

# Wireless Networks

## LAB 4: 802.1X-PEAP

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 a VAP to support 802.1X Authentication
- Configure the corresponding VAP, AAA and SSID profiles
- 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.X0.100. This address translates to 10.1.40.100.
2. This Lab must be completed by the beginning of your next lab period. 2pm Jun 15
3. Complete the Brightspace Lab assignment by ~~the beginning of your next lab.~~ Jun 18 @ 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 serial 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.

- 3.8 Create a RADIUS Server Configuration  
The RADIUS server name is radius1-server.  
The RADIUS server IP address is 10.254.1.21.  
The security key is aruba-ctl-pw.

These 3 section (Server, Svr Grp, and Dot1x auth) are the real new stuff for this lab.

- 3.9 Create a Server Group  
The Server Group is named radius1-server-group.  
Link the server you created to the server group.

- 3.10 Create a dot1x Authentication Profile.  
The name of profile is dot1x-auth-profile. Only the default parameters are used. Therefore there are no other CLI commands required.

- 3.11 Create an aaa Profile.  
The name of the profile is peap-aaa-profile.  
The initial role is logon.  
Link the dot1x-authentication profile you created.

Notice the pattern of configuring these 4 sections (aaa, SSID, VAP, AP grp). We started this in Lab 2....

The dot1x-default-role is authenticated.  
Link the server group that you created.

### 3.12 Create the SSID profile.

The name of the profile is peap-ssid-profile.  
Your SSID name is "PEAP-**X**".  
The opmode or security-mode is wpa2-aes.

### 3.13 Create a VAP profile.

The name of the profile is peap-vap-profile.  
Link the aaa profile that you created.  
Link the ssid profile that you created.  
Use VLAN **X1**

### 3.14 Create the AP Group.

The AP Group is named APGroup**X**  
Link your VAPs to the AP Group.

### 3.15 Enter and Debug Your Script

Your script is now complete. Review it for errors.  
Login to your controller using the serial interface 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.

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

### 3.17 Connect your Access Point as follows:

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

### 3.18 Configure the wireless profile on the wireless client.

Use the procedure in the Background slides to configure the wireless profile.

### 3.19 Connect your wireless device to the SSID.

Disconnect your PC from the controller GUI interface.  
Connect your PC using Wi-Fi to your SSID.

The user name is **test1** and the password is **Aruba123**.  
Verify connectivity by pinging your user gateway at 10.1.**X1**.1.

A msg of "Can't connect to this network" isn't much of a surprise here. #1: You may have had to follow a similar process of manually configuring e.g. the Algonquin network. #2: We're using a non-default security certificate.

### 3.20 View your configuration using VisualCFG.

You should be able to see your profiles in the AP Group as shown in Background slides.

## 4 Questions

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

- 4.1 From the user-table, what is the username, Role, Auth-type and PHY-type of your connected user?
- 4.2 A copy of the CA digital certificate is available in BrightSpace for this lab. Download the certificate to your PC. Double click on the certificate to open it. Click the Details tab and use the information to answer the following questions.
  - a) What is the Signature Algorithm?
  - b) Who is the issuer?
  - c) What is the certificate expiry date?

## 5 Demonstration and Signoff

- 5.1 Answer questions in your lab notebook.
- 5.2 Demonstrate steps 3.19 and 4.1 with your instructor.
- 5.3 A copy of the script has been 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.