INDIVIDUAL ASSIGNMENT

CT133-3-2-SRE

SWITCHING AND ROUTING ESSENTIALS

APU2F2111CS (CYB), APD2F2111CS (CYB)

HAND OUT DATE: 29th November 2021

HAND IN DATE: 27th February 2022

Weightage: 40%

Online Submission Time before = 12: 59 PM

Student Name: Lee Jun Lam [Section A]

Student ID: TP055697

INSTRUCTIONS TO CANDIDATES:

1. Assignment is to be submitted through online submission (Moodle).
2. Students are advised to underpin their answers with the use of references (cited using the Harvard Name System of Referencing).
3. Late submission will be awarded zero (0) unless Extenuating Circumstances (EC) are upheld.
4. Cases of plagiarism will be penalized.
5. You must obtain 50% overall to pass this module.

Table of Contents

Section A: Report

1.0 Introduction

1.1. Company's Background

A fiber optic firm named Fiberoptic Systems Inc. has declared a planning to expand its services and locations in numerous locations (Remote Office Branch) and online (Remote Branch).

1.2. Objectives

A representative from the firm, Fiberoptic Systems Inc has request the network administrator to work on the new network's design and prototype in accordance with the network logical topology specified in the Cisco Packet Tracer's network request. The client's requests, such as various VLANs for each department in each branch, security methods such as implement port security to mitigate LAN attacks and MAC address table attacks, and a wireless network topology by implementing DHCPv4 to operate across multiple LANs for Cyberjaya Remote Branch, must be included in the prototype network. End devices, such as desktops and laptops from the HQ branch and the Cyberjaya Remote Branch, must be able to connect with one another and with the server farm. Any further detail about any additional features or security mechanisms will be updates and further stated in the report.

1.3. Assumptions

In order to increase the network's efficiency and security, the network executive announced plans to replace the current structure with a new VLAN design, notably at the HQ branch in KL based on the number of departments. Aside from that, the Remote Office Branch (Server Farm) will be managed remotely by the Management department at HQ. To make wireless network configuration and access easier, the network administrator decides to introduce WLC WLAN at the Cyberjaya Remote Branch.

2.0 Proposed WLAN Architecture

The network executive has proposed to implement a Wireless Architecture at the Cyberjaya remote branch (WLC Management Network). Wireless architecture typically utilizes an access point which allows host device to connect. There are one type of access points in a Wireless architecture is utilize which is Controller-based Access Points.

Lightweight Access Point (LAP), also known as controller-based access points, require a Wireless LAN Controller (WLC) for centralised management (updates, configuration, etc.) and individual configuration of APs is not necessary. Thus, Lightweight access points are established in opposition to autonomous access points. Controller-based access points are most commonly seen in big environments. The intention of this architecture is to make expanding a wireless network easier. The WLC is used to configure the lightweight controllers that are dependent on it. To put it another way, they're just plug-and-play network additions. It is possible to turn on a new little device and following with searching and download WLC settings. Protocols, security, and any other configuration-related elements are included.

In short, the network executive proposed to incorporate LAPs for each floor of the remote branch: LAP-Floor 1, LAP-Floor 2, LAP-Floor 3, LAP-Mgmt, LAP-IT.

2.1 WLC Configuration

Step 1: Setting the network configuration of RB-Admin-PC and RB-WirelessLAN Controller

A WLC does not have an inbuilt user interface thus it must be configured through an end device. Thus, Admin PC is used to assigned a static IPv4 address to both Admin PC and WLC in order to handling WLC configurations and other network configuration are configured.

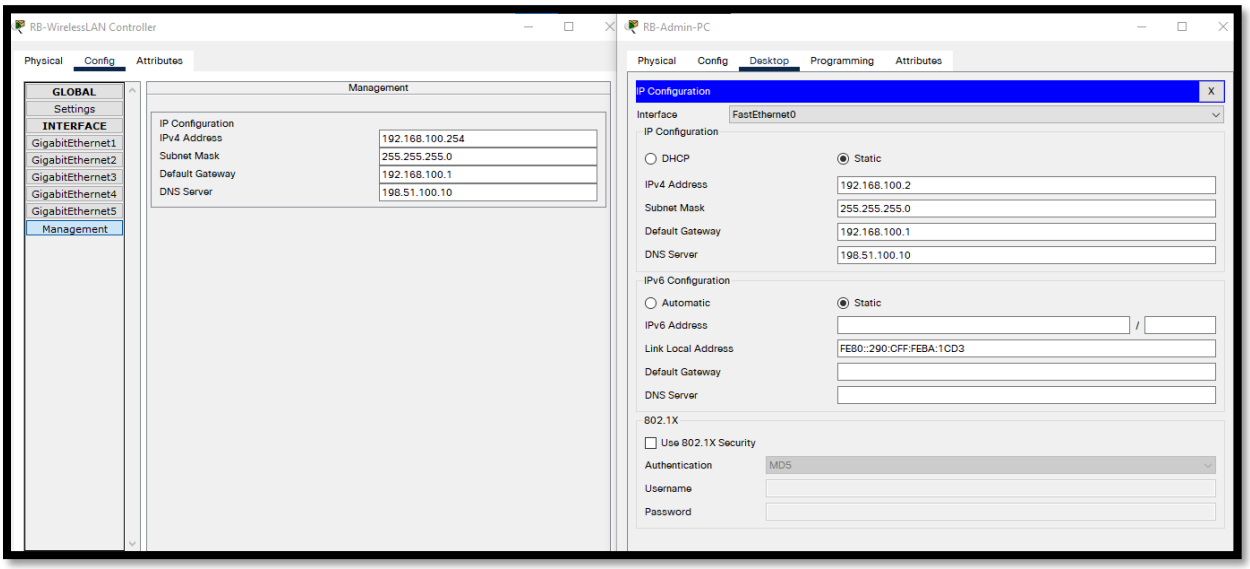

Figure 1: Setting up the network configuration of RB-Admin-PC and RB-WirelessLAN Controller

Step 2: Registration of WLC through RB-Admin-PC

Browse to http://192.168.100.254 in web browser by using RB-Admin-PC. A configuration wizard will display for WLC initial setup. In this scenario, username is configured to admin and the password is Cisco123.

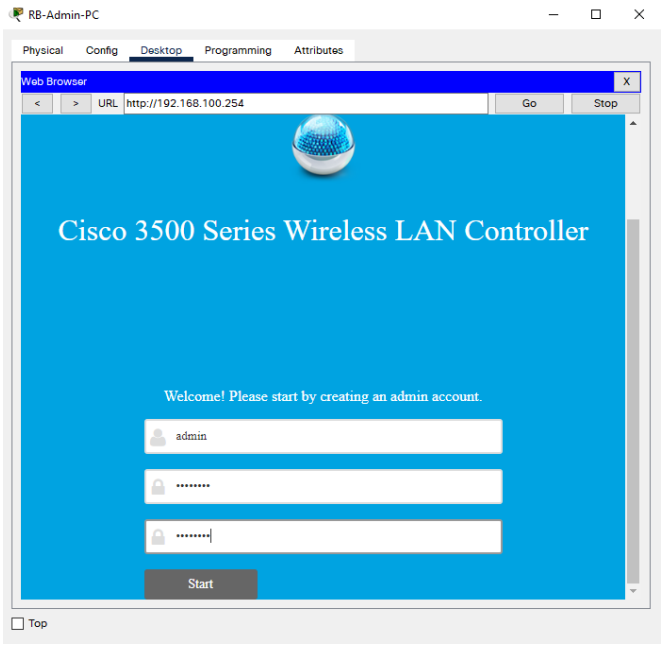

Figure 2: Configuration Wizard Appears for WLC registration

Step 3: Complete WLC Setup

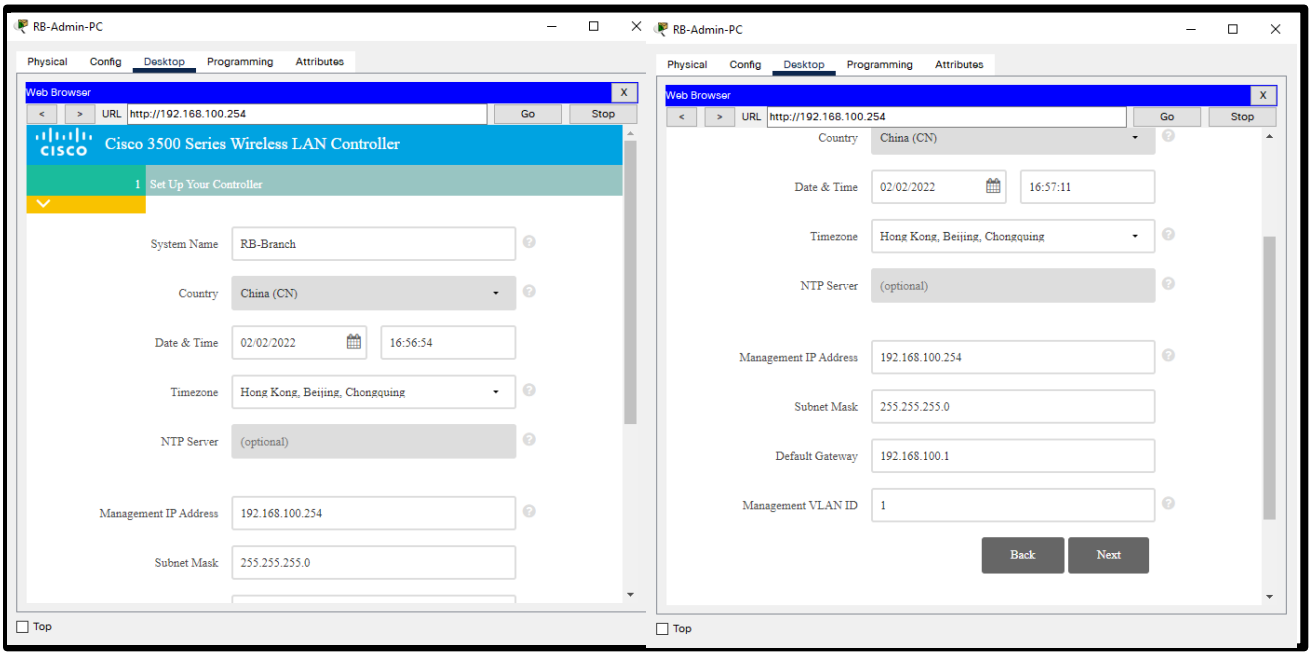

Figure 3: Initial setup for WLC (first setup page)

In the first setup page, fill in the suitable system name, management IP address, subnet mask, default gateway and management VLAN ID.

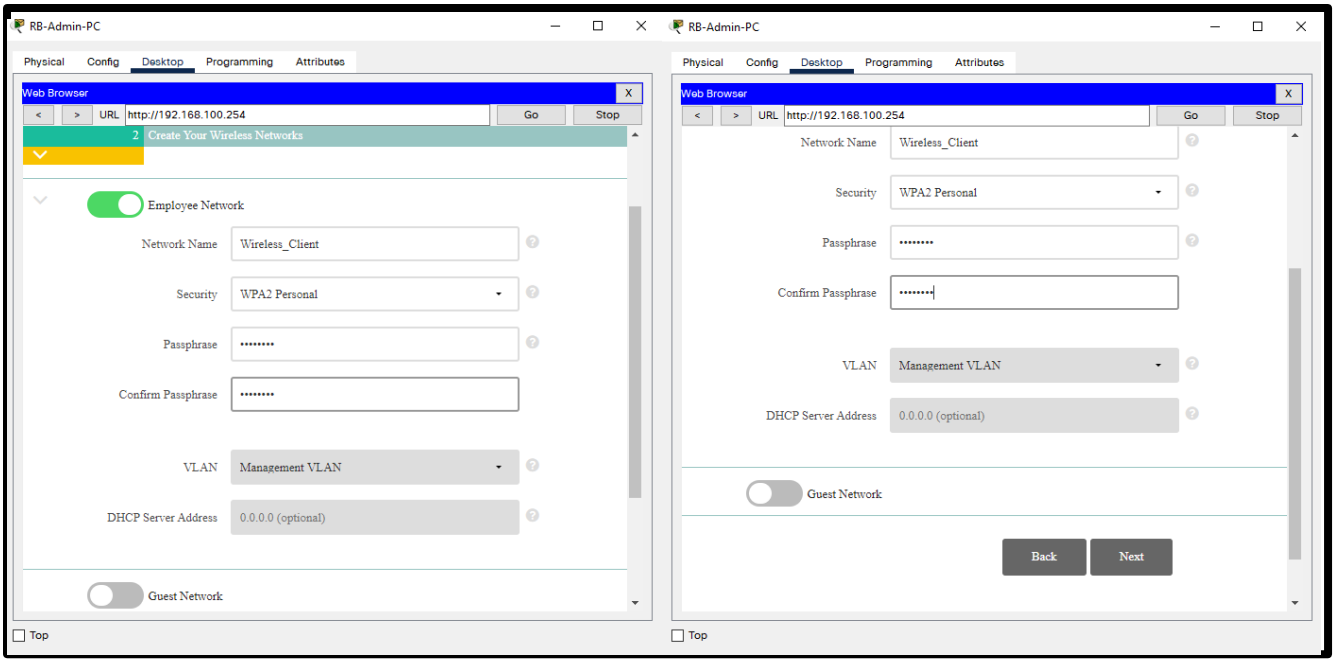

Figure 4: Initial setup for WLC (second setup page)

In the second setup page, fill in the Network Name, Security, Passphrase (Cisco123)

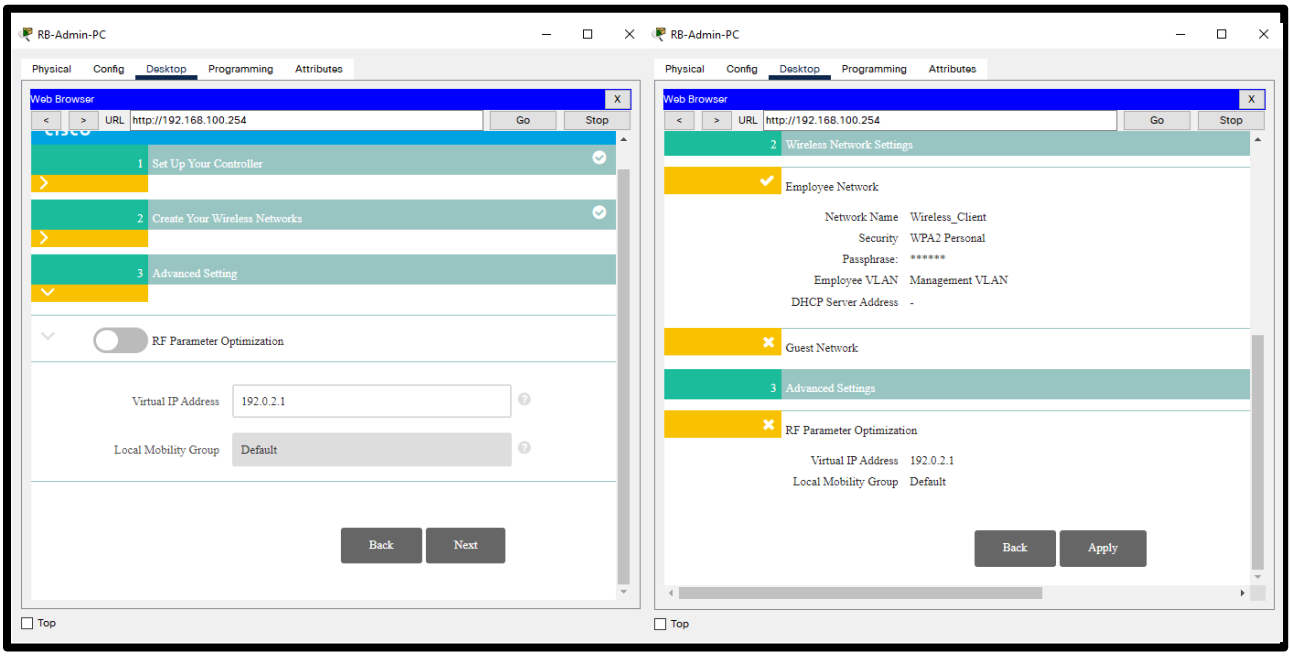

Figure 5: Initial setup for WLC (third setup page)

No changes should be made in the third setup page. Double check all the information and select “Apply” button to proceed. A confirm message will display, select “OK” option to save the setup configuration.

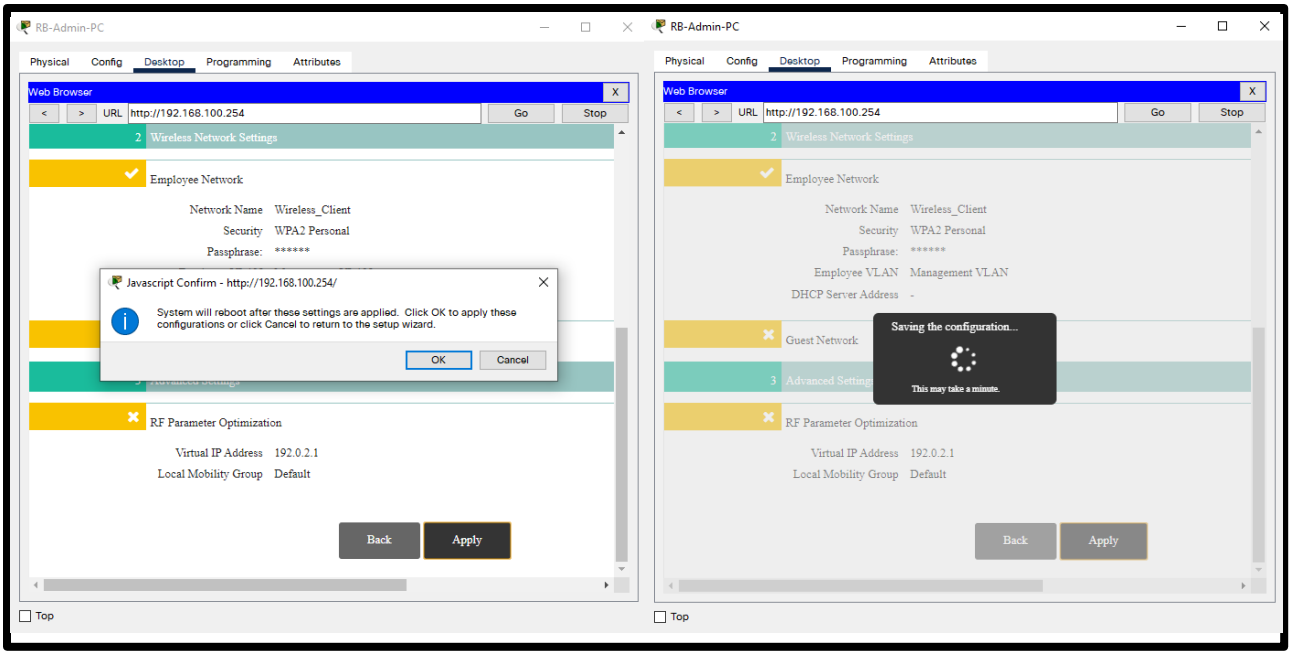

Figure 6: Saving the configuration

Step 4: Accessing WLC

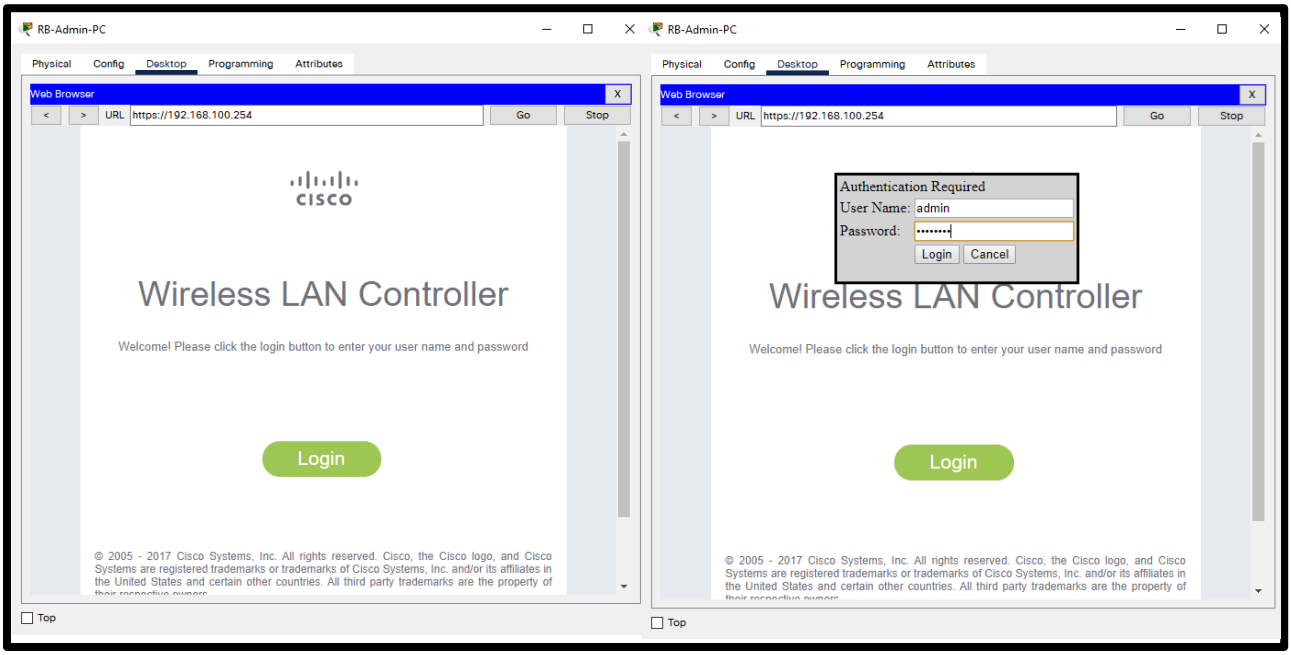

Figure 7: Accessing Wireless LAN Controller by using https

Once the setup configuration in Step 3 is completely saved, access the WLC by using https://192.168.100.254 (https instead of http) in the RB-Admin-PC web browser. Username is admin and the password is Cisco123 (configured in Step 2).

Step 5: Creating new interface in WLC

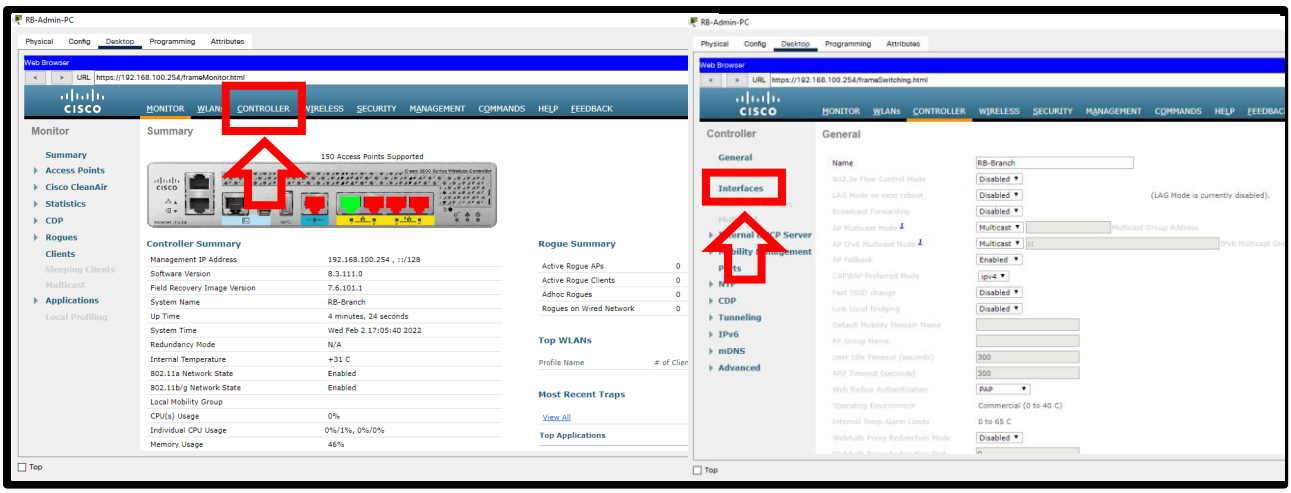

Figure 8: Accessing Interface tab in WLC

The LEDs on the front panel provide the system status, if the LED is solid green, it means the WLC is ready. Access the **Controller** tab follow by **Interface** tab to create or edit existing interfaces in the WLC.

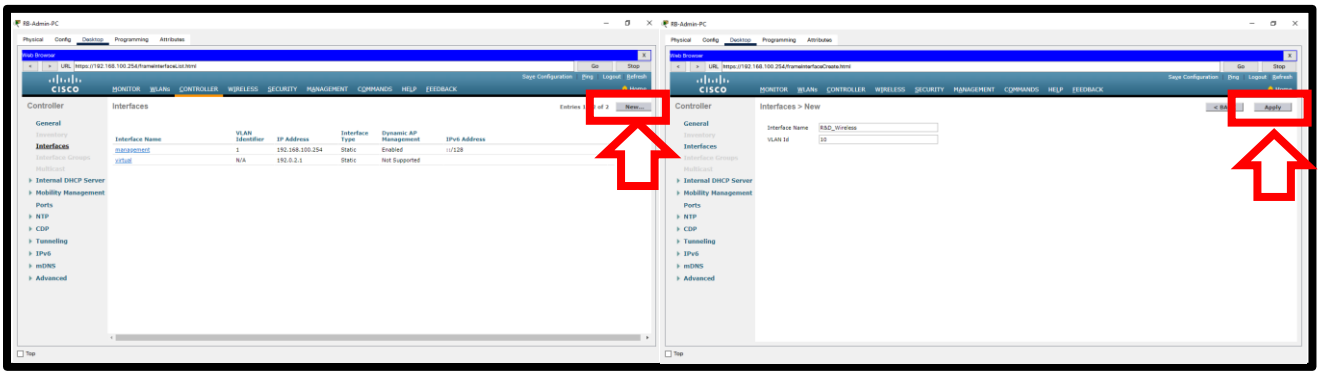

Figure 9: Creating a new interface with VLAN 10 in the WLC

From the interface page, select **New…** to create new interface with the name **R&D_Wireless** and set the VLAN ID as 10. This VLAN will be used as R&D Department data traffic and select **Apply** to create new interface.

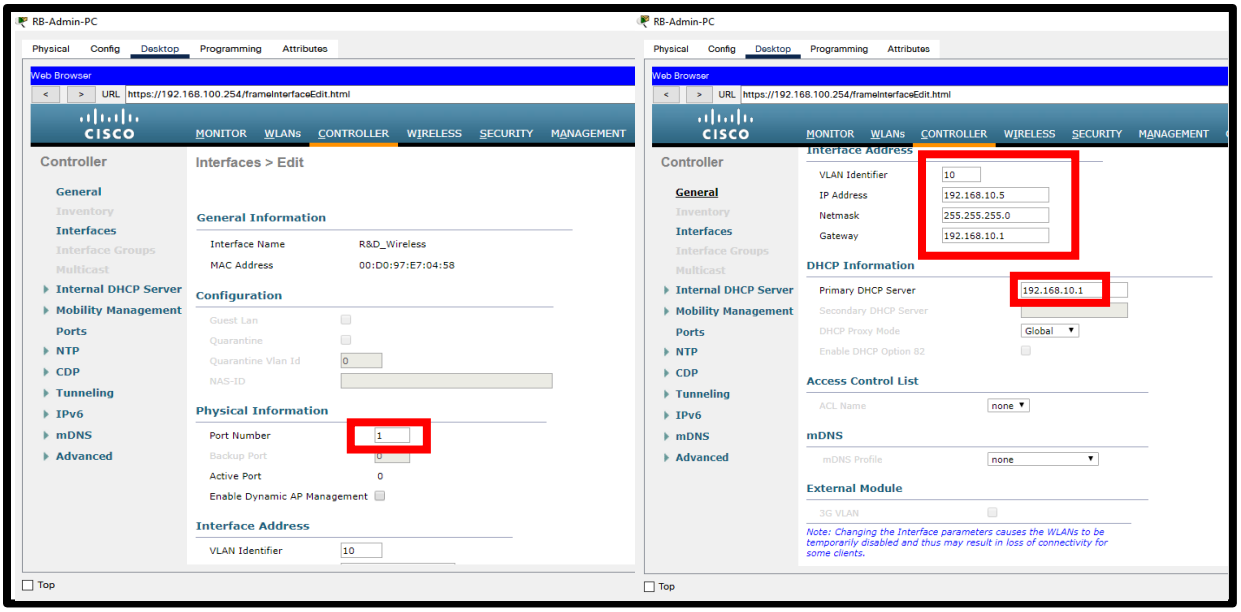

Figure 10: Configuring port number, interface address and DHCP information for WLC

The port number, VLAN Identifier, IP Address, Netmask, Gateway and Primary DHCP Server is configured for the interface R&D_Wireless.

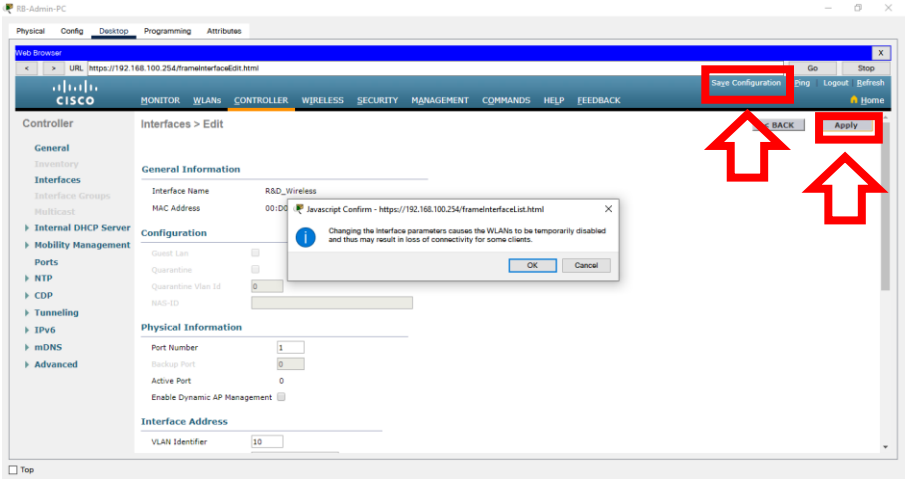

Figure 11: Finalize the creation of an interface

Select **Apply** and a pop-up message will display. Select the **OK** option follow by selecting the **Save Configuration** label to save the configuration.

Step 6: Creating an internal DHCP Server

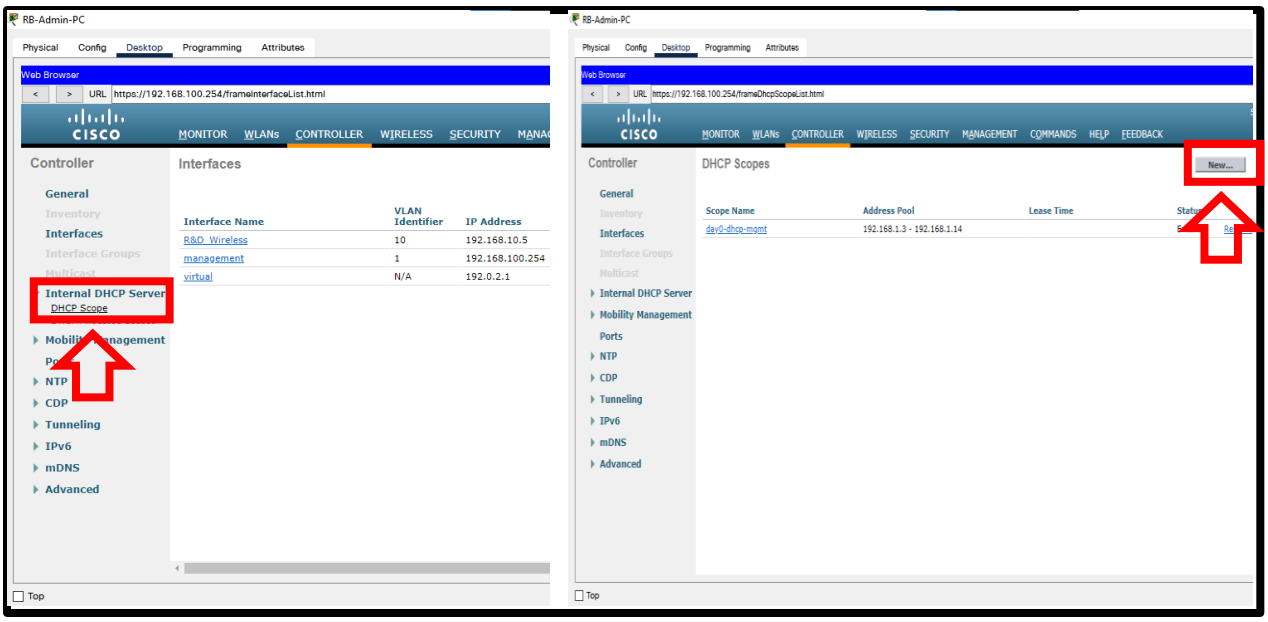

Figure 12: Navigate to DHCP Scope page

Select **DCHP Scope** under the Internal DHCP Server Tab. From the DHCP Scope page, select **New…** to create new DHCP Scope.

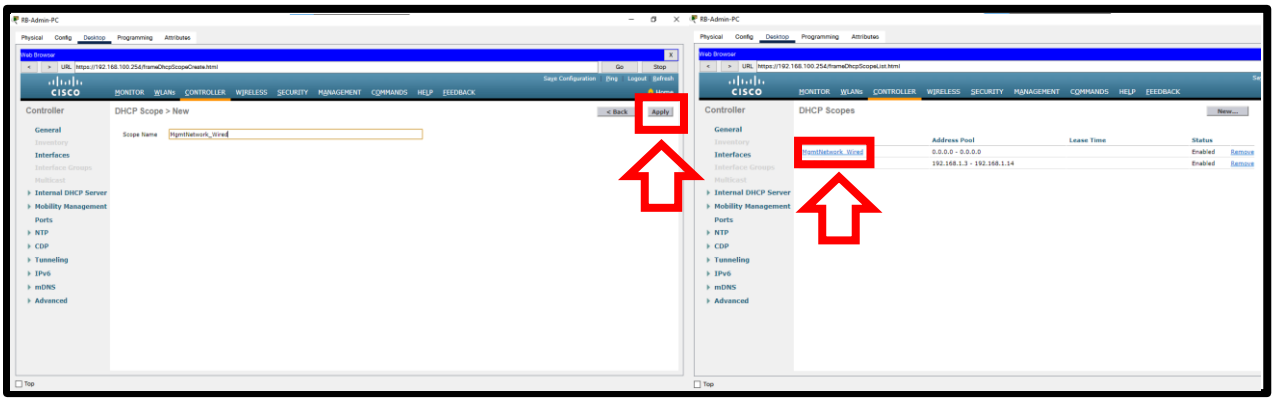

Figure 13: Create New DHCP Scope

Select **Apply** to create the new DHCP Scope and select on the newly created DHCP Scope link for configuration purpose.

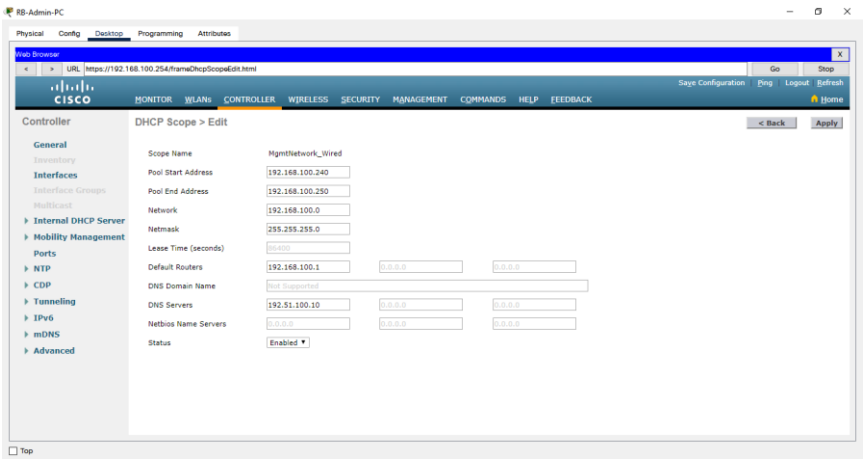

Figure 14: Configuring DHCP Scope Information

Enter the appropriate Pool Start Address and Pool End Address, network and its netmask, default-router gateway IP Address, DNS Server IP Address and select **Apply** to save the configuration.

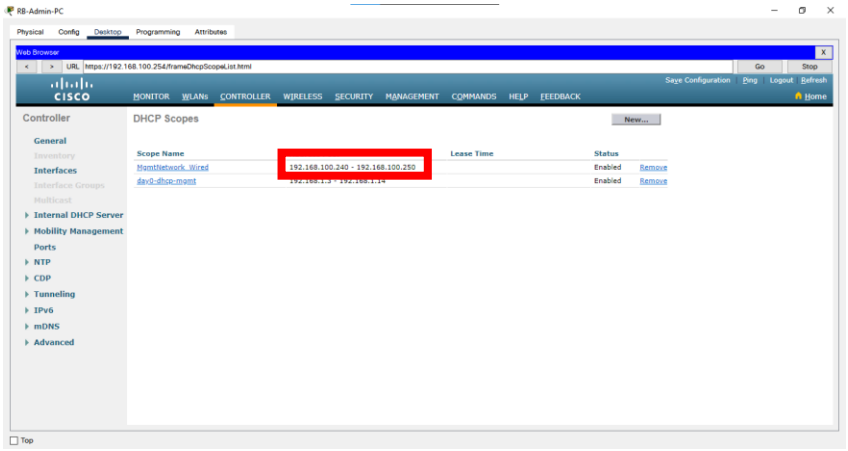

Figure 15: Confirmation that DHCP Scope has configure

Step 7: WLANs Creation

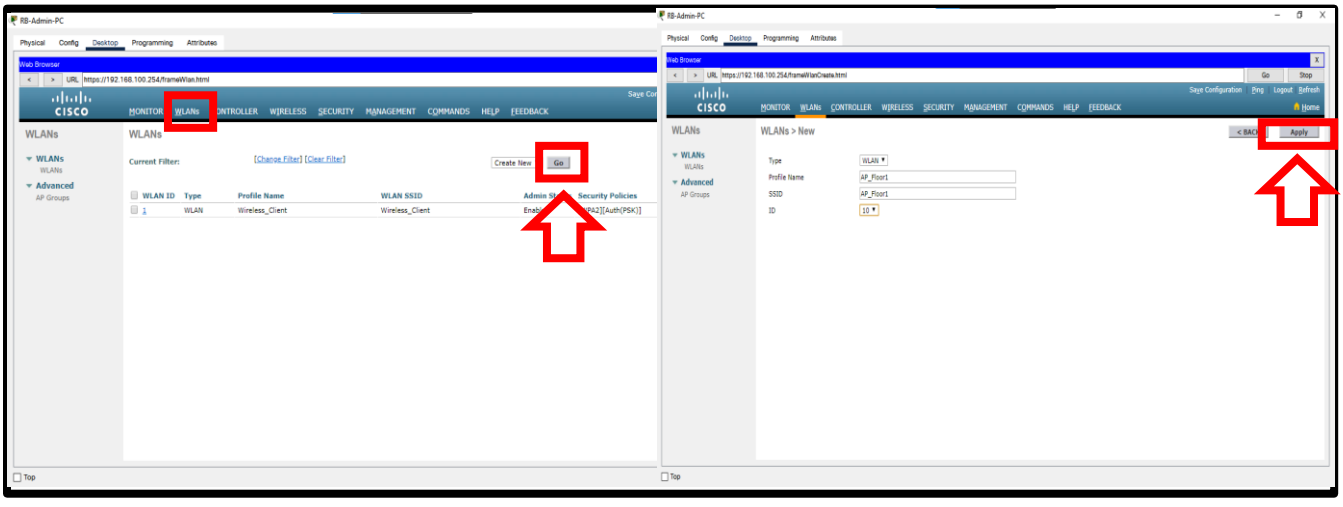

Figure 16: Navigate to WLANs Page to Create New WLANs

Select **WLANs** on the horizontal tab to navigate to WLANs Page. Select **GO** to create new WLAN. In this scenario, Profile Name and SSID is AP_Floor 1 and the ID is set to 10. Then, select **Apply** to navigate to the next page.

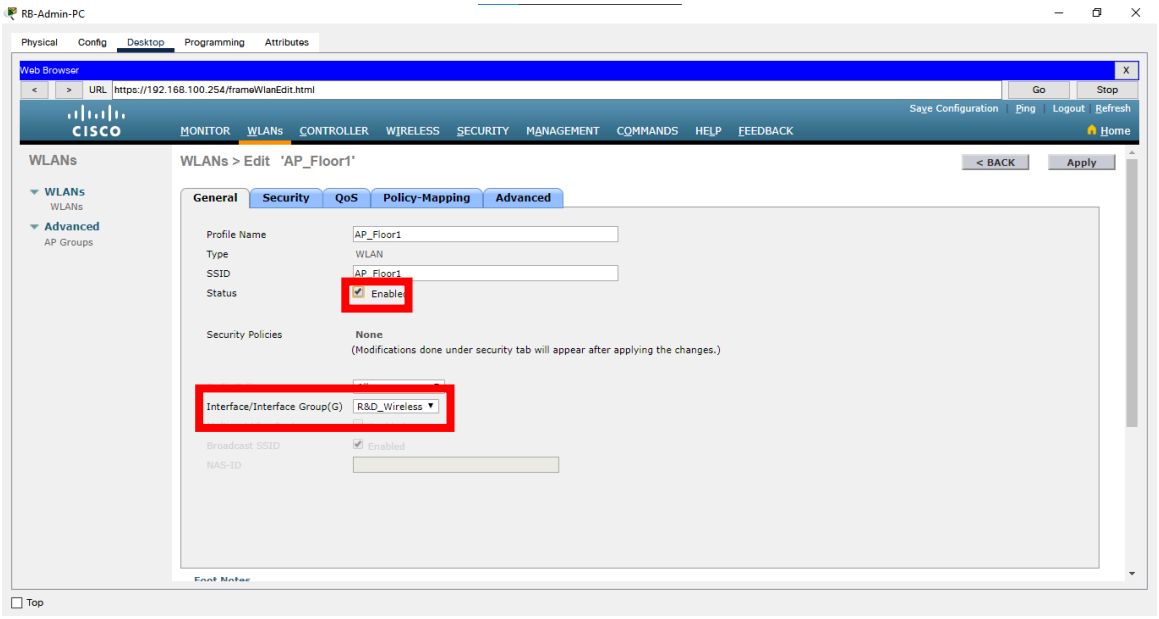

Figure 17: General Configuration for WLANs (AP_Floor 1)

It is important to enable the status and change the interface group to R&D Wireless.

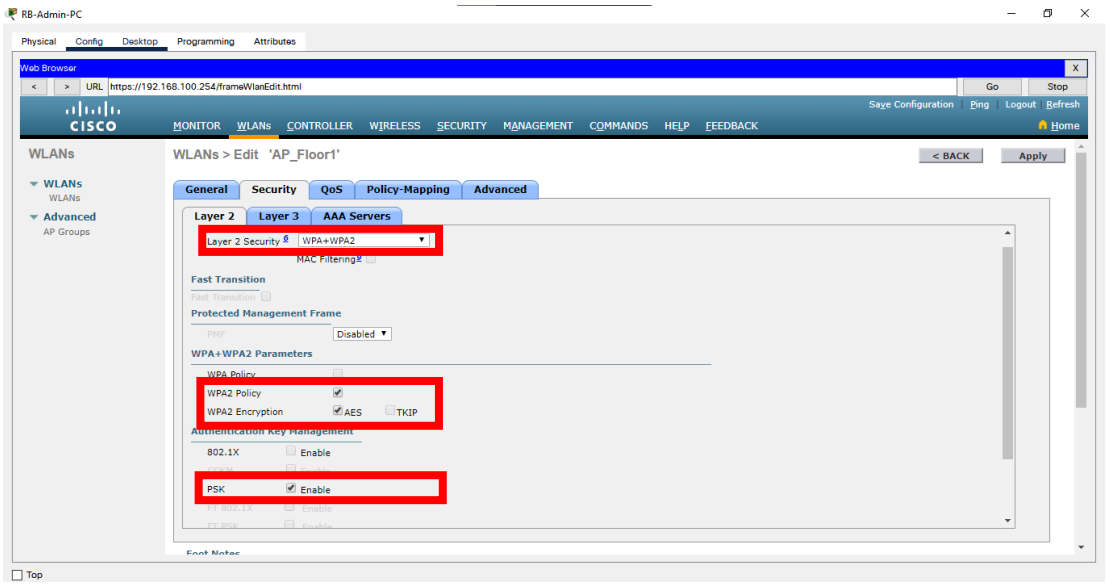

Figure 18: Security Configuration for WLANs (AP_Floor 1)

Set the Layer 2 security to WPA+WPA2, enable the WPA2 Policy and PSK (802.1X for WLANs AP_Mgmt and AP_IT since both groups' end devices is utilizing radius server concept). Advanced Encryption Standard (AES) is enabled also. Currently, AP_Floor 1, AP_Floor 2 and AP_Floor 3 will be implemented pre-shared key authorization via WPA2 PSK while AP_Mgmt and AP_IT is via WPA2 Enterprise.

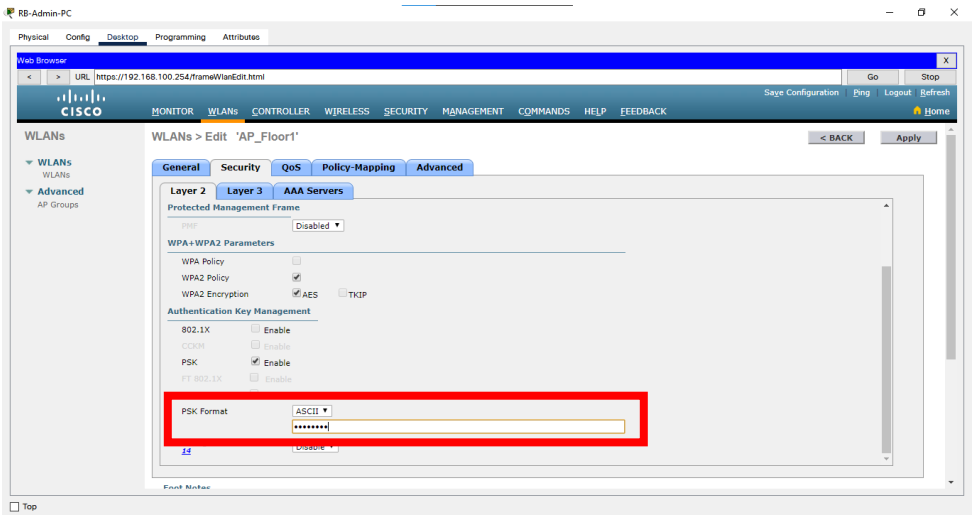

Figure 19: Continue Security Configuration for WLANs (AP_Floor 1)

Set the pre-shared to Cisco123

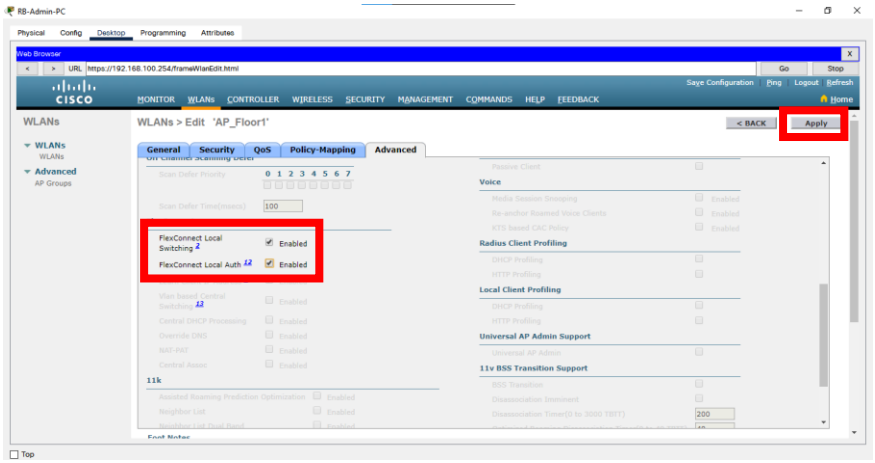

Figure 20: Advanced Configuration for WLANs (AP_Floor 1)

Enable **FlexConnect Local Switching** and **FlexConnect Local Auth** and select Apply to save all configuration update for WLAN (AP_Floor 1)

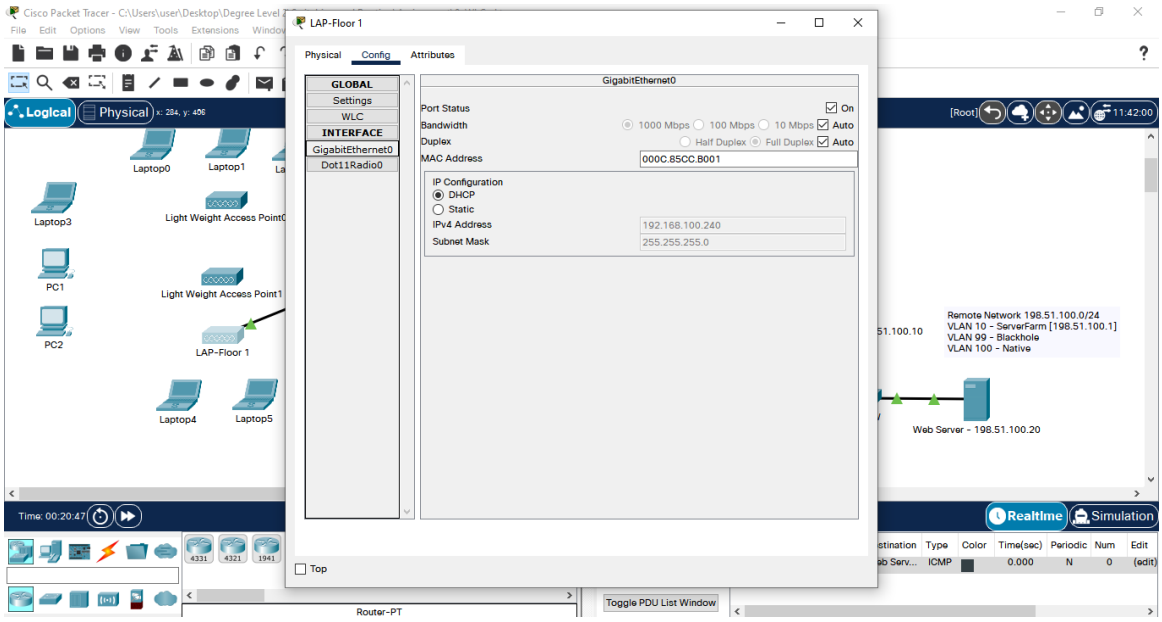

Figure 21: Setting Lightweight Access Point to get IP address through DHCP

Set the Access Point to use DHCP for IP Addressing. If the IP address is between 192.168.100.240 to 192.168.100.250 (due to DHCP scope configuration), the access point successfully received the IP Address. Test the connectivity with any end devices that chosen to connect to the access point.

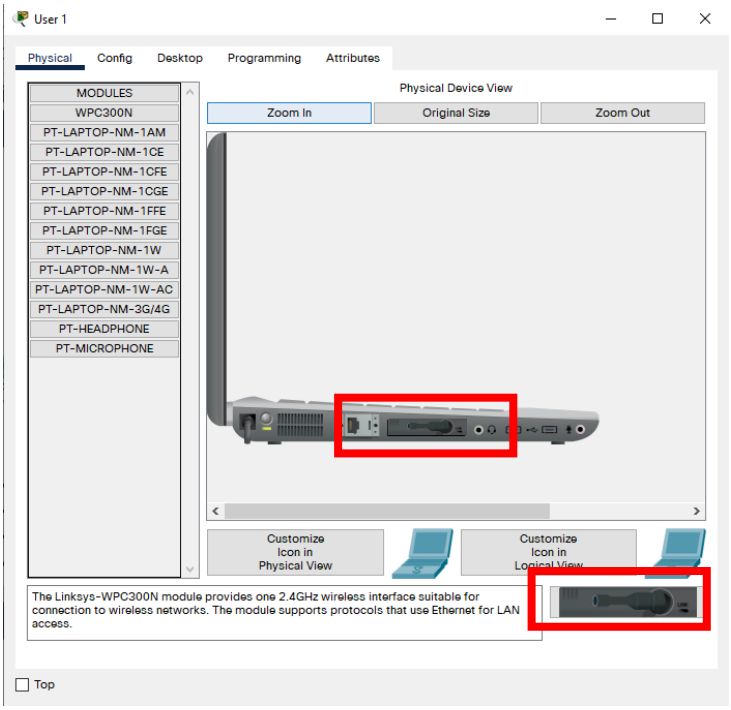

Figure 22: Replace WPC300N module to the laptop

Switch of the laptop and ensure the module is place with the WPC300N module, then switch on the laptop.

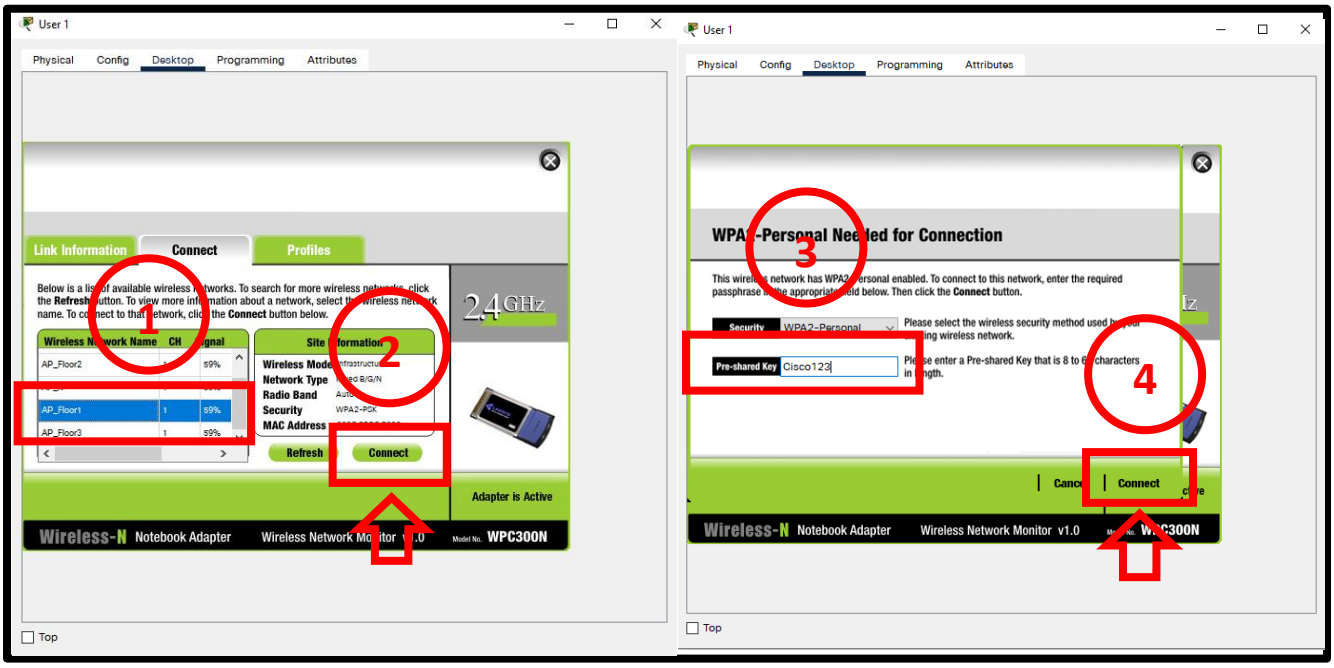

Figure 23: Connect the laptop to the WLAN through AP_Floor 1

Highlighted AP_Floor 1 then select connect. Enter correct pre-shared key then select connect,

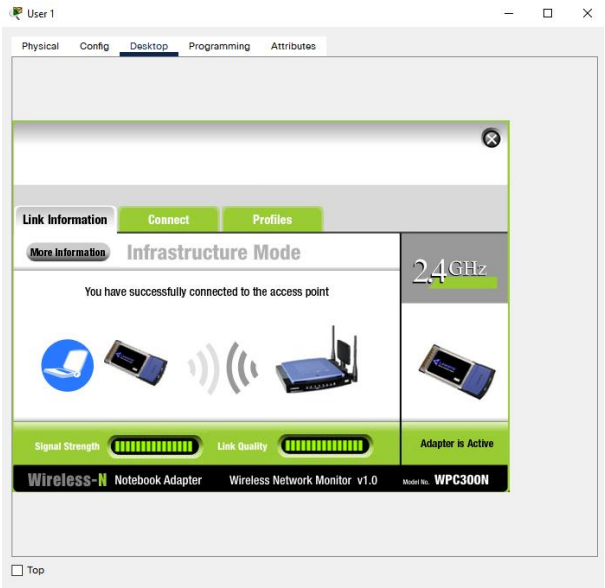

Figure 24: Connect Successful

Navigate to **Link Information**, if the connection is successful, a message "You have successfully connected to the access point" will display.

Step 8: Configuring Access Point group

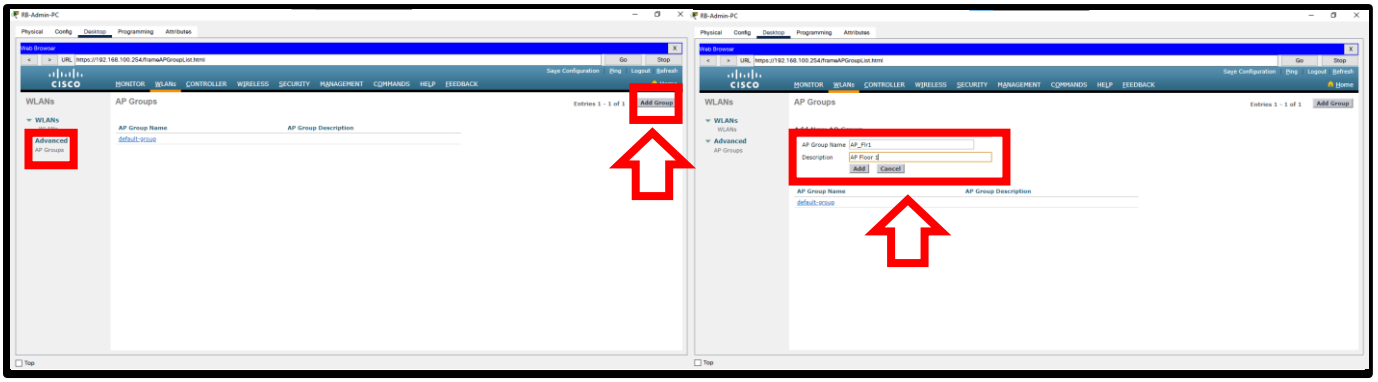

Figure 25: Adding a new AP Group

Navigate to **AP Groups** in the Advanced Tab to the AP Groups page and select **Add Group**. Fill in the details for the new AP Group and finalize the creation of the new AP Group by selecting **Add**.

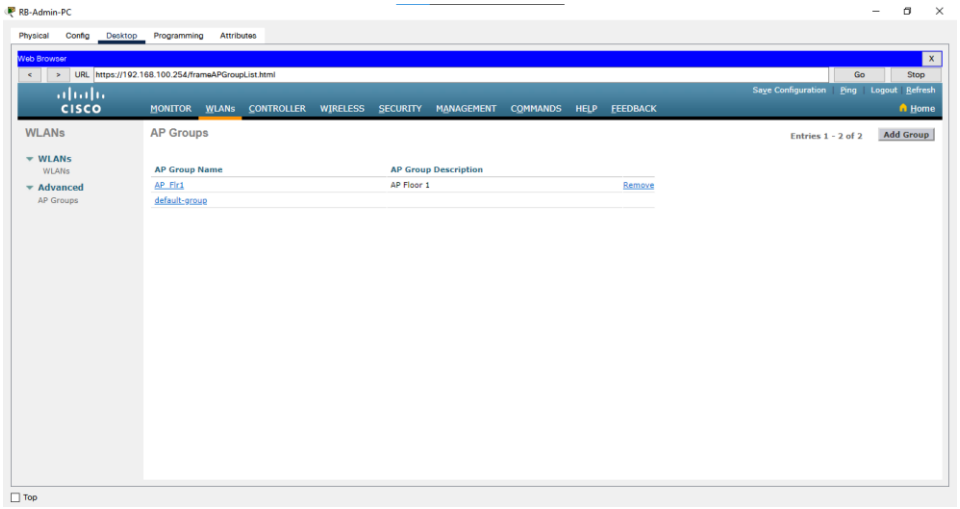

Figure 26: AP Group Created

Once the AP Group Created, selected the link. (In this scenario, AP_Flr 1 is created, thus the AP_Flr 1 link is select)

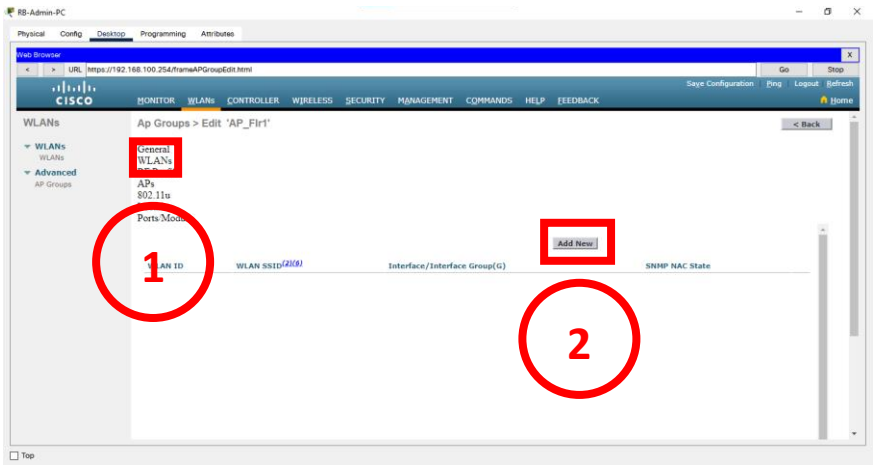

Figure 27: AP Group WLANs page

Navigate to WLANs page by selecting **WLANs** then select **Add New**

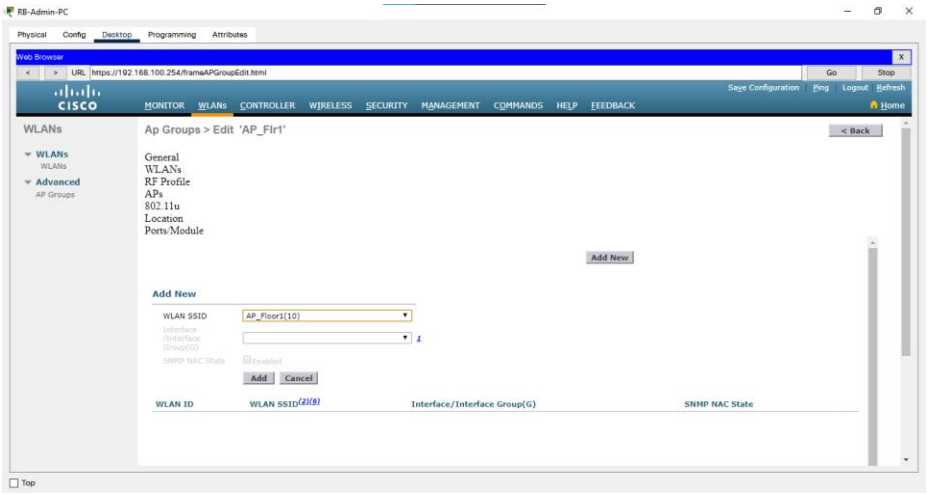

Figure 28: Add New WLANs SSID

Add new WLANs SSID then select **Add**

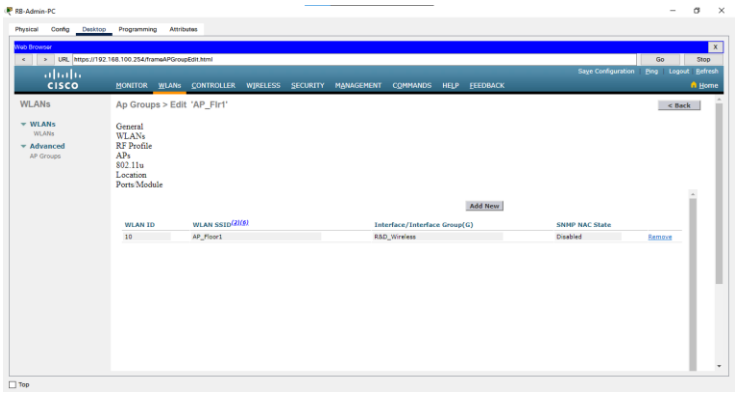

Figure 29: Add New WLAN ID Successful

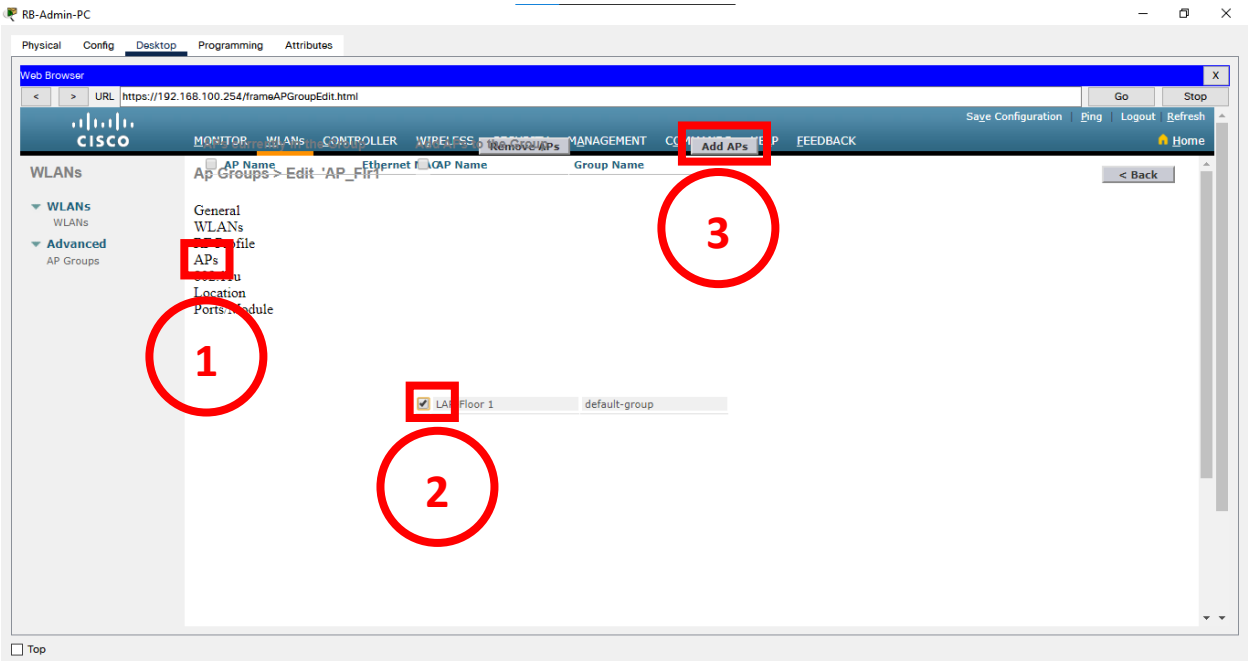

Figure 30: Add APs

Navigate to APs page by selecting **APs**. Then, tick the correct option and select **Add APs**. Repeat Step 7 and Step 8 to create WLAN and APs for other access point.

Note: AP_Flr 1 should choose LAP-Floor 1 controller to ensure LAP-Floor 1 controller only provide AP_Floor 1 WLAN. Meanwhile, AP_Flr 2 should choose LAP-Floor 2 controller and the same concept is apply to the remaining access point group to avoid confusion.

2.2 Radius Server Configuration

Step 1: Accessing WLC via RB-Admin-PC

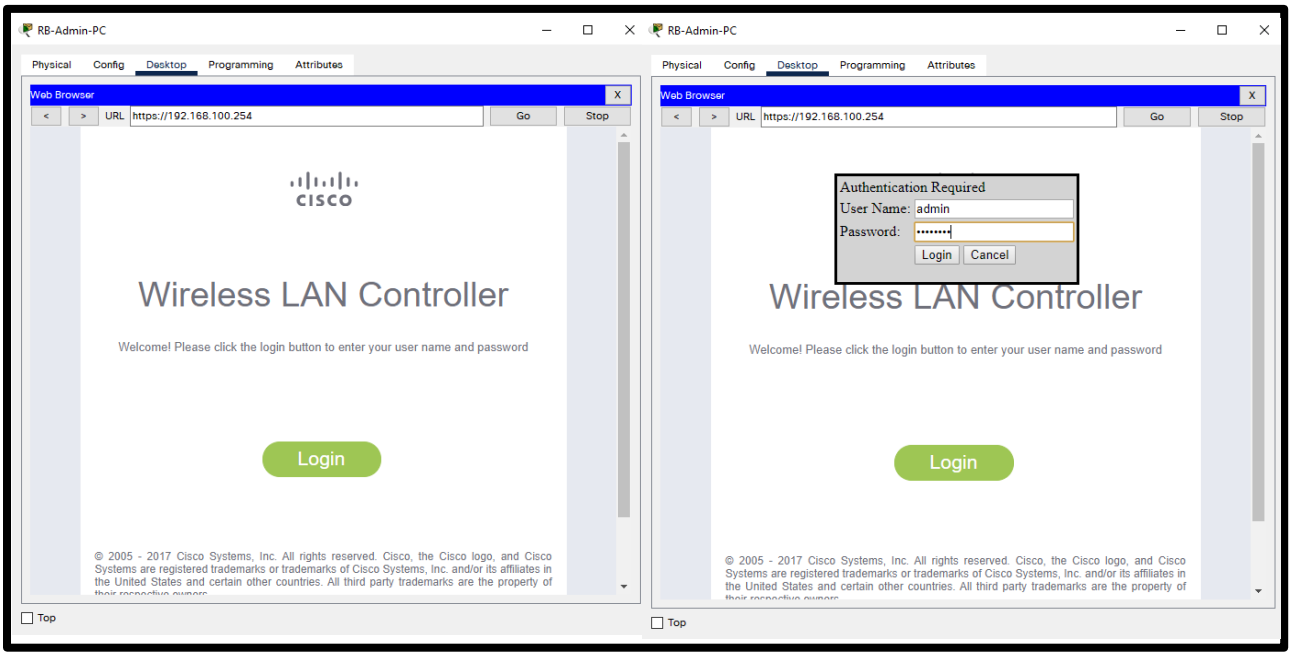

Figure 31: Accessing Wireless LAN Controller by using https

Access the WLC by using https://192.168.100.254 (https instead of http) in the RB-Admin-PC web browser. Username is admin and the password is Cisco123.

Step 2: Creating Radius Authentication Server

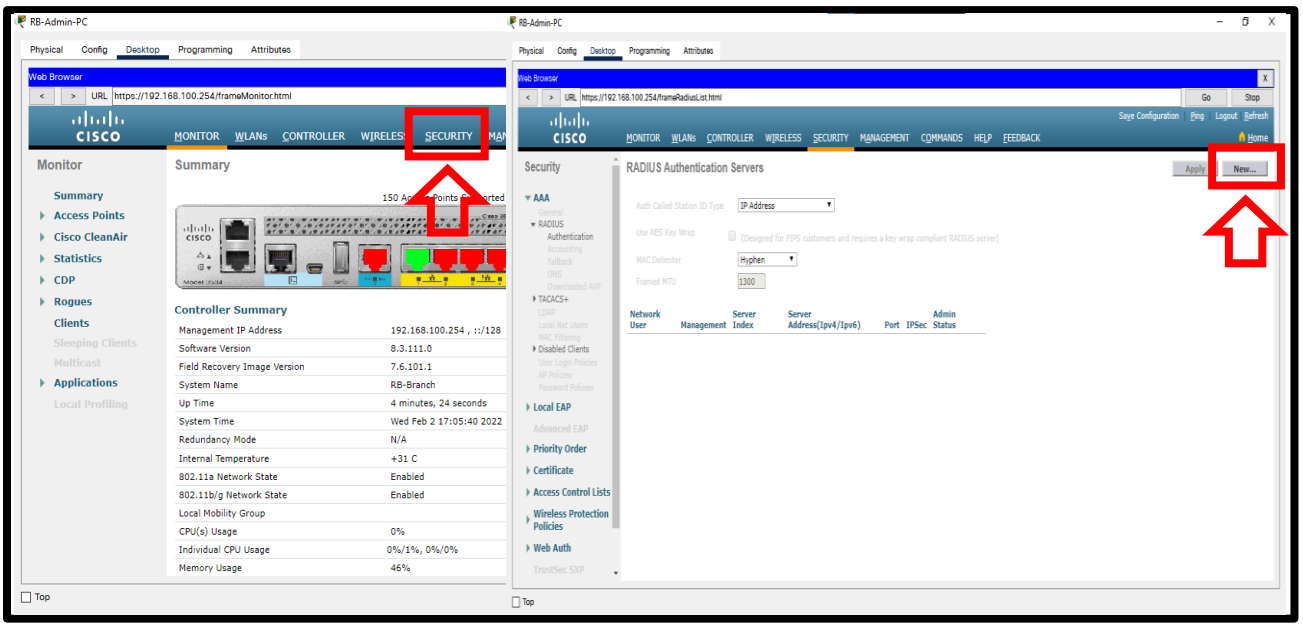

Figure 32: Creating a new Radius Authentication Server

Navigate to the **Security** tab then select **New…** to create new radius authentication server

Step 3: Finalizing the new Radius Authentication Server

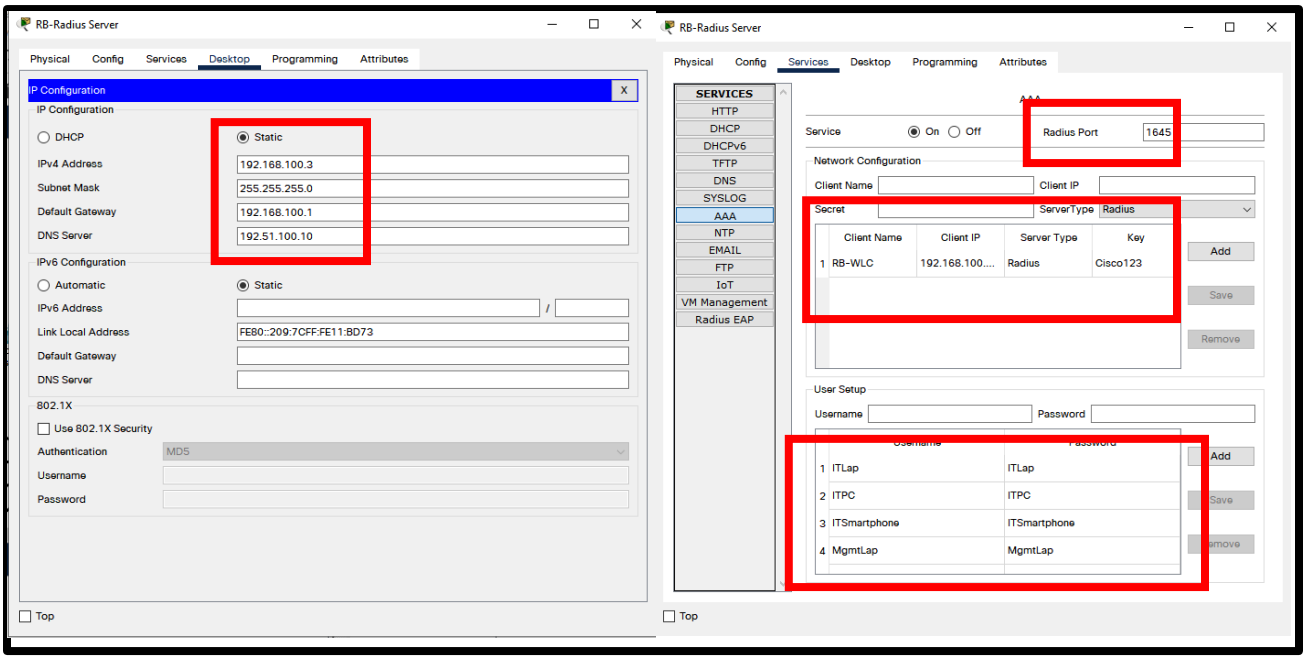

Figure 33: Radius Server Configuration

It is important to configure radius server information first as the IP Address of the radius server, share key and radius port number in AAA will be used in finalizing Radius Authentication Server. At the same time, add new users for new host devices to connect to WLAN (device that connet via WPA2 Enterprise instead of WPA2 PSK).

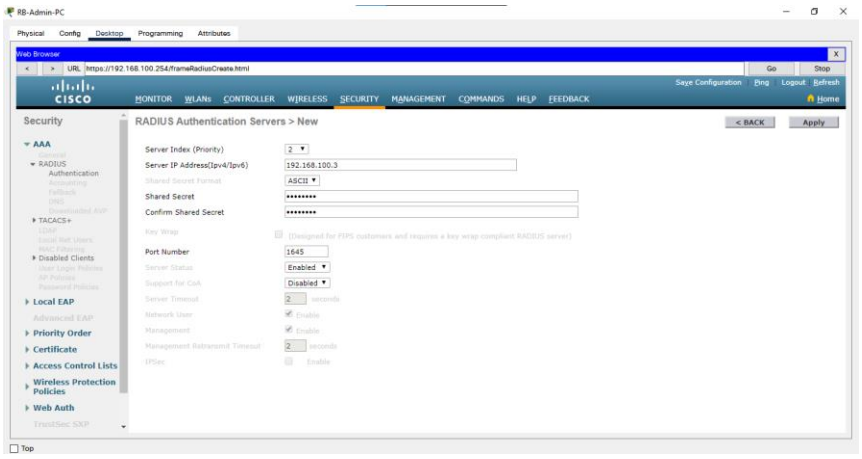

Figure 34: Finalizing Radius Authentication Server

Fill in the Server IP Address (Radius Server IP Address), Shared Secret (Must Match with Radius Server Network Configuration Shared Key) and Port Number (Radius Server port number) and select **Apply**.

Step 4: Edit WLAN Security Policies

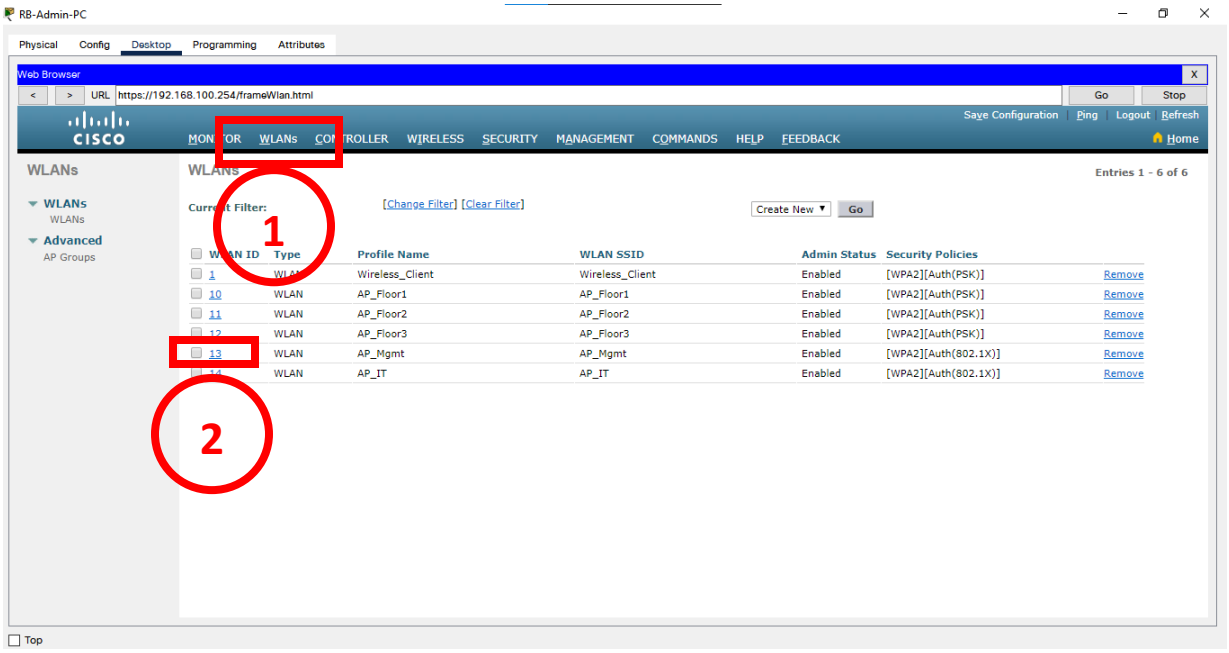

Figure 35: WLANs Page, edit WLAN ID 13, AP_Mgmt

Navigate back to the WLANs Page by selecting WLANs tab then select WLAN ID 13.

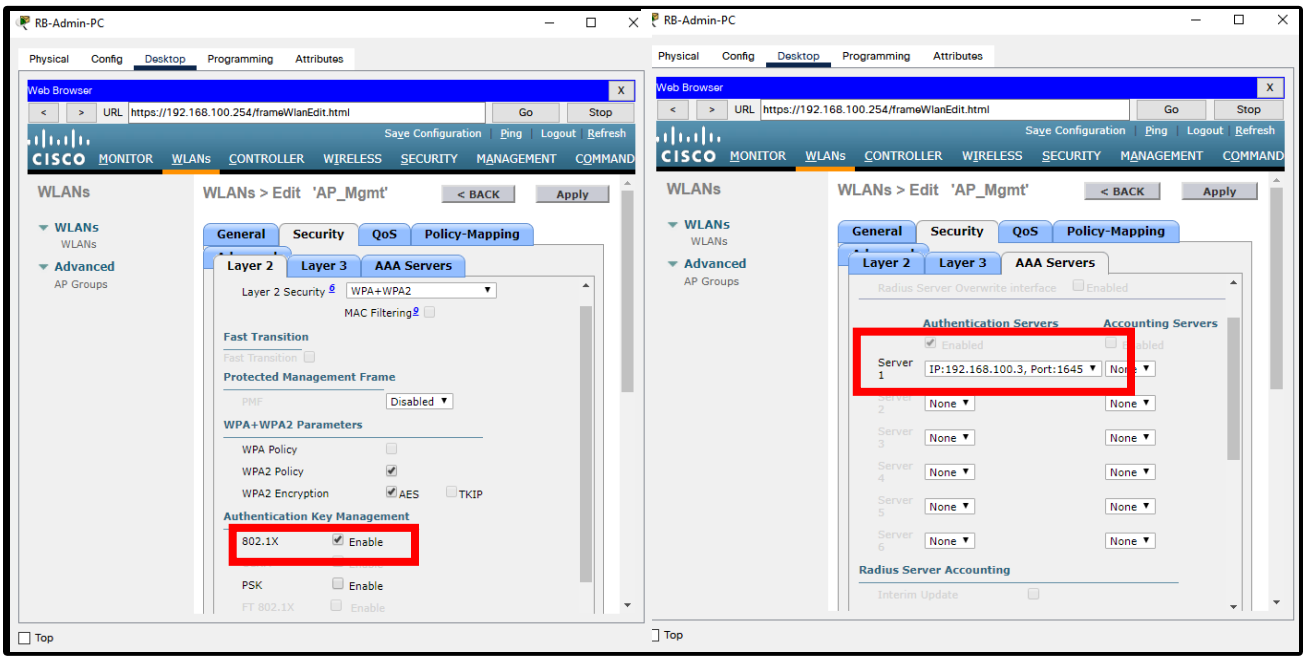

Figure 36: Changing Authentication method

In security tab Layer 2, enable 802.1X. Meanwhile in AAA Servers section, select the Radius Authentication Server which has the IP Address and Port Number **Equals** to the Radius Server.

Then select **Apply** to save changes. Repeat Step 4 for WLAN ID 14, AP_IT.

2.3 Connecting User to the WLAN through WPA2 Enterprise

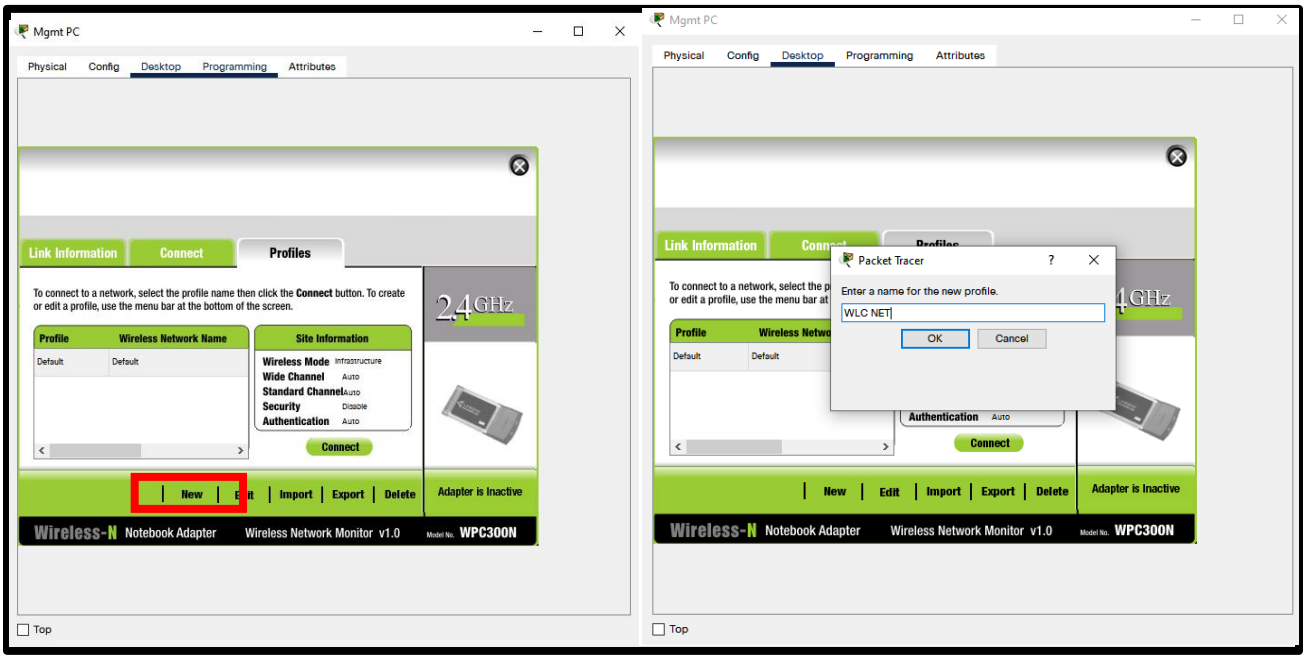

Figure 37: Create New Profile

In the profile tab, select **New**. A message will pop up and type any new profile name then select **OK**.

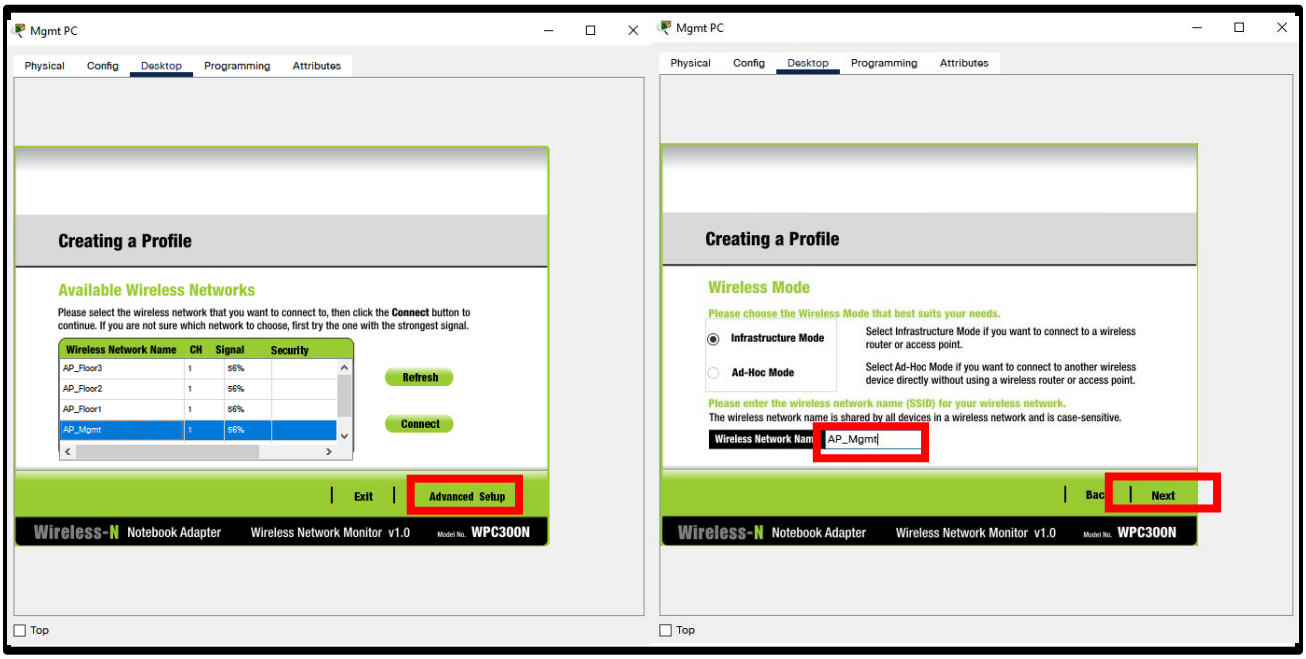

Figure 38: Create New Profile (Choose Appropriate Wireless Network)

Highlight suitable Wireless Network Name and select **Advanced Setup**. If the Wireless Network Name is empty, type in the name and select **Next**.

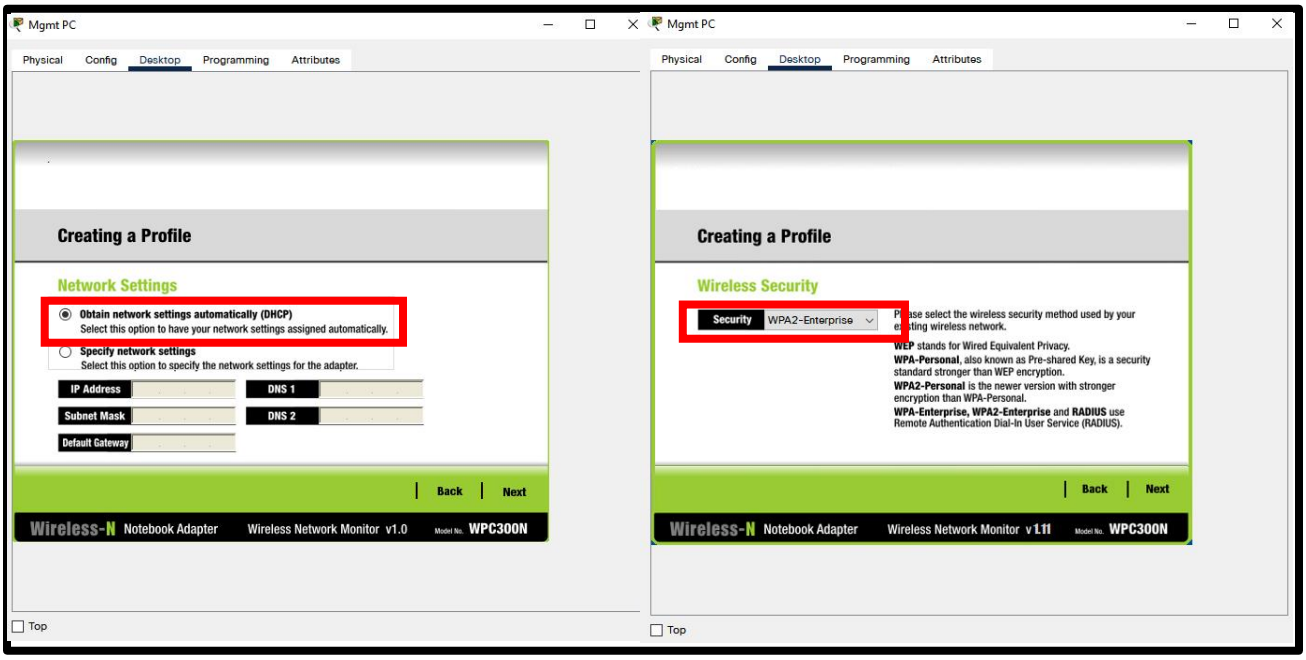

Figure 39: Create New Profile (Network Settings and Wireless Security)

Enable Network Settings to obtain network settings automatically (DHCP) and select **Next**. In the Wireless Security, choose WPA2-Enterprise and select **Next**.

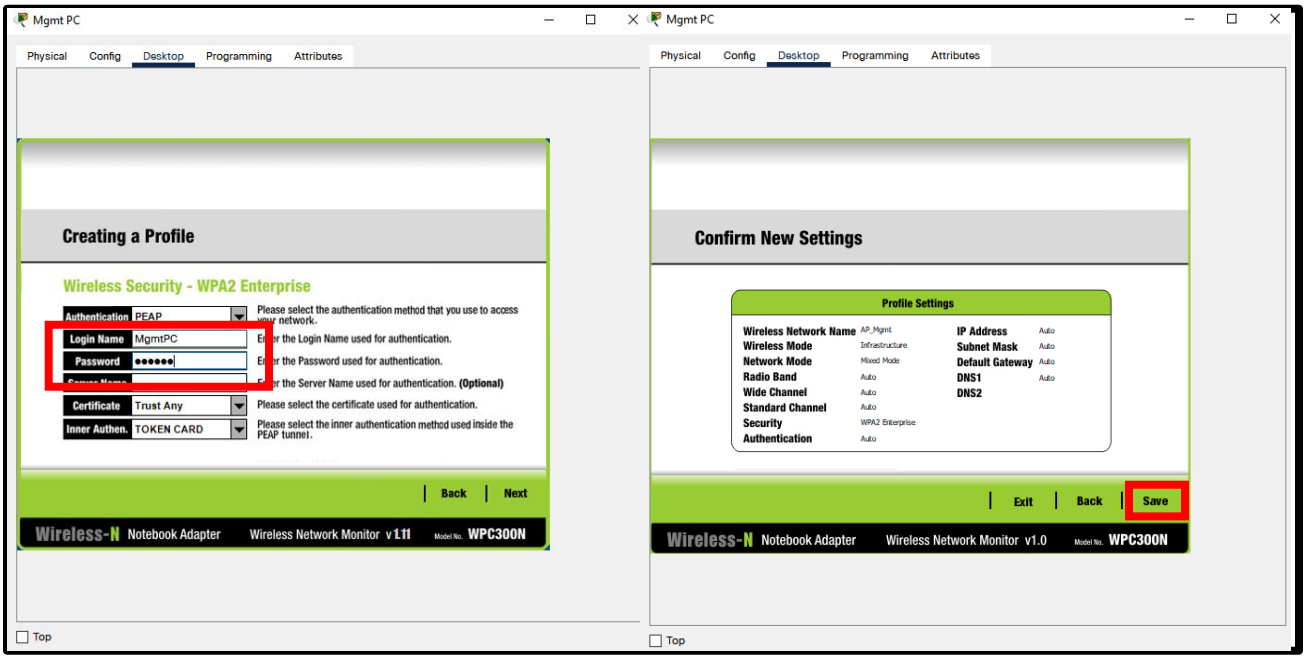

Figure 40: Create New Profile (Configure WPA2-Enterprise)

Fill in login name and password (Must match with any username and password that already configure in Radius Server AAA) and select **Next**. Then, confirm new settings and select **Save**.

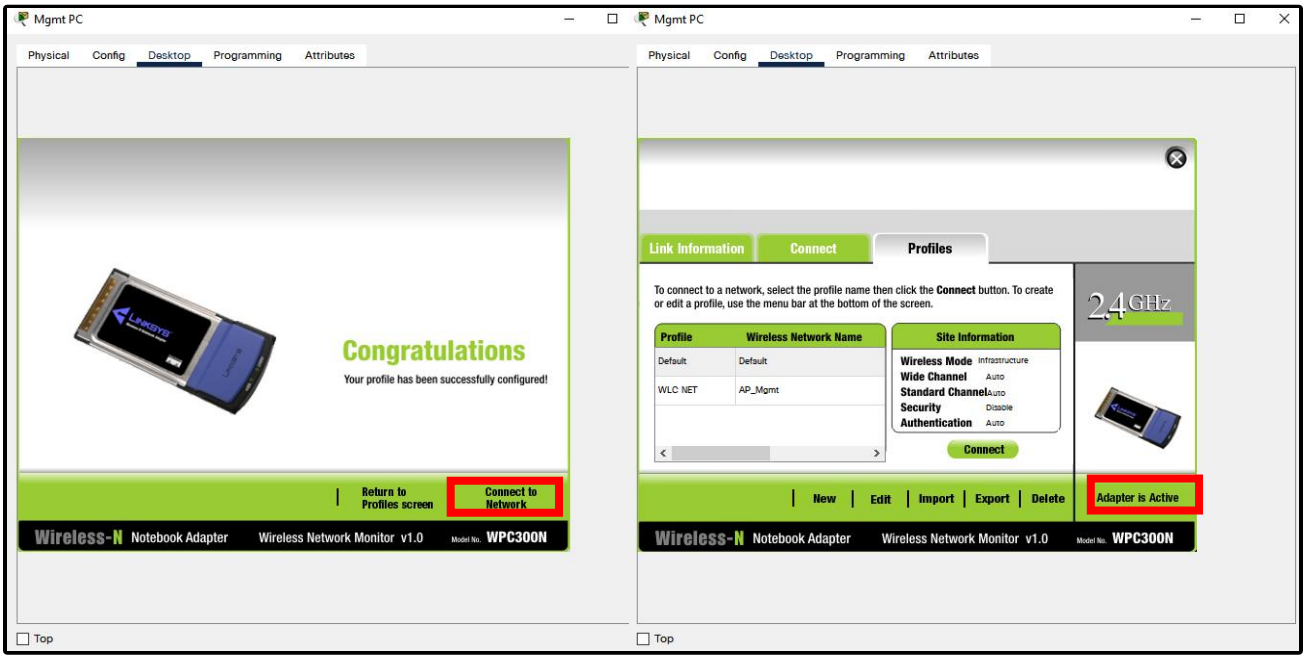

Figure 41: Profile Creation Successful and Adapter Active

Select **Connect to Network**. If the connection is successful, Adaptive is active.

2.4 Authentication, Authorization and Accounting (AAA)

WPA2-Enterprise is one of the components used in the proposed WLAN design, especially when a Remote Authentication Dial-Unit Service (RADIUS) server is used to offer AAA services. WPA2-Enterprise, unlike WPA2-Personal, requires each user to have their own user's name and password. If users follow credential best practices, it will be difficult for an outside attacker to get network access. Furthermore, if a single password is compromised, it can be easily reset, whereas WPA2-Personal needs the password to be changed on each device connected to the network.

AAA in Fiberoptic System Inc. is a system for intelligently limiting access to computer resources by enforcing restrictions, auditing use, and giving the data needed to bill for services. These methods must operate together for good network management and security. **Authentication** is an algorithm for verifying a user before granting access to the network and usually requires the user to enter a valid username and password. To compare a user's credentials with those stored in a database such as Active Directory, authentication relies on each user with a unique set of credentials. If the user's credentials match, the user is granted network access.

After authentication, the user needs to get approval via **authorization** to perform a particular task. For example, a user may try to issue a command after logging in to the system. The approval mechanism determines if the user has the right to issue a particular instruction. Once the individual is identified, they can access and participate in various activities. The authorization can use permissions to determine the VLAN, access control list (ACL), or user role to which a user belongs when using RADIUS and 802.1x network authentication.

Last but not least, AAA can track user access to the service and the amount of network resources user consume using the AAA **accounting** feature. When AAA accounting is enabled, the Network Access server sends accounting records containing user activity to the RADIUS security server. Each accounting record is stored on a security server and contains a pair of accounting attribute values (AV). This information can be used for network management, billing, and reporting. (arubaNETWORKS, n.d.).

3.0 Type of Security Attacks in Layer 2

3.1 Mac Address Table Attack (Mac Address Flooding)

Each port is assigned a MAC address using the MAC address table. This enables traffic to be delivered directly to a server. Traffic would be transmitted to each port individually if the MAC address array was not there, as if it were a hub. A switch may run out of resources for storing MAC addresses since all MAC tables have a fixed capacity. MAC address flooding attacks take use of this flaw by flooding the switch with fraudulent source MAC addresses until it fills up. When this happens, the switch treats the frame as an unknown unicast and begins flooding all incoming traffic from all VLAN ports, bypassing the MAC table. This situation now permits a threat actor to capture all frames sent from one host to another on the local LAN or local VLAN. (CCNA, n.d.).

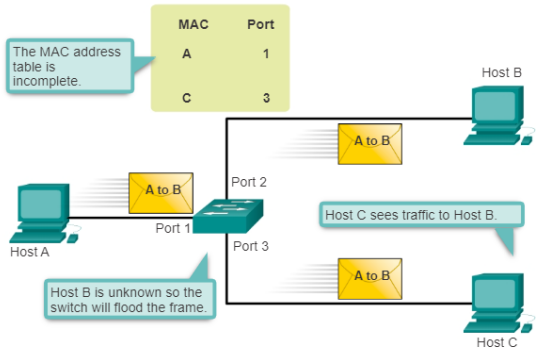

Figure 41: Switch Floods Frame for Unknown Mac

Based on the figure above, it shows how host A delivers data to host B. The switch receives the frames and searches its MAC address table for the destination MAC address. If the switch is unable to locate the destination MAC address in the MAC address database, it replicates the frame and floods (broadcasts) it out of all switch ports saves the one where it was received.

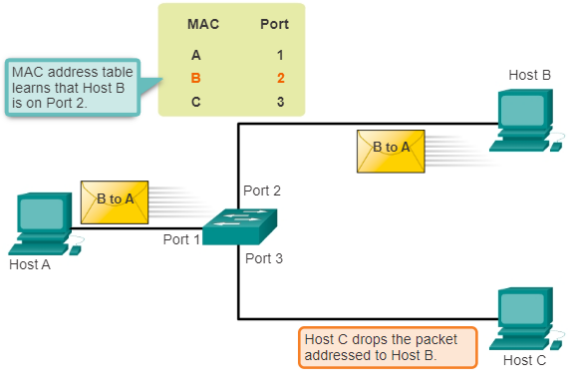

Figure 42: Switch Records Mac Address

When host B gets the frame, it responds to host A. The switch then discovers that host B's MAC address is on port 2 and enters this information into the MAC address database. Host C gets the frame from host A to host B as well, but because the frame's destination MAC address is host B, host C discards it.

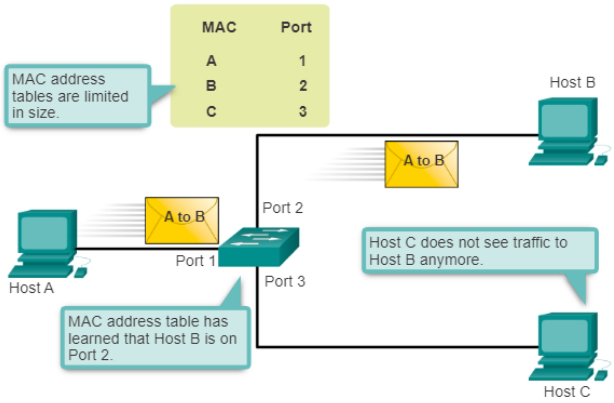

Figure 43: Switch uses Mac Address Table to forward traffic

Any frame transmitted to host B from host A (or any other host) gets sent to port 2 of the switches rather than being broadcast out all ports. The size of MAC address tables is restricted. This shortcoming is exploited by MAC flooding attacks, which flood the switch with bogus source MAC addresses until the MAC address table is filled.

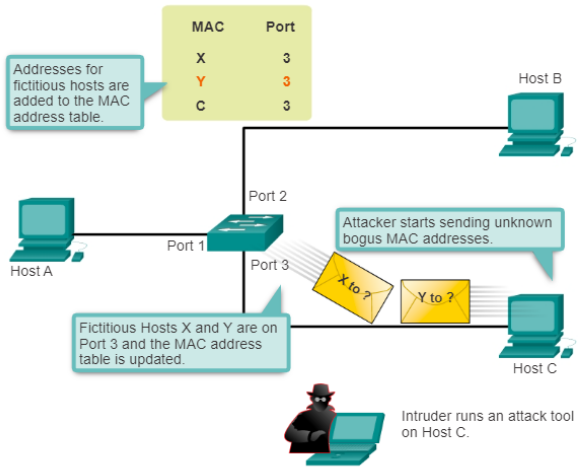

Figure 44: Mac Address Flooding Attack

(Threat Actor-Intruder sending unicast to the switch with fake source and destination)

Based on the figure above, the attacker on Host C randomly falsely generated source and destination MAC addresses and sent to the switch. The wrong frame information is used by the switch to update the MAC address database. In some cases, threat actors use the "macof" to quickly generate a large number of random source and destination MAC and IP addresses. If the MAC address table overflows with the spoofed MAC address, the switch goes into fail open mode. In this mode, the switch broadcasts all frames to all devices on the network. As a result, an attacker can access all frames. Some network attack tools can create up to 155,000 MAC entries per minute on the switch. Maximum MAC address table size differs depending on the switch.

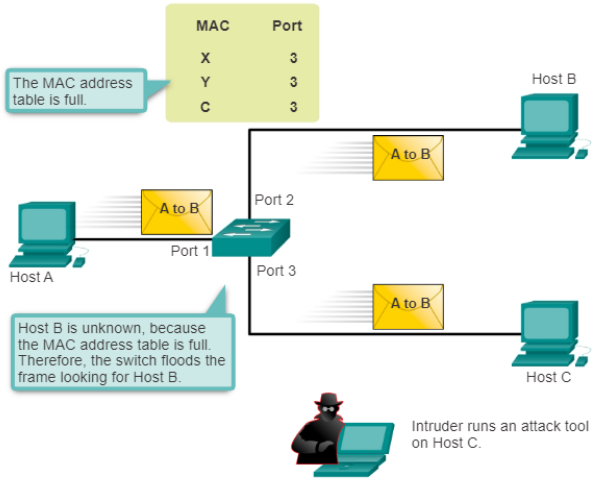

Figure 45: Mac Address Flooding Attack

(Due to Mac Address Table is full, any frame transmitted is become broadcast)

As long as the switch's MAC address table is filled, the switch broadcasts all received frames out of every port. In this case, frames sent from host A to host B are broadcast out of switch port 3 and seen by the attacker at host C. The switch progressively ages out the older MAC address entries from the table and resumes acting like a switch if the threat actor stops "macof" from executing or is detected and stopped.

3.2 VLAN attack (VLAN hopping: Double-tagging attacks, Switch spoofing)

VLAN hopping (virtual local area network hopping) is a method of delivering packets to a port that is not ordinarily accessible from an end system in order to target the VLAN's network resources. The goal of this sort of violence is to get access to other VLANs on the same network. Before attempting VLAN hopping, a threat actor must first infiltrate at least one VLAN on the network. As a result, attackers can establish a base of operations from which to attack other VLANs on the network. Hackers utilize this strategy to break into and infiltrate other VLANs on the same network. VLAN hopping may be used to modify or delete data, install malware, and distribute threat vectors like as viruses, worms, and Trojans across a network, in addition to allowing authorized party to steal passwords and other sensitive information from network users. VLAN hopping can occur in one of two ways: Double-Tagging and Switch Spoofing (Zola, n.d.).

Double-Tagging

VLAN hopping attacks with double-tagging are also known as double-encapsulated VLAN hopping attacks. The attacker takes advantage of the hardware's style of working in this form of attack. Threat actors add and change tags on the Ethernet frame, resulting in double tagging vulnerabilities. This method uses numerous switches that process tags to allow packets to be sent across any VLAN on the trunk as the native untagged VLAN. The hacker sends frames with two 802.1Q tags, one for the attacker switch and the other for the victim switch, to transport data from one switch to another. This deceives the victim into believing that the frame was made for them. The frame is subsequently sent to the victim port via the target switch.

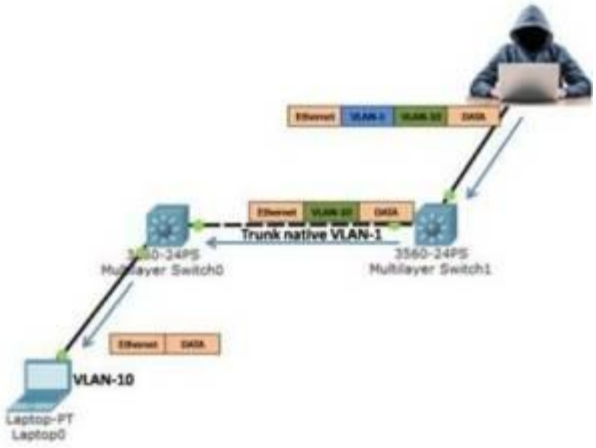

Figure 46: Double-Tagging Attack

According to the diagram, the attacker transmits a double-tagged 802.1Q message to multilayer switch1. The outer tag on the packet is the attacker's tag, which is the same as the native VLAN of the trunk port (VLAN1). Because a tagged Ethernet packet on an access port should not be accepted, the switch treated it as if it were on a trunk port or a port with a voice VLAN. The inner tag is VLAN 10 (victim VLAN). Because the trunk is also part of native VLAN, the switch will send the frame on a trunk port without re-tagging it, thus the VLAN 10 tag is still there in the packet despite switch1's failure to verify it. At this time, the 802.1Q tag on switch0 is an inside tag of VLAN-10, indicating that the packet was delivered for VLAN 10, the target VLAN. Switch0 removes the VLAN-10 tag and sends the packet to the victim port or floods it, depending on the current MAC address table entry. (Ijaz, 2019).

The attacker can only perform a double tagging attack if they have physical access to an interface that is part of the trunk port's native VLAN. A unidirectional assault is a double tagging strike. Halting this sort of attack is more difficult than stopping typical VLAN hopping attempts.

Switch Spoofing

The Cisco-proprietary Dynamic Trunking Protocol (DTP) is activated by default in Cisco switches. This protocol allows a trunk link to be established between two switches if the associated interfaces are configured in trunking mode, which simplifies network architecture configuration. To get access to all of the VLANs authorised on the trunk port, the attacker converts it into a switch that appears to be in constant need of trunking. This security weakness is essentially a one-way attack because the return packet cannot be wrapped. It's only possible if the hacker and the victim share the same native VLAN trunk link. (Ijaz, 2019).

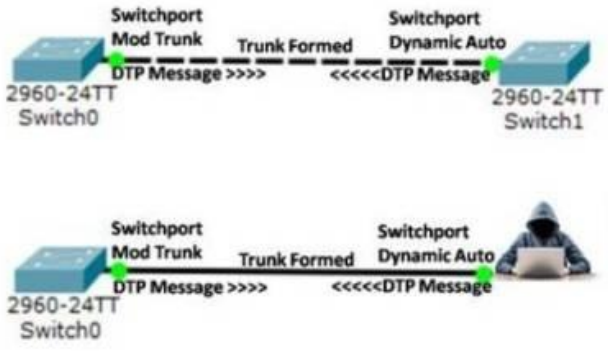

Figure 47: Switch Spoofing

3.3 DHCP Attack (DHCP Spoofing Attack, DHCP Starvation Attack)

DHCP spoofing occurs when an attacker attempts to respond to DHCP queries by putting themselves (spoofing) as the default gateway or DNS server. The network attacker can then use his or her workstation to set up a rogue DHCP server and reply to fresh DHCP requests from network clients. A network attacker can give clients with addresses and other network information by creating a rogue DHCP server on the network. Because DHCP answers frequently include information about the default gateway and DNS server, a network attacker can operate as the default gateway and DNS server using his or her own system. As a consequence, a man-in-the-middle assault is launched.

Meanwhile, a DHCP starvation attack broadcasts DHCP requests using forged MAC addresses. If enough requests are sent, the network attacker can deplete the address space available to the DHCP servers for a period of time. (CCIESecurity, 2022). Attackers send a large number of DHCP packets with different media access control (MAC) addresses in frame headers to a Dynamic Host Configuration Protocol (DHCP) server to request IP addresses. As a result, the address pool of IP addresses is depleted, and authorized clients are unable to receive IP addresses. Denial of service generally occurs when the address pool is depleted.

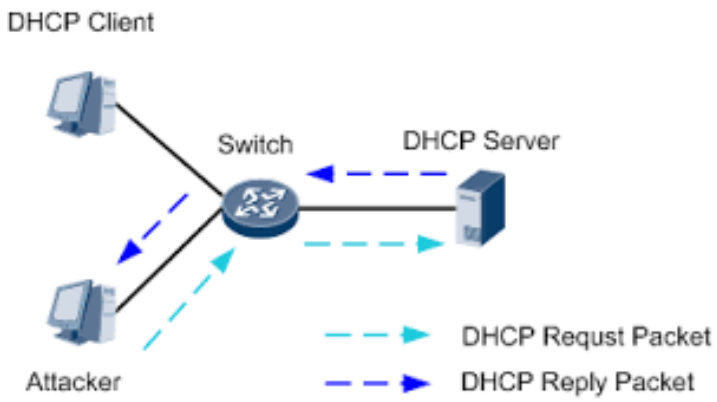

Figure 48: DHCP Starvation, Attacker set up a rogue DHCP Server

3.4 STP Attack (Spanning Tree Protocol Attack)

In a Layer 2 switch design, redundant connections can be added to increase network availability. Duplicate connections, on the other hand, might result in Layer 2 loops and broadcast storms. Fortunately, the Spanning Tree Protocol (STP) allows network administrators to have redundant physical links while preserving a logical loop-free topology, which prevents broadcast storms. STP creates a loop-free topology by designating one switch as the root bridge.

The attacker spoofs the topology's root bridge in a STP attack by sending out a STP configuration/topology change BPDU to force a recalculation of STP. According to the BPDU sent out, the attacker's system has a lower bridge priority. Once the rogue switch releases its "superior BPDUs," the STP topology converges. All communication between switches now passes through the rogue switch, making it possible for the attacker to intercept it. As a result, the attacker has access to a variety of frames sent to it by other switches. Each time the root bridge changes, STP recalculation might possibly cause a network denial-of-service (DoS) problem by causing a 30-45 second disruption. (AuthenticationProxy, 2022).

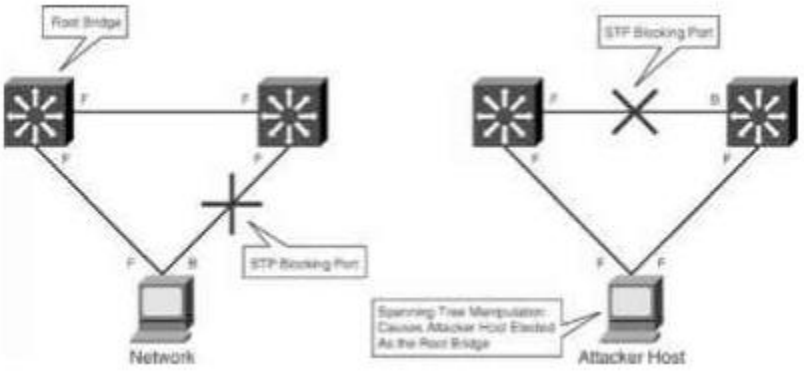

Figure 49: Attacker change the priority ID for the root bridge.

Now the attacker host become the root bridge (rogue switch)

4.0 Layer 2 Security Deployment to Mitigate the Attacks

4.1 MAC Address Table Attack Mitigation (Port Security)

The number of valid MAC addresses that can be used on a port on a switch is limited by switch port security. When a MAC address (or a combination of MAC addresses) is used to enable switch port security, packets are only forwarded to devices with those MAC addresses. The switch immediately rejects any packet from another device that comes on the switch port. After the maximum number of secure MAC addresses has been reached, attempting to connect to a port with a device that has a different MAC address is a security violation. When a switch detects a security breach, it either shuts down the port or restricts the number of packets let through, depending on the security breach.

Based on the three types of secure MAC addresses, the network administrator strongly suggested that Sticky Secure MAC addresses are the ideal option: ~

Static - are established manually, kept in the address database, and added to the switch operational configuration using the switchport port-security mac-address interface configuration command.

Dynamic - are dynamically assigned, are only kept in the address database, and are wiped when the switch is restarted.

Sticky - can be learned dynamically or manually and saved in an address database before being added to the operating system. The interface does not need to dynamically alter these addresses when the switch restarts since they are saved in the configuration file.

Meanwhile, three types of security violations can be configured in the Cisco Switch when the interface's maximum number of MAC addresses is reached and a new device with a MAC address that isn't in the address database tries to connect to it, or when a learnt MAC address on one secure interface is seen on another secure interface in the same VLAN.: ~

Protect - When the port's maximum number of secure MAC addresses is reached, any packets with unknown source addresses are denied until the maximum number of secure MAC addresses is reduced or the maximum number of acceptable addresses is increased. However, if a security breach has occurred, no notice is displayed.

Restrict - When the number of secure MAC addresses approaches the maximum value permitted on the port, packets with unknown source addresses are discarded unless the network administrator deletes a significant number of secure MAC addresses to drop below the maximum value or raises the number of maximum authorized addresses. If a security breach occurs, the network administrator will be notified. The violation counter is incremented after an SNMP trap is produced and a syslog message is written.

Shutdown - If a port security breach occurs, the interface becomes error-disabled and shuts down promptly, with the port LED turning off. When a secure port is disabled due to an issue, network administrators can manually reinstate it using the shutdown and no shutdown interface configuration commands. This is the best concept setup for a server farm.

4.2 VLAN Attack Mitigation

Certain Cisco switches were set to auto mode by default for trunking. If some of the switch ports receive Dynamic Trunking Protocol (DTP) frames, the ports will become trunk ports right away. This is a severe security risk since an attacker might swiftly convert a switch port into a trunk, allowing the party to conduct VLAN hopping attacks. Thus, attacker has direct access to all VLANs on the switch, bypassing the router.

Double-Hopping Attack Mitigation (Create new VLAN for Native VLAN)

To help defend against a VLAN hopping attack using double tagging, don't send user traffic across the default native VLAN. This may be done by creating a VLAN that has no ports. The only use of this unused VLAN is to allocate native VLANs.

```
Switch1(config)# interface gigabitethernet 0/4
Switch1(config-if)# switchport trunk native vlan 400
```

Figure 50: Example of an interface assign to VLAN 400 (only for native VLAN usage with no ports)

Switch Spoofing Mitigation (Disable Trunking on unused access port, Disable DTP)

To prevent switch spoofing, network administrators should assign switchport mode access with new VLANs to all ports that do not need to form trunks (avoid using default VLAN 1, and shut down unused access ports is strongly recommended), and disable DTP on ports that do need to be trunks with the command switchport no negotiate.

```
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
```

Figure 51: Example of interface range assign to VLAN 1000 (for access port)

```
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
```

Figure 52: Example of interface range assign with switchport no negotiate (only for trunk ports)

4.3 DHCP Attack Mitigation (DHCP Snooping)

DHCP Snooping is a built-in function of the operating system of a competent network switch that rejects DHCP communication that is deemed improper. DHCP Snooping increases protection for DHCP clients from unauthorized (rogue) DHCP servers that issue IP addresses by checking and filtering DHCP packets received from untrusted sources. It also develops and maintains the DHCP Snooping binding database, which keeps track of untrusted hosts with leased IP addresses. Finally, the DHCP Snooping binding database is used to check for future requests from untrustworthy hosts.

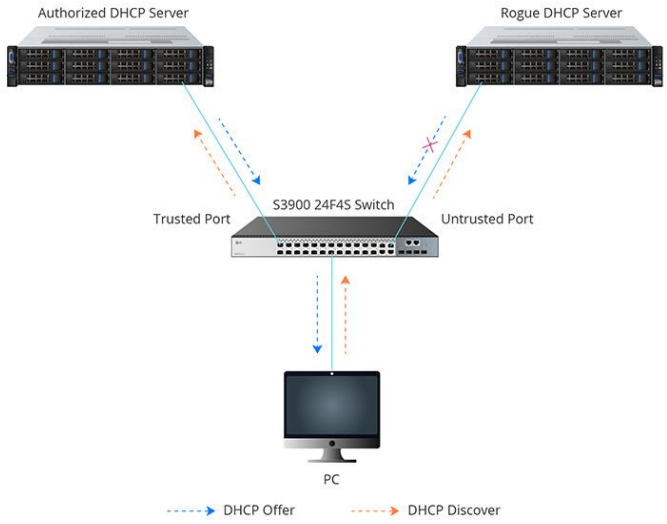

Figure 53: DHCP Snooping differentiate trusted port and untrusted ports.

DHCP Snooping divides switch interfaces into two groups: trustworthy and untrusted ports. A trusted source or port is one that can confidently receive DHCP server communications. Untrusted ports are those that do not trust connections from DHCP servers. If DHCP Snooping is enabled, the DHCP offer message can only be transmitted over the trusted port. If this does not happen, it will be abandoned. At the acknowledgement stage, a DHCP binding table will be generated based on the DHCP ACK message. It also maintains the VLAN number and interface information, as well as the host's MAC address, leased IP address, lease duration, binding type, and VLAN number. If the next DHCP packet received from an untrusted host does not match the information, it will be rejected. (Howard, 2021).

4.4 STP Attack Mitigation (PortFast and BPDU guard)

PortFast

PortFast immediately switches an interface configured as an access or trunk port from blocking to forwarding, skipping the listening and learning processes. This is true for any end-user port. Only the access ports, which are linked to end devices, should have PortFast enabled. If the trunk ports are set using PortFast, the entire VLAN will go down.

BPDU Guard

As a further step to enhanced defense in avoiding a STP attack, consider implementing BPDU guard on an interface where PortFast is configure. When BPDU guard is activated, when an interface receives a BPDU, it might be blocked. With BPDU protection enabled, an attacker will be unable to force root bridge election since the BPDU will be refused on the port to which they are connected. It's also utilized to enforce the spanning tree's boundaries, as loop-causing redundancies are frequently installed only in specific parts of a network. When portfast is enabled worldwide, enable BPDU guard on all ports that has portfast at the same time.

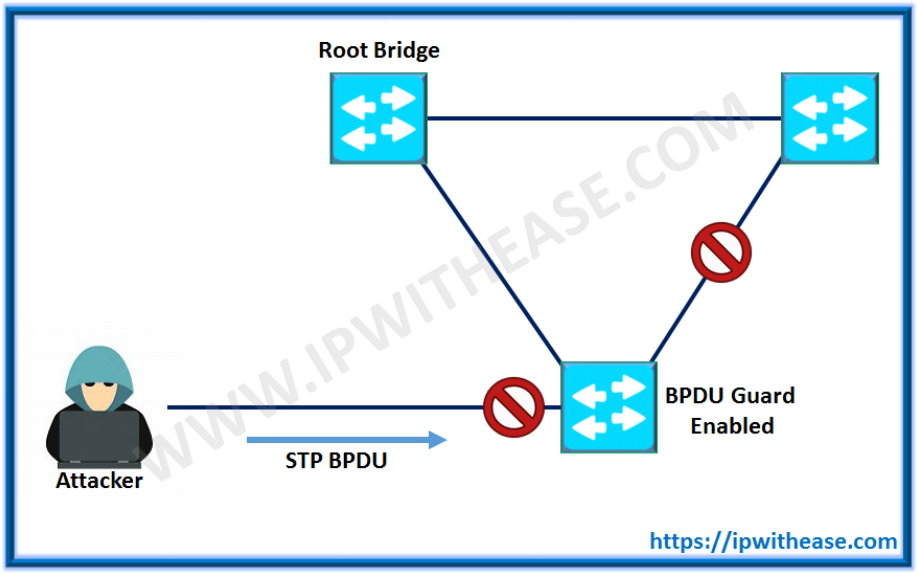

Figure 54: Example of BPDU guard enable on access port thus attacker unable to send STP BPDU

.

5.0 Secure Remote Access (SSH and ACL)

There is a chance that the management department from Fiberoptic System Inc. Headquarters or a Remote Branch will need access to the switches on occasion. As a result, Secure Shell (SSH) must be deployed. SSH (Secure Shell) is a network protocol that allows network administrators to remotely access and control devices. It is a more secure version of Telnet. It is now a widely used protocol for connecting to network devices and servers over the internet, allowing network administrators to log into another computer through a network and execute instructions on a remote computer. Files can be moved from one computer to another. By safeguarding logins and file transfers while protecting user identities, passwords, and data from network surveillance threats, the SSH protocol prevents trafficking, sniffing, and password theft (Brent, 2022). The second version of SSH is far superior to the first (first version has a history of vulnerable to Man in the Middle Attacks).

Telnet	SSH
Telnet is the standard TCP/IP protocol for virtual terminal service. It enables you to establish a connection to a remote system in such a manner that it appears as a local system.	SSH or Secure Shell is a program to log into another computer over a network to execute commands in a remote machine.
Telnet uses port 23, which was designed specifically for local area networks	SSH runs on port 22 by default, which you can change it.
No privileges are provided for the user's authentication.	SSH is a more secure protocol, so it uses public-key encryption for authentication.
Suitable for private networks	Suitable for public networks
Telnet transfers the data in plain text.	The encrypted format should be used to send data and also uses a secure channel.
Telnet is vulnerable to security attacks.	SSH helps you to overcome many security issues of Telnet.
Required low bandwidth usage.	Required high bandwidth usage.
Data sent using this protocol cannot be easily interpreted by the hackers.	Usernames and Passwords can be prone to malicious attacks.
Used in Linux and Windows Operating system.	All popular Operating systems.

Figure 55: Characteristic of SSH

In addition, the HQ Network uses Access Control Lists (ACLs) to allow or prohibit access to network devices (any device that has connection to the management VLAN). By filtering or outgoing traffic, ACL is used to regulate traffic in the network and reduce assaults by threat actors. ACL will deny access to any device that is not connected to the management VLAN since it filters out non-management or non-SSH traffic.

6.0 Conclusion for Section A

As requested by representatives at Fiberoptic Systems Inc., the remote branch utilizes a Wireless LAN topology which incorporates lightweights access points and a Wireless LAN Controller. At the same time, RADIUS server has been configured for the WLC to provide AAA services which stands for Authenticate, Authorize, Accounting purpose that allows remote access servers to interact with a central server in order to authenticate dial-in users and grant them access to the system or service they've requested.

To better comprehend the idea of security violations, the network executive did extensive study on any possible Layer 2 Security Attacks. As a result, the network executive has done further study to find strategies to protect against Layer 2 Security Attacks (MAC Address Table Attack, VLAN Attack, DHCP Attack, STP Attack). After doing different studies, SSH and ACL are also recommended for additional security enhancement purposes.

References

arubaNETWORKS. (n.d.). *What Is AAA*. Retrieved February 24, 2022, from arubaNETWORKS: https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Default.htm#802.1X%20Authentication/About_AAA.htm

AuthenticationProxy. (2022, February 18). *STP Manipulation Attacks*. Retrieved February 23, 2022, from Cisco Certified Expert: https://www.ccexpert.us/authentication-proxy/stp-manipulation-attacks.html

Brent, M. (2022, February 19). *Telnet vs SSH: Key Differences*. Retrieved February 23, 2022, from Guru99: https://www.guru99.com/telnet-vs-ssh.html#:~:text=SSH%20is%20a%20more%20secure,public%2Dkey%20encryption%20for%20authentication.&text=Telnet%20transfers%20the%20data%20in%20plain%20text.,is%20vulnerable%20to%20security%20attacks.

CCIESecurity. (2022, February 22). *DHCP Starvation Attacks*. Retrieved February 23, 2022, from Cisco Certified Expert: https://www.ccexpert.us/ccie-security/dhcp-starvation-attacks.html

CCNA. (n.d.). *MAC Address Table Attack*. Retrieved February 23, 2022, from CCNA: https://ccna-200-301.online/mac-address-table-attack/

Howard. (2021, December 24). *What Is DHCP Snooping and How It Works*. Retrieved February 23, 2022, from FS Community: https://community.fs.com/blog/what-is-dhcp-snooping-and-how-it-works.html

Ijaz, A. (2019, August 18). *What is VLAN Attacks – Brief Explanation*. Retrieved February 23, 2022, from NETWORKUSTAD THE LEARNING PLATFORM: https://networkustad.com/2019/08/18/vlan-attacks/

Zola, A. (n.d.). *virtual local area network hopping (VLAN hopping)*. Retrieved February 23, 2022, from TechTarget: https://www.techtarget.com/searchsecurity/definition/VLAN-hopping