Managing Campus Networks with Aruba Central
Table of Contents

Managing Campus Networks with Aruba Central

Lab 1: Remote LAB information

Overview

The Aruba Live Labs center provides you with an Aruba Wireless LAN controller, Aruba Wireless Access Point, Virtual Laptops, as well as the servers you need for your training. You should be aware of the procedures to access each and every device and clients available in the live labs.

Objectives

After completing this lab:

- You will have all the information needed for your oncoming labs.

Lab Information

Your class has been assigned a POD and table numbers.

Your instructor will give you information to access the specific remote lab. All students will have different logins. In this section, you will write down the information on your access to the remote lab.

- What is your User/ Password login to the remote lab? U: ____________ P: ___________
- What is your POD and table number POD? _____________ Table : ________________

Lab equipment

These labs were designed for the following equipment:

- Three Aruba 303 series APs
- Two Aruba Switches
- One client (VLT2) running Windows 10 with an Ethernet NIC that connects to the lab network.
- One client (VLT1) running Windows 10 with a wireless NIC and wired connection to Lab equipment.
- Shared equipment list:
  - ClearPass, AD, DHCP, DNS and Skype for Business Server.

Table 1.1: Device Names

You have been assigned a POD and table number in your remote lab location. When configuring your equipment, you must follow a naming and numbering plan based on your POD and table number. In these labs, the value # is your POD number and X is your table number.

The naming convention is listed. Under My devices write the name you will assign to your devices.

Device model	Device name in these labs	User and Password
VC Names	**VC1-B1** **VC2-B2**	admin / admin admin / admin
Aruba IAP	**AP1-B1** **AP1-B2** **AP2-B2**	admin / admin admin / admin admin / admin
Aruba Switches	**Aruba-2930F-Switch1** **Aruba-2930F-Switch2**	No User/password No User/password

Throughout these labs, the instructions will refer to devices by names that indicate their place in the topology.

Don't forget: In these labs, the value # and X = your assigned student table number (where # is your pod number, and X is your table number).

Task 1.1: Remote Training Lab Access

Objectives

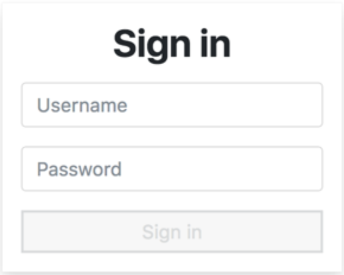
During this training, you will use Aruba's Live Labs. The Live Labs center provides you with an, Aruba wireless Unified Access Points, Switches, virtual laptops, as well as the servers you need for your training. In this lab you will test the access to your remote lab

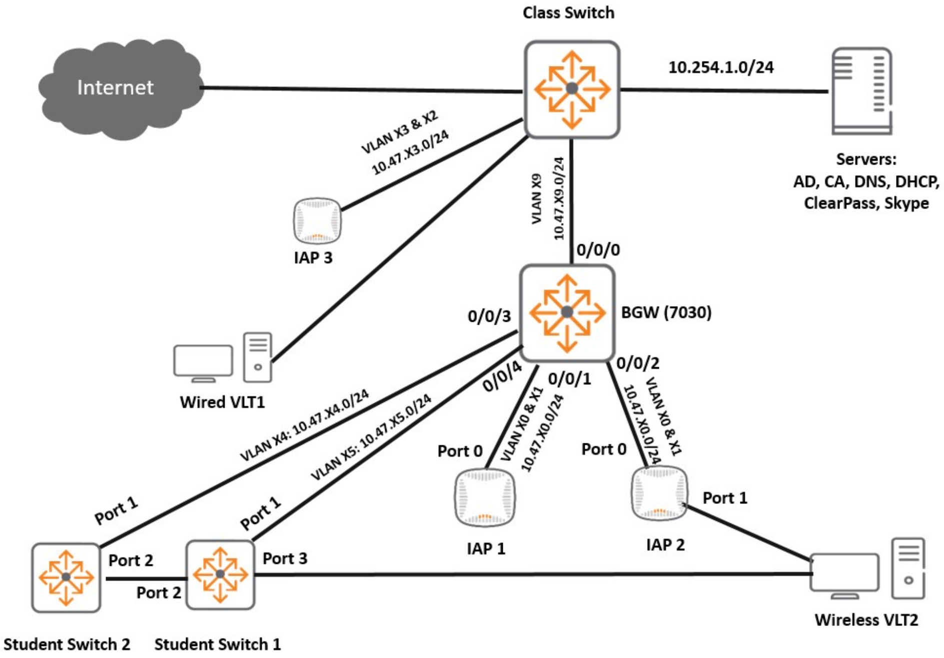
Step 1 - Initial Access and Control

1. Launch a web browser and browse to the Live Labs access portal, at the URL:

Remote Lab access: https://arubatraininglab.computerdata.com/login

2. Enter the username and the password (if you don't have one, ask your instructor for the credentials) and click the **Login** or **Sign in** button.


Sign in
Username
Password
Sign in


Class Switch
Internet
10.254.1.0/24
Servers:
AD, CA, DNS, DHCP,
ClearPass, Skype
VLAN X3 & X2
10.47.X3.0/24
IAP 3
VLAN X9
10.47.X9.0/24
0/0/0
BGW (7030)
0/0/3
Wired VLT1
0/0/4
0/0/1
0/0/2
VLAN X4: 10.47.X4.0/24
VLAN X5: 10.47.X5.0/24
VLAN X0 & X1
10.47.X0.0/24
VLAN X0 & X1
10.47.X0.0/24
Port 0
Port 0
IAP 1
IAP 2
Port 1
Port 1
Port 1
Port 2
Port 2
Port 3
Student Switch 2
Student Switch 1
Wireless VLT2

LiveLabs Interface

Throughout the Aruba Lab Guide students are asked to connect to devices and client PCs. A left mouse click will either open an access window to the device/PC or a menu to select an option.

Wired Mgmt VLT2: You will use this client to access the Switches and the IAPs.

Wireless Client VLT1: You will use this client primarily for wireless connectivity and testing.

Aruba IAP-1: This is your Instant Access Point.

Aruba IAP-2: This is your second Instant Access Point.

Aruba IAP-3: This is your third Instant Access Point but in a different subnet.

Table Switch1: This is one of your Aruba Switches.

Table Switch2: This your second Aruba Switch.

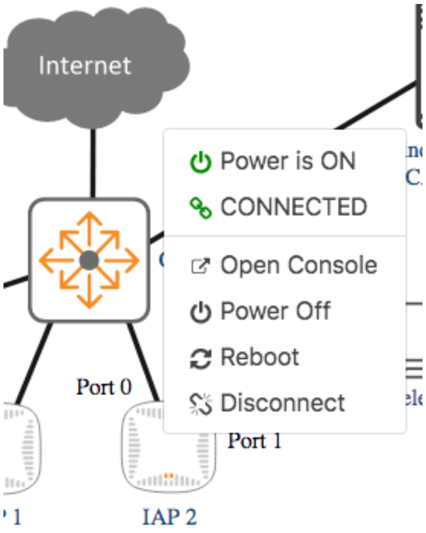
BGW: This is your Branch Gateway to simulate a branch deployment. It has been preconfigured for you and is not used in this class.

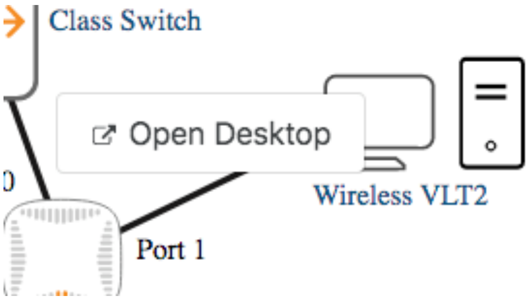
Class Switch: You have NO access to this switch.

AD/DNS/DHCP: You have no access to this server.

ClearPass: You have no access to this server.

You can open a console of these devices (Switches and AP) by simply clicking on the desired device and selecting "Open Console". A new browser page will open as the console page.





a. Open Console: This will give you CLI access of the device.

b. Power Off: This will power off the device.

c. Reboot: This will reboot the device.

d. Disconnect: This will reset the connection with the Live Labs.

e. On the desktop: Open another page to the VLTs Windows 10.

You will now complete the reference sheet on the next page. If you can, print this sheet or keep a copy on your laptop as reference. This will help you when configuring the network. Use the remote lab screen to help you fill in the fields.

Task 1.2: Reference sheet

Objectives

Your instructor has assigned you a pod number, table number and server IP addresses (for those classes using servers). Please complete the following information where # is your Pod number and X is your table number.

Step 1 – Fill in the information given.

Note: you will add some information later.

Servers have their own subnets.

Keep this sheet close by as you will reference it throughout the labs.

Remote Lab URL:	
POD (#)	
Table (X)	
Username and Password for access to Remote Lab	
Central URL:	
Central Username:	
Central Password:	
MSP Username and Password	
VC 1 IP: 10.47.X0.100	
IAP-1 IP : Via DHCP	
IAP-2 IP : Via DHCP	
VC 2 IP: 10.47.X3.100	
IAP-3 IP: Via DHCP	
Switch 1 IP : 10.47.X4.__	
Switch 2 IP : 10.47.X5.__	
NOTE: Use the Live Labs topology for reference to all server IP addressing and other devices you'll use in the lab	

Task 1.3: Customer Central Account

Objectives

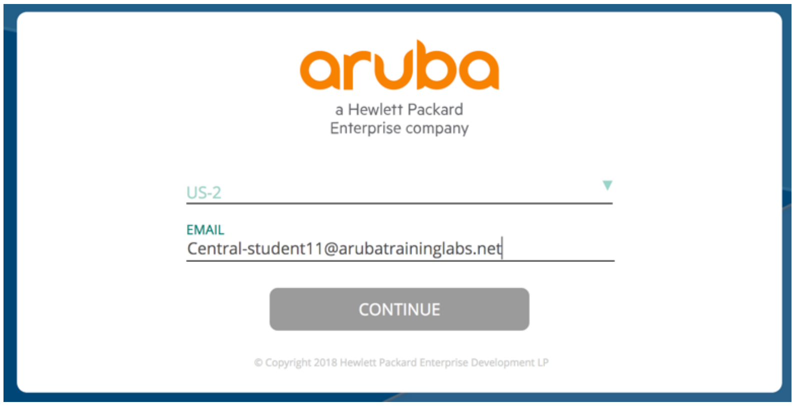
Your instructor has assigned you a Central Customer Account.

Step 1 – Access your customer Central account.

1. Launch a web browser and browse to the central portal URL.

central.arubanetworks.com

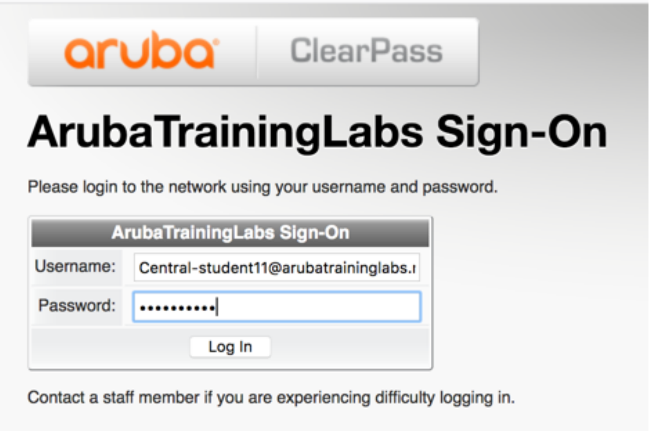
2. First select ZONE: **Provided by your instructor**
3. Then enter the username that was assigned to you. (if you don’t have one, ask your instructor for the credentials) and click **Continue**



US-2

EMAIL
Central-student11@arubatraininglabs.net

4. You will fall into the single sign on authentication (SSO)
5. Then enter the same user name that was assigned to you and the Password for this class.



ArubaTrainingLabs Sign-On

Please login to the network using your username and password.

ArubaTrainingLabs Sign-On

Username: Central-student11@arubatraininglabs.ı

Password: ••••••••••

Contact a staff member if you are experiencing difficulty logging in.

6. You should now be into your customer Central account.

You have completed Lab 1.

aruba
a Hewlett Packard Enterprise company

EDUCATION
SERVICES

Managing Campus Networks with Aruba Central

Lab 2: MSP APPs

You will look at the different application between the MSP and a Central customer account.

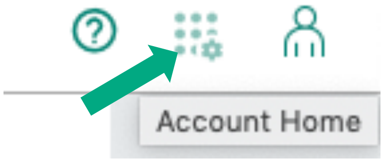
Task 2.1: APPs in your central account

Objectives

- In this task, you will login to the Central account and verify your available APPs.

Steps: Login to Central account and verify available APPs

1. Open a browser page and get access your customer Central account.
2. Login with the User/Password given to you.
3. Click on **Account Home** on the top right corner.



4. List the APP available to your central account:

   a. APP Name: ___________________

   b. APP Name: ___________________

5. Note the available options under **Global Settings**:

   a. 1st Box; Users and Roles

b. 2nd Box: _______________

c. 3rd Box: _______________

d. 4th Box: ________________

e. 5ft Box: _________________

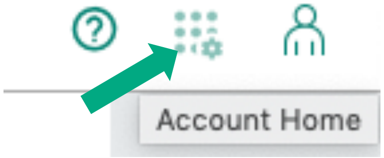
Task 2.2: APPs in the MSP account

Objectives

– In this task, you will login to the MSP Central account and verify what Central APPs are available.

Steps: Login to the MSP Central Account.

1. Logout of your customer Central account. Click the icon 👤 and select **Logout**.
2. Login into the **MSP** <u>Central account</u>: Username and password provided by your instructor
3. Click on **Account Home** ⚙ on the top right corner.



4. List the Application:

a. APP Name: ___________________

b. APP Name: ___________________

5. Note the available options under **Global Settings**:

a. 1st Box; Users and Roles

b. 2nd Box: _______________

c. 3rd Box: _______________

d. 4th Box: ________________

e. 5ft Box: _________________

f. 6th Box: _________________

g. 7th Box:_________________

h. 8th Box:_________________

6. For **Global Settings**, list the boxes the MSP view has but the central customer account does not have.

    a. MSP Box 1: ____________________

    b. MSP Box 2: _____________________

    c. MSP Box 3: _____________________

You have completed Lab 2

Managing Campus Networks with Aruba Central

Lab 3: Onboarding

The deployment team has been busy installing IAPs and Switches in your sites. The Activate cloud server has automatically directed those devices to your Central account.

A partner company has already assigned the keys and subscribed the devices.

In this lab, you will list all the devices assigned to your Central account. You will also logon to an MSP account to see the keys and subscriptions.

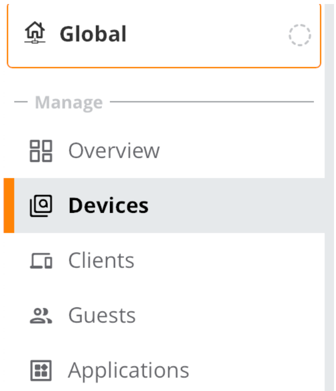
Task 3.1: Onboarded Devices

Objectives

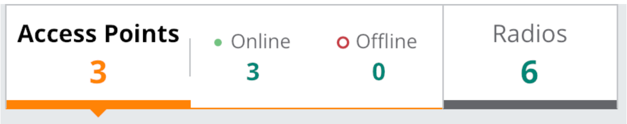
– In this task, you will login to your assigned Central account and verify your assigned devices.

Steps: Login and verify devices

1. Open a browser page and get access to your customer Central account.
2. Login with your assigned User ID and password.
3. From the **Context Scope Menu** on the left go to **Devices**.



4. Notice that under the Access Points tab all APs are listed, including devices that are currently Offline. To filter APs based on their current status or to verify radios status use respective tabs at the right side of the number of APs.



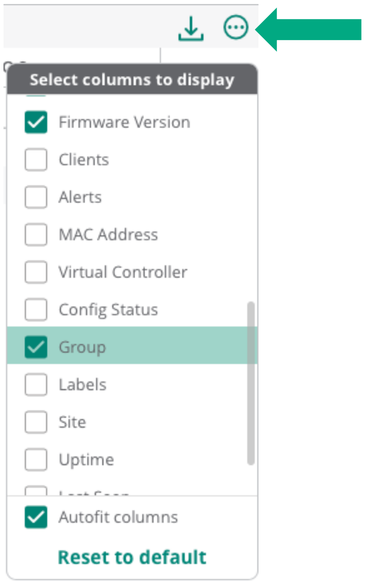
5. List the device name and model of your IAPs:

   a. Name: ____________________ Model: ______________

   b. Name: ____________________ Model: ______________

   c. Name: ____________________ Model: ______________

6. Click on the 3-point icon on the top right-hand side and select Groups then click on the background to close the popup window.



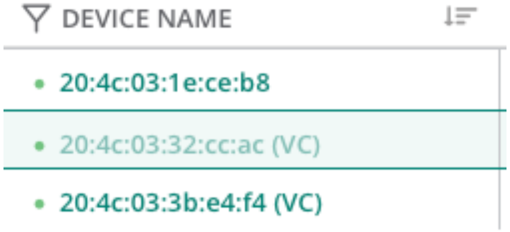
Select columns to display

☑ Firmware Version
☐ Clients
☐ Alerts
☐ MAC Address
☐ Virtual Controller
☐ Config Status
☑ Group
☐ Labels
☐ Site
☐ Uptime

☑ Autofit columns

Reset to default

7. What is the selected group for all the IAPs? ___________________
8. Click on one of the VC IAPs.



DEVICE NAME

- 20:4c:03:1e:ce:b8
- 20:4c:03:32:cc:ac (VC)
- 20:4c:03:3b:e4:f4 (VC)

9. Note the following information:

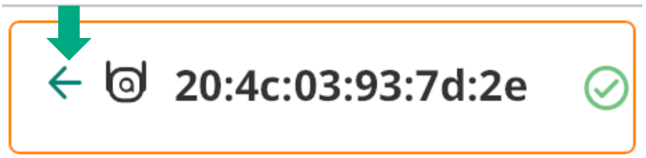
   a. Country code: ____________

   b. Firmware Version: _____________

   Note: Ignore if you see "update available" link under the firmware version

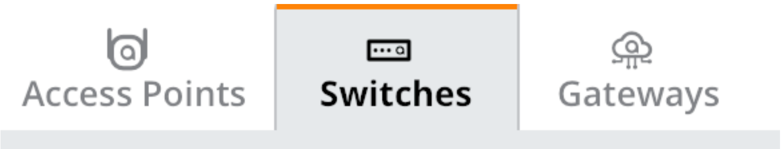
   c. IAP IP address: _______________

10. Click on ← at the top to return to the devices page.



← 20:4c:03:93:7d:2e

11. On the top bar, select **Switches.**



12. List the device name and model of your switches:
    a. Name: ______________________ Model: _________________
    b. Name: ______________________ Model: _________________
13. Click on the 3-point Icon on the top right-hand side and select Groups then click on the background to close the popup window.
14. What is the selected group for all the switches? __________________

15. Click on one of the switches.
16. Note the following information:
    a. Model: ___________
    b. J-Number : ______________
    c. Firmware Version: ____________

       Note: Ignore if you see “update available” link under the firmware version

    d. IP address: ______________
    e. Stack/Standalone status: _______________

Task 3.2: Keys and Subscription

Objectives

– In this task, you will login to the MSP account and verify your assigned subscriptions.

Steps: Login to MSP account and verify Subscription

1. **Click** on the <u>person Icon</u> at the top right-hand side of the GUI page.
2. **Select Logout**.
3. Login to the <u>Central MSP account</u>.
4. Login with the User/Password given to you. This is a read only User.
5. From the navigation Icon go to **Account Home** .

6. Select **Key Management**.
7. Answer the following questions:
   a. Type of Key: ______________ Expiration date: _____________
   b. Type of Key: ______________ Expiration date: _____________
   c. Type of Key: ______________ Expiration date: _____________
8. What is the total Assigned Device subscription? ____________
9. How many subscriptions per device:
   a. IAP: ___________
   b. Switches: ___________
   c. Gateway Devices: ___________
10. How many Available Device subscription? ____________

11. At the top of the page select **Go to account home**.

GO TO ACCOUNT HOME

12. Under Global Settings select **Subscription and Assignment**.
13. Scroll down to Network Services Subscription and click on **Clarity.**
14. Verify if your IAPs have been assigned a Clarity Subscription.

NOTE: You can find your IAPs based on the MAC address.

15. What is the Total Subscriptions? ______________
16. What are the Available subscriptions? _____________

17. On the top right click the little person ICON 👤 and **Logout** from the MSP account.

You have completed Lab 3

Managing Campus Networks with Aruba Central

Lab 4: Groups, Sites and Labels

In this lab, you will create groups for configuration. You can also use groups for monitoring. The main purpose of sites is installation and monitoring. You can use labels to organize and filter your monitoring views.

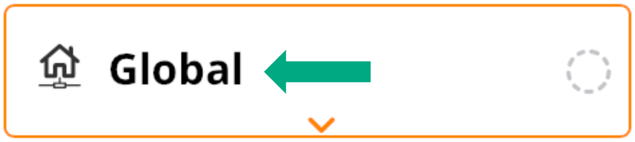
Task 4.1: Groups

Objectives

– In this task, you will view the existing filter then create groups.

Step 1: Existing Filters

1. Open a browser page and get access to Central customer account.
2. Login with your assigned User ID and password.
3. From the **Context Scope Menu** on the left go to **Overview**.
4. At the navigation tabs select **Summary.**
5. Click on the **Filter** Icon.



6. Answer the following questions:

   a. What is the name of the only group? __________

7. Then from the **Context Scope Menu** on the left go to **Devices**.

   Note: There are 2 VCs in your list of devices but you can see 3 IAPs.

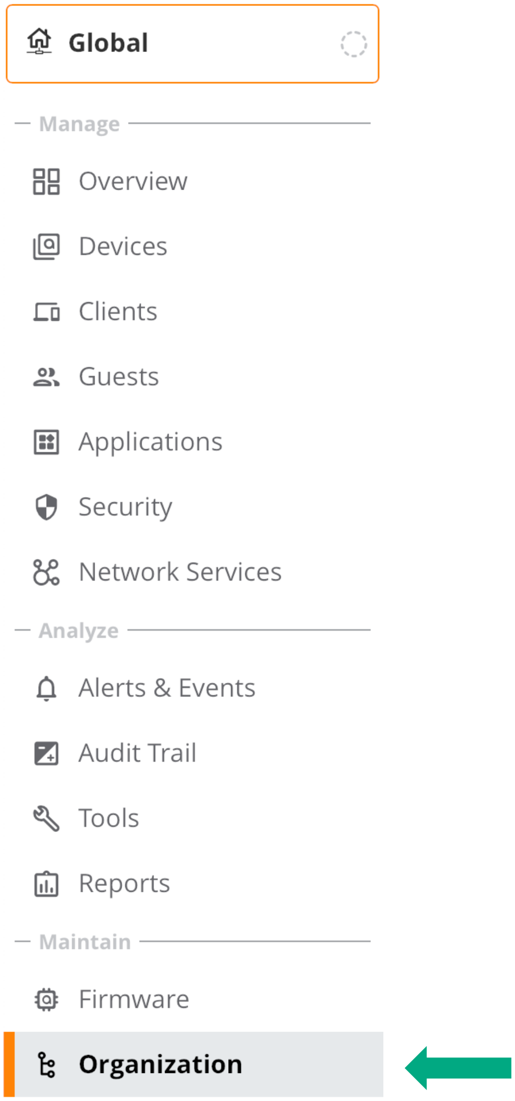
   a. The IAP that is not a VC is part of what Cluster (VC name)? _______________

   Help: Look at the device name then look at the Virtual controllers.

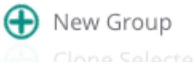
   b. We will need this information in another task.

Step 2: Adding Groups

1. From the **Context Scope Menu** on the left go to **Organization**.



2. You should be in the **Groups** section.

3. Below the Group section there is the  to add a new group. **Click** on the '+' New Group Icon.

4. Add the Group with the following information

   a. Name: **IAP-Group**.

   b. Make sure **IAP and Gateway** and **Switch** checkboxes are unselected.

   c. Password: **admin1**

   d. Confirm Password: **admin1**

5. Click on **Add Group.**

NOTE: You did not select 'IAP and Gateway or Switch' checkboxes since we want to use this group as a GUI group.

6. **Click** on the '+' New Group Icon to add a new group.
7. Enter the name '**Group-Switches-site1**"
8. Enable **Switch**. This will make this group a template group.
9. Set password to **admin1**
10. Click on **Add Group.**
11. In the list of Group names notice that the '**Group-Switches-site1'** has a TG marker. What does this signify? _______________

Step 3: Adding Devices to Groups

1. On the right-hand side, you have your switches and VC clusters. Click on a switch and drag it over to the group **Group-Switches-site1.** Click on **YES** to confirm.
2. Select the second switch and drag it over to the group **Group-Switches-site1.**

NOTE: If you are not sure what switch you previously selected then simply click on the group **Group-Switches-site1** to see what switch is already part of this group.

3. Now select a VC cluster and drag it over to **IAP-Group**. Then select the other VC cluster and drag it to the same group **IAP-Group**.
4. In the Group list you should have 2 devices in the **Group-Switches-site1** group and 2 devices in the group **IAP-Group**.
5. Click on the **Group-Switches-site1** group and confirm that the 2 devices are the 2 switches.
6. Click on the **IAP-Group** group and confirm that the 2 devices are the 2 VC clusters.

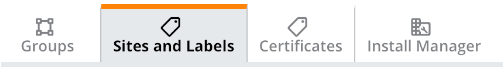
Task 4.2: Sites

Objectives

- In this task, you create two sites. You will simulate two buildings in the same campus.

Step 1: Create Two Sites

1. From the **Context Scope Menu** on the left go to **Organization**.
2. At the navigation tabs, select **Sites and Labels.**



3. In the context page make sure you have **Sites** selected .
4. At the bottom of the site list click on the "+" New Site .
5. In the create New Site popup window enter the following information:
   a. Site Name: **Building1**
   b. Street Name: **1 Boardwalk**
   c. City: **New York**
   d. Country: **United States**
   e. State: **New York**
   f. Zip code: leave blank
6. In the create second Site with the following information:
   a. Site Name: **Building2**
   b. Street Name: **1 Park Place**
   c. City: **New York**
   d. Country: **United States**
   e. State: **New York**
   f. Zip code: leave blank

Step 2: Place devices in the Sites

1. On the right-hand side, you have your switches and IAPs. Click on a switch and drag it over to the site **Building 1.** Click on **YES** to confirm.

2. Click on the second switch and drag it over to the site **Building 2.** Click on **YES** to confirm.
3. Select the single IAP cluster and drag it over to **Building 1**. Take the two IAP cluster and move them to **Building 2.**

NOTE: If you are not sure of what IAPs are in what clusters you can click on "Devices" in the left hand navigation pane to figure it out.

4. You should now have two devices in Building 1 and three devices in Building 2.
5. Click on the **Building 1** site and confirm that you have one switch and one IAP in this site.
6. Click on the **Building 2** site and confirm that you have one switch and two IAPs in this site.

Task 4.3: Labels

Objectives

– In this task, you create Labels to make filters for monitoring. We will simulate two buildings in the same campus.

Step 1: Create Labels

1. Move the slide bar over to **Labels** .
2. Below the Labels section there is the to add a new Label. **Click** on the '+' **Add Label** Icon.
3. Create the Label Name **All-IAPs** and click on **ADD**.
4. Create the Label **All-Switches** and click on **ADD**.
5. Create the Label **All-Devices-NY** and click on **ADD**.
6. Create the Label **Conference-Rooms** and click on **ADD**.

Step 2: Assign Devices to the Labels

1. Drag the following devices to the specified Label
   a. Drag all the IAPs to Label **All-IAPs**. You can select all the IAPs and move them over together.
   b. Drag the switches to Label **All-Switches**.
   c. Drag the three IAPs and two switches to Label **All-Devices-NY.**

d. Drag the One IAP and one switch to Label **Conference-Rooms.**

2. Click on the **All-IAPs** Label and confirm that the three IAPs are there.
3. Click on the **All-Switches** Label and confirm that both switches are there.
4. Verify your other Labels.

You have completed Lab 4

Managing Campus Networks with Aruba Central

Lab 5: IAP and Switch Configuration

In this lab, you will configure the IAPs and switches. You will give names to the IAPs and VCs and add in a WLAN in GUI mode. You will also configure the switches in template mode.

Task 5.1: VC Names

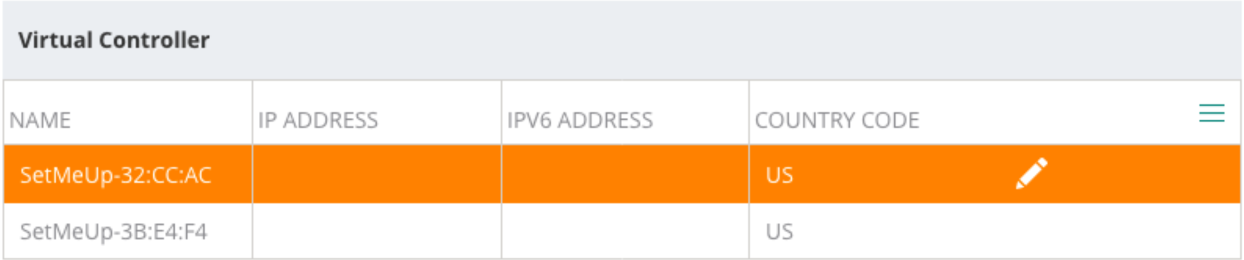
Objectives

– In this task, you will configure a VC name and IP address.

Step 1: VC Names and IP addresses

1. Open a browser page and get access to a Central customer account.
2. Login with your assigned User ID and password.
3. From the **Context Scope Menu** on the left go to **Devices**.
4. Click on the filter Icon and select the group **IAP-Group**
5. Under the “Device Name” section, you have two VC listed.

6. Click on **Configuration** ⚙ icon located at the top right corner.
7. Click on **Show Advanced**.
8. From the navigation tabs, select **System**.
9. Set the country code for group to **US**
10. Click on **Save Settings** and ignore for now the reboot message.
11. Click on the **Virtual Controller** with the single IAP then click on the pencil.



Virtual Controller

NAME	IP ADDRESS	IPV6 ADDRESS	COUNTRY CODE
SetMeUp-32:CC:AC			US
SetMeUp-3B:E4:F4			US

12. In the popup window enter the following information:
    a. Name: **VC1-B1.**
    b. IP address: **10.1.X3.100.** (X is your table number)

13. Click on **OK**.
14. Click on the **Virtual Controller** with the two IAPs then click on the pencil.
15. In the popup window enter the following information:
    a. Name: **VC2-B2**
    b. IP address: **10.1.X0.100** (X is your table number)
16. Click on **OK**.

17. At the bottom of the screen on the right click on **Save Settings**.

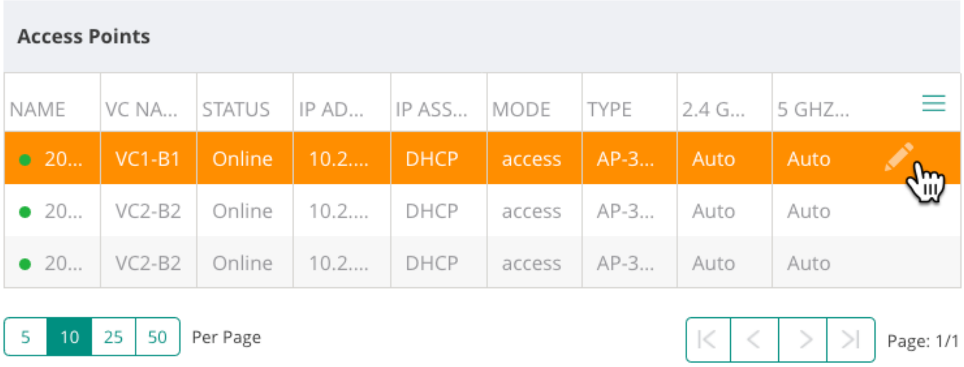
Task 5.2: IAP names

Objectives

– In this task, you will give each IAP a name.

Step 1: IAP Names

1. In the navigation tabs select **Access Points**.
2. Select the IAP with the VC **VC1-B1** and click on the **pencil**.



Access Points

NAME	VC NA...	STATUS	IP AD...	IP ASS...	MODE	TYPE	2.4 G...	5 GHZ...	☰
● 20...	VC1-B1	Online	10.2....	DHCP	access	AP-3...	Auto	Auto	✎
● 20...	VC2-B2	Online	10.2....	DHCP	access	AP-3...	Auto	Auto	
● 20...	VC2-B2	Online	10.2....	DHCP	access	AP-3...	Auto	Auto	

3. In the Access point window change the name to **AP1-B1**.
4. At the bottom of the screen on the right click on **Save Settings**.
5. Select one of the IAPs in **VC2-B2** and click on the **pencil**.
6. In the Access point window change the name to **AP1-B2**.
7. At the bottom of the screen on the right click on **Save Settings**.
8. Select the second IAP in **VC2-B2** and click on the **pencil**.
9. In the Access point window change the name to **AP2-B2**.
10. At the bottom of the screen on the right click on **Save Settings**.

Task 5.3: Reboot the IAP

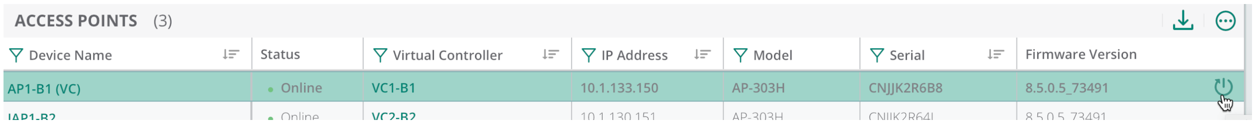
Objectives

– You will now reboot the IAP for the country code to take effect.

Step 1: Networks Employee

1. In the top Menu bar select List ☰ List .

2. Move your mouse over the one of the IAP and select the reboot option and confirm **Reboot**.



ACCESS POINTS (3)

Device Name	Status	Virtual Controller	IP Address	Model	Serial	Firmware Version
AP1-B1 (VC)	Online	VC1-B1	10.1.133.150	AP-303H	CNJJK2R6B8	8.5.0.5_73491
IAP1-B2	Online	VC2-B2	10.1.130.151	AP-303H	CNJJK2R64L	8.5.0.5_73491

3. Repeat this step for all the IAPs
4. Give your IAP a few minutes to reboot and rejoin Central.

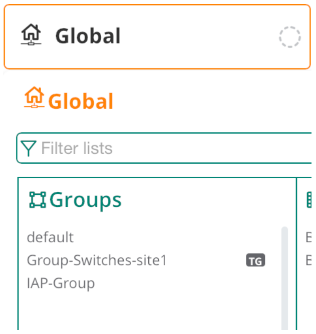
Task 5.4: WLAN network

Objectives

- You have named your VCs and given them static IPs. You have also named your IAPs. Now it is time to setup a WLAN.

Step 1: Networks Employee

1. From your filter select your IAP group



Global

Global

Filter lists

Groups

default

Group-Switches-site1 TG

IAP-Group

2. Select the gear Icon Config for Configuration.
3. In the navigation tabs select **WLANs.**
4. Click on the "**+**" sign to add in a new SSID.
5. In the general section add in the following information:

   Name: **employee"P""<u>X</u>"** <- Note the "P" is your POD number and "X" is your table number.

   Click on **Next**.
6. For the VLANs set the following:

   Select **External DHCP server assigned**

   Select **Static**.

VlanID: **X1** <- Note the "X" is your table number.

Click on **Next**.

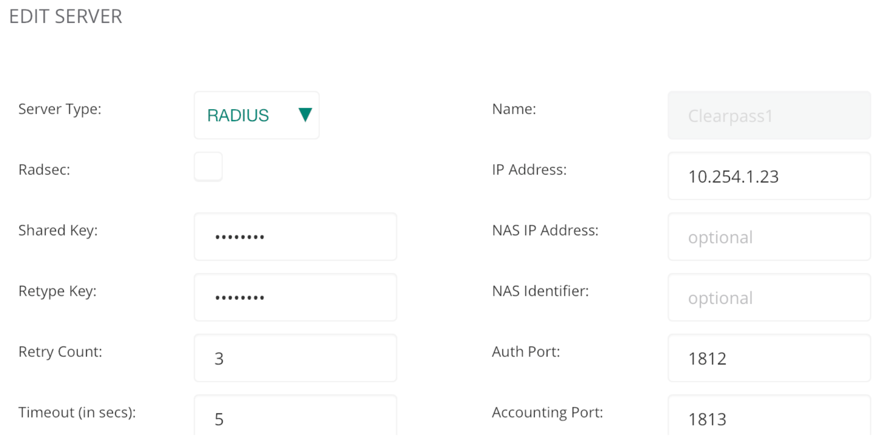
7. For the Security do the following:

   Security Level: **Enterprise**

   Key Management: WPA2-Enterprise

   Next to Primary server click the **"+"** to add a new server and enter the following information:

   a. Server Type: **RADIUS**
   b. Name: **Clearpass1**
   c. IP Address: **10.254.1.23**
   d. Shared Key: **aruba123**
   e. Retype Key: **aruba123**
   f. Leave all other fields blank or at defaults
   g. Click on **ok**.



EDIT SERVER

Server Type:	RADIUS ▼	Name:	Clearpass1
Radsec:	□	IP Address:	10.254.1.23
Shared Key:	••••••••	NAS IP Address:	optional
Retype Key:	••••••••	NAS Identifier:	optional
Retry Count:	3	Auth Port:	1812
Timeout (in secs):	5	Accounting Port:	1813

Click on **Next** at the bottom right of your screen.

You will leave the Access Rule as **Unrestricted**.

8. Click on **Next**.
9. Click on **Finish**.

NOTE: It is not advisable to have an unrestricted rule. In an IAP course the firewall will be explained.

10. Which IAPs will advertise this newly created WLAN?: ___________________

Step 2: Guest Networks

1. We will create a new Guest SSID. Click on the "**+**" sign to add in a new SSID.

2. In the general section add in the following information:

   Name: **Guest”P””<u>X”</u>** <- Note Note the “P” is your POD number and the “X” is your table number.

   Click on **Next**.

3. For the VLANs set the following:

   Select **Instant AP Assigned**

   Select **Internal VLAN**

   Click on **Next**.

4. For the security section set the following:

   Security Level: **Captive Portal**

   Captive Portal Type: **Cloud Guest**

   Guest Captive portal Profile: **default**

   Encryption: **disabled**

   Key Management: **Enhanced Open**

   Expand the **Advanced Settings** Menu

   Disable WPA3 Transition

   Click on **Next**.

5. We will leave the Access Rule as **Unrestricted**. Click on **Next**

6. Click on **Finish**.

   NOTE: Not advisable to have an unrestricted rule. In an IAP course the firewall will be explained.

Task 5.5: WLAN Services

Objectives

– You have VC network and you need to enable some service features.

Step 1: Services

1. Click on the Filter Icon and select the group **IAP-Group**
2. In the left menu select **Devices.**
3. Click on **Show Advanced** at the upper right side.
4. At the navigation tabs select **Services**.
5. Expand **AppRF** and set **Deep Packet Inspection** to **ALL**. You will need this in subsequent labs.

6. Click on **Save Settings** at the lower right side.

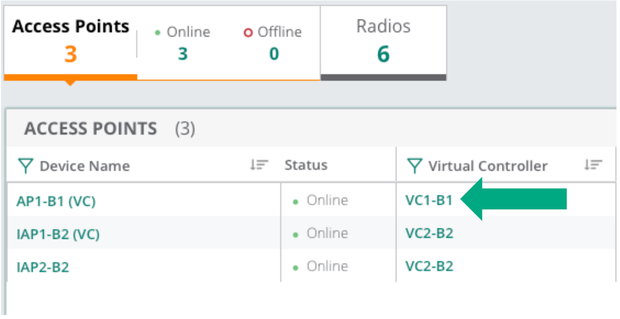
Task 5.6: WLAN Cluster Customization

Objectives

– You have both clusters advertising the SSID. However each cluster has its own VLANS. So right now, IAP1-B1 is advertising the SSID but is assigning the incorrect VLAN. You will make a modification on this cluster.

Step 1: Networks

1. Click on the Filter Icon and select the group **IAP-Group**
2. In the left menu select **Devices.**
3. Select the Virtual Controller **VC1-B1** in the virtual Controller column.



Access Points 3 | ● Online 3 | ○ Offline 0 | Radios 6

ACCESS POINTS (3)

Device Name	Status	Virtual Controller
AP1-B1 (VC)	● Online	VC1-B1
IAP1-B2 (VC)	● Online	VC2-B2
IAP2-B2	● Online	VC2-B2

4. Select the gear ICON for configuration.
5. In the navigation tabs select **WLANs.**
6. Select the network **employee”P””X”** and click on the **pencil**.
7. Click on **VLAN**.
8. Change the VLAN ID to **X2**.
9. At the bottom of the screen on the right click on **Save Settings**.

NOTE: Both IAP clusters are advertising the employee”P””X” SSID.

VC1-B1 cluster will place their users in VLAN X2.

VC2-B2 will place their users in VLAN X1.

Task 5.7: Switch Template

Objectives

– You have two switches in the same group. The group was configured as a template group. You will import a configuration as the first template.

Step 1: Adding a template

1. Click on the Filter Icon and select the group **Group-Switches-site1**.
2. From the **Context Scope Menu** on the left go to **Devices**.
3. From the Navigation tabs select **Switches**.
4. On the upper right side, click at **Configuration** icon ⚙.
5. You will be placed on the **Templates** page.
6. Click the **'+'** to add the first template.
7. In the POP up window select the following:
   a. Template Name: **First-switch-template**.
   b. Device: **Aruba Switch**
   c. Model: **2930F**
   d. Select your Part name **Aruba 2930F 24G PoE+ 4SFP+ switch (JL255A)**
   e. Click on **Next**
   f. Click on **IMPORT CONFIGURATION AS TEMPLATE**
   g. Select device to Import configuration: **Select one of your switches.**
   h. Add the following at the end of the template:

```
password manager plaintext Admin1
```

   i. Click on **Save**.

Task 5.8: Switch Configuration

Objectives

– You have imported a configuration. You will make modifications to the template.

Step 1: Modifying a template

1. In the Templates list select **First-switch-template** and click the **pencil** to edit.
2. Scroll down to see the Template and also click on Show Variable List to display the Template Variables on the right.
3. In the Template window add the following at the end of the template:

```
vlan
 name "vlan13"
 untagged 15
exit
```

4. Click on **Save**.

Step 2: Verify the Configuration

1. In the navigation tabs go to **Configuration Audit**.
2. Do you have any Failed/Pending Changes? ______
3. Click on the link Failed/Pending config changes.
4. Click on any of the two View Config Difference.
5. What is your invalid input line? ___________
6. What is the error? ___________________________
7. Click on **Close.**

Step 3: Fix the Configuration

1. In the navigation tabs go to **Templates**.
2. In the Templates list select **First-switch-template** and click the **pencil** to edit.
3. Scroll down to see the template and also note the Template Variables on the right.
4. The VLAN command you entered needs a VID value. In the template window change “vlan” for “vlan 13”.

```
vlan 13
 name “vlan13”
 untagged 15
exit
```

5. Click on **Save**.

   NOTE: you want to make sure that the configuration template is set up in the same format as you would see if you ran a “show running-config” command in the CLI of the switch.

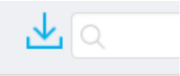
6. In the left-hand menu go to **Configuration Audit**.
7. Do you have any Failed/Pending Changes? ______. If you still have failed changes go back to the template and fix your error.

Task 5.9: Variable Configuration

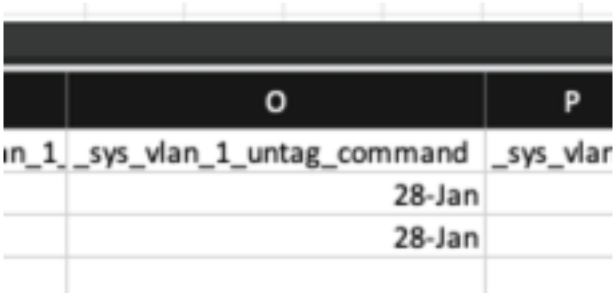
Objectives

– You now have a working template file, but the switches need different configurations. You will make modifications to the variables file to make per switch modifications.

Step 1: Modifying Variables

1. Click on the group filter button at the top left of the screen and choose "Group-Switches-Site1"
2. In the left-hand navigation pane, click "Devices"
3. In the navigation tabs, select "Switches"
4. Select the configuration gear in the top right corner to enter into the configuration context
5. In the navigation tabs go to **Variables**.
6. In the variables window click on the down arrow  to download the variables file in CSV format.
7. Save it in Excel.
8. Open the variable excel file.
9. In the _*sys*_hostname field change the names of the switches.
    a. For the first switch: **Aruba-2930F-Switch1**
    b. For the second switch: **Aruba-2930F-Switch2**
10. Change the modified field for both switches from "N" to "Y".
11. Save your excel sheet on your desktop as **SwitchVariable1.**
12. Check the Config status and make sure your switches are in Sync.
13. Click on the Configuration Audit to make sure all is good with your changes.
14. If not you may have to fix your CSV file.

Hint: Check the variable file for *_sys_vlan_1_untag_command.*



	O	P
n_1_	_sys_vlan_1_untag_command	_sys_vlar
	28-Jan	
	28-Jan	

The _*sys*_vlan_1_untag_command is not a date field.

Change this field to TXT format and replace 28-Jan with 1-28

15. In your Central account in the left-hand menu go to **Variables**.
16. Click on **Upload Variable File**.
17. Select your file **SwitchVariable1.**
18. In the variables list look at the variable **_sys_hostname.** There should be one entry for each switch. Has the name been changed on both switches?

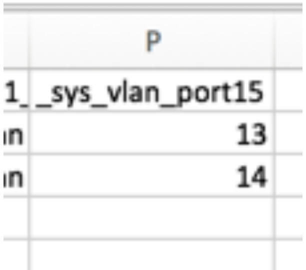
Task 5.10: Custom Variable

Objectives

– In this task, you will customize your variable file.

Step 1: Change the variable file

1. On your desktop open the excel file **SwitchVariable1.**
2. In the last vertical cell add in the Following:
    - **a. _sys_vlan_port15**
    - b. With a value of **13** for the first switch and **14** for the second switch.



	P
1_	_sys_vlan_port15
in	13
in	14

3. Save your excel sheet on your desktop as **SwitchVariable2.**

4. In your Central account in the left-hand menu go to **Variables**.
5. Click on **Upload Variable File**.
6. Select your file **SwitchVariable2.**
7. In the variables list look at the variable **_sys_vlan_port15**. There should be one entry for each switch.

NOTE: If your customized variable is not there then go back to your variable file. The cells should be in text format. Also, only underscores and no dashes.

8. Once you have confirmed you have the variables then proceed.
9. In the navigation tabs go to **Templates**.
10. In the Templates list select **First-switch-template** and click the **pencil** to edit.

You will now set the custom variable as the VID for the VLAN value. This will allow you to have different VID on different switches. You will also use this variable to give a proper name to the descriptive name field.

11. In the Template window make the following modification to the VLAN you added previously:

```
vlan %_sys_vlan_port15%
name "vlan%_sys_vlan_port15%"
untagged 15
exit
```

12. Click on **Save**.
13. In the left-hand menu go to **Configuration Audits**.
14. Do you have any Failed Changes? ______. If you still have failed changes go back to the template and fix your error.

Task 5.11: Verification of Configuration

Objectives

– You now check the configuration on the switches to validate your configuration.

Step 1: Verification

1. From the **Context Scope Menu** on the left go to **Tools**.
2. In the navigation tabs go to **Commands**.
3. Select **Switch** as device type.
4. Select both of your switches at the available devices.
5. Select **Management** under categories**.**
6. At the command box select **Show Config VLAN** and click on **ADD**.
7. Click on **Run**.
8. Click on Aruba-2930F-switch1: should have VLAN 1 and 13.
9. Click on Aruba-2930F-switch2: should have VLAN 1 and 14.

You have completed Lab 5

Managing Campus Networks with Aruba Central

Lab 6: VRF

You can use VRF for two purposes. You can plan the deployment of the RF coverture in new buildings. Once your network is deployed then VRF is used to show heatmaps, AP locations, and Client locations.

In this lab, you will setup VRF with a floorplan then add in the deployed APs.

Task 6.1: VRF Setup

Objectives

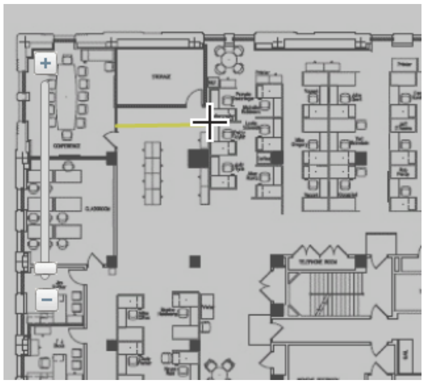
- In this task, you will create a campus, building and browse in a floorplan.

Steps: Login and verify devices

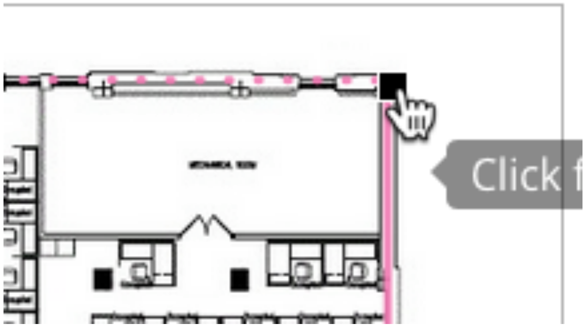
1. Open a browser page and get access to Central customer account.
2. Login with your assigned User ID and password.
3. In the Filter select you Site **Building1.**
4. From the **Context Scope Menu** on the left go to **Overview**
5. From the navigation tabs select **Floorplans**.
6. Click on **Add Floors** to add a new floor
7. Give a right-click on the background and select **New Floorplan**.
8. **Browse** in a **new floorplan** and **Save.**

NOTE: Use a floorplan from your own laptop, or download a floorplan from the internet.

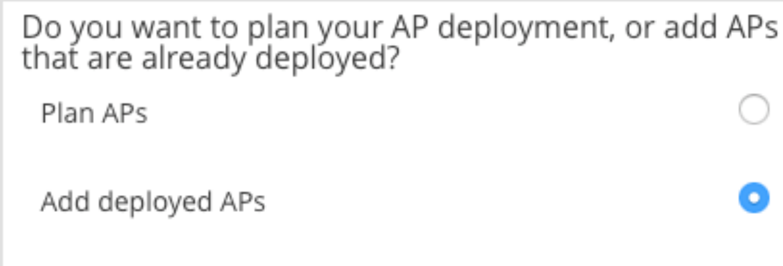
9. **Click** on **Measure** and a cross hair will appear. Move the cross hair to a wall click and drag the cross hair to another wall.



10. In the **Enter Distance** enter a value in feet. Try to be fairly accurate in your estimation.
11. Click on **Next**.
12. Click on **Define Planning Region.**
13. Move your mouse to one corner of the building.
14. Click on the **corner** then move your mouse to the **next corner**. Work your way around the building from corner to corner until you return to the original corner.
15. Click on the **black square box** to complete the region.



16. **Click** on **Next**.
17. If you had a CAD file with wall partition, simply click on **Next.**
18. In the Access Point window select **Add Deployed APs.**



Do you want to plan your AP deployment, or add APs that are already deployed?

Plan APs ○

Add deployed APs ●

19. **Click** on **Next**.
20. Select the radial button next to **Add Deployed APs**
21. Your deployed APs should appear in the **Deployed AP** box.
22. Click and hold one of your IAPs and drag it to a location on the floorplan.
23. Do the same and drag all the IAPs onto the floorplan.
24. Once all the IAPs are on the floorplan click on **Finish**.
25. Click on **Exit Edit Mode**

Proceed to Task 6.2

Task 6.2: VRF Heatmaps

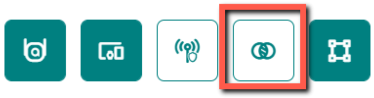
Objectives

- ~~In this task, you will create a campus, building and browse in a floorplan.~~
- In this task, you will learn about different view options such as, show APs, show clients, Heat maps, show rogues etc.

Steps: Login and verify devices

~~1. On the right-side menu bar click on **View**~~ ~~.~~

~~2. Click on **Heatmap**.~~

1. In the floor details view find the view buttons  and click on the **Heatmaps** button to view the heatmaps of the deployed APs to understand the coverage.
2. Click on the APs button to view/hide the APs on the floorplan
3. You can try other view buttons

NOTE: If you have no heatmap then you may need to wait a few minutes for updated information

---

3. Look at the coverage of your IAPs. Do these IAPs provide sufficient coverage for your building? Your report on the RF coverture will be sent to your co-worker who is attending an Aruba Design course this week.

You have completed Lab 6

Managing Campus Networks with Aruba Central

Lab 7: Troubleshooting

You now have a deployed network. You must now monitor and troubleshoot the network or client problems.

In this lab, you will associate your wireless and wired client. Then you will monitor the AP and client activity. You will then verify the network health.

Task 7.1: Associate your Wireless Client.

Objectives

– In this task, you will login to your wireless client and associate to your IAP network. You will also bring up an Ethernet port on the switch.

Step1: Associate your Wireless Client

1. In the remote lab dashboard, open the desktop to your wireless VLT2.
2. Associate your VLT2 wireless connection to the employee”P””X” SSID. Remember that “X” is your table number.
3. Use the following credentials:

   Username: test

   Password: aruba123
4. Start running browser traffic (e.g.: Go to YouTube).

NOTE: If you are not sure how-to setup wireless on a Windows 10 environment then go to Appendix 1.

Step2: View the Wireless Network

1. Login to your Central customer account with your assigned user ID and password.
2. Click on the filter Icon and select **Global**
3. From the **Context Scope Menu** on the left go to **Overview**.
4. From the Network Health page hover your mouse over one of the sites. Note the summation of information you can see.
5. From the navigation tabs, select **Summary.**
6. This is the main **Network overview** page for all devices in the network. Answer the following questions:

   a. What is the Usage In: ______ Usage Out:__________.

   b. Clients Count: ______
7. From the navigation tabs, select **Wi-Fi Connectivity .**
8. What is the percentage of:

   a. Associations: _______

   b. Authentications: ____________

   c. DHCP: ____________

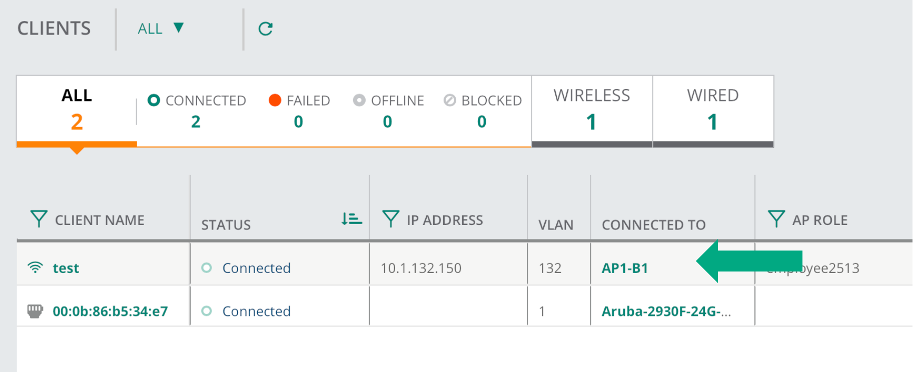
d. DNS: _____________

9. Are there any connection problems? _____________

Note: This would be much better in a network with more than 1 client.

10. From the **Context Scope Menu** on the left go to **Clients**.

11. Click on one of the IAP that has your client.



CLIENTS | ALL ▼ | ↻

ALL	○ CONNECTED	● FAILED	◎ OFFLINE	⊘ BLOCKED	WIRELESS	WIRED
2	2	0	0	0	1	1

CLIENT NAME	STATUS	IP ADDRESS	VLAN	CONNECTED TO	AP ROLE
test	○ Connected	10.1.132.150	132	AP1-B1	employee2513
00:0b:86:b5:34:e7	○ Connected		1	Aruba-2930F-24G-...	

12. The Overview page has information on the IAP. Look at the page and answer these questions on the state of the IAP:

a. What is the IAP IP address: ______________

b. What is the Configuration Status? _____________

c. Scroll down and what is the Health Status? ____________.

13. In the Menu bar click on **USAGE**.

14. In the Menu bar Click on **RF.**

15. In the **RF** graph, scroll your mouse over the highest utilization;

a. What is your highest Utilization %? _____________.

b. What is your Noise Floor in dBm? ______________.

c. What is you highest Frame Errors? ____________.

d. What is the Lowest channel quality? _____________

16. In the menu bar click on **Floorplan.**

a. The VRF map is displayed with the floorplan and location of the AP.

17. In the menu bar click on **AI Insights**

a. How many insights do you have? ______________.

18. In the Menu bar click on **Performance.**

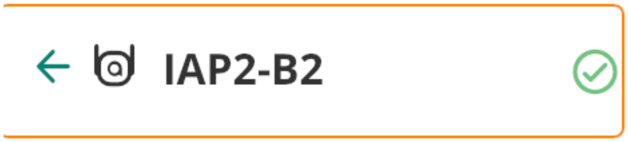
19. In the Throughput graph, scroll your mouse over the highest usage;

a. What is your highest Usage Sent? _____________.

b. What is your highest Usage Received? _____________.

NOTE: You may need to wait an hour or so for AI insights to provide any usage information.

20. From the **Context Scope Menu** on the left go to **Clients.**
21. Clear the device filter by clicking on the arrow **<-.**



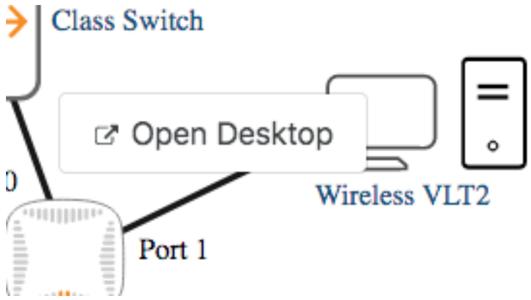
22. Select your client name from the list and answer the following questions**:**

a. Looking at all the charts, what is the status of your client? _____________.

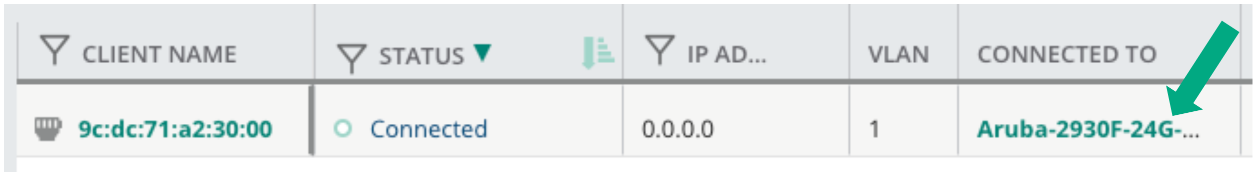
b. Any AI insight warnings: _____________

Step 3: View the Wired Network

1. In the remote lab dashboard, open the desktop to your wireless VLT2.



2. Enable your VLT2 wired connection to the switch.
3. Return to your Central customer account and from the Context Scope Menu on the left go to **Clients**.
4. **Click** on one of the switches that has the wired client.
5.



CLIENT NAME	STATUS	IP AD...	VLAN	CONNECTED TO
9c:dc:71:a2:30:00	○ Connected	0.0.0.0	1	Aruba-2930F-24G-...

6. The Overview page give you information about the switch.
7. Scroll down to **PORTS**.
8. Note the following information:

a. Ports Status UP: ___________.

b. Port Status Down: ___________.

c. Any Alerts? _____________

9. In the menu bar click on **Hardware.**
10. Do you see any problems with Power Supplies, Fans, Utilization or Temperature? _____
11. Any **AI Insight** warnings? ______________
12. Clear the device filter by clicking on the ← **arrow**.

Task 7.2: Network Health

Objectives

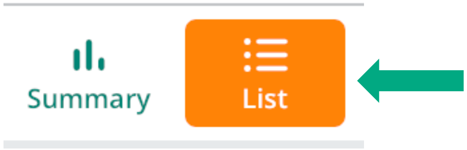
– In this task, you will monitor the network health.

Steps: Building Network Health

1. From the Context Scope Menu on the left go to **Overview** and choose **Network Health** from the navigation tabs**.**
2. In this window showing the buildings do you see any issues? ___________.

   a. If yes in what category:___________________.
3. In the map click on one of the sites and a site summation will pop up.
4. Do you see any issues? ________

   a. If yes in what category:___________________.
5. Click on **List** and click on **Building1**.



6. Answer these questions:

   a. How many AI Insight warnings: _______ Number of devices: ________ Clients:_______; is anything shown in red ?_______

Task 7.3: Applications Overview Page

Objectives

– In this task, you will monitor the applications in use in this network.

Steps: Client Overview

1. From the Context Scope Menu on the left go to **Applications.**
2. Answer these questions:

   a. **Application Category**: Highest category: ___________ Percentage: ______

   b. Select **Websites**

   c. **Web Reputation**:

   d. What category has the Highest Usage: ___________ Percentage: ______

   e. **Web Reputation**: Anything to be concerned about? _______

Task 7.4: Clients page

Objectives

– In this task, you will monitor the specific clients in this network.

Steps: Client Overview

1. From the Context Scope Menu on the left go to **Clients.**
2. List the values in these categories:

   a. Wireless: Connected: _______, Failed: _______ Offline: _______

   b. Wireless clients: ___________ Wired clients: __________

3. There is a list of clients. Look at your wireless client and answer these questions:

   a. What is the Client Status? _____________

   b. What is the Client Health? ___________

4. Look at your wired client and answer these questions:

   a. What is the Client Status? _____________

   b. The Clients is Connected to what switch? _________________

5. **Click** on the wireless client name.
6. Look at the top summation bar and answer these questions:

   a. What is the Client overall Health? ____________

7. Note the **Datapath** and status in each step:
   a. Client status: _________
   b. SSID Status: _________
   c. AP Status: __________
   d. Switch Status: ___________. Why is there no switch? ________________
   e. Look at the Client Info, the Network Info and the Connection Info. What are the Client Capabilities(Connection section)? _____________
8. Click **AI insight**, is there any warnings? _______________
9. Click on **Location**.
   a. What is the clients Building? _______Floor? _______
   b. Visually in what area of the floorplan is the client (eg: North side)? _______
10. In the left-hand menu click on the filter <- arrow.
11. **Click** on the wired client name. What is the clients port?: _________
12. Scroll down to Throughput. What is the highest Sent: _____ and Received; _______ usage.

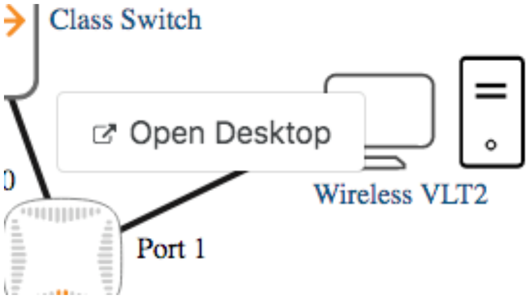
Task 7.5: Associate your Wireless client to the Guest network.

Objectives

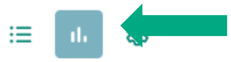
- In this task, you will login to your wireless client and associate to your Guest SSID. You will then verify the visitors on your network.

Step1: Associate your wireless client

1. In the remote lab dashboard, open the desktop to your wireless VLT2.



2. Associate your VLT2 wireless connection to the “Guest”P””X”” SSID. Remember that “X” is your table number.
3. Open a browser page. In the cloud captive portal, click “Sign in” to be authenticated onto the network
4. Once authenticated then start running browser traffic (e.g.: Go to YouTube).
5. From the Context Scope Menu on the left go to **Guests.**

6. From the navigation tabs select **Visitors.**
7. On the top right corner, select **Summary**
8. 
9. In the **Overview** page what is the number of:
   a. Guests: _________
   b. Guest SSIDs: ___________
   c. AVG. Duration in seconds: ____________
   d. Max Concurrent Connections: __________
10. Scroll down and look at the **Guest Count by Authentication, Guest Count by SSID, Client Type**.
11. In the top right hand menu click on **List**. Answer these questions:
   a. How long has this visitor client been associated: _____________ (look at Session time).
   b. Device Type: ____________
   c. OS Name: _______________

Task 7.6: Security

Objectives

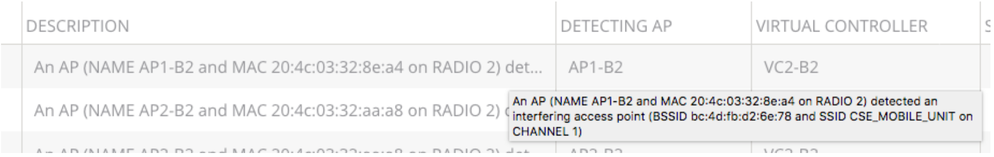
– In this task, you will monitor the security of your network.

Steps: Client Overview

1. Click on the filter Icon and select **Global**
2. From the Context Scope Menu on the left go to **Security.**
3. In the navigation tabs select **IDS**(**Intrusion Detection)**. Are there any detected attacks in your network? ________
4. In the navigation tabs select **Rogues.**
5. Do you have any detected **Rogues? ____________.** If yes look at one entry and answer these questions:
   a. First seen: ___________
   b. Reason for Classification: ______________________________
   c. Detecting AP: ______________
   d. Containment Status: _________________
6. Pick one of the interfering events and answer the following questions:

a. Detecting AP: ____________

b. Note for description you can place your mouse over the description to get the entire line.



DESCRIPTION	DETECTING AP	VIRTUAL CONTROLLER
An AP (NAME AP1-B2 and MAC 20:4c:03:32:8e:a4 on RADIO 2) det...	AP1-B2	VC2-B2
An AP (NAME AP2-B2 and MAC 20:4c:03:32:aa:a8 on RADIO 2)		

An AP (NAME AP1-B2 and MAC 20:4c:03:32:8e:a4 on RADIO 2) detected an interfering access point (BSSID bc:4d:fb:d2:6e:78 and SSID CSE_MOBILE_UNIT on CHANNEL 1)

c. What is the Interfering SSID name: __________

Task 7.7: Alerts

Objectives

– In this task, you will monitor and configure the Alerts.

Step 1: View existing Alerts

1. From the Context Scope Menu on the left go to **Alerts & Events**
2. How many alerts do you have in each category:
   a. Critical: ___________
   b. Major: __________
   c. Minor: __________
   d. Warning: __________
3. Click on the Critical Alerts (if you have any) or select Major Alerts.
4. The alert(s) are in what category? ___________________

You have completed Lab 7

Managing Campus Networks with Aruba Central

Lab 8: Application Visibility, Presence Analytics and Unified Communication

Now that the network is deployed you will be troubleshooting your clients. However, many times, it’s not a Wi-Fi issue but a back-end server issue. Clarity will indicate these types of issues. Application Visibility gives you an idea of the type of the traffic in your network. Presence Analytics is a great tool for businesses for trying to get an idea of customer patterns.

Now that the network is deployed you will be monitoring UC Clients. The Unified Communications dashboard provides a view of the voice and video traffic trends along with the desktop sharing sessions, for the devices that are provisioned in Central.

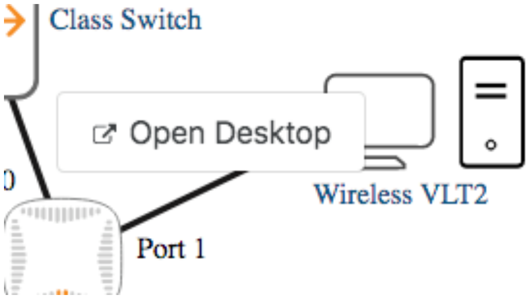
Task 8.1: Application Visibility

Objectives

– In this task, you will monitor the types of traffic in your network.

Step1: Associate your wireless client

1. In the remote lab dashboard, open the desktop to your wireless VLT2.



2. Associate your VLT2 wireless connection to the employee”P””X” SSID. Remember that “X” is your table number.
3. Start running browser traffic (e.g.: Go to YouTube).

NOTE: If you are not sure how to setup wireless on a Windows 10 environment then go to Appendix A.

Step 2: Monitor Applications

1. Open a browser page and get access to Central customer account.
2. Click on the filter Icon and select **Global**
3. From the **Context Scope Menu** on the left go to **Applications.**
4. What is the highest usage application? ____________
5. Click on **Websites**. What percentage or usage is trustworthy? __________
6. What **Category** has the highest usage? __________
7. Click on **Blocked Traffic**. Here you could select a group and download a CSV file of the blocked traffic. The IAP firewall will block all traffic.
8. Scroll back to the top of the page and click on the **Summary** 📊 .
9. Here you can see the Application listed in a bar chart and based on a timeframe.
10. Click on **Websites** and click on the Summary 📊 Icon**.**

Task 8.2: Wi-Fi Connectivity

Objectives

- In this task, you will see any issues with associations, authentication on the Wi-Fi network. You will also see any issues with external services such as the DHCP and DNS.

Step1: Wi-Fi Connectivity Activities

1. Your VLT2 should still be associated to the IAP and generating traffic. If not re-associate your VLT2 to an IAP and generate traffic.
2. From the **Context Scope Menu** on the left go to **Overview**.
3. From the navigation tabs, select **Wi-Fi Connectivity**
4. On the top of the page **(right corner)** select **Activity for the last 1 day**.

5. Answer the following questions:

   a. What is your Connectivity Health (CH) value (look under ALL)? _________

   b. What is the Attempts value (sum of all attempts)? _________
6. Scroll down to Stage-wise Performance and answer these questions:

   a. For Association, what is your Connectivity health percentage: _______

   b. For Authentication, what is your Connectivity health percentage: _______

   c. For DHCP, what is your Connectivity health percentage: _______

   d. For DNS, what is your Connectivity health percentage: _______
7. Is there any area of concern? ________________
8. Scroll down and look at Delay- Causes, Failure – Causes, Device Performance and Authentication Performance.

Step2: Insights

1. From the **Overview** tabs, select **AI Insights**.
2. How many insights incidences have you found?: __________
3. Have a look at the Insights. Do you see any patterns of issues?___

   a. If yes write the area of concern: ___________________
4. From the **Context Scope Menu** on the left go to **Clients**

5. Click on your client name.
6. In **Client** section select **AI Insights.**
7. Has this client had any issues? ________
   a. If so (pick one) what:
      i. Status? ______________,
      ii. and Reason? _____________,
8. Clear the client filter by clicking at the <- arrow at the top of the page.

NOTE: you may need to wait some time in order to generate some AI Insights

Task 8.3: Presence Analytics

Objectives

– In this task, you will monitor the behavior of your clients.

Step 1: Presence Analytics Settings

1. In the upper-right side click on **Config** ⚙.
2. Enable **“Enable all Access points to collect data for site analytics”.**
3. Edit Default Thresholds.
4. You see here that you can modify the settings.
5. Click on Cancel

Step 2: Presence Analytics Monitoring

1. Your VLT2 should still be associated to the IAP and generating traffic. If not re-associate your VLT2 to an IAP and generate traffic.
2. Click on the filter Icon and select **Global**
3. From the **Context Scope Menu** on the left go to **Guests**.
4. From the navigation tabs, Select **Presence Analytics**
5. In **Presence Analytic** note the following:
   a. Unique Passersby: ___________
   b. Unique Visitors; ___________
   c. Draw rate percentage: __________
   d. Avg Dwell Time: ___________
   e. Loyal Visitors: __________
6. For **Presence Analytics** select the **Summary** icon
7. Here the information is displayed in graph and bar chart form.

8. The store would like an analysis of the data you have collected. What would be your answer to this request?______________________________

Task 8.4: Unified Communication

Objectives

– In this task, you will login to your assigned central account and verify UCC subscription assigned to your devices.

Step 1: Verifying UCC Subscription assignment

9. Open a browser page and get access to the Central MSP account.
10. Login with the User/Password given to you. This is a read only User.
11. Click on the APP ICON .
12. Select the Subscription Assignment
13. Scroll down to ~~NETWORK~~ SERVICES MANAGEMENT SUBSCRIPTIONS.
14. Verify if your IAPs have been assigned a **UCC** Subscription.
15. You can select your IAP and see what services have been assigned.

NOTE: You can find your IAPs based on the MAC address.

16. If your IAP have not been assigned UCC licenses then drag your IAP to the UCC subscription. This will assign the UCC service to your IAP.
17. On the upper right click the little person ICON and Logout from the MSP account and get back into your student account.

Step 2: Monitor a UCC call

Objectives

– In this step, you will make a Skype for business call and monitor call quality at UC application.

Steps: Associate your wireless client and make a S4B call

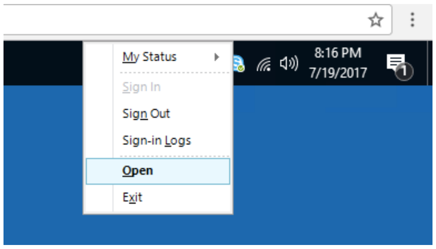
1. From the Live Labs Dashboard: click on Wireless VLT2 to open a new browser...
2. Select **Network Settings** at the bottom

3. In settings click on **Ethernet**
4. Click “**Change adaptor options**”
5. Ensure **“IAPX**” and **Switch ~~1~~** are disabled.
6. Close the windows
7. Click on the **Network connectivity** icon
8. Associate your VLT2 wireless connection to the employee47”X” SSID. Remember that “X” is your table number.

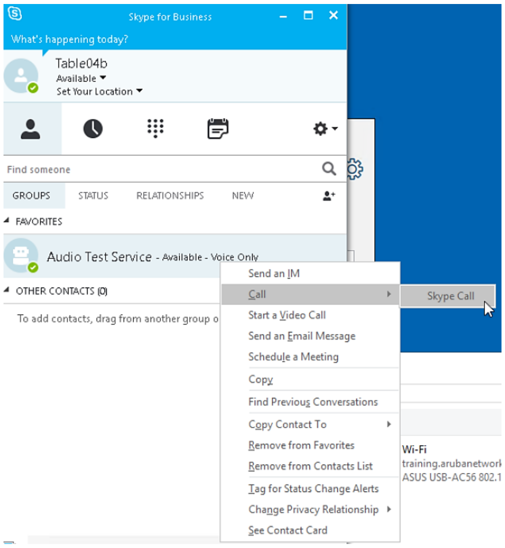
NOTE: If you are not sure how-to setup wireless on a Windows 10 environment then go to Appendix 1.

---

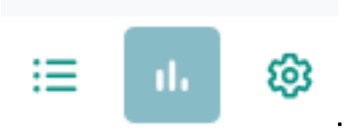
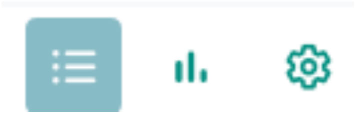
9. Associate your VLT2 wireless connection to the employee”P””X” SSID. Remember that P”is your POD number and “X” is your table number.
10. Open the **Skype for Business** application.



11. Right click on “**Audio Test Service**”, then choose “**call” → “skype call**”
12. Repeat Step 11 multiple times to make several calls to the in-built test user.
13. If you receive a warning from the **windows firewall** accept it



Step 3: UCC Activity

1. Open a browser page and get access to Central student account.
2. Login with your assigned User ID and password.
3. Click on the filter Icon and select **Global**
4. From the side menu select the Applications(Top right corner)
5. On the top menu bar select UCC.
6. Answer the following questions:
   a. How many calls have been made?____________
   b. How many calls are
      i. Good: ______
      ii. Fair: _______
      iii. Poor: _______
      iv. Unknown: ___________
7. For the last call on the top of the chart answer these questions:
   a. What is the client health? ________________
   b. What is the Protocol Used? __________
8. Select the **Summary** Icon on the top right side.  .
9. Here you have the Health chart for all the calls Made.
10. Click on the Calls Health drop down menu and you can filter the calls based on what 6 categories?
    ______________, _____________, _____________, ____________,
    ______________, ______________.
11. On the bottom charts, you have Access Points and Clients.
    a. Access Point can be filtered by what 2 categories? __________, _________.
    b. Clients can be filtered by what 2 categories? __________, _________.
12. Click on the List Icon 

Now we will select a specific client to view.

1. Click on the MAC address of your first call.
2. In the Client information what is the Manufacturer? ____________
3. What is the Device OS? _________________
4. In the Sub Menu select UCC

    a. Under Calls CLIENT HEALTH you see a chart for the calls made by this user and you can see how many of those call were Good, Fair, Poor or Unknown.

    b. Scroll your mouse over one of the dots and answer these questions:

        i. What is the from address? ___________

        ii. What is the TO address? ___________

        iii. What was the duration of the call? ___________

    c. From the Calls drop down menu select Sessions Type.

    d. What is the session type? ________

    e. For the Calls drop down menu select Quality.

    f. What is the quality of the calls? ______________

5. Is there any areas of concern? _______________

You have completed Lab 8.

Managing Campus Networks with Aruba Central

Lab 9: Administration and Maintenance

Now that the network is deployed you have some Administrative tasks to complete. Also a few maintenance tasks to keep the OS level constant in your network. You want to generate reports to get information on the network.

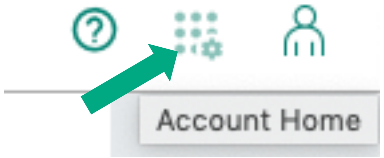
Task 9.1: Users and Roles

Objectives

- In this task, you will assign a User with a role created by the MSP admin account.

Step 1: Create a User

1. Open a browser page and get access to your Customer Central account.
2. Click on **Account Home** on the top right corner.



3. Under **Global Settings** Select **Users and Roles.**
4. Click on **Roles**.
5. Look for your Role **Reports-Only** has been pushed down from the MSP account to your Central account. All the other student roles are there as well.
6. **Click** on the **Users.** At the bottom of the page click on **Add User.** Enter the following information:

   a. Username: (**Your email address**).

   NOTE: The domain must be one of the following: arubanetworks.com hpe.com gmail.com hotmail.com outlook.com. If you don't have one then go create one.

   b. Description: **For Reports.**

   c. Language: **English** (or your native language).

   d. Account home: **Readonly.**

   e. Network Operations: **Reports-Only.**

   f. Select Groups: **All Groups**

   g. **Click** on **Save**

7. **Click** on the person Icon at the top right-hand side of the GUI page.
8. **Logout**.
9. In the login page login with your email address and your password.

10. What can you do in this account?______________________
11. What is barred for this account: ______________________
12. Logout and Log back in as administrator with your original U/P.

Task 9.2: Reports

Objectives

– In this task, you will create new reports to give information about the network.

Step 1: Reports

1. Open a browser page and get access to Central customer account.
1. From the **Context Scope Menu** on the left go to **Reports.**
1. Click on **Create**.
2. Report Type: **AppRF**, click **Next.**
3. Select **Groups** and select your IAP group, click **Next.**
4. Period: **Custom range**
    a. Start date: **First day of your course.**
    b. End Date: **Today's date.**
    c. Click **Next**
5. Recurrence: **One Time (Now)**
6. Title: **Applications on IAP**
7. Click on **Generate**.
8. In the Configured report section, you can see your report Running. Soon the report will be in the Generated Reports section.
9. In the Generated Reports section click on your report **Applications on IAP.**
10. Scroll down and have a look at the report.

11. Export this report to a PDF file by clicking on the PDF icon PDF at the top.
12. On your laptop Open the **Applications on IAP** PDF file. How many pages do you have: _______

Task 9.3: Firmware Verification

Objectives

– In this task, you will verify the current OS levels of the devices.

Step 1: Firmware

1. From the **Context Scope Menu** on the left go to **Firmware.**
2. In the Firmware page answer these questions:
   a. What is the Access Points firmware version: ___________
   b. Recommended: _______________
   c. Upgrade status: ________________
   d. Compliance Status: _______
3. Click on **Set Compliance** green wheel.
4. Here you could select what group would require specific OS levels.
5. Click on **CANCEL** **---- DO NOT CHANGE the IAP OS -----**

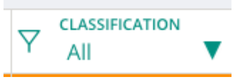
Task 9.4: Audit trails and API Gateway

Objectives

– In this task, you will verify Audit information and look at the API parameters.

Step 1: Audit trail

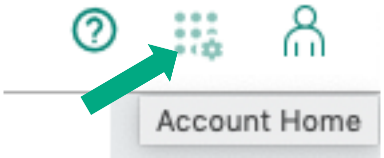
1. From the **Context Scope Menu** on the left go to **Audit Trail.**
2. What is the date and time of the last event: _________
3. In what category: _____________
4. Click on Category Title

.
5. Click on the green arrow 

to display the menu choises.
6. Select **Device Management**.
7. What is the date and time of the last Device management event: _________
8. What user made this Device Management event: _____________

Step 2: API

1. Click on **Account Home** on the top right corner.



2. Under Global Settings select **API Gateway**.
3. This is where you could investigate your API Apps and Tokens.
4. API is beyond the scope of this course.

Proceed to Task 9.5

Task 9.5: Certificates

Objectives

- In this task, you will audit the present certificate

Step 1: Audit trail

1. From the **Context Scope Menu** on the left go to **Organization.**
2. From the navigation tabs, select **Certificates.**
3. Answer these questions:

   a. What is the Certificate name? __________

   b. What is the Certificate Status? ____________

   c. What is the Certificate Expiry Date? ___________
4. What would you recommend: ______________

You have completed Lab 9