Wireless Networks
LAB 2: VAP Configuration with Open Security

Student Name (Please Print):_____ Annotated for Lab sect 011 http://michaelanderson.ca/20S-CST8304/

Controller Number:__**X =**____ Check BrightSpace grades for your assigned PC & Controller. This is your "X".

1 Objectives:

- Configure an AP Group to support Access Points with Open Authentication
- Configure the corresponding VAP and SSID
- Purge the AP configuration
- Use the GUI to install an AP
- Connect a wireless station to the SSID and verify the connection
- Questions
- Sign-off

2 Notes:

1. The Value **X** is your Controller ID. Substitute your Controller ID for **X** in this lab. For example, your Controller ID = 4 and your IP address is 10.1.**X**0.100. This address translates to 10.1.40.100.
2. This Lab must be completed by the beginning of your next lab period. 2pm Jun 8
3. Complete the Brightspace Lab assignment by ~~the beginning of your next lab.~~ Jun 4 @ 11:59pm

3 Lab Procedure

Review the Background slides for this lab. Review the Configuration guide for the required profiles.

3.1 ~~Connect the Serial (Green) and Management (Red) Interfaces~~ S20 - already done

3.2 Reset to Factory Default (if not already done) and run setup script.
<Ctrl-X> to restart setup questions from the beginning!

3.3 Upload your initial configuration (lab 1), enter write mem and reload to activate your initial configuration. This is the starting point for the following configuration.

3.4 Verify that the licenses are correctly installed and enabled.

WRITE A SCRIPT TO CONFIGURE THE FOLLOWING STEPS.

You must write a configuration script in Notepad first. Please save this configuration script. You may need this for the Brightspace Lab assignment and future labs.

All configuration commands must be entered in global configuration mode. Use the "config t" command.

NOTE: Please read sect 3 (2nd half) and **Sect 4 of the Config Guide** for info on all the commands required for this section!

3.5 Disable Control Plane Security - CPsec

3.6 Create a VLAN for Employee Users

The VLAN ID=X1. Wireless-connected users are placed on this VLAN. Add the following description to this VLAN: Employee. The user gateway is on the Cisco switch and is already configured. Wireless devices will receive their IP configuration from the DHCP server on the Cisco switch.

3.7 Add the Employee VLAN to the Trunk on Port gi 0/0/0.

This will allow the user to reach their gateway on the switch.

Define the following Profiles in your script.

3.8 Create the AAA profile. (Item 1B; sect 4.4)

The AAA profile is named open-aaa-profile.

Since the SSID uses open security (i.e. no security), only the default values are used. Only the initial-role needs to be configured. The Initial-role is "authenticated". This is a predefined role. No other parameters are configured.

Deceptively simple in this lab!

3.9 Create the SSID profile. (Item 1A; sect 4.3)

The ssid profile is named open-ssid-profile.

Your SSID name is "Open-**X**". Aruba calls this the essid-name.

~~No other parameters are used.~~ You also need to define the opmode (see Lab background)

3.10 Create a VAP profile. (Item 2; sect 4.2)

The VAP profile is named open-vap-profile.

Link the ssid profile and aaa profile to the VAP.

Configure the vlan as the Employee VLAN.

3.11 Create the AP Group profile. (Item 3; sect 4.1)

The AP Group is named APGroup**X.**

Link the your VAP profile to the AP Group.

3.12 Enter and Debug Your Script

Your script is now complete. Review it for errors.

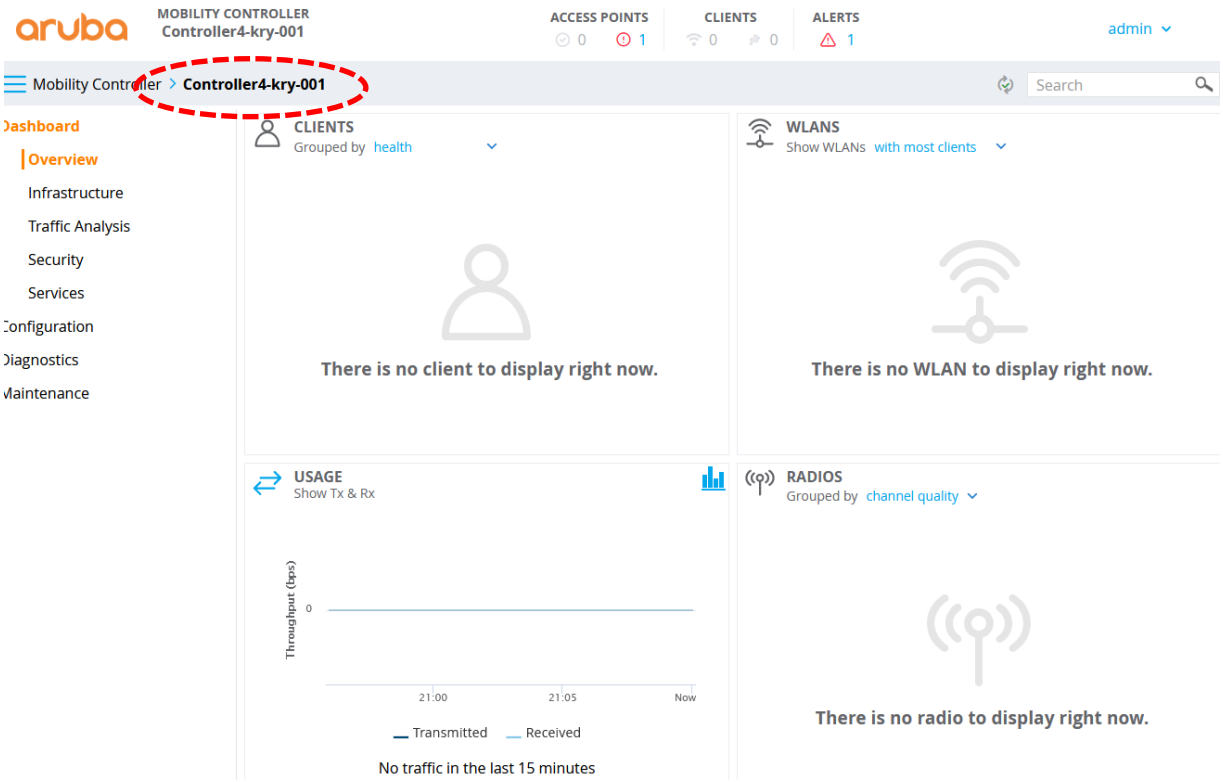
ALL required CLI config for the **Controller** is *done*, so this is the "1/2 way" point. Configuring the **AP** will be done via the Controller GUI.

Using the serial interface, enter Global Configuration Mode. Copy the commands from your script into PuTTY. Only enter a few lines at a time (i.e. commands for 3.7, 3.8, etc.)

If you have errors correct the script and re-enter the code.
If it is error free, return to Privileged EXEC mode and save using write mem. DO NOT RELOAD.

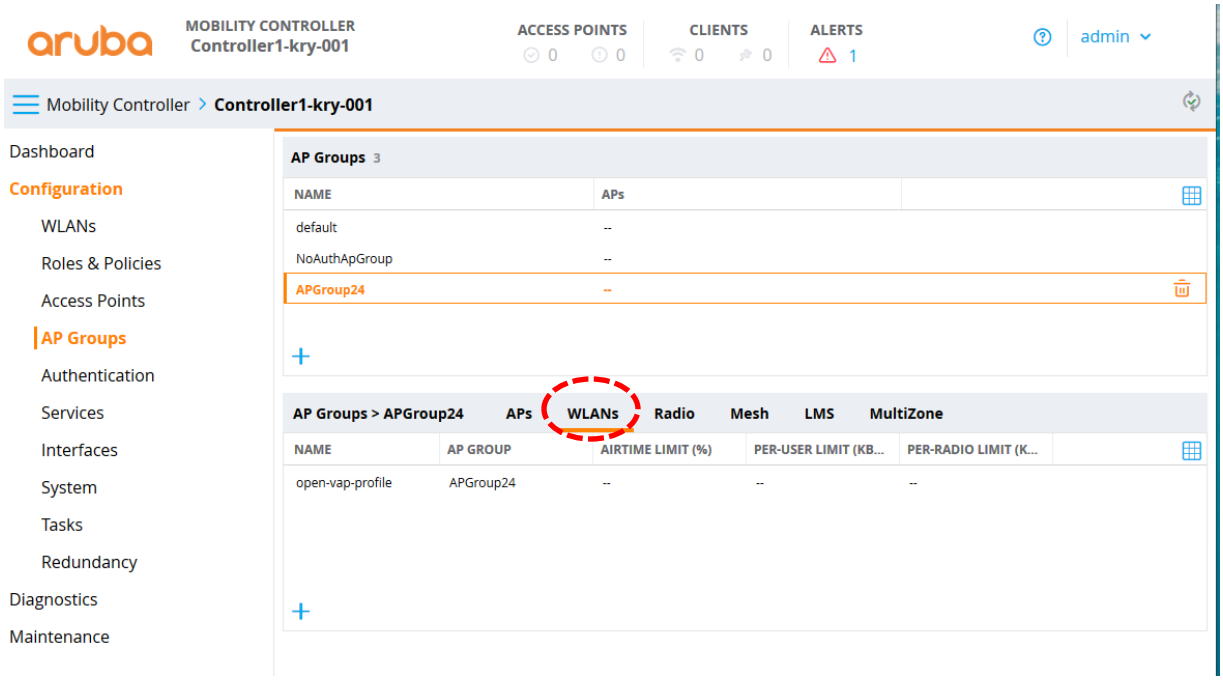
3.13 Review your configuration using the GUI.

a) Connect to your controller via GUI. You will see a screen like this.

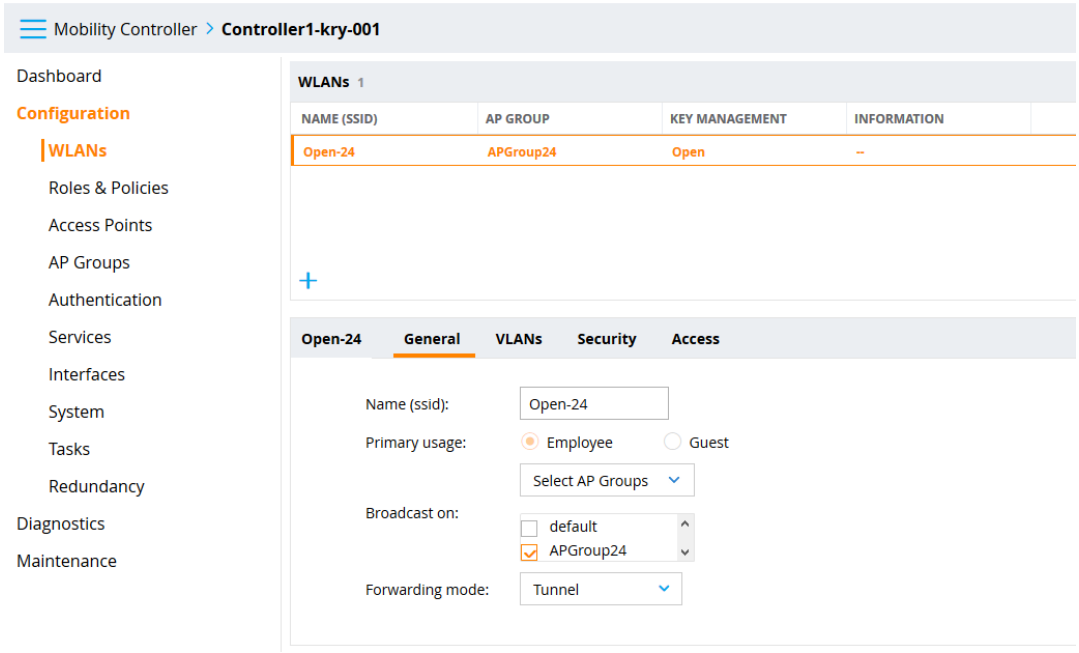


b) Verify that your controller system name is showing – see dotted oval.

c) Click Configuration and then click APGroup. Then click on your APGroup, APGroupX. Then click on WLANs shown in the dotted circle. You will see a screen like this. Your VAP should be listed. If you do not see this screen, then you may have a configuration error.



d) Next we look at the VAP details. The VAP includes the configuration for (i) the SSID, (ii) the VLAN and (iii) identify the security policy. To see these details go to Configuration>WLANs. Then click on your SSID. You will see a screen that looks like this.

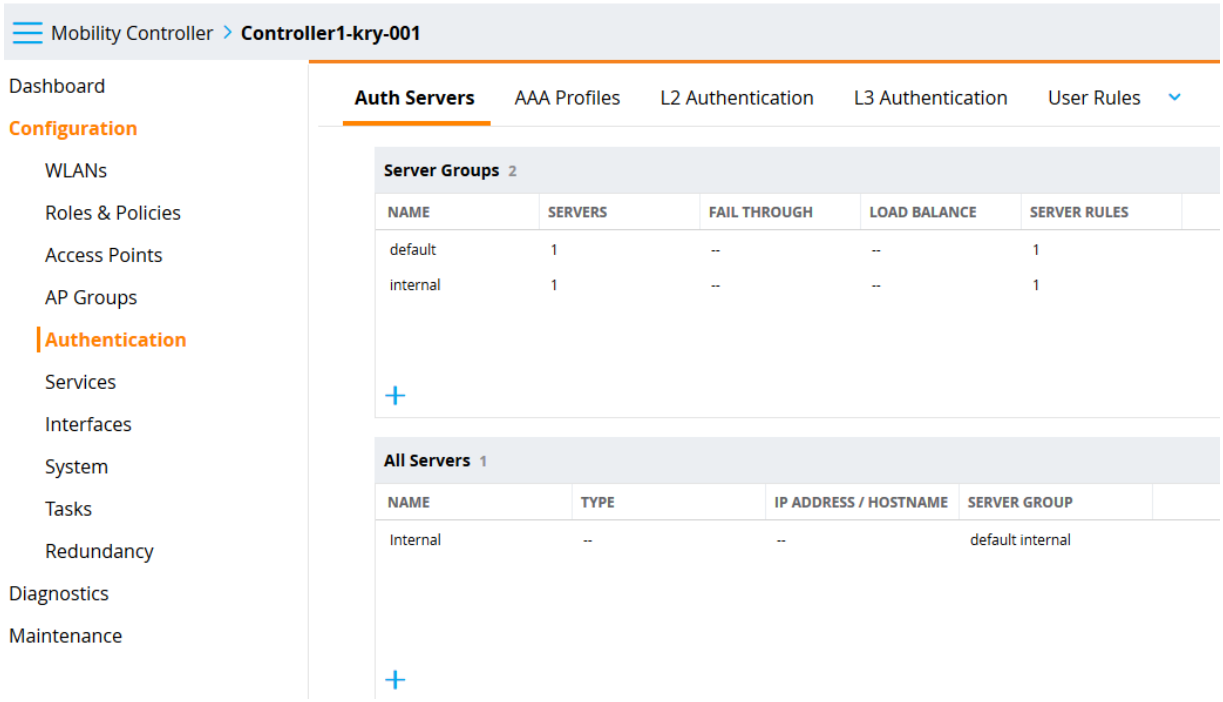


Note the SSID name, the APGroup to which this VAP belongs and the Forwarding mode. You will learn more about forwarding modes later in the course.

e) Now click on the VLANs tab. Here you will see the VLAN for your VAP. If it is not correct you may have a configuration error.

f) Next click on the security tab. Here you will see that the VAP has open security. This means that there is no security configured. You will learn more about the other security methods Enterprise and Personal late in the course.

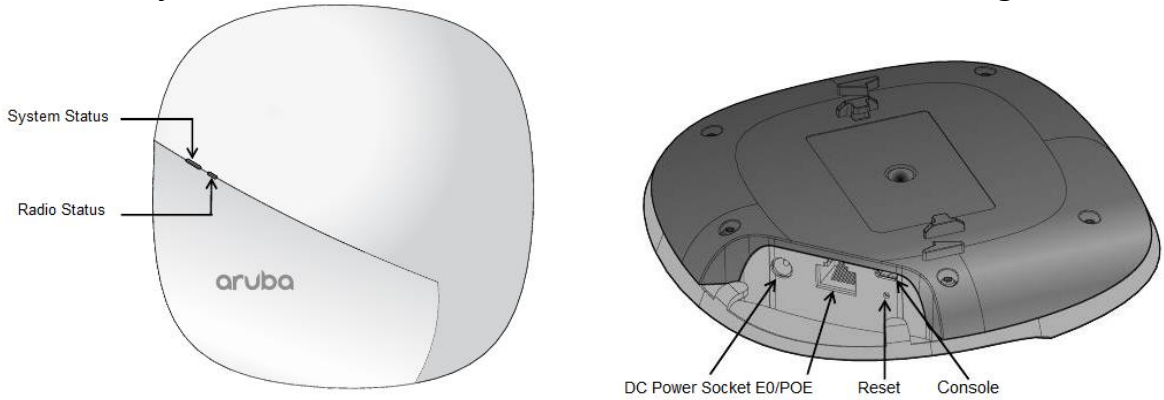
g) Now we will look at the authentication security details. Go to Configuration > Authentication. You will see a screen that looks like this.



Note the tabs at the top of the screen. The AAA profile is a container profile which groups the authentication details such as “Auth Server” and “L2 Authentication” details. This will be covered in more detail later in the course.

3.14 Purge the Access Point

For this lab you will use the AP303 Access Points as shown in the diagram below.



For this lab we will only use the PoE ENET port and Console port. ~~To reset your Access Point, use the orange console cable. The micro USB end will plug into the AP. The USB end plugs into your PC.~~ 20S: pre-cabled

Open a serial connection using PuTTY to the AP. Use Device Manager to determine which COM port to use. ~~Power on the AP by connecting the Ethernet cable to the Access Switch via the blue patch panel on your desk.~~
Ask the Lab Professor to power-cycle the AP when you're **already** connected via Putty.

Click Enter when asked to stop the autoboot process.
Enter the following commands:
purge
boot

Look for: "Hit <Enter> to stop autoboot"
Quick! You only have 2 secs!!

The Access Point will now boot normally.
Do not proceed to the next step until the AP completes it boot.
Note: Human admins don't/can't use a password to log in; config is done via the Controller GUI.

3.15 Configure the Installation of your Access Point

See Aruba Configuration Guide. **Section 2.5**, and the "Lab 2 Background" slide deck.
Note: Monitor the AP via the Putty serial connection.

DO NOT disconnect the NIC used for RDP access!

3.16 Connect your PC to the SSID.

Disconnect your PC from the controller GUI interface and enable the PC's wireless NIC. Connect your PC using Wi-Fi to your SSID. You may also use your own laptop. Verify connectivity by pinging your user gateway at 10.1.**X**1.1 and the controller gateway at 10.1.X0.1. These should be success

Note: Good 'ol MS-Windows; you may need to disable & re-enable Wifi to see your AP.

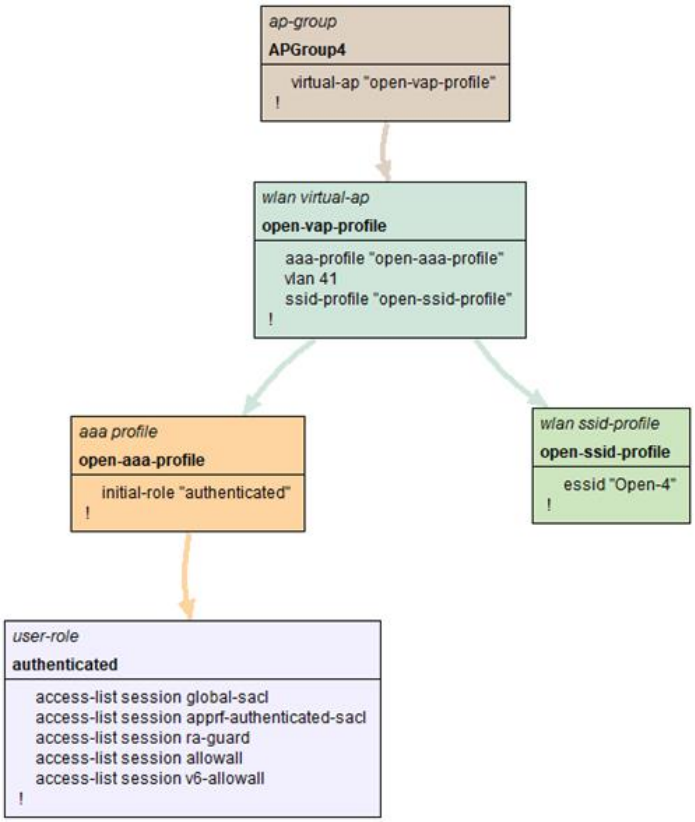
3.17 View your configuration using VisualCFG

Disable the firewalls on your Management station. Copy your running configuration file to your Management Station. Name your configuration file backup.cfg. The copied file will be found on your PC in the folder c:TFTProo. Open the configuration file using VisualCFG and display your AP-Group. You should see a diagram of your profiles, which will look like the following diagram.

Use the wifi addr!!

Please see **sect 2** of the Config Guide for info on commands for the Aruba controller.

– For a TFTP server, download Win64 version from:
http://tftpd32.jounin.net/
(I used the "portable edition"; just unzip & run; no installation necessary)
– Start the server
– WATCH for any popup asking whether the firewall should allow access;
if you see this, make sure you ALLOW access.
- In the server window, CHECK where/what directory is the destination for files so you know where to find your config file afer transferring.



4 Questions

Reconnect your serial interface to your controller and PuTTY to the controller to answer the following questions. You should learn these commands which you will need for

4.1 What is your user IP address? The Address should be in the following subnet: 10.1.**X**1.0/24. You many need troubleshooting commands from Lab 1.

4.2 Use a show command to display the controller IP address. Verify that it is correct.

4.3 Use the show command to verify the default gateway. Verify that it is correct.

4.4 Use a show command to list the tunnels. Use the following table to identify the tunnels types listed.

8000 -- shared split tunnel

8080 -- 651/653 internal AP FW
8180 -- Ethernet port 0
8100 -- Ethernet port 1
8101 -- Ethernet port 2
8102 -- Ethernet port 3
8103 -- Ethernet port 4
82x0 -- BSSIDs on radio 0
83x0 -- BSSIDs on radio 1
9000 -- Base-tunnel for heartbeats/keepalives
IPSE -- IPsec map

4.5 Use a show command to show the connected user. Based on this information what are the ESSID, BSSID and PHY Type?

4.6 Use the show command to show the configured VLANs. Verify that the VLANs are associated to the correct ports.

4.7 Use the show commands to show the port status. Verify that port gi 0/0/0 and gi 0/0/1 are correct.

4.8 Use a show command to show the BSSIDs. List the BSSIDs for your configuration.

5 Demonstration and Signoff:

5.1 1. Answer the questions in your lab notebook.

5.2 2. Demonstrate step 3.15 and 3.16 to your lab instructor.

5.3 A copy of your script has been placed in the Dropbox on BrightSpace and saved on your memory stick. You will need it for future labs and your lab exam.

5.4 Instructor signoff_____

6 Cleanup:

6.1 RESET the controller to factory default. Use CLI "write erase" and enter. Enter y when asked to proceed and then enter. You do not need to wait for the reload to complete.
See example below:

(Controller24-kry001) [mynode] #**write erase**
All the configuration will be deleted and the controller will be reloaded.
Press 'y' to proceed : [y/n]: **y**
Write Erase successful

System will now restart!

6.2 ~~Clean up your cabling. Be careful not to disconnect a neighbour controller.~~
Note: Omit for 20S