Lab 5: Authentication with 802.1X. Wireless networking concepts

Contents

SoftUni

© SoftUni – https://softuni.org. Copyright document. Unauthorized copy, reproduction or use is not permitted.

Follow us:

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

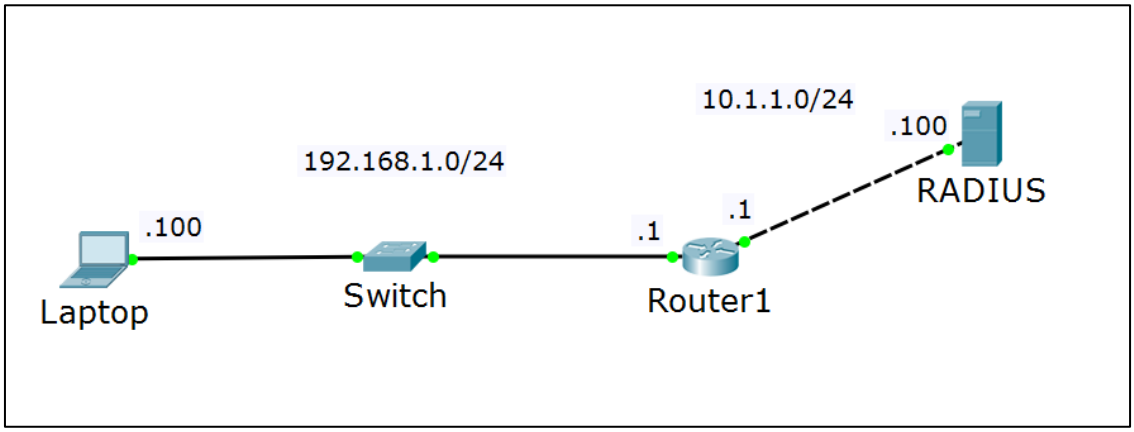
Task 1: Create the topology

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)



© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

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

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

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)

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

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

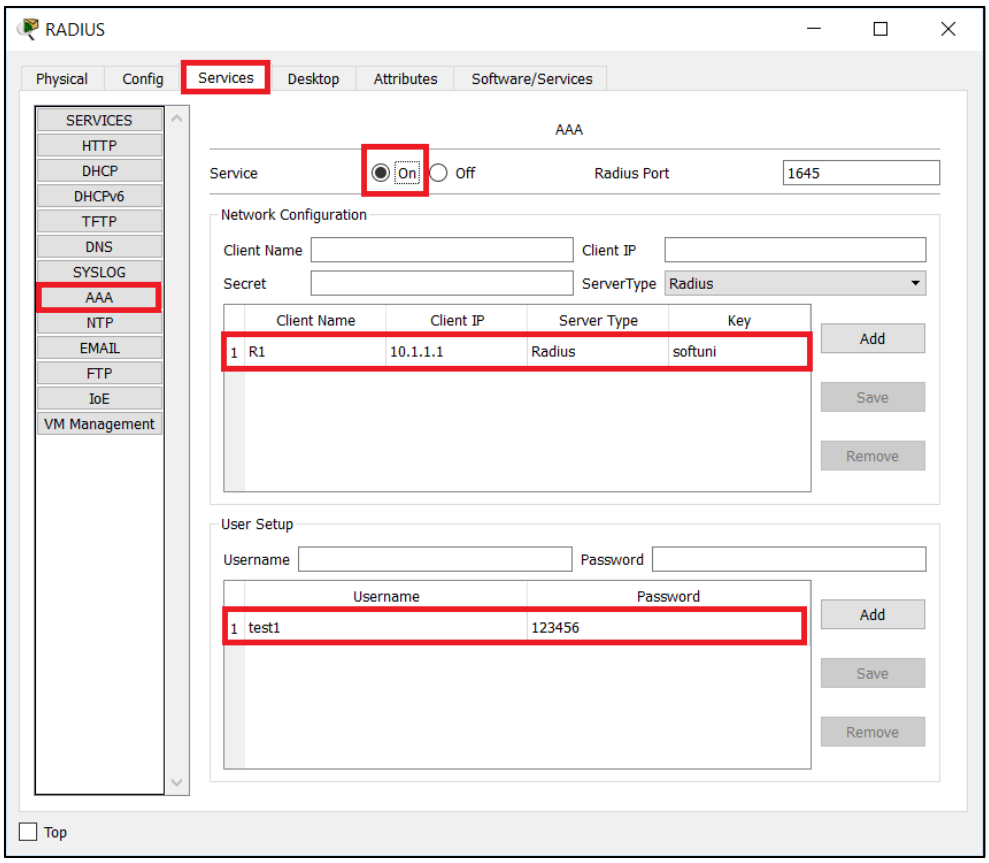
   Configure the following in the Network Configuration section and then click Add:

   - 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

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.



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.

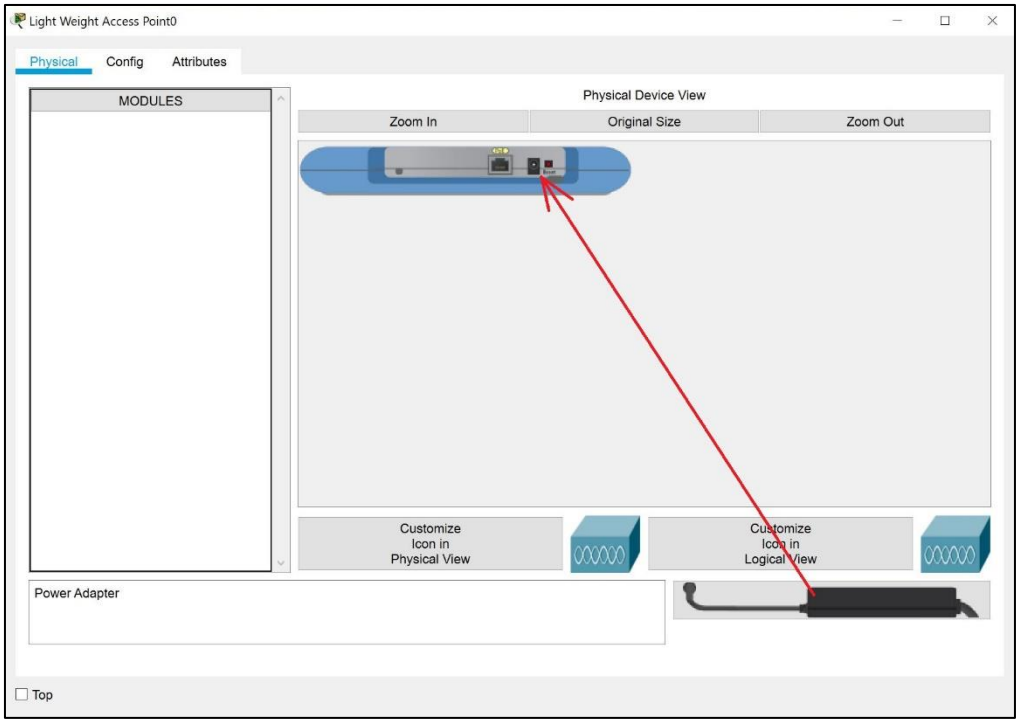
© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

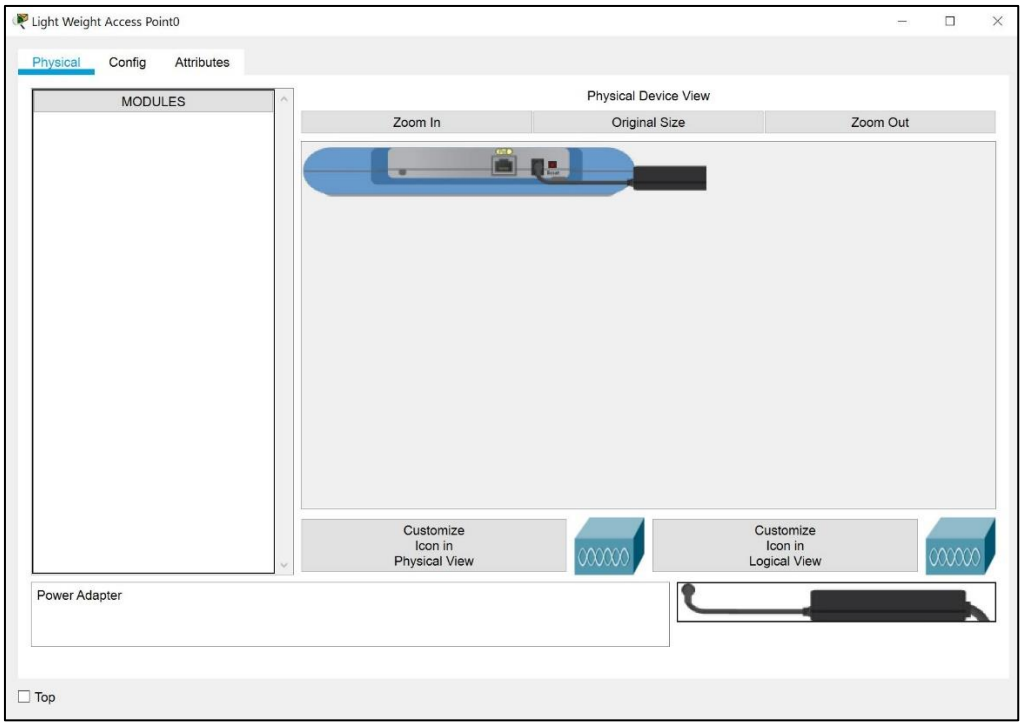
Task 1: Create the topology

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 SMARTHONE-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

© SoftUni – https://softuni.org. Copyright document. Unauthorized copy, reproduction or use is not permitted.
Follow us:

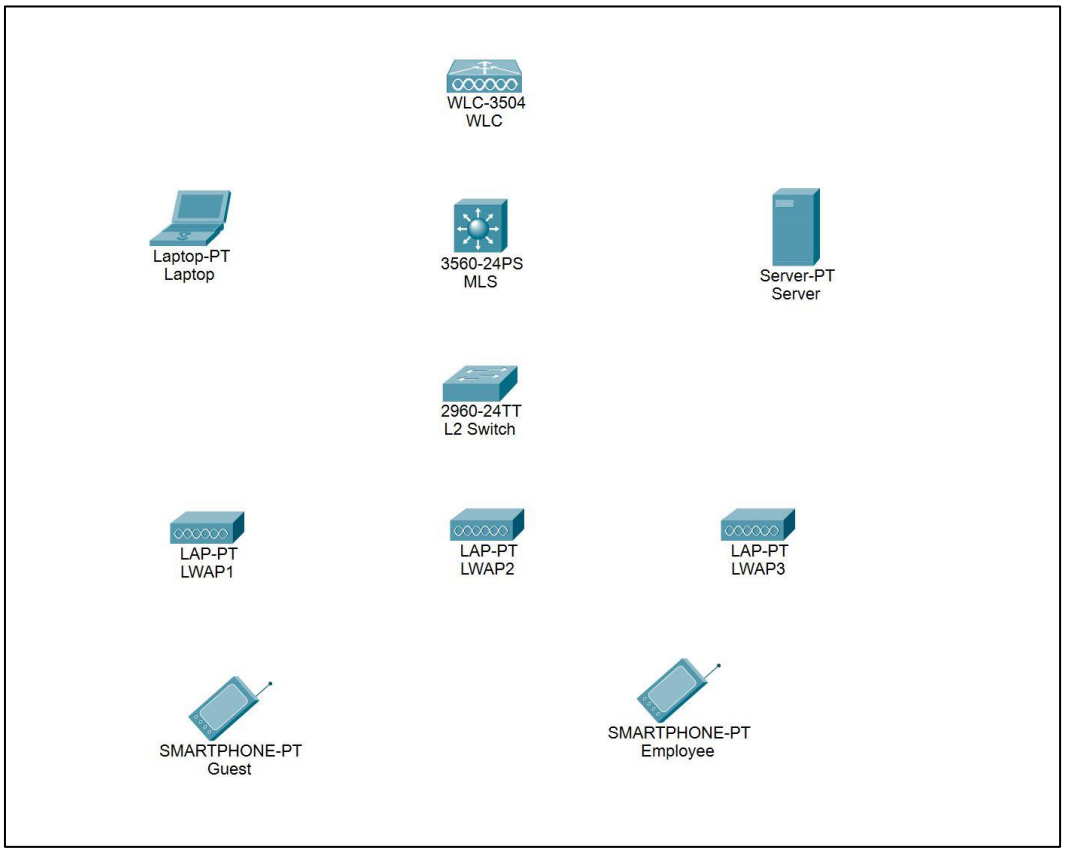




Once you are ready with this for all of the three access points, they will be powered and you can go to the Config tab, where you can change their names.

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

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

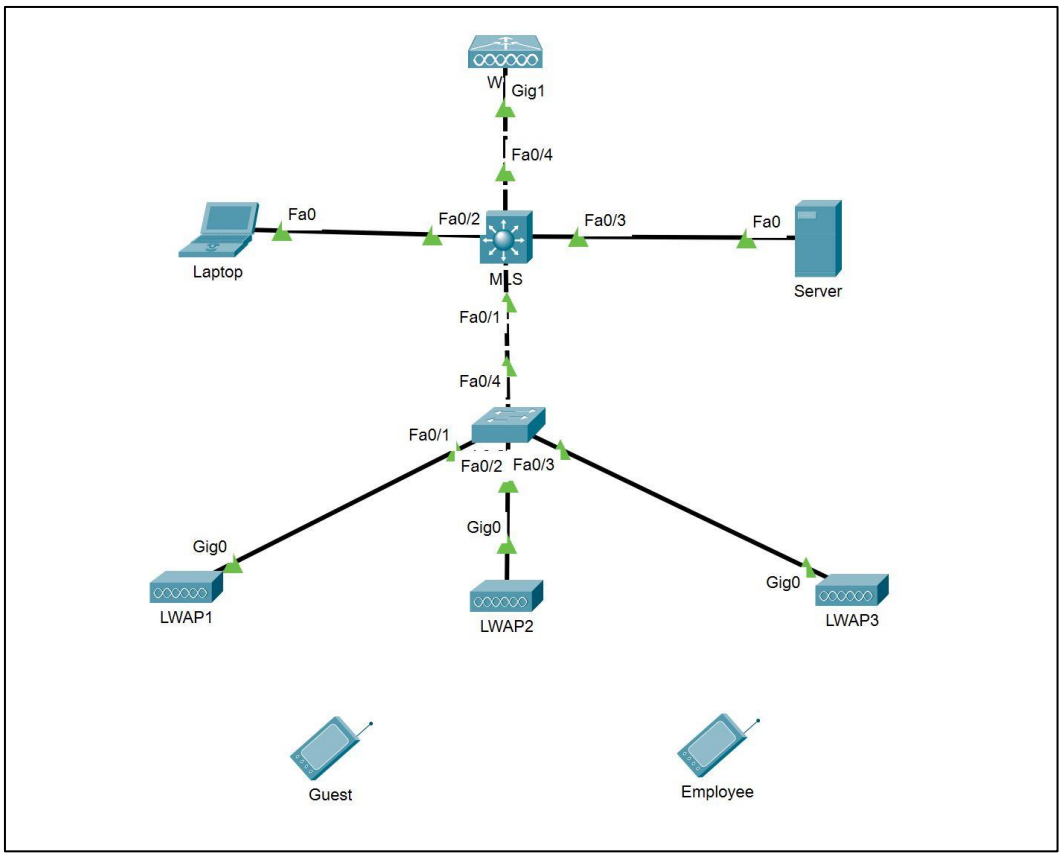


The abbreviations from the above picture:

- 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

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.



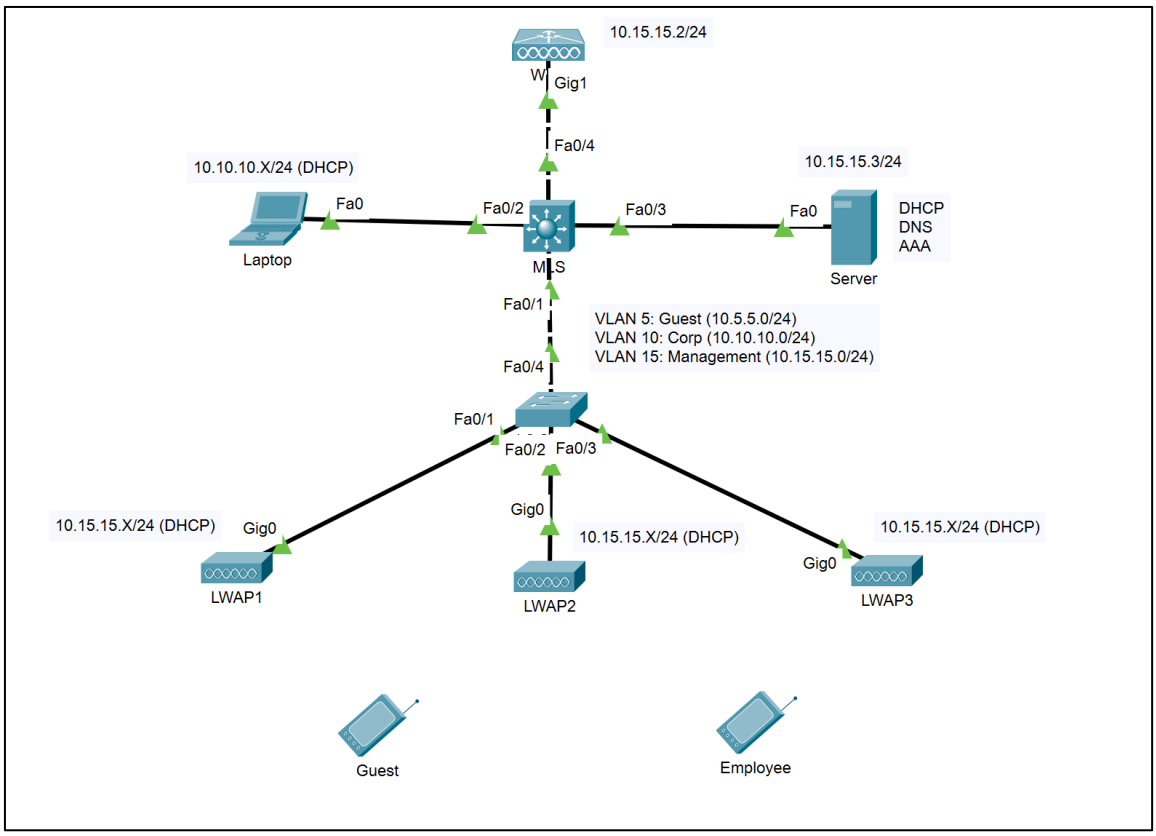
Note: The device model is now hidden in order to free some space for the device names and the port numbers/labels. Your port numbers maybe different, depending on which you connect first, second, etc.

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.

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.



We will have three VLANs – VLAN5 (Guests), VLAN 10 (Corp) and VLAN15 (Management). They will be mapped to the 10.5.5.0/24, 10.10.10.0/24 and 10.15.15.0/24 subnets, respectively. Let's discuss each device and its function.

The MLS switch (Multi-Layer Switch) will route between these VLANs, so it will have an IP address for each of them. These addresses will act as default gateways for the respective VLANs.

The Laptop is only required for one single purpose – in order to configure the controller (WLC). When you click on the controller, you can only configure its IP address and some other port details, but you need a browser to connect to the web management and make all the configurations. For that purpose, we will use the browser from the Laptop (and we also need routing between these devices)

The WLC, as you can guess, is our Wireless Lan Controller. This is "the brain" for the access points (LWAP1, LWAP2 and LWAP3), which will not have individual configurations and settings. Instead, they will build a tunnel to the controller (called CAPWAP) and take their settings from there. In the WLC, you will configure

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 on overview what is the purpose of each device, lets 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

© SoftUni – https://softuni.org. Copyright document. Unauthorized copy, reproduction or use is not permitted.
Follow us:

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:

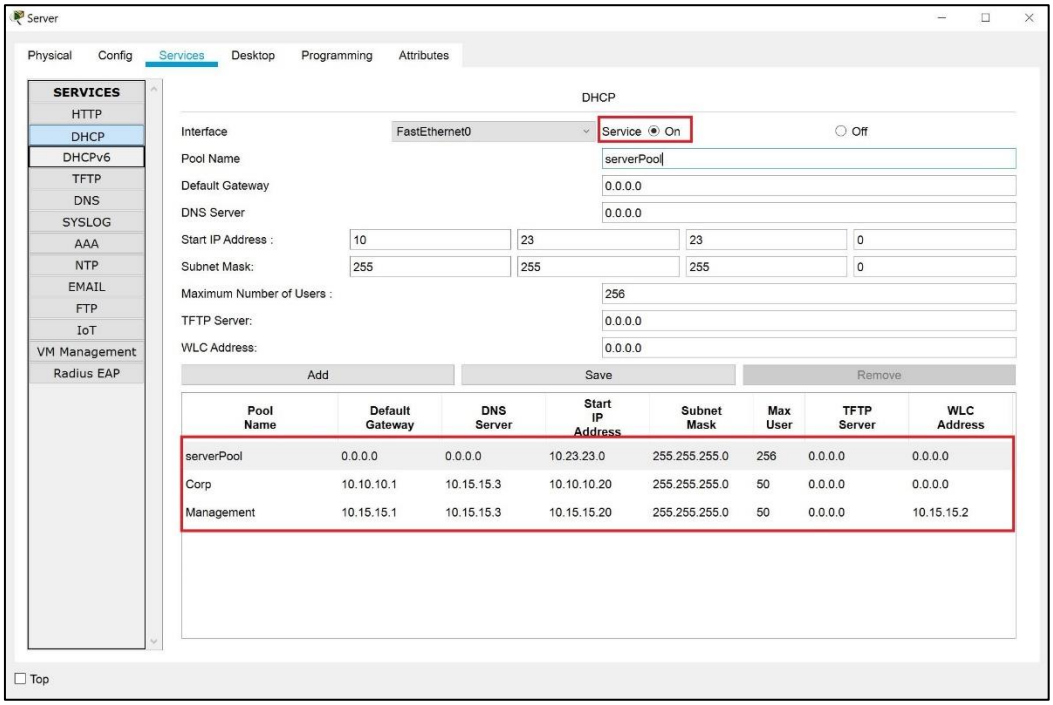
- **Corp**
  - Default Gateway: **10.10.10.1**
  - DNS Server: **10.15.15.3**
  - Start IP address: **10.10.10.20**
  - Subnet Mask: **255.255.255.0**
  - Maximum number of users: **50**
  - TFTP Server: leave default
  - WLC Address: leave default
- **Management**
  - Default Gateway: **10.15.15.1**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

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

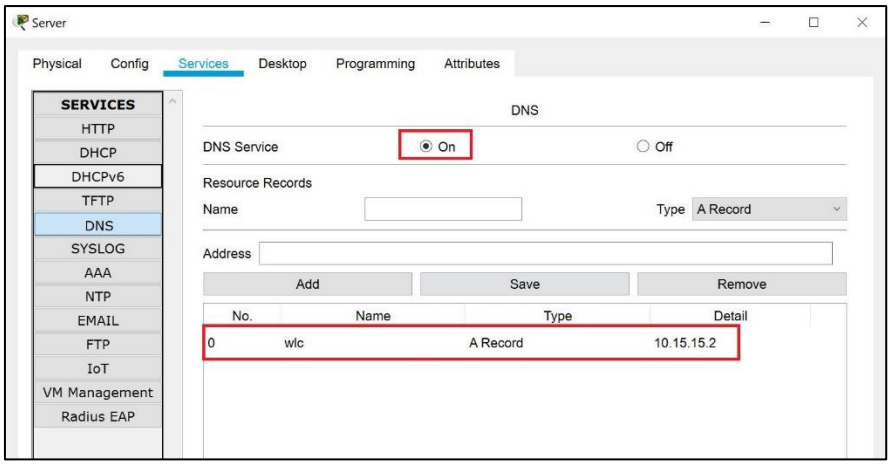
- WLC Address: **10.15.15.2** (this is how the access points will find their controller)

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.



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



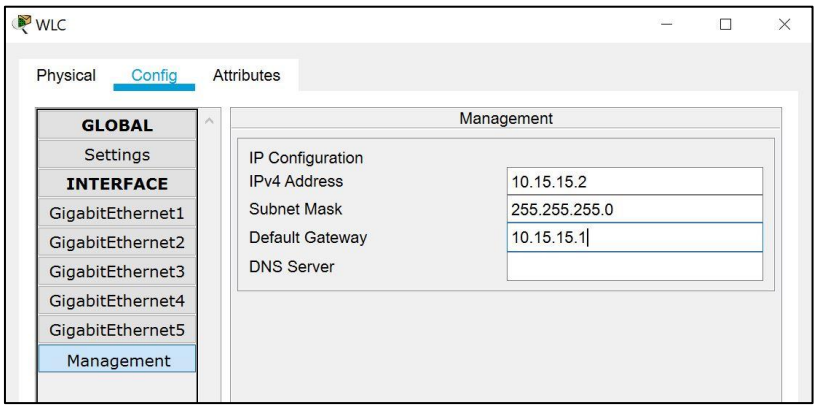
© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

❖ 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:

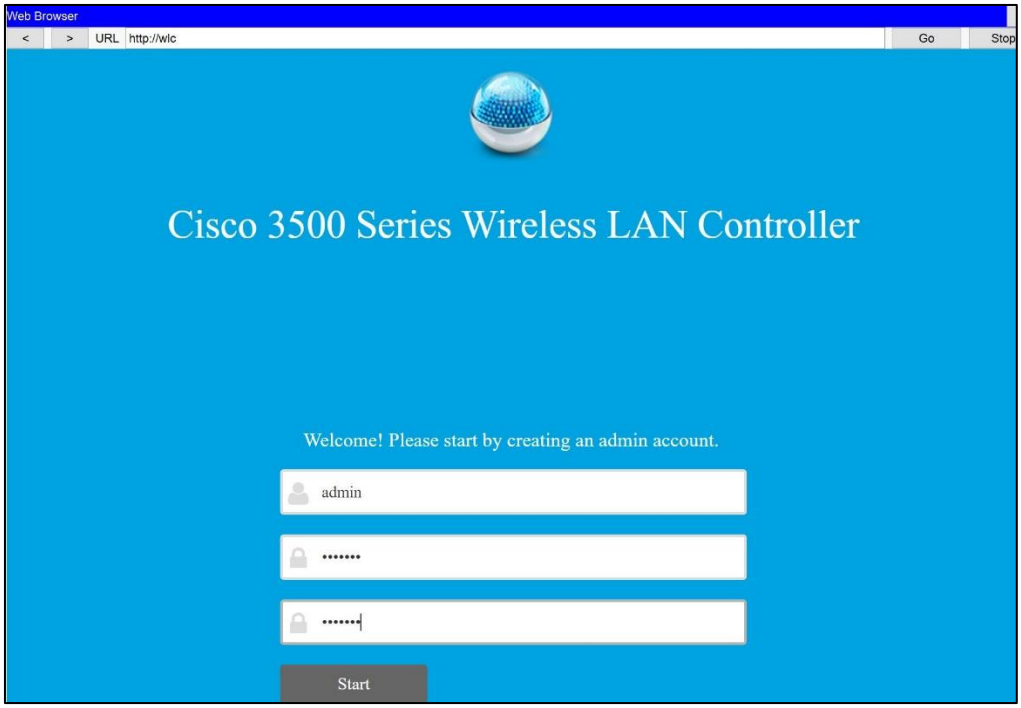
1. Go to Config -> Management and configure the IP settings of the controller:
   - IP address: 10.15.15.2
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 10.15.15.1



   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

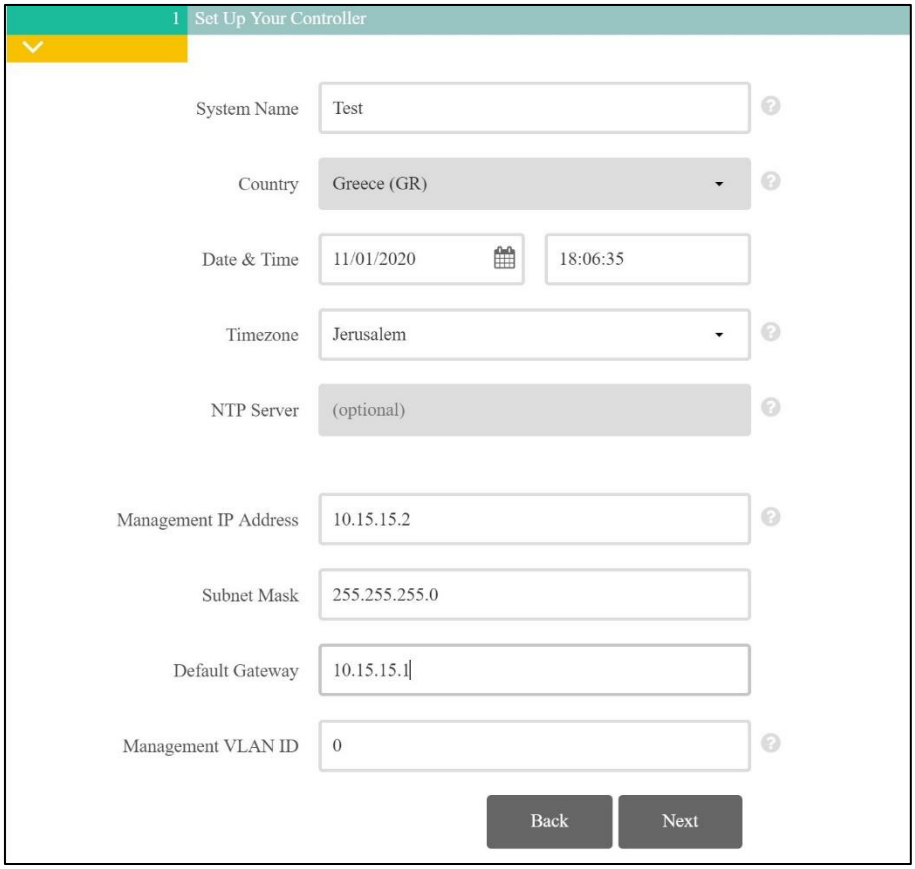
© SoftUni – https://softuni.org. Copyright document. Unauthorized copy, reproduction or use is not permitted.
Follow us:



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

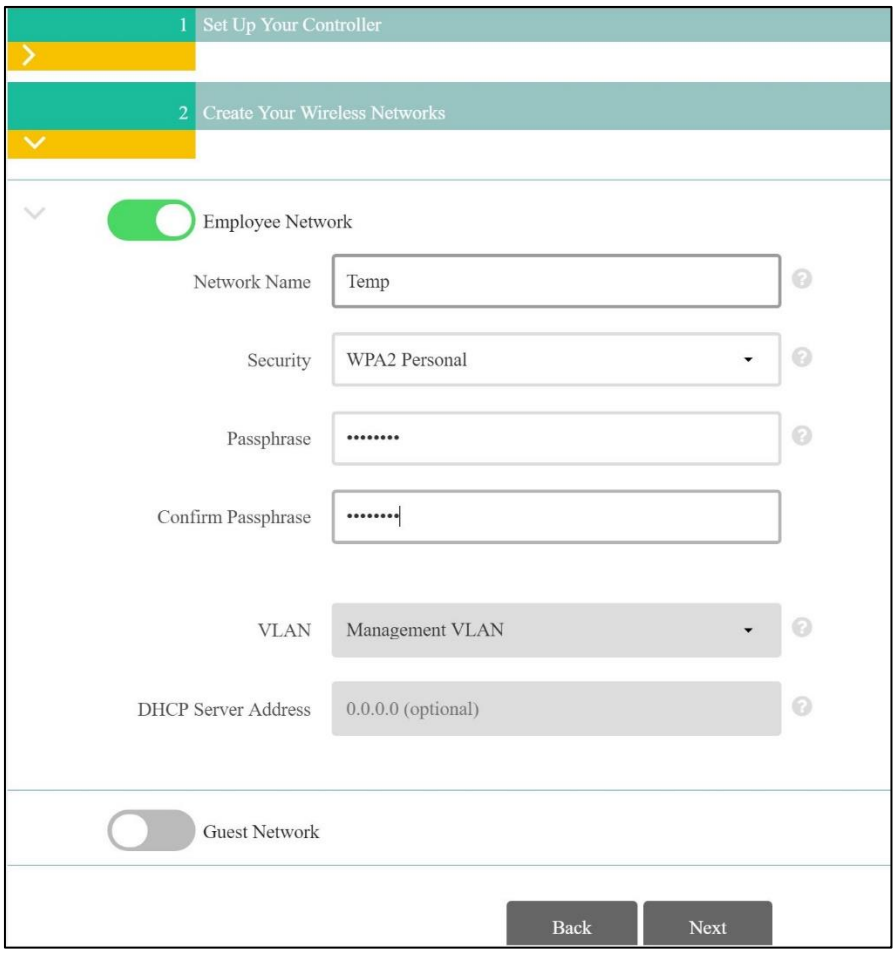
© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.



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

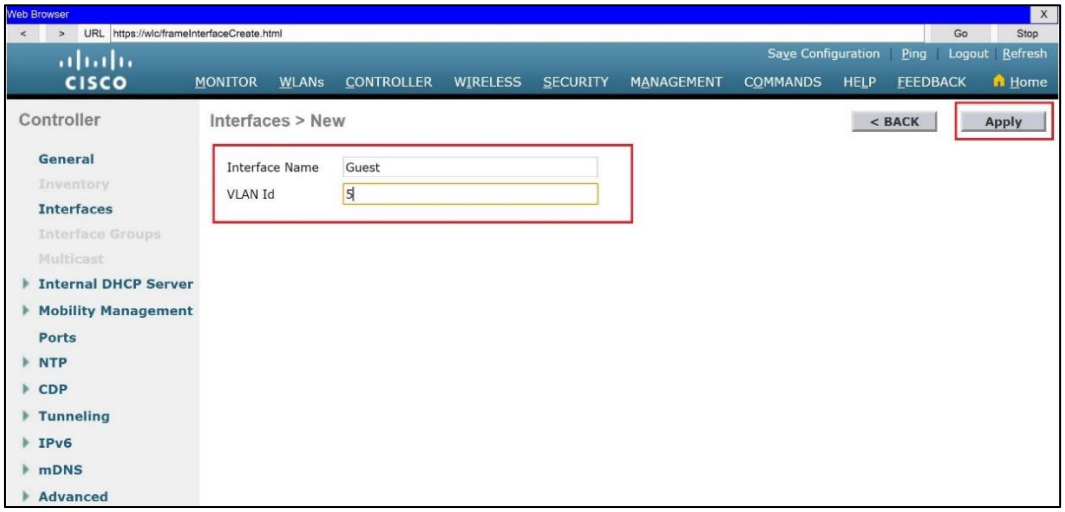
© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.



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

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

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**

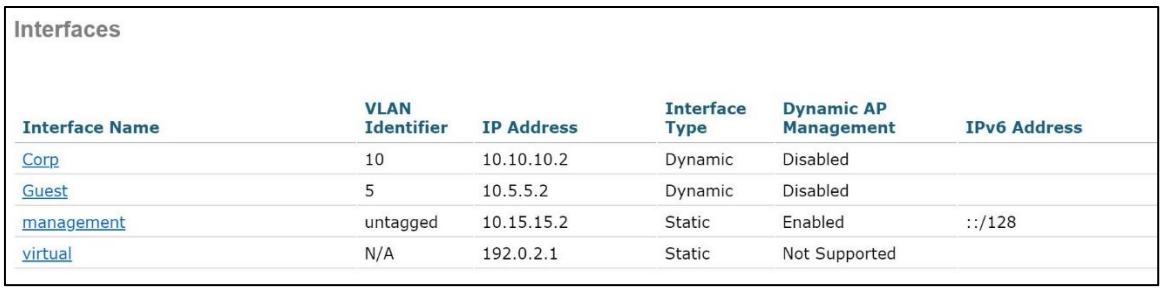
Then go to the upper right corner and click Apply (confirm the warning message)

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

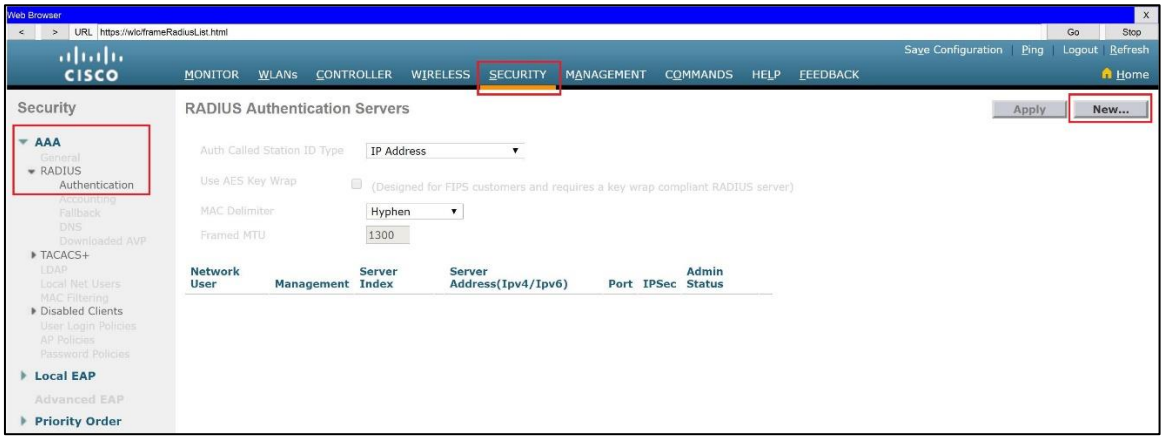
Go back to Controller -> Interfaces and create one more. This time your interface should be named **Corp** and associated with VLAN 10. The other settings of this interface should be:

- 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:



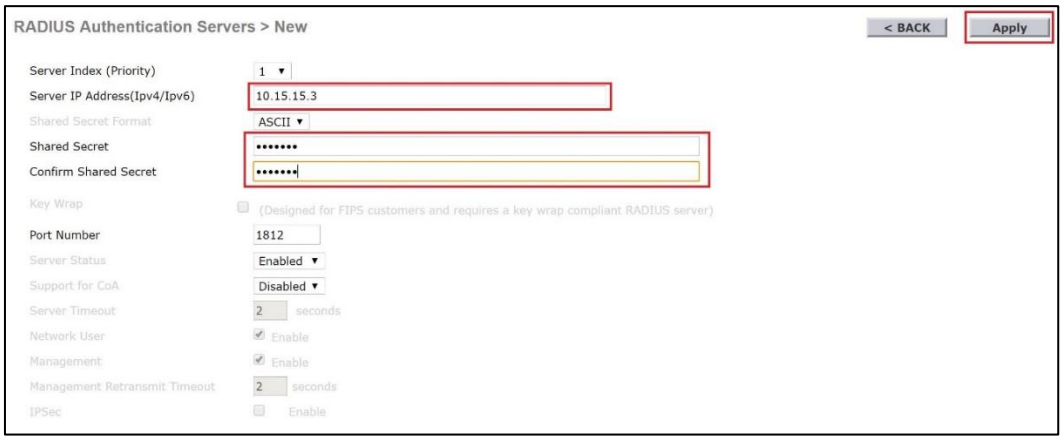
9. Put the RADIUS (AAA) server in the configuration.
   Before we create the WLANs, we will configure the WLC to know where our RADIUS/AAA server is, so later we will point to it. To do this, go to SECURITY -> AAA -> RADIUS -> Authentication and click on New



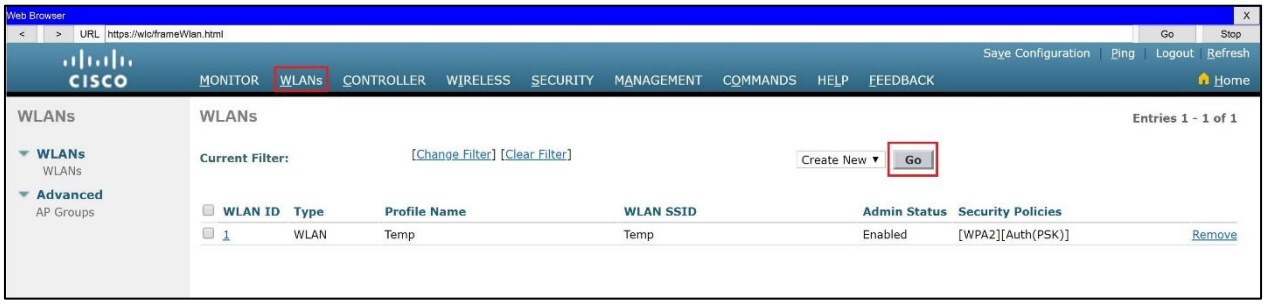
© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

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

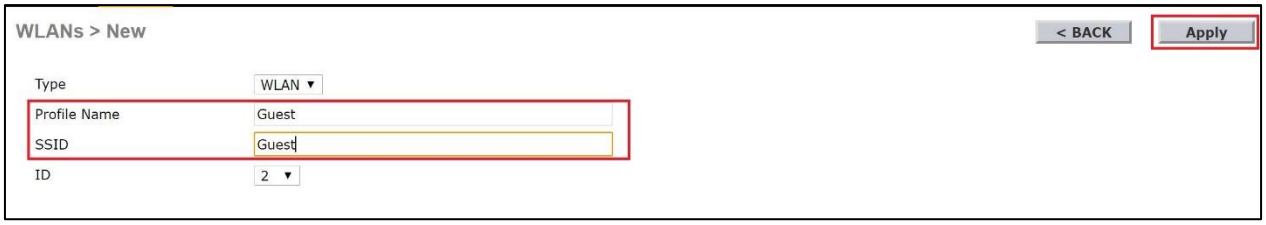
- Server IP Address(Ipv4/Ipv6): **10.15.15.3**
- Shared Secret: **SoftUn1**
- Confirm Shared Secret: **SoftUn1**



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

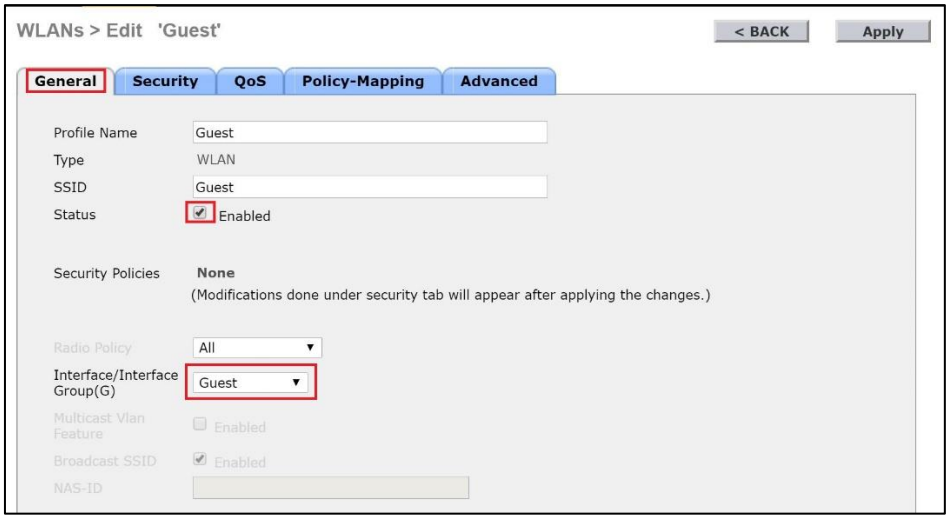


For Profile Name and SSID type **Guest**. Then click Apply.

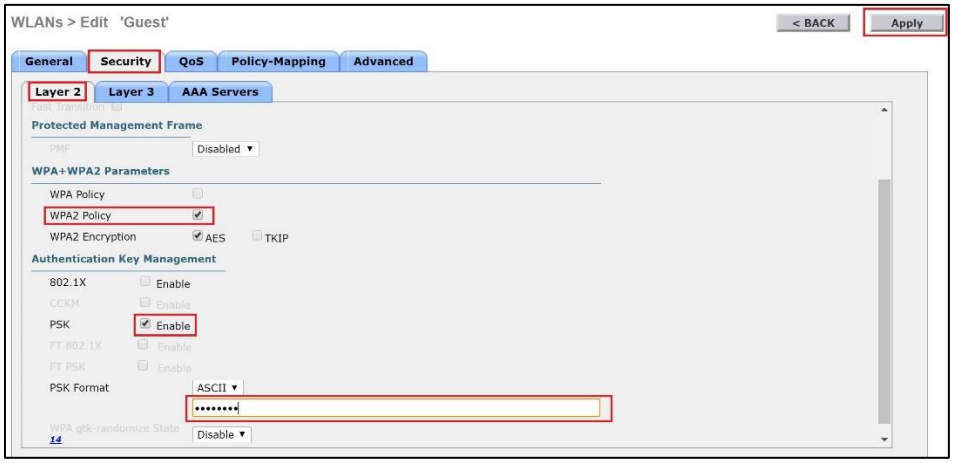


Next, enable the SSID and associate it with the Guest interface.

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

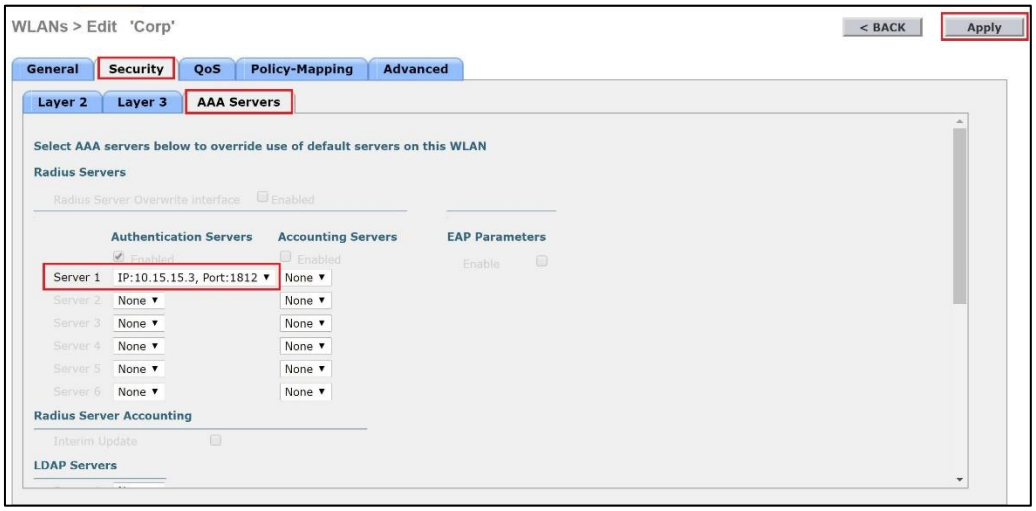


Go to the Security -> Layer 2 tab and select WPA + WPA2.
Then click on WPA2 Policy. After this click on Enable next to PSK and enter **Guest123** as a password (the pre-shared key). Click on Apply.



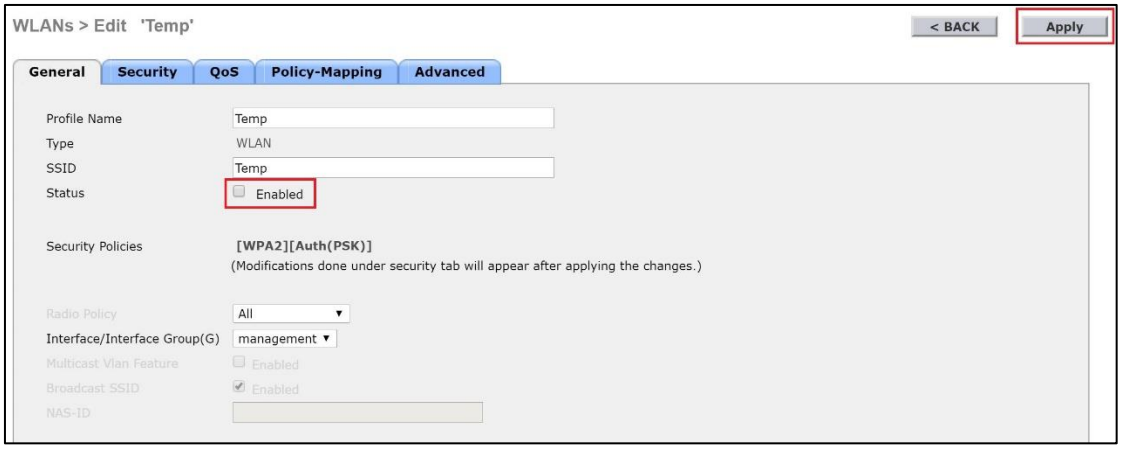
Go back to WLANs and create one more, this time it will be named **Corp** (for both Profile Name and SSID). Then enable it and associate it with the Corp interface.
In the Security -> Layer2 tab of this WLAN, select again WPA + WPA2 and WPA2 Policy but this time click Enable next to 802.1X.

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.



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.

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.



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):

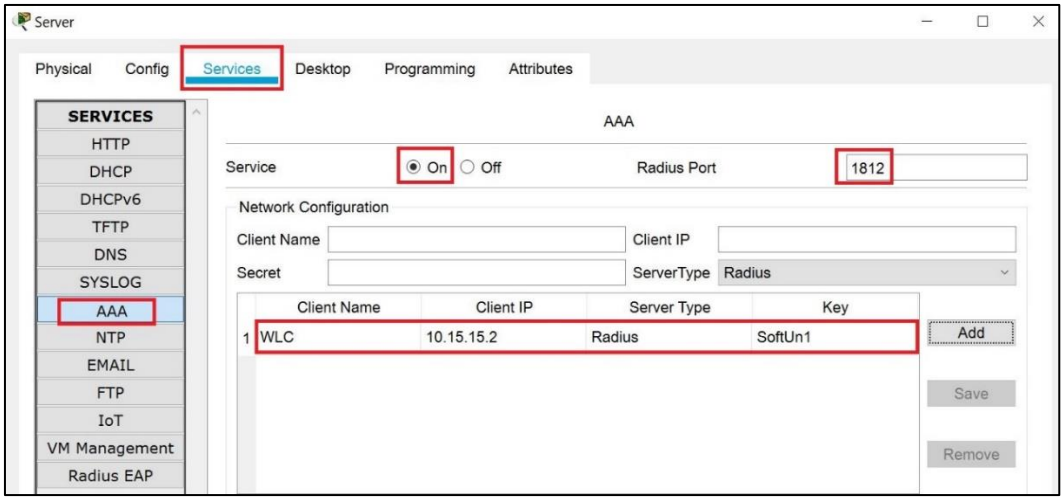
We have configured the WLC to point to a RADIUS/AAA server when it comes to authentication for the Corp WLAN/SSID which means that the credentials will be checked on an external server. Let's configure this server to accept those authentication request from the WLC (which is the RADIUS client!) and also 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)

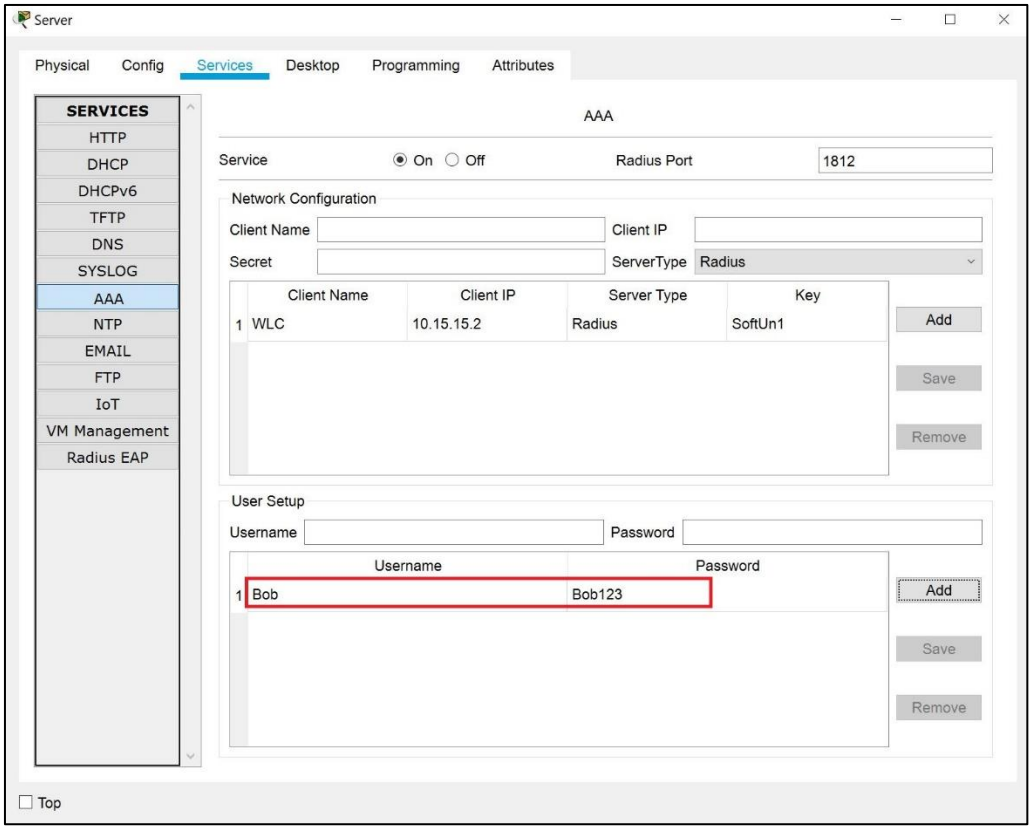
© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

- 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)



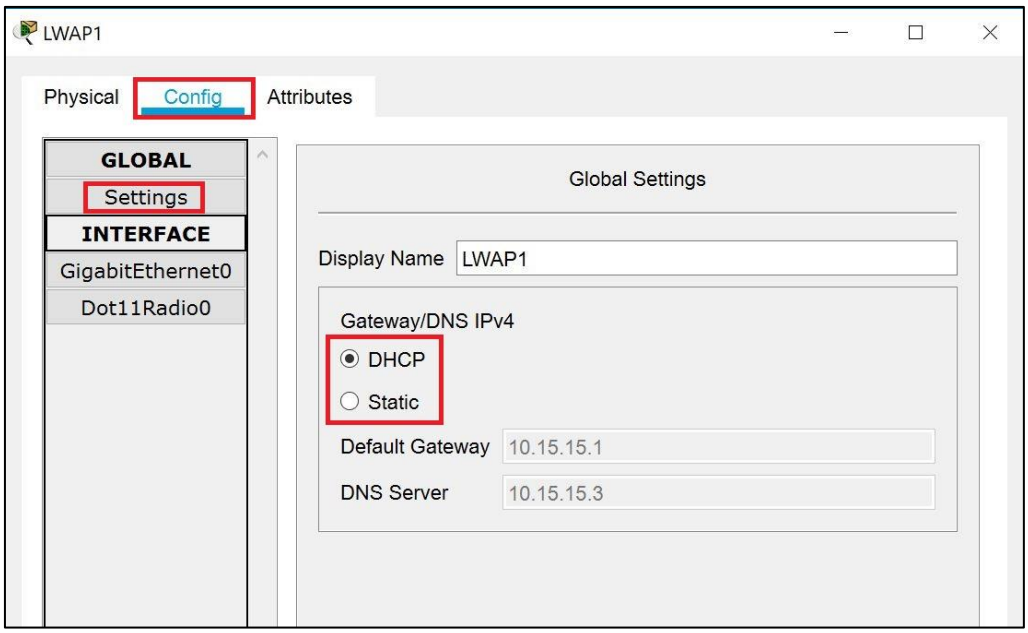
Then, configure one user account - again there (Services -> AAA) but in the second part of the window (called User Setup). For Username type **Bob** and for Password type **Bob123**. Then click on Add

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

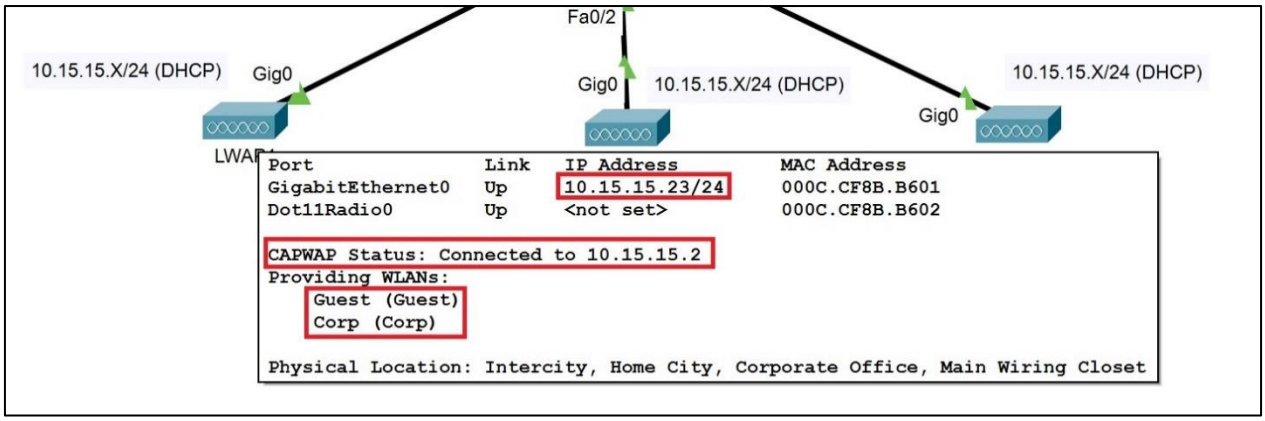


- The access points (LWAP1, LWAP2 and LWAP3):
  You don't need to configure anything there because each access point should automatically receive its IP address, subnet mask, default gateway, DNS server and information about where the controller is, from the DHCP. Then, it will build the CAPWAP tunnel 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

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.



After several seconds, you should see the Default Gateway configured for 10.15.15.1 and the DNS Sever 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

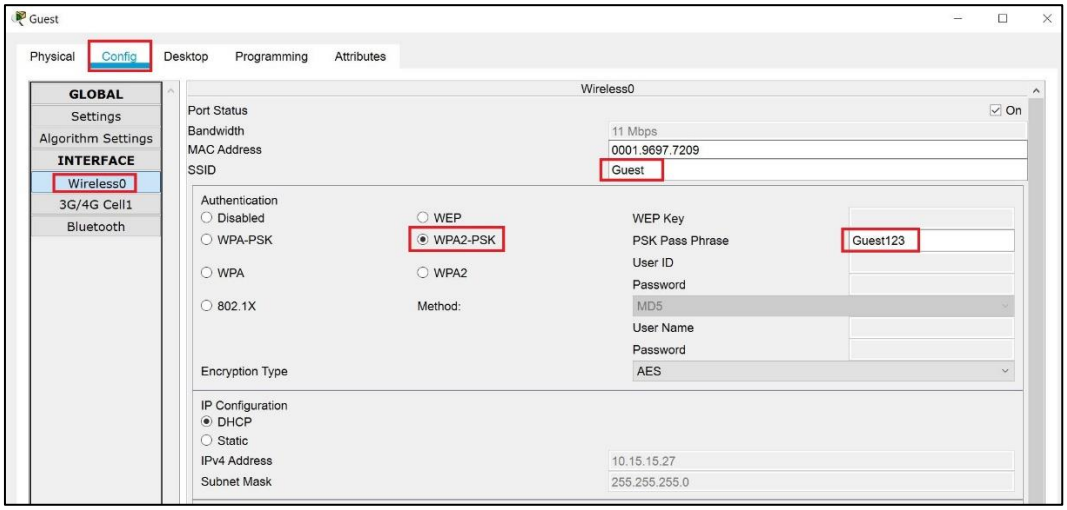


© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

Task 3: Connect the clients

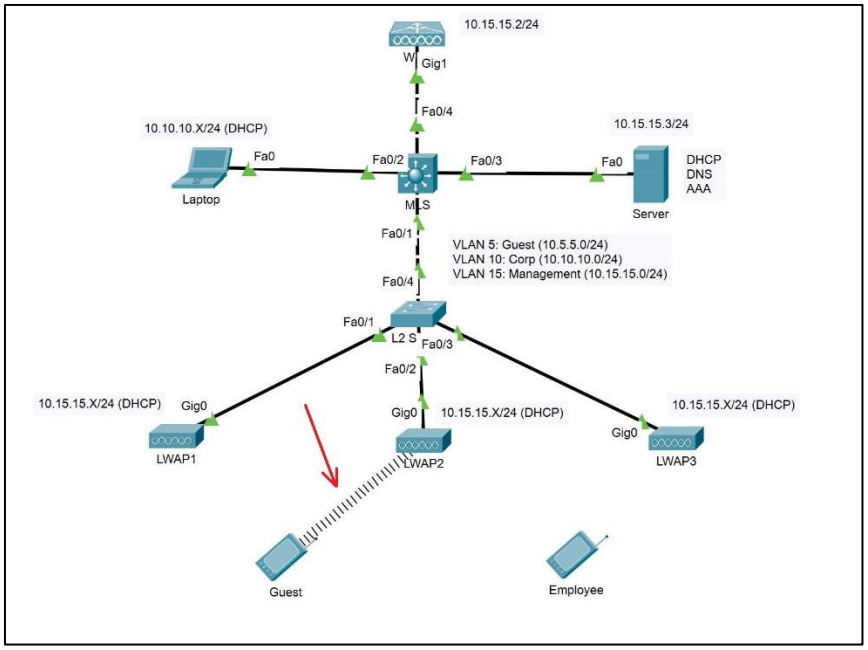
Now that our infrastructure is ready, it is time to connect the wireless clients to the network.

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)



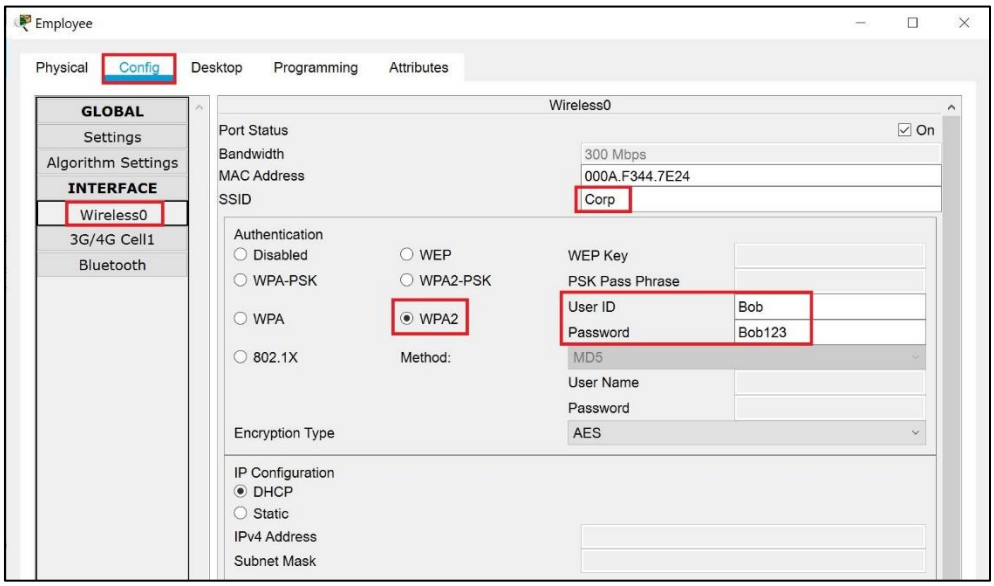
   Wait several seconds and look at the topology – you should see the wireless connection between the Guest device and one of the access points (either LWAP1, LWAP2 or LWAP3 – you cannot control which one, it is random here)

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

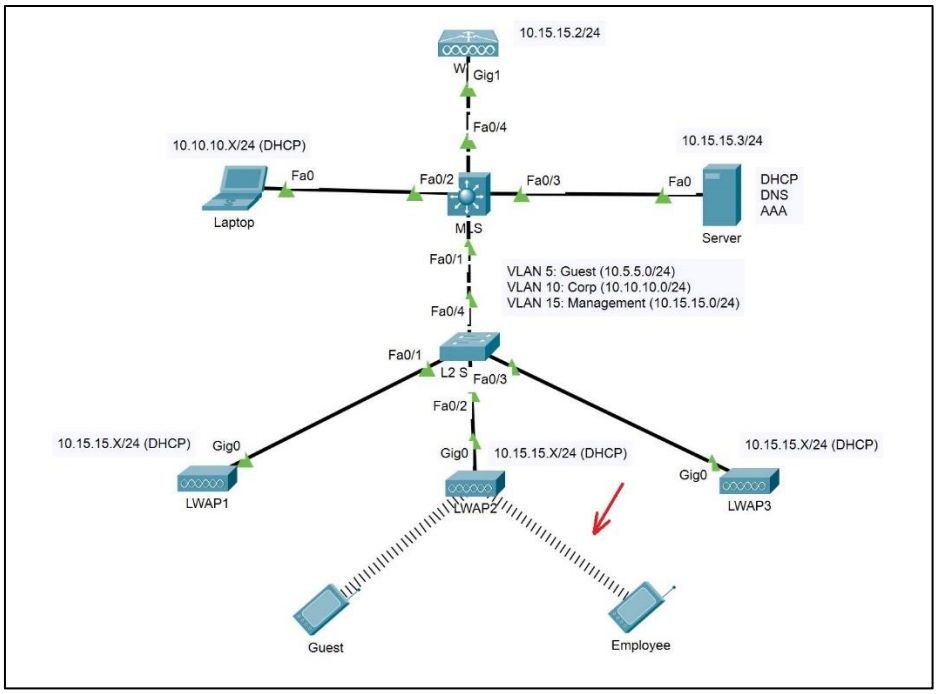


2. The Employee device.
   Go to Config -> Wireless0 and next to SSID type **Corp**. Then under Authentication select WPA2 (instead of WPA2-PSK). Then, type the credentials that you have in your RADIUS/AAA server:
   - User ID: **Bob**
   - Password: **Bob123**

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.

© SoftUni – https://softuni.org. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.