Wireless Networks
LAB 3: MAC and PSK Security

Annotated for Lab sect 011
http://michaelanderson.ca/20S-CST8304/

Student Name (Please Print):_____

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

1 Objectives:

- Configure an AP Group to support 2 VAPs; one with MAC Authentication and one with PSK (Pre Shared Key) Authentication
- Configure the corresponding VAP, AAA and SSID profiles
- Use the GUI to install an AP
- Connect a wireless station to the each of the SSIDs and verify the connection

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 Post-Lab assignment by ~~the beginning of your next lab.~~ Jun 11 @ 11:59pm

3 Lab Procedure

Complete 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.

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

Log into your controller using the seral connection.
(Configure PuTTY for **9600 baud, 8 bits, No parity, 1 stop bit and flow control Xon/Xoff**.)

~~Connect the Management Ethernet Cable (red) to the management port on the controller. Configure your PC's internal NIC (RED) to use DHCP.~~ 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), save and reload activate your initial configuration.

This is the starting point for the following configuration.
You must reload the controller to set the Controller IP address.

3.4 Verify that the licenses are correctly installed and enabled. See Config Guide.

WRITE A SCRIPT TO CONFIGURE THE FOLLOWING STEPS.
All configuration commands must be entered in global configuration mode. Use the "config t" command.

3.5 Disable Control Plane Security - CPsec (Repeat from Lab 2)

3.6 Create a VLAN for Employee Users (Repeat from Lab 2)

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. (Repeat from Lab 2)

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

Configure the Virtual Access Point (VAP) with MAC Authentication.

3.8 Create a MAC Authentication profile

The profile is named mac-auth-profile.
Set delimiter to none and case to upper.

3.9 Create a Server Group

The Server Group is named mac-local-server-group.
The server group will contain 1 server which is the Internal server.

3.10 Create an aaa profile to be used with MAC Authentication.

The aaa profile is named mac-aaa-profile.
The initial role is logon.
Create a link to the authentication-mac profile.
The MAC default role is "authenticated".
Create a link to the mac-server-group profile.

Similar to Lab 2: create a hierarchy of profiles, including:
1B: aaa profile
1A: SSID profile
2: VAP profile
3: AP Group profile (next page)

3.11 Create the SSID profile to be used with MAC Authentication.

The ssid profile is named mac-ssid-profile.
The SSID name is "MAC-**X**".
The opmode is opensystem

3.12 Create a VAP profile to be used with MAC Authentication.

The VAP profile is named mac-vap-profile.
Link the ssid profile and aaa profile to the VAP.
Use VLAN **X**1.

A VAP with PSK Authentication is configured next.

Similar to Lab 2: create a hierarchy of profiles:
1B: aaa profile
1A: SSID profile
2: VAP profile
3: AP Group profile

3.13 Create a aaa profile to be used with PSK Authentication.

profile name: psk-aaa-profile
The initial role is "authenticated" (predefined)
Create the following psk profile links.
Link to the authentication-dot1x with profile name "default-psk". This is predefined profile.

3.14 Create the SSID profile to be used with PSK Authentication.

The ssid profile is named psk-ssid-profile
The essid name is "PSK-**X"**
The wpa passphrase is passwordX.
The opmode is wpa2-psk-aes.

3.15 Create a VAP profile to be used with PSK Authentication.

profile name: PSK-vap-profile
Link the ssid profile and aaa profile to the VAP.
Use VLAN **X**1

3.16 Create the AP Group.

profile name: APGroup**X**
Link both of your VAPs to the AP Group.

3.17 Enter and Debug Your Script

Your script is now complete. Review it for errors.
Login to your controller SSH and enter Global Configuration Mode.
Copy your script into puTTY, one section at a time.
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"

3.18 Review your configuration using the GUI. This was explained in Lab 2.

3.19 Add your wireless device's MAC address to the Internal server

See background slides.
For user name enter the MAC Address of your PC.
For user password enter the MAC Address of your PC.

Hopefully you know how to get the MAC. If not, there's at least 3 options:
– C:\>ipconfig /all
– C:\> netstat -rn
– GUI: wifi adapter Properties, then hover mouse over adapter name

3.20 Connect your Access Point as follows:

Purge your Access Point.
Connect your Access Point by provisioning an AP name and AP Group.

3.21 Test both VAPs as follows.

a) MAC SSID:
Disconnect your PC from the controller GUI (i.e. red cable)
Connect your PC to the MAC SSID.
From the CLI run the command "show user". Verify that the role is authenticated and aaa profile is your MAC profile. If the role is logon then the user was not authenticated and you need to troubleshoot.
Verify connectivity by pinging your user gateway at 10.1.**X**1.1.

You can clear a user session with:
aaa user delete <ip addr>

b) PSK SSID:
Connect your PC to the PSK SSID.
Enter the passphrase when prompted.
Enter "show user" to verify the role (authenticated) and aaa profile as your PSK profile.

Windows 10 problems again: If you get the message "Can't connect to this network" then in Windows go to Network settings, Wifi, Manage known networks, and manually add the PSK network.

3.22 View your configuration using VisualCFG.

You should be able to see both VAPs in the AP Group as shown in Background slides.

20S: Reminder - you'll need to TFTP your running config to the PC; you may need to install & run TFTP32 (see Lab 2); you'll definitely want to **completely DISABLE** the windows firewall.

4 Questions

Connect to your controller using SSH and answer the following questions.

4.1 How many GRE tunnels were created to support your 2 SSIDs? Why?
You can use the troubleshooting command to list the tunnels.

List to Tunnel Types:

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

2 options:
(a) remove the MAC credentials on your controller via GUI or CLI (*local-userdb del username <macaddr>*); or
(b) work with a classmate and use their VAP

4.2 Attempt to connect to MAC-X with a device whose MAC address is not in the internal database. Use a troubleshooting command to identify the role. Connect with a device whose MAC address is in the database and use the "show user" command to identify the role. What role is assigned in each case? Why are the roles assigned to the user different?

4.3 Use a show command to the list the BSSIDs. How many BSSIDs do you have? Why?

4.4 Record the ESSID, BSSID and PHY Type for each of your SSIDs?

5 Demo and Signoff

5.1 Answer questions in your lab notebook.

5.2 Demonstrate steps ~~3.22 and 3.23~~ 3.21 and 3.22 for both VAPs.

5.3 Explain your answer to 4.2.

5.4 A copy of the script has been saved on your memory stick. You will need it for future labs and your lab exam.

5.5 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 S20