
**INDIVIDUAL ASSIGNMENT**

**CT133-3-2-SRE**

**SWITCHING AND ROUTING ESSENTIALS**

**APU2F2211CS (CYB), APD2F2211CS (CYB)**

**APU2F2211IT (CE), APD2F2211IT (CE)**

**HAND OUT DATE: 12th December 2022**

**HAND IN DATE: 25th February 2022**

**Weightage: 40%**

**Online Submission Time before = 11: 59 PM**

**Lecturer: Noris Ismail**

**Student Name:** Kuan Zhi Hui [Report A]

**Student ID:** TP067195

## Table of Contents

# Table of figures

## Introduction

In this part A of this report will be discussing wireless network configuration, WLAN architecture, WLC, WPA2, deployment layer 2 security attacks, and mitigation strategies in order to design and purpose a new wireless network for MicroTech Sdn Bhd. Wireless networking has become an essential component of modern business operations, providing the flexibility and mobility that businesses require to operate efficiently for MicroTech Sdn Bhd.

## 1.0 Proposed the WLAN Architecture

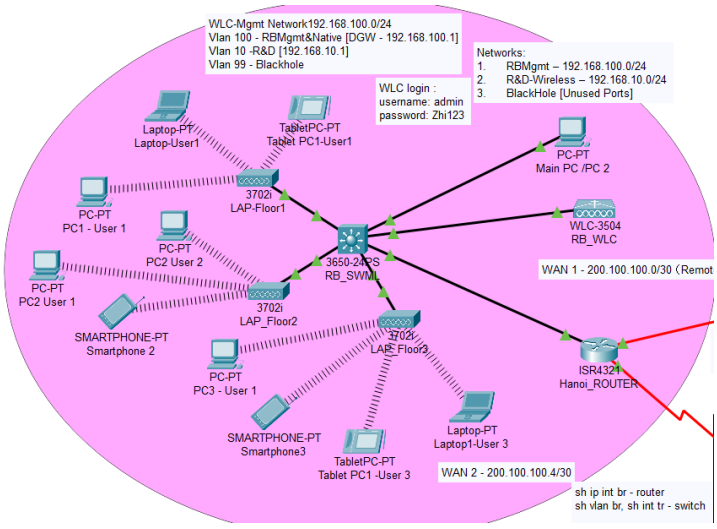


*Figure 1: Wireless network for Hanoi*

In order to configure a well-designed WLAN, it is required to use a WLC-3504 device, a PC, and 3702i LAPs linked by a Multilayer switch. The WLC-3404 device management IP addresses must first be configured in order to implement the WLAN. After that, use the management IPv4 addresses to access to PC web browser by setting up the WLC and configure the wireless network.

The full definition of WLAN is Wireless Local Area Network, which means a wireless network that connects the access point and end devices (techopedia, 2022).

In addition, a lightweight access point is one that delegated the majority of control and management functions to a centralized device, such as a wireless LAN controller (WLC). This simplifies WLAN management and scalability the network.

The devices 3702i acts as a lightweight access point in a WLAN, providing wireless connectivity only to end devices. The WLC, which is in charge of tasks such as authentication, encryption, and traffic management, manages and controls the 3702i by assigning the IP addresses dynamically.

Therefore, the measure to improve data security is to set data encryption in wireless network. Since the key length of WPA2 reaches 256 bits, it is currently the strongest encryption algorithm. By deploying WPA2 with high data encryption strength, the data transmitted by users in through wireless will not be cracked easily.

## 1.1 Configure static IP addresses for PC and the WLC-3540

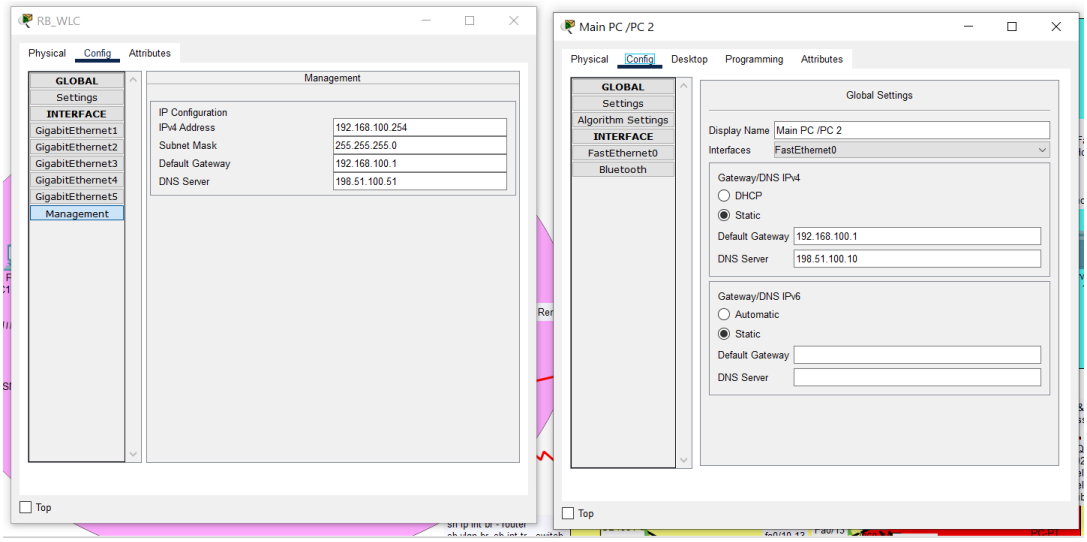


*Figure 2: configuration for the WLC-3504 and the PC*

Before configuring the WLC it is a must configure the static IP addresses in WLC-3504 and the PC which connected with the multilayer switch. After that, use the management IPv4 address log in to the PC web browser, for initial set up the WLC configuration.

### 1.2 WLC Configuration – Sign up for WLC.


*Figure 3: Create user account on WLC.*

The requirement to configure the WLC successfully for the initial setup we must use the Access Point WLC-3504 config to multilayer switch after that access to the WLC-3504 management and use the IPv4 Address access to the web browser in Main PC. In the PC web browser, we must access to

http://192.168.100.254 first for create new username and password purpose. The username is **admin,** and the password is **Kzh123** is setup for account credentials.


*Figure 4 The login page of WLC*

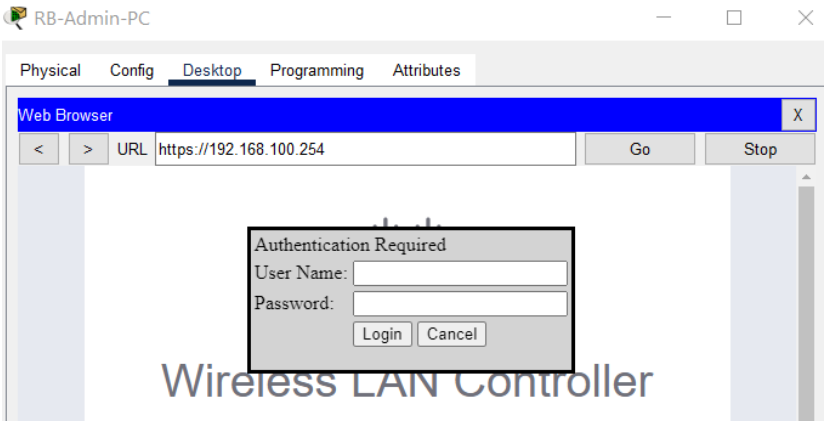


*Figure 5: username and password for WLC*

When the setup of WLC is completed, we can use https://192.168.100.254 to access the web browser again, for access the WLC login page. The HTTP with s is the secure socket layer with encrypt format, while HTTP without s is a request for sign into the web browser.

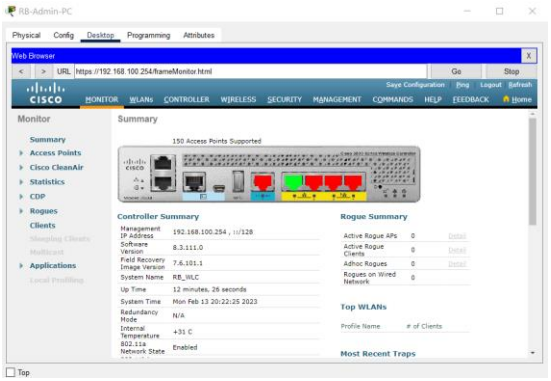


*Figure 6: Home page of WLC (Monitor)*

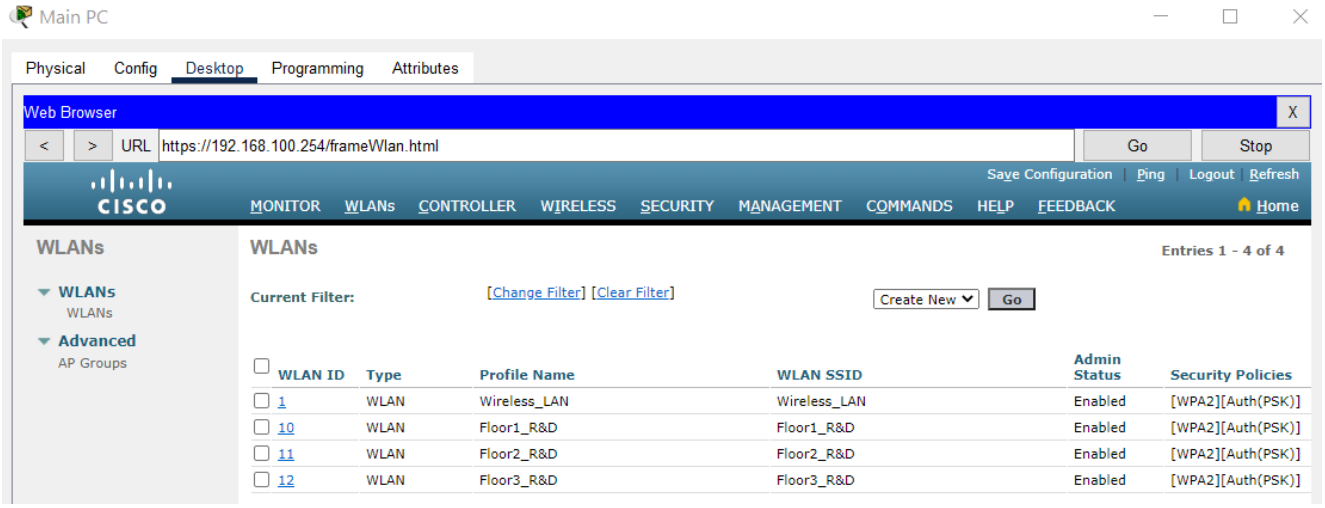


*Figure 7: Home of WLC (WLANs)*

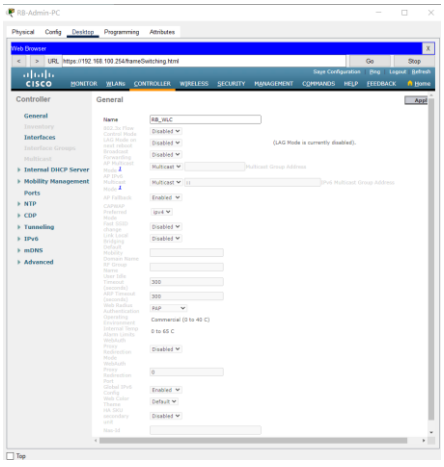


*Figure 8 The home page of WLC configuration (Controller)*

From figure 5,6, & 7, it shows that once the login is successful, then the main page will display the interface design of WLC which have Monitor, WLANs, Controller and so on.

## 1.3 Create or Setup new WLAN

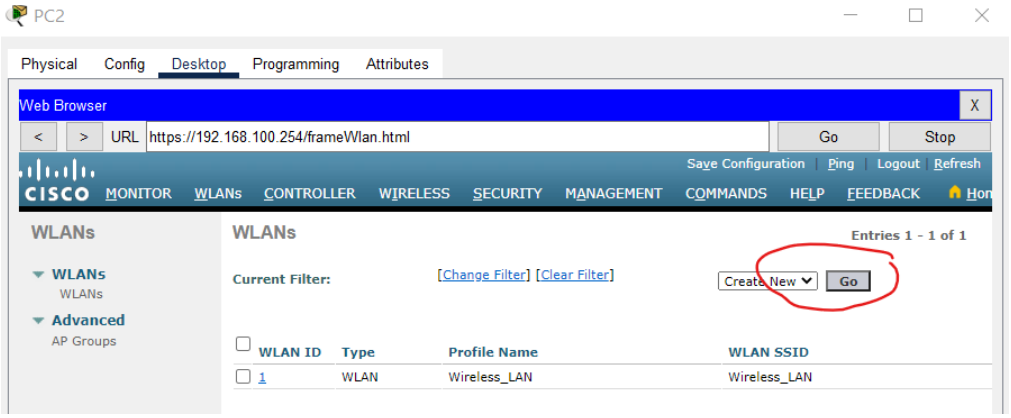


*Figure 9: Create new WLAN.*

The purpose of login WLC is to create new WLAN for configure the wireless network. From figure 8, we can click button **go** to create new WLAN.

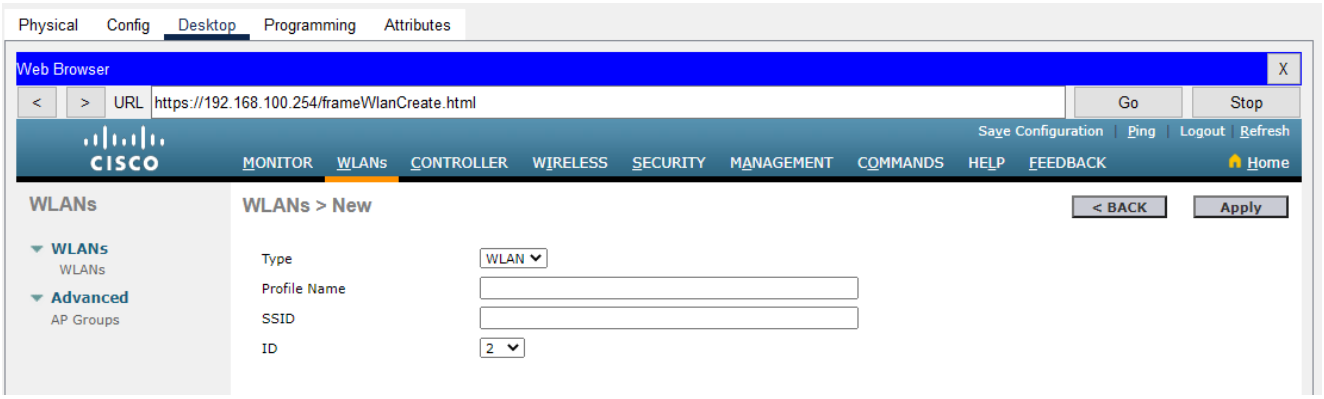


*Figure 10: Create new WLAN (New page)*

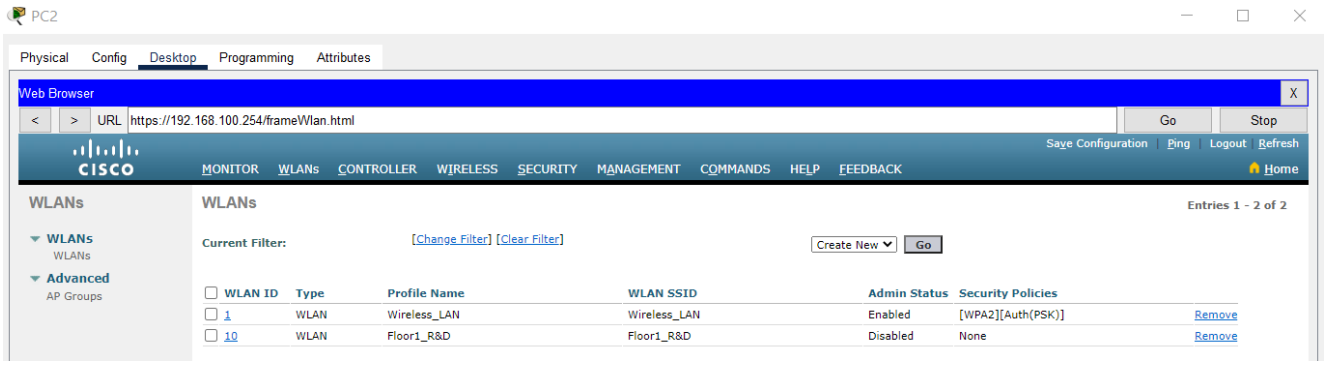


*Figure 11: Create new WLAN successful.*

From figure 9, it shows that when clicked button **go,** we will access to the **New** page for create the new WLAN profile name, SSID and ID. In figure 10, once it created click save configuration and go back to WLANs page for verify again.

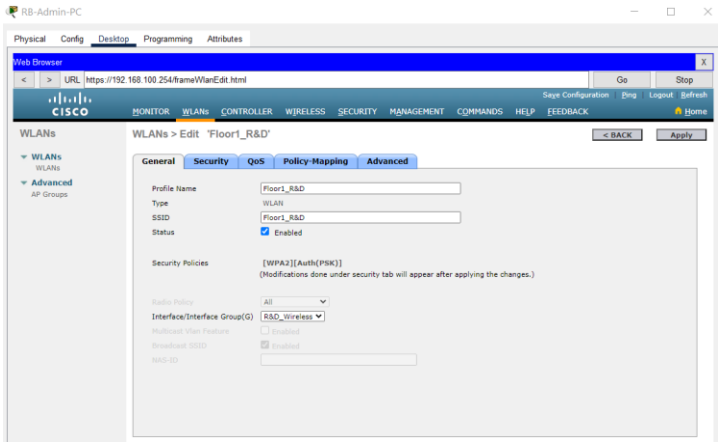


*Figure 12: Edit the general details of WLAN.*

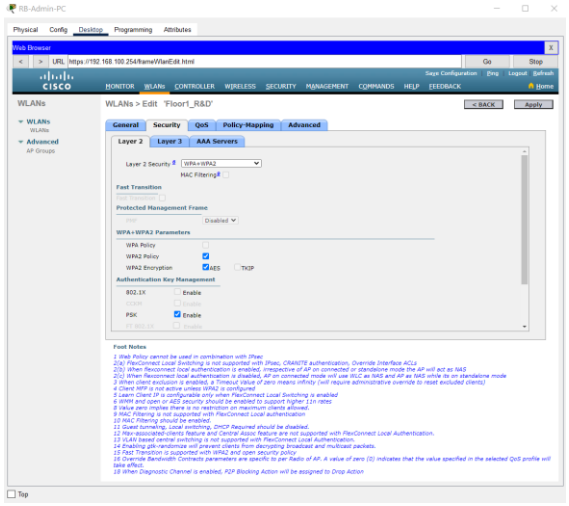

*Figure 13: Edit the security details of WLAN.*


*Figure 14: Edit advanced details in authentication key management by enable PSK and adding PSK Format*

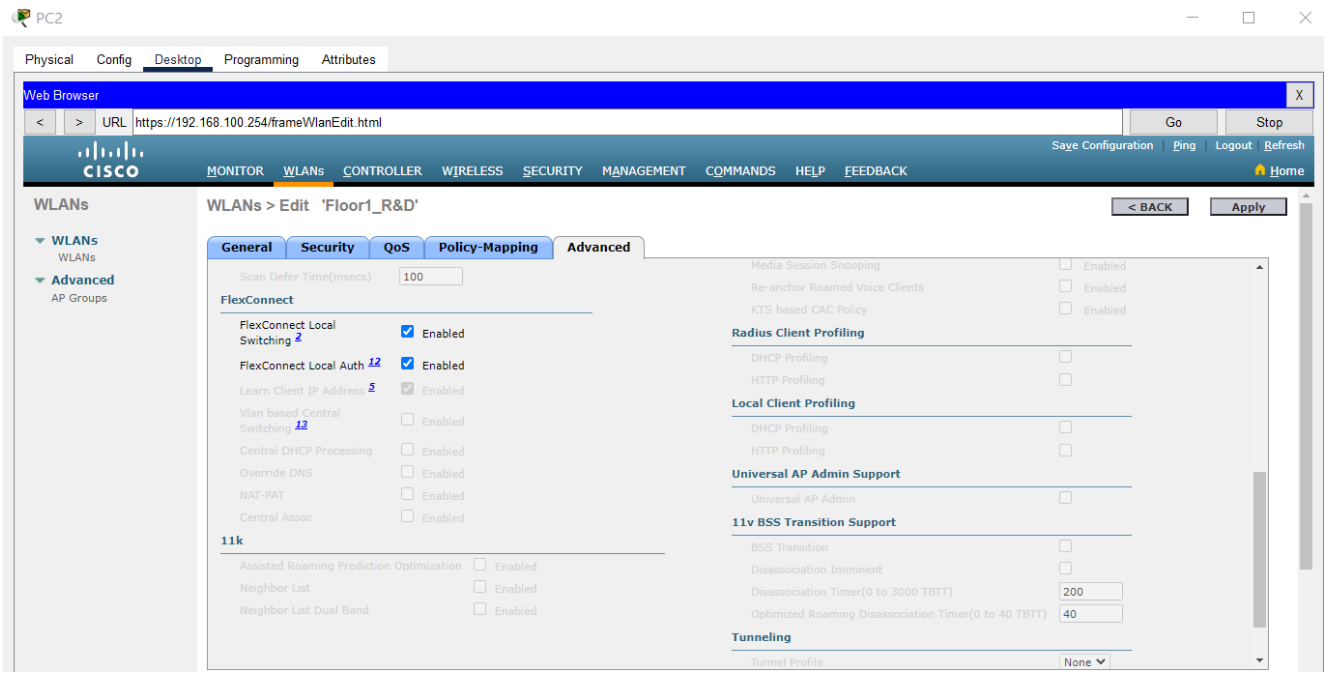


*Figure 15: Edit advanced details (FlexConnect by enabling FlexConnect Local Switching & FlexConnect Local Auth)*

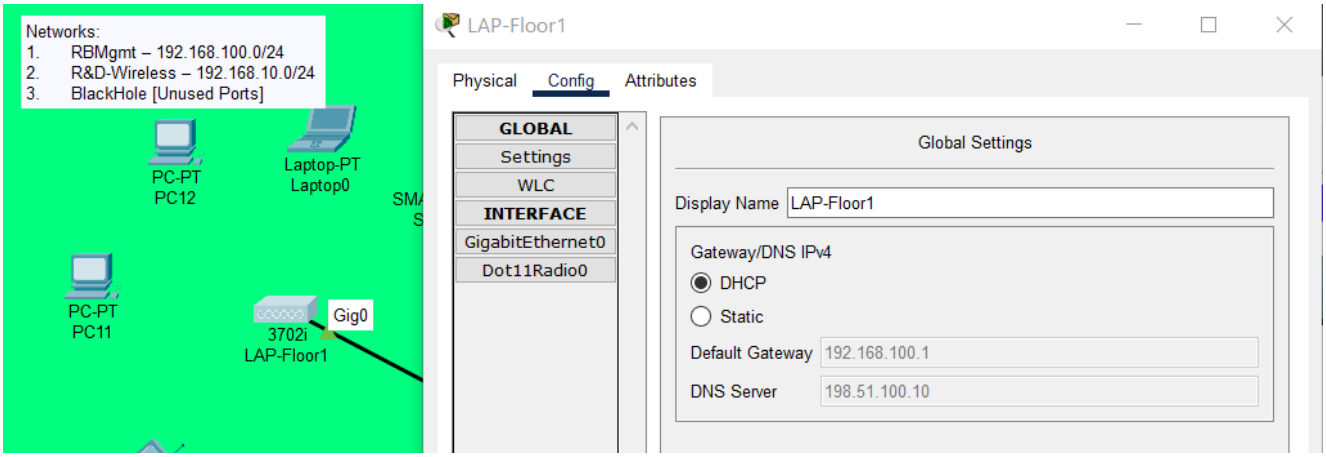


*Figure 16: Go to LAP-Floor 1 to click DHCP.*

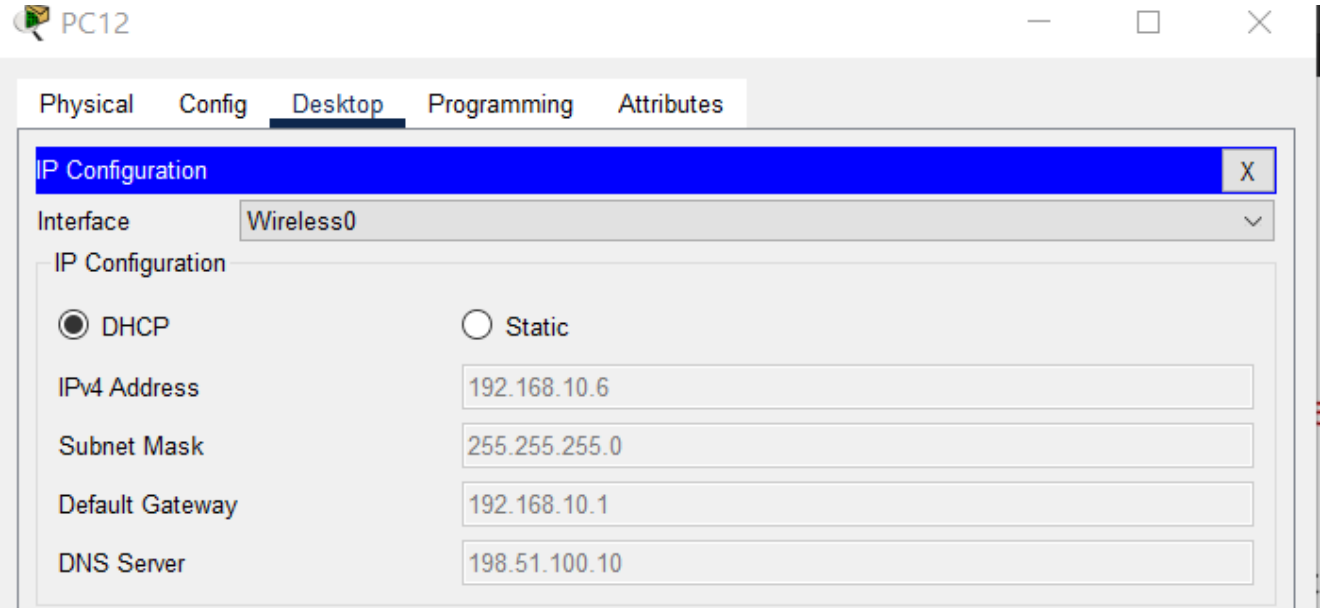


*Figure 17: Go end devices (PC 12) change the IP configuration to DHCP.*

### 1.1 Assign new interfaces name and ID.

When assigning an interface name, one can create a descriptive label that identifies the interface's purpose, such as "WLAN" for a wireless LAN interface or "LAN" for a wired LAN interface. Assigning an ID to an interface it is also important because it ensures that each interface within the WLC has a unique identifier that can be used to reference the interface in configuration settings and monitoring tools.

By giving WLC interfaces names and IDs, one can make it easier to manage and troubleshoot the network, as well as ensure that your configuration settings are applied to the correct interface.

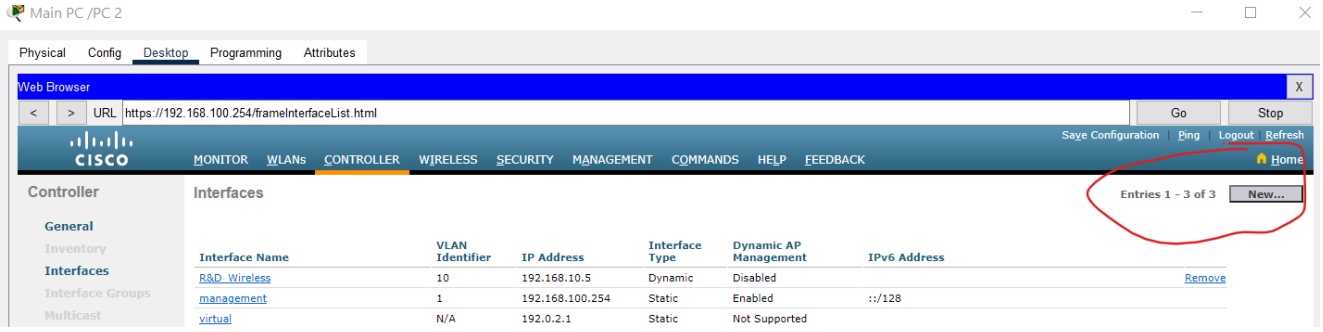


*Figure 18: The home page of interfaces*

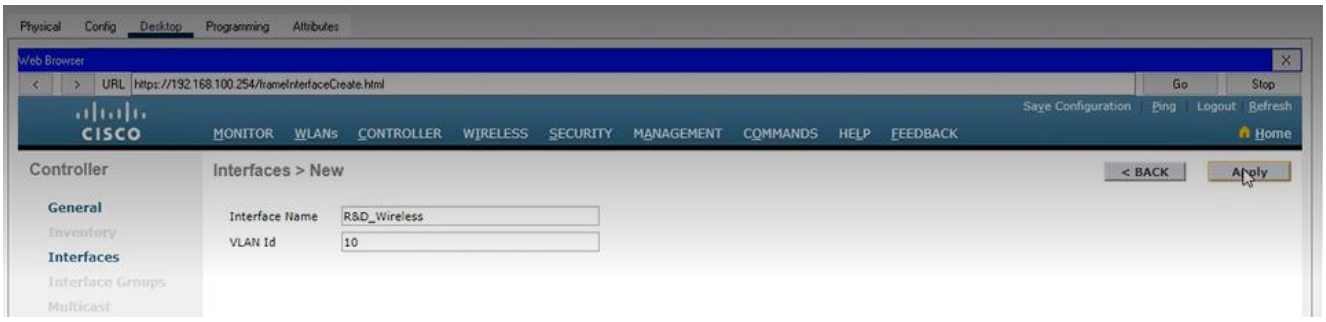


*Figure 19: Create new interfaces name and id (New)*

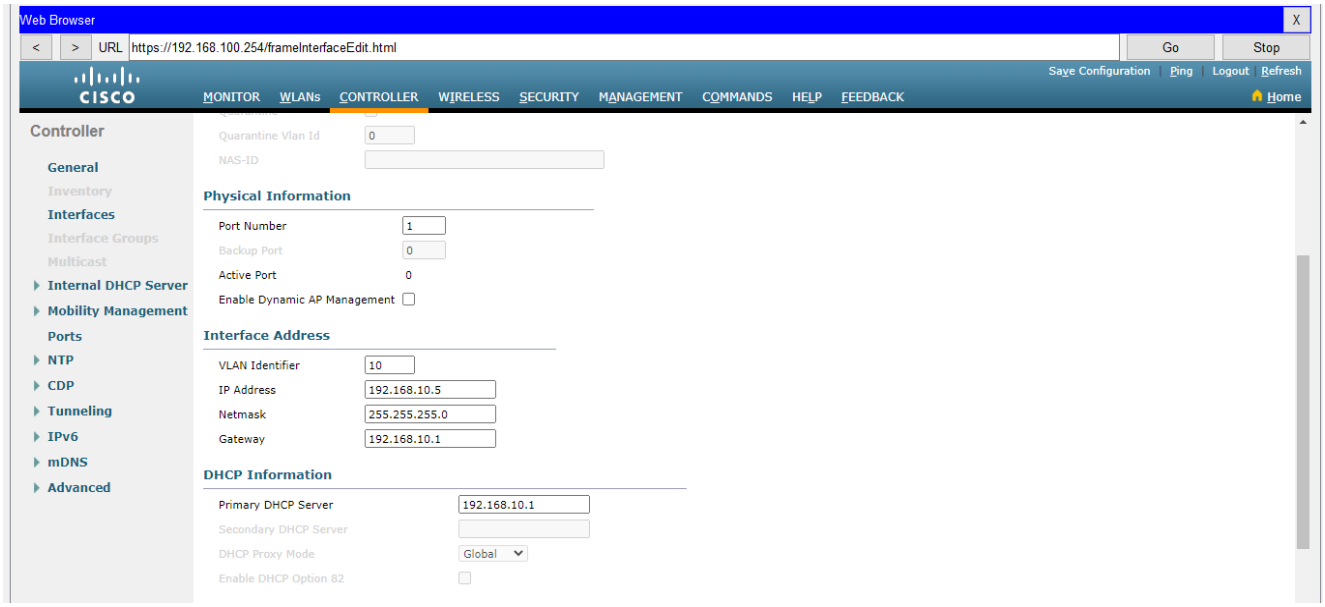


*Figure 20: Edit the details on physical information, interfaces address and DHCP information.*

## 1.4 Set up internal DHCP Servers

By reusing IP addresses that are no longer in use and by supplying setup like DNS server IP addresses, domain names, and DNS server IP addresses, a DHCP server also contributes to more effective management of IP address allocation. This makes it less likely that IP address conflicts will occur and guarantees that network devices are configured correctly for optimum performance.

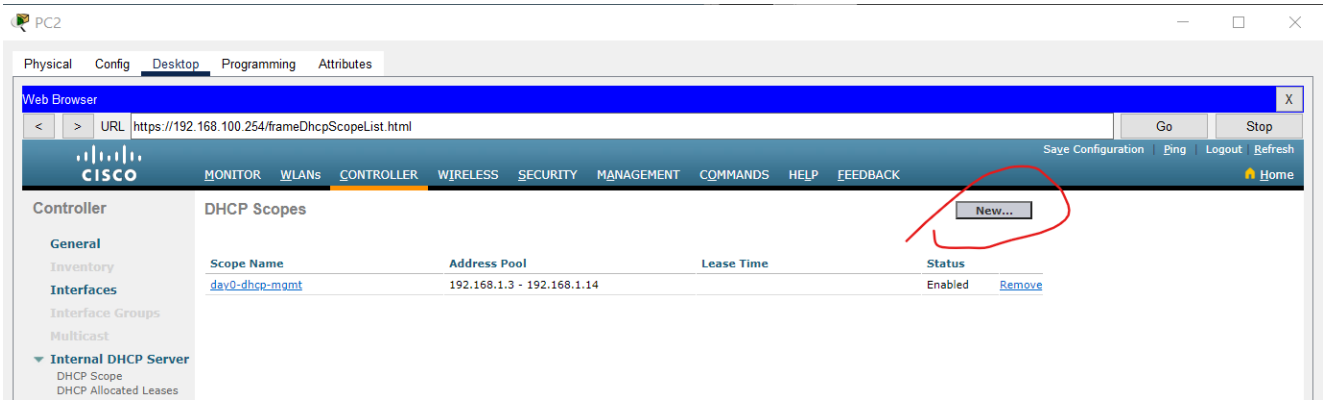


*Figure 21: DHCP Server (DHCP scope)*

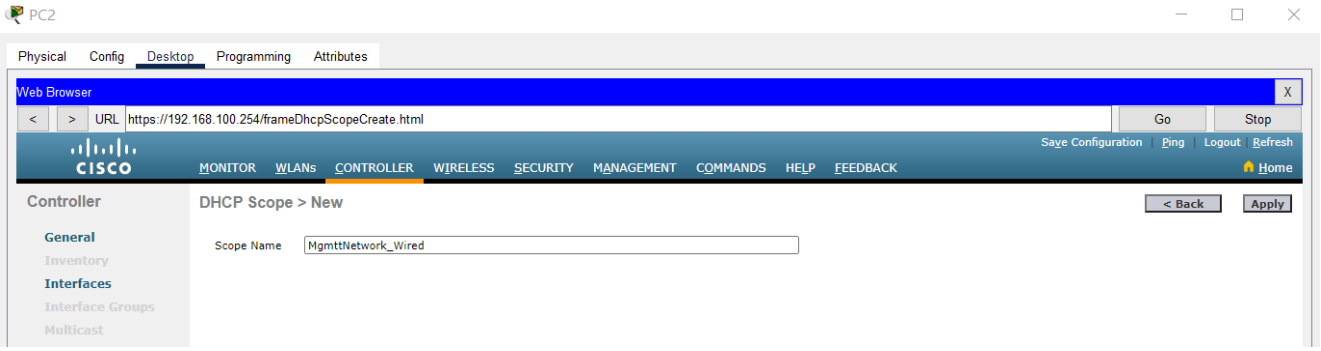


*Figure 22: Create new scope name and click apply.*

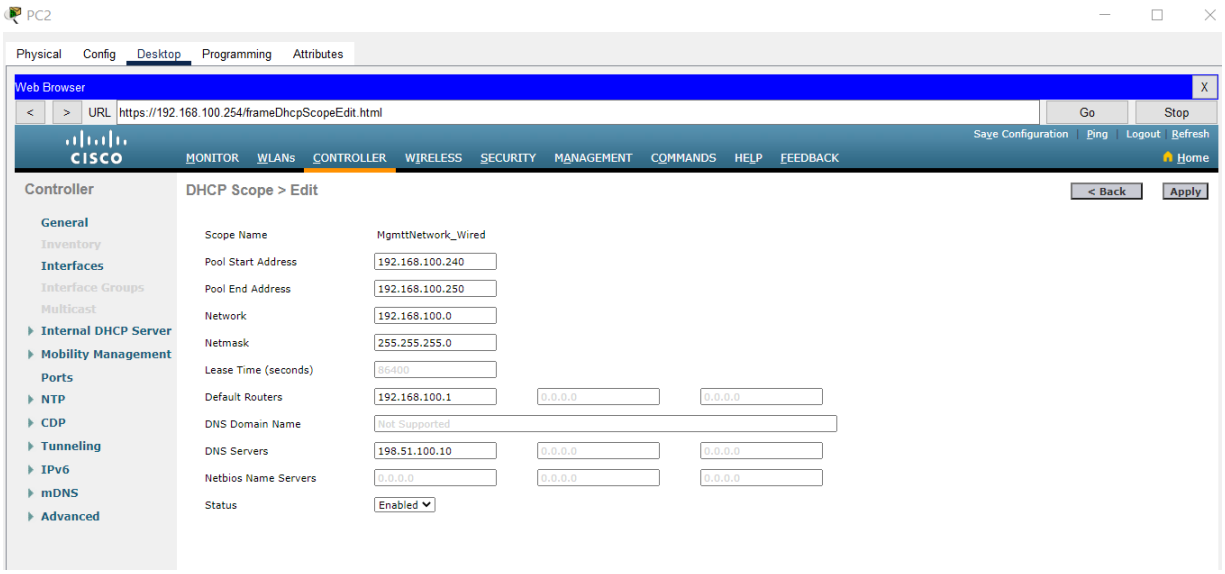


*Figure 23: Edit the DHCP scope details.*

## 1.5 AP Groups Set up and Configuration.

According to the security needs of each location or user group, AP group configuration also enables one to apply various security settings to various groups of APs. By doing so, network security is enhanced and unwanted access to the wireless network is prevented. One can apply particular configuration settings, such as wireless LAN settings, QoS settings, VLAN settings, and more to each group by grouping APs together. As a result, managing and maintaining the wireless network is made simpler because you may configure one AP at a time rather than having to configure every AP individually.

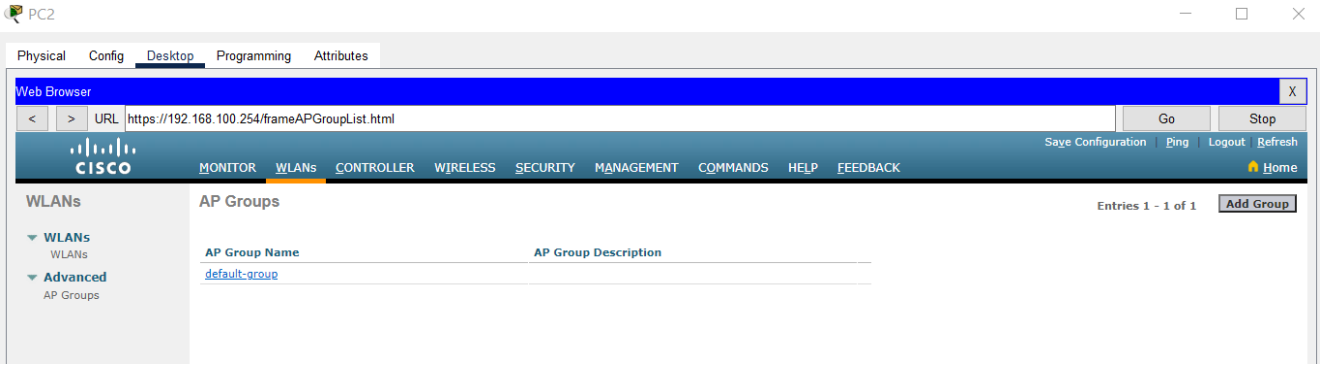


*Figure 24: the main page of AP Groups*

After setting up the wireless pc and laptop successful now go back to WLANs click AP Group go add new group for continue configure new wireless network.

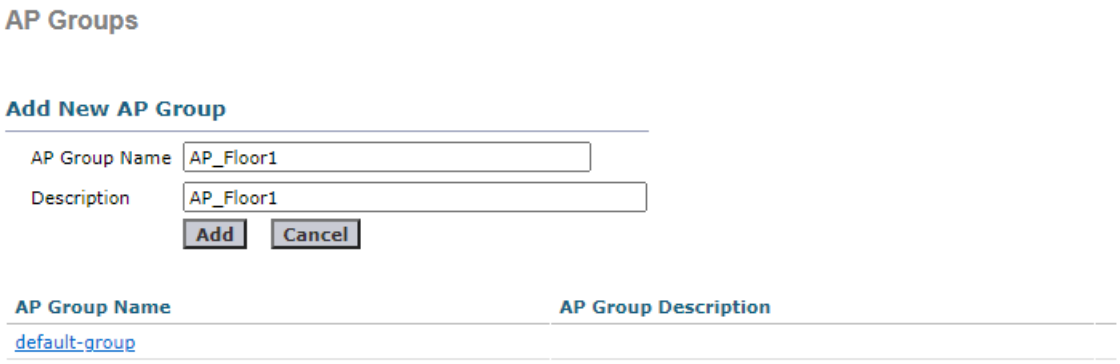


*Figure 25: Create new AP Group name and description.*

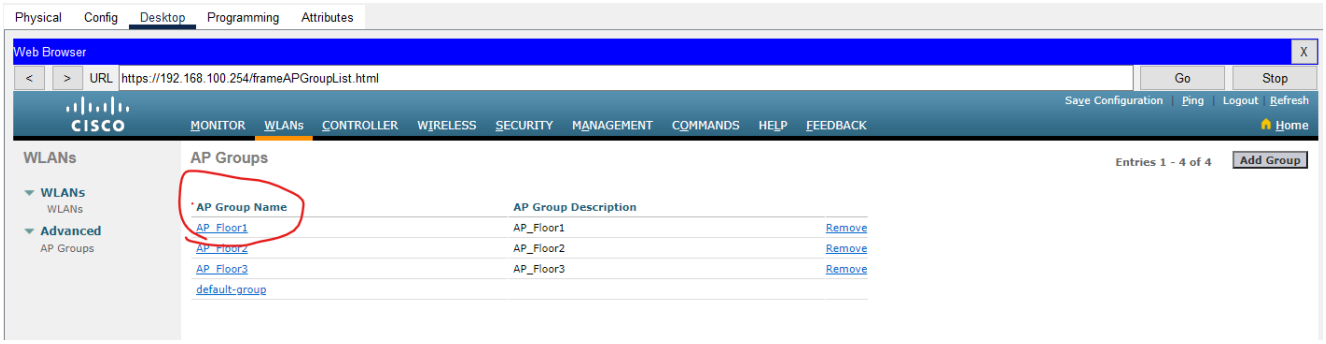


*Figure 26: Click one of the AP_Group for edit details.*

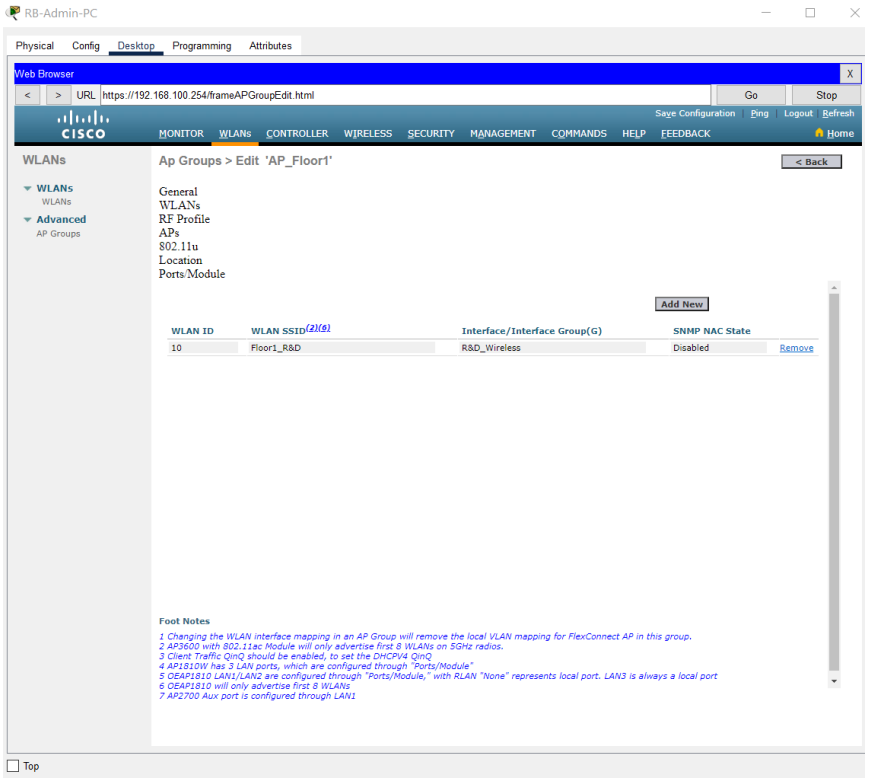


*Figure 27: Add new group at AP_Floor 1*

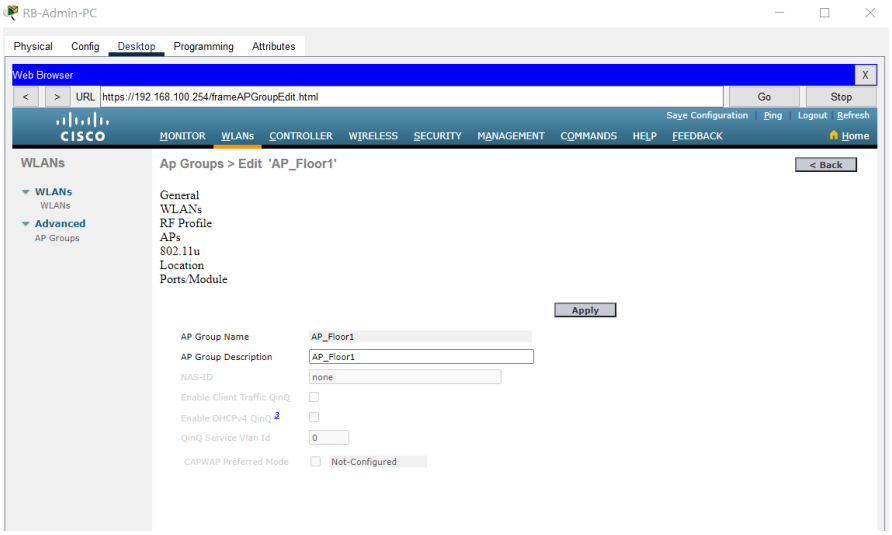


*Figure 28: Click apply after setting up the new AP group and go WLANs verify.*

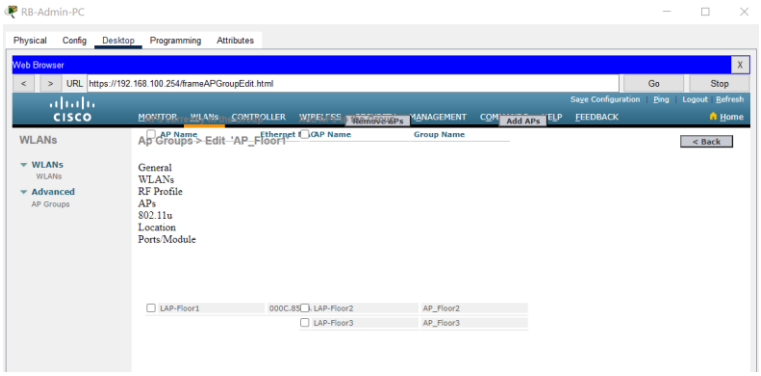


*Figure 29: Click APs> tick LAP_Floor1 > add API*

### 1.6 Set up the end devices for configure wireless.

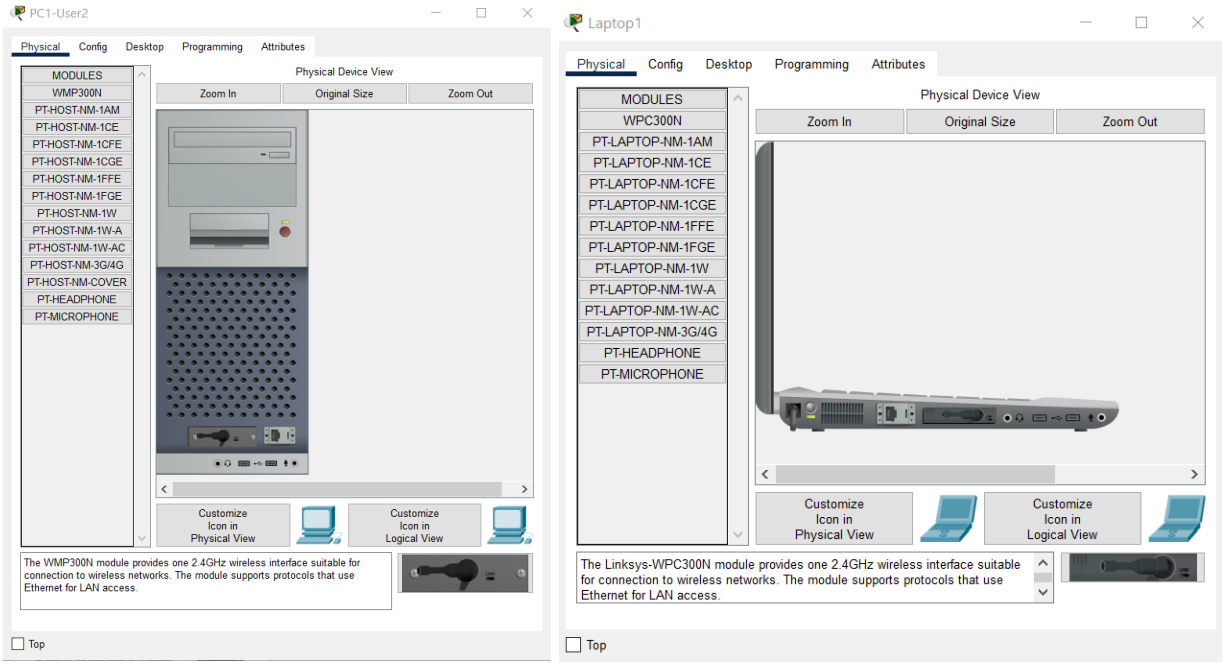


*Figure 30: change the manual set up to wireless.*

## 1.7 configure WLANs. – WPA2

WPA2 is the second generation of the Wi-Fi Protected Access security standard, resulting in it being more secure than WPA (Ghimiray, 2022). The WPA protocol is based on the previous generation of WEP. It is more rigorous in terms of security protection such as encryption mechanism, identity authentication, and data packet inspection. WPA2 is an upgraded version of WPA encryption. It is an IEEE 802.11i standard authentication form verified by the WiFi Alliance. It is considered to be a safer encryption method. Therefore, most devices and Wi-Fi routers will rely on it to encrypt Wi-Fi flow.

To encrypt data in the network, WPA2-PSK requires a device with a passphrase of 8 to 63 characters. It will generate unique encryption keys for each network device based on the network SSID and the passphrase. In Packet Tracer, the permit is typically defined in the access point, and the user must enter the same PSK with paraphrase key on end devices to connect to the wireless network dynamically.

AES is a type of strong symmetric encryption that is used in everything from web traffic encryption to password managers (Orphanides, 2022). It is generally used for server-to-server Encrypt and decrypt between data. AES encryption and decryption feature reversible and symmetric block encryption, and its speed is much faster than that of other encryption algorithms such as public key encryption. According to the AES standard, the block length has only one value, which is fixed at 128 bits, and the

corresponding byte is 16 bits. The AES algorithm specifies only three key lengths: 128Bit, 192Bit, and 256Bit, with corresponding bytes of 16 bits, 24 bits, and 32 bits. The key KEY, which is used to encrypt and decrypt data, cannot be publicly transmitted.

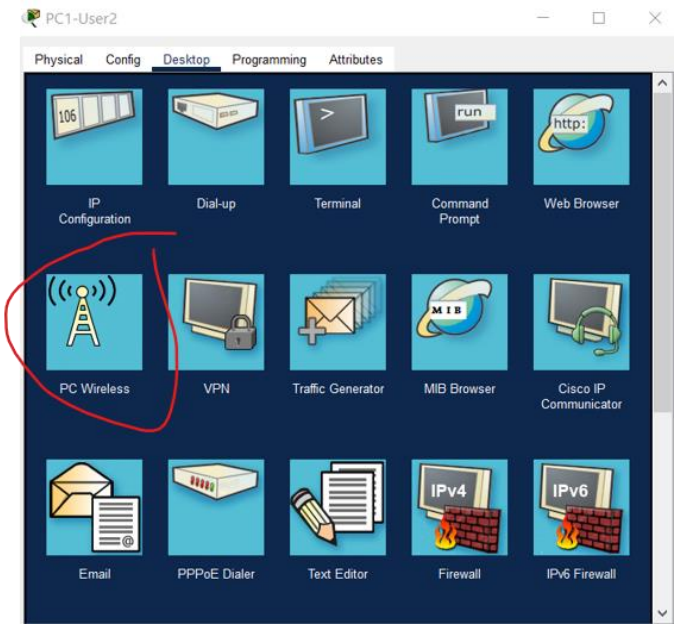


*Figure 31: Go to Wireless*


*Figure 32: The wireless (link information interface)*


*Figure 33: Wireless network connection interface*

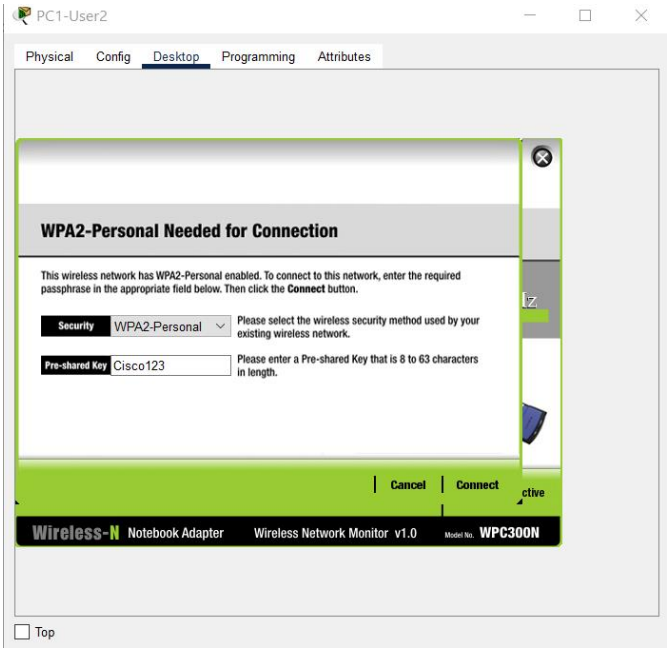


*Figure 34: Wireless configuration set up for PC or Laptop*

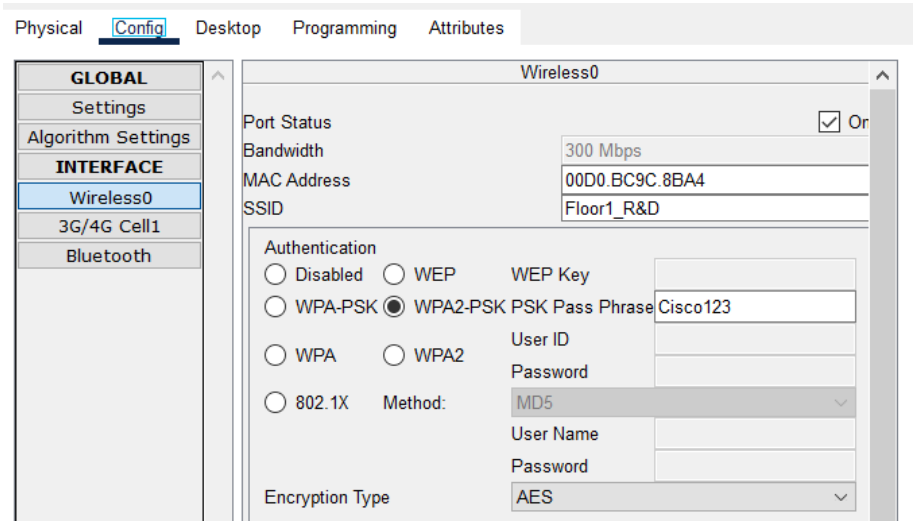


*Figure 35: WPA 2 creation*

## 2.0 Layer 2 Security Attacks

### 2.1 VLAN Hopping Attack

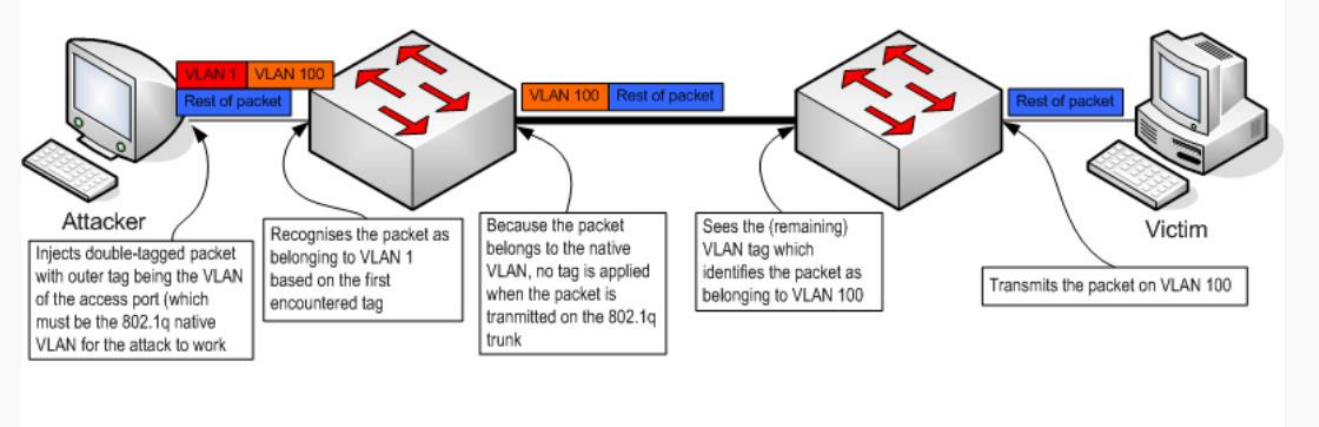


*Figure 36: The illustration of VLAN hopping attacks*

VLAN hopping attacks enable data frames from one VLAN to gain access to other VLANs on the same network. As a result, attackers can send traffic to a VLAN that their host shouldn't be able to access. Switch spoofing and double tagging are the two main methods used in VLAN hopping attacks (Redfox Security, 2022).

### 2.1.1 Switch Spoofing VLAN Hopping Attack

VLAN hopping attacks rely on the Dynamic Trunking Protocol (DTP). If there are two switches connected to each other, DTP can negotiate whether they should become 802.1Q trunks, and the negotiation process is completed by checking the configuration status of the ports.

VLAN hopping attacks take advantage of DTP. In a VLAN hopping attack, an attacker can trick a computer into sending a fake DTP negotiation message masquerading as another switch, announcing that he wants to be a relay and stealing data from an end device (Morales, 2023). After the relay is established, the attackers can continue to detect the information flow, or specify which VLAN to send the attack traffic to by adding 802.1Q information to the frame. It works when the 802.1Q trunking function should be enabled, and once the trunking function is enabled, the traffic through all VLANs will be sent to the attacker's computer. Therefore, it is important to disable DTP on all unused and non-trunking interfaces, including the Null0 interface, to prevent security vulnerabilities.

By convincing a switch into forming a trunk link with the attacker's device, the Switched Spoofing VLAN Hopping Attack allows attackers to view traffic from all VLANs on a network. The attacker can do this by creating a DTP message on their computer, attaching it to a switch interface, and then switching the switch interface to "dynamic desired," "dynamic auto," or "trunk" modes (Azad, 2022).

### 2.1.2 Double Tagging VLAN Hopping Attack

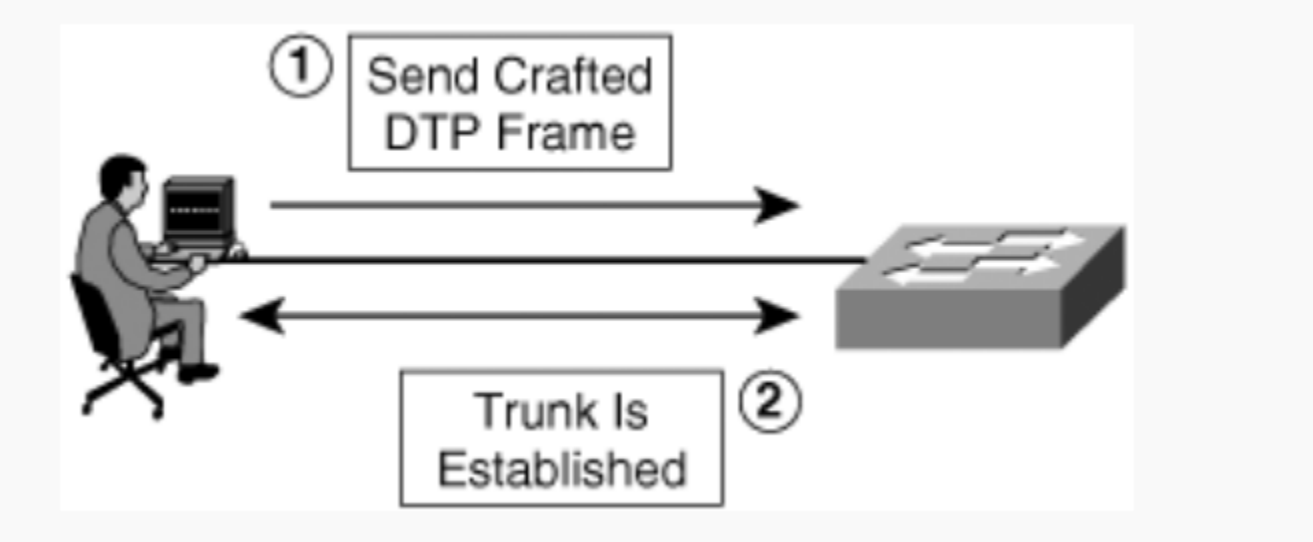


*Figure 37: illustration of Double tagging VLAN hopping attacks*

Doubling up on VLAN tags is another type of VLAN Hopping attack. The double tagging attack will only work if the attacker is connected to an interface that belongs to the trunk port's native VLAN. The double tagging attack is one-way. The Double Tagging VLAN Hopping Attack is when an attacker adds

two tags to the original frame. Since switches typically only remove the outer tag and can only identify the outer tag, the inner tag is preserved. The outer tag is associated with the attacker's VLAN, while the inner tag is associated with the victim's VLAN.

When the maliciously crafted double-tagged frame reaches the switch, the switch identifies the outer tag as belonging to the attacker's specific VLAN and forwards the frame to all native VLAN links while also sending a copy of the frame to the trunk link to the next switch. The first VLAN tag identifies the target VLAN, while the second VLAN tag identifies the VLAN on which the attacker is currently operating. The attacker would then send packets to devices connected to both the target and attacker VLANs with a double tagged VLAN header. The packets will be processed and forwarded to the attacker's VLAN by this device. This allows the attacker to gain access to traffic from the victim's VLAN, for the double tagging attack only works in one direction and it is impossible to contain the return packet (Morales, 2023).

## 2.2 MAC Address TABLE Flooding Attack

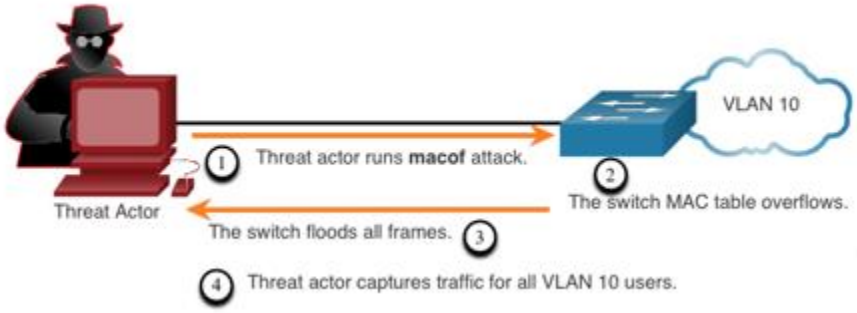


*Figure 38: mac address table flooding attacks illustration*

MAC (Media Access Control) flooding is a type of network cyber-attack that compromises the security of network switches. The network is flooded with fake MAC addresses in this attack. This attack is used by the hacker to steal sensitive data that is being transferred across the network. The attack is used to force the switch's legitimate MAC table contents out and to force unicast flooding behaviour, potentially sending sensitive information to parts of the network where it is not normally intended to go (opengenus.org, n.d.).

With the false source, the attacker will generate a large number of data frames. In these data frames, MAC addresses are forged and constantly changing. When the MAC address table is full, the network

switch enters fail-open mode and functions as a network hub, broadcasting all packets across all switch ports.

## 2.3 STP Attack

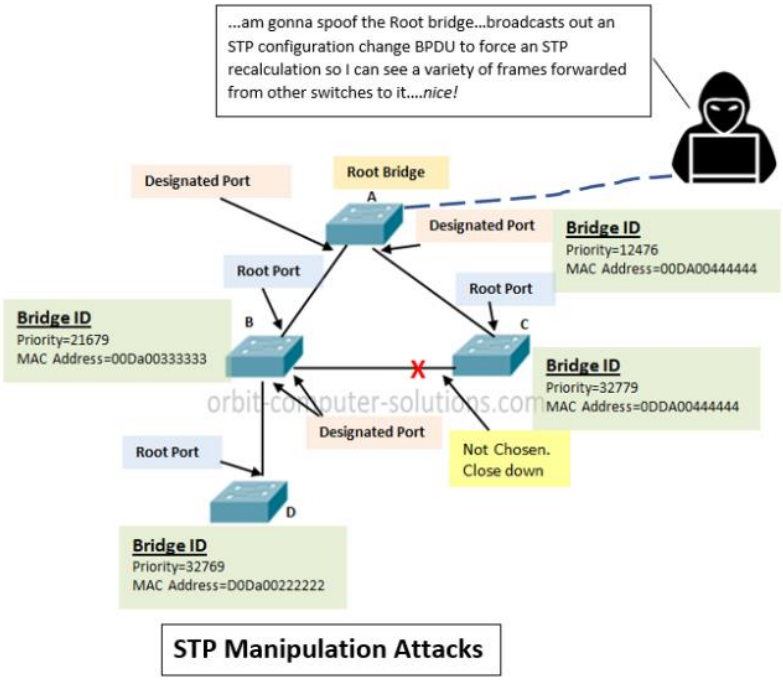


*Figure 39: STP attack illustration*

An STP manipulation attack is when an unauthorized user alters the STP topology by spoofing the root bridge. This is achieved by broadcasting an STP configuration change BPDU with the lowest ID as an unauthorized switch to initiate an STP recalculation. By doing so, the attacker's system becomes the root bridge, and most traffic will pass through their switch. The attacker can then manipulate the traffic by enabling switch ports to become trunk ports and sniffing on all traffic within the company. In addition, they can redirect traffic from high-bandwidth links between other switches to their own 100 Mbps links. Attackers can also connect a rogue switch to a company's network wall jack to negotiate a trunk link with a switch in the company. It is important to note that an STP recalculation can cause a 30 to 45 second outage, which can lead to a denial of service (DoS) condition on the network (orbitco, 2020).

# 3.0 security deployment to mitigate the attacks.

## 3.1 Mitigation for switch spoofing VLAN Hopping Attack

- switch1 (config) # interface gigabit ethernet 0/3
- Switch1(config-if) # switchport mode access
- Switch1(config-if)# exit

- Switch1(config)# interface gigabitethernet 0/4
- Switch1(config-if) # switchport trunk encapsulation dot1q
- Switch1(config-if) # switchport mode trunk
- Switch1(config-if) # switch port nonegotiate

*Figure 40: Configure trunk port to disable trunking and prevent the use of DTP.*

Switch spoofing is a network attack technique in which the attacker redirects network traffic to a location controlled by the attacker by deceiving the switch to steal network information or launch other attacks. In a switched spoofing VLAN hopping attack, the attacker pretends to be a switch to exploit a legitimate switch by tricking it into creating a trunking link between the attacker's device and the switch. A trunk link is used to transport traffic between switches or switches and routers while storing VLAN data. Data frames passing through the trunk link are tagged so that the VLAN can be identified, allowing the link to transport traffic from multiple VLANs. However, if the attacker successfully establishes the trunk link, they gain access to traffic from all VLANs on the network. While packets from any VLAN can travel across the trunking link, the attacker is able to exploit the vulnerability and access all VLAN traffic (Azad, 2022).

In order to prevent a Switched Spoofing attack "dynamic desirable," "dynamic auto," or "trunk" modes should not be configured. It is compulsory to manual configuring trunk ports, disabling DTP and shutting down blackhole ports by hardcoding switchport mode access, switchport trunk encapsulation dot1q, switchport mode trunk and switchport nonegotiate (AT&T Cybersecurity, 2019).

## 3.2 Mitigation for Double Tagging for VLAN Hopping Attack

```
Delivery_SW(config)#int ra fa0/1-2, fa0/11-11, fa0/10-13, fa0/12-12, fa0/14-14
Delivery_SW(config-if-range)#switchport trunk native vlan 100
```

*Figure 41: Prevent double tagging.*

Setting the trunk native VLAN for a trunk port is important for mitigating the risk of double tagging VLAN attacks. Double tagging VLAN attacks can occur when an attacker sends packets with two VLAN tags, one inside the other, to a switch port mode to trunk port (ccexpert.us, 2023). It will transfer the outer VLAN tag as the VLAN for the port and forwards the packet accordingly once the switch receives packet. However, the attacker's intended VLAN tag inside the outer tag may also be interpreted by the switch, leading to unauthorized access to other VLANs on the network.

By configuring the trunk port's native VLAN, the switch will treat any packets received on that port that lack a VLAN tag as belonging to the native VLAN. This helps to prevent double-tagging attacks because any packets with an inner VLAN tag are dropped by the switch. Furthermore, configuring the native VLAN can help avoid potential issues with misconfigured ports or devices that do not support VLAN tagging, ensuring that traffic flows as intended and avoiding unnecessary network management complications.

## 3.3 Mitigation for MAC Address Table Flooding Attack

```
S4(config)# interface fastEthernet 0/10
S4(config-if)# switchport mode access
S4(config-if)# switchport port-security
S4(config-if)# switchport port-security maximum 5
S4(config-if)# switchport port-security violation shutdown
S4(config-if)# switchport port-security mac-address sticky
```

*Figure 42: mitigation of mac address hardcode*

Port security can be used to prevent MAC flooding attacks. This can be accomplished by enabling this feature in port security with the switchport port-security command. Using the "switchport port-security maximum" setting, specify the maximum number of addresses that can be assigned to the interface and set violation mode (Shais, 2020).

To prevent MAC address flooding attacks, it's essential to limit the number of MAC addresses a switch can learn from a port. When an attacker floods the switch with fake MAC addresses, the switch may stop learning new ones and legitimate devices would not be able to communicate on that port. Setting a maximum number of MAC addresses helps prevent this situation and configuring the violation mode to "restrict" alerts the network administrator without causing a network outage. Alternatively, the violation mode can be set to "protect" or "shutdown," but "restrict" is preferred because it allows the switch to continue operating while still providing an alert to the administrator. If a violation occurs in "protect" mode, the port takes action to limit the impact of the violation while remaining active. However, the difference between the "protect" and "restrict" modes lies in the actions taken by the switch when a violation occurs. In the "protect" mode, when a violation occurs, the switch will still send an SNMP trap or log a message indicating that a violation has occurred, but it will also drop any frames that have a source MAC address that is not allowed on the port. The "protect" mode can be useful in certain situations where a more aggressive response is required to mitigate a security threat. However, it can also potentially cause issues if legitimate traffic is dropped because of a violation. For this reason, the "restrict" mode is typically a more commonly used and safer option for most networks. Ultimately, the choice of which violation mode to use depends on the specific security requirements ( Cisco Certified Expert, 2023).

## 3.4 Mitigation for STP attack

Preventing Spanning Tree Protocol (STP) manipulation attacks which are PortFast and Bridge Protocol Data Unit (BPDU) Guard can be configured for the network. PortFast is used on end-user ports to immediately forward an access or trunk port, bypassing the listening and learning states. It should, however, only be used on ports that are connected to end devices. BPDU Guard, on the other hand, disables a port as soon as it receives a BPDU, similar to PortFast (ccna-200-301.online, n.d.). However, it can potentially cause network loops and disrupt network connectivity if PortFast is enabled on a port that is connected to another switch. Since PortFast is a feature that allows a switch to initiate communication much more quickly and it is suggested only enabled on switch ports that are in access mode. Whereas BPDU Guard is a feature that helps protect against STP attacks by deactivating a port upon receiving a BPDU on a non-BPDU receiving port. This enables PortFast. Once enabled, any BPDU received on the port will disable it to prevent possible network interruptions. This can help to prevent an attacker from manipulating the STP topology by sending fake BPDUs. Hence, it is vital for enabling both PortFast and BPDU Guard on ports that are connected to end devices can help to prevent STP attacks and improve network performance, while still maintaining the integrity of the STP topology.

## Conclusion

In conclusion, there are several important aspects of configuring a wireless LAN controller (WLC) and deploying WPA2 security to ensure a secure wireless network to design for the new network for MicroTech Sdn Bhd. The process of configuring a WLC, which involves configuring the basic settings, creating wireless networks, and configuring security settings. The importance of WPA2 security, which provides strong encryption and authentication mechanisms to protect wireless networks from unauthorized access and attacks. In addition, the deployment of layer 2 security, which includes techniques such as VLANs, disabling DTP and port security to prevent attacks and unauthorized access. By following these best practices, MicroTech Sdn Bhd can effectively mitigate wireless network attacks and ensure the confidentiality, integrity, and availability of their wireless networks.

# References

*Cisco Certified Expert*. (2023, February 19). Retrieved from https://www.ccexpert.us/configuration-mode/port-security-configuration.html

(2020, July 1). Retrieved from https://www.orbit-computer-solutions.com/network-security-stp-manipulation-attacks/

*arubanetworks*. (n.d.). Retrieved from https://www.arubanetworks.com/techdocs/ArubaOS_83x_Web_Help/Content/ArubaFrameStyles/Network_Parameters/Portfast%20and%20BPDU%20Guard.htm#:~:text=The%20PortFast%20and%20BPDU,free%20topology%20for%20Ethernet%20networks.%20.

*AT&T Cybersecurity*. (2019, December 19). Retrieved from https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation#:~:text=To%20prevent%20a%20Double%20Tagging,ports%20different%20from%20user%20VLANs.

Azad, U. (2022). Retrieved from https://linuxhint.com/vlan-hopping-attack-mitigation/

Azad, U. (2022). Retrieved from https://linuxhint.com/vlan-hopping-attack-mitigation/

Azad, U. (2022). Retrieved from https://linuxhint.com/vlan-hopping-attack-mitigation/

*ccexpert.us*. (2023, Febrauary 19). Retrieved from https://www.ccexpert.us/bcmsn/importance-of-native-vlans.html

*ccna-200-301.online*. (n.d.). Retrieved from https://ccna-200-301.online/mitigate-stp-attacks/#:~:text=To%20mitigate%20Spanning%20Tree%20Protocol,the%20listening%20and%20learning%20states.

Ghimiray, D. (2022, January 20). Retrieved from https://www.avast.com/c-wep-vs-wpa-or-wpa2#:~:text=WPA2%20is%20the%20second%20generation,most%20secure%20Wi%2DFi%20protection.

Goel, S. (2021, April 28). Retrieved from https://www.encryptionconsulting.com/is-wpa2-psk-vulnerable/

Morales. (2023, January 3). Retrieved from https://lemp.io/how-to-use-dtp-for-vlan-hopping-attacks/

Morales. (2023, January 3). Retrieved from https://lemp.io/how-to-use-dtp-for-vlan-hopping-attacks/

*opengenus.org*. (n.d.). Retrieved from https://iq.opengenus.org/mac-flooding-attack/

orbitco. (2020, July 1). Retrieved from https://www.orbit-computer-solutions.com/network-security-stp-manipulation-attacks/

Orphanides, K. (2022, April 29). Retrieved from https://www.trustedreviews.com/explainer/what-is-wpa2-4229330

*pearsonitcertification*. (2016, Feb 25). Retrieved from https://www.pearsonitcertification.com/articles/article.aspx?p=2491767#:~:text=Spanning%20Tree%20Protocol%20(STP)%20Attacks&text=Its%20primary%20function%20is%20removing,flood%20the%20switches%20with%20traffic.

Popeskic, V. (n.d.). Retrieved from https://howdoesinternetwork.com/2012/mitigate-vlan-hopping

*Redfox Security*. (2022, June 2). Retrieved from https://redfoxsecurity.medium.com/vlan-hopping-attack-33a8b109c068

Shais. (2020, July 29). Retrieved from https://www.technig.com/prevent-mac-flooding-attack/

Soulages, P. D. (2023, January 14). Retrieved from https://formip.com/en/portfast-and-bpdu-guard-spanning-tree-loop/

*techopedia*. (2022, March 31). Retrieved from https://www.techopedia.com/definition/5107/wireless-local-area-network-wlan