab you will integrate the wired switches with the Aruba gateway. The gateway can provide firewall functions for the wired clients.

In the first task you will prepare the gateway by creating a user role that will be used to control the wired client network access.

In the second task you will configure the switch with a User Based Tunneling (UBT) zone that points to the gateway cluster. You will then connect to the network with PC4 and verify that the contractor user wired traffic is now tunneled to and firewalled by the gateway.

In the last task you will perform some troubleshooting for UBT and review the gateway default tunneled user AAA profile.

Objectives

After completing this lab, you will be able to:

- Configure the gateway with a user role for the wired clients.
- Configure a VLAN assignment in a gateway user role.
- Configure the switch with a UBT zone.
- Configure a switch user role for UBT forwarding.
- Understand the default role in the gateway default tunneled user AAA profile.

Task 1: Prepare the Gateway

In this task you will first review the gateway status and cluster.

Next you will prepare the gateways with a user role to apply firewall control to the wired network.

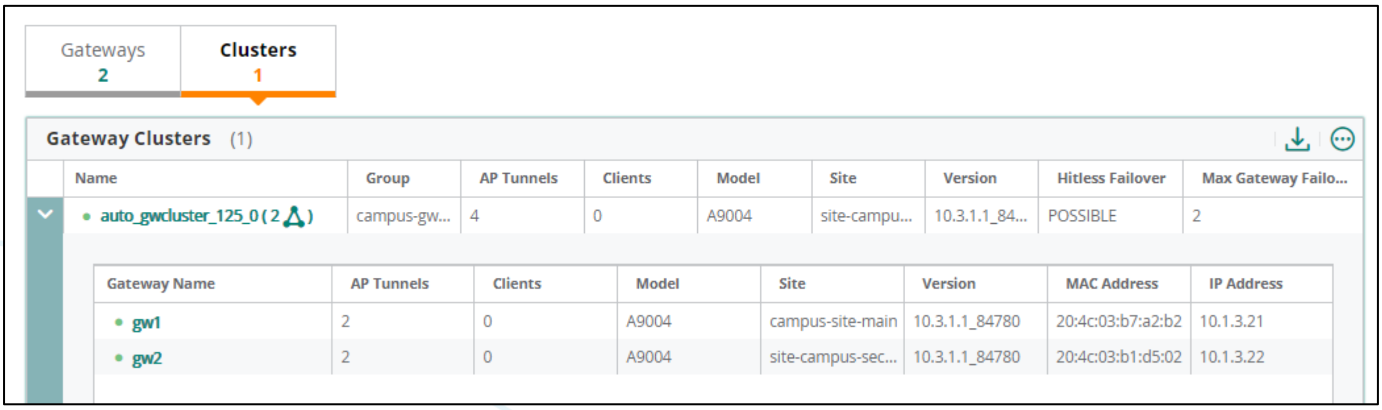
Objectives

- Configure a gateway user role with VLAN assignment.
- Verify the policies of a gateway user role.

Steps

Verify Gateway and Cluster Setup

1. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **List**.
2. Click **Clusters**.



3. Verify that both gw1 and gw2 are *active* in the auto group cluster.

NOTE: If the gateways are not part of this cluster, check these items:
- Are both gateways moved to the group campus-gw-main?
- Is auto group cluster enabled In the High Availability configuration of the group campus-gw-main?
- Is the manual cluster configuration disabled for the group cluster?

Prepare the Contractor VLAN on the Gateways

In this section, you will prepare the VLAN that will be used by the tunneled contractor users.

4. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).

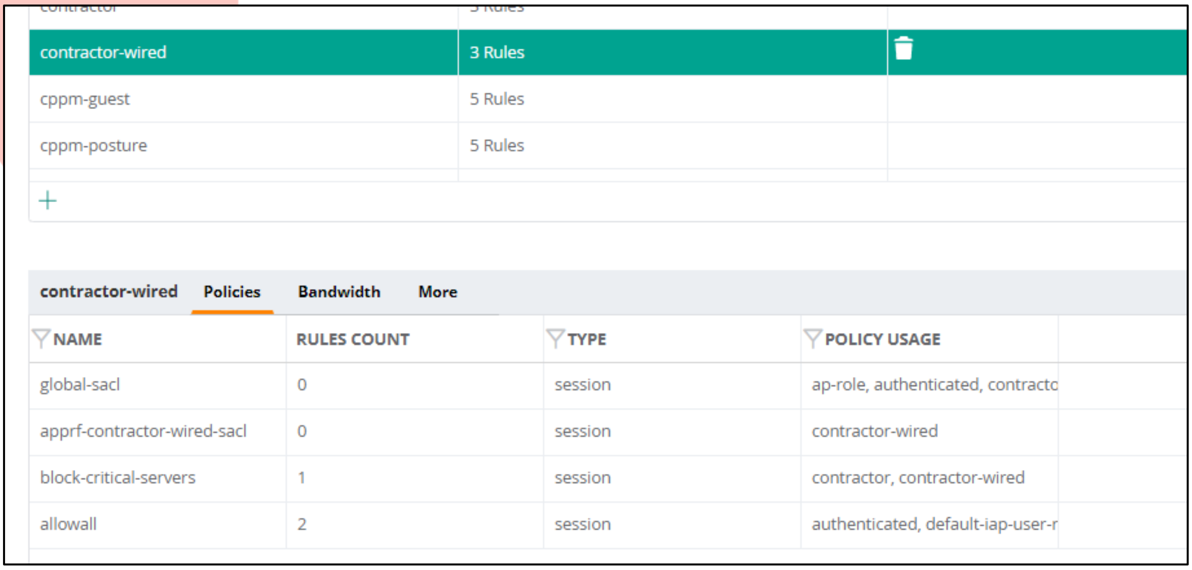
5. Navigate to **Interface > VLANs**.
6. Add a new named VLAN with these settings:
   - VLAN Name: **contractor-wired**
   - VLAN ID/Range: **42**
7. Click **Save Settings**.

Create a User Role for contractor-wired

Contractors' access to the network will be controlled by the gateway firewall:

- Block access to critical servers (this policy was previously created on the gateway for the wireless clients)
- Allow all other access
- Assign VLAN contractor-wired VLAN (42)

8. Navigate to **Security > Roles**.
9. Add a new role with name **contractor-wired**.
10. Click **Save Settings**.
11. Select the user role **contractor-wired**. The bottom of the page will show Policies, Bandwidth and More options.
12. Click **Policies**. The two default user role policies will be displayed (global-sacl and the apprf role based sacl).
13. In the policy list of the role, click the **+** button to add a new policy.
14. Click **Add an existing policy** and leave the Policy Type as **Session**.
15. In the policy name list, select the policy **block-critical-servers**.
16. Click **Save Settings**.
17. Click the **+** button to add another session policy.
18. Click **Add an existing policy** and leave the Policy Type as **Session**.
19. In the policy name list, select the policy **allow-all**.
20. Click **Save Settings**.
21. Verify the order of the policies:
    - First, the 2 default policies will be listed.
    - Next, the policy to block critical servers is listed.
    - The last policy will allow all traffic.



The last step for the role configuration is to assign the role to VLAN 42.

22. Click **More**.
23. For **VLAN**, assign the name VLAN **contractor-wired**.

24. Click **Save Settings**.

Task 2: Configure the Switch-to-Gateway Cluster Connection

In this task you will configure the switch to establish a connection to the gateway cluster.

The UBT client on the switch **must** be configured with a source IP address.

This source IP can be configured specifically for the UBT feature or for all the switch features.

In the lab template, the source IP has been set for all the management features.

On the sw-edge2, you will now verify that SVI 3 is used as source interface for UBT.

Objectives

- Review the switch UBT source IP address.
- Configure a UBT zone on the switch.
- Verify the UBT state on the switch.
- Configure a switch user role for UBT forwarding.
- Verify the tunneled user state and firewall sessions.

Steps

Verify the IP Source IP for the UBT Connection

1. Verify if a UBT specific source IP was configured.

```
show ip source-interface ubt
```

```
sw-edge2(config)# show ip source-interface ubt
Source-interface Configuration Information

Protocol        Src-Interface       Src-IP
VRF
ubt
```

2. Review the source interface default settings.

```
show ip source-interface all
```

```
sw-edge2(config)# show ip source-interface all
Source-interface Configuration Information

Protocol        Src-Interface       Src-IP
VRF

all             vlan3               10.1.3.5 default
```

3. Review the running config for the **source** command.

```
show running-config | include source
```

```
sw-edge2(config)# show running-config | include source
ip source-interface all interface vlan3
```

Configure the UBT Client VLAN

When the wired client traffic is sent over the GRE tunnel to the gateway, the inner traffic in the tunnel is marked with a VLAN tag. This is the UBT Client VLAN.

When the traffic arrives at the gateway, the gateway can override the VLAN ID or leave the UBT VLAN intact. In this lab environment, you have configured the contractor-wired user role on the gateway with VLAN 42. This means that the UBT client VLAN will be overridden by the gateway with the role based VLAN ID.

The UBT client VLAN is configured on the switch side.

4. Create VLAN 4001 and set VLAN 4001 as the UBT client VLAN.

```
vlan 4001
exit
ubt-client-vlan 4001
```

```
sw-edge2(config)# vlan 4001
sw-edge2(config-vlan-4001)# exit
sw-edge2(config)# ubt-client-vlan 4001
```

NOTE: Any VLAN can be used, VLAN ID 4001 is just an example in the lab.

Configure the UBT Zone

In the next steps, you will configure a UBT zone. The zone on the switch points to a gateway cluster.

5. Configure a UBT zone, use GW1 as the primary IP.

```
ubt zone campus-main vrf default
primary-controller ip 10.1.3.21
enable
exit
```

```
sw-edge2(config)# ubt zone campus-main vrf default
sw-edge2(config-ubt-campus-main)# primary-controller ip 10.1.3.21
sw-edge2(config-ubt-campus-main)# enable
sw-edge2(config-ubt-campus-main)# exit
```

The switch will now attempt to establish a control plane connection to the gateway.

6. Verify the connection state with the gateway.

```
show ubt state
```

```
sw-edge2(config)# show ubt state

Zone campus-main:

Local Conductor Server (LCS) State:
LCS Type      IP Address    State               Role

Primary     : 10.1.3.21  ready_for_bootstrap operational_primary
Switch Anchor Controller (SAC) State:
IP Address      MAC Address          State

Active      : 10.1.3.21       20:4c:03:b7:a2:b2    registered
Standby     : 10.1.3.22       20:4c:03:b1:d5:02    registered
```

NOTE: If you don't see the two gateways in the list yet, repeat the command after a few moments.

Update the Switch Contractor User Role

To tunnel traffic for a wired client to the gateway, the user role configuration must be updated with the gateway zone that should be used to handle the client traffic.

Since the gateway firewall policy will be used to control the user traffic, there is typically no need to apply a port access policy at the switch level anymore.

In the next steps, you will remove the existing switch port access policy from the contractor role and assign the gateway zone to the role.

7. On the sw-edge2, enter the port access role contractor and remove the existing policy.

```
port-access role contractor
no associate policy
exit
```

```
sw-edge2(config)# port-access role contractor
sw-edge2(config-pa-role)# no associate policy
sw-edge2(config-pa-role)# exit
```

8. Configure the contractor user role with the UBT gateway zone and the contractor-wired gateway role.

```
port-access role contractor
gateway-zone zone campus-main gateway-role contractor-wired
```

```
exit
```

```
sw-edge2(config)# port-access role contractor
sw-edge2(config-pa-role)# gateway-zone zone campus-main gateway-role contractor-wired
sw-edge2(config-pa-role)# exit
```

IMPORTANT: Pay attention that you don't make any spelling mistakes for the gateway-role **contractor-wired**, since this is the name ClearPass uses!

9. Review the port access contractor user role configuration.

```
show port-access role name contractor
```

```
sw-edge2(config)# show port-access role name contractor Role Information:
Name  : contractor
Type  : local

    Reauthentication Period              :
    Cached Reauthentication Period       :
    Authentication Mode                  :
    Session Timeout                      :
    Client Inactivity Timeout            :
    Description                          :
    Gateway Zone                         : campus-main
    UBT Gateway Role                     : contractor-wired
    UBT Gateway Clearpass Role           :
    Access VLAN                          : 22
    Native VLAN                          :
    Allowed Trunk VLANs                  :
    Access VLAN Name                     :
    Native VLAN Name                     :
    Allowed Trunk VLAN Names             :
    VLAN Group Name                      :
    MTU                                  :
    QOS Trust Mode                       :
    STP Administrative Edge Port         :
    PoE Priority                         :
    PVLAN Port Type                      :
    Captive Portal Profile               :
    Policy                               :
    GBP                                  :
    Device Type                          :
```

Verify the PC4 Contractor Access

In the next steps you will connect with PC4 using 802.1X wired authentication to sw-edge2. The PC4 can use the contractor certificate to authenticate using EAP-TLS.

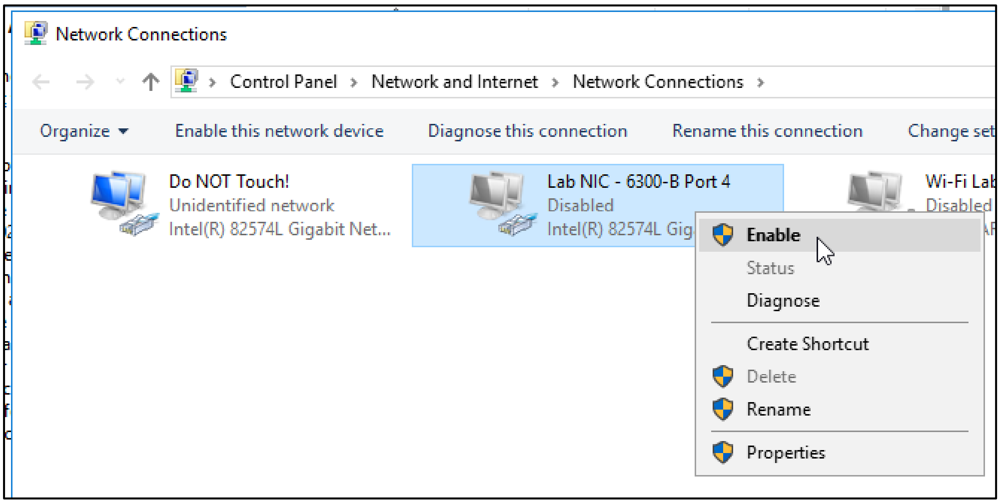
10. On sw-edge2, bounce the port 1/1/4 (connected to PC4 / contractor).

```
interface 1/1/4
```

```
shutdown
no shutdown
exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# shutdown
sw-edge2(config-if)# no shutdown
sw-edge2(config-if)# exit
```

11. On PC4, bounce the wired LAB NIC (*Disable* / *Enable*).



NOTE: The Wired AutoConfig service was enabled again at the end of Lab 10.01. Make sure you have the service enabled for the wired 802.1X authentication.

12. On PC4, open a command prompt (cmd.exe) and check the IP Address with ipconfig.

```
ipconfig
```

```
C:\Users\student> ipconfig
Windows IP Configuration

Ethernet adapter Do NOT Touch!:
Connection-specific DNS Suffix  . :
IPv4 Address. . . . . . . . . . . : 172.16.28.83
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . :
Ethernet adapter Lab NIC - 6300-B Port 4:
Connection-specific DNS Suffix  . : aruba-training.com
IPv4 Address. . . . . . . . . . . : 10.1.42.50
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.1.42.1
```

13. Verify that you can successfully access 10.254.1.21.

```
ping 10.254.1.21
```

```
C:\Users\student>ping 10.254.1.21
Pinging 10.254.1.21 with 32 bytes of data:
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
...
```

14. Verify access to 10.1.0.2 is blocked using a continuous ping.

```
ping 10.1.0.2 -t
```

```
C:\Users\student>ping 10.1.0.2 -t
Pinging 10.1.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
...
```

15. On sw-edge2, review the details for active port access clients on port 1/1/4.

```
show port-access clients interface 1/1/4 detail
```

```
sw-edge2(config)# show port-access clients interface 1/1/4 detail

...

Port Access Client Status Details:
Client 00:50:56:b1:b9:0d, host/contractor
Session Details
Port         : 1/1/4
Session Time : 454s
IPv4 Address :
IPv6 Address :
Device Type  :
VLAN Details
VLAN Group Name :
VLANs Assigned  : 4001
Access          : 4001
Native Untagged :
Allowed Trunk   :
Authentication Details
Status          : dot1x Authenticated
Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
    Auth History    : dot1x - Authenticated, 324s ago
                      mac-auth - Attempted, 324s ago
                      dot1x - Authenticated, 379s ago
                      mac-auth - Attempted, 379s ago
                      dot1x - Authenticated, 386s ago

Authorization Details
Role   : contractor
Status : Applied
```

```
Role Information:
Name  : contractor
Type  : local

    Reauthentication Period            :
    Cached Reauthentication Period     :
    Authentication Mode                :
    Session Timeout                    :
    Client Inactivity Timeout          :
    Description                        :
    Gateway Zone                       : campus-main
    UBT Gateway Role                   : contractor-wired
    UBT Gateway Clearpass Role         :
    Access VLAN                        : 22
    Native VLAN                        :
    Allowed Trunk VLANs                :
    Access VLAN Name                   :
    Native VLAN Name                   :
    Allowed Trunk VLAN Names           :
    VLAN Group Name                    :
    MTU                                :
    QOS Trust Mode                     :
    STP Administrative Edge Port       :
    PoE Priority                       :
    PVLAN Port Type                    :
    Captive Portal Profile             :
    Policy                             :
    GBP                                :
    Device Type                        :


UBT Zone Details:
Zone Name                : campus-main
UBT Mode                 : local-vlan
Primary Controller       : 10.1.3.21
Backup Controller        : ---/---
SAC HeartBeat Interval : 1
UAC KeepAlive Interval : 60
VLAN Identifier          : 4001
VRF Name                 : default
Admin State              : Enabled
PAPI Security Key        : Disabled
Operational State        : up
```

Review the Client to Gateway Bucket Index Mapping

When the switch establishes the PAPI control plane connection with the gateway, the gateway will update the switch with the active bucket map.

The switch will use this bucket map to assign clients to the gateway cluster members.

In the next steps you will review the bucket map and the client assignment.

16. On sw-edge2, review the client to bucket id mapping, the active client MAC addresses are listed at the bottom of the command output.

```
show ubt state
```

Example output:

```
sw-edge2(config)# show ubt state

Zone campus-main:

Local Conductor Server (LCS) State:
LCS Type      IP Address    State              Role

Primary     : 10.1.3.21   ready_for_bootstrap operational_primary
Switch Anchor Controller (SAC) State:
IP Address      MAC Address         State

Active      : 10.1.3.21      20:4c:03:b7:a2:b2    registered
Standby     : 10.1.3.22      20:4c:03:b1:d5:02    registered

User Anchor Controller(UAC): 10.1.3.21
User                Port   State                          Bucket ID  Gre Key  VLAN

00:50:56:b1:b9:0d   1/1/4  registered                     5          4        4001
```

- **Question:** What is the bucket ID for your client MAC address?
- **Answer:** This depends on your client MAC address. In the example output, the assigned bucket ID is 5, but this will likely be different in your lab setup.

Take note of your client bucket ID: ____________________

17. On the sw-edge2, review the bucket map index to gateway mapping. For each bucket ID you will see the A-UAC (Active User Anchor Controller) and the S-UAC (Standby User Anchor Controller).

```
show ubt information
```

```
sw-edge2(config)# show ubt information

Zone campus-main:
SAC Information :
  Active         : 10.1.3.21
  Standby        : 10.1.3.22

Node List Information :
Cluster Name        : auto_gwcluster_125_0
Cluster Alias Name  :
Node List      :
10.1.3.21
10.1.3.22

Bucket Map Information :
```

```
Bucket Map Active   : [0...255]

Bucket ID  A-UAC           S-UAC                Connectivity

0          10.1.3.21       10.1.3.22            L2
1          10.1.3.21       10.1.3.22            L2
2          10.1.3.21       10.1.3.22            L2
3          10.1.3.21       10.1.3.22            L2
4          10.1.3.21       10.1.3.22            L2
5          10.1.3.21       10.1.3.22            L2
6          10.1.3.21       10.1.3.22            L2
7          10.1.3.21       10.1.3.22            L2
8          10.1.3.21       10.1.3.22            L2
...
```

NOTE: You can filter the output based with your bucket ID.

```
show ubt information | include “5 “
```

```
sw-edge2(config)# show ubt information | include “5 “
5          10.1.3.21       10.1.3.22            L2
15         10.1.3.21       10.1.3.22            L2
25         10.1.3.21       10.1.3.22            L2
...
```

For the bucket ID of your client, take note of the active controller IP.

- Active UAC: ________________

18. Use the MGMT PC to open an SSH connection to this A-UAC.
19. Review the active firewall user table.

```
show user-table
```

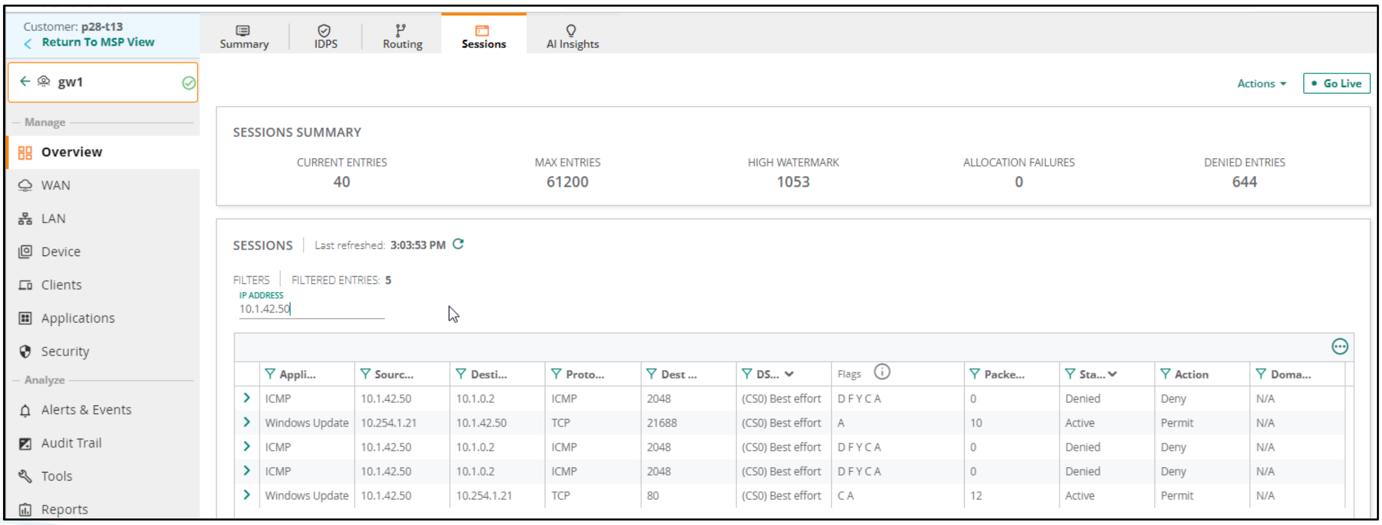
```
(gw1) *# show user-table
Users

    IP            MAC            Name              Role              Age(d:h:m)  Auth
VPN link      Connected To     Roaming   Essid/Bssid/Phy                      Profile
Forward mode   Type   Host Name  User Type
----------  ------------      ------            ----              ----------  ----
10.1.42.50  00:50:56:b1:b9:0d  host/contractor  contractor-wired  00:00:22
Tunneled-User-802.1X           10.1.3.5             Tunneled  tunnel
16/64:e8:81:3f:b5:00/1/1/4  default-tunneled-user  tunnel
TUNNELED USER

User Entries: 1/1
Curr/Cum Alloc:1/2 Free:0/1 Dyn:1 AllocErr:0 FreeErr:0
```

- Take note of the client IP address: ________________

Review the Client Firewall Sessions in Aruba Central

Under the device level of the gateway, the firewall sessions can be reviewed.

20. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **List**.
21. Click the gateway name used by your client to switch to the device level view.
22. Navigate to **Overview > Sessions**. This shows the full firewall session table of the gateway.
23. Enter the IP address of the client in the filter field and press <**Enter**>.



- **Question**: Do you see a denied ICMP session with a destination IP of 10.1.0.2?
- **Answer**: Yes, all the wired client sessions can now be seen in the gateway firewall list.

24. On PC4, stop the continuous ping to 10.1.0.2.

Optional Task 3: Troubleshooting and Failover for UBT

In this task you can explore some issues in the configuration of UBT.

In the first section you will explore what happens when the switch user role does not include the gateway role configuration.

The next section will show an example of an invalid gateway role configuration.

Objectives

- Understand the default tunneled user AAA profile on the gateway.
- Troubleshoot an invalid user role reference.
- Verify the impact of a gateway failure in a cluster for the UBT clients.

Steps

Switch the User Role without Gateway User Role

When a switch role has a UBT zone configured, but there is no gateway role specified, the gateway will assign a default role to the client.

In the next steps you will explore this process and the assigned default role.

1. On sw-edge2, update the contractor role. Only specify the zone, but do not configure a gateway role.

```
port-access role contractor
gateway-zone zone campus-main
exit
```

```
sw-edge2(config)# port-access role contractor
sw-edge2(config-pa-role)# gateway-zone zone campus-main
sw-edge2(config-pa-role)# exit
```

2. Bounce port 1/1/4.

```
interface 1/1/4
shutdown
no shutdown
exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# shutdown
sw-edge2(config-if)# no shutdown
sw-edge2(config-if)# exit
```

NOTE: You can also bounce the Lab NIC on PC4 to trigger a new authentication.

3. Review the port access clients.

```
show port-access clients interface 1/1/4
```

```
sw-edge2(config)# show port-access clients interface 1/1/4
Port Access Clients
Status Codes: d device-mode, c client-mode, m multi-domain

  Port      MAC-Address       Onboarding     Status      Role
Device Type
                             Method
-----------------------------------------------------------------------------------
------------------
c 1/1/4    ec:b1:d7:1b:07:00                Fail
c 1/1/4    00:50:56:b1:b9:0d dot1x          Success     contractor
```

4. On the gateway used by the client, review the user-table.

```
show user-table
```

```
(gw1) *#show user-table
Users

    IP           MAC       Name    Role   Age(d:h:m)  Auth  VPN link      Connected To
Roaming  Essid/Bssid/Phy  Profile  Forward mode  Type  Host Name  User Type
----------  ------------  ------  ----  ----------  ----  --------  -----------------
-  -------  ---------------  -------  ------------  ----  ---------  ---------

User Entries: 0/0
 Curr/Cum Alloc:1/5 Free:0/4 Dyn:1 AllocErr:0 FreeErr:0
```

- **Question**: Do you see any clients?
- **Answer**: No.
- **Question**: Does this mean there is no client active?
- **Answer**: No. It only means that the firewall has not learned an IP address for the client. This could happen for example when the client would be assigned to a VLAN without DHCP access.

5. Review the L2 station table on the gateway.

```
show station-table
```

```
(gw1) *#show station-table
```

```
Station Entry

     MAC            Name             Role       Age(d:h:m)  Auth      Connected To
Essid  Phy    Remote  Profile                 User Type
------------        ------           ----      ----------  ----  ------------------  -
----  ---    ------  -------                 ---------
00:50:56:b1:b9:0d  host/contractor  guest     00:00:02    Yes   10.1.3.5            -
1/1/4  No      default-tunneled-user  TUNNELED USER

Station Entries: 1
```

- **Question**: What is the user role that was assigned to the client?
- **Answer**: guest.
- **Question**: What is the profile (AAA Authentication profile) that was used for this client?
- **Answer**: The name of the AAA profile is default-tunneled-user.

6. Check the last entries of the authentication trace buffer to see the VLAN assignment. The last 3 columns show the assigned VLAN id and the assigned role name.

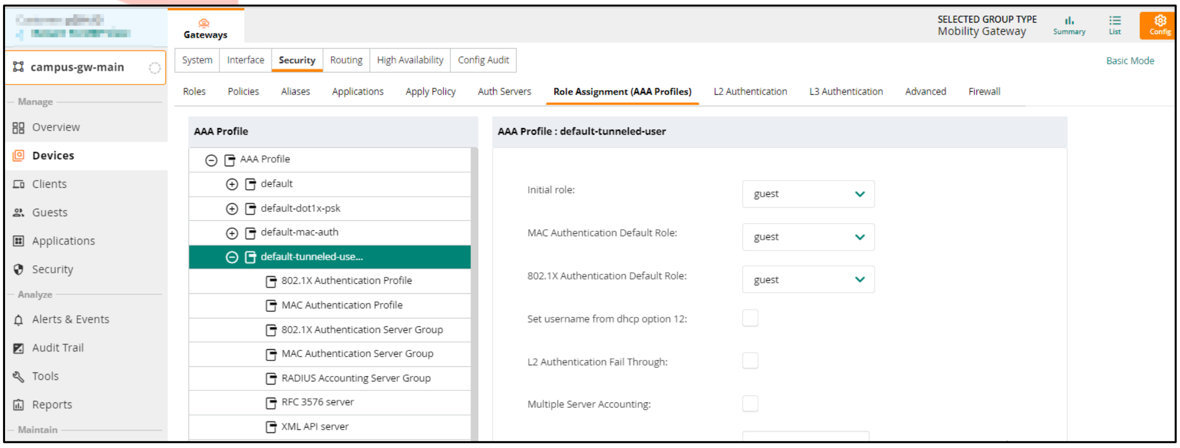
```
show auth-tracebuf count 4
```

```
(gw1) *#show auth-tracebuf count 4
Auth Trace Buffer



Dec 26 09:18:07 Role, Vlan assigned * 00:50:56:b1:b9:0d  64:e8:81:3f:b5:00  3  4001
guest
Dec 26 09:18:07 Role, Vlan assigned * 00:50:56:b1:b9:0d  64:e8:81:3f:b5:00  3  4001
guest
Dec 26 09:18:07 Role, Vlan assigned * 00:50:56:b1:b9:0d  64:e8:81:3f:b5:00  3  4001
guest
```

- **Question**: What is the assigned user role?
- **Answer**: The assigned user role is guest. This is based on the initial role of the default-tunneled-user AAA profile on the gateway.
- **Question**: What is the assigned VLAN ID?
- **Answer**: 4001. This is the UBT client VLAN you have configured on the switch. Since the guest user role on the gateway does not include a VLAN override, the UBT client VLAN is *unchanged*. However, since VLAN 4001 does not exist on the gateway or the uplink VLAN trunk, the client does not get a IP addressing information via DHCP.

Review the Default Tunneled User AAA Profile on the Gateway

7. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
8. Navigate to **Security** > **Role Assignment (AAA Profiles).**
9. Expand the list of profiles and select the **default-tunneled-user** AAA Profile.



- **Question**: What is the initial role in this AAA profile?
- **Answer**: The initial role is **guest** by default. If you want to create a default limited or no-access role, it can be assigned here as the initial role.

Switch User Role Refers to an Invalid Gateway Role

A network admin could make a mistake in the switch user role configuration and assign a gateway role that does not exist on the gateway.

In this section you will explore what happens when an invalid role is configured.

10. On sw-edge2, configure the gateway role with name test. This role does not exist on the gateway.

```
port-access role contractor
gateway-zone zone campus-main gateway-role test
exit
```

```
sw-edge2(config)# port-access role contractor
sw-edge2(config-pa-role)# gateway-zone zone campus-main gateway-role test
sw-edge2(config-pa-role)# exit
```

11. Bounce the port 1/1/4.

```
interface 1/1/4
shutdown
no shutdown
exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# shutdown
sw-edge2(config-if)# no shutdown
sw-edge2(config-if)# exit
```

NOTE: You can also bounce the Lab NIC on PC4 to trigger a new authentication.

12. Review the port access client list on port 1/1/4.

```
show port-access clients interface 1/1/4
```

```
sw-edge2(config)# show port-access clients interface 1/1/4
Port Access Clients
Status Codes: d device-mode, c client-mode, m multi-domain

  Port      MAC-Address       Onboarding     Status      Role
Device Type
                              Method
-------------------------------------------------------------------------------------
-------------------
c 1/1/4     ec:b1:d7:1b:07:00                In-Progress
c 1/1/4     00:50:56:b1:b9:0d                Fail        contractor
```

13. Review the port access client details of port 1/1/4.

```
show port-access clients interface 1/1/4 detail
```

For the contractor user, you should check the authorization details in the output:

```
...
Authorization Details
Role   : contractor
Status : Failed, Failed to setup User Based Tunnel
...
```

14. On the gateway, review the user and station table.

```
show user-table
```

```
(gw1) #show user-table
Users

    IP            MAC        Name    Role   Age(d:h:m)  Auth  VPN link     Connected To
Roaming  Essid/Bssid/Phy  Profile  Forward mode  Type  Host Name  User Type
----------  ------------  ------  ----  ----------  ----  --------  -----------------
-  -------  ---------------  -------  ------------  ----  ---------  ---------

User Entries: 0/0
 Curr/Cum Alloc:0/2 Free:2/2 Dyn:2 AllocErr:0 FreeErr:0
```

```
show station-table
```

```
(gw1) #show station-table

Station Entry
-------------
     MAC        Name   Role  Age(d:h:m)  Auth    Connected To     Essid  Phy  Remote
Profile  User Type
------------  ------  ----  ----------  ----  -----------------  -----  ---  ------
-------  ---------

Station Entries: 0
```

15. Review tunneled-node-mgr authentication trace buffer.

```
show tunneled-node-mgr trace-buf count 20
```

```
(gw1) *#show tunneled-node-mgr trace-buf count 10
TNM Trace Buffer



Dec 26 09:33:10  gsm  Publish tun user     10.1.3.5  00:50:56:b1:b9:0d.
Dec 26 09:33:10  <--  User bootstrap ack   10.1.3.5  00:50:56:b1:b9:0d status=18:User
Bootstrap Failed, Auth Module Could Not Create Entry.
Dec 26 09:33:10  sos  User tunnel removed  10.1.3.5  00:50:56:b1:b9:0d tunnel 16.
Dec 26 09:33:10  gsm  Delete tun user      10.1.3.5  00:50:56:b1:b9:0d.
Dec 26 09:36:09  -->  User bootstrap req   10.1.3.5  00:50:56:b1:b9:0d rsvd-vid=1
vlan=4001 key=4 role=test flags=6 mtu=1500 server=0.0.0.0.
Dec 26 09:36:09  sos  User tunnel created  10.1.3.5  00:50:56:b1:b9:0d dormant=0
tunnel 16.
Dec 26 09:36:09  gsm  Publish tun user     10.1.3.5  00:50:56:b1:b9:0d.
Dec 26 09:36:09  <--  User bootstrap ack   10.1.3.5  00:50:56:b1:b9:0d status=18:User
Bootstrap Failed, Auth Module Could Not Create Entry.
Dec 26 09:36:09  sos  User tunnel removed  10.1.3.5  00:50:56:b1:b9:0d tunnel 16.
Dec 26 09:36:09  gsm  Delete tun user      10.1.3.5  00:50:56:b1:b9:0d.
```

- **Question**: What is the name of the role in the user bootstrap request?
- **Answer**: The switch requests the gateway with a user bootstrap request to create an entry with role name **test**.

Restore the Contractor User Role

16. On sw-edge2, restore the contractor user role with the correct contractor-wired role.

```
port-access role contractor
gateway-zone zone campus-main gateway-role contractor-wired
exit
```

```
sw-edge2(config)# port-access role contractor
sw-edge2(config-pa-role)# gateway-zone zone campus-main gateway-role contractor-wired
sw-edge2(config-pa-role)# exit
```

17. Bounce the port 1/1/4.

```
interface 1/1/4
shutdown
no shutdown
exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# shutdown
sw-edge2(config-if)# no shutdown
sw-edge2(config-if)# exit
```

NOTE: You can also bounce the Lab NIC on PC4 to trigger a new authentication.

18. Verify that PC4 has connected successfully to the network again as *contractor*.

```
show port-access clients interface 1/1/4
```

```
sw-edge2(config)# show port-access clients interface 1/1/4
Port Access Clients
Status Codes: d device-mode, c client-mode, m multi-domain

  Port      MAC-Address        Onboarding     Status      Role            Device Type
                               Method
-----------------------------------------------------------------------------------
-----
c 1/1/4     00:50:56:b1:b9:0d  dot1x          Success     contractor
c 1/1/4     ec:b1:d7:1b:07:00                 In-Progress
```

Cluster Gateway Failover

The gateway clustering also provides redundancy for the wired clients that are tunneled via the cluster.

In these steps you can verify the operation by rebooting the active gateway for the client.

19. On the PC4, start a continuous ping to 10.1.1.2

```
ping 10.1.1.2 -t
```

20. Reboot the gateway that is currently used by PC4 and confirm the system restart message.

```
reload
y
```

21. On the PC4, verify that the ping continues.

```
Reply from 10.1.1.2: bytes=32 time<1ms TTL=64
Reply from 10.1.1.2: bytes=32 time<1ms TTL=64
```

```
Request timed out.
Reply from 10.1.1.2: bytes=32 time<1ms TTL=64
Reply from 10.1.1.2: bytes=32 time<1ms TTL=64
```

22. Use the MGMT PC to open a console/SSH connection to the other gateway.
23. Verify that PC4 is listed in the user table

```
show user-table
```

Example output, in the example GW2 is now used for the client.

```
(gw2) #show user-table
Users

    IP            MAC             Name             Role                 Age(d:h:m)  Auth
VPN link     Connected To     Roaming   Essid/Bssid/Phy                          Profile
Forward mode  Type  Host Name  User Type
----------  ------------       ------           ----                 ----------  ----
10.1.42.50  00:50:56:b1:b9:0d  host/contractor  contractor-wired  00:00:06
Tunneled-User-802.1X            10.1.3.5            Tunneled  tunnel
16/64:e8:81:3f:b5:00/1/1/4  default-tunneled-user  tunnel
TUNNELED USER

User Entries: 1/1
Curr/Cum Alloc:1/1 Free:0/0 Dyn:1 AllocErr:0 FreeErr:0
```

It takes about 5 minutes for the gateway to complete the reboot.

After the reboot, it will join the cluster again and update the bucket map to distribute the clients again over the active cluster members. This will happen about 4-5 minutes after the reload was completed.

About 9-10 minutes after you have initiated the reload of the gateway, the PC4 client should be active on the original gateway again.

You have completed this Lab!

Lab 11.01 Group-Based Policies with EVPN

Overview

In this lab you will explore how group-based policies can be used to enforce access control an EVPN network.

In the first task, you will load a preconfigured template to the aggregation and edge switches. This will provide you with a working EVPN setup. In the remainder of that task, you will review the operation of the EVPN network.

In the second task, you will review the configuration of the group-based policies. This will include the review of the global role IDs and user roles.

In the last task you will configure an example group-based policy and apply it to the user roles to verify the operation.

Objectives

After completing this lab, you will be able to:

- Review an existing EVPN deployment.
- Understand the use of group-based policies in an EVPN network.
- Review global role to role ID mapping.
- Configure a group-based policy in a user role.
- Verify the operation of group-based policy access control.

Task 1: Prepare your lab environment

In this task you will load preconfigured templates in Aruba Central for your aggregation and edge switches.

The templates include the base EVPN configuration and will provide you with a functional EVPN setup.

The configuration is a *brownfield* configuration. This means that you can still use the existing underlay VLANs (3,4,11-15, 21-25) that have been used in the training labs up to this point as classic switched/tagged VLANs. They are not affected at all by this EVPN setup.

Only the new VLANs (51-55) will be transported over the EVPN VXLAN network.

The EVPN setup will establish an L3 routed topology on VLAN 3. This will be used as the underlay IP network to transport the EVPN VXLAN traffic.

The EVPN client VLANs are in a completely different range (51-55, however only VLAN 51 is used in this lab), these VLANs are not enabled on the uplink LAG and exist only *locally* on the edge switches.

Any client assigned to the VLAN 51 will be transported over the network using EVPN.

The AP management VLAN 4 is not bound to EVPN and will just be L2 switched (on the underlay network).

The EVPN network SVIs have been configured in a dedicated VRF named *iot*.

The aggregation switch sw-agg1 provides the default gateway function for SVI 51 in this VRF iot. To keep the setup simple, only sw-agg1 has been configured as default gateway.

Sw-agg1 performs route leaking between the VRF iot and the VRF default. This ensures that any client that is assigned to EVPN VLAN 51 (in the 10.1.51.0/24 subnet) can access all the existing resources and subnets in the network.

The clients in this setup will have the following functions:

- PC1: This PC will act as an iot device with a user role iot-ac (HVAC - air conditioning). It will be assigned the user role iot-ac based on MAC authentication.
- PC4: This PC will act as a corporate authenticated PC. You will configure it with both users—contractor and employee—to see the differentiated access. The assigned user roles will be contractor and employee based on the authenticated user.

The authentication settings have been prepared in the template. You will need to configure the clients and verify the client access to the network.

Objectives

- Review the EVPN configuration and state.
- Review the MAC address table in an EVPN network.

Steps

Update Aggregation Switch Configuration

In these steps, you will update the aggregation switch configuration by changing their template in Aruba Central.

1. In Aruba Central, navigate to Context: **Groups / campus-sw-agg-tpl** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
2. On the Templates page, edit the **sw-agg** template.
3. On the desktop of MGMT PC, in the IACA Student Files folder, copy the contents of the file **iaca – lab 11.01 – sw-agg – evpn.txt**.
4. In Aruba Central, delete the text in the current template text and paste contents of the **iaca – lab 11.01 – sw-agg – evpn.txt** file.
5. Click **Save**.

Update the Edge Switch Configuration

In the next steps, you will update the edge switch configuration by changing their template in Aruba Central.

6. In Aruba Central, navigate to Context: **Groups / campus-sw-edge-tpl** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
7. On the Templates page, edit the **sw-agg** template.
8. On the desktop of MGMT PC, in the IACA Student Files folder, copy the contents of the file **iaca – lab 11.01 – sw-edge – evpn.txt**.
9. In Aruba Central, delete the text in the current template text and paste contents of the **iaca – lab 11.01 – sw-edge – evpn.txt** file.
10. Click **Save**.

Enable Aruba Central Feature on sw-edge2

In lab 10.01, you disabled the Aruba Central feature on sw-edge2. You will now enable Aruba Central again.

11. Use the MGMT PC to open an SSH session to sw-edge2.
12. Enable the Aruba Central feature.

```
aruba-central
 enable
 exit
```

```
sw-edge2(config)# aruba-central
sw-edge2(config-aruba-central)# enable
sw-edge2(config-aruba-central)# exit
```

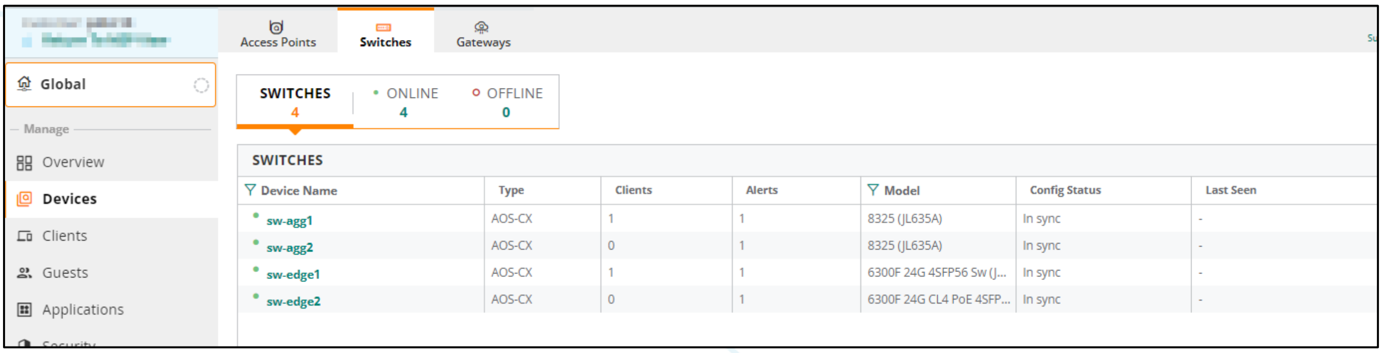
13. After a few moments, verify the status that Aruba Central is connected.

```
show aruba-central
```

```
sw-edge2(config)# show aruba-central
Central admin state                      : enabled

Central location                         : device-uswest4-d2.central.arubanetworks.com
VRF for connection                       : default
Shared Token                             : N/A
Central connection status                : connected

Central source                           : activate
Central source connection status         : connected
Central source last connected on         : Mon Dec 26 15:45:42 UTC 2022
System time synchronized from Activate   : True

Activate Server URL                      : devices-v2.arubanetworks.com
CLI location                             : N/A
CLI VRF                                  : N/A

Source IP                                : 10.1.1.53
Source IP Overridden                     : False

Central support mode                     : disabled
```

Verify the Switch Configuration Deployment

14. In Aruba Central, navigate to Context: **Global**> Navigation: **Devices** > Top **Switches**.



15. Verify that all four switches have Config Status **In Sync**.

NOTE: It may take a minute to complete the configuration push.

Review the EVPN BGP Connections

16. Use the MGMT PC to open an SSH connection to sw-edge1 and sw-edge2.

17. On sw-edge1, review the BGP L2 EVPN summary.

```
show bgp l2vpn evpn summary
```

```
sw-edge1# show bgp l2vpn evpn summary
VRF : default
BGP Summary
-----------
 Local AS               : 65001        BGP Router Identifier  : 10.1.0.4
 Peers                  : 1            Log Neighbor Changes   : No
 Cfg. Hold Time         : 180          Cfg. Keep Alive        : 60
 Confederation Id       : 0

 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 10.1.0.2        65001        7       5       00h:01m:04s  Established   Up
```

- **Question**: What BGP peers do you see in the configuration?
- **Answer**: 10.1.0.2. This is sw-agg1, it acts as the central BGP EVPN route reflector.
- **Question**: What is the status for this peer?
- **Answer**: Established. This means there is a successful BGP connection with the sw-agg1.

18. On sw-edge2, review the BGP L2 EVPN summary. Verify there is an established peer to 10.1.0.2.

```
show bgp l2vpn evpn summary
```

```
sw-edge2# show bgp l2vpn evpn summary
VRF : default
BGP Summary
-----------
 Local AS               : 65001        BGP Router Identifier  : 10.1.0.5
 Peers                  : 1            Log Neighbor Changes   : No
 Cfg. Hold Time         : 180          Cfg. Keep Alive        : 60
 Confederation Id       : 0

 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 10.1.0.2        65001        8       7       00h:01m:56s  Established   Up
```

19. On sw-edge1, review the BGP configuration

```
show running-config bgp
```

```
sw-edge1(config)# show running-config bgp
router bgp 65001
    bgp router-id 10.1.0.4
    neighbor 10.1.0.2 remote-as 65001
    neighbor 10.1.0.2 update-source loopback 0
    address-family l2vpn evpn
        neighbor 10.1.0.2 activate
        neighbor 10.1.0.2 send-community both
```

```
    exit-address-family
!
```

Review the EVPN Configuration

In the next steps you will used sw-edge1 to review the basic EVPN configuration that has been loaded by the template.

20. On sw-edge1, review the loaded EVPN VXLAN VNI to VLAN mapping.

```
show running-config interface vxlan
```

```
sw-edge1(config)# show running-config interface vxlan
interface vxlan 1
    source ip 10.1.0.4
    no shutdown
    vni 10051
        vlan 51
```

21. Review the EVPN configuration.

```
show running-config evpn
```

```
sw-edge1(config)# show running-config evpn
evpn
    vlan 51
        rd auto
        route-target export auto
        route-target import auto
```

22. Verify that VLAN 51 is not enabled on the uplink port LAG 256. Traffic for remote hosts in VLAN 51 will be tunneled through VXLAN tunnels.

```
show vlan 51
```

```
sw-edge1# show vlan 51

-----------------------------------------------------------------------------------
-----
VLAN  Name                                 Status   Reason                  Type
Interfaces
-----------------------------------------------------------------------------------
-----
51    VLAN51                               up       ok                      static      vxlan1
```

Configure Client PC1

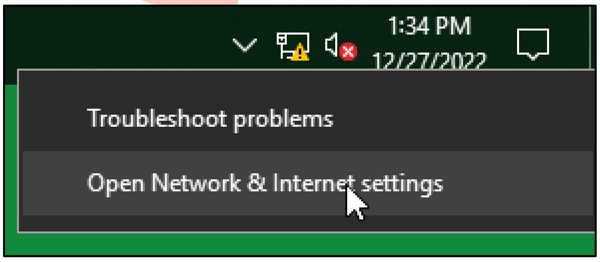
PC1 will acts as the iot-ac device in this lab. It will be authenticated using MAC-auth.

You need to set a MAC address on PC1 to match the iot-ac MAC range.

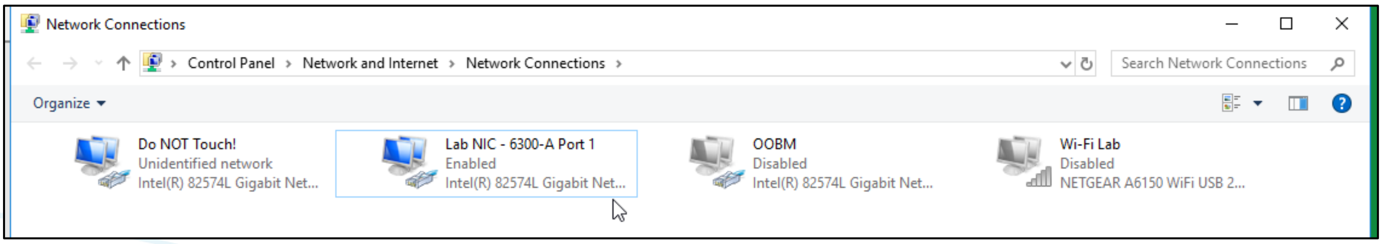
The MAC address prefix will be C6C001 + pod + table + 01 (PC01).

For example, for Pod 28, Table 13, the MAC would be: **c6c001**281301

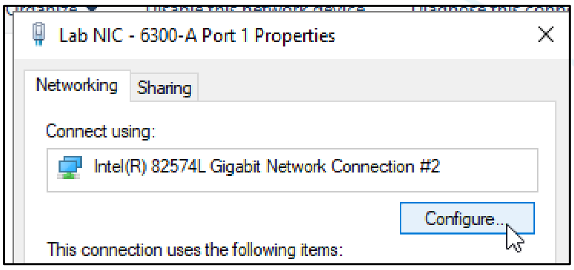
23. Open a connection to PC1.
24. Open **Network & Internet Settings**.



25. Click **Change Adapter Options**.
26. *Disable* the WLAN NIC.
27. Verify the OOBM NIC is disabled.
28. Enable the Lab NIC.
29. Review the result status of the network interfaces.



30. Right-click Lab NIC and select **Properties**.
31. Click **Configure**.



32. Click **Advanced**.
33. Scroll down and select the property **Locally Administered Address**.
34. Set the value to:
    - c6c001 pod# table# 01
      For example: **c6c001**281301 for pod 28 table 13 PC01
35. Click **OK** to close the network properties.

NOTE: If Windows would prompt you about network discovery, you may click **Yes**.

36. Open a command prompt and execute **ipconfig**. Take note of the PC1 IP address.

```
ipconfig
```

```
C:\Users\student> ipconfig

Windows IP Configuration


...

Ethernet adapter Lab NIC - 6300-A Port 1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.1.51.151
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.51.1
```

- **Question**: What IP address is assigned to PC1?
- **Answer**: The user role of the client assigns the client to VLAN 51. In this VLAN the PC1 should receive an IP address in the 10.1.51.0/24 subnet.

Take note of the IP address. You will attempt to ping to this IP address using PC4 in the next task.

- PC1 Lab IP address: 10.1.51._____

37. Start a continuous ping to **10.254.1.21**.

```
ping 10.254.1.21 -t
```

38. On sw-edge1, review the port-access clients for port 1/1/1.

```
show port-access clients interface 1/1/1
```

```
sw-edge1# show port-access clients interface 1/1/1

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-------------------------------------------------------------------------------------
-------------------
  Port      MAC-Address        Onboarding     Status      Role
Device Type
                               Method
```

```
-------------------------------------------------------------------------------------
-------------------
c 1/1/1    00:50:56:b1:ee:e9                Fail
c 1/1/1    c6:c0:01:28:13:01 mac-auth       Success     iot-ac
c 1/1/1    68:b5:99:a3:a1:c0                Fail
```

- **Question**: Do you see a successfully authenticated client on port 1/1/1?
- **Answer**: Yes, based on the MAC-auth of port 1/1/1, the PC1 is authenticated with user role iot-ac.

NOTE: You may see other MAC addresses on the port. This could be the transit switch between the PC1 VM and your lab switch, or the original PC1 MAC address (or both). The only important result is the success iot-ac authentication based on the new MAC address.

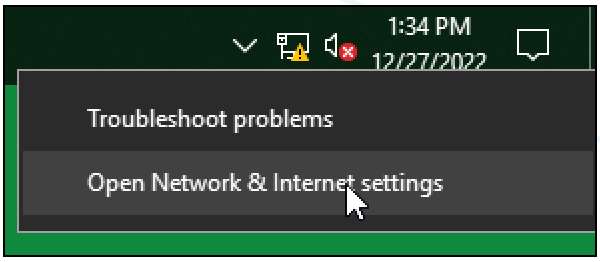
Configure Client PC4

PC4 will connect with 802.1X authentication using two different user accounts: employee and contractor.

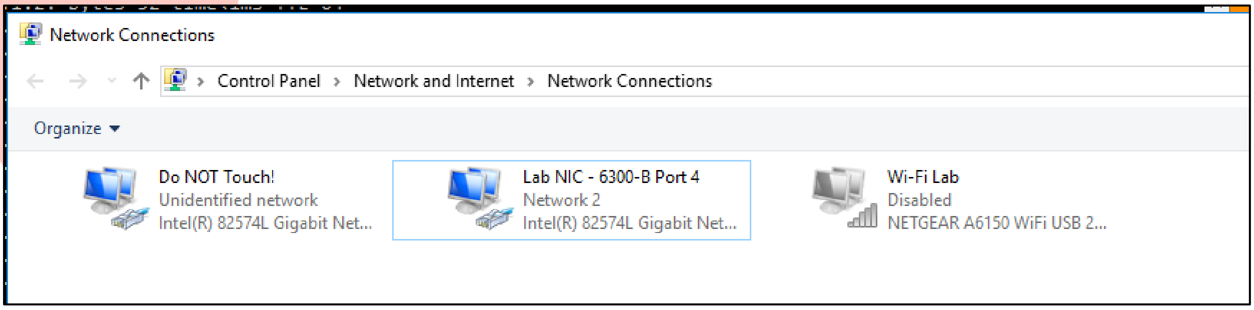
PC4 has been configured with a certificate for the contractor user in previous labs that was used with EAP-TLS.

To simplify the switching of user roles, you will used EAP-PEAP (username and password) in this lab instead of EAP-TLS (certificate based).

39. Open a connection to PC4.
40. Open **Network & Internet Settings**.



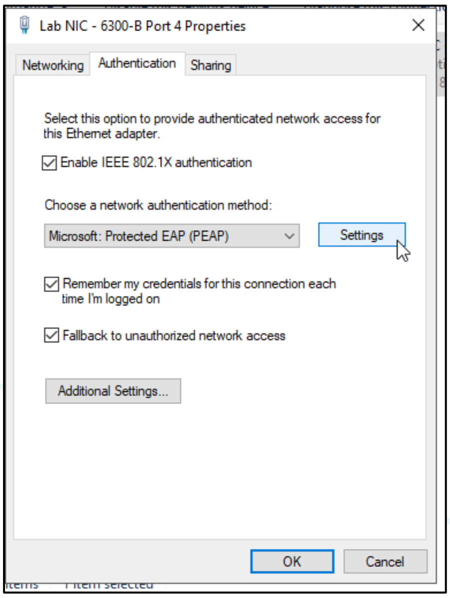
41. Click **Change Adapter Options**.
42. The WLAN NIC should still be disabled (should be no change).
43. The Lab NIC should be enabled (should be no change).
44. Review the status of the network interfaces.



45. Right-click **Lab NIC** and select **Properties**.
46. Click **Authentication**.

NOTE: If you don't see the Authentication page, you need to start the Wired AutoConfig service.

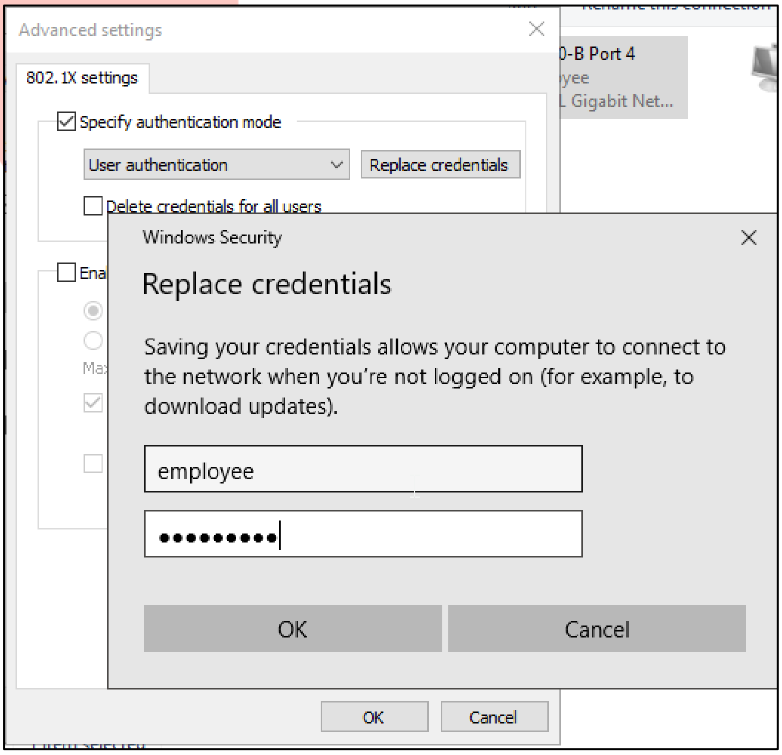
47. Set the Authentication Method to **Microsoft: Protected EAP (PEAP)**.



48. Click **Settings**, **uncheck** the **Verify the Server Identity** option.

NOTE: In a production environment it is recommended to enable the Certificate Validation.

49. Click **OK**.
50. Click **Additional Settings**. Specify **User authentication** as the mode.
51. Click **Save credentials** and enter **employee / Aruba123!** for the credentials.



52. Click **OK** to submit the credentials.
53. Click **OK** to close the settings.
54. Click **OK** to close the properties.

PC4 will now authenticate with EAP-PEAP to the network using the employee credentials.

55. Open a command prompt, use ipconfig to review the assigned IP address.

```
ipconfig
```

```
C:\Users\student> ipconfig

Windows IP Configuration


...

Ethernet adapter Lab NIC - 6300-B Port 4:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.1.51.150
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.51.1
```

- **Question**: What IP address was assigned to PC4?

- **Answer**: The employee user role assigns VLAN 51. The PC4 should have an IP address in the 10.1.51.0/24 subnet.

56. Start a continuous ping to 10.254.1.21 to verify network connectivity.

```
ping 10.254.1.21 -t
```

57. On sw-edge2, review the port-access clients on interface 1/1/4. Verify the employee is successfully authenticated on the port.

```
show port-access clients interface 1/1/4
```

```
sw-edge2# show port-access clients interface 1/1/4

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

------------------------------------------------------------------------------------
-------------------
  Port      MAC-Address       Onboarding     Status      Role
Device Type
                              Method
------------------------------------------------------------------------------------
-------------------
c 1/1/4    ec:b1:d7:1b:07:00                Fail
c 1/1/4    00:50:56:b1:b9:0d dot1x          Success     employee
```

Task 2: Verify the Group-Based Policy Configuration

The template contains three user roles that have been preconfigured with basic settings to ensure the clients can get connected to the network:

- employee
- contractor
- iot-ac

These roles currently have the same configuration:

- They are bound to a group-based policy (GBP)
- The GBP allows traffic from the role *default* to the individual role

Each user role used with GBP is assigned a role ID. This role name to role id mapping must be known to all switches.

In this task you will review this mapping and role configuration that was applied by the template.

Objectives

- Understand the global role id to role mapping.
- Review an existing group-based policy configuration.

Steps

Review the Global GBP Role Mapping

1. Use the MGMT PC to open an SSH connection to sw-edge1 and sw-edge2.
2. On sw-edge1, review the global GBP role mapping.

```
show gbp role-mapping
```

```
sw-edge1(config)# show gbp role-mapping

GBP status : Enabled
GBP_ROLE                       GBP_ROLE_ID
-------------                  ---------------
contractor                     101
default                        0
employee                       102
infra                          2
iot-ac                         103
```

3. Repeat this on sw-edge2.

```
show gbp role-mapping
```

```
sw-edge2(config)# show gbp role-mapping

GBP status : Enabled
GBP_ROLE                       GBP_ROLE_ID
```

```
-------------                -------------
contractor                   101
default                      0
employee                     102
infra                        2
iot-ac                       103
```

- **Question**: What do you notice?
- **Answer**: Both edge switches have the same role name to role id mapping table. When the administrator configures a rule with a role name, such as **employee**, the hardware knows how to translate this role name employee to an id.

  Since the same role mapping is applied on all switches, the traffic that is marked with the id of employee can be recognized by the other switches in the network.

Review a User Role with Group Based Policy

4. On sw-edge1, review the user role iot-ac.

```
show port-access role name iot-ac
```

```
sw-edge1(config)# show port-access role name iot-ac

Role Information:

Name  : iot-ac
Type  : local
----------------------------------------------
    Reauthentication Period              :
    Cached Reauthentication Period       :
    Authentication Mode                  :
    Session Timeout                      :
    Client Inactivity Timeout            :
    Description                          :
    Gateway Zone                         :
    UBT Gateway Role                     :
    UBT Gateway Clearpass Role           :
    Access VLAN                          : 51
    Native VLAN                          :
    Allowed Trunk VLANs                  :
    Access VLAN Name                     :
    Native VLAN Name                     :
    Allowed Trunk VLAN Names             :
    VLAN Group Name                      :
    MTU                                  :
    QOS Trust Mode                       :
    STP Administrative Edge Port         :
    PoE Priority                         :
    PVLAN Port Type                      :
    Captive Portal Profile               :
    Policy                               :
    GBP                                  : iot-ac
```

```
    Device Type                                  :
```

5. Review the GBP policy iot-ac.

```
show port-access gbp iot-ac
```

```
sw-edge1(config)# show port-access gbp iot-ac

Port Access GBP Details:
======================

GBP Name   : iot-ac
GBP Type   : Local
GBP Status : Applied

SEQUENCE    CLASS                            TYPE     ACTION
----------- -------------------------------- -------- -----------------------
10          iot-ac-arp                       gbp-mac  permit
20          iot-ac-ip                        gbp-ipv4 permit
```

6. Review the two GBP classes.

```
show class gbp-ip iot-ac-ip
```

```
sw-edge1(config)# show class gbp-ip iot-ac-ip
Type        Name
            Additional Class Parameters
  Sequence Comment
            Action                          L3 Protocol
            Source Role name                Source L4 Port(s)
            Destination Role name           Destination L4 Port(s)
            Additional Entry Parameters
-------------------------------------------------------------------------------
GBP-IPv4    iot-ac-ip
        10
            match                           any
            default
            iot-ac
            Hit-counts: enabled
-------------------------------------------------------------------------------
```

```
show class gbp-mac iot-ac-arp
```

```
sw-edge1(config)# show class gbp-mac iot-ac-arp
Type        Name
            Additional Class Parameters
  Sequence Comment
            Action                          EtherType
            Source Role name
            Destination Role name
            Additional Entry Parameters
-------------------------------------------------------------------------------
GBP-MAC     iot-ac-arp
        10
```

```
        match                        arp
        any
        iot-ac
        Hit-counts: enabled
-------------------------------------------------------------------------------
```

- **Question**: What access control does this GBP policy provide?
- **Answer**: A GBP policy controls traffic outbound to the client (from the network **to** the controlled client). Based on the source role ID of the incoming packet.
- This policy allows:
  - ARP traffic from any role.
  - IP traffic from the default role, the role with ID 0. This is all traffic that is not sourced from a client with GBP id.
- **Question**: Do you see a rule for the role employee?
- **Answer**: No, only the traffic from role default (no role set) can reach the iot-ac.
- **Question**: Would traffic from another iot-ac client be able to reach this iot-ac client?
- **Answer**: No. With this configuration, only traffic from the default role will be accepted.

7. The loaded configuration includes a count option. Review the class **iot-ac-ip** gbp hitcount.

```
show port-access gbp iot-ac hitcount
```

```
sw-edge1(config)# show port-access gbp iot-ac hitcount

Port Access GBP Hit-Counts Details:
======================================

GBP Name   : iot-ac
GBP Type   : Local
GBP Status : Applied

SEQUENCE    CLASS                            TYPE     ACTION
----------- -------------------------------- -------- -----------------------
10          iot-ac-arp                       gbp-mac  permit
20          iot-ac-ip                        gbp-ipv4 permit


Class Name : iot-ac-arp
Class Type : gbp-mac

SEQUENCE    CLASS-ENTRY                                             HIT-COUNT
----------- ------------------------------------------------------- -----------
10          match arp any iot-ac count                              1
```

```
Class Name : iot-ac-ip
Class Type : gbp-ipv4

SEQUENCE    CLASS-ENTRY                                                    HIT-COUNT
----------- -------------------------------------------------------------- -----------
10          match any default iot-ac count                                 16
```

8. Wait about 10 seconds, then repeat the command.

```
show port-access gbp iot-ac hitcount
```

```
sw-edge1(config)# show port-access gbp iot-ac hitcount

Port Access GBP Hit-Counts Details:
======================================

GBP Name   : iot-ac
GBP Type   : Local
GBP Status : Applied

SEQUENCE    CLASS                             TYPE     ACTION
----------- -------------------------------- -------- -----------------------
10          iot-ac-arp                        gbp-mac  permit
20          iot-ac-ip                         gbp-ipv4 permit


Class Name : iot-ac-arp
Class Type : gbp-mac

SEQUENCE    CLASS-ENTRY                                                    HIT-COUNT
----------- -------------------------------------------------------------- -----------
10          match arp any iot-ac count                                     1

Class Name : iot-ac-ip
Class Type : gbp-ipv4

SEQUENCE    CLASS-ENTRY                                                    HIT-COUNT
----------- -------------------------------------------------------------- -----------
10          match any default iot-ac count                                 38
```

- Question: What do you observe?
- Answer: The counter increases. The PC1 is performing a continuous ping to 10.254.1.21. The **return** traffic of this ping will be counted by the hit counter.

TIP: You can make it easier to read the counter by clearing the hit count using this command: **clear port-access gbp iot-ac hitcounts**.

9. Switch to the SSH connection to sw-edge2.
10. On sw-edge2, review the user role employee and contractor. They have a similar configuration as the iot-ac user role: allow only traffic from default.

```
show port-access role name employee
```

```
sw-edge2# show port-access role name employee

Role Information:

Name  : employee
Type  : local
----------------------------------------------
    Reauthentication Period             :
    Cached Reauthentication Period      :
    Authentication Mode                 :
    Session Timeout                     :
    Client Inactivity Timeout           :
    Description                         :
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 51
    Native VLAN                         :
    Allowed Trunk VLANs                 :
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      :
    STP Administrative Edge Port        :
    PoE Priority                        :
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              :
    GBP                                 : employee
    Device Type                         :
```

```
show port-access role name contractor
```

```
sw-edge2# show port-access role name contractor

Role Information:

Name  : contractor
Type  : local
----------------------------------------------
    Reauthentication Period             :
    Cached Reauthentication Period      :
    Authentication Mode                 :
    Session Timeout                     :
    Client Inactivity Timeout           :
    Description                         :
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
```

```
Access VLAN                        : 51
Native VLAN                        :
Allowed Trunk VLANs                :
Access VLAN Name                   :
Native VLAN Name                   :
Allowed Trunk VLAN Names           :
VLAN Group Name                    :
MTU                                :
QOS Trust Mode                     :
STP Administrative Edge Port       :
PoE Priority                       :
PVLAN Port Type                    :
Captive Portal Profile             :
Policy                             :
GBP                                : contractor
Device Type                        :
```

The configured GBP is based on the same logic as the iot-ac:

- Traffic from default to the role is allowed
- All ARP traffic is allowed.

Task 3: Configure Access Control Between Roles

Based on the loaded template configuration, no IP traffic is allowed between the roles employee, contractor, and iot-ac.

In this task you will allow traffic between the GBP roles.

First you will verify that there is no access between the employee and the iot-ac device.

Next you will configure the roles to allow access between the employee and the iot-ac device and verify the access.

After this verification, you will use PC4 to login with the contractor user account. The PC4 will still have the same MAC and IP address, but it will have a different role.

Based on this contractor role, access to the iot-ac device will be blocked.

The last step will be to allow only ICMP traffic between the contractor and the iot-ac device.

Objectives

- Configure group-based policy classes.
- Configure group-based policy in a user role.
- Verify the operation of the group-based policy.

Steps

Verify No Access Between PC1 iot-ac and PC4 employee

First, as an employee, you will try to access the iot-ac device. This will fail since currently no role-to-role rule exists.

1. On PC4, start a new command prompt (you may leave the continuous ping to 10.254.1.21 running in its own window).
2. On PC4, attempt to ping the IP address of PC1. You have noted this IP address in the first task. This ping will fail.

```
ping 10.1.51.x
```

```
C:\Users\student> ping 10.1.51.x

Pinging 10.1.51.x with 32 bytes of data:
Request timed out.
```

3. On PC4, review the ARP table entry for the PC1 IP address. ARP traffic is allowed in the loaded template, therefore you should see an ARP entry with the MAC address of PC1 as iot-ac device (the MAC address begins with **C6C001**)

```
arp -a 10.1.51.x
```

```
C:\Users\student> arp -a 10.1.51.151

Interface: 10.1.51.150 --- 0xc
  Internet Address      Physical Address      Type
  10.1.51.151           c6-c0-01-28-13-01     dynamic
```

4. Start a continuous ping to the IP address of PC1.

```
ping 10.1.51.x -t
```

```
C:\Users\student>ping 10.1.51.x -t

Pinging 10.1.51.x with 32 bytes of data:
Request timed out.
Request timed out.
...
```

Allow employee to iot-ac Access

Now you will update the iot-ac and employee roles to allow access to each other.

NOTE: In a production network, the role configuration should be consistent on all switches. You should use Aruba Central templates or Aruba NetConductor to deploy consistent roles to all your devices.

In this lab, you are manually testing the function of the GBP roles; therefore you are accessing the sw-edge1 and sw-edge2 and performing the configuration individually.

5. On sw-edge1, the PC1 iot-ac device is connected and assigned the user role iot-ac. This iot-ac role must be updated to allow outbound traffic to the client:
   - traffic FROM role employee TO role iot-ac.

```
class gbp-ip iot-ac-ip
 10 match ip default iot-ac count
 20 match ip employee iot-ac count
 exit
```

```
sw-edge1(config)# class gbp-ip iot-ac-ip
sw-edge1(config-class-gbp-ip)#  10 match ip default iot-ac count
sw-edge1(config-class-gbp-ip)#  20 match ip employee iot-ac count
sw-edge1(config-class-gbp-ip)#  exit
```

Now not only traffic from the default (unmarked) role will be allowed, but IP traffic from the role employee will also be allowed to the role iot-ac.

The global role mapping table will be used to translate the name employee to a role id.

6. On sw-edge2, the PC4 employee device is connected and assigned the user role employee. This employee role must be updated to allow outbound traffic to the client:
    - traffic FROM role iot-ac TO role employee.

```
class gbp-ip employee-ip
 10 match ip default employee count
 20 match ip iot-ac employee count
 exit
```

```
sw-edge2(config)# class gbp-ip employee-ip
sw-edge2(config-class-gbp-ip)#  10 match ip default employee count
sw-edge2(config-class-gbp-ip)#  20 match ip iot-ac employee count
sw-edge2(config-class-gbp-ip)#  exit
```

Verify employee to iot-ac Access

7. On PC4, review the ping status to the IP address of PC1.

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.1.51.52: bytes=32 time<1ms TTL=128
Reply from 10.1.51.52: bytes=32 time<1ms TTL=128
Reply from 10.1.51.52: bytes=32 time<1ms TTL=128
...
```

- **Question**: What do you observe?
- **Answer**: After the GBP policy was updated for both user roles, the ping is successful.

8. On sw-edge1, review the port access gbp iot-ac hitcounts.

```
show port-access gbp iot-ac hitcount
```

```
sw-edge1(config)# show port-access gbp iot-ac hitcount

Port Access GBP Hit-Counts Details:
======================================

GBP Name   : iot-ac
GBP Type   : Local
GBP Status : Applied

SEQUENCE    CLASS                            TYPE     ACTION
----------- -------------------------------- -------- ----------------------
10          iot-ac-arp                       gbp-mac  permit
20          iot-ac-ip                        gbp-ipv4 permit
```

```
Class Name : iot-ac-arp
Class Type : gbp-mac

SEQUENCE    CLASS-ENTRY                                                    HIT-COUNT
----------- -------------------------------------------------------------- -----------
10          match arp any iot-ac count                                     7

Class Name : iot-ac-ip
Class Type : gbp-ipv4

SEQUENCE    CLASS-ENTRY                                                    HIT-COUNT
----------- -------------------------------------------------------------- -----------
10          match any default iot-ac count                                 184
20          match any employee iot-ac count                                54
```

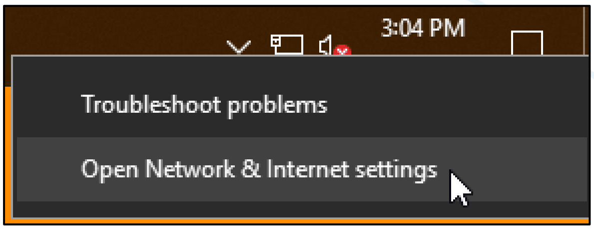
- **Question**: What do you observe?
- **Answer**: The continuous ping from the PC4 to the PC1 arrives on sw-edge1 as outbound for PC1, with the role id of employee. It will match the employee role rule and that counter will be increasing.

Verify the Same Device with a Different Role

Now that you have enabled access between employee and the iot-ac device, you want to check if another user account on PC4 can still access the iot-ac device.

On PC4, you will now connect via 802.1X using the contractor account. This user will be assigned a different user role (contractor) from the employee. The result will be that the contractor will not be able to access the iot-ac device, even when it has the same MAC and IP address as the original employee system.

9. On PC4, open the **Network & Internet settings**.



10. Click **Change Adapter Options**.
11. Open the **Properties** of the Lab NIC.
12. Click **Authentication**.
13. Click **Additional Settings**.
14. Click **Replace Credentials** and change the credentials to **contractor / Aruba123!**
15. Click **OK** to submit the credentials.
16. Click **OK** to close the settings.

17. Click **OK** to close the properties.

PC4 will now authenticate with the updated *contractor* credentials.

18. Verify the continuous ping to 10.254.1.21 is still working.

```
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
Reply from 10.254.1.21: bytes=32 time=4ms TTL=126
Reply from 10.254.1.21: bytes=32 time=2ms TTL=126
...
```

19. Confirm the continuous ping to the PC1 IP address is no longer working.

```
Reply from 10.1.51.52: bytes=32 time<1ms TTL=128
Reply from 10.1.51.52: bytes=32 time<1ms TTL=128
Reply from 10.1.51.52: bytes=32 time<1ms TTL=128
Request timed out.
Request timed out.
```

20. Open a new command prompt to check the IP address of PC4.

- **Question**: Did the IP address change?
- **Answer**: No, the client still has the same MAC and IP address as before. The access to iot-ac is not blocked based on the IP address but based on the source user role. This has changed from employee to contractor. Contractor is not allowed in the GBP of the iot-ac.

21. On sw-edge2, verify the updated port access clients on interface 1/1/4.

```
show port-access clients interface 1/1/4
```

```
sw-edge2(config)# show port-access clients interface 1/1/4

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-------------------------------------------------------------------------------------
-------------------
  Port     MAC-Address       Onboarding     Status      Role
Device Type
                             Method
-------------------------------------------------------------------------------------
-------------------
c 1/1/4    00:50:56:b1:b9:0d dot1x          Success     contractor
c 1/1/4    ec:b1:d7:1b:07:00                Fail
```

Allow ICMP Access between the Roles contractor and iot-ac

In the next steps you will allow ICMP access between the contractor and the iot-ac device.

You must make the change in 2 places:

- In the iot-ac role configuration, you must allow outbound ICMP traffic from the contractor role.
- In the contractor role configuration, you must allow outbound ICMP traffic from the iot-ac role.

You will first update the iot-ac role and verify the status when only one side is configured.

22. On sw-edge1, update the iot-ac-ip policy to allow traffic from the contractor role.

```
class gbp-ip iot-ac-ip
 10 match ip default iot-ac count
 20 match ip employee iot-ac count
 30 match icmp contractor iot-ac count
 exit
```

```
sw-edge1(config)# class gbp-ip iot-ac-ip
sw-edge1(config-class-gbp-ip)#  10 match ip default iot-ac count
sw-edge1(config-class-gbp-ip)#  20 match ip employee iot-ac count
sw-edge1(config-class-gbp-ip)#  30 match icmp contractor iot-ac count
sw-edge1(config-class-gbp-ip)#  exit
```

Now the iot-ac policy allows ICMP traffic traffic from the contractor.

23. Review the iot-ac hitcounts. Repeat the command after about 10 seconds.

```
show port-access gbp iot-ac hitcount
```

```
sw-edge1(config)# show port-access gbp iot-ac hitcounts

Port Access GBP Hit-Counts Details:
======================================

GBP Name   : iot-ac
GBP Type   : Local
GBP Status : Applied

SEQUENCE    CLASS                            TYPE     ACTION
----------- -------------------------------- -------- -----------------------
10          iot-ac-arp                       gbp-mac  permit
20          iot-ac-ip                        gbp-ipv4 permit


Class Name : iot-ac-arp
Class Type : gbp-mac

SEQUENCE    CLASS-ENTRY                                            HIT-COUNT
----------- ------------------------------------------------------ -----------
10          match arp any iot-ac count                             2

Class Name : iot-ac-ip
Class Type : gbp-ipv4
```

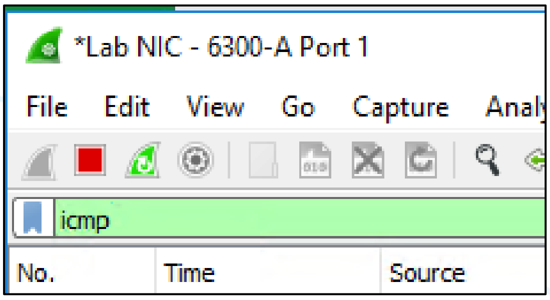
```
SEQUENCE    CLASS-ENTRY                                                    HIT-COUNT
----------- -------------------------------------------------------------- -----------
10          match any default iot-ac count                                 213
20          match any employee iot-ac count                                0
30          match icmp contractor iot-ac count                             4
```

```
...
SEQUENCE    CLASS-ENTRY                                                    HIT-COUNT
----------- -------------------------------------------------------------- -----------
10          match any default iot-ac count                                 220
20          match any employee iot-ac count                                0
30          match icmp contractor iot-ac count                             6
```

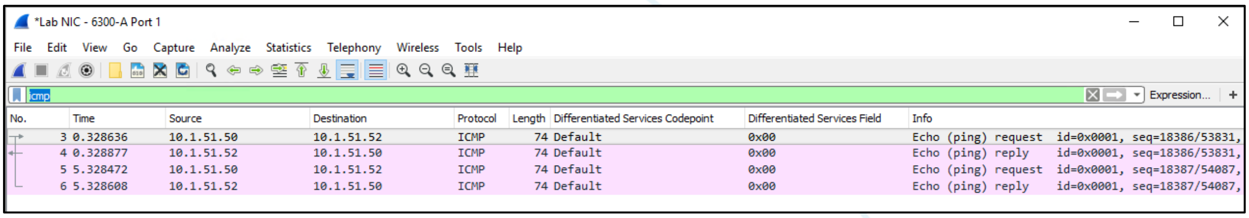
- **Question**: Do you see traffic matching the rule for the traffic from the contractor role?
- **Answer**: Yes, the hitcount value is increasing.

Use Wireshark on PC1 to Confirm the ICMP traffic

24. On PC1, stop the continuous ping to 10.254.1.21. This will reduce the number of packets you would see in the packet trace.
25. On PC1, start a Wireshark trace on the Lab NIC.
26. Set the display filter to **icmp** and press ENTER.



27. Stop the trace after about 5 seconds.



- **Question**: What ICMP traffic do you see?
- **Answer**: The iot-ac device receives ICMP requests from the PC4 (10.1.51.0/24) and it responds with an ICMP reply packet.

28. On PC4, check the ping status to PC1.

```
Request timed out.
Request timed out.
Request timed out.
...
```

- **Question**: Is the ping working?
- **Answer**: No. On the iot-ac role you have allowed traffic from the contractor, but on the contractor role you have not allowed traffic from the role iot-ac. You must ensure that traffic is allowed in both roles to have bi-directional communication.

Update the Contractor Role to Allow Traffic from the iot-ac Role

29. On sw-edge2, update the contractor role.

```
class gbp-ip contractor-ip
 10 match ip default contractor count
 20 match ip iot-ac contractor count
 exit
```

```
sw-edge2(config)# class gbp-ip contractor-ip
sw-edge2(config-class-gbp-ip)#  10 match ip default contractor count
sw-edge2(config-class-gbp-ip)#  20 match ip iot-ac contractor count
sw-edge2(config-class-gbp-ip)#  exit
```

30. On PC4, review the status of the ping to PC1.

```
...
Request timed out.
Request timed out.
Reply from 10.1.51.151: bytes=32 time=980ms TTL=128
Reply from 10.1.51.151: bytes=32 time<1ms TTL=128
...
```

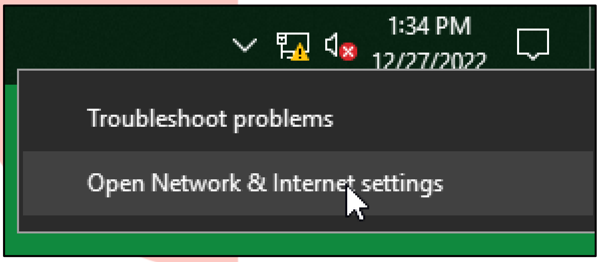
You have now enabled ICMP traffic between the contractor and the iot-ac, but any other traffic would still be blocked between these two roles.

This concludes the group-based policies activity.

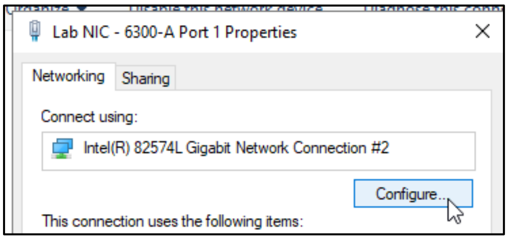
Cleanup

In the next steps, you will revert the PC1 Lab NIC to use the default MAC address.

1. On PC1, Open **Network & Internet Settings**.



2. Click **Change Adapter Options**.
3. Right-click Lab NIC, click **Properties**.
4. Click **Configure**.



5. Click **Advanced**.
6. Scroll down and select the property **Locally Administered Address**.
7. Set the value to **Not Present**.
8. Click **OK** to close the Properties.

You have completed this Lab!

Lab 12.01 Service Survivability

Overview

In this lab you will explore service survivability.

In the first task you will review how the tunneled WLAN can survive when the internet connection is unavailable.

After verifying the AP to gateway tunnel, you will block access to the internet and reboot all devices. This will demonstrate how the AP stores survivability information to establish tunnels to the gateways.

In the second task, you will review how the switches can be configured with cached re-authentication and a critical role. In case access to the RADIUS server is lost, these features can ensure that clients can stay connected to the network or connect to the network using a minimal service level.

Objectives

After completing this lab, you will be able to:

- Understand AP to gateway tunnel setup without an Internet connection.
- Understand switch cached reauthentication.
- Understand the switch critical role.

Task 1: Tunnel WLAN Central Survivability

The tunnels between APs and gateways are orchestrated by the overlay tunnel orchestrator service in Aruba Central. When Aruba Central is not reachable, the APs and GWs cannot reach the OTO service.

For the tunnels that are provisioned by the OTO service, backup tunnel information and IPsec keys are stored in the existing GW and AP systems. This can be used when Aruba Central could be unreachable for the devices due to an Internet link failure, for example.

Note that this only works for existing tunnel WLANs on *existing* gateways and APs. New APs or new tunnel WLAN configurations will work after the devices have established contact with Central's OTO service.

Objectives

- Review AP to gateway tunnel status.
- Verify AP to gateway tunnel setup without internet connection.

Steps

Verify Cluster and AP Operation

In the next steps you will review and verify that the gateway cluster is online, the APs are successfully connected to the cluster, and the APs are providing WLAN services.

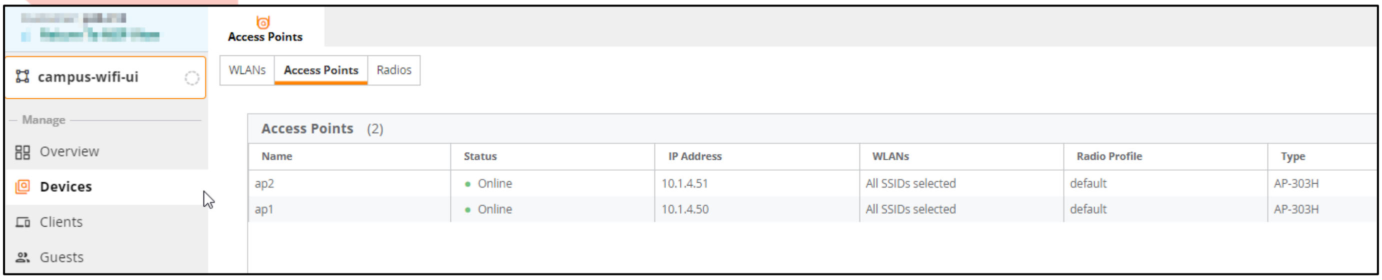
First, verify the gateways are online in the group cluster.

1. In Aruba Central, navigate to Context: **Global**> Navigation: **Devices** > Top **Gateways**.
2. Click **Clusters**.
3. Verify there are 4 AP tunnels (AP1 to GW1/GW2 and AP2 to GW1/GW2).

NOTE: If the cluster would be missing a gateway, verify:
- Both GW1 and GW2 are assigned to the group *campus-gw-main*
- The group campus-gw-main gateway configuration is set to *auto-group cluster*.
- The group campus-gw-main gateway configuration auto_gwcluster is set to *automatic*.

Verify that the APs have all WLANs enabled.

4. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
5. Click **Access Points**.



6. Verify the WLANs column shows **All SSIDs selected** for both ap1 and ap2.

NOTE: If one of the APs does not have this option, use the pencil button to edit the AP configuration and enable the WLANs.

Disable Internet Access

In the next steps, you will configure the rtr-core1 with an ACL to block access to the Internet. This will simulate a cloud connection failure.

7. Use the MGMT PC to open an SSH connection to rtr-core1.
8. Create a new IP access-list that blocks the device access to Aruba Central.

- Your management subnets (10.1.1.0, 10.1.3.0 and 10.1.4.0) are all in the 10.1.0.0/21 block
- Allow access to your internal network (devices should still be able to reach ClearPass).
- Block any other access for 10.1.0.0/21.
- Allow all other traffic.

```
access-list ip no-inet
 10 permit any 10.1.0.0/21 10.0.0.0/8
 20 deny any 10.1.0.0/21 any
 30 permit any any any
 exit
```

```
rtr-core1(config)# access-list ip no-inet
rtr-core1(config-acl-ip)# 10 permit any 10.1.0.0/21 10.0.0.0/8
rtr-core1(config-acl-ip)# 20 deny any 10.1.0.0/21 any
rtr-core1(config-acl-ip)# 30 permit any any any
rtr-core1(config-acl-ip)# exit
```

NOTE: The hostname of the rtr-core1 may be slightly different in your lab environment; it may include the pod and/or table number or the course title (IACA). This can be ignored.

9. Apply the IP ACL outbound on the port 1/1/9.

```
interface 1/1/9
 apply access-list ip no-inet out
 exit
```

```
rtr-core1(config)# interface 1/1/9
rtr-core1(config-if)# apply access-list ip no-inet out
rtr-core1(config-if)# exit
```

Reboot the Gateways and APs

To demonstrate that the survivability also works when the devices are rebooted while the cloud connection is down, you will now reboot the gateways and the APs.

10. Use the MGMT PC to open an SSH connection to gw1 (10.1.3.21).
11. Attempt to **ping pqm.arubanetworks.com**.

```
ping pqm.arubanetworks.com
```

```
(gw1) *# ping pqm.arubanetworks.com

! - Success  . - Failure  D - Duplicate Response
Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 52.207.118.149, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

12. After about 1 minute, check the Aruba Central control-channel. It should show as **DOWN**. Repeat the command until the connection status shows down.

```
show aruba-central details
```

```
(gw1) *#show aruba-central details

Aruba Central
-------------
Parameter                       Value
---------                       -----
Aruba Central IP/URL            device-uswest4.central.arubanetworks.com
Connection Status               DOWN
Time of last disconnect         Wed Dec 28 06:47:51 2022
SmartAmon MON Bootstrap Status  Init
Number of times WS connected    2
Time of last connect            Wed Dec 28 06:47:51 2022
```

13. Reboot the GW1 and confirm the reload.

```
reload
```

```
(gw1) *# reload
Do you really want to restart the system(y/n): y
```

```
System will now restart!
```

14. Open an SSH connection to GW2.
15. Verify you cannot access the internet.

```
ping pqm.arubanetworks.com
```

```
(gw2) # ping pqm.arubanetworks.com

! - Success   . - Failure  D - Duplicate Response
Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 3.232.163.149, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

16. Reboot the GW2 and confirm the reload.

```
reload
```

Let's reboot the APs now.

17. Use the lab dashboard to reboot the AP1 and AP2.

NOTE: If there is no power option in the lab dashboard, you can login on the console of the AP using admin / Aruba123! and use the reload command.

```
ap1# reload
Do you really want to reset the system(y/n): y
Reloading
```

Post Reboot Verification

The APs will be the first to complete the reboot.

18. Use the lab dashboard to connect to the console of either ap1 or ap2 using **admin / Aruba123!**
19. Review the AP Tunnel Agent (ATA) tunnel configuration. This shows that the AP is still aware of the required tunnels and tunnel endpoints, even without the cloud connection.

```
show ata current-cfg
```

```
ap1# show ata current-cfg

Current Central is Down
Microbranch AP is Disabled
Microbranch System IP is 0.0.0.0/::
[Current Configuration For cluster(auto_gwcluster_125_0)]
<Tunnel list>
```

```
-----pub_ip=10.1.3.22, local_ip=10.1.3.22, vlan=1,3,31-32,34-35, mcast=0,
Tun_Type=GRE, peer_device_type=Gateway
     key_exp=0, dstNatt=0, HBT_interval=3, HBT_Threshold=10
-----pub_ip=10.1.3.21, local_ip=10.1.3.21, vlan=1,3,31-32,34-35, mcast=0,
Tun_Type=GRE, peer_device_type=Gateway
     key_exp=0, dstNatt=0, HBT_interval=3, HBT_Threshold=10
<SSID list for primary>
-----ssid=p28t13-psk, type=0
-----ssid=p28t13-employee, type=0
-----ssid=p28t13-guest-cppm, type=0
```

20. Review the active tunnel status.

```
show ata endpoint
```

```
ap1# show ata endpoint

ATA Endpoint Status
-------------------
UUID  IP ADDR  STATE  TUN DEV  TUN SPI(OUT/IN)  LINK TAG  VALID TIME(s)  TUNNEL TYPE
GRE VLANs  HBT(Jiff/Missed/Sent/Rcv)  INNER IP  UP TIME(s)
----  -------  -----  -------  ---------------  --------  -------------  -----------
---------  ------------------------  --------  ----------
Total Endpoints Count: 0
```

- **Question**: Are the any tunnels currently active?
- **Answer**: No, the AP will first attempt to connect to Aruba Central.

21. Review the AP BSS-table.

```
show ap bss-table
```

```
ap1# show ap bss-table

Aruba AP BSS Table
------------------
bss                ess              port  ip       phy    type  ch/EIRP/max-EIRP
cur-cl  ap name  in-t(s)  tot-t  flags  mu-mimo
---                ---              ----  --       ---    ----  ----------------  ---
---  -------  -------  -----  -----  -------
f4:2e:7f:7b:15:f0  p28t13-employee  ?/?   0.0.0.0  a-VHT  ap    100E/15.0/25.5    0
ap1      0        2m:5s   W3r    1
f4:2e:7f:7b:15:e0  p28t13-employee  ?/?   0.0.0.0  g-HT   ap    11/7.0/23.0       0
ap1      0        2m:4s   W3r    0

Channel followed by "*" indicates channel selected due to unsupported configured
channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:2
Num Associations:0
```

```
Flags:       K = 802.11K Enabled; W = 802.11W Enabled; r = 802.11r Enabled; 3 = WPA3
BSS; O = Enhanced-open BSS with transition mode; o = Enhanced-open transition mode
open BSS; M = WPA3-SAE mixed mode BSS; E = Enhanced-open BSS without transition mode;
m = Agile Multiband (MBO) BSS; c = MBO Cellular Data Capable BSS; I = Imminent VAP
Down; T = Individual TWT Enabled; t = Broadcast TWT Enabled; d = Deferred Delete
Pending; a = Airslice policy; A = Airslice app monitoring; D = VLAN Discovered;
```

- **Question**: What do you observe?
- **Answer**: The p#tx-employee SSID is enabled on the AP, the other WLANs are not active.
- **Question**: What is the difference between the p#tx-employee WLAN and the other WLANs?
- **Answer**: The p#tx-employee is a mixed mode WLAN. The other WLANs are tunnel mode WLANs.
  - By default, a mixed mode WLAN will remain active when the tunnel to the gateways is down.
  - By default, a tunnel WLAN will be disabled when the tunnel is down for more than 30 seconds.

22. The AP will keep trying to reach Aruba Central for several minutes. After about 6 minutes, the AP will start using the survivability information and connect to the gateways. Repeat this command every minute until you see the survived tunnels.

```
show ata endpoint
```

Example output after the reboot. No tunnels have been established.

```
ap1# show ata endpoint

ATA Endpoint Status
-------------------
UUID  IP ADDR  STATE  TUN DEV  TUN SPI(OUT/IN)  LINK TAG  VALID TIME(s)  TUNNEL TYPE
GRE VLANs  HBT(Jiff/Missed/Sent/Rcv)  INNER IP  UP TIME(s)
----  -------  -----  -------  ---------------  --------  -------------  -----------
---------  -------------------------  --------  ----------
Total Endpoints Count: 0
```

Example after 6 minutes, with the tunnels established in a *survived* state.

```
ap1# show ata endpoint

ATA Endpoint Status
-------------------
UUID                                  IP ADDR    STATE              TUN DEV  TUN
SPI(OUT/IN)    LINK TAG  VALID TIME(s)  TUNNEL TYPE  GRE VLANs
HBT(Jiff/Missed/Sent/Rcv)  INNER IP   UP TIME(s)
----                                  -------    -----              -------  --------
-------    --------  -------------  -----------  ---------        -------------------
------  --------   ----------
```

```
9cdaa2df-2f0e-421f-be71-66794accd1af  10.1.3.22  SM_STATE_SURVIVED  tun0
c1284200/11450700  inet      6725          GRE          1,3,31-32,34-35
944/0/484/473                10.1.4.50  2022-12-28 12:09:42
a4a37eba-4742-4a84-ae17-297722b21f40  10.1.3.21  SM_STATE_SURVIVED  tun1
ba9d9600/b97dcc00  inet      6725          GRE          1,3,31-32,34-35
944/0/484/473                10.1.4.50  2022-12-28 12:09:42
Total Endpoints Count: 2
```

23. Open an SSH connection to GW1 and review the IPsec tunnels.

```
show crypto ipsec sa
```

```
(gw1) *# show crypto ipsec sa


IPSEC SA (V2) Active Session Information
-----------------------------------
Initiator IP                              Responder IP
SPI(IN/OUT)        Flags   Start Time        Tunnel Type   Inner IP
------------                              ------------                             -
---------------    ------  ---------------   ------------  ----------
10.1.4.51                                 10.1.3.21
a2192400/805ed900  UT2     Dec 28 07:10:14                 10.1.4.51
10.1.4.50                                 10.1.3.21
ba9d9600/b97dcc00  UT2     Dec 28 07:09:42                 10.1.4.50
10.1.3.22                                 10.1.3.21
4b66b400/c5ff3000  T2      Dec 28 06:55:28   N/A             -

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
       L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
       l = uplink load-balance; t = Tunnel Service; P = Reverse-Pinning Enabled

Total IPSEC SAs: 3
```

- **Question**: What are the IPsec connections in the list?
- **Answer**: 3 in total. 2 IPsec connections to the APs. They were initiated by the APs based on their survivability information. There is 1 IPsec connection to the GW2 for the cluster function. This connection was never orchestrated by the OTO and was always using the certificate-based authentication.

24. Review the ISAKMP SA list.

```
show crypto isakmp sa
```

```
(gw1) *# show crypto isakmp sa

ISAKMP SA Active Session Information
------------------------------------
Initiator IP                            Responder IP                        Flags
Start Time        Private IP                              Peer ID
------------                            ------------                        -----
----------        ----------                              -------------
```

```
10.1.3.22                              10.1.3.21                             r-v2-
c      Dec 28 06:55:28     -
CN=CNJJKLB09H::20:4c:03:b1:d5:02 L=SW
10.1.4.50                              10.1.3.21                             r-v2-
c-C    Dec 28 07:09:42   10.1.4.50
CN=CNJ2K2R0YR::20:4c:03:8c:27:42
10.1.4.51                              10.1.3.21                             r-v2-
c-C    Dec 28 07:10:14   10.1.4.51
CN=CNHSK2R4KP::20:4c:03:5b:27:e2

Flags: i = Initiator; r = Responder
       m = Main Mode; a = Agressive Mode; v2 = IKEv2
       p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature
       x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
       3 = 3rd party AP; C = Campus AP; R = Microbranch AP;  Ru = Custom Certificate
RAP; I = IAP
       V = VIA; S = VIA over TCP; l = uplink load-balance; P = Reverse-Pinning
Enabled

Total ISAKMP SAs: 3
```

- **Question**: How many of these ISAKMP sessions did you have when the OTO service was available?
- **Answer**: Only 1: the IPsec connection between the gateway cluster members. The IPsec keys for the AP to Gateways connections were setup by the OTO.
- **Question**: What type of IPsec authentication is used between the AP and the GW?
- **Answer**: The flag **c** indicates a certificate-based authentication. The AP is using its factory TPM certificate to authenticate to the GW. The GW only needs to have a list of authorized AP MAC addresses to validate the AP certificate subject name.

25. On the AP console, review the BSS table.

```
show ap bss-table
```

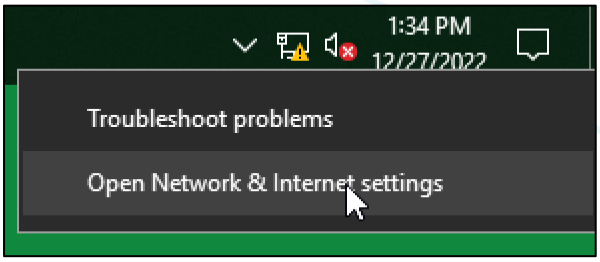
```
ap1# show ap bss-table

Aruba AP BSS Table
------------------
bss                ess                           port  ip          phy    type
ch/EIRP/max-EIRP  cur-cl  ap name            in-t(s)  tot-t     flags  mu-mimo
---                ---                           ----  --          ---    ----  ----
------------  ------  -------            -------  -----    -----  --------
f4:2e:7f:7b:15:f0  p28t13-employee               ?/?   0.0.0.0     a-VHT  ap
100E/15.0/25.5    0       20:4c:03:8c:27:42  0        18m:26s  W3r    1
f4:2e:7f:7b:15:f1  p28t13-psk                    ?/?   10.1.4.50   a-VHT  ap
100E/15.0/25.5    0       20:4c:03:8c:27:42  0        12m:46s  r      1
f4:2e:7f:7b:15:f2  p28t13-guest-cppm             ?/?   10.1.4.50   a-VHT  ap
100E/15.0/25.5    0       20:4c:03:8c:27:42  0        12m:46s  o      1
f4:2e:7f:7b:15:f3  _owetm_p28t13-guest-c311025731  ?/?   10.1.4.50   a-VHT  ap
100E/15.0/25.5    0       20:4c:03:8c:27:42  0        12m:45s  WO     1
```

```
f4:2e:7f:7b:15:e0  p28t13-employee                  ?/?   0.0.0.0    g-HT   ap
11/7.0/23.0       0       20:4c:03:8c:27:42  0        18m:26s  W3r    0
f4:2e:7f:7b:15:e1  p28t13-psk                       ?/?   10.1.4.50  g-HT   ap
11/7.0/23.0       0       20:4c:03:8c:27:42  0        12m:46s  r      0
f4:2e:7f:7b:15:e2  p28t13-guest-cppm                ?/?   10.1.4.50  g-HT   ap
11/7.0/23.0       0       20:4c:03:8c:27:42  0        12m:45s  o      0
f4:2e:7f:7b:15:e3  _owetm_p28t13-guest-c311025731   ?/?   10.1.4.50  g-HT   ap
11/7.0/23.0       0       20:4c:03:8c:27:42  0        12m:45s  WO     0

Channel followed by "*" indicates channel selected due to unsupported configured
channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:8
Num Associations:0

Flags:       K = 802.11K Enabled; W = 802.11W Enabled; r = 802.11r Enabled; 3 = WPA3
BSS; O = Enhanced-open BSS with transition mode; o = Enhanced-open transition mode
open BSS; M = WPA3-SAE mixed mode BSS; E = Enhanced-open BSS without transition mode;
m = Agile Multiband (MBO) BSS; c = MBO Cellular Data Capable BSS; I = Imminent VAP
Down; T = Individual TWT Enabled; t = Broadcast TWT Enabled; d = Deferred Delete
Pending; a = Airslice policy; A = Airslice app monitoring; D = VLAN Discovered;
```

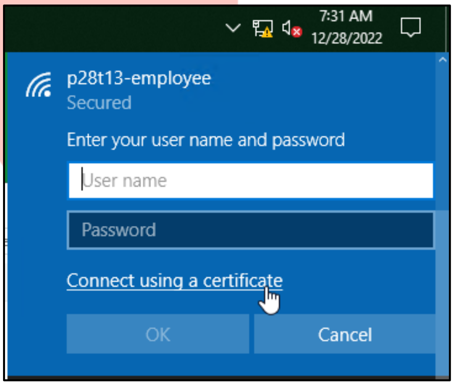
- **Question**: Do you have any active WLANs?
- **Answer**: Yes, the AP is broadcasting all the configured WLANs now, including the tunnel WLANs.

Verify Connectivity Using a Wireless Client

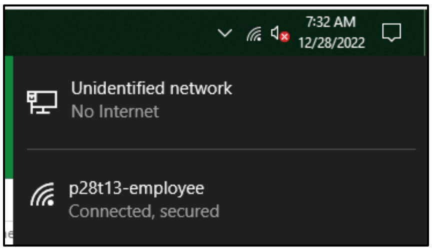
26. Open a connection to PC1.
27. Open **Network & Internet Settings**.



28. Click **Change Adapter Options**.
29. Disable the Lab NIC.
30. Enable the WLAN NIC.
31. Make a connection to your p#tx-employee WLAN using the employee certificate (EAP-TLS). Confirm the certificate message.



32. Verify that you are successfully connected.



This concludes the WLAN cloud survivability activity.

Restore the Internet Connection

33. On rtr-core1, remove the ACL from port 1/1/9.

```
interface 1/1/9
 no apply access-list ip no-inet out
 exit
```

```
rtr-core1(config)# interface 1/1/9
rtr-core1(config-if)# no apply access-list ip no-inet out
rtr-core1(config-if)# exit
```

Task 2: Wired Cached Re-Authentication and Critical Role

In this task you will enable cached re-authentication and the critical role on the edge switch.

Both are features that can assist when the RADIUS server is not reachable anymore.

When the RADIUS server is not reachable:

- With cached re-authentication, clients that are already authenticated and that need to perform reauthentication, can be reauthenticated based on the existing connection. The administrator can set the cache period.
- With the critical role, new clients, or existing clients that are outside of the cached re-authentication period, can be allowed access to the network based on a dedicated role, known as the critical role. By default, the network will be *closed* when the RADIUS server is unreachable, with this option, the network can be *open* when the RADIUS server is unreachable. This can be useful, for example, in industrial or medical environments.

Objectives

- Understand switch cached reauthentication.
- Understand switch critical role.
- Verify the operation of cached reauthentication and critical role.

Steps

Cached Re-Authentication

1. Use thee eMGMT PC to open an SSH connection to sw-edge2.
2. Disable Aruba Central support to allow local configuration changes.

```
aruba-central
 disable
 exit
```

```
sw-edge2(config)# aruba-central
sw-edge2(config-aruba-central)# disable
sw-edge2(config-aruba-central)# exit
```

NOTE: While you could make the configuration changes without disabling Aruba Central, you should be aware that the configuration of Aruba Central will overwrite the local configuration when the switch reboots or the Aruba Central connection is reconnected. Since you just blocked and then unblocked Internet access in the previous task, your initial configuration in this task could be lost when the switch restores the connection to Aruba Central.

3. On sw-edge2, configure port 1/1/4 with cached re-authentication.

```
interface 1/1/4
 aaa authentication port-access dot1x authenticator
```

```
  cached-reauth
   cached-reauth-period 120
 aaa authentication port-access mac-auth
  cached-reauth
  cached-reauth-period 120
  exit
 exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# aaa authentication port-access dot1x authenticator
sw-edge2(config-if-dot1x-auth)# cached-reauth
sw-edge2(config-if-dot1x-auth)# cached-reauth-period 120
sw-edge2(config-if-dot1x-auth)#aaa authentication port-access mac-auth
sw-edge2(config-if-macauth)# cached-reauth
sw-edge2(config-if-macauth)# cached-reauth-period 120
sw-edge2(config-if-macauth)# exit
sw-edge2(config-if)#  exit
```

NOTE: The cached re-authentication period starts after the first failed RADIUS authentication. Within the cache period, any number of re-authentications can be performed. Once the cache period expires, the next client re-authentication will fail.

NOTE: In production environments, the cached period can be set much higher, for example, up to 86,400 seconds (24 hours). This provides time to restore the link or RADIUS service while the existing systems will remain connected. The lab uses a short timer to show what happens when the cache expires.

4. For testing purposes, configure the contractor role with a re-authentication period of 60 seconds. First remove the role, this ensures the role does not have any settings from previous lab activities.

```
no port-access role contractor
```

```
port-access role contractor
 vlan access 21
 reauth-period 60
 exit
```

```
sw-edge2(config)# no port-access role contractor
sw-edge2(config)# port-access role contractor
sw-edge2(config-pa-role)# vlan access 21
sw-edge2(config-pa-role)# reauth-period 60
sw-edge2(config-pa-role)# exit
```

NOTE: In production environments, the reauthentication time will depend on your security policy. It will typically be several hours. The lab uses a short timer to speed up the demonstration process.

Critical Role

5. Configure a new role named critical-role-pc. Assign VLAN 21.

```
port-access role critical-role-pc
 vlan access 21
 reauth-period 60
 exit
```

```
sw-edge2(config)# port-access role critical-role-pc
sw-edge2(config-pa-role)#  vlan access 21
sw-edge2(config-pa-role)#  reauth-period 60
sw-edge2(config-pa-role)#  exit
```

NOTE: You can use any name for this role name; this is just a lab example.

6. On port 1/1/4, configured the critical role. Each port can have its own critical role configured.

```
interface 1/1/4
 aaa authentication port-access critical-role critical-role-pc
 exit
```

```
sw-edge2(config)# interface 1/1/4
sw-edge2(config-if)# aaa authentication port-access critical-role critical-role-pc
sw-edge2(config-if)# exit
```

RADIUS Tracking

In case the RADIUS server is unreachable, the cache re-authentication and critical roles will be used to provide continuous or limited services for the clients.

When the RADIUS server is reachable again, the switch will not immediately be aware of this. By using RADIUS tracking, the switch will perform tracking (by sending test authentication requests) to the RADIUS server. This allows the switch to detect that the RADIUS server is reachable again and clients can be re-authenticated.

7. Configured RADIUS tracking to be performed every minute (60 seconds). The tracking must be enabled per RADIUS server. The mode *dead-only* indicates that the tracking will only start when the RADIUS server was found unreachable during a normal authentication event.

```
radius-server tracking interval 60
radius-server tracking user-name radius-track password plaintext Aruba123!
```

```
radius-server host cppm.aruba-training.com tracking enable tracking-mode dead-only
```

NOTE: The configured tracking user does not have to exist on the RADIUS server. Any RADIUS reply (accept or reject) will be considered by the switch as a reachable RADIUS server. If you are concerned about the number of failed authentications in the RADIUS log, you can configure a dedicated RADIUS service to handle the RADIUS tracking requests.

```
sw-edge2(config)# radius-server tracking interval 60
sw-edge2(config)# radius-server tracking user-name radius-track password plaintext
Aruba123!
sw-edge2(config)# radius-server host cppm.aruba-training.com tracking enable
tracking-mode dead-only
```

8. Verify the current RADIUS server status.

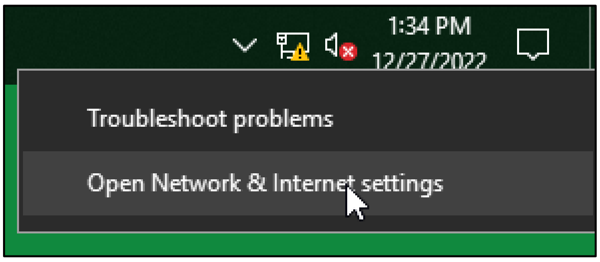
```
show radius-server detail
```

```
sw-edge2(config)# show radius-server detail
******* Global RADIUS Configuration *******

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 60
Tracking Retries: 1
Tracking User-name: radius-track
Tracking Password:
AQBapenDkJR2yAvSlHReiujyK8CvCB8fZZW27nKBejxBznV2CQAAAOmIWOPdfKBWsw==
Number of Servers: 1
AAA Server Status Trap: Disabled

****** RADIUS Server Information ******
Server-Name                : cppm.aruba-training.com
Auth-Port                  : 1812
Accounting-Port            : 1813
VRF                        : default
TLS Enabled                : No
Shared-Secret              :
AQBapTjm3+3uP95qPMMZpf1TiDVJvWcfeLM9kDVHcMSsavmoCQAAAI93dwaxRjUaVw==
Timeout                    : 5
Retries                    : 1
Auth-Type                  : pap
Server-Group               : pa
Group-Priority             : 1
ClearPass-Username         :
ClearPass-Password         : None
Tracking                   : enabled
Tracking-Mode              : dead-only
Reachability-Status        : reachable, Since Wed Dec 28 12:53:57 UTC 2022
```

```
Tracking-Last-Attempted   : Wed Dec 28 12:53:53 UTC 2022
Next-Tracking-Request     : 53 seconds
```

Verify the Operation When the RADIUS Server is Unreachable

9. On PC4, verify the WLAN NIC is disabled and the LAB NIC (wired) is authenticated with 802.1X using the contractor certificate.
10. Open **Network & Internet Settings**.



11. Click **Change Adapter Options**.
12. Right-click the **Lab NIC** and click **Properties**.
13. Click **Authentication**.

> **NOTE:** If the Authentication tab is not visible, make sure the Windows service Wired AutoConfig is running.

14. Set **Network authentication method** to **Microsoft: Smart Card or other certificate**.
15. Click **Settings**.
16. **Uncheck** the option **Verify the server's identity**.

> **NOTE:** In a production environment it is recommended to have this option enabled.

17. Click **OK**.
18. Click **Additional Settings**.
19. Set **Specify authentication mode** to **Computer authentication**.
20. Click **OK** to close the Additional settings.
21. Click **OK** to close the NIC properties, the PC4 will now attempt to authenticate.

Verify the client authentication.

22. On sw-edge2, verify PC4 is authenticated as contractor on port 1/1/4.

```
show port-access clients interface 1/1/4
```

```
sw-edge2(config)# show port-access clients interface 1/1/4

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-----------------------------------------------------------------------------------
-------------------
  Port      MAC-Address        Onboarding     Status      Role
Device Type
                               Method
-----------------------------------------------------------------------------------
-------------------
c 1/1/4     00:50:56:b1:b9:0d dot1x          Success     contractor
c 1/1/4     ec:b1:d7:1b:07:00                In-Progress
```

23. Use MGMT PC to connect to ClearPass using **admin** / **Aruba123!**

```
https://10.254.1.23/tips
```

24. Navigate to **Monitoring > Live Monitoring > Access Tracker**.

25. Check the Access Tracker list. Every minute you should see an authentication event for the PC4 contractor user. This is based on the reauthentication timer that was set in the user role contractor.

NOTE: Just wait a minute watching this screen. The access tracker will auto-refresh every 10 seconds by default.

#	Server Name	Source	NAS IP Address	NAS Port	Host MAC Address	Username	Service	Login Status	Request Timestan	Enforcement Prof
1.	P58-T01-CPPM	RADIUS	10.1.3.5	4	00-50-56-B1-B9-0D	host/contractor	acap - wired - dot1x	ACCEPT	2022/12/28 13:07:04	aruba-role-contractor
2.	P58-T01-CPPM	RADIUS	10.1.3.5	4	00-50-56-B1-B9-0D	host/contractor	acap - wired - dot1x	ACCEPT	2022/12/28 13:06:04	aruba-role-contractor
3.	P58-T01-CPPM	RADIUS	10.1.3.5	4	00-50-56-B1-B9-0D	host/contractor	acap - wired - dot1x	ACCEPT	2022/12/28 13:05:04	aruba-role-contractor
4.	P58-T01-CPPM	RADIUS	10.1.3.5	4	00-50-56-B1-B9-0D	host/contractor	acap - wired - dot1x	ACCEPT	2022/12/28 13:04:03	aruba-role-contractor

26. On sw-edge2, review the port access client details on interface 1/1/4.

```
show port-access clients interface 1/1/4 detail
```

```
...
  Authentication Details
  ----------------------
    Status          : dot1x Authenticated
    Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
    Auth History    : dot1x - Authenticated, 47s ago
                      mac-auth - Attempted, 47s ago
                      dot1x - Authenticated, 108s ago
                      mac-auth - Attempted, 108s ago
                      dot1x - Authenticated, 169s ago
...
```

NOTE: The output may contain 2 MAC addresses. Make sure to look for the host/contractor (PC4) Authentication details section in the output.

- **Question**: What is the current authentication status?
- **Answer**: dot1x authenticated.
- **Question**: What is the interval for the 802.1X events in the Auth History?
- **Answer**: 60 seconds (1 min).

Configure a RADIUS Block ACL on rtr-core1

In the next steps you will activate an ACL on the rtr-core1 that blocks traffic to 10.254.1.23, the IP address of the ClearPass RADIUS server in the lab.

27. Use the MGMT PC to open an SSH connection to rtr-core1.
28. On rtr-core1, create a new ACL that blocks access from the device management subnets to 10.254.1.23. Permit all other traffic.

```
access-list ip no-radius
 10 deny any 10.1.0.0/21 10.254.1.23
 20 permit any any any
 exit
```

```
rtr-core1(config)# access-list ip no-radius
rtr-core1(config-acl-ip)# 10 deny any 10.1.0.0/21 10.254.1.23
rtr-core1(config-acl-ip)# 20 permit any any any
rtr-core1(config-acl-ip)# exit
```

29. Activate the ACL on the port 1/1/9 in the outbound direction.

```
interface 1/1/9
 apply access-list ip no-radius out
 exit
```

```
rtr-core1(config)# interface 1/1/9
rtr-core1(config-if)# apply access-list ip no-radius out
rtr-core1(config-if)# exit
```

Monitor Status on sw-edge2

After a maximum of one minute, PC4 will be re-authenticated. This attempt will fail.

This failed attempt will start the cached reauthentication timer and initiate the RADIUS tracking function.

30. Review the port access interface 1/1/4 authentication details. You can filter on the text **Auth** to get a filtered output.

```
show port-access clients interface 1/1/4 detail | include Auth
```

NOTE: The filtered output may include duplicate lines due to the 2 MAC addresses on the port. You only need to focus on the dot1x lines for the PC4.

These are some states you may observe.

Every 60 seconds, the client will be re-authenticated, during this re-authentication you may see:

```
    Auth Precedence : dot1x - Re-Authenticating, mac-auth - Not attempted
    Auth History    : dot1x - Authenticated, 64s ago
```

When the server cannot be reached, the cached re-authentication timer starts, and the client will be re-authenticated based on the cache:

```
    Auth Precedence : dot1x - Cached-Re-Authenticated, mac-auth - Not attempted
    Auth History    : dot1x - Authenticated, 72s ago
```

Finally, when the cache expires, the status will be:

```
    Status          : Authentication Failed, Server-Timeout
    Auth Precedence : dot1x - Unauthenticated, mac-auth - Not attempted
    Auth History    : dot1x - Unauthenticated, Server-Timeout, 46s ago
                      dot1x - Authenticated, 274s ago
```

NOTE: You may also notice a status of Authentication Failed, Supplicant-Timeout. This is the Windows supplicant that goes into a quiet mode when authentication could not complete for several times. The Windows systems in the lab have been configured with a short quiet timer of 1 minute, therefore this state should disappear after 1 minute.

31. Review the port-access clients again. The PC is now assigned the critical role.

```
show port-access clients interface 1/1/4
```

```
sw-edge2(config)# show port-access clients interface 1/1/4

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-------------------------------------------------------------------------------------
-------------------
  Port     MAC-Address       Onboarding     Status      Role
Device Type
                             Method
-------------------------------------------------------------------------------------
-------------------
c 1/1/4    00:50:56:b1:b9:0d                Success     critical-role-pc, Critical
c 1/1/4    ec:b1:d7:1b:07:00                In-Progress
```

```
...
```

32. Review the RADIUS tracking status

```
show radius-server detail
```

```
sw-edge2(config)# show radius-server detail

...
Tracking                    : enabled
Tracking-Mode               : dead-only
Reachability-Status         : unreachable, Since Wed Dec 28 13:36:20 UTC 2022
Tracking-Last-Attempted     : Wed Dec 28 13:38:35 UTC 2022
Next-Tracking-Request       : 49 seconds
```

Restore the RADIUS Connection

Now you can restore the connection to the RADIUS server.

33. On rtr-core1, remove the ACL from the port 1/1/9.

```
no apply access-list ip no-radius out
```

```
rtr-core1(config-if)# no apply access-list ip no-radius out
```

34. Within about 1- 2 minutes, the RADIUS tracking will detect that the RADIUS server is reachable again. The client will be authenticated against the RADIUS server. Repeat this command every minute until you see PC4 is authenticated as contractor again.

```
show port-access clients interface 1/1/4
```

```
sw-edge2(config)# show port-access clients interface 1/1/4

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-----------------------------------------------------------------------------------
-------------------
  Port      MAC-Address       Onboarding     Status      Role
Device Type
                              Method
-----------------------------------------------------------------------------------
-------------------
c 1/1/4     00:50:56:b1:b9:0d dot1x          Success     contractor
c 1/1/4     ec:b1:d7:1b:07:00                Fail
```

35. Use the MGMT PC to review the latest ClearPass Access Tracker authentication events.

P58-T01-CPPM	RADIUS	10.1.3.5	4	00-50-56-B1-B9-0D	host/contractor	acap - wired - dot1x	ACCEPT	2022/12/28 13:39:41	aruba-role-contractor
P58-T01-CPPM	RADIUS	10.1.3.5	4	EC-B1-D7-1B-07-00	ecb1d71b0700	acap - wired - macauth	REJECT	2022/12/28 13:39:40	[Deny Access Profile]
P58-T01-CPPM	RADIUS	10.1.3.5			radius-track		REJECT	2022/12/28 13:39:35	
P58-T01-CPPM	RADIUS	10.1.3.5	4	00-50-56-B1-B9-0D	host/contractor	acap - wired - dot1x	ACCEPT	2022/12/28 13:34:34	aruba-role-contractor

- **Question**: Why is there a radius-track authentication request?
- **Answer**: This is default username for the RADIUS tracking feature performed by the switch.
- **Question**: You configured the RADIUS track with an interval of 60 seconds. Why is the RADIUS track only shown once in the list?
- **Answer**: You are looking at the RADIUS server logs now. After the ACL blocked access to the RADIUS server, the switch started to track the RADIUS server. These requests were generated every 60 seconds, but they never reached the RADIUS server due to the ACL.

  After the ACL was removed, the next tracking request will mark the RADIUS server as reachable again. Therefore, no more tracking requests need to be sent, since the tracking is configured as dead-only.

You have completed this Lab!

Lab 12.02 Admin Authentication

Overview

In this lab you will configure administrator authentication on the network devices.

In the first task you will configure TACACS on the Aruba gateways; in the second task you will configure the Aruba switches with TACACS authentication.

The ClearPass server has been configured as a TACACS server to support the gateway and switch logins.

Objectives

After completing this lab, you will be able to:

- Configure the Aruba gateways with TACACS authentication.
- Configure the Aruba switches with TACACS authentication.

Task 1: Gateway Admin Authentication

In this task you will configure the gateways to support centralized authentication with a TACACS server. The ClearPass system in the lab environment has been prepared as a TACACS server. You will configure the gateway.

Objectives

- Configure the Aruba gateway with TACACS authentication.
- Verify TACACS authentication.

Steps

Enable Fallback Local

1. In Aruba Central, navigate to Context: **Groups / campus-gw-main** > Navigation: **Devices**> Top: **Gateways** > **Config** (gear icon).
2. Navigate to **System** > **Admin**.
3. Set **Fallback to local authentication** to **enabled**.
4. Click **Save Settings**.

Add TACACS Server

5. Expand **Admin Authentication Servers**.
6. In the lower window (*All Servers*), use the **+** button to add a new server.
7. Configure these settings for the new server:
   - Name: **cppm1-tac**
   - IP address / hostname: **10.254.1.23**
   - Type: **Tacacs**
8. Click **Save Settings** to add the server.
9. In the **All Servers** list, **select** the server **cppm1-tac**. The server options window will appear under the server list.
10. In the Server options, configure these settings:
    - Key: **Aruba123**!
    - Confirm the key
    - Session authorization: **enabled**
11. Click **Save Settings** to update server options.

Add a Server Group

12. In the *Server groups* list, use the **+** button to add a new server group.
13. For the name, enter **admin_auth_svg**.
14. Click **Save Settings**.

15. Select the group **admin_auth_svg**. This will open the **Servers** page for the server group.
16. Use the **+** button to add the existing server **cppm1-tac** to the group **admin_auth_svg**.
17. Click **Save Settings**.

Configure Admin Authentication

18. On the System > Admin page, expand **Admin Authentication Options**.
19. For the default role, select **read-only**.

> **NOTE:** This requires the TACACS or RADIUS server to assign an admin role. Any admin authentication that would not receive an explicit assignment from the TACACS or RADIUS server, will be authorized with read-only privileges.

20. For Server Group, select **admin_auth_svg**.
21. Set the **Enable** checkbox to **check**.
22. Click **Save Settings**.

Verify a TACACS Login

23. Use the MGMT PC to open a new SSH connection to gw1 using username **itadmin** / **Aruba123!**

> **NOTE:** The **itadmin** credentials have been prepared on the lab's ClearPass system.

24. Run the login audit-trail command to review the latest 2 login events.

```
show audit-trail login 2
```

```
(gw1) *# show audit-trail login 2

Dec 28 07:34:16 2022  cli[13075]: USER: admin connected from 10.254.1.90 has logged
out.
Dec 28 09:48:54 2022  cli[17991]: USER: itadmin has logged in from 10.254.1.90.
```

25. Review your current login and privilege level.

```
whoami
```

```
(gw1) *# whoami
user itadmin - role root
```

26. Logout of the gw1 system.

```
exit
```

This concludes the gateway admin authentication.

Task 2: Switch Admin Authentication

In this task you will configure the switches to support centralized authentication with a TACACS server. The ClearPass system in the lab environment has been prepared as the TACACS server. You will configure the switch sw-edge2.

Objectives

- Configure the Aruba switches with TACACS authentication.

Steps

Configure TACACS Authentication

1. Use the MGMT PC to open an SSH connection to sw-edge2.
2. Define a new TACACS server.

```
tacacs-server host 10.254.1.23 key plaintext Aruba123!
```

```
sw-edge2(config)# tacacs-server host 10.254.1.23 key plaintext Aruba123!
```

3. For the lab setup, enable fail-trough. This ensures that you can still connect with the local admin account, even when the TACACS server would reject the login.

```
aaa authentication allow-fail-through
```

```
sw-edge2(config)# aaa authentication allow-fail-through
```

4. Enable SSH TACACS and local auth.

```
aaa authentication login ssh group tacacs local
```

```
sw-edge2(config)# aaa authentication login ssh group tacacs local
```

NOTE: By default, a new TACACS server is added to the default group named tacacs. Therefore you did not have to create a new group or add the server to the group, but you could simply use the group named **tacacs**. If required, custom groups can be created.

Verify Access

5. On the MGMT PC, open an SSH session to sw-edge2 (10.1.3.5) using **itadmin** / **Aruba123!**
6. Verify you can re-authenticate a client

```
port-access reauthenticate interface 1/1/4
```

7. Review the accounting log for entries with itadmin

```
show accounting log last 20 | include itadmin
```

```
sw-edge2# show accounting log last 20 | include itadmin
type=USER_START msg=audit(Dec 28 2022  14:54:57.916:24453) : msg='rec=ACCT_EXEC
op=start session=SSH timezone=UTC user=itadmin priv-lvl=15 auth-method=TACACS auth-
type=pap service=shell isconfig=no hostname=sw-edge2 addr=10.251.1.90 res=success'

type=USYS_CONFIG msg=audit(Dec 28 2022  14:54:57.920:24454) : msg='rec=ACCT_CMD
op=stop session=SSH timezone=UTC user=itadmin priv-lvl=15 auth-method=TACACS auth-
type=pap service=shell isconfig=no data="enable" hostname=sw-edge2 addr=10.251.1.90
res=success'

type=USYS_CONFIG msg=audit(Dec 28 2022  14:55:45.708:24456) : msg='rec=ACCT_CMD
op=stop session=SSH timezone=UTC user=itadmin priv-lvl=15 auth-method=TACACS auth-
type=pap service=shell isconfig=no data="port-access reauthenticate interface 1/1/4"
hostname=sw-edge2 addr=10.251.1.90 res=success'
```

8. Review your current login and privilege level.

```
show user information
```

```
sw-edge2# show user information
Username             : itadmin
Authentication type  : TACACS
User group           : administrators
User privilege level : 15
```

9. Logout from the switch.

```
exit
```

You have completed this Lab!

Lab 13.01 Traffic Optimization

Overview

In the first task of this lab, you will apply some WLAN optimization based on settings that are recommended in the *Aruba Validated Solutions Guide*.

In the next task, you will configure a switch user role with a QoS policy to queue and remark selected traffic.

In the wireless QoS remark task, you will configure a WLAN user role with a QoS policy to remark selected traffic and verify the marking using some test traffic.

In the wireless WMM voice class task, you will first explore how, by default, the traffic with the voice DSCP value of EF is assigned to the WMM video class. After adjusting the WMM classes, the traffic marked with DSCP EF will be handled by the WMM voice queue.

In the last task you will configure the Airmatch schedule and review the configuration deployment in Aruba Central and on the APs.

Objectives

After completing this lab, you will be able to:

- Apply WLAN optimization settings.
- Configure and verify Wired QoS settings.
- Configure Wireless QoS Marking using a user role.
- Configure voice traffic to use the wireless WMM voice queue.
- Configure and verify the Airmatch deployment schedule.

Task 1: WLAN Optimization

In this task you will configure the employee WLAN with some of the recommendations of the Aruba Validated Solution Guide.

Please make sure to refer to the latest VSG (Validated Solution Guide) for latest recommendations:

https://www.arubanetworks.com/techdocs/VSG/

The settings used in this task can be found in the **Campus Deploy** guide.

This task is based on the recommended values at the time of publishing.

Objectives

- Apply recommendations from the Aruba Validated Solutions Guide.

Steps

1. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
2. Edit the WLAN **p#tx-employee**.
3. On the General page, expand the **Advanced Settings**.

Broadcast Filter

4. Expand **Broadcast/Multicast**.
5. Set the broadcast filtering to ARP.

   - **Question**: What is the effect of this setting?

   - **Answer**: This setting is the same as **ALL**, but with ARP enhancements. All broadcasts on the WLAN will be dropped, and ARP packets are converted to unicast when sent to the wireless clients.

Dynamic Multicast Optimization

6. Set Dynamic Multicast Optimization (DMO) to enabled.
7. Set the DMO Client Threshold to 40.

Legacy Transmit Rates

8. Expand **Transmit Rates (Legacy Only)**.
9. Set the 2.4 GHz Minimum value to **5**.

10. Set the 5 GHz Minimum value to **18**.
11. Click **Save Settings**.
12. Click **OK** when the wizard completes.

Task 2: Wired QoS

In this task you will configure wired QoS settings. First you will review the existing QoS trust values.

In the next section of the lab, you will configure a wired user role with a port access policy that will remark selected traffic DSCP value and queue. Using some test traffic, you will be able to verify that the selected traffic is remarked and handled by the correct queue.

Objectives

- Configure a switch user role to remark selected traffic with DSCP.
- Verify the selected traffic has been remarked.

Steps

Configure Global Trust DSCP on All the Switches

1. Use the MGMT PC to open an SSH connection to *all four* switches: sw-agg1 / sw-agg2 / sw-edge1 / sw-edge2.
2. On sw-edge2, review the default QoS trust.

```
show qos trust
```

```
sw-edge2(config)# show qos trust
qos trust none
```

3. On sw-edge2, configure the QoS trust as DSCP.

```
qos trust dscp
```

```
sw-edge2(config)# qos trust dscp
```

4. Verify the updated QoS trust.

```
show qos trust
```

```
sw-edge2(config)# show qos trust
qos trust dscp
```

5. Configure QoS trust DSCP on the *other three* switches: sw-agg1 / sw-agg2 and sw-edge1.

```
qos trust dscp
```

```
sw-agg1(config)# qos trust dscp
```

```
sw-agg2(config)# qos trust dscp
```

```
sw-edge1(config)# qos trust dscp
```

6. On sw-edge2, review the queue statistics for the uplink LAG, lag256. This allows you to see how many packets and bytes were transmitted in each of the eight queues of an interface. In case of a LAG, the member port statistics are aggregated. In this example, the statistics of the ports 1/1/27 and 1/1/28 are aggregated when the LAG256 statistics are displayed.

```
show interface lag256 queues
```

```
sw-edge2(config)# show interface lag256 queues
 Aggregate-name lag256
 Aggregated-interfaces :
 1/1/27  1/1/28
 Speed 20000 Mb/s
                 Tx Bytes      Tx Packets        Tx Drops
 Q0                     0               0               0
 Q1             435338954         1744653               0
 Q2              37139627          325522               0
 Q3                     0               0               0
 Q4                     0               0               0
 Q5                   588               6               0
 Q6               2233713           23562               0
 Q7               2974217           21949               0
```

Configure DSCP Trust in a User Role

There could be guests, contractors, and employees connected to the same switch, if the network administrator doesn't want guest users to take advantage of the global trust settings, the QoS trust can also be set in the user role on the switch.

The role based trust overrides the global trust configuration.

In the next steps you will set the DSCP trust in the dev-ap user role. This ensures that the port that connects to the AP will automatically be configured with trust DSCP, independent of the global trust setting.

7. On sw-edge2, review the current QoS trust on the interface 1/1/2 (connected to AP2).

```
show interface 1/1/2 qos
```

```
sw-edge2(config)# show interface 1/1/2 qos
Interface 1/1/2 is up
 Admin state is up
 qos trust dscp (global)
 qos queue-profile factory-default (global)
 qos schedule-profile factory-default (global)
```

8. On sw-edge2, configure the user role dev-ap with qos trust dscp.

```
port-access role dev-ap
 trust-mode dscp
```

```
 exit
```

```
sw-edge2(config)# port-access role dev-ap
sw-edge2(config-pa-role)# trust-mode dscp
sw-edge2(config-pa-role)# exit
```

9. Review the QoS Trust setting on interface 1/1/2 again.

```
show interface 1/1/2 qos
```

```
sw-edge2(config)# show interface 1/1/2 qos
Interface 1/1/2 is up
 Admin state is up
 qos trust dscp (secure)
 qos queue-profile factory-default (global)
 qos schedule-profile factory-default (global)
```

- **Question**: What is the method for the qos trust setting?
- **Answer**: Secure. It indicates that the setting was applied by port access.

Configure a QoS Policy in a User Role (Wired)

The customer has a voice application that uses UDP port 5060 and they want to ensure this traffic is assigned the DSCP marking EF (Expedited Forwarding, which is DSCP value 46).

In the next steps, you will define a class to select the UDP port 5060 traffic. In a port-access policy, you will assign the class with a DSCP value and a local priority.

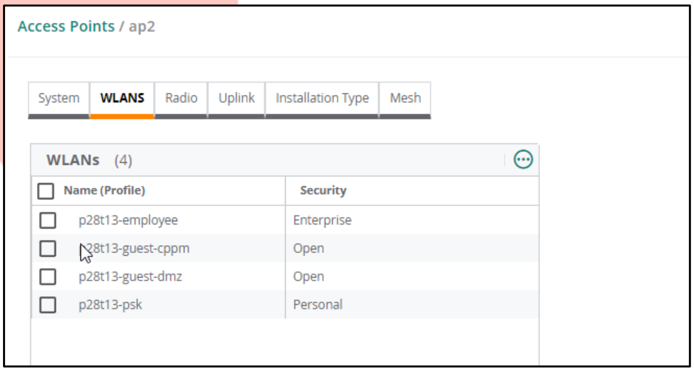
The policy needs to be linked to the user role. You will link it to the contractor user role on sw-edge2.

Test scenario for the traffic flow is as follows:
Wired PC4 > sw-edge2 > sw-agg1/2 > GW > sw-agg1/2 > sw-edge1 > ap1 > wireless PC1.

Disable WLANs on AP2

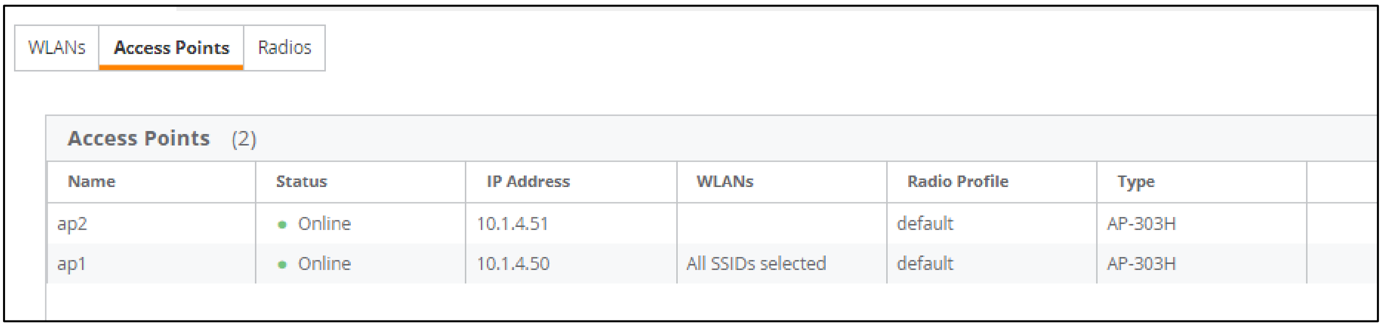
To make sure PC1 connects to AP1, you will disable all WLANs on AP2.

10. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
11. Open the **Access Points** page.
12. Use the pencil to **edit ap2**.
13. Click **WLANs**.
14. **Uncheck** all the WLANs.



15. Click **Save Settings**.

16. In the Access Points list, verify that **ap1** has **all SSIDs selected** in the WLANs column.



Configure the Wired contractor Role on sw-edge2

17. On sw-edge2, make sure the PC4 is active as user contractor on interface 1/1/4.

```
show port-access clients interface 1/1/4
```

```
sw-edge2(config)# show port-access clients interface 1/1/4

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain


  Port     MAC-Address        Onboarding     Status      Role
Device Type
                              Method

c 1/1/4    ec:b1:d7:1b:07:00                 Fail
c 1/1/4    00:50:56:b1:b9:0d  dot1x          Success     contractor
```

18. During the wired port access lab, you created a port access policy for the role *contractor*. This policy was unassigned from the contractor user in the GBP lab, but it should still be in your configuration.

```
show port-access policy contractor
```

```
sw-edge2(config)# show port-access policy contractor

Access Policy Details:


Policy Name   : contractor
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ----------------------------------
10          critical-servers             ipv4 drop
20          any                          ipv4 permit
```

- **Question**: What was the purpose of this policy?
- **Answer**: Contractors were not allowed to access the critical servers (class), they could access all other resources.
- **Question**: Is your QoS policy going to block access for the UDP port 5060?
- **Answer**: No, therefore the action will also be permit (this is the default, implicit action in a policy), as well as a DSCP action. This shows how user roles can also be used for QoS policies, so it is possible that there is no drop action at all in a user role.

19. Configure a new class for UDP port 5060.

```
class ip voice
 match udp any any eq 5060 count
 exit
```

```
sw-edge2(config)# class ip voice
sw-edge2(config-class-ip)# match udp any any eq 5060 count
sw-edge2(config-class-ip)# exit
```

20. Bind the new class to the policy contractor with a DSCP action of EF and Local Priority 5.

NOTE: Do not exit the context in the next step, the upcoming steps will assume you are still in the policy context!

```
port-access policy contractor
 class ip voice action dscp ef action local-priority 5
```

```
sw-edge2(config)# port-access policy contractor
sw-edge2(config-pa-policy)# class ip voice action dscp ef action local-priority 5
```

- **Question**: Why do you set both DSCP and local priority value?

- **Answer**: The DSCP action only marks the packet with the DSCP value but does not assign it locally to a new priority class. This only helps upstream devices in their classification and trust, but not the local system. To ensure that the packets are locally (on this switch) assigned to the current queue, the local priority action is used.

21. Review the current configuration of the current context (the class).

```
show running-config current
```

```
sw-edge2(config-pa-policy)# show running-config current
port-access policy contractor
    10 class ip critical-servers action drop
    20 class ip any
    30 class ip voice action dscp EF action local-priority 5
```

- **Question**: What do you observe?
- **Answer**: The new class rule was added to the end of the list.
- **Question**: Will the QoS rule be used with this configuration?
- **Answer**: No. All traffic will match the previous class any rule. That rule does not include a DSCP marking, therefore no QoS marks will be applied.
- **Question**: Why is there no action for the class ip any rule?
- **Answer**: The action permit is an implicit action in a port access policy. When no action is shown in the configuration, it means the traffic is permitted and no other actions will be applied to the class.

22. Change the order of the class rule and exit the policy.

```
no 30
15 class ip voice action dscp ef action local-priority 5
exit
```

```
sw-edge2(config-pa-policy)# no 30
sw-edge2(config-pa-policy)# 15 class ip voice action dscp ef action local-priority 5
sw-edge2(config-pa-policy)# exit
```

23. Review the port access policy rules.

```
show port-access policy contractor
```

```
sw-edge2(config)# show port-access policy contractor

Access Policy Details:


Policy Name    : contractor
Policy Type    : Local
```

```
Policy Status : Applied

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ----------------------------------
10          critical-servers             ipv4 drop
15          voice                        ipv4 dscp EF local-priority 5
20          any                          ipv4 permit
```

24. Re-sequence the rules in the contractor policy

```
port-access policy contractor resequence 10 10
```

```
sw-edge2(config)# port-access policy contractor resequence 10 10
```

25. Verify the updated sequence numbers.

```
show port-access policy contractor
```

```
sw-edge2(config)# show port-access policy contractor

Access Policy Details:


Policy Name   : contractor
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ----------------------------------
10          critical-servers             ipv4 drop
20          voice                        ipv4 dscp EF local-priority 5
30          any                          ipv4 permit
```

26. Remove the existing contractor role.

```
no port-access role contractor
```

```
sw-edge2(config)# no port-access role contractor
```

27. Configure the contractor role and bind the policy to the user role.

```
port-access role contractor
 vlan 21
 associate policy contractor
 exit
```

```
sw-edge2(config)# port-access role contractor
sw-edge2(config-pa-role)# vlan access 21
sw-edge2(config-pa-role)# associate policy contractor
sw-edge2(config-pa-role)# exit
```

28. Trigger reauthentication on port 1/1/4.

```
port-access reauthenticate interface 1/1/4
```

```
sw-edge2(config)# port-access reauthenticate interface 1/1/4
```

The updated policy will now be applied to the port 1/1/4.

29. Verify that the contractor is successfully authenticated on port 1/1/4.

```
show port-access clients interface 1/1/4
```

```
sw-edge2(config)# show port-access clients interface 1/1/4

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain


  Port      MAC-Address       Onboarding     Status      Role
Device Type
                              Method

c 1/1/4    ec:b1:d7:1b:07:00                 Fail
c 1/1/4    00:50:56:b1:b9:0d dot1x           Success     contractor
```

Verify the QoS Configuration and Markings

30. On sw-edge2, review the port access client details of interface 1/1/4.

```
show port-access clients interface 1/1/4 detail
```

```
sw-edge2(config)# show port-access clients interface 1/1/4 detail

…

Port Access Client Status Details:

Client 00:50:56:b1:b9:0d, host/contractor


…


Access Policy Details:

Policy Name   : contractor
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                         TYPE ACTION
----------- ---------------------------- ---- ----------------------------------
```

```
10          critical-servers             ipv4 drop
20          voice                        ipv4 dscp EF local-priority 5
30          any                          ipv4 permit


Class Details:

class ip critical-servers
    10 match any any 10.1.0.0/255.255.255.0 count
class ip voice
    10 match udp any any eq 5060 count
class ip any
    10 match any any any
```

Generate Test Traffic using UDP Port 5060

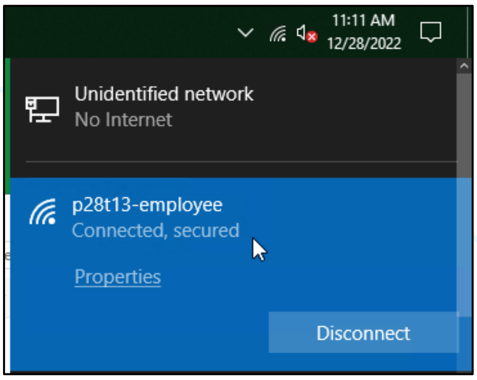
You will now generate test traffic using wired PC4 as the *sender* and wireless PC1 as the *receiver*.

The test traffic will be sent to destination UDP port 5060.

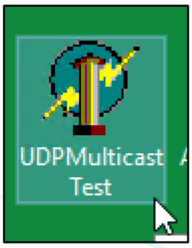
First you will configure the wireless connected PC1 as the receiver; next the wired PC4 will be configured as the sender.

Prepare PC1 as a Receiver

31. On PC1, connect to your p#tx-employee WLAN using the certificate.



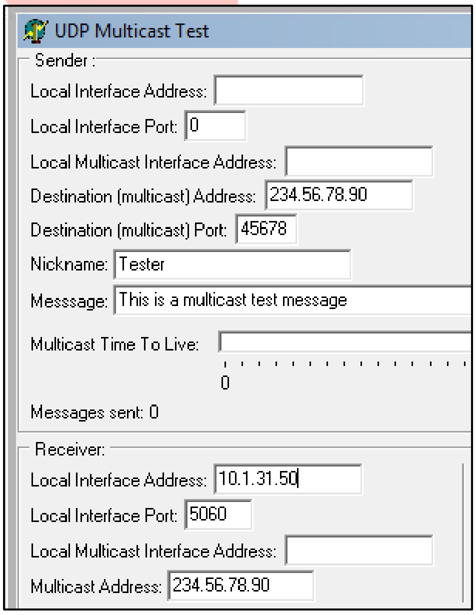
32. On PC1, launch the **UDP Multicast Test** tool on the desktop.



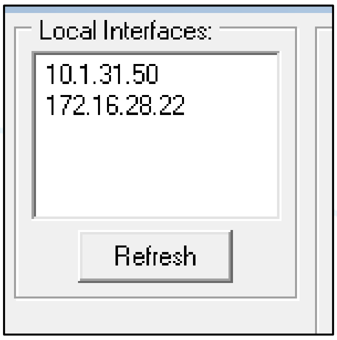
NOTE: Although the tool is named UDP Multicast Test, it can generate *unicast* UDP traffic as well.

There are two sections in the tool: Sender and Receiver.

For PC1 you will configure the *Receiver* (lower) section.



In the top-middle of the Test tool, the Local Interfaces will be listed, this includes the local IP address.

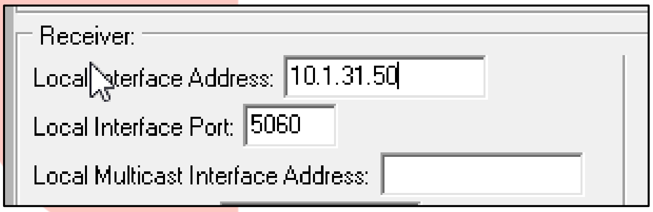


33. Take note of the PC1 IP address.
    - PC1 IP address: **10.1.31.**_______

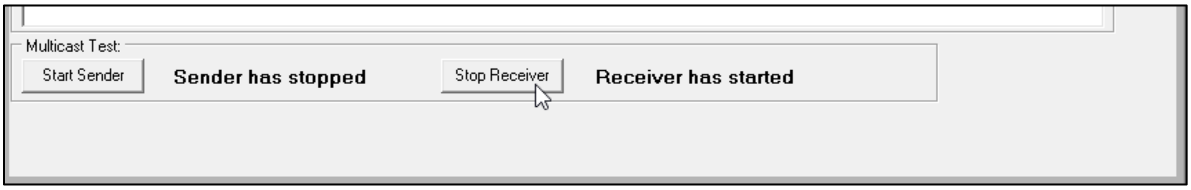
34. In the **Receiver** section, for the **Local Interface Address**, enter the **<u>local</u>** IP of PC1.

    IMPORTANT: Make sure not to use the Local Multicast Interface Address!

35. In the next field, the **Local Interface Port**, enter **5060**.



36. Scroll down to the bottom (the **Start Receiver** button may be hidden by default) and click **Start Receiver**.



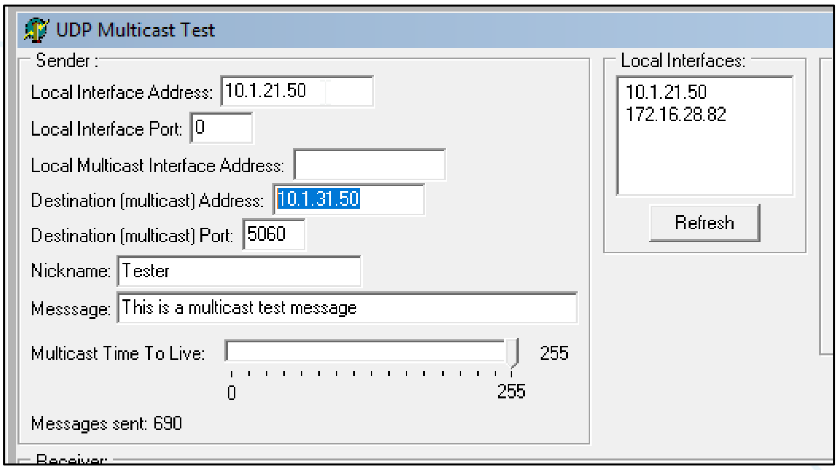
The text next to the button will show **Receiver has started**.

TIP: You can also resize the window to make the buttons visible.

Prepare PC4 as a Sender

37. On PC4, launch the **UDP Multicast Test** tool on the desktop.

This time you will use the **Sender** (Top) section.

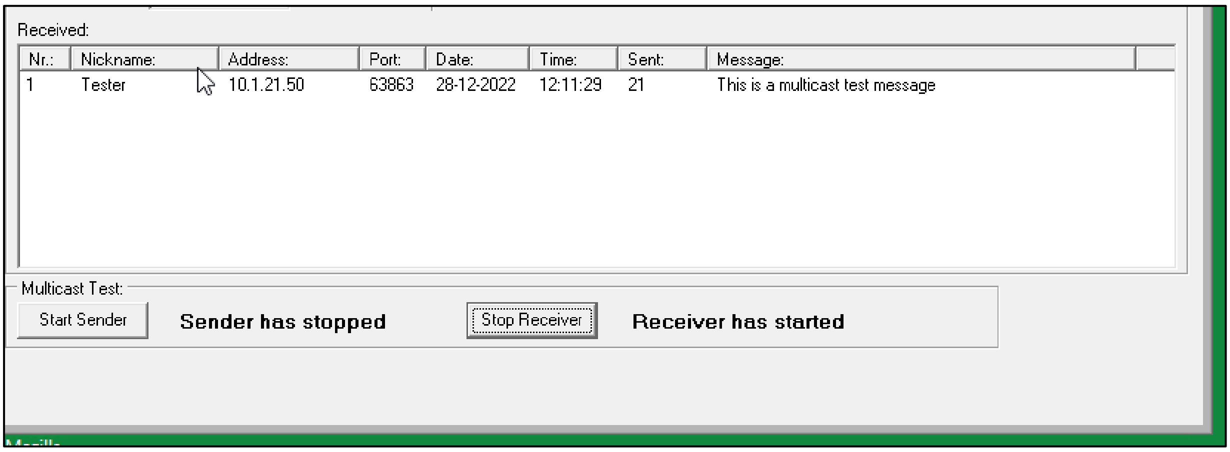


38. For **Local Interface Address**, enter the **local IP of PC4** (use the Local Interfaces window next to it to see the PC4 local 10.1.21.x IP address)
39. In *Destination (multicast) address*, enter the PC1 IP address (10.1.31.x).
40. In Destination (multicast) port, enter 5060.
41. Scroll down to the bottom (the **Start Sender** button may be hidden by default) and click **Start Sender**. You can also resize the window to make the buttons visible.

The text next to the button will show **Sender has started**.

The Sender will now send one UDP packet every second to the configured destination address.

42. On PC1, verify that the UDP packets are received from 10.1.21.x: the Sent column value will increase every second.



Verify the Remarked Traffic Handling

Now that test traffic is sent from the wired PC4 to the wireless PC1, you can review the queue statistics on the path.

Review the sw-edge2 queue statistics. The queue statistics should confirm that the traffic is processed by the correct queue (Q5).

43. On sw-edge2, clear the interface statistics for uplink interface lag256.

```
clear interface lag256 statistics
```

```
sw-edge2(config)# clear interface lag256 statistics
```

NOTE: It may be required to run the clear statistics command a second time to clear the statistics.

44. Review the queue statistics of the uplink lag 256.

```
show interface lag256 queue
```

```
sw-edge2(config)# show interface lag256 queues
 Aggregate-name lag256
```

```
 Aggregated-interfaces :
 1/1/27  1/1/28
 Speed 20000 Mb/s
                 Tx Bytes      Tx Packets        Tx Drops
 Q0                     0               0               0
 Q1                480166            1810               0
 Q2                  4788              44               0
 Q3                     0               0               0
 Q4                     0               0               0
 Q5                  2562              21               0
 Q6                  6078              27               0
 Q7                   542               4               0
```

45. After about 5 seconds, review the statistics again.

```
sw-edge2(config)# show interface lag256 queues
 Aggregate-name lag256
 Aggregated-interfaces :
 1/1/27  1/1/28
 Speed 20000 Mb/s
                 Tx Bytes      Tx Packets        Tx Drops
 Q0                     0               0               0
 Q1                652413            2459               0
 Q2                  6384              58               0
 Q3                     0               0               0
 Q4                     0               0               0
 Q5                  3510              29               0
 Q6                  9080              39               0
 Q7                   542               4               0
```

- **Question**: What do you observe for the traffic in Q5?
- **Answer**: Q5 should have an increase in the Tx Packets since you have assigned the traffic to local-priority 5.
- **Question**: Is traffic for local priority 5 always assigned to Queue 5?
- **Answer**: No, this is the default configuration. You can change the LP to Queue mapping table if that would be required. You will review this mapping in the next steps.

46. Review the LP to queue assignment profiles.

```
show qos queue-profile
```

```
sw-edge2(config)# show qos queue-profile
profile_status profile_name
-------------- ------------
applied        factory-default
```

47. Review the queue-profile named factory-default.

```
show qos queue-profile factory-default
```

```
sw-edge2(config)# show qos queue-profile factory-default
queue_num local_priorities name
--------- ---------------- ----
0         0                Scavenger_and_backup_data
24        1
2         2
3         3
4         4
5         5
6         6
7         7
```

Verify Tunneled DSCP Markings

Scenario:
Wired PC4 > sw-edge2 > sw-agg1/2 > GW > sw-agg1/2 > sw-edge1 > ap1 > wireless PC1.

The traffic from the wired PC4 will be sent through the GW to the wireless PC1. The GW encapsulates the traffic in a GRE tunnel and forwards the GRE packet to the AP.

During this process, any DSCP marking in the IP packet is automatically propagated to the outer IP header of the GRE IP packet. This means the IP GRE packet DSCP value will also have the EF marking.

This GRE traffic will enter sw-edge1 via the uplink port lag256. Based on the global DSCP trust, the packet will be assigned to local priority 5 and queue 5.

First you will review the global DSCP to local priority mapping table.

48. On sw-edge1, review the DSCP to LP mapping table.

```
show qos dscp-map
```

```
sw-edge1(config)# show qos dscp-map
DSCP     code_point local_priority cos color   name
-------- ---------- -------------- --- ------- ----
000000   0          1                  green   CS0
…
001000   8          0                  green   CS1
001001   9          0                  green
001010   10         0                  green   AF11
001011   11         0                  green
001100   12         0                  yellow  AF12
001101   13         0                  green
001110   14         0                  yellow  AF13
001111   15         0                  green
010000   16         2                  green   CS2
010001   17         2                  green
010010   18         2                  green   AF21
010011   19         2                  green
010100   20         2                  yellow  AF22
010101   21         2                  green
010110   22         2                  yellow  AF23
```

```
010111   23        2                  green
011000   24        3                  green   CS3
011001   25        3                  green
011010   26        3                  green   AF31
011011   27        3                  green
011100   28        3                  yellow  AF32
011101   29        3                  green
011110   30        3                  yellow  AF33
011111   31        3                  green
100000   32        4                  green   CS4
100001   33        4                  green
100010   34        4                  green   AF41
100011   35        4                  green
100100   36        4                  yellow  AF42
100101   37        4                  green
100110   38        4                  yellow  AF43
100111   39        4                  green
101000   40        5                  green   CS5
…
101110   46        5                  green   EF
101111   47        5                  green
110000   48        6                  green   CS6
…
111000   56        7                  green   CS7
…
```

- **Question**: To what local priority is the DSCP value EF (46) mapped?
- **Answer**: Based on the default table, DSCP value EF (46) is mapped to LP 5. This LP 5 is by default mapped to Q5.

The GRE encapsulated traffic will leave the sw-edge1 to AP1 via port 1/1/2.

49. On sw-edge1, clear and review the queue statistics of the port to the AP1.

```
clear interface 1/1/2 statistics
show interface 1/1/2 queues
```

```
sw-edge1(config)# clear interface 1/1/2 statistics
sw-edge1(config)# show interface 1/1/2 queues
Interface 1/1/2 is up
 Admin state is up
                 Tx Bytes      Tx Packets         Tx Drops
 Q0                     0               0                0
 Q1                 46854             154                0
 Q2                     0               0                0
 Q3                     0               0                0
 Q4                     0               0                0
 Q5                  3528              21                0
 Q6                  5018              21                0
 Q7                  1499              12                0
```

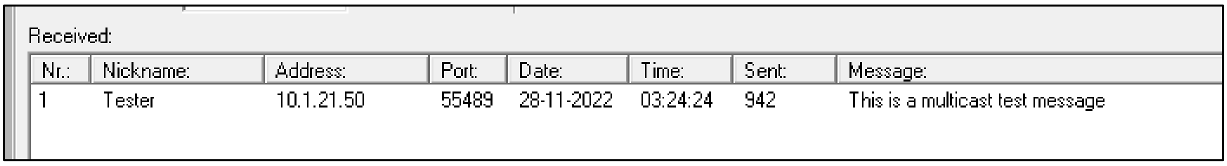
- **Question**: What do you observe?

- **Answer**: The GRE packets that were sent by the GW to the AP also have the DSCP mark. This can be noticed by the traffic statistics of Q5.

Review the Received Traffic on PC1

The last step in the process verifies the traffic on the receiving PC1.

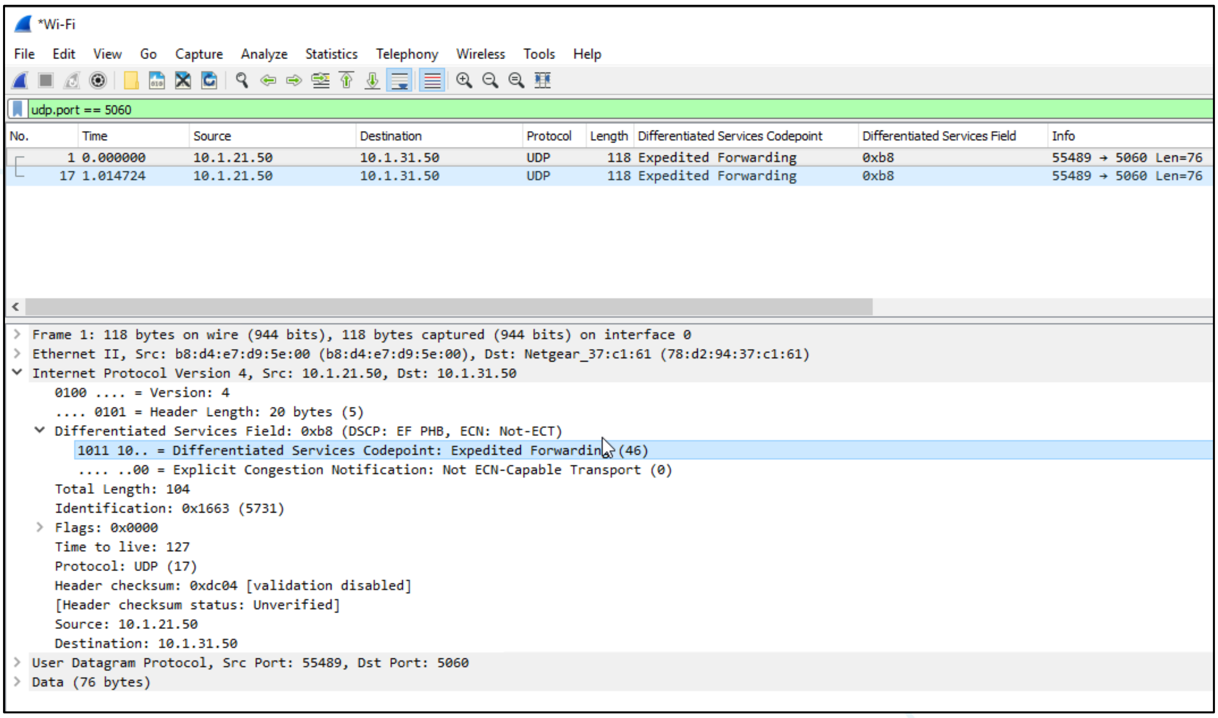
50. On PC1, verify in the UDP Multicast Test – Received window that the traffic is arriving. The counter of the Sent messages will increase every second.


Received:

Nr.:	Nickname:	Address:	Port:	Date:	Time:	Sent:	Message:
1	Tester	10.1.21.50	55489	28-11-2022	03:24:24	942	This is a multicast test message

You will now start Wireshark to verify the DSCP markings for these packets.

51. On PC1, open Wireshark, start a trace on the Wifi NIC.
52. Stop the trace after a few seconds.
53. You may enter **udp.port == 5060** in the display filter to make the packet list easier to read.



54. Select the UDP port 5060 packet and expand the IP section.

- **Question**: What is the Differentiated Services Code Point value?

- **Answer**: 101110 > Expedited Forwarding (EF) – 46. This was set by the sw-edge2 by the contractor port-access policy configuration.

Wired Voice VLAN Configuration

VOIP Phones can dynamically learn the Voice VLAN from their connected switch port using LLDP MED.

The switch must be configured with the correct voice VLAN ID that needs to be advertised to the phones using LLDP MED.

There is no real phone in the remote lab environment; instead, the commands in the next section are for practice only.

55. On sw-edge2, configure VLAN 24 as a voice VLAN for LLDP MED.

```
vlan 24
 voice
 exit
```

```
sw-edge2(config)# vlan 24
sw-edge2(config-vlan-24)#  voice
sw-edge2(config-vlan-24)#  exit
```

56. Review the voice VLAN list.

```
show vlan voice
```

```
sw-edge2(config)# show vlan voice


VLAN  Name                                    Status  Reason                   Type
Interfaces

24    VLAN24                                  up      ok                       static
lag256
```

This VLAN will be advertised to an LLDP MED-capable client on any port that has VLAN 24 in the allow list. This VLAN membership can be statically configured using a trunk port or through a port access authenticated user role configuration with a tagged VLAN.

Task 3: Wireless QoS Marking

The customer has informed you that the voice application is also used on certain wireless clients. The customer informs you that the application is not adding a DSCP marking to the traffic. They want to ensure this traffic is assigned the DSCP marking of EF.

In the next steps, you will configure the wireless solution to assign DSCP 46 for the traffic associated with UDP port 5060.

The rule will be linked to the employee wireless user role.

Test scenario traffic flow will use the opposite direction of the previous task:
Wireless PC1 > AP1 > sw-edge1 > sw-agg1/2 > GW > sw-agg1/2 > sw-edge2 > Wired PC4

Objectives

- Configure wireless QoS marking using a user role.
- Verify QoS marked wireless traffic.

Steps

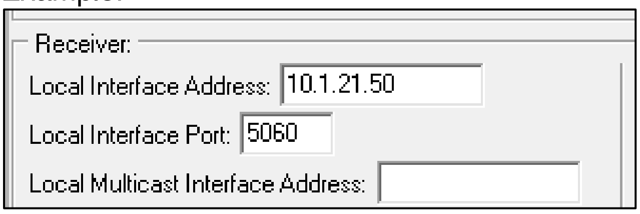
Wireless-to-Wired Markings

In the next steps you will have wireless PC1 sent traffic to the wired PC4. You will set up the test before the QoS configuration in order to review the default operation first.

Reconfigure the UDP Multicast test direction and configure PC4 as the Receiver.

1. On PC4, in the UDP Multicast test tool, **stop the Sender**.
2. On PC4, configure the **Receiver** options:
   - Local Interface Address: enter the **local PC4 IP Address** (10.1.21.xyz) and take note of the IP.
   - Local Interface port: **5060**

Example:



3. At the bottom, click **Start Receiver**.

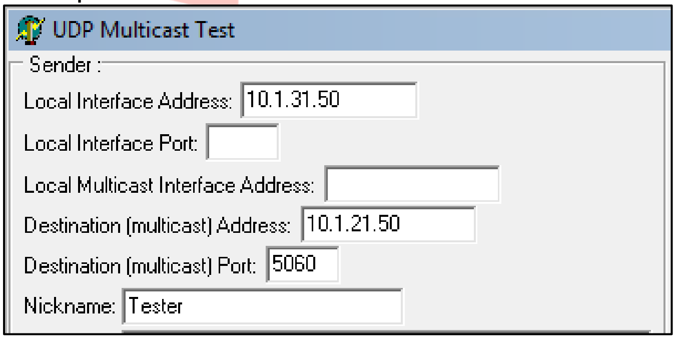
Now configure PC1 as the Sender.

4. On PC1, configure the **Sender** options:

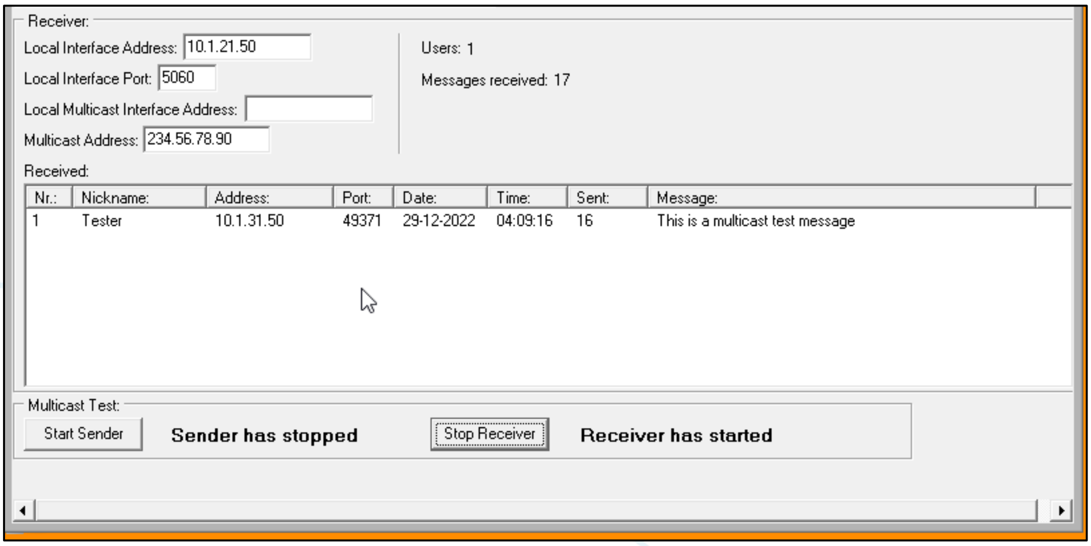
NOTE: You may leave the Receiver running.

- Local Interface Address — **enter the local PC1 IP Address** (10.1.31.xyz)
- Destination (multicast) address — **enter the PC4 IP Address** (10.1.21.xyz)
- Destination (multicast) port — **5060**

Example:

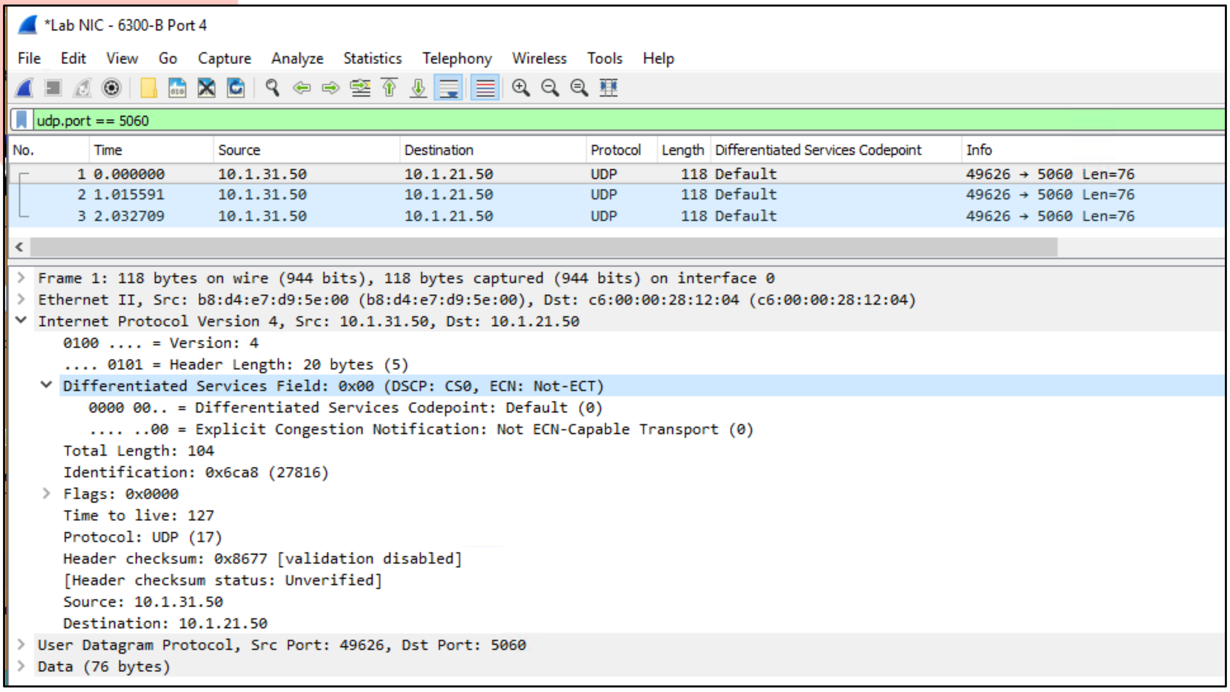


5. At the bottom, click **Start Sender**.
6. On PC4, verify the test packets are received every second.



Review Unmarked Traffic

7. On PC4, start a Wireshark trace on the Lab NIC.
8. Stop the trace after a few seconds.
9. Apply a display filter **udp.port == 5060**.
10. Open the IP header of a packet and verify that the current DSCP value is CS0 (no marking).



This shows the default, unmarked traffic.

11. On PC1, click **Stop the Sender**.

IMPORTANT: In the next steps you will update the user role firewall rules. The AP firewall will process the updated rules for new sessions. If you leave the UDP test tool active, the marking of the DSCP will not be effective since it is an existing session. By stopping the Sender, the UDP session will age out within the next minute.

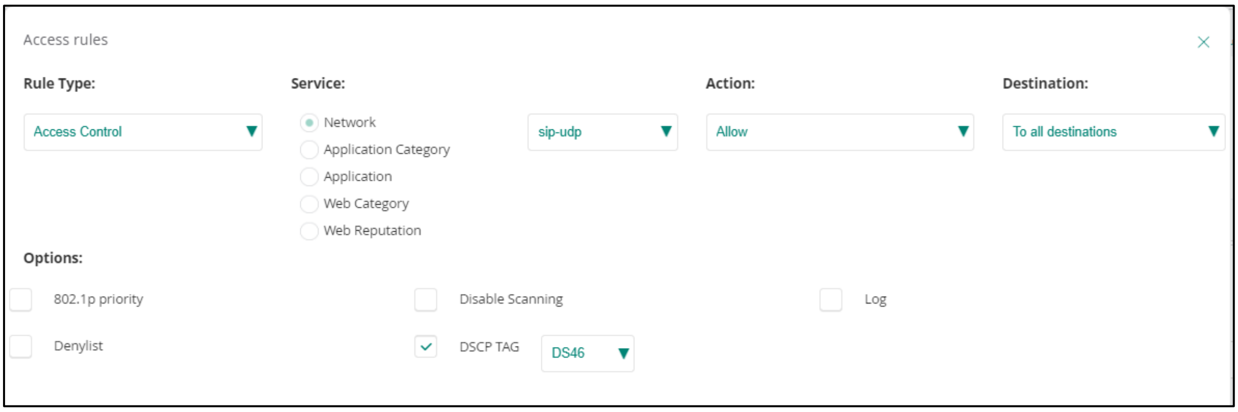
User Role-Based Markings

In the next steps, you will configure the WLAN to mark traffic for UDP port 5060 with DSCP value 46.

This will be applied in the user role employee.

By using the WLAN wizard, the user role will be updated on *both* the AP and the GW. This ensures that the AP will already mark the traffic, as well as the GRE encapsulated packet to the GW, with the DSCP value 46.

12. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
13. On the WLAN page, **edit** the p#tx-employee WLAN.
14. On the **Access** page, move the slider to **Role Based** to see the roles.
15. Select the role **employee**.
16. Use the **+** button to add a new rule
    - Type: **Access Control**
    - Service: **Network** **sip-udp**
    - Action: **Allow**
    - Destination: **To All Destinations**
    - DSCP Tag: **DS46**



17. Click **OK** to add the rule.
18. Verify that the rule is listed at the top of the list.
19. Click **Save Settings**.
20. Click **OK** when the wizard completes.

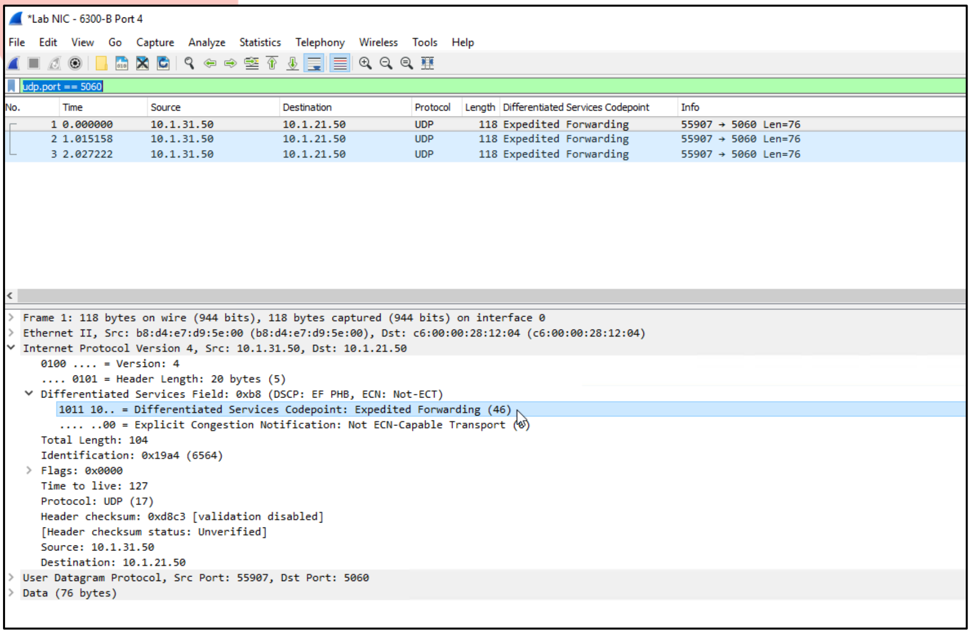
Since this is a tunnel WLAN, the WLAN wizard will push the role configuration to both the AP and GW.

On PC4 Verify Marked Traffic

21. On PC1, click the **Start the Sender** button again. Verify that the message states **Sender has started**.

22. On PC4, start a Wireshark trace on the Lab NIC.
23. Stop the trace after a few seconds.

24. Apply display filter **udp.port == 5060**.
25. Select a UDP packet and expand the IP header to review the DSCP value.



- **Question**: What is the DSCP value in the UDP packet?
- **Answer**: The AP has remarked the UDP port 5060 traffic with DSCP value 46 (EF).

Verify the Wired Network uses the Qos Markings

The AP will apply the DSCP mark on the GRE tunneled traffic. You verify this on the sw-edge1 uplink port lag 256.

26. On sw-edge1, clear the interface lag256 statistics and review the statistics for Q5. Repeat after about 5 seconds to see the delta.

```
clear interface lag256 statistics
show interface lag 256 queues
```

```
sw-edge1(config)# clear interface lag256 statistics
```

```
sw-edge1(config)# show interface lag 256 queues
 Aggregate-name lag256
 Aggregated-interfaces :
 1/1/27  1/1/28
 Speed 20000 Mb/s
                Tx Bytes      Tx Packets        Tx Drops
 Q0                21949             125               0
 Q1                 5441              32               0
 Q2                 2736              24               0
 Q3                    0               0               0
 Q4                    0               0               0
```

```
Q5                  1804          11            0
Q6                  4068          16            0
Q7                   286           2            0
```

```
sw-edge1(config)# show interface lag 256 queues
 Aggregate-name lag256
 Aggregated-interfaces :
 1/1/27  1/1/28
 Speed 20000 Mb/s
                 Tx Bytes      Tx Packets         Tx Drops
 Q0                 32264             183                0
 Q1                  8063              47                0
 Q2                  4104              36                0
 Q3                     0               0                0
 Q4                     0               0                0
 Q5                  2788              17                0
 Q6                  6097              27                0
 Q7                   286               2                0
```

27. On PC1, click **Stop Sender**.

NOTE: Do not close the UDP Multicast Tool; you'll use it in the next task.

This concludes the marking of traffic from a wireless client.

Task 4: Wireless WMM Voice Class

In the previous tasks you have seen how client traffic can be assigned with the correct DSCP marking. This DSCP mark was then used by the wired network to assign the traffic to the correct queue.

In this task you will review the wireless transmission between the AP and the Wireless client.

First, you will review the traffic from the AP to the wireless client PC1. Next you will review the traffic from the wireless client PC1 to the AP.

Objectives

- Understand the issue for voice marked traffic with the default WMM classes.
- Configure WMM voice class with DSCP value EF.
- Verify traffic in the WMM queues.

Steps

Traffic from AP to Wireless Client PC1

When an AP receives traffic from the wired network with a DSCP mark, it will automatically map this to a WMM class and transmit it based on that class.

You will now review the result of the default DSCP to WMM mapping.

1. On PC4, click **Start Sender**.
2. On PC1, verify the test packets are arriving in the UDP Multicast Test tool.
3. Use the lab dashboard to open a console connection to AP1.
4. Review the AP radio statistics, filtering on the *WMM* output. Repeat the command after about 5 seconds.

```
show ap debug radio-stats | include WMM
```

```
ap1# show ap debug radio-stats | include WMM
Tx WMM [BE]                     1213
Tx WMM [VI]                     17
Tx Auto WMM Boost Pkts          0
Rx WMM [BE]                     1632
Rx WMM [VO]                     6
```

```
ap1# show ap debug radio-stats | include WMM
Tx WMM [BE]                     1213
Tx WMM [VI]                     26
Tx Auto WMM Boost Pkts          0
Rx WMM [BE]                     1643
Rx WMM [VO]                     6
```

NOTE: Only WMM classes that have processed packets are shown in the list. Therefore, you may not see all four queues (BK, BE, VI, and VO) or both directions (Tx Transmit and Rx Receive).

NOTE: The example output was collected after an AP reboot; therefore, the counters were low.

- **Question**: What Transmit (Tx) WMM queues do you see?
- **Answer**: Depending on your setup, you may see BE (Best Effort), VI (Video) and VO (Voice).
- **Question**: Do you see the VO queue increase with 1 every second?
- **Answer**: No, the VI queue is increasing.
- **Question**: Why is the VI queue increasing for your traffic with DSCP mark 46?
- **Answer**: The Aruba AP default DSCP to WMM mapping is listed in this table:

DSCP Value	WMM Access Category
8	Background
16	
0	Best effort
24	
32	Video
40	
48	Voice
56	

The table represents the starting value for a range of 8. For example, 0, in the best effort access category, represents the DSCP values 0-7.

This means that the value 46 is in the range 40-47 and this range is assigned to the Video class.

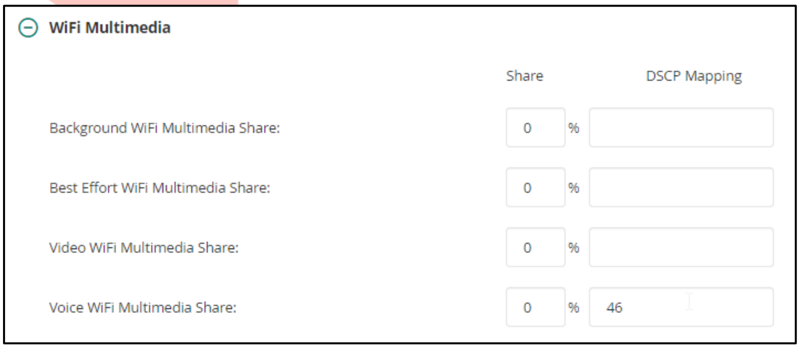
Adjust the WLAN WMM Voice Class DSCP Mapping

In the next steps, you will adjust the AP configuration to assign the DSCP value 46 to the WMM Voice class.

When the AP receives a packet from the wired network with the DSCP value 46, it will transmit this packet using the voice WMM queue instead of the default video WMM queue.

5. In Aruba Central, navigate to Context: **Groups / campus-wifi-ui** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).

6. On the WLANs page, **edit** the WLAN p#tx-employee.
7. On the General page, expand **Advanced Settings**.
8. Expand **Wifi Multimedia**.
9. In the **Voice Wifi Multimedia** share text box, enter the DSCP mapping value of **46**.



10. Click **Save Settings**.
11. Click **OK** when the wizard completes.

Verify the WMM Queue Statistics on AP1

12. On the AP1 console, review the WMM statistics of the radio, repeat after about 5 seconds to confirm the voice queue statistics increase.

```
show ap debug radio-stats | include WMM
```

```
ap1# show ap debug radio-stats | include WMM
Tx WMM [BE]                      9252
Tx WMM [VI]                      7207
Tx WMM [VO]                      6
Tx Auto WMM Boost Pkts           0
Rx WMM [BE]                      11686
Rx WMM [VO]                      6
```

```
ap1# show ap debug radio-stats | include WMM
Tx WMM [BE]                      9252
Tx WMM [VI]                      7207
Tx WMM [VO]                      10
Tx Auto WMM Boost Pkts           0
Rx WMM [BE]                      11686
Rx WMM [VO]                      6
```

- **Question**: As the voice queue now processing traffic?
- **Answer**: Yes, the traffic marked with DSCP 46 is now processed by the voice queue.

You have now completed the AP to Wireless client section. In the next section you will review the traffic from the Wireless client to the AP.

Traffic from the Wireless Client PC1 to the AP

The wireless PC1 is not applying any WMM markings by default: all traffic is sent as best effort (BE).

First you will review the AP Received WMM statistics.

You want to investigate traffic from the wireless PC1 to wired PC4, therefore you need to adjust the test traffic direction.

13. On PC4, **stop** the Sender. The receiver should still be running.
14. On PC1, **start** the Sender.
15. On AP1, review the received AP radio statistics WMM classes. Repeat the command after about 5 seconds to see the delta in Rx packets.

```
show ap debug radio-stats | include WMM
```

```
ap1# show ap debug radio-stats | include WMM
Tx WMM [BE]                       11266
Tx WMM [VI]                       7207
Tx WMM [VO]                       1016
Tx Auto WMM Boost Pkts            0
Rx WMM [BE]                       14252
Rx WMM [VO]                       6
```

```
ap1# show ap debug radio-stats | include WMM
Tx WMM [BE]                       11525
Tx WMM [VI]                       7207
Tx WMM [VO]                       1016
Tx Auto WMM Boost Pkts            0
Rx WMM [BE]                       14598
Rx WMM [VO]                       6
```

- **Question**: What do you observe?

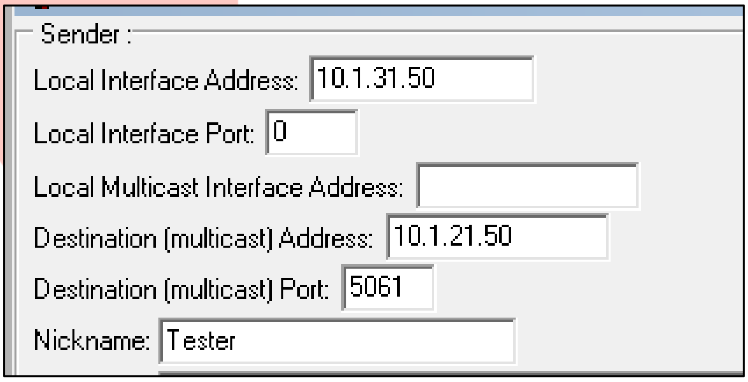
- **Answer**: The client traffic is received by the AP as best effort (BE). In a wireless deployment it is important that the endpoints are properly configured to transmit their flows with the correct WMM class.

Adjust the Wireless Client WMM Configuration

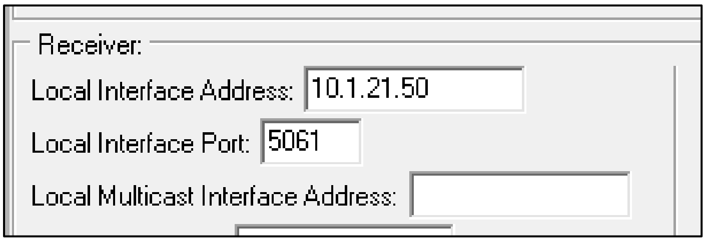
In this section you will configure the wireless PC1 to send traffic using the WMM voice queue. You will use a different UDP port to see the impact of the WMM marking on the traffic.

Adjust UDP Multicast Test tool

16. Reconfigure PC1 as Sender with **Destination Port <u>5061</u>**. Note that you are using port **<u>5061</u>**, ***not*** port 5060 as in the previous tests. **Stop** and **Start** the Sender.



17. Reconfigure PC4 as a Receiver with **Local Interface Port <u>5061</u>**. **Stop** and **Start** the Receiver.



18. Verify on PC4 that test packets are received every second.

Configure PC1 to transmit UDP port 5061 as WMM VO

19. On PC1's desktop, from the IACA student files folder, run the following command:

```
lab13-pc1-udp 5061 wmm voice - enable.cmd
```

20. This will run the following PowerShell code as administrator:

```
New-NetQosPolicy -Name "port5061" -IPDstPortMatchCondition 5061 -
PriorityValue8021Action 6
```

NOTE:
If you want to remove the policy again, you can run

```
lab13-pc1-udp 5061 wmm voice - disable.cmd
```

or you can use the PowerShell command

```
Remove-NetQosPolicy -name "port5061"
```

In this lab, you don't have to remove the policy!

Verify the WMM Radio Statistics on AP1

21. On the console of AP1, review the radio WMM statistics. Focus on the RX queues. Repeat the command after about 5 seconds.

```
show ap debug radio-stats | include WMM
```

```
ap1# show ap debug radio-stats | include WMM
Tx WMM [BE]                       12503
Tx WMM [VI]                       7207
Tx WMM [VO]                       1016
Tx Auto WMM Boost Pkts            0
Rx WMM [BE]                       16296
Rx WMM [VO]                       544
```

```
ap1# show ap debug radio-stats | include WMM
Tx WMM [BE]                       12504
Tx WMM [VI]                       7207
Tx WMM [VO]                       1016
Tx Auto WMM Boost Pkts            0
Rx WMM [BE]                       16296
Rx WMM [VO]                       551
```

This shows that the AP is now receiving WMM VO marked traffic on the radio.

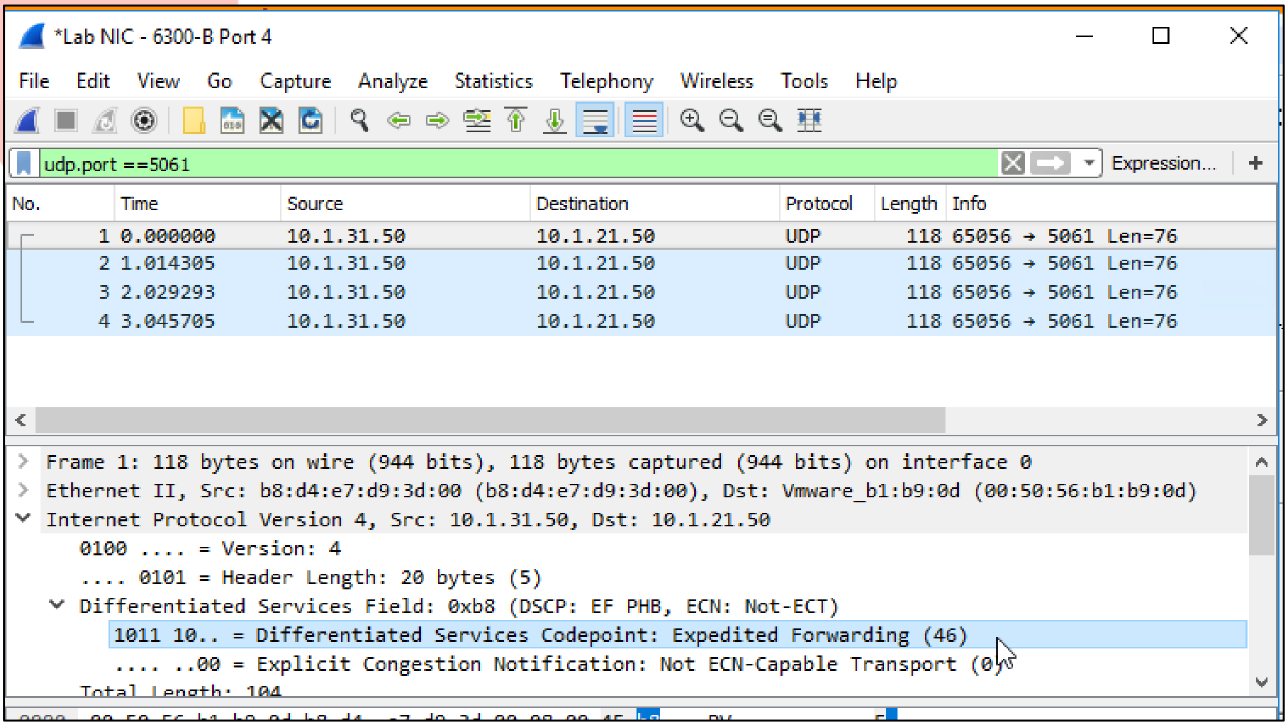
AP WMM Voice DSCP Remark

Since you have applied a DSCP value on the VO Class, the AP will remark the DSCP value.

This means that applying a DSCP value to a WMM class will not only apply to traffic that is transmitted by the AP, but also to wireless traffic *received* by the AP.

Any traffic received with the WMM class will be remarked by the AP to the first DSCP value in the list.

22. On PC4, start the Wireshark trace.
23. After a few seconds, stop the trace again.
24. Set the display filter to **udp.port == 5061**.
25. Analyze the received UDP port 5061 packets DSCP value.



- **Question**: What do you observe?
- **Answer**: The DSCP value has been set to EF by the AP. This was not based on the user role QoS rule, but based on the WMM class Voice received by the AP.

26. On both PC1 and PC4, close the UDP Multicast test tool and Wireshark.

This concludes the WMM task.

Optional Task 5: Airmatch Configuration

In this task you will review the Airmatch schedule configuration and review the channel and radio changes that were applied on the APs.

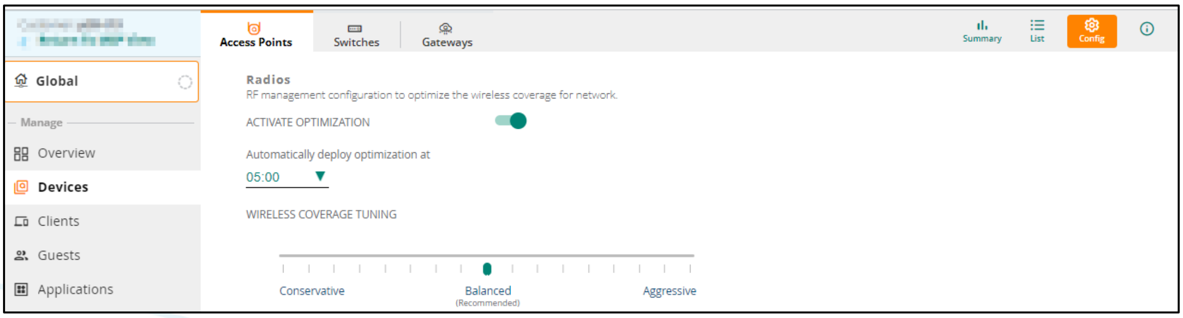
Objectives

- Configure the Airmatch schedule.
- Review the Airmatch deployment history for the radios.
- Review the deployment history on the AP.

Steps

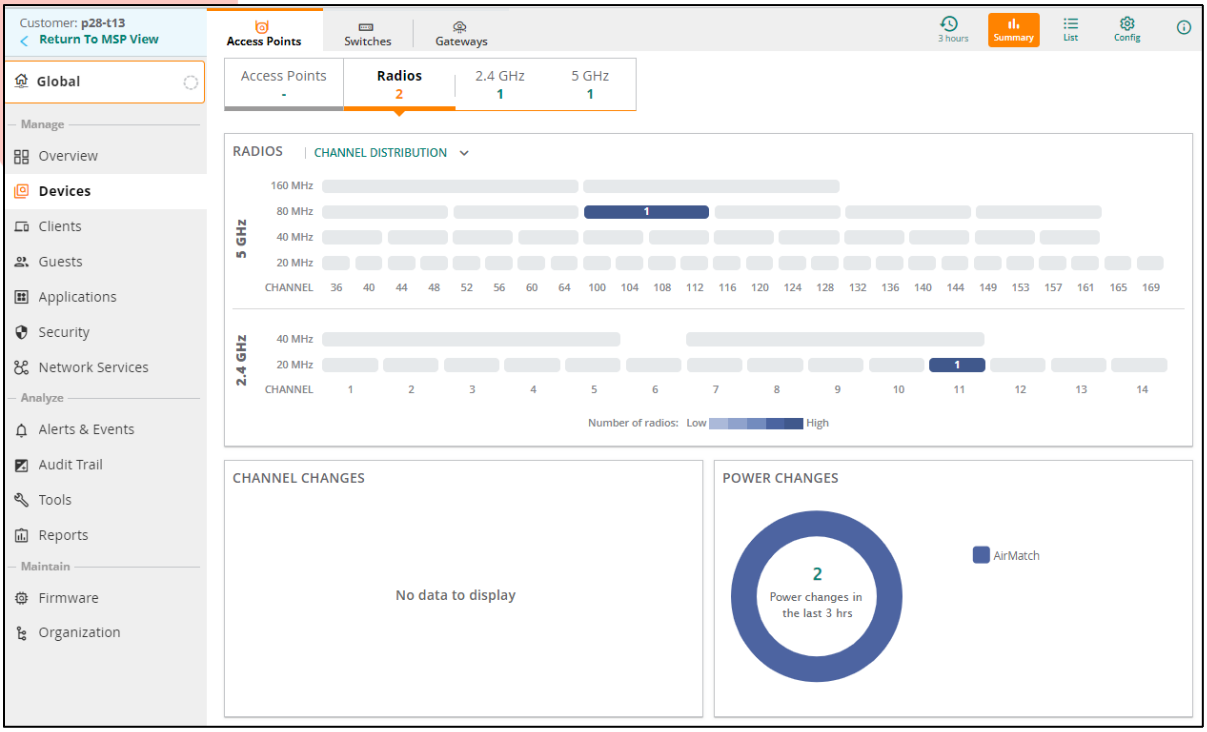
Airmatch Schedule Configuration

1. In Aruba Central, navigate to Context: **Global** > Navigation: **Devices**> Top: **Access Points** > **Config** (gear icon).
2. This allows you to configure the deployment time for the Airmatch scenario.

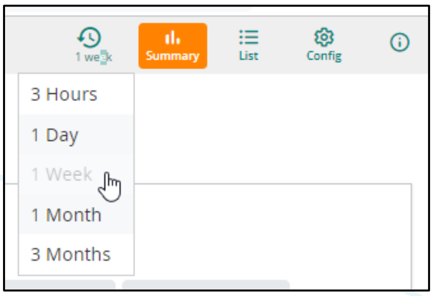


Review Airmatch Deployment on the AP

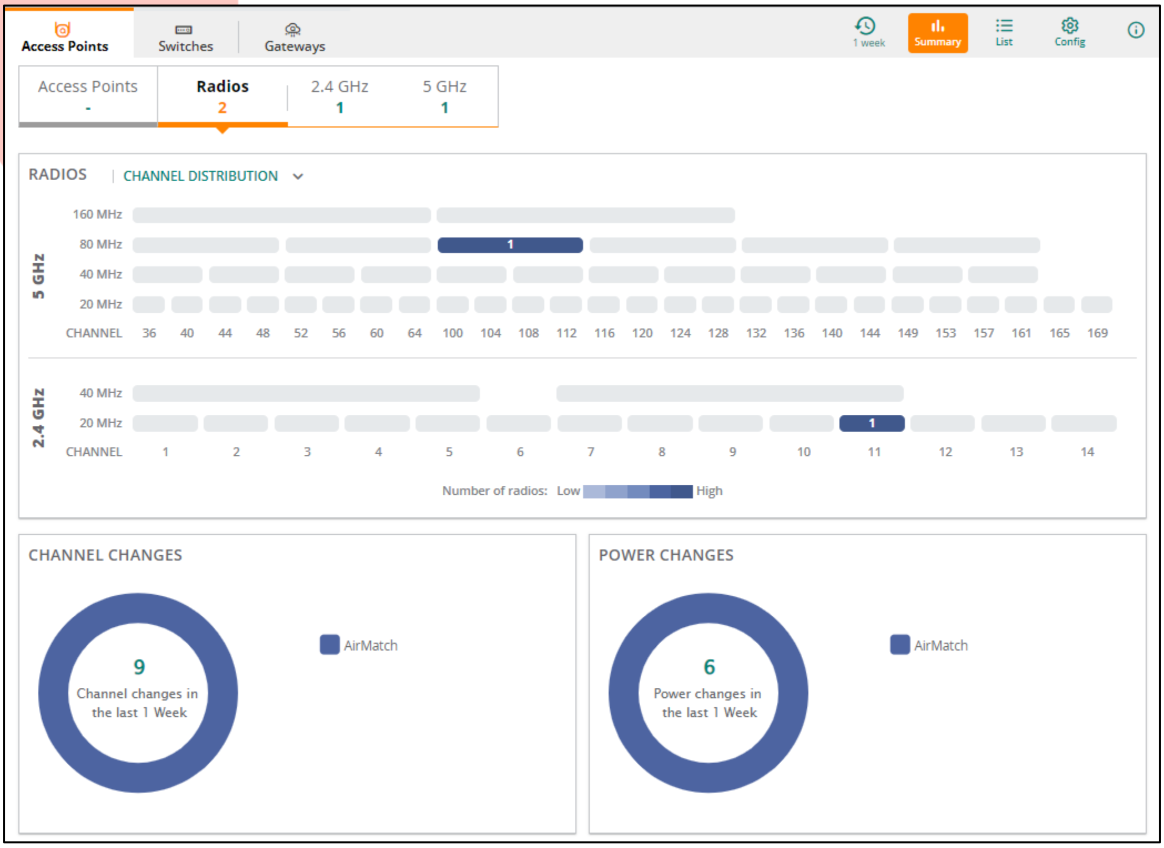
3. In Aruba Central, navigate to Context: **Global** > Navigation: **Devices**> Top: **Access Points** > **Summary** > **Radios**.



4. At the top right, adjust the history time to **1 week**.



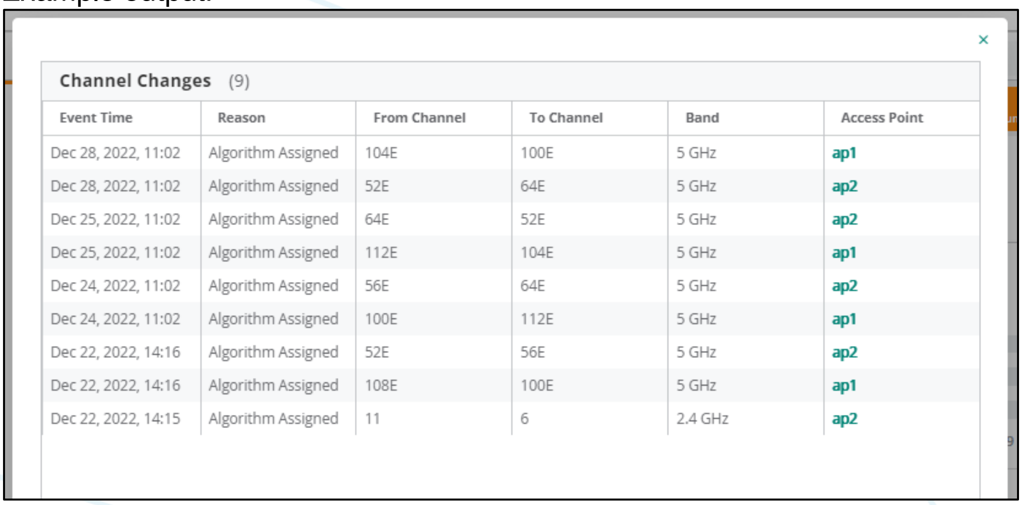
5. The window will now show the number of channel and power changes over the last week.



Review Changes and Reasons

6. Click the number in the **Channel Changes** circle to see the time of the channel changes and the affected APs.

Example output:

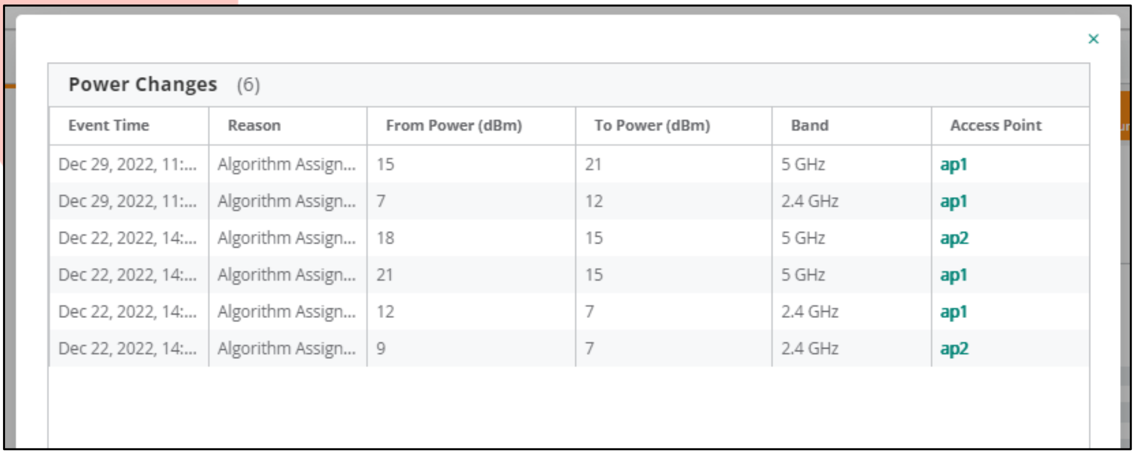


Channel Changes (9)

Event Time	Reason	From Channel	To Channel	Band	Access Point
Dec 28, 2022, 11:02	Algorithm Assigned	104E	100E	5 GHz	ap1
Dec 28, 2022, 11:02	Algorithm Assigned	52E	64E	5 GHz	ap2
Dec 25, 2022, 11:02	Algorithm Assigned	64E	52E	5 GHz	ap2
Dec 25, 2022, 11:02	Algorithm Assigned	112E	104E	5 GHz	ap1
Dec 24, 2022, 11:02	Algorithm Assigned	56E	64E	5 GHz	ap2
Dec 24, 2022, 11:02	Algorithm Assigned	100E	112E	5 GHz	ap1
Dec 22, 2022, 14:16	Algorithm Assigned	52E	56E	5 GHz	ap2
Dec 22, 2022, 14:16	Algorithm Assigned	108E	100E	5 GHz	ap1
Dec 22, 2022, 14:15	Algorithm Assigned	11	6	2.4 GHz	ap2

7. Click the number in Power Changes.

Example output:



Power Changes (6)

Event Time	Reason	From Power (dBm)	To Power (dBm)	Band	Access Point
Dec 29, 2022, 11:...	Algorithm Assign...	15	21	5 GHz	ap1
Dec 29, 2022, 11:...	Algorithm Assign...	7	12	2.4 GHz	ap1
Dec 22, 2022, 14:...	Algorithm Assign...	18	15	5 GHz	ap2
Dec 22, 2022, 14:...	Algorithm Assign...	21	15	5 GHz	ap1
Dec 22, 2022, 14:...	Algorithm Assign...	12	7	2.4 GHz	ap1
Dec 22, 2022, 14:...	Algorithm Assign...	9	7	2.4 GHz	ap2

Review ARM History on the AP

8. In Aruba Central, navigate to Context: **Global** > Navigation: **Tools** > **Commands**.
9. For device type, select **Access Point**.
10. In the *Available devices* list, select both **ap1** and **ap2**.
11. In the *Categories* list, select **ARM**.
12. In the *Commands* list, select **AP ARM History**.
13. Click **Add** to move the command to the Selected Commands list.
14. Click **Run**.

After a few moments the output will be collected from the APs.

15. Review the **show ap arm history command** output for both APs. This should reflect the last channel and power changes you have reviewed in the previous steps in Aruba Central.

Example output for AP1

```
=== Troubleshooting session started ===


===================================
Output Time: 2022-12-29 10:37:07 UTC


COMMAND=show ap arm history

Interface :wifi0
ARM History
-----------
Time of Change       Old Channel  New Channel  Old Power  New Power  Reason     Result
--------------       -----------  -----------  ---------  ---------  ------     ------
-
2022-12-29 10:01:09  100E         100E         15.0       21.0       AM Solver  -
2022-08-06 03:53:17  0            100E         Max        15.0       AM Init    -
```

```
Interface :wifi1
ARM History
-----------
Time of Change       Old Channel  New Channel  Old Power  New Power  Reason
Result
--------------       -----------  -----------  ---------  ---------  ------     -----
-
2022-12-29 10:00:13  11           11           7.0        12.0       AM Solver  -
2022-08-06 03:53:17  0            11           Max        7.0        AM Init    -

I: Interference, R: Radar detection, N: Noise exceeded, Question: Bad Channel Quality
E: Error threshold exceeded, INV: Invalid Channel, G: Rogue AP Containment, M: Empty
Channel, P+: Increase Power, P-: Decrease Power, 40INT: 40MHZ intol detected on 2.4G,
NO40INT: 40MHz intol cleared on 2.4G, OFF(R): Turn off Radio due to Radar,
OFF(CONFIG): Turn off Radio due to Wrong Config, ON: Turn on Radio, D: Dynamic
Bandwidth Switch, I*: CCA Interference, C: Radar cleared, DM: Dynamic Mode Change, O:
Opmode change, AIRMATCH: AirMatch Event, AM Solver: AirMatch(AM) service selected
channel/power, AM Init: Initialized channel/power from flash, AM N: Noise exceeded,
AM NC: Noise Cleared, AM RD: Reg-Domain Profile Change, AM Rogue: Rogue AP
Containment, AM DRT: DRT File Change, AM MinEIRP: Min EIRP Change, AM MaxEIRP: Max
EIRP Change, AM Freeze: set static channel/power, AM Unfreeze: unset static
channel/powerNC: Noise Cleared, Random: Random Channel, RMC: Radio Mode Change, RCP:
Radio Client Preference Change

=== Troubleshooting session completed ===
```

You have completed this Lab!

Lab 14: Monitoring with UXI Sensors

Overview

In this lab you will learn how to monitor the network using a UXI sensor.

Aruba UXI sensors continuously test network services and internal and external applications; then they can generate alerts when issues are detected.

In the first task you will start by onboarding the sensor and then you will complete the initial setup of the UXI customer environment.

You will configure the sensor to log into the corporate WLAN, the PSK WLAN, and test the wired network.

In the second task you will integrate the UXI dashboard with Aruba Central. This integration provides visibility of the UXI status in the Aruba Central dashboard.

In the last task you will reset the customer environment back to factory default settings.

Objectives

After completing this lab, you will be able to:

- Complete the initial setup of a UXI sensor.
- Configure additional wireless tests for a UXI sensor.
- Configure a wired test for a UXI sensor.
- Configure an internal application test.
- Verify the status of the UXI tests.

Task 1: Monitoring with the Aruba UXI Sensor

In this task you will first verify the connection of the UXI sensor to the sw-edge1 switch port 1/1/4.

In the next section of the lab, you will configure the UXI sensor using the UXI dashboard. This includes an optional reset of the UXI customer environment.

When configuring the UXI sensor, you will add wireless and wired tests that will be performed by the sensor.

Objectives

- Verify the UXI sensor is connected to the switch.
- Optionally reset the UXI customer environment.
- Complete the initial setup for a UXI customer.
- Configure a wireless test.
- Configure a wired test.
- Verify the operation of the sensor and the test results.

Steps

Verify the UXI Sensor Connection

1. On the MGMT PC, open an SSH connection to sw-edge1.
2. Assign port 1/1/4 (connected to the UXI sensor) to VLAN 24 and enable the port.

```
interface 1/1/4
 vlan access 24
 no shutdown
 exit
```

```
sw-edge1(config)# interface 1/1/4
sw-edge1(config-if)# vlan access 24
sw-edge1(config-if)# no shutdown
sw-edge1(config-if)# exit
```

3. Review the MAC address table for port 1/1/4. This is the port that connects to the UXI sensor.

```
show mac-address interface 1/1/4
```

```
sw-edge1(config)# show mac-address interface 1/1/4
MAC age-time            : 300 seconds
Number of MAC addresses : 1

MAC Address          VLAN     Type                       Interface
-------------------------------------------------------------------
20:4c:03:9c:44:82    24       dynamic                    1/1/4
```

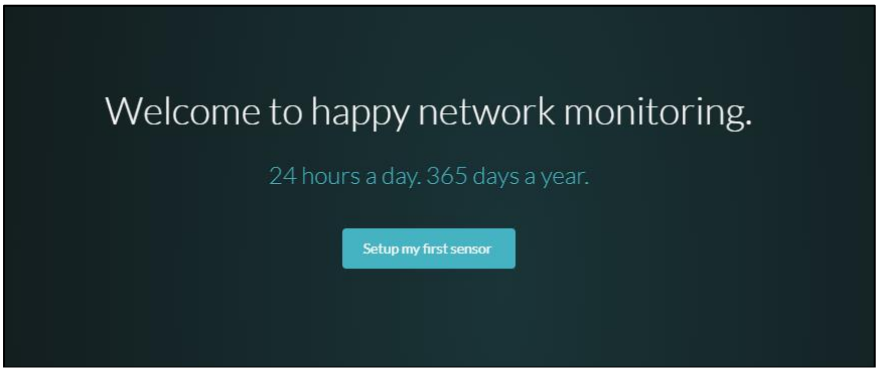
4. Take note of the MAC address.

- UXI sensor wired MAC address: ________________

5. On your local PC, open a browser session to

```
https://dashboard.capenetworks.com
```

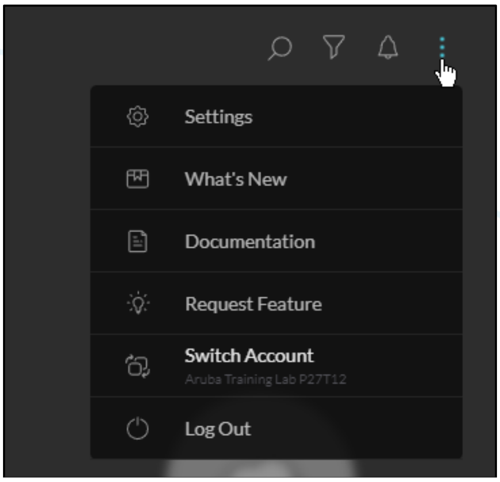
6. Login with the provided credentials.You should be presented by the Welcome Screen. If you don't see the welcome screen, you should follow the procedure in the next section to reset the environment.



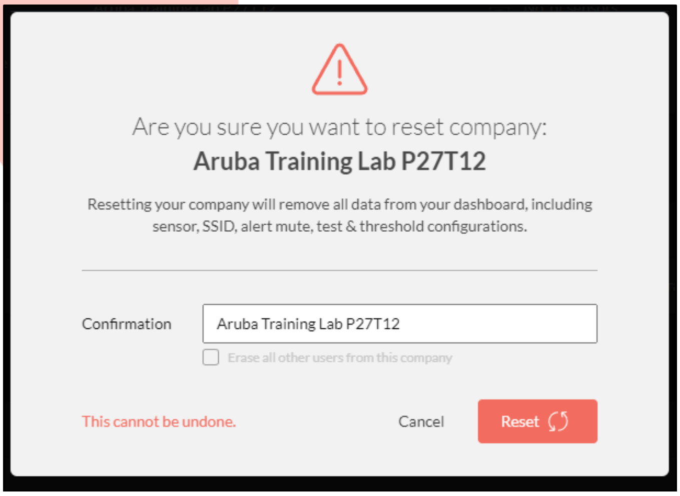
7. If you see the Welcome screen, you may skip the next 8 steps.

Only perform the next 8 steps if you do <u>NOT</u> see the *Welcome to happy networking* message.

8. At the right-top, click the **3 dots**; then click **Settings** to open the Settings page.



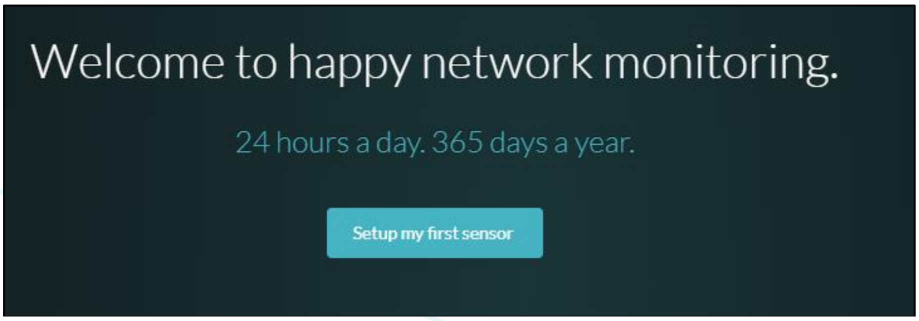
9. Under *Account*, click **Company**.
10. Under *Danger Zone*, click **Reset Customer**.
11. Copy the company name that is presented in the screen.
12. In the Confirmation field, paste the customer name.



13. Click **Reset**.
14. Click **Confirm**.
15. Click **Go To Setup**.

This concludes the customer reset process, continue with the next steps.

Welcome to Happy Network Monitoring



16. Click **Setup my first sensor**.
17. Select the sensor with the *MAC address* you noted previously.
18. Click **Next**.
19. In the SSID list, select your **p#tx-employee** SSID.
    - Security **Enterprise**
    - Auth Method **Password**
    - EAP Type **PEAP**
    - Phase2 **MSCHAPv2**
    - Username **employee**
    - Password **Aruba123!**
20. Click **Add**.
21. In the *Testing 1,2,3* screen, you need to select 3 services.
    - If you can't choose, select the first 3 services.

22. Click **Ready to test**.
23. In the *Add users* screen, no action is required. Click **Next**.
24. In the *Setup is complete* screen, click **Go to the dashboard**.
25. You will now be presented with the result of the sensor test.

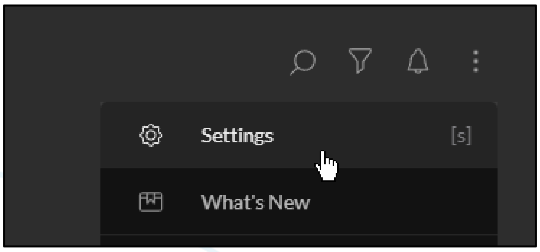
NOTE: It may take several minutes before your services appear in green. You do not need to wait for this status right now. Continue the lab activity. You can check the status again after you have added the next test.

Add a Wired Test ServiceNet

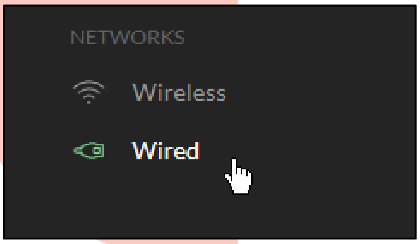
A single sensor can test multiple services. In the next steps you will add a new wired network that will be tested by the sensor.

Adding a new wired test will require these steps:
- Define a global wired network definition.
- At the sensor level, enable the wireless network to test.

26. At the right-top, Click the **3 dots** and then **Settings**.



27. In the *Settings* page, you will be on the *Networks* > *Wireless* page.
28. Navigate to the **Networks > Wired** page.



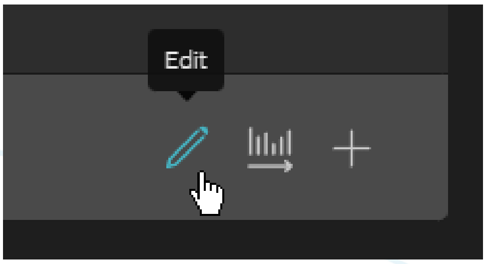
29. Click **Add Network** to create a new wired test profile.
    - Alias: **campus-wired**
    - Security: **none**

NOTE: The sensor can be configured to perform wired 802.1X authentication or use VLAN tagged traffic. In this lab environment, the sensor is connected through other transit switches to your lab devices. Therefore, 802.1X or VLAN tags do not work in this lab environment, and thus a different type of test will be performed.

30. Click **Add**.

You are now ready to bind the test to the sensor.

31. Navigate to **Locations > Sensors**.
32. In the *Configured Sensors* list, click the **pencil** icon to edit the UXI sensor.



By default, a single network is tested by the sensor.

33. Click **Enable multiple networks**.
34. Read the information message about multiple networks.
35. Click **Enable** in the information message.
36. On the *General* page of the sensor, click **Add wired network**.
37. Select the wired network **campus-wired** from the list.
38. Click **Add**.

Add a Wireless Test Service for PSK

A single sensor can test multiple WLAN services. In the next steps you will add a new wireless network that will be tested by the sensor.

The steps are very similar to the wired network test.

Adding a new test will require these steps:

- Define a global wireless network definition.
- At the sensor level, enable the wireless network to test.

39. On the *Settings* page, navigate to **Networks > Wireless**.
40. Click **Add Network**.
41. For the SSID, select your **p#tx-psk** from the list.

TIP: You can use the search field to filter the SSID list.

42. For the *Passphrase*, enter **Aruba123!**
43. Click **Add**.

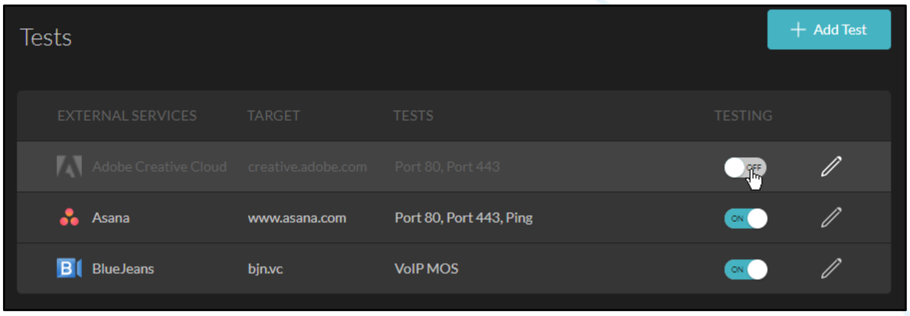
You are now ready to bind the WLAN network to the sensor.

44. Navigate to **Locations > Sensors**.
45. In the *Configured Sensors* list, click the **pencil** icon to edit the Sensor.
46. On the *General* page of the sensor, click **Add wireless network**.
47. Select your wireless network **p#tx-psk** from the list.
48. Click **Save**.

Add an Internal Test Service for an Internal Web Server

You can have the sensor test reachability to internal servers, as well as external services. In the next steps you will add a custom test to the internal 10.254.1.21 web server.

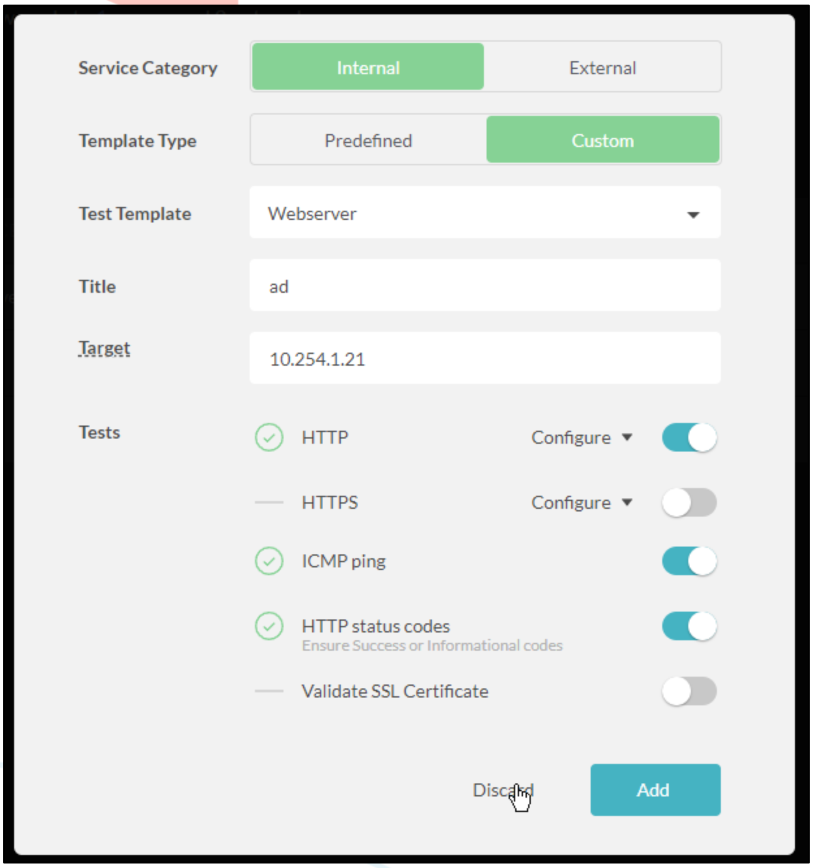
49. On the *Settings* page, find the *Testing* section and click **Service & App Tests**.
50. This page will show the three previously enabled service tests.
51. You can disable the testing of these external services here by moving the slider.



52. Click **Add Test** to create a new test.

- Service Category **Internal**
- Template Type **Custom**
- Test Template **Webserver**
- Title **ad**

- Target **10.254.1.21**
- Tests
  - Set HTTPS to **disabled**
  - Set Validate SSL Certificate to **disabled**
  - Leave other tests default.
- Click **Add**.



Task 2: Integrate the UXI Dashboard with Aruba Central

In this task you will setup the integration between the UXI dashboard and Aruba Central. The goal of this integration is to have visibility of the UXI sensor data within the Aruba Central dashboard screen.

Please note that it may take several hours after configuring the integration before the data is visible in Aruba Central; therefore, this task is only focused on the configuration. You will probably not observe the result during this lab activity.

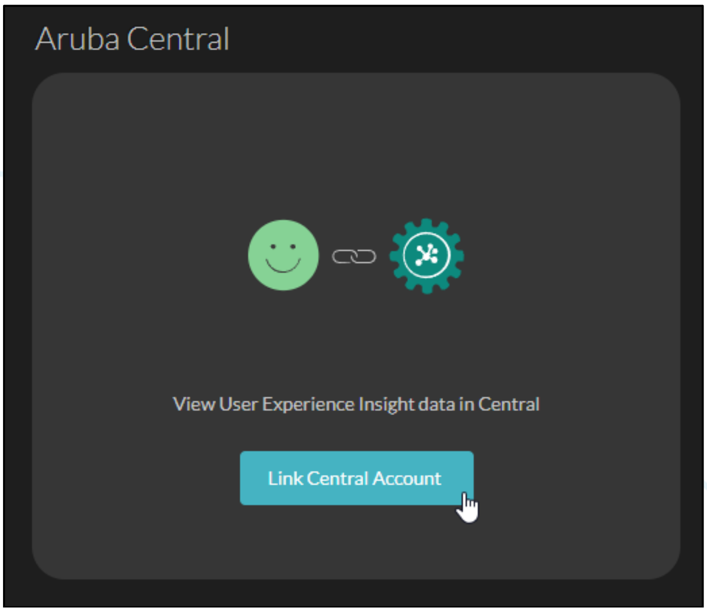
Objectives

- Configure integration between UXI and Aruba Central.

Steps

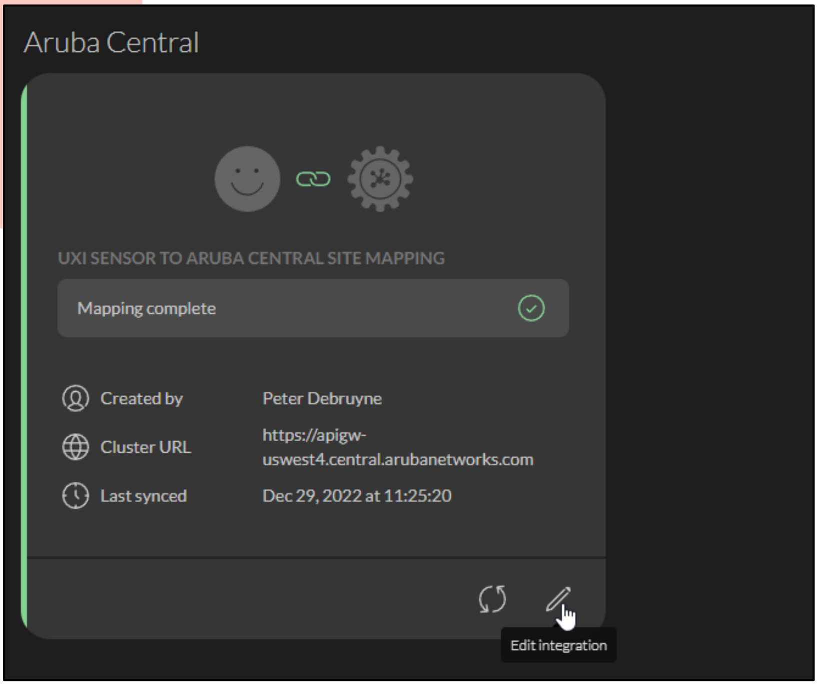
UXI Integration with Central

1. Open the UXI **Settings** page.
2. Under the *ACCOUNT* section, click **Integrations**.
3. Under the Aruba Central section, click **Link Central Account**.

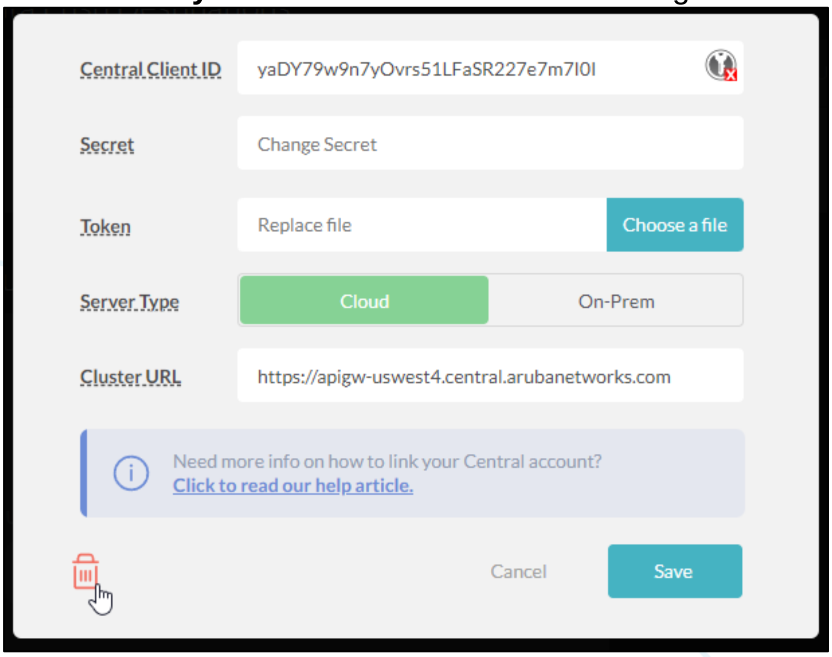


NOTE: If there is an existing integration, you can remove it with these steps:

Click **Edit Integration**.

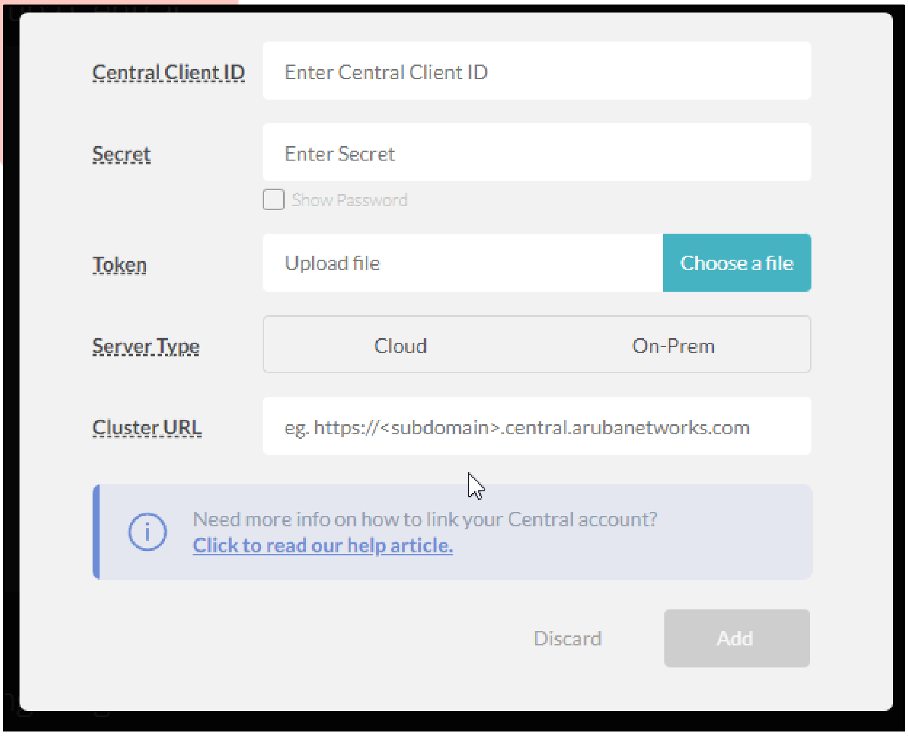


Click the **Recycle Bin** icon to remove the settings.



Click **Yes, Remove**.

4. This window shows the information that is required to configure the integration with Aruba Central.

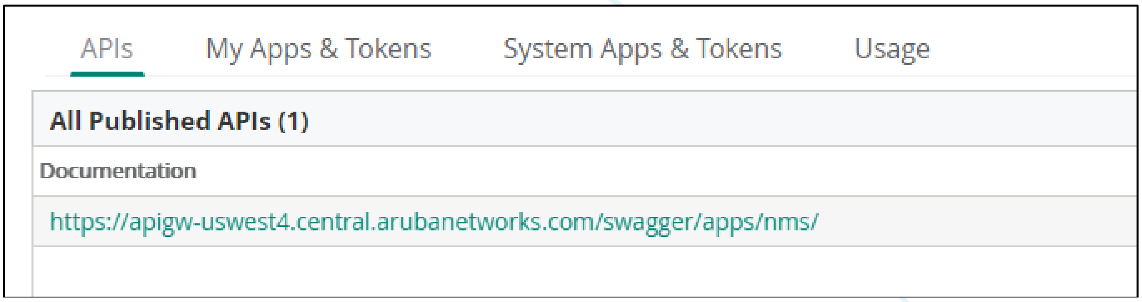


You will now collect this information in Aruba Central.

Collect Information in Aruba Central

First, you need to find the API URL that is used in Central.

5. In Aruba Central, navigate to Context: **Global**> Navigation: **Organization**> > **Platform Integration**.
6. Under **API Gateway**, click **Rest API**. Take note of the Documentation URL.
   - You should only take note of the FQDN section (remove the /swagger/apps/nms from the URL).



   - Example in the remote lab:

```
https://apigw-uswest4.central.arubanetworks.com/
```

Next, you need to finding the Client ID and Client Secret. The API access allows user applications or system applications to connect via an API to Aruba Central. For an application to access the API, it will need to login and provide a Client ID and Client secret.

In the next steps, you will generate the Client ID that the UXI application can use to access Aruba Central.

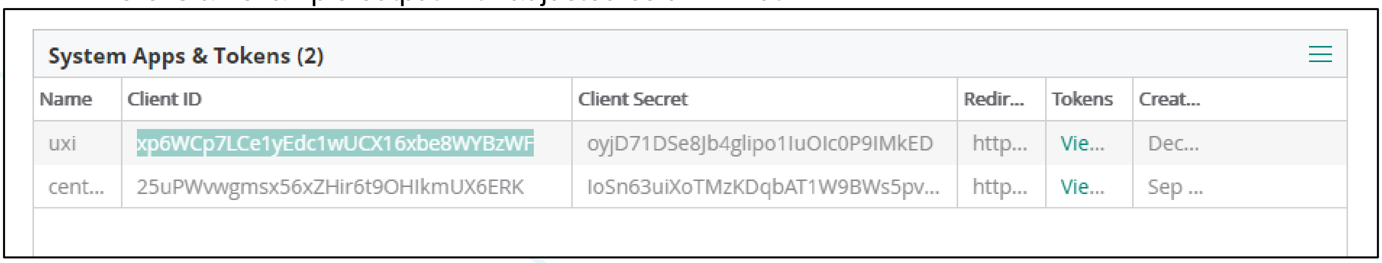
7. Click **System Apps & Tokens**.
8. Click **Add Apps & Tokens**.
   - Application Name **uxi**

NOTE: This could be any name. The name *uxi* is used as a reference to the application here.

9. Click **Generate**.
10. In the *System Apps and Tokens* list, a new entry will be displayed for *uxi* with the Client ID and Client secret.

TIP: You can change the column width to see the complete Client ID and Client Secret.

Here is an example output with adjusted column width:

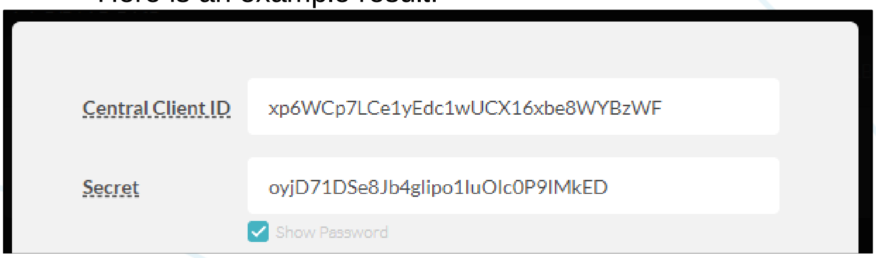


System Apps & Tokens (2)

Name	Client ID	Client Secret	Redir...	Tokens	Creat...
uxi	xp6WCp7LCe1yEdc1wUCX16xbe8WYBzWF	oyjD71DSe8Jb4glipo1IuOIc0P9IMkED	http...	Vie...	Dec...
cent...	25uPWvwgmsx56xZHir6t9OHIkmUX6ERK	IoSn63uiXoTMzKDqbAT1W9BWs5pv...	http...	Vie...	Sep ...

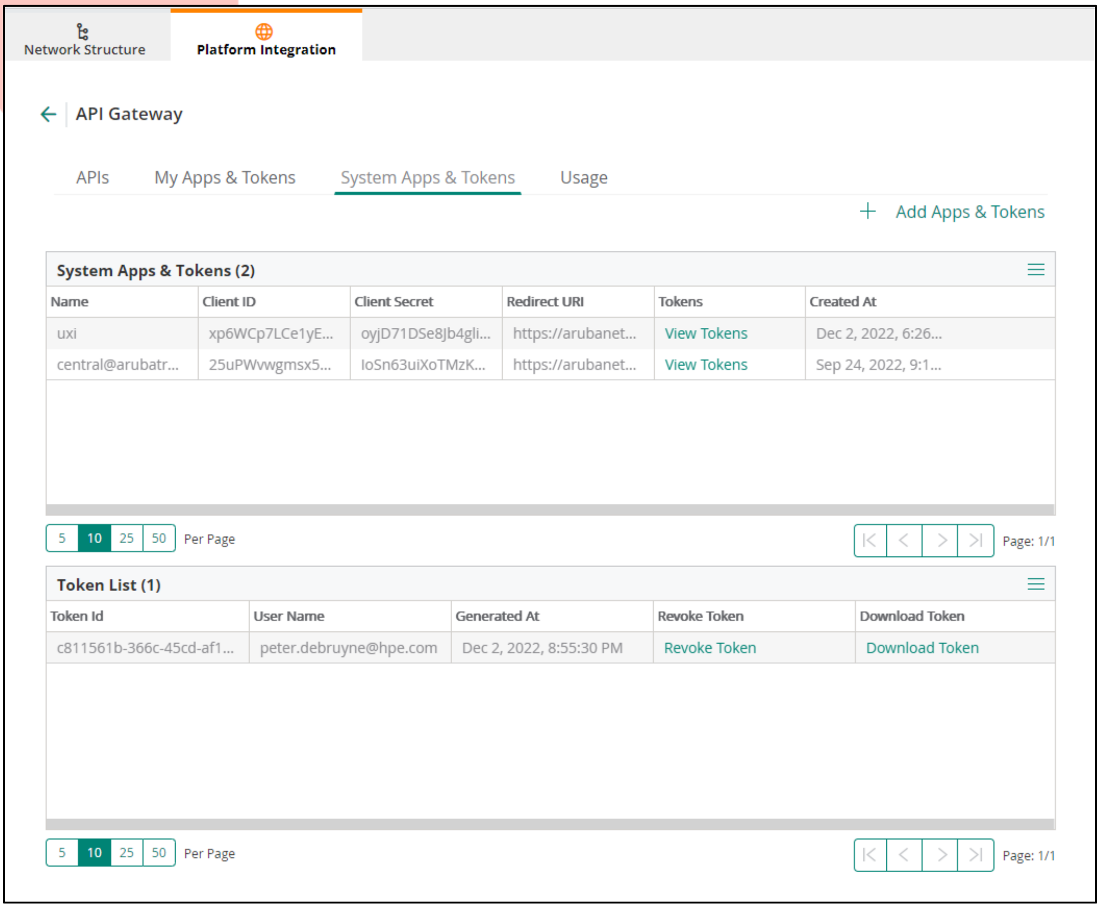
11. Copy the **Client ID** and paste it in the UXI Central Integration screen.
12. Copy the **Client Secret** and paste it in the UXI Central Integration screen.

Here is an example result:



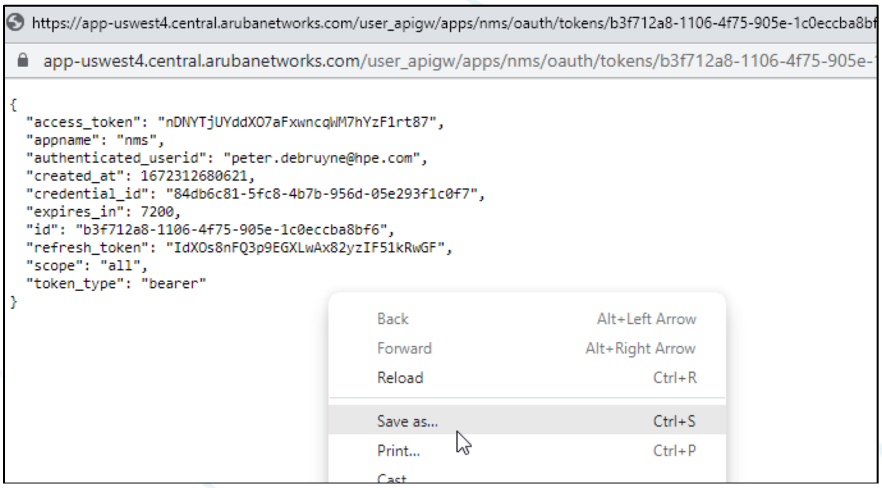
13. Leave the Integration screen open; you'll use it again in a moment.
14. Switch to the *Aruba Central > System Apps & Tokens* window.

15. The lower window is the *Token List*. In the Token List, click **Download Token**.



16. Save the token as a file on your local system.

NOTE: Depending on your local browser and platform, it may be downloaded as a file already, or you may need to right-click on the browser window and select **Save** as to save it as a file.

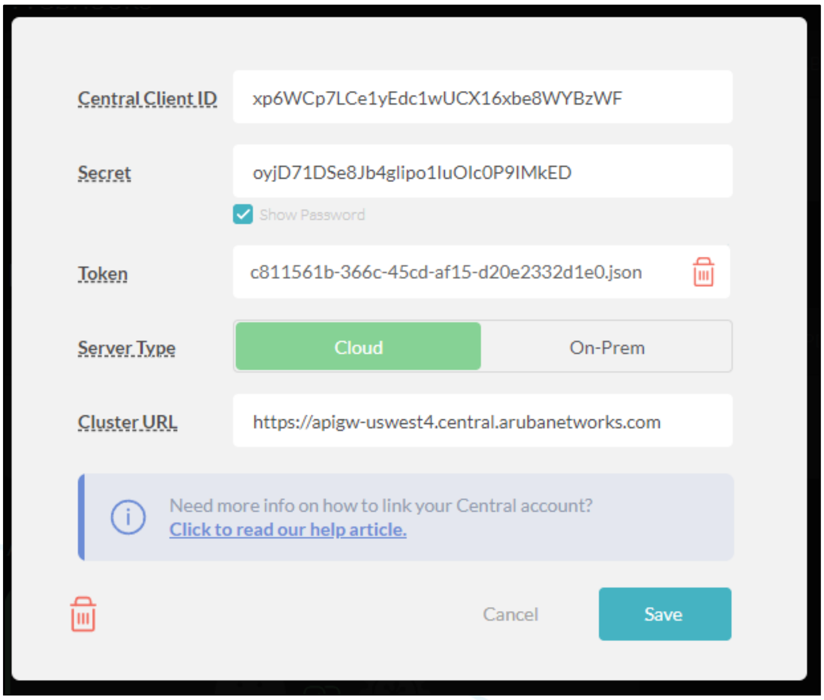


17. Switch to the UXI dashboard and click **Choose a file** to upload the token file.
18. Complete the Integration with the remaining fields:
    - Server Type: **Cloud**
    - Cluster URL: The URL you have noted for Aruba Central API.

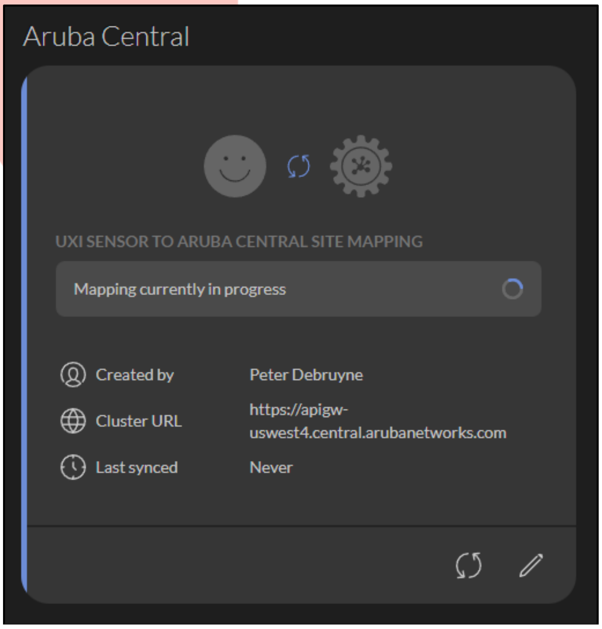
NOTE: The remote lab will typically use this URL:

```
https://apigw-uswest4.central.arubanetworks.com/
```

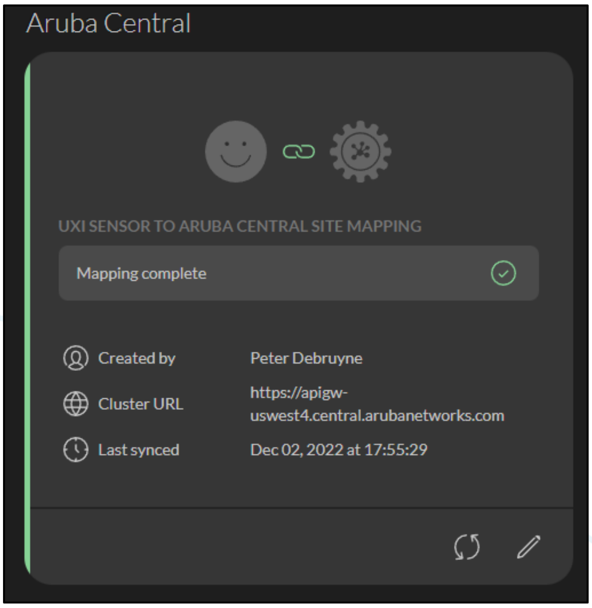
Compare this URL to your actual lab setup before you just copy and paste it!



19. Click **Add**.
20. Review the Aruba Central integration tile. You may have several status screens while the connection is established. You may use the refresh icon at the bottom of the integration tile to refresh the information.



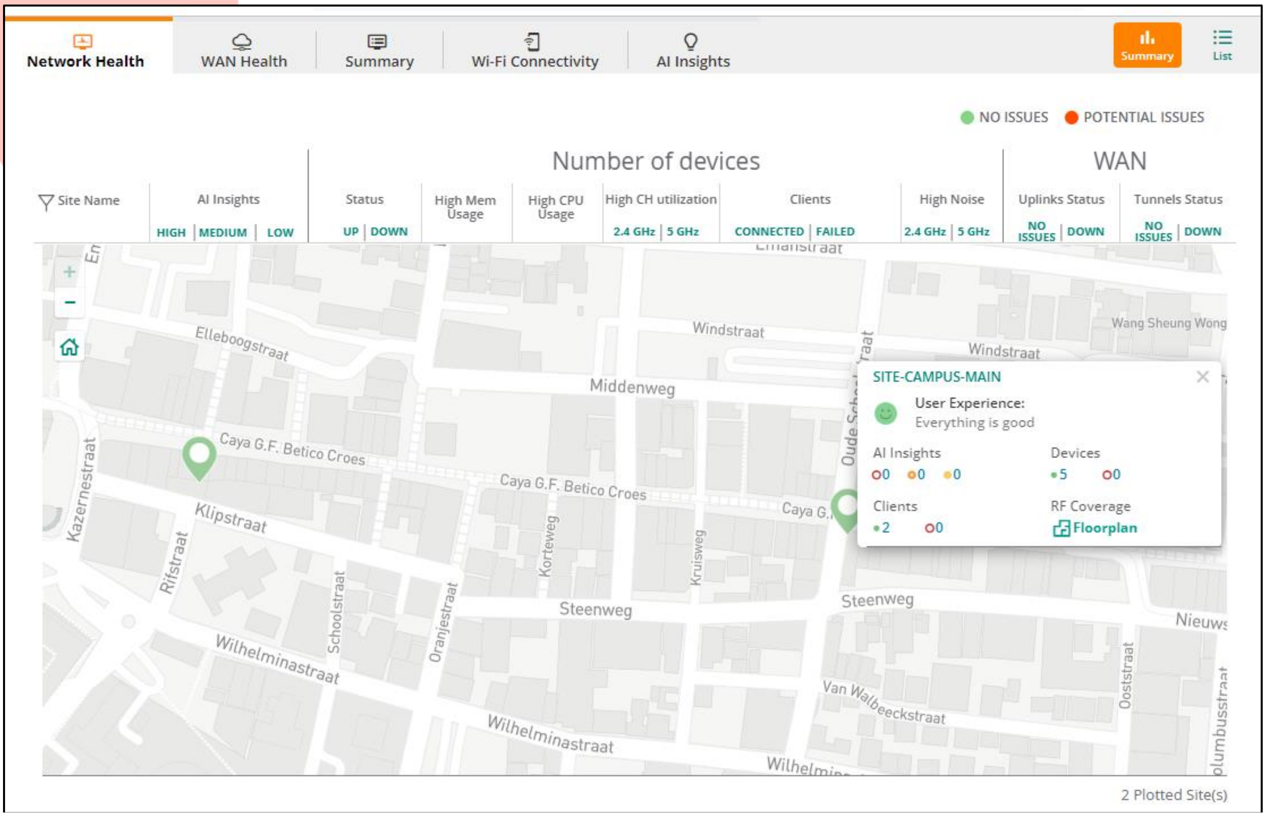
21. Once the sync is complete, you will see a mapping complete message.



22. Now the UXI can report the status of the tests to Aruba Central.

Example output of the UXI status that is visible in the Global > Overview > Network Health screen in Aruba Central:

NOTE: It may take several hours to complete the initial test sensor to site mapping. **You do not need to wait for this in this lab activity!**



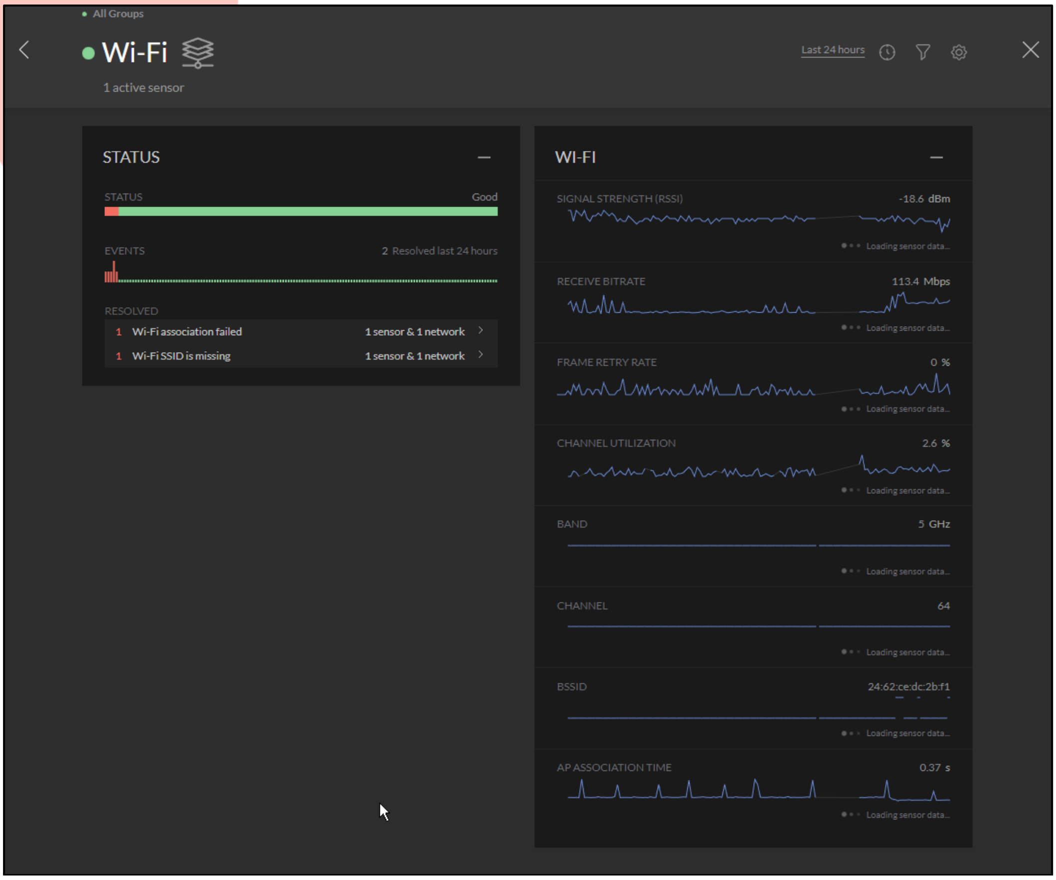
Review the UXI Dashboard

23. In the UXI dashboard, click on the Dashboard link (Top left).

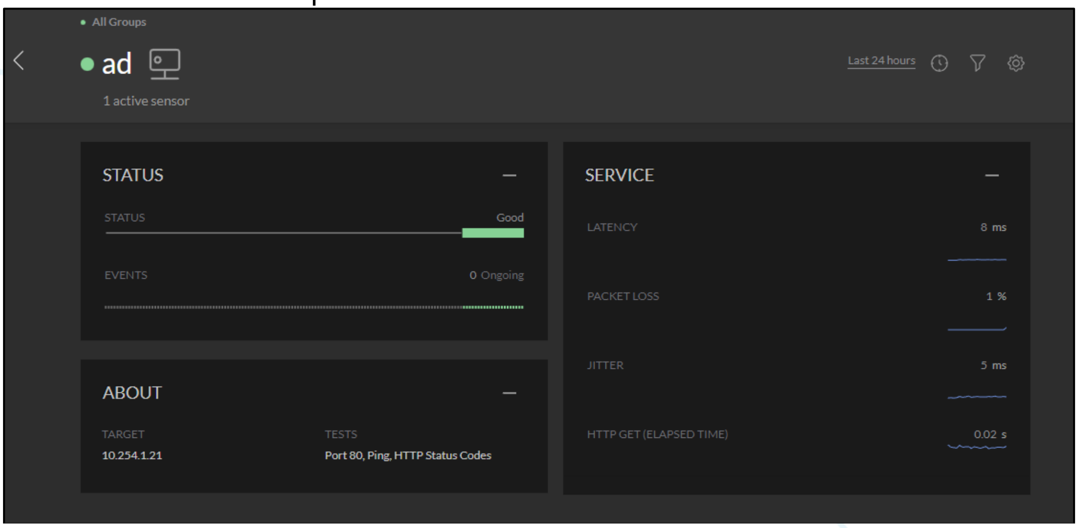
    Here is an example dashboard:

24. You may click on any of the Services or Internal Tests to see details about the history and success of each of the tests.

    Here is an example for the Wi-Fi link:



Here is an example for the ad web server test:



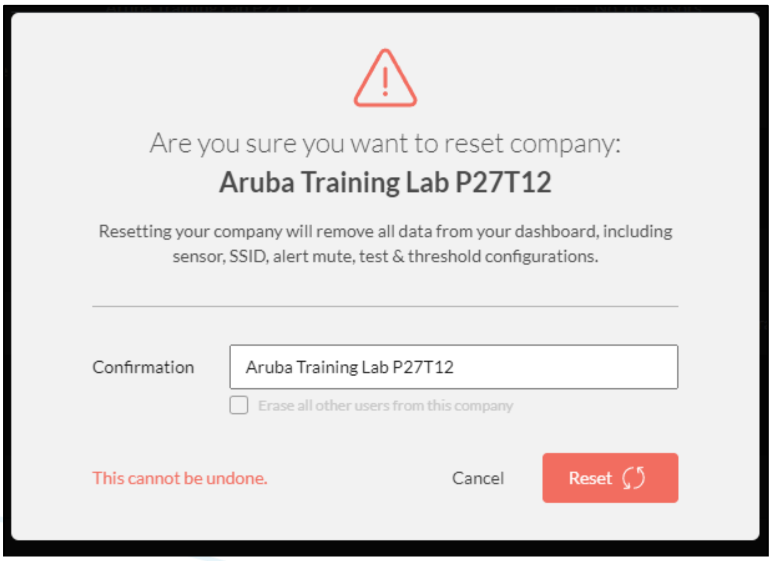
This concludes the UXI Sensor integration activity.

Task 3: Reset the Lab Customer Environment

In this task you will reset the UXI customer environment. This ensures the next student can start with a default UXI environment.

Steps

1. In the UXI system, open the **Settings** page.
2. Under *Account*, click **Company**.
3. Under *Danger Zone*, click **Reset Customer**.
4. Copy the company name that is presented in the screen.
5. In the Confirmation field, paste the customer name.



6. Click **Reset**.
7. Click **Confirm**.
8. Close the browser session.

This completes the UXI customer reset task.

You have completed this Lab!

6280 AMERICA CENTER DR. SAN JOSE, CA 95002
TEL: 408.227.4500 | FAX: 408.227.4550
www.ARUBANETWORKS.com

EDU-ICAC-RLABS-v23.11