

Lab 5: 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	3
Exercise 2: Configuring a wireless network using Cisco Wireless LAN Controller.....	7
Task 1: Create the topology	8
Task 2: Configure the infrastructure	11
Task 3: Connect the clients.....	29

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

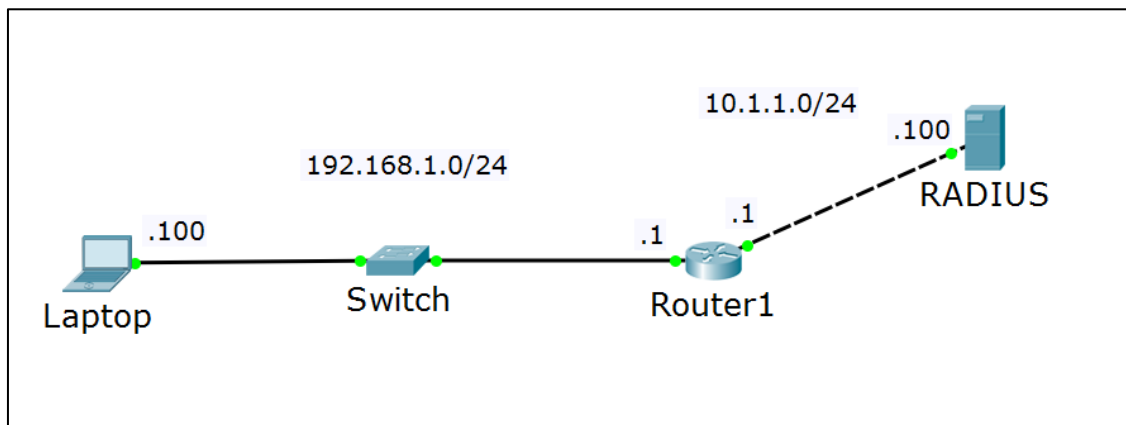
Task 1: Create the topology

1. Create the physical topology

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

- One end device (use Laptop, the second in the list)
- One switch (2960)
- One router (2911)
- One server (Server, 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 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 softuni**
- **address ipv4 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 creates the softuni radius config
- The third command sets the IP address of the radius server from the softuni radius config
- The fourth command sets the password for the router-to-radius communication - **SoftUni**
- the fifth 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

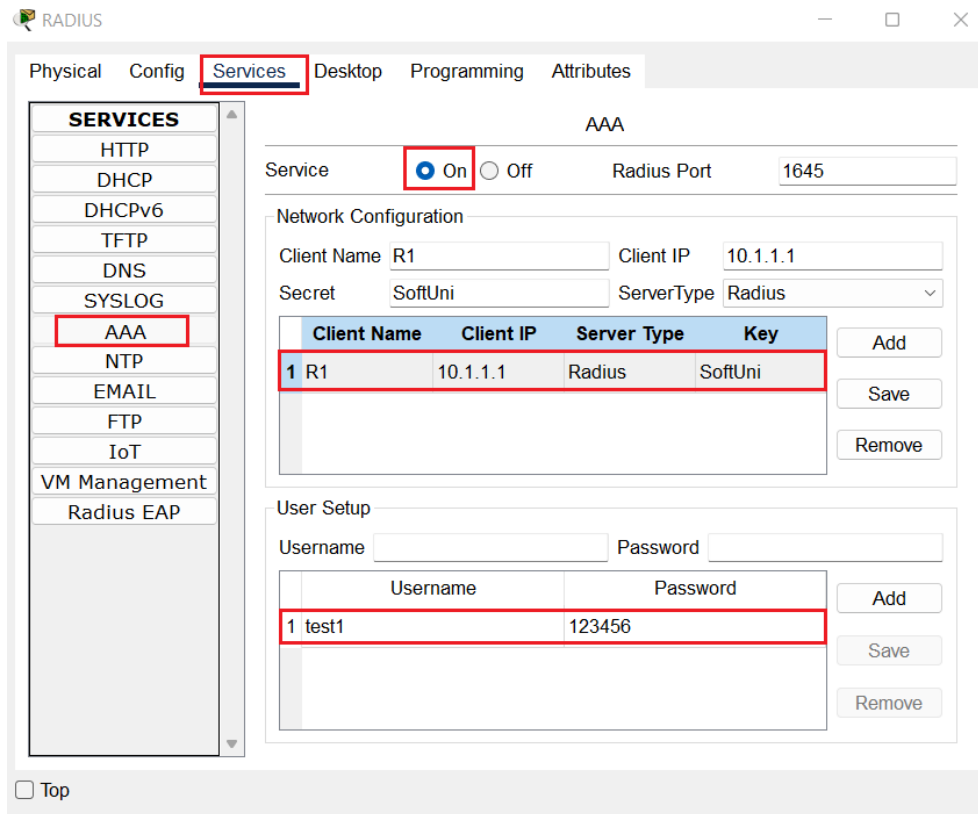
This is the section where you configure the user accounts which the Radius server will validate

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



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 (Corp) and one for the guests (Guest). They will have different security requirements and configurations – the Guest network will use WPA2 with pre-shared key (PSK), while the Corp network will use external Radius (AAA) server for authentication. You will also have a DHCP and DNS server for your network. You will (optionally) group the access points to see how you can control which SSIDs to be advertised by which access points.

Task 1: Create the topology

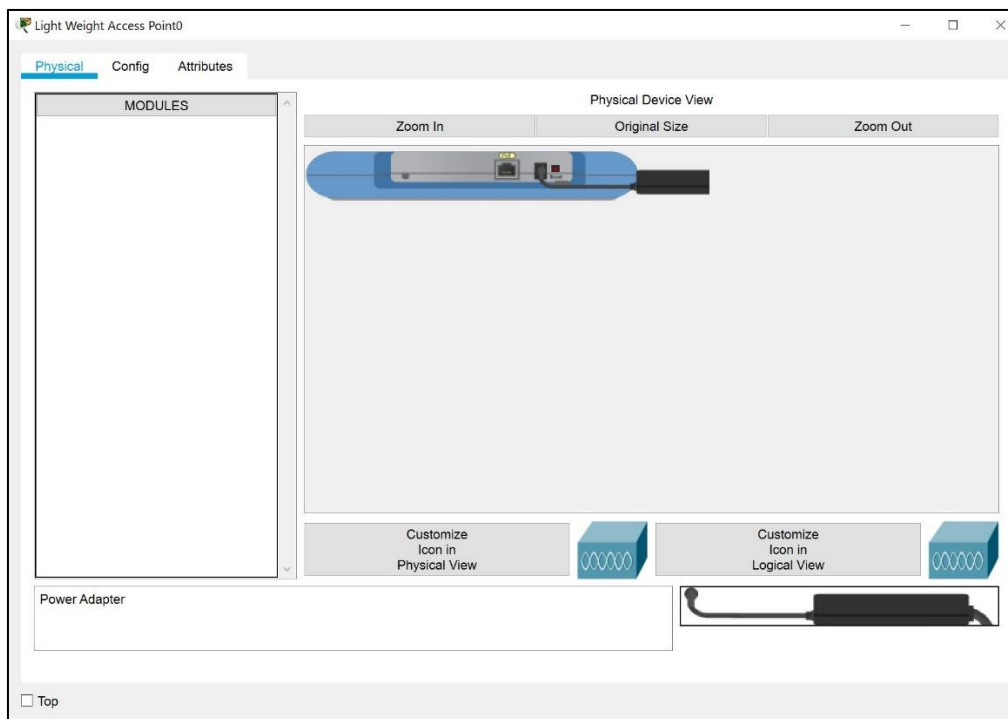
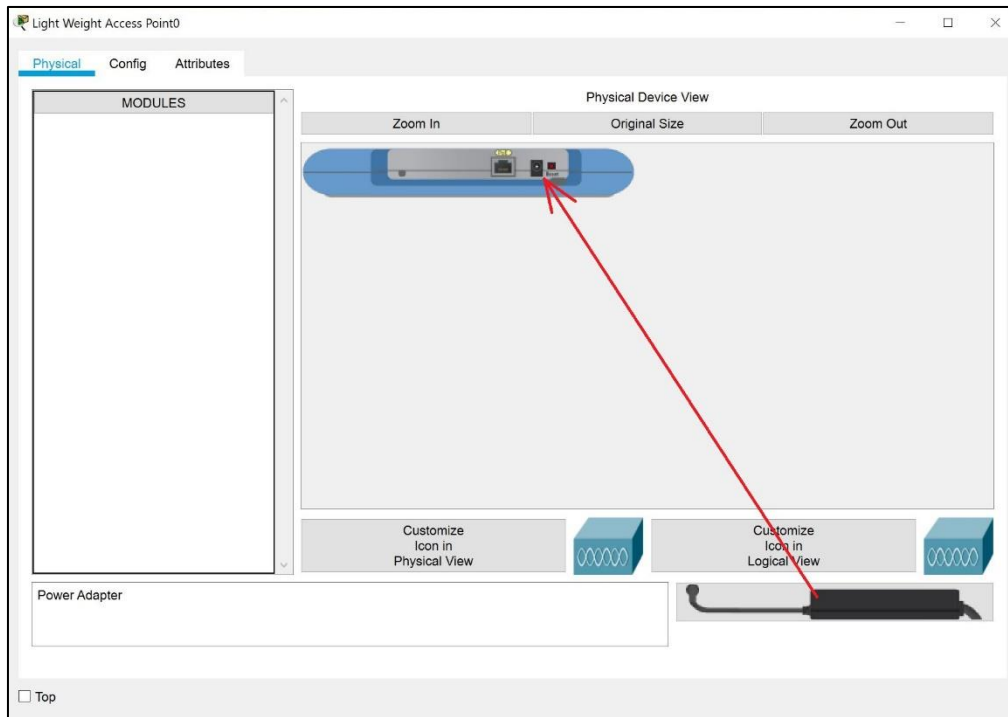
1. Add the devices

Move the following devices to the logical workspace:

- One laptop
- One server
- One L3 switch (3560-24PS)
- One L2 switch (2960-24TT)
- Three Lightweight Access Points (LAP-PT)
- One Wireless Lan Controller (WLC-3504)
- Two smart devices (the name will be SMARTPHONE-PT when moved to the topology). These will be the wireless clients

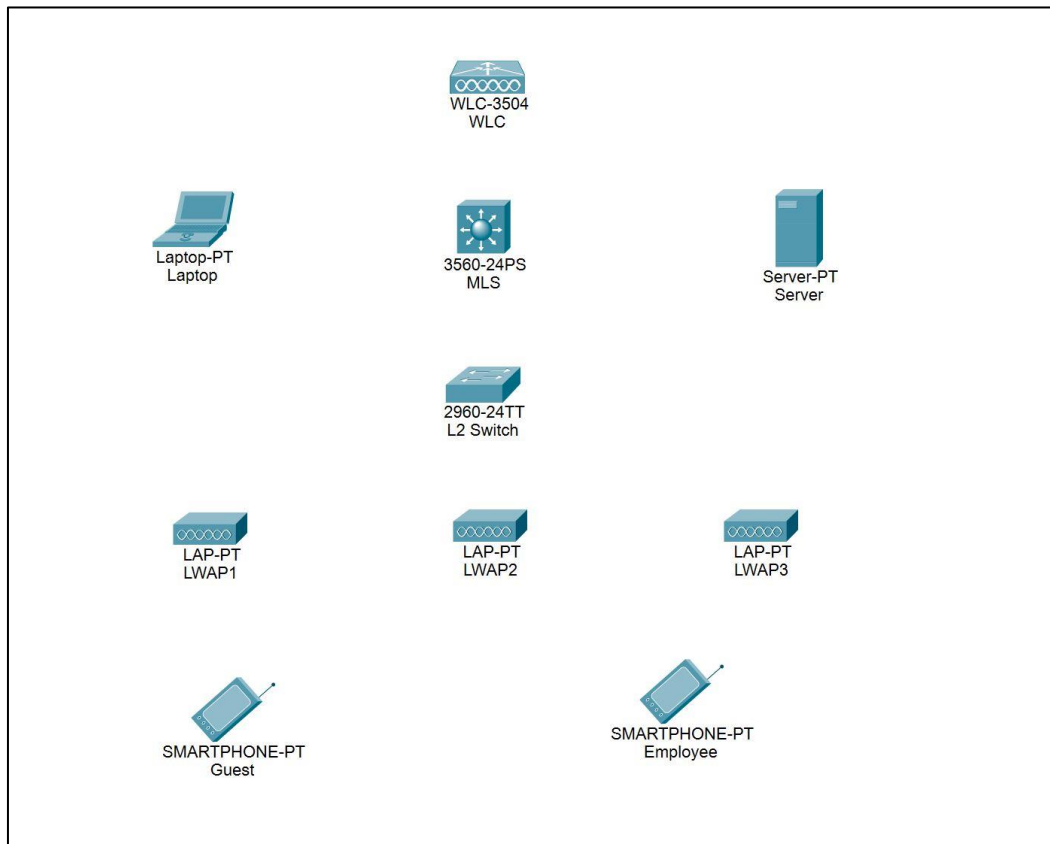
2. Power up the access points and rename all devices

As usual, we want to rename the devices in our topology. But for the access points (the three **LAP-PT** devices), this requires one more step. We need to first power them up. In order to do this, we need either Power over Ethernet (PoE), meaning to connect them to a switch, which can supply them with power, or to add a power adapter to each of them. We will use the second approach. To do this, click on one of them and on the Physical tab, move the power adapter to the correct place



Once you are ready with this for all of the three access points, they will be powered and you can go to the Config tab, where you can change their names.

This is how your picture should look like when you rename the devices:

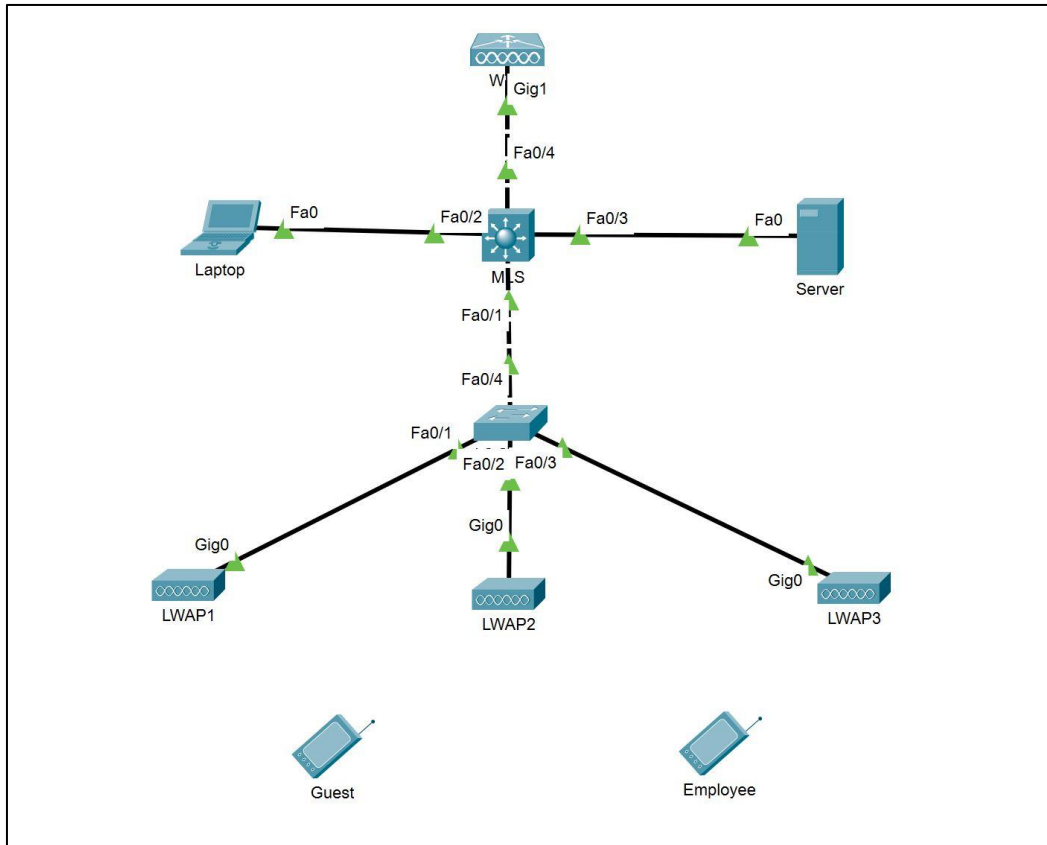


The abbreviations from the above picture:

- WLC = Wireless Lan Controller
- MLS = Multi-Layer Switch (this will be our L3 switch, which will route between the VLANs)
- LWAP = Light Weight Access Point

3. Connect the devices

When you have renamed the devices, connect them as per the picture below



Note: The device model is now hidden in order to free some space for the device names and the port numbers/labels. Your port numbers maybe different, depending on which you connect first, second, etc.

Note: The Guest and Employee smart devices are not connected at this time. Later, when you make the configurations, they will automatically connect (wirelessly) to the access points (either LWAP1, LWAP2 or LWAP3)

Task 2: Configure the infrastructure

The picture below tries to summarize what is required and what will be configured in this scenario.

the wireless networks, the SSIDs, the security settings for the authentication, and the SSID/WLAN to VLAN mappings.

The Server will have three purposes - it will be a DHCP server, a DNS server and an authentication server (AAA), where the employees (from the Corp SSID/VLAN) will authenticate.

The L2 Switch will have its uplink to the MLS as a trunk and the other three ports, going to the access points, will be in the management VLAN – VLAN15.

The LWAP1, LWAP2 and LWAP3, are our Light Weight Access Points. They are “Light Weight” because they cannot do their job alone – they need a controller. We need to make sure that these access points will build CAPWAP (Control And Provisioning of Wireless Access Points) tunnels to the WLC and take their configurations from there.

Finally, the Guest and Employee devices will be our clients. Once we create the infrastructure configurations, we will put the correct SSID and password (or a username and password) inside them and will expect that they will connect to an access point.

Now that we have an overview what is the purpose of each device, let's get started with the actual configuration.

❖ MLS:

- Create the three VLANs and assign IP addresses to the VLAN interfaces as follows:
 - VLAN 5, 10.5.5.1/24
 - VLAN 10, 10.10.10.1/24
 - VLAN 15, 10.15.15.1/24
- This is L3 switch, but you need to enable the L3 functionality. To do this, type **ip routing** from the global config mode
- Make the port to VLAN assignments. The port which goes to the Laptop should be access port in VLAN 10 (Corp). The port which goes to the Server should be in VLAN 15 (Management). The two ports which go to the WLC and to the L2 Switch should be trunk ports. But on these trunk ports change

the Native VLAN to VLAN 15! To do this, you need the command **switchport trunk native vlan 15** for each of the trunk ports.

Note: At this moment you may receive error messages from spanning tree and from CDP and this is because of the different native VLANs between the MLS and the L2 Switch. When we configure the L2 Switch, this will be fixed.

- DHCP relay
Our DHCP server will be on a separate VLAN than our clients, so we need to configure DHCP relay for VLAN 5 (Guest) and VLAN 10 (Corp). In order to do this, go to these VLAN interfaces and type **ip helper-address 10.15.15.3**
Note that you do not need to do this for VLAN 15, because this VLAN is the native VLAN on all trunk ports and this is where the Server belongs

❖ Server:

As you already know, our server will be used for three purposes – DHCP, DNS and AAA. We will configure the first two now. Before this, setup the server's IP address to be **10.15.15.3/24** and the default gateway to be **10.15.15.1**

DHCP – go to the Services -> DHCP and configure two DHCP pools:

- **Corp**
 - Default Gateway: **10.10.10.1**
 - DNS Server: **10.15.15.3**
 - Start IP address: **10.10.10.20**
 - Subnet Mask: **255.255.255.0**
 - Maximum number of users: **50**
 - TFTP Server: leave default
 - WLC Address: leave default
- **Management**
 - Default Gateway: **10.15.15.1**
 - DNS Server: **10.15.15.3**
 - Start IP address: **10.15.15.20**
 - Subnet Mask: **255.255.255.0**
 - Maximum number of users: **50**
 - TFTP Server: leave default

- WLC Address: **10.15.15.2** (this is how the access points will find their controller)

Then, modify the default serverPool to have the Start IP Address to something non-existent, like 10.23.23.0 (as in the screenshot) in order not to be confused with the Management pool (otherwise it will also have the 10.15.15.X subnet and you may have problems)

Finally, do not forget to enable the DHCP service.

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 10 23 23 0

Subnet Mask: 255 255 255 0

Maximum Number of Users: 256

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

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	10.23.23.0	255.255.255.0	256	0.0.0.0	0.0.0.0
Corp	10.10.10.1	10.15.15.3	10.10.10.20	255.255.255.0	50	0.0.0.0	0.0.0.0
Management	10.15.15.1	10.15.15.3	10.15.15.20	255.255.255.0	50	0.0.0.0	10.15.15.2

DNS – go to Services -> DNS and create an A record for the WLC, pointing to 10.15.15.2. Also, enable the service.

DNS Service: ☒ On ☐ Off

Resource Records

Name: wlc Type: A Record

Address: 10.15.15.2

No.	Name	Type	Detail
0	wlc	A Record	10.15.15.2

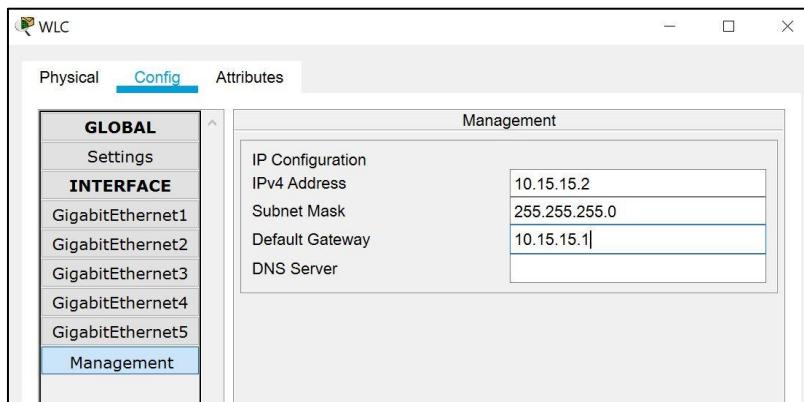
❖ L2 Switch:

You need to create the three VLANs here (5, 10 and 15) and then to associate the ports going to the access points with VLAN 15 and the port going to the MLS as a trunk port. Make VLAN 15 the native VLAN on the trunk port (**switchport trunk native vlan 15**)

❖ WLC:

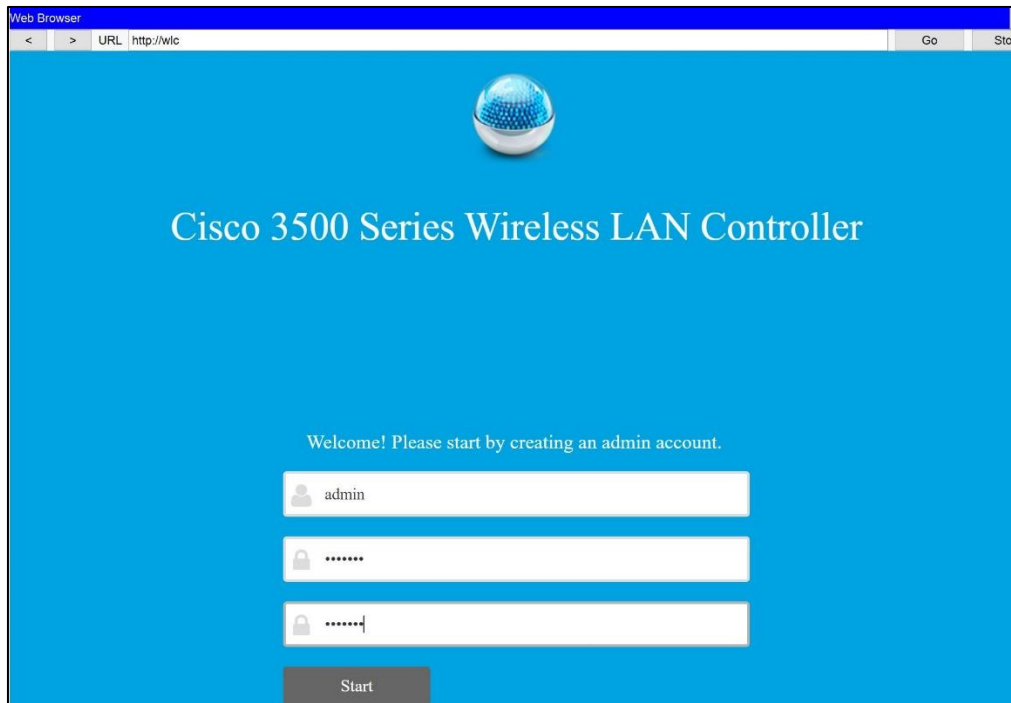
1. Go to Config -> Management and configure the IP settings of the controller:

- IP address: 10.15.15.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.15.15.1



At this point, you should be able to reach the WLC web interface from the Laptop. First, go to the Laptop and make sure that you configure it to receive its IP setting from the DHCP server. Check the IP address settings (it should receive an IP address from the 10.10.10.X subnet, gateway address of 10.10.10.1 and a DNS of 10.15.15.3). Confirm that you can ping the Server and the WLC before you continue

2. From the Laptop, open a browser and type WLC (just this, should be enough). After a while you should see the initial configuration. Type **admin** for username and **SoftUn1** for password. Then click Start



3. On the next screen, enter the required information. The important things that you should enter are:

- System name: **Test**
- Management IP address: **10.15.15.2** (the same address that you configured before)
- Subnet Mask: **255.255.255.0**
- Default Gateway: **10.15.15.1**

Click on Next

1 Set Up Your Controller

System Name

?

Country

Greece (GR)

?

Date & Time

11/01/2020

18:06:35

Timezone

Jerusalem

?

NTP Server

(optional)

?

Management IP Address

?

Subnet Mask

Default Gateway

Management VLAN ID

?

Back

Next

4. On the Create Your Wireless Networks page, you will configure something temporary (because you have to), which we will disable later

- Network Name: **Temp**
- Security: leave default
- Passphrase: **00000000**
- Confirm Passphrase: **00000000**

Click on Next

1 Set Up Your Controller

2 Create Your Wireless Networks

Employee Network ☒

Network Name

Security

Passphrase

Confirm Passphrase

VLAN

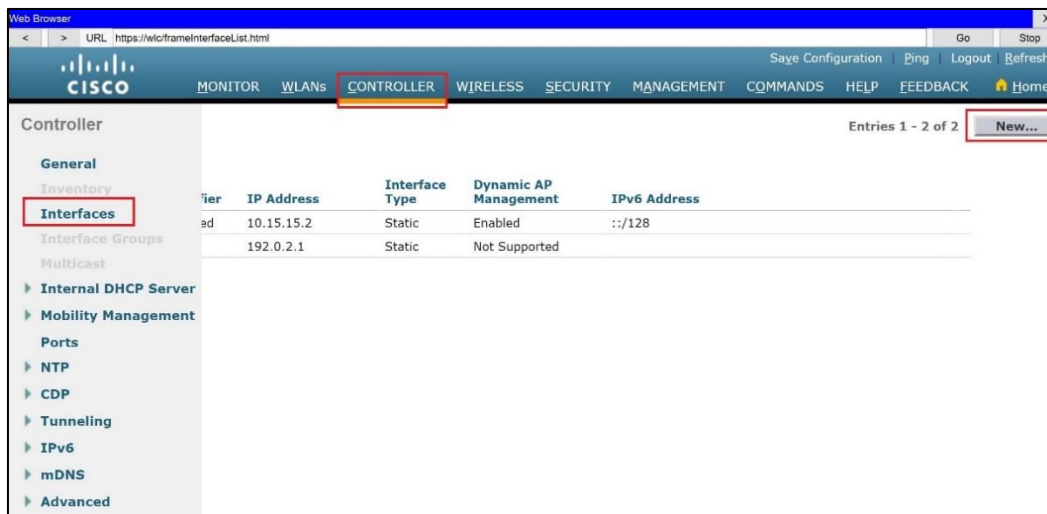
DHCP Server Address

Guest Network ☐

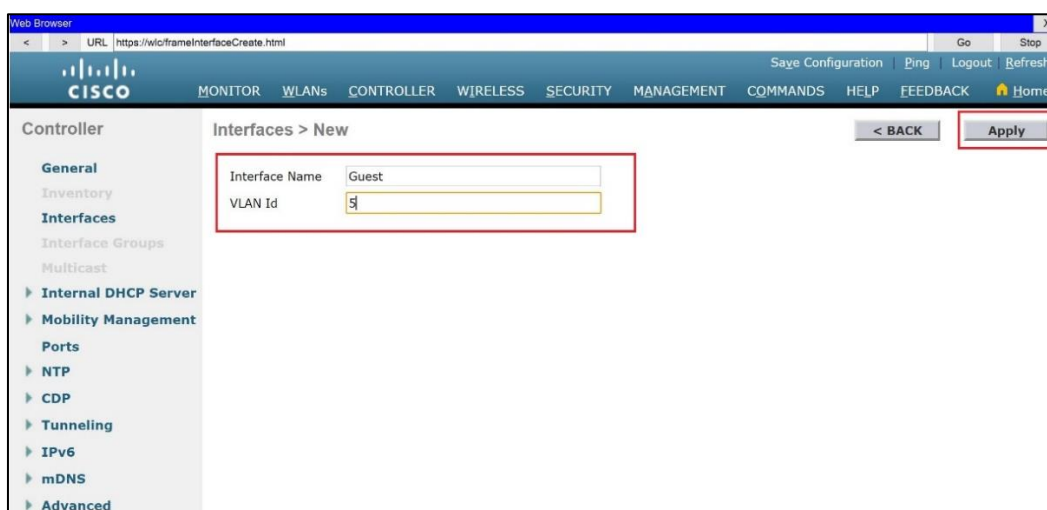
Back Next

5. On the Advanced Settings page, leave the defaults and click on Next
6. Then, on the Please confirm settings and apply, click on Apply (and confirm the warning message)
7. When you see the message **Saving the configuration...this may take a minute**, wait for about 5-10 seconds, then close the browser and re-open it. Now, it is very important that when you enter the URL, it should be **httpS** in front of it, otherwise it will not load the web configuration. So, go to <https://wlc> and enter your credentials (User: **admin**, password: **SoftUn1**)
8. Create the Interfaces.

The first thing (after the initial configuration) would be to define the so-called “interfaces” in the controller. These interfaces are logical and has to be associated with the correct VLAN and the correct WLAN (this is how we associate the SSID (WLAN) with the correct VLAN). Go to Controller -> Interfaces and click on New



For **Interface Name** type **Guest** and for **VLAN Id** type **5**. Then click on **Apply**



On the next screen, configure the following (leave others to the default):

- Port number: **1**
- IP address: **10.5.5.2**
- Netmask: **255.255.255.0**
- Gateway: **10.5.5.1**
- Primary DHCP Server: **10.15.15.3**

Then go to the upper right corner and click **Apply** (confirm the warning message)

Go back to Controller -> Interfaces and create one more. This time your interface should be named **Corp** and associated with VLAN 10. The other settings of this interface should be:

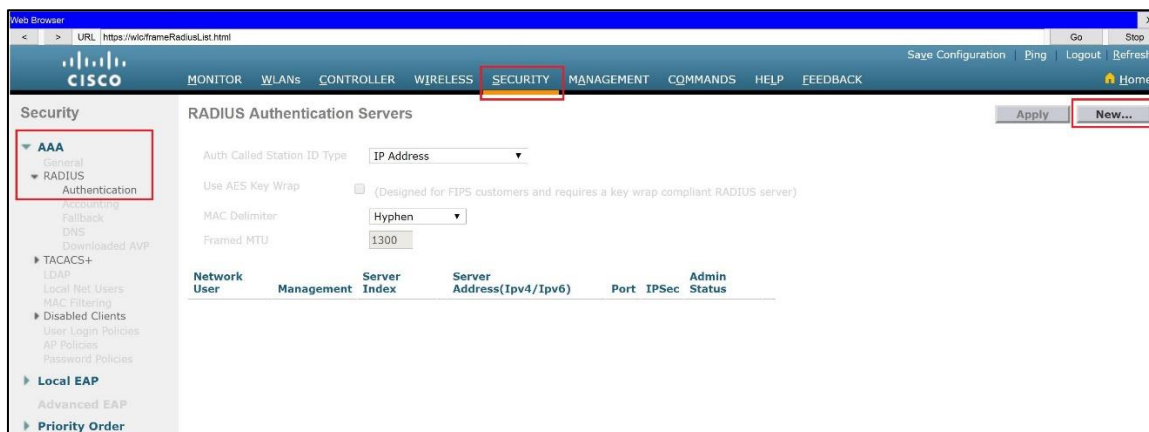
- Port number: **1**
- IP address: **10.10.10.2**
- Netmask: **255.255.255.0**
- Gateway: **10.10.10.1**
- Primary DHCP Server: **10.15.15.3**

When you apply and go back to Interfaces, you should see the following:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
Corp	10	10.10.10.2	Dynamic	Disabled	
Guest	5	10.5.5.2	Dynamic	Disabled	
management	untagged	10.15.15.2	Static	Enabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

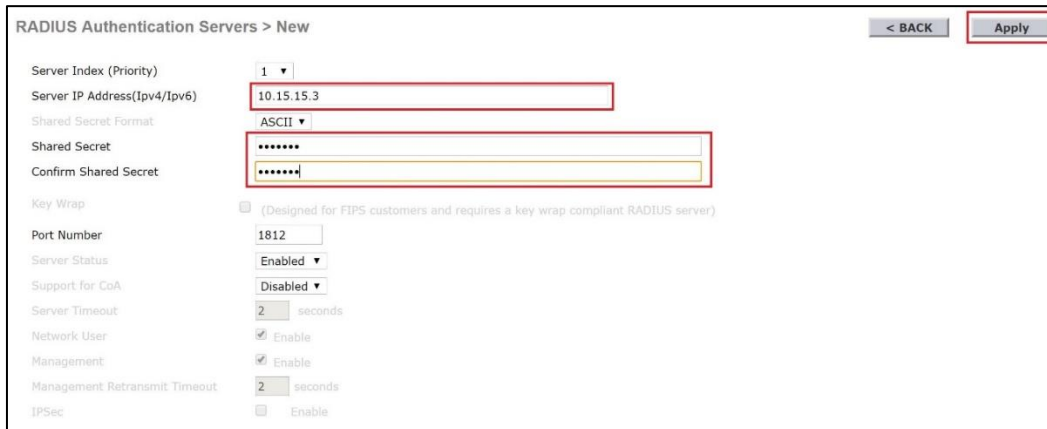
9. Put the RADIUS (AAA) server in the configuration.

Before we create the WLANs, we will configure the WLC to know where our RADIUS/AAA server is, so later we will point to it. To do this, go to SECURITY -> AAA -> RADIUS -> Authentication and click on New



Make the following configurations (leave others to the default) and click on Apply:

- Server IP Address(Ipv4/Ipv6): **10.15.15.3**
- Shared Secret: **SoftUn1**
- Confirm Shared Secret: **SoftUn1**



RADIUS Authentication Servers > New

< BACK Apply

Server Index (Priority) 1

Server IP Address(Ipv4/Ipv6) 10.15.15.3

Shared Secret Format ASCII

Shared Secret *****

Confirm Shared Secret *****

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for CoA Disabled

Server Timeout 2 seconds

Network User Enable

Management Enable

Management Retransmit Timeout 2 seconds

IPSec Enable

10. Create the WLANs and associate them with the interfaces.
Go to WLANs and right next to Create New click on Go.



Web Browser

URL https://wloframeWlan.html

Save Configuration Ping Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs

Advanced AP Groups

Current Filter: [Change Filter] [Clear Filter]

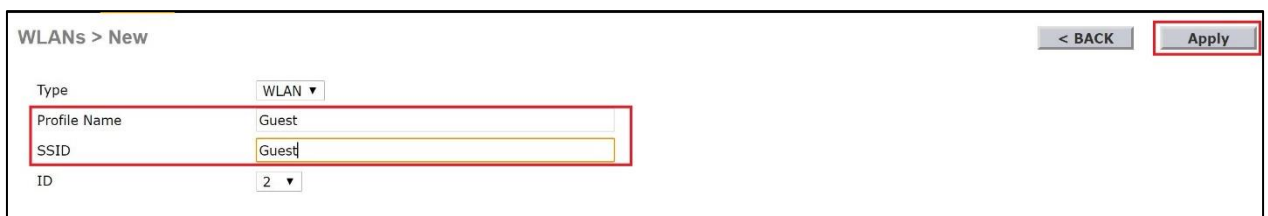
Create New Go

Entries 1 - 1 of 1

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Temp	Temp	Enabled	[WPA2][Auth(PSK)]

Remove

For Profile Name and SSID type **Guest**. Then click Apply.



WLANs > New

< BACK Apply

Type WLAN

Profile Name Guest

SSID Guest

ID 2

Next, enable the SSID and associate it with the Guest interface.

WLANs > Edit 'Guest' < BACK Apply

General Security QoS Policy-Mapping Advanced

Profile Name: Guest

Type: WLAN

SSID: Guest

Status: ☒ Enabled

Security Policies: None
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): Guest

Multicast Vlan Feature: ☐ Enabled

Broadcast SSID: ☒ Enabled

NAS-ID:

Go to the Security -> Layer 2 tab and select WPA + WPA2. Then click on WPA2 Policy. After this click on Enable next to PSK and enter **Guest123** as a password (the pre-shared key). Click on Apply.

WLANs > Edit 'Guest' < BACK Apply

General **Security** QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Protected Management Frame: Disabled

WPA+WPA2 Parameters

WPA Policy: ☐

WPA2 Policy: ☒

WPA2 Encryption: ☒ AES ☐ TKIP

Authentication Key Management

802.1X: ☐ Enable

CCMK: ☐ Enable

PSK: ☒ Enable

FT 802.1X: ☐ Enable

FT PSK: ☐ Enable

PSK Format: ASCII

WPA gtk-randomize State: Disable

Go back to WLANs and create one more, this time it will be named **Corp** (for both Profile Name and SSID). Then enable it and associate it with the Corp interface.

In the Security -> Layer2 tab of this WLAN, select again WPA + WPA2 and WPA2 Policy but this time click Enable next to 802.1X.

WLANs > Edit 'Corp'

< BACK Apply

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: WPA+WPA2

MAC Filtering: Disabled

Fast Transition: Disabled

Protected Management Frame: Disabled

WPA+WPA2 Parameters

WPA Policy: Disabled

WPA2 Policy: ☒

WPA2 Encryption: ☒ AES ☐ TKIP

Authentication Key Management

802.1X: ☒ Enable

CKIP: ☐ Enable

PSK: ☐ Enable

FT 802.1X: ☐ Enable

Go to Security -> AAA Servers tab and in the dropdown menu next to Server 1, select IP:10.15.15.3, Port:1812 (this is why we have put the RADIUS (AAA) server in the configuration in the previous step). Click on Apply.

WLANs > Edit 'Corp'

< BACK Apply

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface: ☒ Enabled

Authentication Servers	Accounting Servers	EAP Parameters
Server 1: IP:10.15.15.3, Port:1812	None	None
Server 2: None	None	None
Server 3: None	None	None
Server 4: None	None	None
Server 5: None	None	None
Server 6: None	None	None

Radius Server Accounting: ☐ Interm Update

LDAP Servers

Finally, you can either delete or simply disable the Temp WLAN by going to WLANs, select the Temp WLAN (select the WLAN ID number 1) and remove the checkbox next to Enabled. Click on Apply.

WLANs > Edit 'Temp'

< BACK Apply

General Security QoS Policy-Mapping Advanced

Profile Name Temp

Type WLAN

SSID Temp

Status ☒ Enabled

Security Policies [WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface/Interface Group(G) management

Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☒ Enabled

NAS-ID

11. Optional: create AP groups.

This step is optional because the GUI here sometimes does not show the graphics correctly (this is why we do not have screenshots here). You can go to WLANs -> Advanced -> AP groups and create different AP groups in order to limit which WLANs (SSIDs) will be advertised by which access points. For example, you can configure LWAP1 to broadcast only the Guest WLAN/SSID, LWAP2 to broadcast both Guest and Corp WLANs/SSIDs and LWAP3 to broadcast only the Corp WLAN/SSID.

❖ Server (again):

We have configured the WLC to point to a RADIUS/AAA server when it comes to authentication for the Corp WLAN/SSID which means that the credentials will be checked on an external server. Let's configure this server to accept those authentication request from the WLC (which is the RADIUS client!) and also create one account (username and password) in the Server which will be used by our simulated "employee" to connect to the Corp network (WLAN/SSID).

Click on the Server and go to Services -> AAA. Make the following configurations:

- Enable the service
- Change the Radius Port to **1812** (this is what we configured on the WLC)
- For Client Name put **WLC** (the name does not really matter)
- For Client IP put **10.15.15.2** (remember, the client in this communication is the WLC)

- For Secret type **SoftUn1** (the same secret that we configured on the WLC)
- Leave **Radius** for Server Type
- Click on Add to add your RADIUS client (The WLC)

The screenshot shows the 'Server' configuration window with the 'Services' tab selected. In the left sidebar, 'AAA' is highlighted. The main area shows the 'AAA' service configuration. The 'Service' is set to 'On' and the 'Radius Port' is '1812'. Under 'Network Configuration', the 'Client Name' is empty, 'Client IP' is empty, 'Secret' is empty, and 'ServerType' is 'Radius'. Below this is a table with columns: Client Name, Client IP, Server Type, and Key. The first row is highlighted with a red box and contains the values: 1, WLC, 10.15.15.2, Radius, and SoftUn1. To the right of the table are 'Add', 'Save', and 'Remove' buttons.

	Client Name	Client IP	Server Type	Key
1	WLC	10.15.15.2	Radius	SoftUn1

Then, configure one user account - again there (Services -> AAA) but in the second part of the window (called User Setup). For Username type **Bob** and for Password type **Bob123**. Then click on Add

The screenshot shows the 'Server' configuration window with the 'Services' tab selected. On the left, a sidebar lists various services: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA (highlighted), NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main area is titled 'AAA' and contains the following sections:

- Service:** A radio button set with 'On' selected and 'Off' unselected. A 'Radius Port' field is set to '1812'.
- Network Configuration:**
 - Fields for 'Client Name', 'Client IP', and 'Secret'.
 - A 'ServerType' dropdown menu set to 'Radius'.
 - A table with columns: Client Name, Client IP, Server Type, and Key.

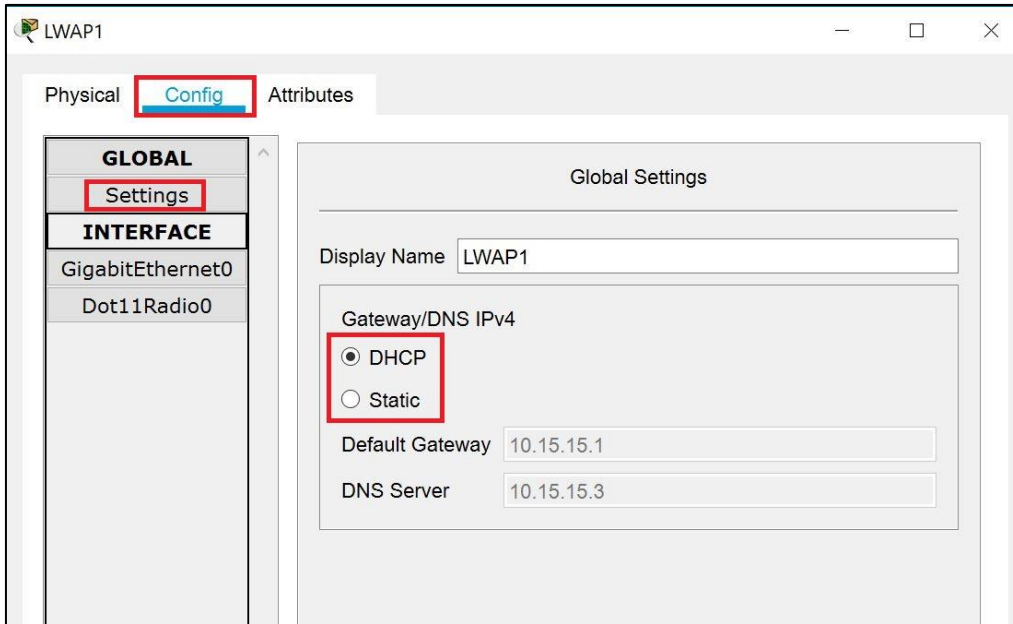
	Client Name	Client IP	Server Type	Key
1	WLC	10.15.15.2	Radius	SoftUn1
 - Buttons: 'Add', 'Save', and 'Remove'.
- User Setup:**
 - Fields for 'Username' and 'Password'.
 - A table with columns: Username and Password.

	Username	Password
1	Bob	Bob123
 - Buttons: 'Add', 'Save', and 'Remove'.

At the bottom left, there is a 'Top' button.

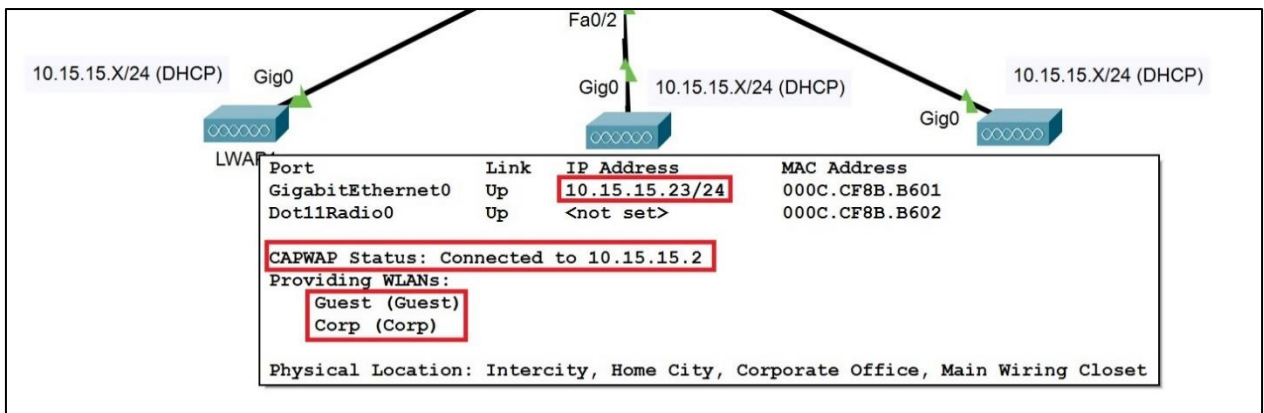
❖ The access points (LWAP1, LWAP2 and LWAP3):

You don't need to configure anything there because each access point should automatically receive its IP address, subnet mask, default gateway, DNS server and information about where the controller is, from the DHCP. Then, it will build the CAPWAP tunnel to the WLC and take its configuration from there. What you need to do though is to refresh the DHCP process from them in order to force them to start looking for these configurations again (because everything else is now configured). Go to each of the access points, go to Config -> Settings and click on Static, then click again on DHCP



After several seconds, you should see the Default Gateway configured for 10.15.15.1 and the DNS Server configured for 10.15.15.3.

Also, when you go to the topology and hover your cursor over each access point, you should see the access point's IP address, the CAPWAP connection to the WLC and the SSIDs that it broadcasts

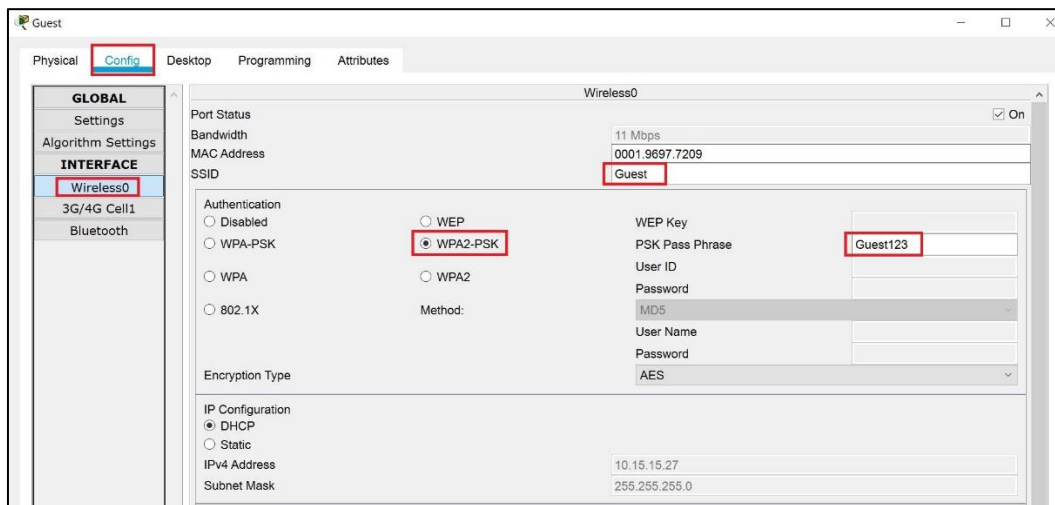


Task 3: Connect the clients

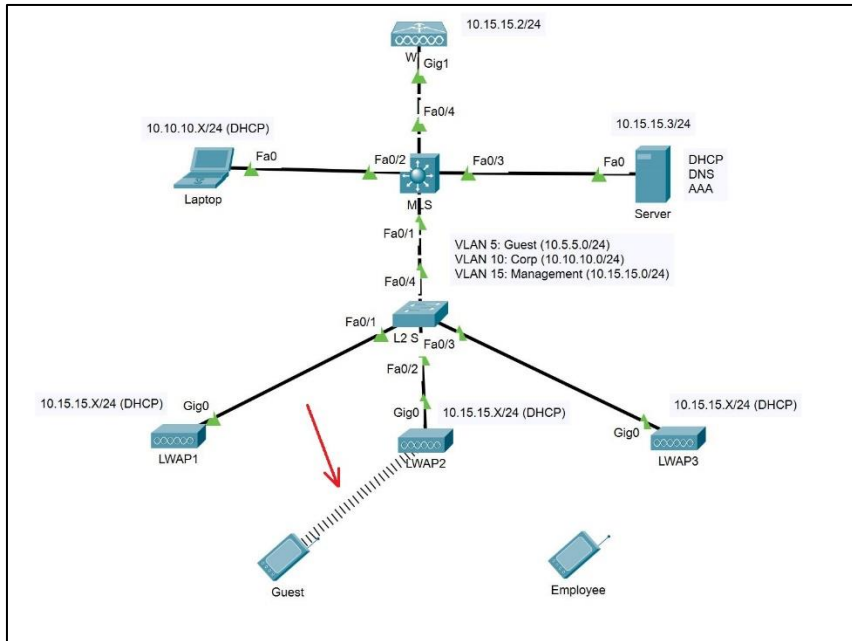
Now that our infrastructure is ready, it is time to connect the wireless clients to the network.

1. The Guest device.

Go to Config -> Wireless0 and next to SSID type **Guest**. Then under Authentication select WPA2-PSK and type the password: **Guest123** (after this you can press the TAB key, it acts like Apply in the Packet Tracer)



Wait several seconds and look at the topology – you should see the wireless connection between the Guest device and one of the access points (either LWAP1, LWAP2 or LWAP3 – you cannot control which one, it is random here)

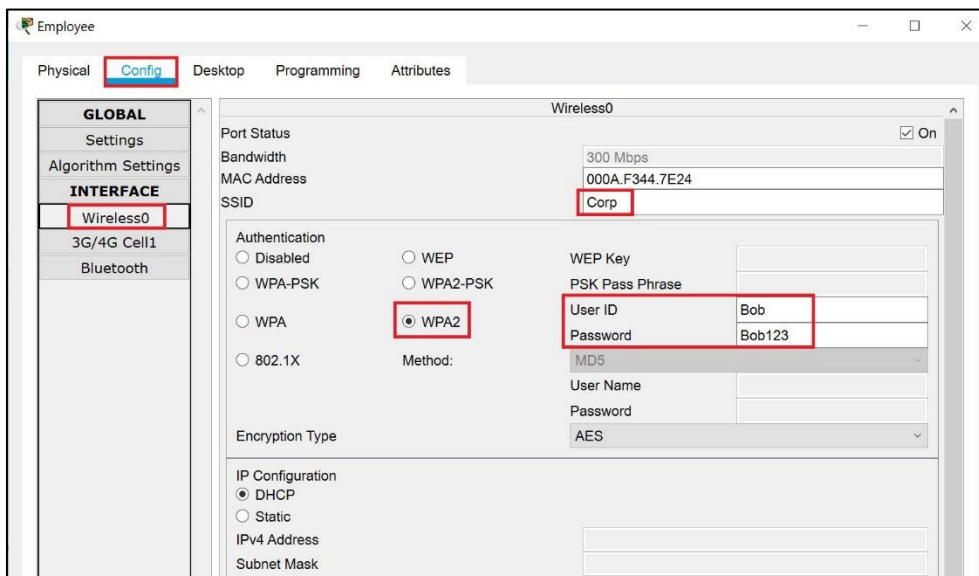


2. The Employee device.

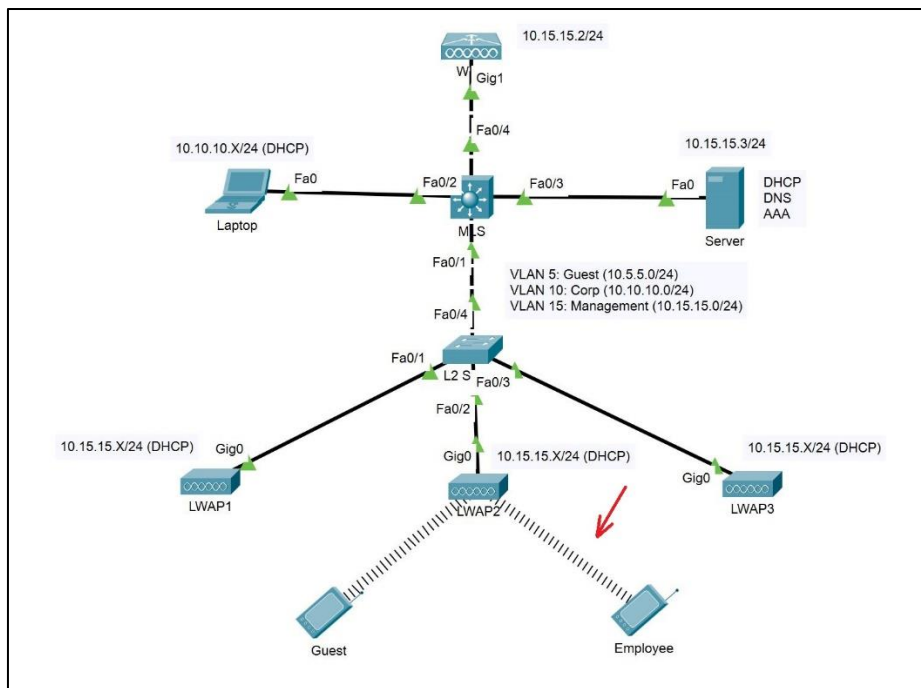
Go to Config -> Wireless0 and next to SSID type **Corp**. Then under Authentication select **WPA2** (instead of **WPA2-PSK**). Then, type the credentials that you have in your RADIUS/AAA server:

- User ID: **Bob**
- Password: **Bob123**

Note: Both the User ID and the password are case-sensitive



Again, wait several seconds and look at the topology – you should see the wireless connection between the Employee device and one of the access points (either LWAP1, LWAP2 or LWAP3 – it can be the same or different one that the Guest is connected to. Also, it depends if you have configured AP Groups or not)



Note: Hover your cursor over the Guest and Employee devices after they are successfully connected to an access point. You will notice that both of them have received IP addresses from the management VLAN – 10.15.15.0/24. Why? The answer is – Packet Tracer limitations. And the thing is that the WLC cannot put a VLAN tag on the packets (at least in the current version which is 7.3.1). This is why we do not have a Guest DHCP pool in the Server (the Corp pool is only for the Laptop). This is also why we have VLAN 15 as a native VLAN on the MLS uplink to the WLC and on the trunk between the MLS and the L2 Switch.

You have completed LAB 5.