

Lab 5: Advanced authentication with 802.1X.

Wireless networking concepts

Contents

Introduction to LAB 5	2
Exercise 1: Configure RADIUS authentication for telnet access	2
Task 1: Create the topology	2
Task 2: Configure telnet access to the router using RADIUS authentication	4
Exercise 2: Configuring a wireless network using Cisco Wireless LAN Controller.....	8
Task 1: Create the topology	8
Task 2: Configure the DHCP servers	9
Task 3: Create the initial configuration of the controller	11
Task 4: Configure the controller	14
Task 5: Check the results	22

Introduction to LAB 5

In the first exercise, you will configure a router to allow telnet access but instead the router itself to check the credentials, an external server (RADIUS) will be responsible for this task.

In the second exercise, you will explore the Wireless Access Point configuration using Cisco Wireless LAN Controller.

Exercise 1: Configure RADIUS authentication for telnet access

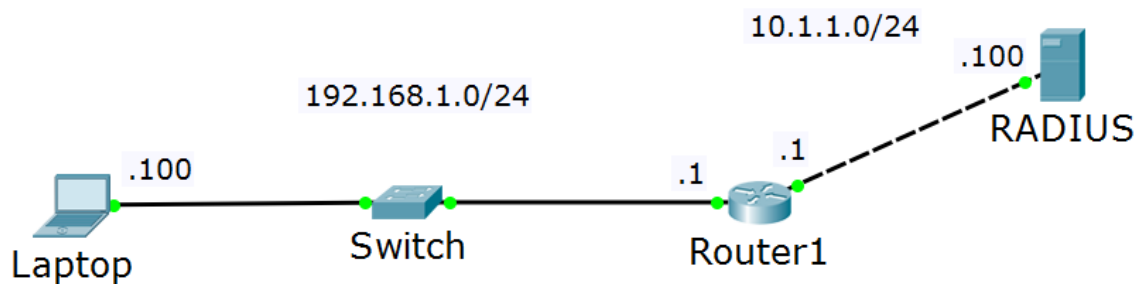
Task 1: Create the topology

1. Create the physical topology

In the packet tracer, move the following devices to the workspace:

- One end device (use Generic, the second in the list)
- One switch (2960)
- One router (2911)
- One server (Generic, the third one from the End Devices list)

Rename and connect the devices as per the picture below (IP addressing will be discussed in a second)



2. Assign IP addresses

This is a simple topology with two IP subnets: 192.168.1.0/24, which will be the client network and 10.1.1.0/24, which will be the server network. Refer to the table for the exact IP address assignments:

Device/Port	IP Address	Belongs to network (informational only)
Laptop	192.168.1.100	192.168.1.0
Router1/port-to-Laptop	192.168.1.1	192.168.1.0
Router1/port-to-RADIUS	10.1.1.1	10.1.1.0
RADIUS	10.1.1.100	10.1.1.0

Note: All masks are /24

3. Configure the connectivity

The laptop needs to communicate with the server. The “client” and the “server” networks are separated by a single router, which knows for both of

these networks/subnets. As you have learned before, this is known as direct routing and no additional routing configuration on Router1 is required.

Still, you will need to set up default gateway addresses on the client and on the server. Configure them as following:

- the laptop should have default gateway of **192.168.1.1**
- The server should have default gateway of **10.1.1.1**

4. Test the connectivity

You should be now able to ping between the client, the server (RADIUS) and the router.

Task 2: Configure telnet access to the router using RADIUS authentication

In previous LABs you have configured telnet access to a router using the router's internal database for authentication. Now you will use the RADIUS server which will be used to validate the credentials.

1. Configure the router

One thing to start with is a creating a local account on the router which can be used as a backup account in case of lost connection to the RADIUS server. To create a local account, type this command from global config mode

- **username BackupAdmin privilege 15 secret SoftUni**

Then, make the following configuration on Router1 from global config mode:

- **aaa new-model**
- **radius-server host 10.1.1.100 key softuni**
- **aaa authentication login default group radius local**

- **line vty 0 15**
- **login authentication default**

Explanations:

- the first command tells the router that you are using RADIUS for authentication (or TACACS+)
- the second command tells the router the IP address of the RADIUS server, as well as the shared password (**softuni** in this case)
- the third command enables RADIUS authentication on the router as default authentication method and “local” as a backup option (remember that you created the **BackupAdmin** account for this purpose)
- The last two commands instruct the router to use this default authentication method for telnet and SSH access (since these are the VTY lines)

2. Configure the server

Open the RADIUS server and go to Services -> AAA tab. Enable the service and accept the default Radius port (1645). Notice that there are two sections:

➤ Network Configuration

This is the “Router1 to Radius” communication section. Note that the term “Client” here refers to the RADIUS client, which is the router!

➤ User Setup

This is the section where you configure the user accounts which the Radius server will validate

Configure the following in the Network Configuration section and then click Add:

- Client Name: **R1** (informative only, does not need to match the actual hostname)

- Client IP: **10.1.1.1** (this is the router's IP address, which is a RADIUS client)
- Secret: **softuni** (the password which protects the router-to-server communication)

Configure the following in the User Setup section and then click Add:

- Username: test1
- Password: 123456

The screenshot shows the RADIUS configuration window with the 'Services' tab selected. The 'AAA' service is enabled (radio button selected) and the 'Radius Port' is set to 1645. The 'Network Configuration' section shows a table with one entry: '1 R1' with Client IP '10.1.1.1', Server Type 'Radius', and Key 'softuni'. The 'User Setup' section shows a table with one entry: '1 test1' with Password '123456'. Red boxes highlight the 'Services' tab, the 'AAA' service, the 'On' radio button, the 'Network Configuration' table, and the 'User Setup' table.

Services

AAA

Service ☒ On ☐ Off Radius Port 1645

Network Configuration

Client Name Client IP Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	R1	10.1.1.1	Radius	softuni

Add Save Remove

User Setup

Username Password

	Username	Password
1	test1	123456

Add Save Remove

☐ Top

3. Test the authentication

From the CLI of your client (Laptop) type:

- **telnet 192.168.1.1**

You should be prompted for username and password. Use the credentials that you configured in the RADIUS server:

- Username: **test1**
- Password: **123456**

You should be successfully logged in the router via telnet.

Note: You will only receive the user exec mode. If you want to go to privilege exec mode, you have to configure enable password or enable secret in the router.

Another interesting thing to note is that with this configuration, the RADIUS authentication is the default method even for the console login – if your console session times out, you will be asked for credentials. Use the **test1** account again. If you break the connection to the server, then you can login with your backup account, **BackupAdmin**.

If you want to configure a specific authentication method (or simply make it without authentication) for the console only, use the following configuration from global configuration mode:

- **aaa authentication login console none**

This command will set another authentication method – console, and it shows that it will be without a password. Then, you need to apply this method to the actual console interface with these commands:

- **line console 0**
- **login authentication console**

Note: even that you will not be prompted for a password when you enter the user exec mode (>) from a console session, you still will be asked for the enable secret, if you have configured it before.

Exercise 2: Configuring a wireless network using Cisco Wireless LAN Controller

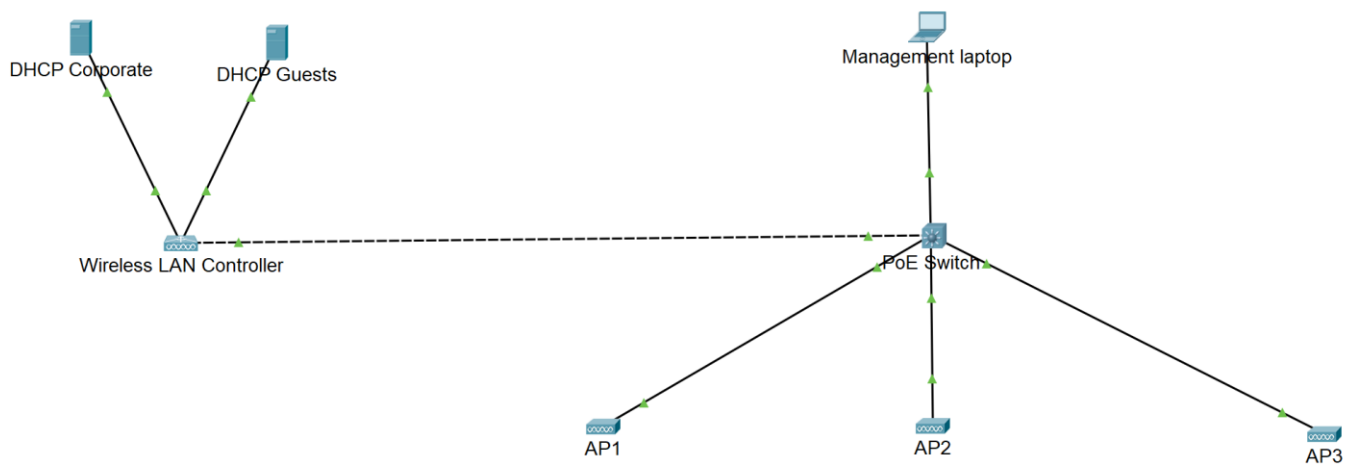
In this exercise, you are going to configure a wireless network using a Wireless LAN controller. You will have two SSIDs – one for the employees and one for the guests. Depending on to which SSID you connect later, you will receive different IP address. You will also group the access points to see how you can control them from the Wireless LAN controller.

Task 1: Create the topology

1. Create the physical topology

From the Wireless Devices section, select **2504** (Wireless LAN Controller) and three **LAP-PT** (Light Weight Access Point) From the Switches section, select a **3560 24PS** device. Also, select one laptop and two servers.

Then, connect them (and also rename them) as per the picture below. Note that you will be able to rename the Access Points only after you power supply them, which means to connect them to the Switch (3560), which is Power over Ethernet (PoE)



2. Verify and assign IP addresses

Hover your mouse over each access point and verify that they have received IP addresses from the 192.168.1.0/28 network. Then, manually configure an IP address from the same network on the **Management laptop** – 192.168.1.2/28

Configure the IP addresses of the two DHCP servers as follows:

- DHCP Corporate: 10.10.10.1/24
- DHCP Guests: 10.5.5.1/24

Task 2: Configure the DHCP servers

On **DHCP Corporate**, enable the DHCP service and create the following pool:

- Start IP address: 10.10.10.5
- Subnet mask: 255.255.255.0
- Maximum number of users: 10

Leave the other settings with the default values.

DHCP Corporate

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 10.10.10.5

Subnet Mask: 255.255.255.0

Maximum Number of Users: 10

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	10.10.10.5	255.255.255.0	10	0.0.0.0	0.0.0.0

Note – you can modify the existing serverPool or create another one.

On **DHCP Guests**, enable the DHCP service and create the following pool:

- Start IP address: 10.5.5.5
- Subnet mask: 255.255.255.0
- Maximum number of users: 10

Leave the other settings with the default values.

DHCP Guests

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 10.5.5.5

Subnet Mask: 255.255.255.0

Maximum Number of Users: 10

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

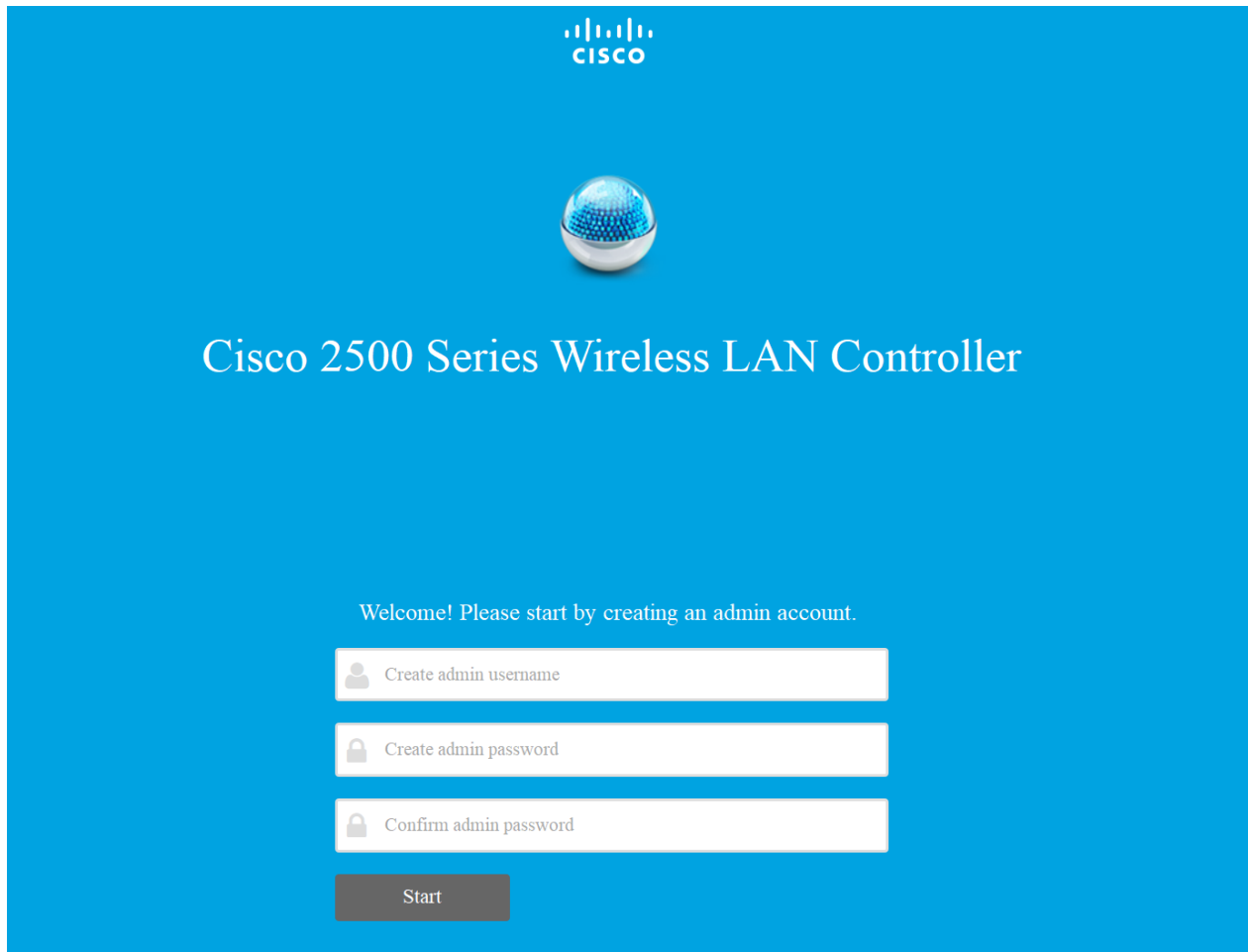
Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	10.5.5.5	255.255.255.0	10	0.0.0.0	0.0.0.0

Note – you can modify the existing serverPool or create another one.

Task 3: Create the initial configuration of the controller

You will need the **Management laptop** in order to make your controller configurations. Open a web browser and navigate to 192.168.1.1. On the Welcome page, configure **admin** as username and **SoftUni1** as password. Then click Start.




The image shows the Cisco 2500 Series Wireless LAN Controller's initial configuration page. The background is blue. At the top center is the Cisco logo. Below it is a small, glowing blue sphere. The title "Cisco 2500 Series Wireless LAN Controller" is displayed in white text. Below the title, a message reads: "Welcome! Please start by creating an admin account." There are three input fields: "Create admin username", "Create admin password", and "Confirm admin password". Each field has a small icon on the left (a person for username, a lock for password). At the bottom is a dark grey button labeled "Start".

On the next page, make the following configurations (the ones which are not mentioned – leave the defaults):

- System name: Test System
- Management IP address: 192.168.1.1

- Subnet Mask: 255.255.255.240
- Default Gateway: 192.168.1.5 (not used, just need to have something here)
- Management VLAN ID: 1

Then click Next.

 Cisco 2500 Series Wireless LAN Controller

1

Set Up Your Controller

System Name

Test System

?


Country

Greece (GR)

?

Date & Time

01/15/2019



0:36:34

Timezone

Jerusalem

?

NTP Server

(optional)

?

Management IP Address

192.168.1.1

?

Subnet Mask

255.255.255.240

Default Gateway

192.168.1.5

Management VLAN ID

1

?

Back

Next

2

Create Your Wireless Networks

3

Advanced Setting

On the next page, make the following configurations (the ones which are not mentioned – leave the defaults):

- Network name: temp (an SSID which we will disable later)
- Passphrase: 00000000

Then click Next.

The screenshot shows the Cisco 2500 Series Wireless LAN Controller configuration interface. At the top, the Cisco logo and title 'Cisco 2500 Series Wireless LAN Controller' are displayed. Below the title is a progress bar with three steps: '1 Set Up Your Controller' (completed, marked with a checkmark), '2 Create Your Wireless Networks' (current step, marked with a checkmark), and '3 Advanced Setting' (next step, marked with a right arrow). The main configuration area is titled 'Employee Network' with a green toggle switch. It contains several input fields: 'Network Name' with the value 'temp', 'Security' with a dropdown menu showing 'WPA2 Personal', 'Passphrase' with masked characters '*****', 'Confirm Passphrase' with masked characters '*****', 'VLAN' with a dropdown menu showing 'Management VLAN', and 'DHCP Server Address' with the value '0.0.0.0 (optional)'. Each input field has a help icon (question mark) to its right. Below the 'Employee Network' section is a 'Guest Network' section with a grey toggle switch. At the bottom of the configuration area are two buttons: 'Back' and 'Next'. The bottom of the page shows the '3 Advanced Setting' step in the progress bar.

Cisco 2500 Series Wireless LAN Controller

1 Set Up Your Controller ✓

2 Create Your Wireless Networks ✓

3 Advanced Setting >

Employee Network

Network Name temp ?

Security WPA2 Personal ?

Passphrase ***** ?

Confirm Passphrase *****

VLAN Management VLAN ?

DHCP Server Address 0.0.0.0 (optional) ?

Guest Network

Back Next

Leave the **Virtual IP Address** with the default setting and click Next.

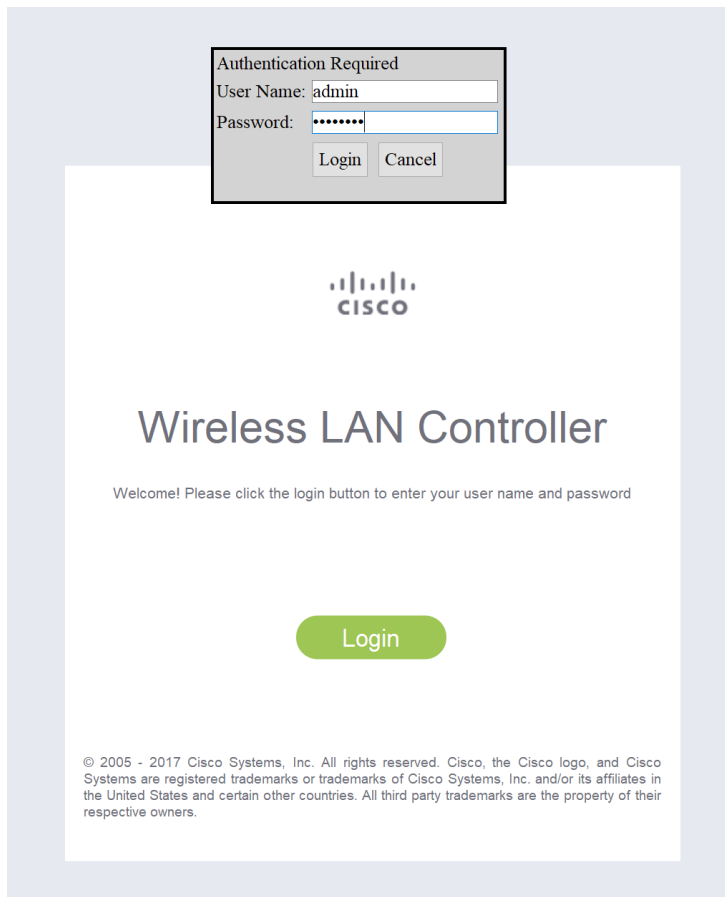
Finally, click Apply and confirm the system reboot message.

Wait about a minute, close the browser and re-open it again. Then, navigate to <https://192.168.1.1>. Note: you have to type **https** in the browser this time since after the initial configuration, the controller responds only to the secure web requests.

Task 4: Configure the controller

All of the AP (Access Point) configurations like SSID, security, etc., will now be configured on the controller and not on the individual Aps.

1. Open <https://192.168.1.1> and authenticate with **admin** and **SoftUni1**.



2. Create the interfaces/VLANs

Go to Controller -> Interfaces -> New and create Interface Name **Employee** which is associated with VLAN **10**. Click Apply.

Web Browser

< > URL

CISCO [MONITOR](#) [WLANs](#) [CONTROLLER](#) [WIRELESS](#) [SECURITY](#) [MANAGEMENT](#)

Controller

General

Inventory

Interfaces

Interface Groups

Multicast

▶ Internal DHCP Server

▶ Mobility Management

Ports

▶ NTP

▶ CDP

▶ Tunneling

▶ IPv6

▶ mDNS

▶ Advanced

Interfaces > New

Interface Name

VLAN Id

Then, for **port number**, type **2** – this is the second port (Gig2) on the controller, the one which goes to **DHCP Corporate** (if you have used different ports, type the correct one), enter the IP address and the mask from the screenshot below and click Apply (confirm it)

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

Create one more interface – **Guests**, which is associated with VLAN 5

Web Browser

< > URL <https://192.168.1.1/frameInterfaceCreate.html>

CISCO [MONITOR](#) [WLANs](#) [CONTROLLER](#) [WIRELESS](#) [SECURITY](#) [MANAGEMENT](#)

Controller

- General
- Inventory
- Interfaces**
- Interface Groups
- Multicast
- ▶ **Internal DHCP Server**
- ▶ **Mobility Management**
- Ports
- ▶ NTP
- ▶ CDP
- ▶ Tunneling
- ▶ IPv6
- ▶ mDNS
- ▶ Advanced

Interfaces > New

Interface Name

VLAN Id

This time for **port number** type **3** (or whatever port goes to **DHCP Guests**) and for the IP address and mask use the ones from the screenshot below. Click Apply and confirm it.

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

3. Create the SSIDs (WLANs)

Go to WLANs -> WLANs and for **Profile Name** and **SSID** type **Employee**

Web Browser

< > URL https://192.168.1.1/frameWlanCreate.html

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

WLANs

- ▼ **WLANs**
WLANs
- ▼ **Advanced**
AP Groups

WLANs > New

Type	WLAN ▼
Profile Name	Employee
SSID	Employee
ID	2 ▼

Click Apply and then from the drop-down menu of **Interface/Interface Group(G)**, select **Employee**. Do not forget to click **Enabled** next to the **Status** section. Click Apply again.

WLANs > Edit 'Employee'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	<input type="text" value="Employee"/>			
Type	WLAN			
SSID	<input type="text" value="Employee"/>			
Status	<input checked="" type="checkbox"/> Enabled			
Security Policies	None (Modifications done under security tab will appear after applying the changes.)			
Radio Policy	<input type="text" value="All"/>			
Interface/Interface Group(G)	<input type="text" value="Employee"/>			
Multicast Vlan Feature	<input type="checkbox"/> Enabled			
Broadcast SSID	<input checked="" type="checkbox"/> Enabled			
NAS-ID	<input type="text"/>			

Repeat the procedure for the other WLAN/SSID – use Guests as **Profile Name** and **SSID** and then associate it with the Guests interface which you have created earlier.

WLANs > Edit 'Guests'

The screenshot shows the 'WLANs > Edit 'Guests'' configuration page. The 'General' tab is selected, and the 'Security' tab is also visible. The configuration fields are as follows:

Field	Value
Profile Name	Guests
Type	WLAN
SSID	Guests
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	None (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	Guests
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	

Go back to the list of WLANs, select the **temp** one (created during the initial controller setup) and remove the checkbox on **Enabled** – we do not need it. Do not forget to click Apply.

4. Secure the SSIDs

At this moment the Wireless networks (SSIDs) does not have authentication on them. Let's create WPA2 security settings and set passwords.

Go to WLANs -> WLANs and select the **Employee** WLAN/SSID. Go to the **Security** tab and from the drop-down menu on **Layer 2 Security**, select **WPA+WPA2**. Enable the checkboxes next to **WPA2 Policy** and **PSK** and then enter the password **012345678**. Click Apply.

WLANs > Edit 'Employee'

GeneralSecurityQoSPolicy-MappingAdvanced

Layer 2Layer 3AAA Servers

Protected Management Frame

PMFDisabled

WPA+WPA2 Parameters

WPA Policy

☐

WPA2 Policy

☒

WPA2 Encryption

☒ AES☐ TKIP

Authentication Key Management

802.1X

☐ Enable

CCKM

☐ Enable

PSK

☒ Enable

FT 802.1X

☐ Enable

FT PSK

☐ Enable

PSK Format

ASCII

.....

WPA gtk-randomize State

Disable

[14](#)

Repeat the same procedure for the Guests WLAN/SSID but this time use the password **11111111**

5. Configure AP groups.

Last thing is to configure AP groups. This will allow you to dictate which of the settings configured so far (like SSID and security settings) apply to which access points.

Go to WLANs -> Advanced -> AP Groups. Click Add Group and create a group called **ALL_SSIDs**. Then click on it and under the **WLANs** tab, add the **Employee** and **Guests** networks (SSIDs)

Ap Groups > Edit 'ALL_SSIDs'

General WLANs RF Profile APs 802.11u Location Ports/Module

Add New

WLAN ID	WLAN SSID ⁽²⁾⁽⁶⁾	Interface/Interface Group(G)
2	Employee	Employee
3	Guests	Guests

Then go to the **APs** tab and add **AP2** and **AP3** to this group.

Ap Groups > Edit 'ALL_SSIDs'

General WLANs RF Profile APs 802.11u Location Ports/Module

APs currently in the Group Remove APs Add APs to the Group Add APs

<input type="checkbox"/> AP Name	Ethernet MAC	<input type="checkbox"/> AP Name	Group Name
<input type="checkbox"/> AP3	0001.960A.4101	<input type="checkbox"/> AP1	default-group
<input type="checkbox"/> AP2	0060.5CD6.7601		

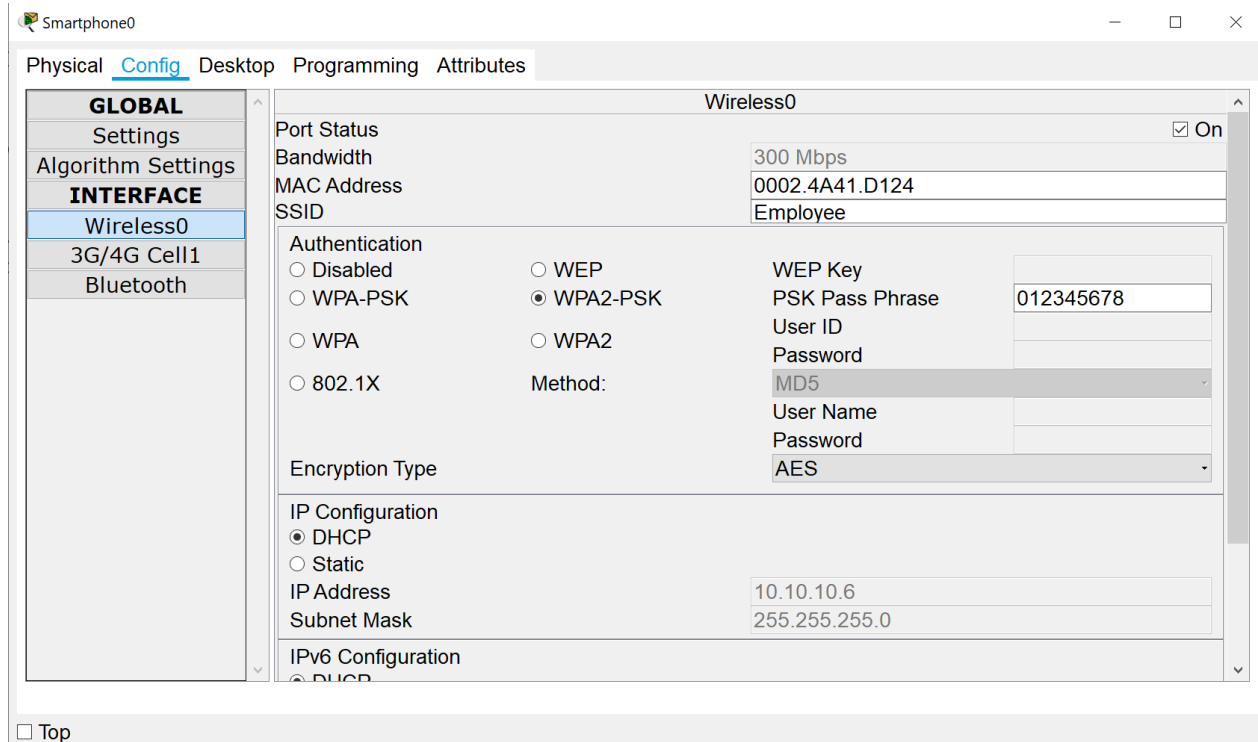
When done, create one more group, called **Employees_Only**. Using the same procedure, associate to this group the **Employee** SSID and **AP1**.

Task 5: Check the results

1. On the topology, hover your mouse over **AP1**. You should see that it is broadcasting only one the **Employee** SSID. Then do the same with **AP2** and **AP3** – they should broadcast both SSIDs – **Employee** and **Guests**. This is the results from the AP groups which you have just created.
2. Connect wireless clients.

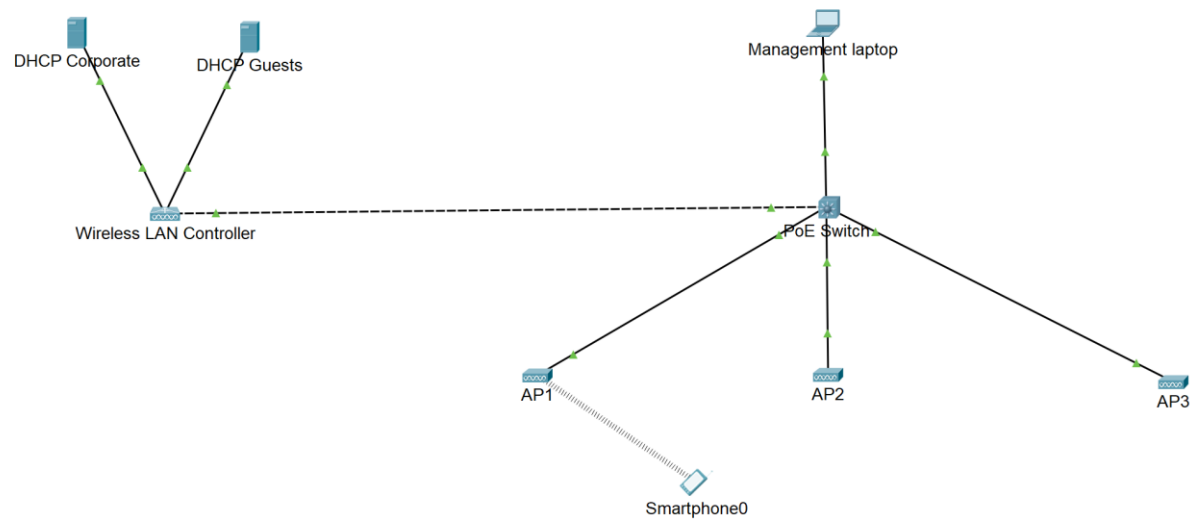
From the **End Devices** section in Packet Tracer, select **Smart Device**. Click on it and under the **Config** tab, **Wireless0**, configure the connection settings for the **Employee** SSID:

- SSID: Employee
- Authentication: WPA2-PSK
- PSK Pass Phrase: 012345678



Switch the windows and look at the packet tracer topology – in several seconds you should see that the wireless client connects to one of the APs.

Also, hover the mouse over it and observe the IP address – it should be 10.10.10.X/24, because this is the **Employee** network.



Make several experiments with more devices and of course – the Guests SSID – observe the connections and the IP addresses given to the devices.

You have completed LAB 5.