ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Switching and Routing Essentials (SRE)

Individual Assignment

Section A

Module Code: CT133-3-2-SRE

Name: Teo Kai Yii - TP058618

Intake code: APD2F2209CS(CYB)

Hand Out Date: 30th September 2022

Hand In Date: 4th December 2022

Lecturer:

SIR JOSHUA SAMUAL

Table of Contents

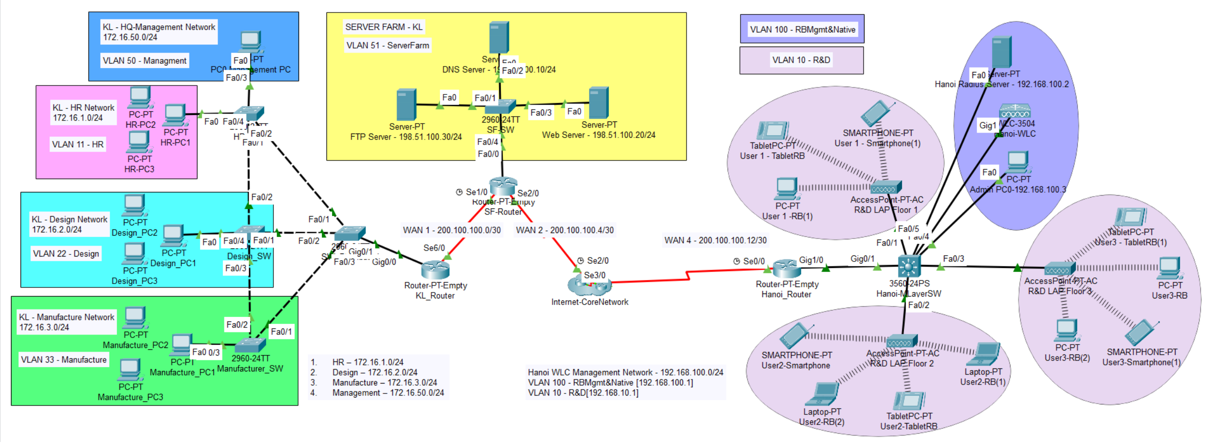
1.0 Introduction

There are plans to enhance the IT services provided by High Dot Tech, a networking company, at its present locations in KL (HQ) and Hanoi (Remote Branch). The network administrator in Hanoi has planned to replace the current configuration with a new VLAN design in order to increase the network's effectiveness and security, notably for the HQ branch in KL. Additionally, the KL Server Farm will be remotely managed by the Management department at HQ. The Hanoi network administrator intends to use WLC WLAN to make wireless network setup and access simpler. The High Dot Tech organization's departments are located in many places. KL Site has departments of Management, Human Resource, Design and Manufacture. Furthermore, Hanoi site has R&D department and WLC Management department. The location of KL Server Farm has a department of Server Farm.

As a newly appointed network executive, I have been given the responsibility of working on the design and prototype of the new network for High Dot Tech company. I've built up the logical architecture provided and configured each device using Cisco Packet Tracer as the simulator to test the design.

The password required in the packet tracer will be “cisco” for all the passwords. This is for the prototype purpose where password can be typed quickly. When goes into the real scenario, High Dot Tech company may choose a strong password.

2.0 Proposed WLAN Architecture



1. HR – 172.16.1.0/24
2. Design – 172.16.2.0/24
3. Manufacture – 172.16.3.0/24
4. Management – 172.16.50.0/24

Hanoi WLC Management Network - 192.168.100.0/24
VLAN 100 - RBMgmt&Native [192.168.100.1]
VLAN 10 - R&D[192.168.10.1]

Figure 1 Logical Topology of High Dot Tech network

2.1 WLAN Components

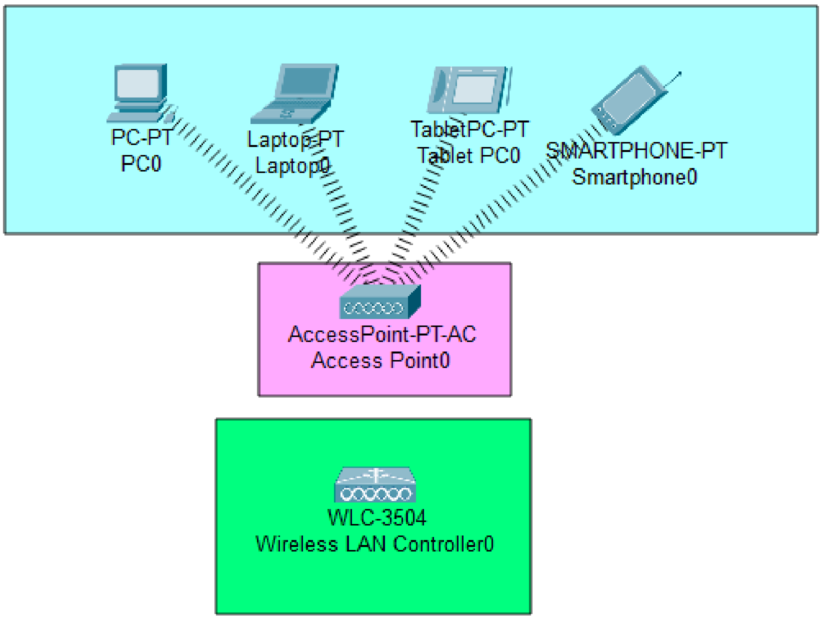


Figure 2 WLAN Components

The WLAN Architecture of High Dot Tech network contains of WLAN components which are the end devices (laptops, tablets, smartphones, PC) with wireless Network Interface Card (NICs) and network devices (Access Points) as shown above. There are three access points used in the High Dot Tech network (Cisco, n.d.).

The Access Points (APs) in High Dot Tech network provide wireless connection when the wireless clients (end devices) look for nearby APs offering their SSID using their wireless NIC. After authenticating with the AP, the end devices may connect to the wireless network. As shown in the Figure 1 Logical Topology of High Dot Tech network, the APs in High Dot Tech network are autonomous APs which are standalone devices that may be set by a GUI. Since High Dot Tech network only requires three APs in the company, autonomous APS will be helpful (Cisco, n.d.).

As the High Dot Tech network expand continuously, the wireless demand increased and more APs would be needed. Each AP would need manual configurations, administration and would function independently of other APs. If more APs were required for High Dot Tech network, this would become overwhelming. To solve this, a WLAN controller (WLC) is prepared. When the number of APs in High Dot Tech network increase to a number that are unable to configure one by one, all APs needs to be replaced with lightweight APs (LAPs) which are controller-based APs. LAPs can communicate with WLC, and each AP is configured automatically and controlled by WLC (Cisco, n.d.).

2.2 Infrastructure WLAN

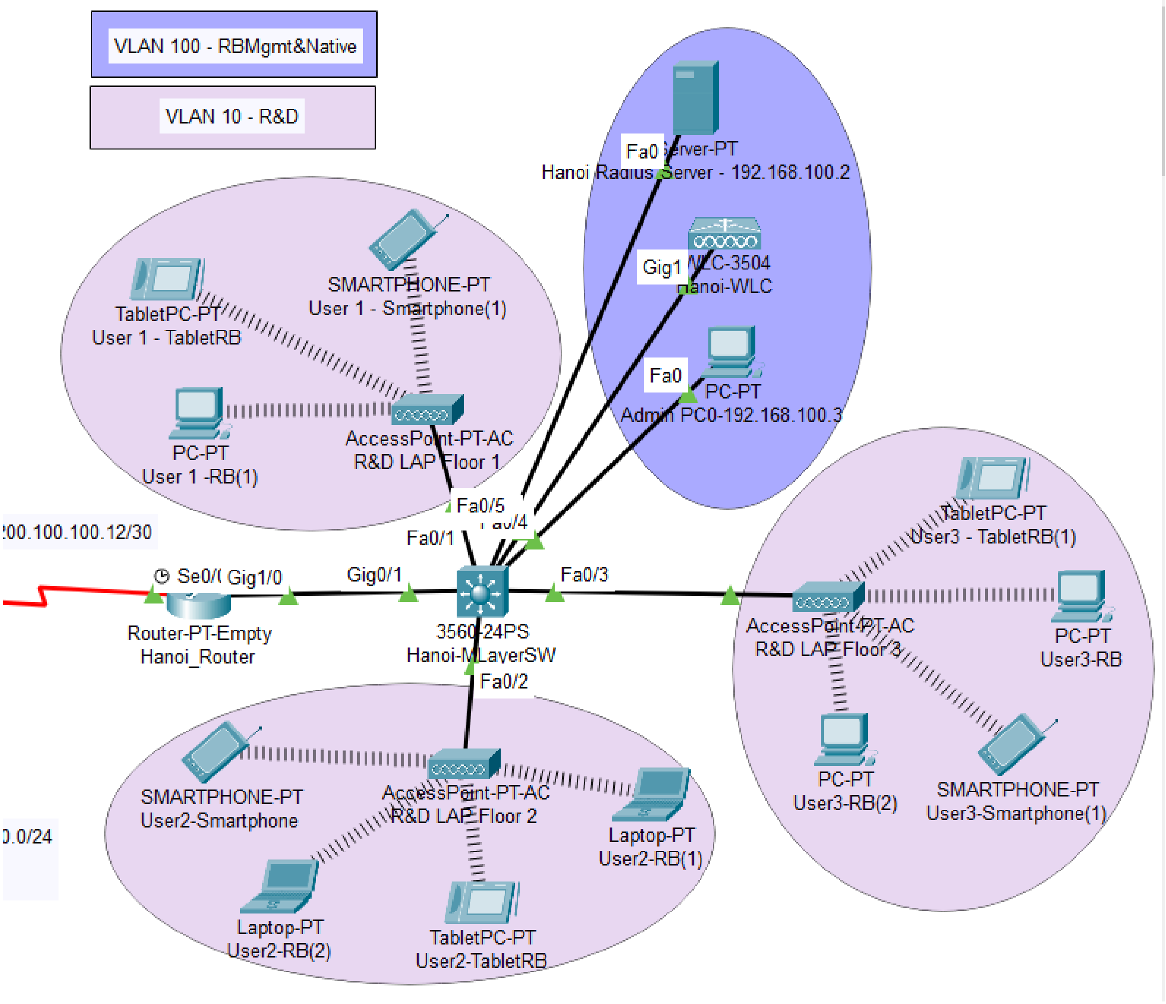


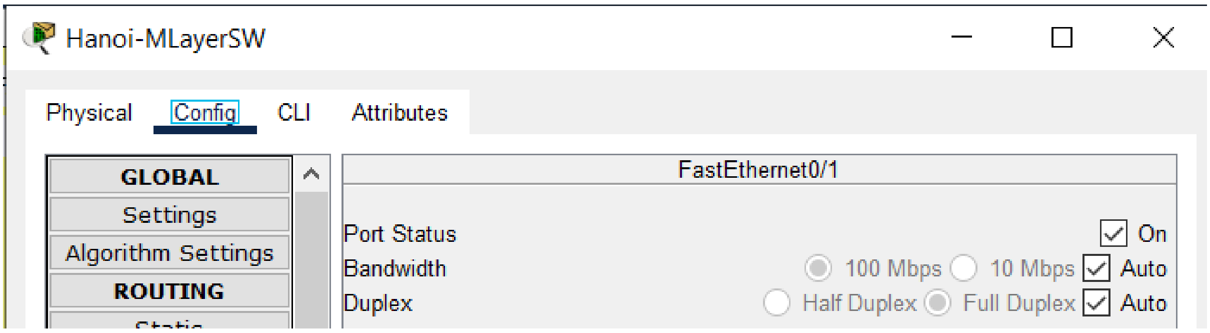
Figure 3 Infrastructure WLAN Architecture

The wireless clients such as Laptop, Smartphone, Tablets and PC connect to the APs. The wired distribution system, Ethernet, is used by the APs to connect with Hanoi-MLayerSW switch, the network infrastructure (Cisco, n.d.).

Each pink circle in the Figure 2 Infrastructure WLAN Architecture contains a Basic Service Area (BSS). The Basic Service Area, or BSS, coverage area is shown by the pick circle (BSA). A wireless client can no longer directly connect with other wireless clients within the BSA if it leaves the BSA. The Basic Service Set Identifier, also known as the Layer 2 MAC address of the AP, is used to specifically identify each BSS (BSSID). Therefore, the BSSID is the BSS's official name and it is always connected to only one AP. High Dot Tech network Infrastructure WLAN has Extended Service Set (ESS) which three BSSs is connected to the Hanoi-MLayerSW switch. Each ESS has a unique SSID, and each BSS has a unique BSSID (Cisco, n.d.).

2.3 Implement WLC WLAN

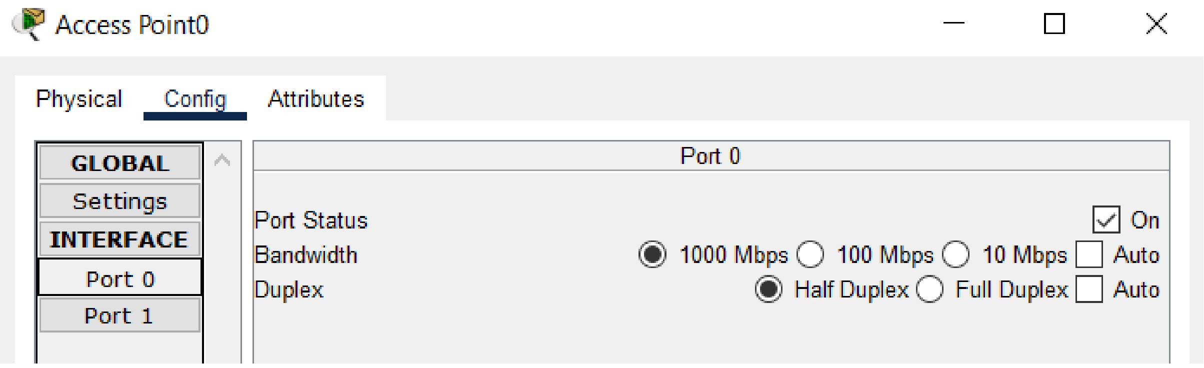
2.3.1 Configure Access Points Ports



FastEthernet0/1

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto

Figure 4 Hanoi-MLayerSW Switch Port

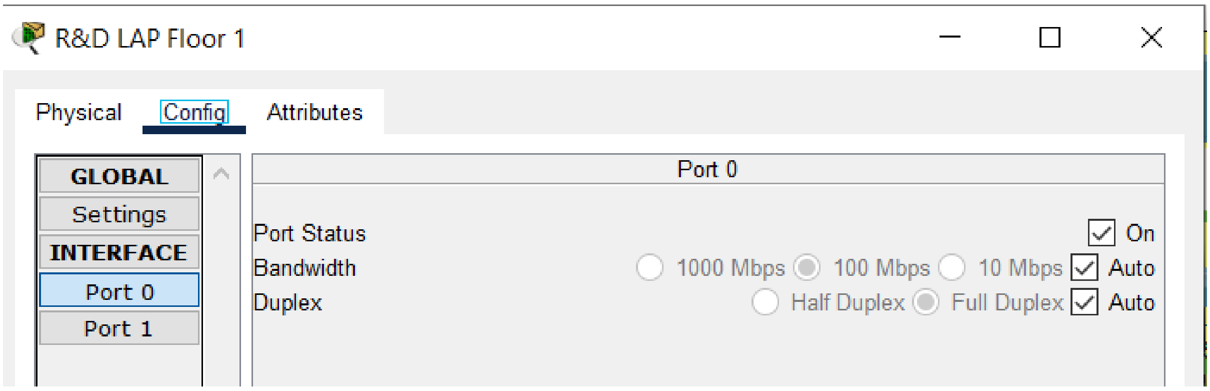


Port 0

Port Status ☑ On
Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps □ Auto
Duplex ● Half Duplex ○ Full Duplex □ Auto

Figure 5 Access Point Port 0

Connectivity problems can be caused by mismatch between the duplex mode and speed settings of access points port and switch port. As shown in Figure 1 Logical Topology of High Dot Tech network and Figure 2 WLAN Components, the auto negotiation fails because of mismatched bandwidth and duplex mode. This problem could be solved using an interface's auto medium-dependent interface crossover (auto-MDIX) capability. When auto-MDIX is activated, the interface of the device will automatically determine whether a crossover cable connection or a straight-through cable connection is needed and at the same time, configures the connection accordingly. The auto-MDIX function is enabled in Hanoi-MLayerSW switch in default. However, the auto-MDIX function is not enabled by default in the access points (Cisco, n.d.).


R&D LAP Floor 1

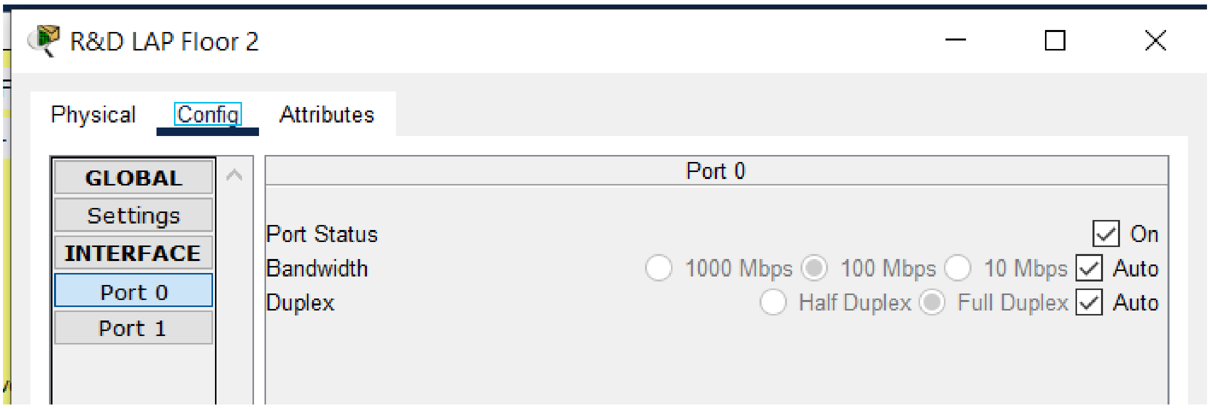
Physical | Config | Attributes

GLOBAL
Settings
INTERFACE
Port 0
Port 1

Port 0

Port Status ☑ On
Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto

Figure 6 R&D LAP Floor 1 Port 0


R&D LAP Floor 2

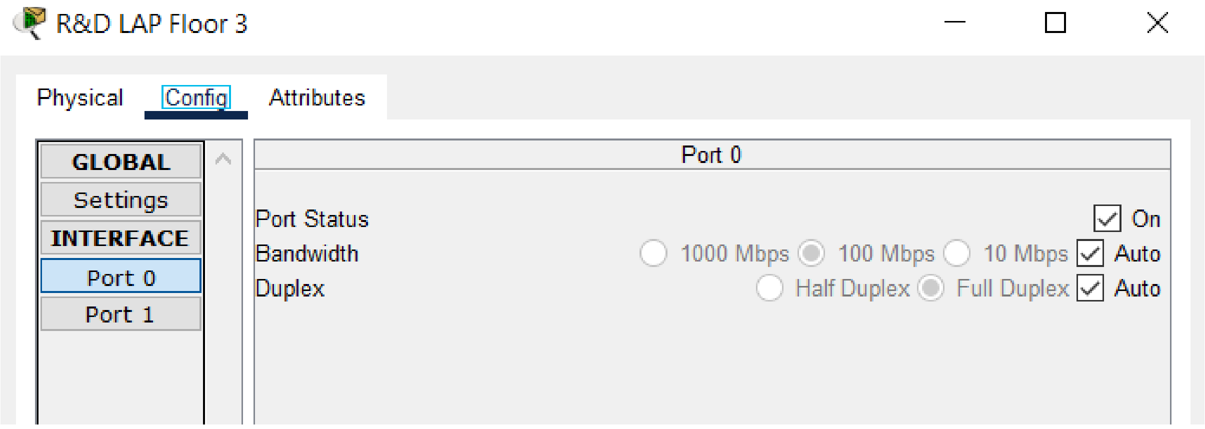
Physical | Config | Attributes

GLOBAL
Settings
INTERFACE
Port 0
Port 1

Port 0

Port Status ☑ On
Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto

Figure 7 R&D LAP Floor 2 Port 0


R&D LAP Floor 3

Physical | Config | Attributes

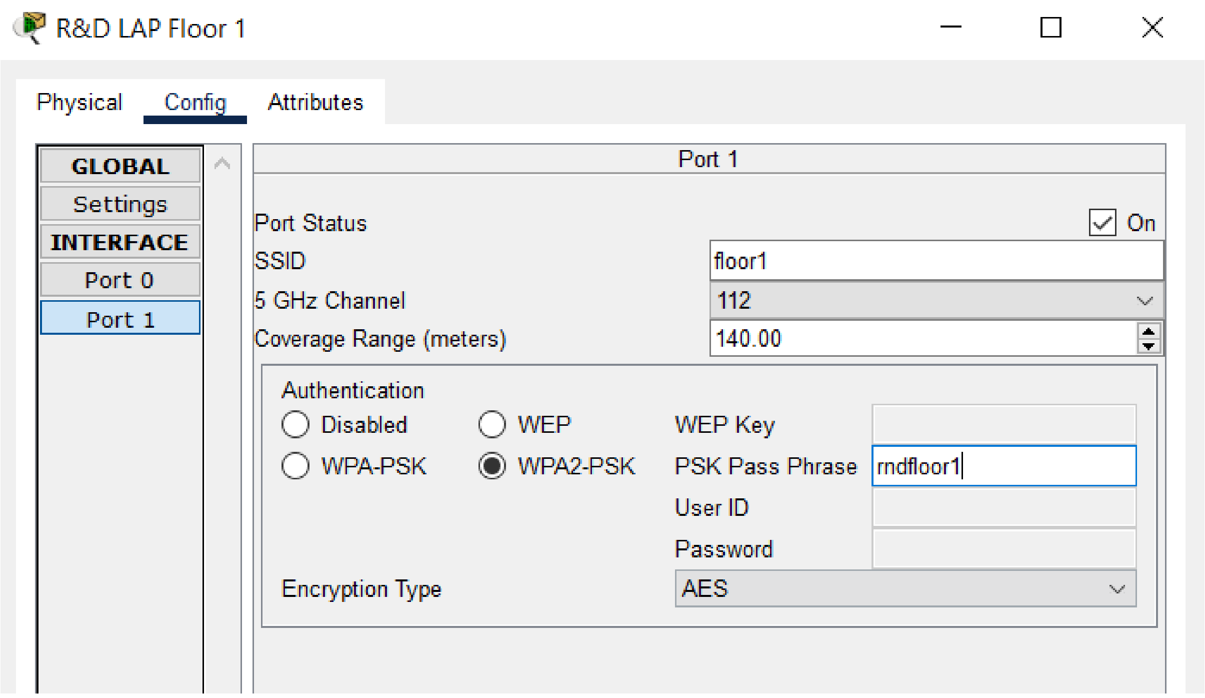
GLOBAL
Settings
INTERFACE
Port 0
Port 1

Port 0

Port Status ☑ On
Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto

Figure 8 R&D LAP Floor 3 Port 0

The interface speed (bandwidth) and the duplex of the access points in High Dot Tech network must be set to auto while utilizing auto-MDIX for the function to work properly. Both access points and the switch will have speed of 100Mbps and Full Duplex mode. Full Duplex mode will enhance the speed by allowing send and receive at the same time (Cisco, n.d.).



Port 1

Port Status ☑ On

SSID: floor1

5 GHz Channel: 112

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

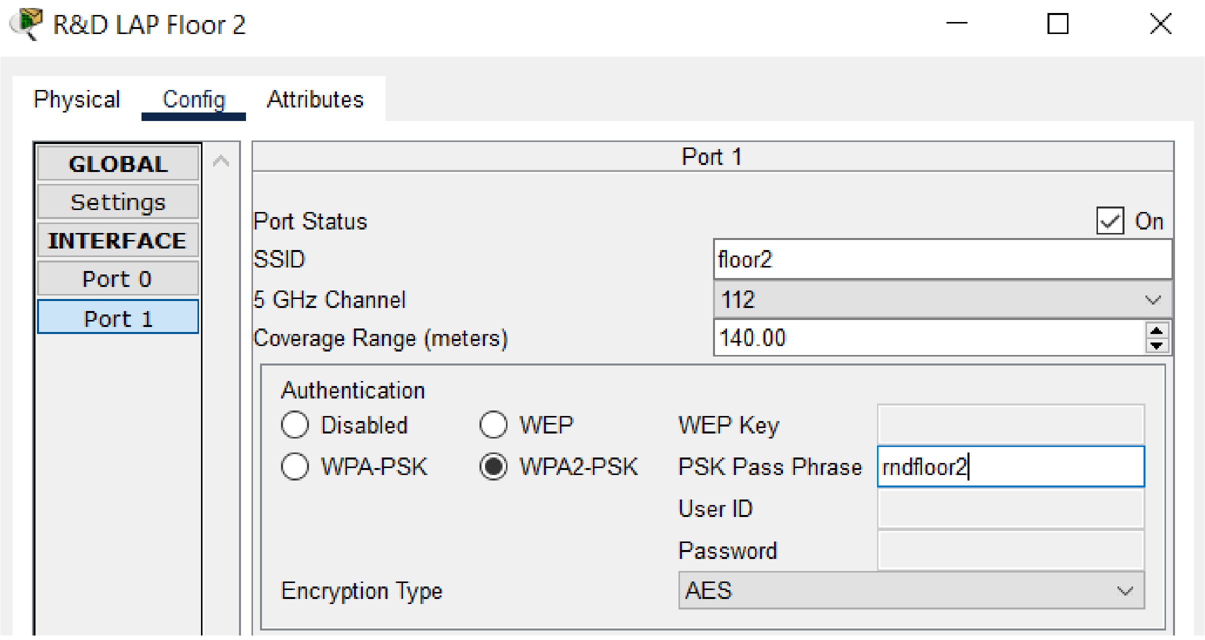
PSK Pass Phrase: rndfloor1

User ID:

Password:

Encryption Type: AES

Figure 9 R&D LAP Floor 1 Port 1



Port 1

Port Status ☑ On

SSID: floor2

5 GHz Channel: 112

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

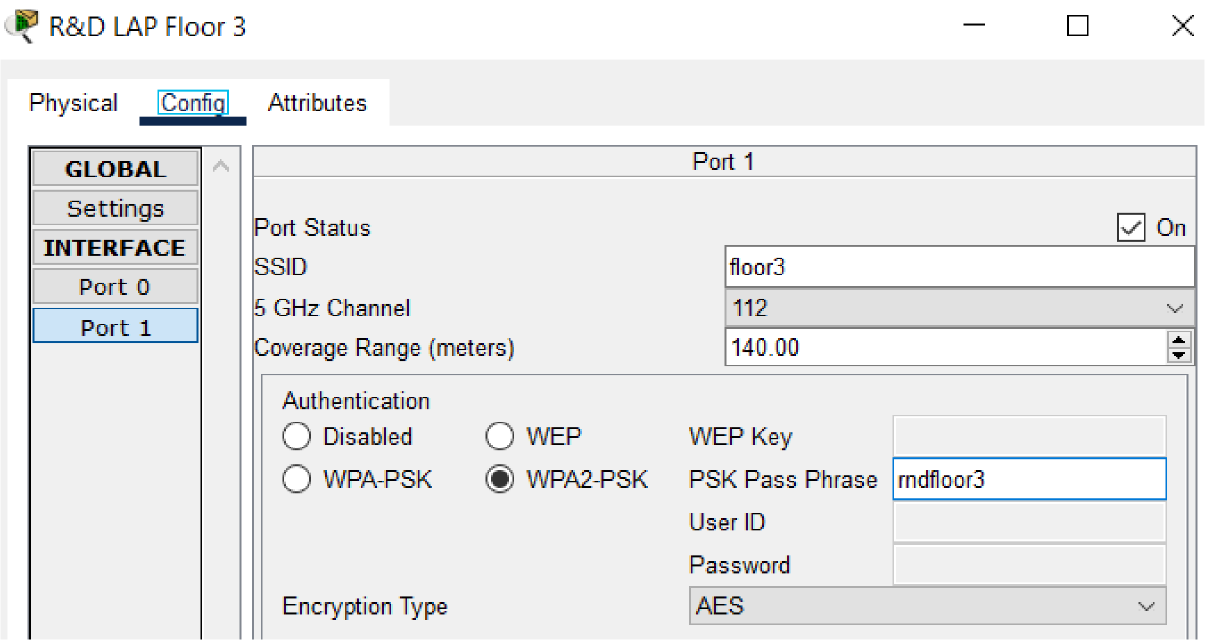
PSK Pass Phrase: rndfloor2

User ID:

Password:

Encryption Type: AES

Figure 10 R&D LAP Floor 2 Port 1



R&D LAP Floor 3

Port 1

Port Status ☑ On

SSID: floor3

5 GHz Channel: 112

Coverage Range (meters): 140.00

Authentication: ○ Disabled ○ WEP ○ WPA-PSK ● WPA2-PSK

WEP Key:

PSK Pass Phrase: rndfloor3

User ID:

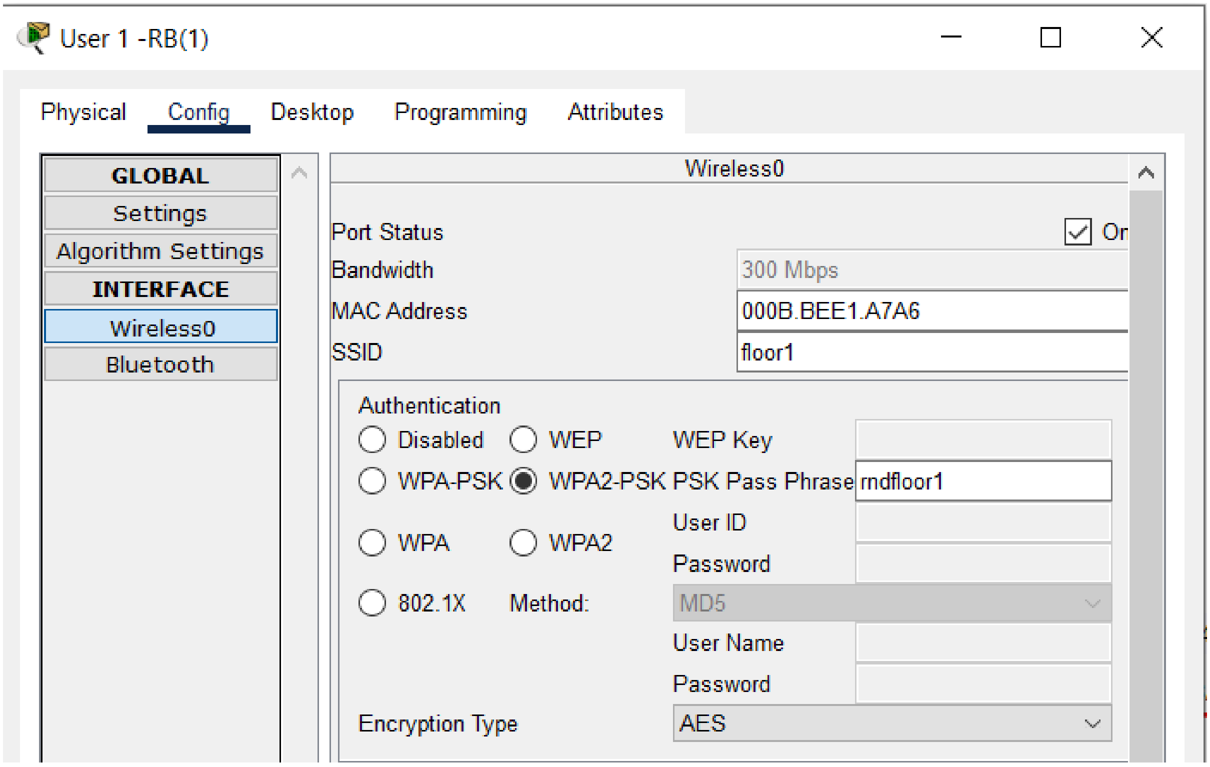
Password:

Encryption Type: AES

Figure 11 R&D LAP Floor 3 Port 1

The SSID name of the APs are changed and the authentication of WPA2-PSK is enabled with the passphrase encrypted by AES type. SSID and WPA2-PSK authentication will help the wireless clients to connect to the respective AP with the accurate SSID and pass phrase.

R&D LAP Floor 1 End Devices



User 1 -RB(1)

Wireless0

Port Status ☑ On

Bandwidth: 300 Mbps

MAC Address: 000B.BEE1.A7A6

SSID: floor1

Authentication: ○ Disabled ○ WEP ○ WPA-PSK ● WPA2-PSK ○ WPA ○ WPA2 ○ 802.1X

WEP Key:

PSK Pass Phrase: rndfloor1

User ID:

Password:

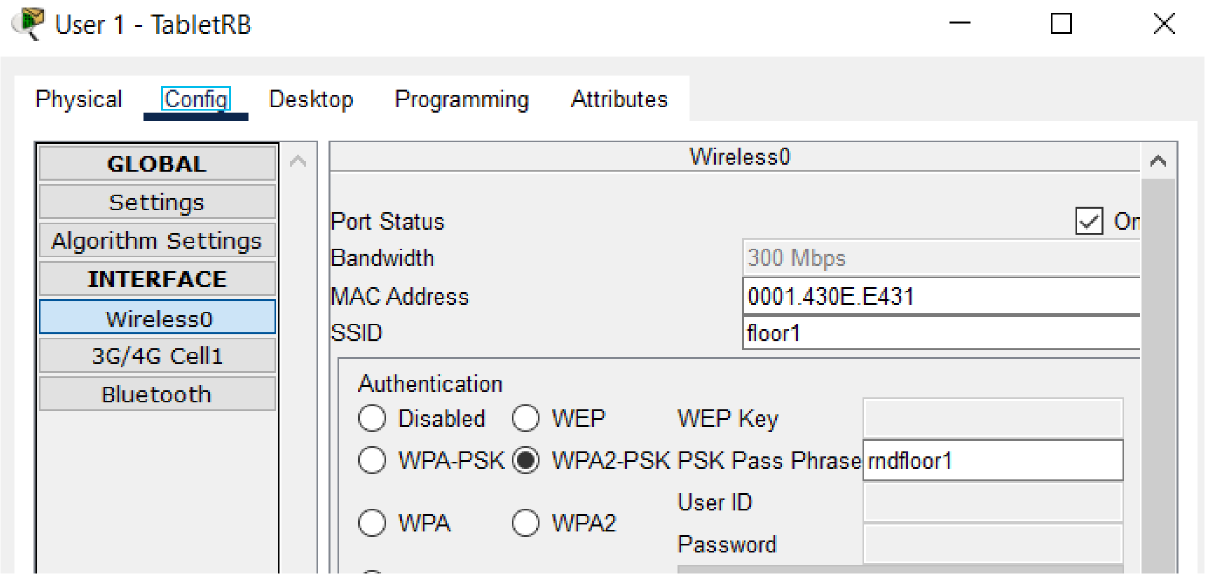
Method: MD5

User Name:

Password:

Encryption Type: AES

Figure 12 User 1 – RB(1)



User 1 - TabletRB

Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0001.430E.E431

SSID floor1

Authentication

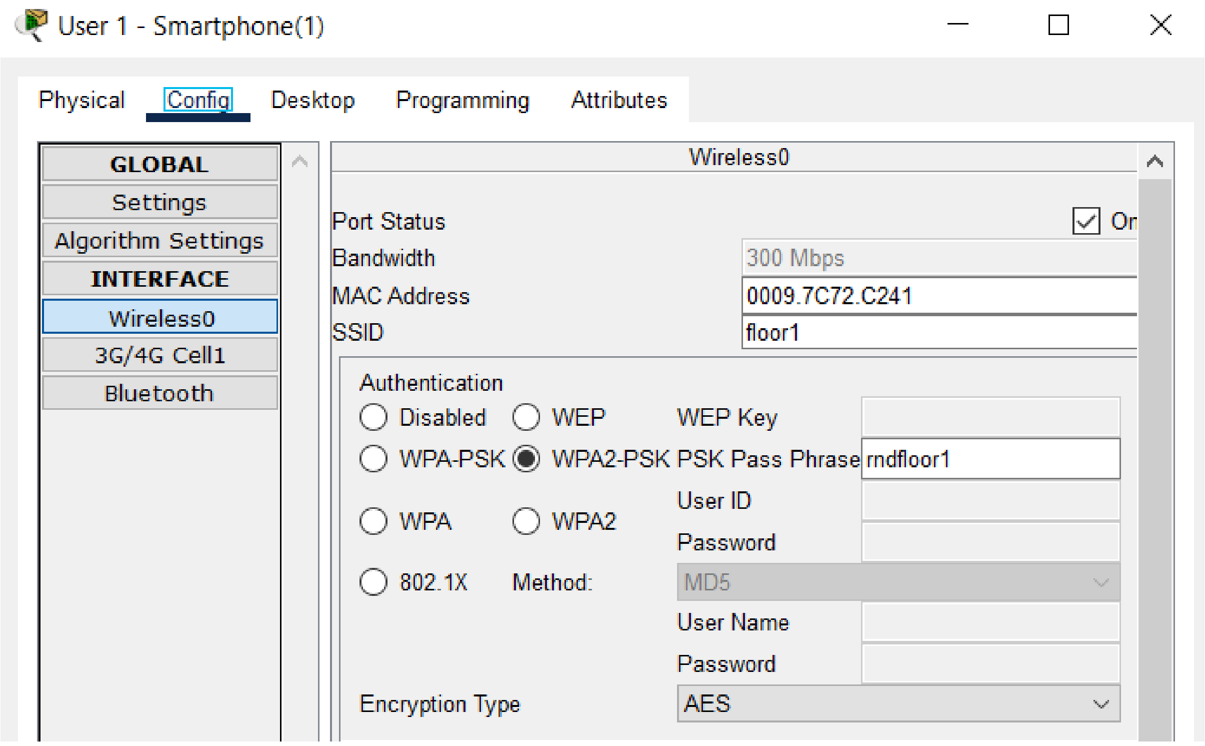
○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor1

○ WPA ○ WPA2 User ID

Password

Figure 13 User 1 – TabletRB



User 1 - Smartphone(1)

Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0009.7C72.C241

SSID floor1

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor1

○ WPA ○ WPA2 User ID

Password

○ 802.1X Method: MD5

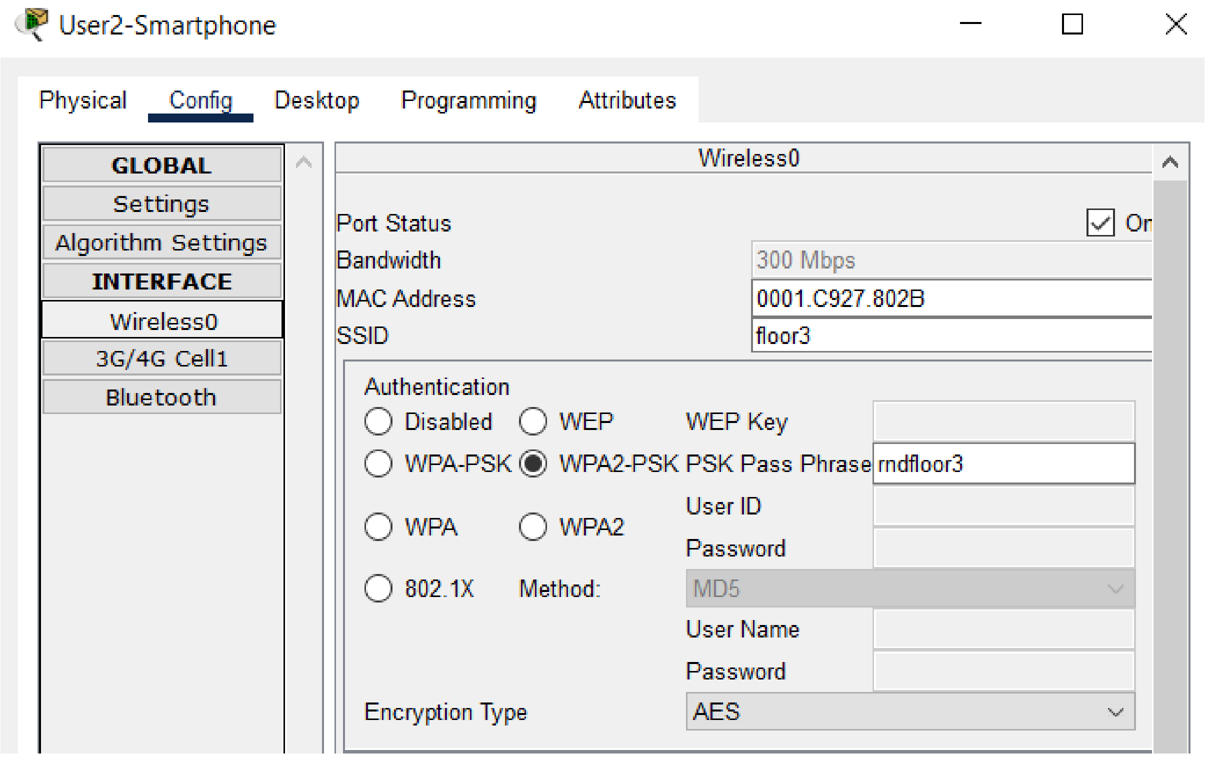
User Name

Password

Encryption Type AES

Figure 14 User 1 – Smartphone(1)

R&D LAP Floor 2 End Devices



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0001.C927.802B

SSID floor3

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor3

○ WPA ○ WPA2 User ID

Password

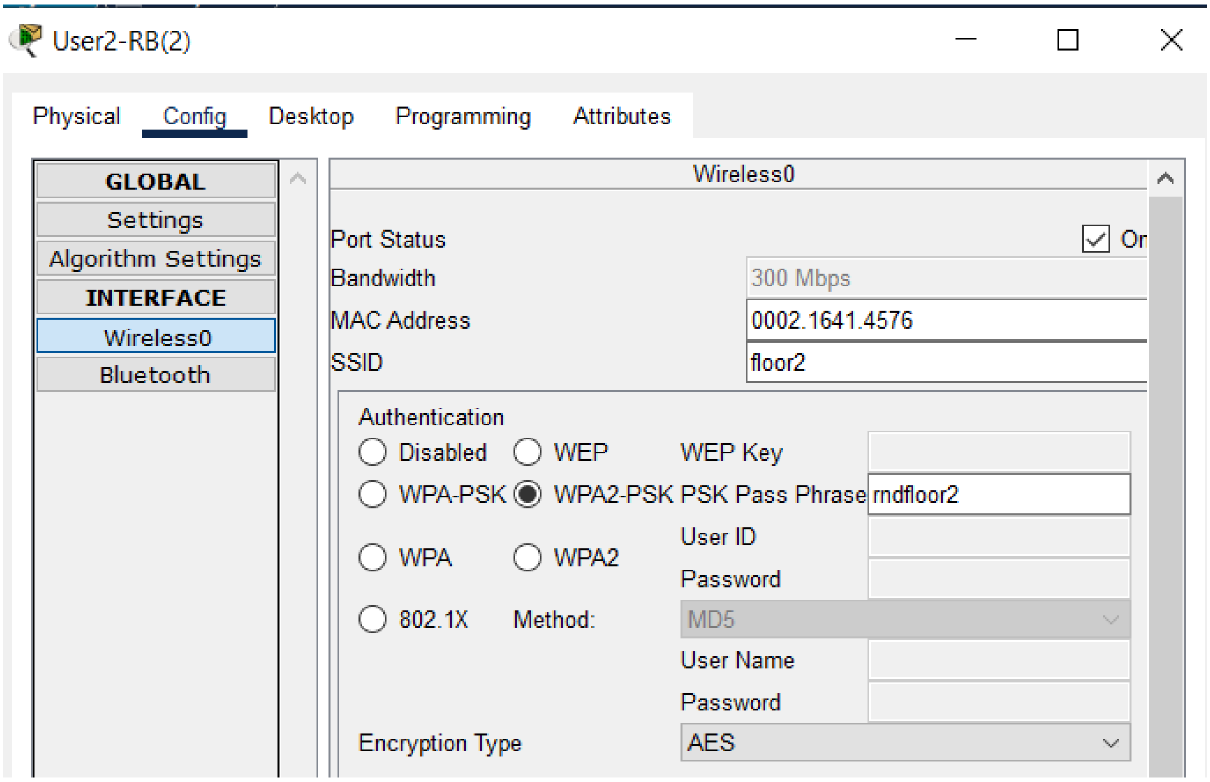
○ 802.1X Method: MD5

User Name

Password

Encryption Type AES

Figure 15 User 2 – Smartphone



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0002.1641.4576

SSID floor2

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor2

○ WPA ○ WPA2 User ID

Password

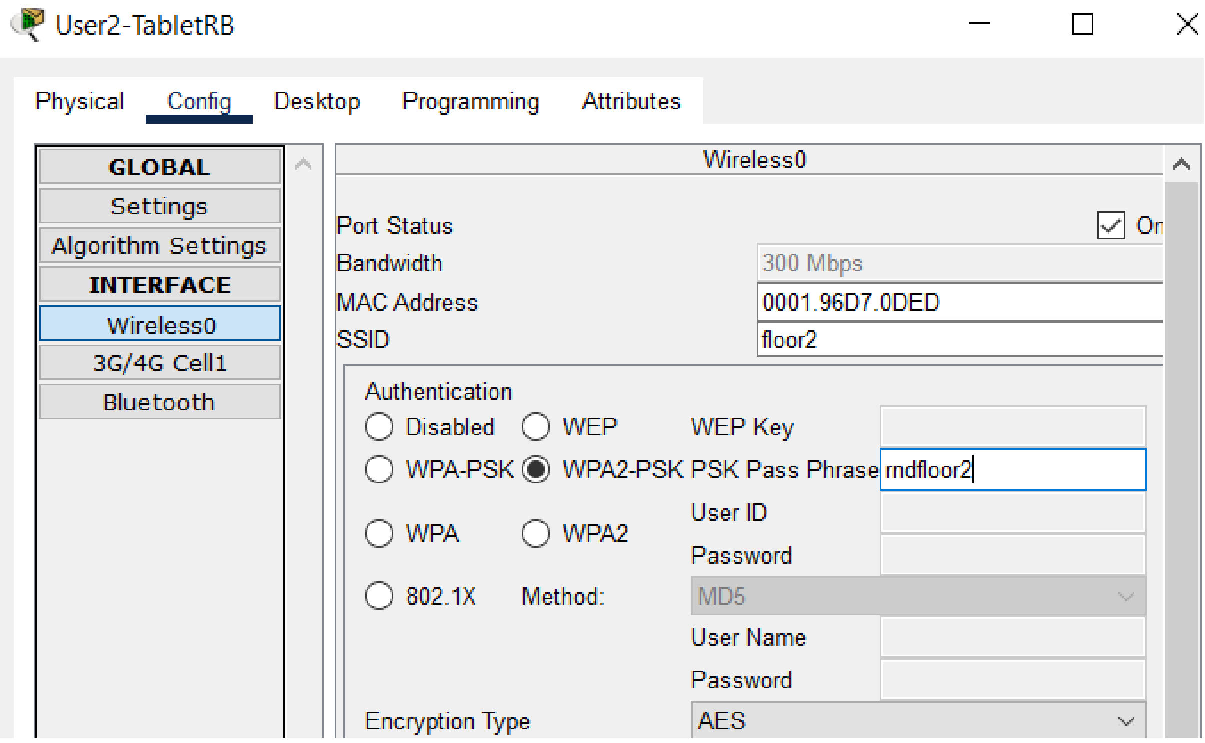
○ 802.1X Method: MD5

User Name

Password

Encryption Type AES

Figure 16 User 2 – RB(2)



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0001.96D7.0DED

SSID floor2

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor2

○ WPA ○ WPA2 User ID / Password

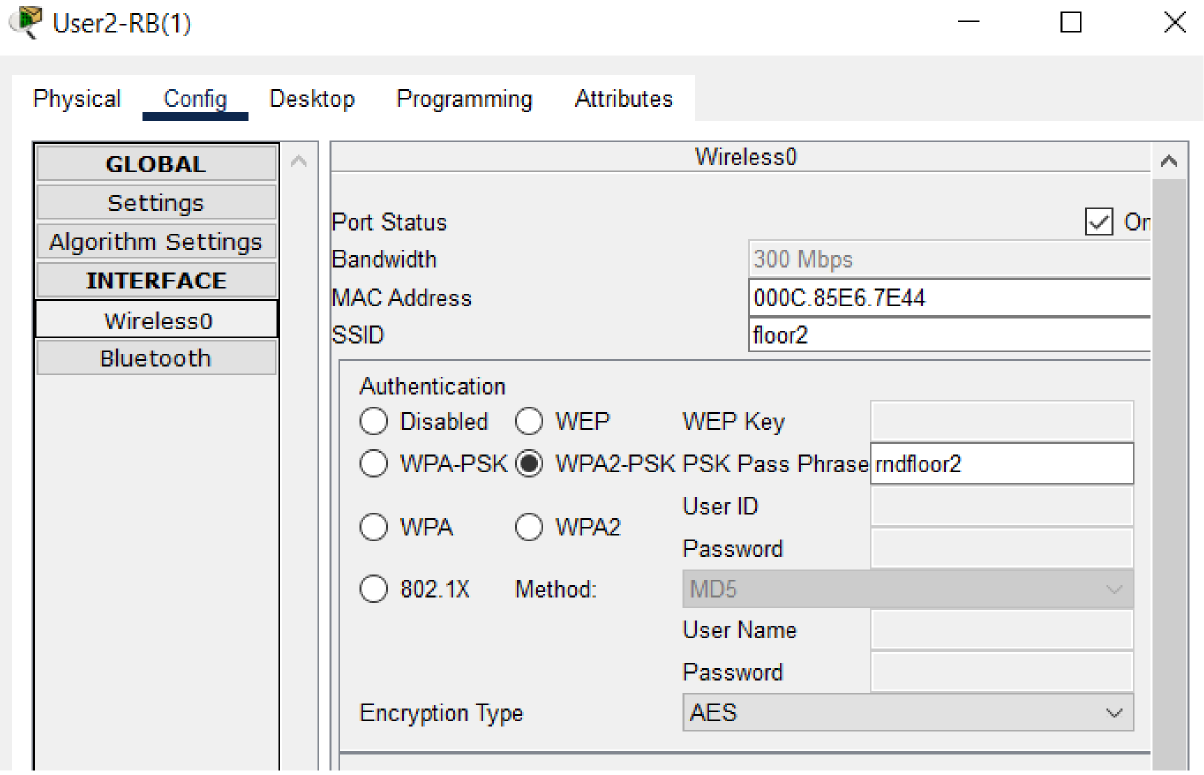
○ 802.1X Method: MD5

User Name

Password

Encryption Type AES

Figure 17 User 2 – TabletRB



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 000C.85E6.7E44

SSID floor2

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor2

○ WPA ○ WPA2 User ID / Password

○ 802.1X Method: MD5

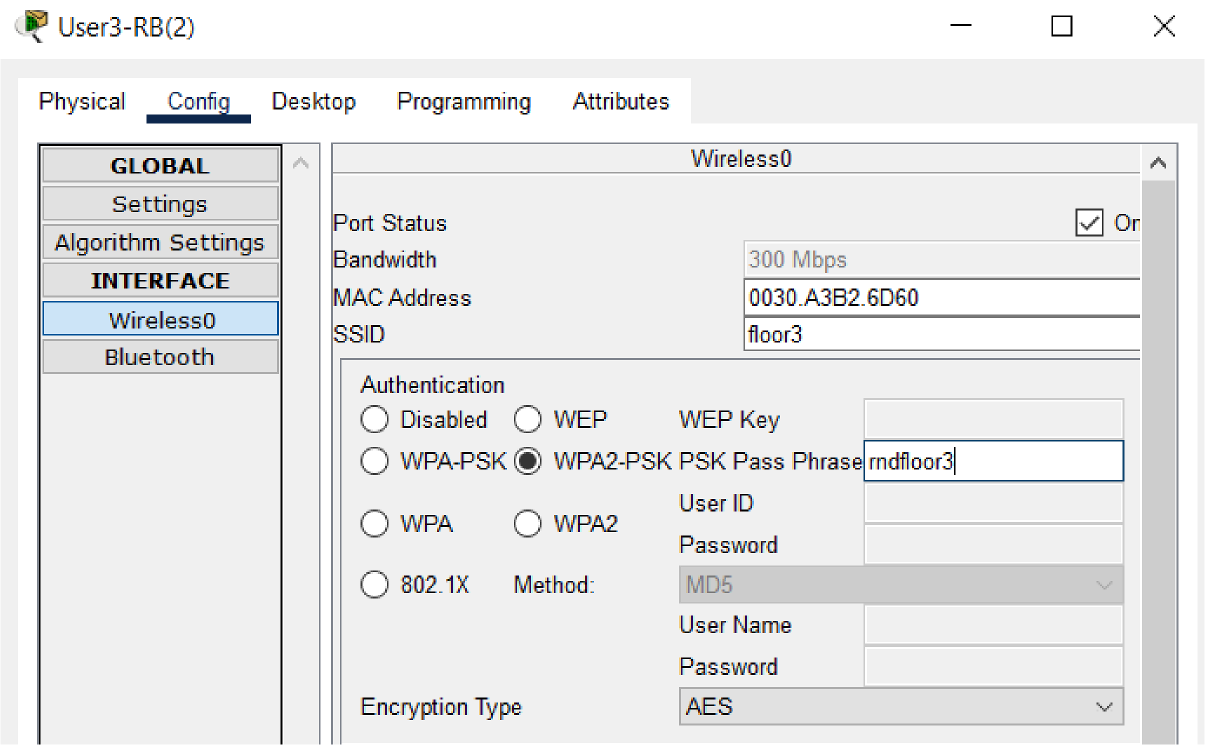
User Name

Password

Encryption Type AES

Figure 18 User 2 – RB(1)

R&D LAP Floor 3 End Devices



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0030.A3B2.6D60

SSID floor3

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor3

○ WPA ○ WPA2 User ID

Password

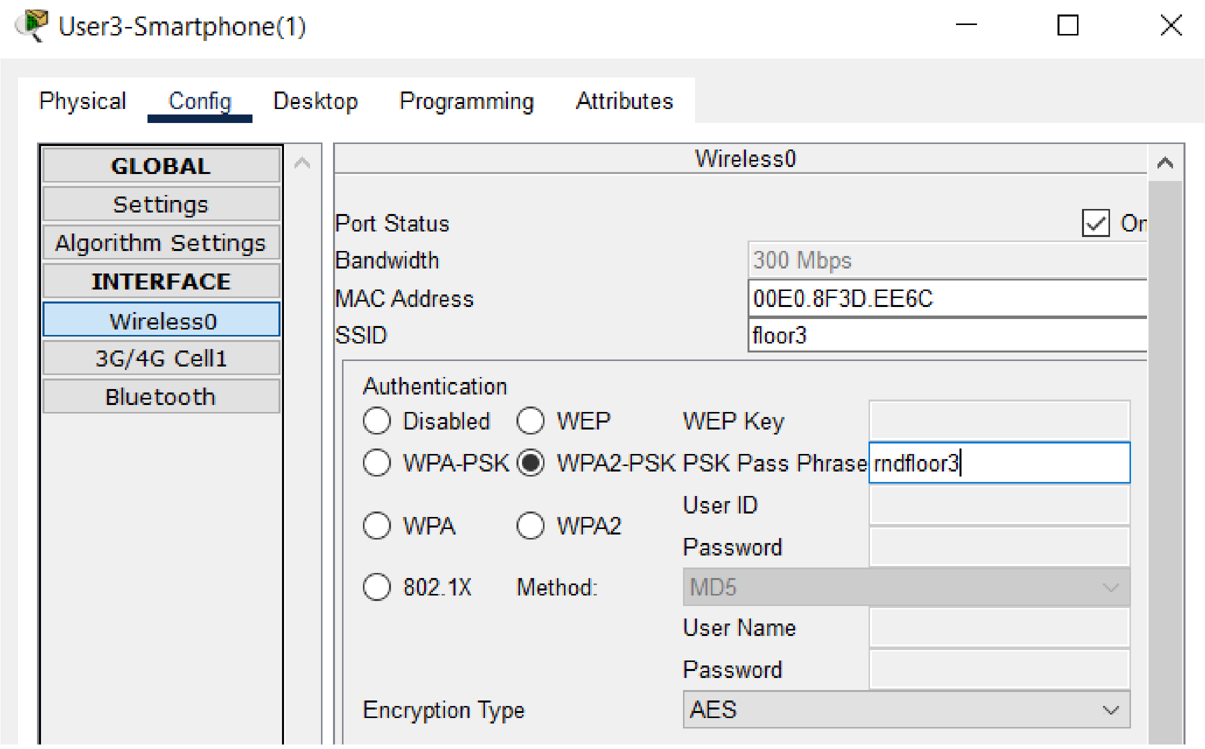
○ 802.1X Method: MD5

User Name

Password

Encryption Type AES

Figure 19 User 3 – RB(2)



Wireless0

Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 00E0.8F3D.EE6C

SSID floor3

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor3

○ WPA ○ WPA2 User ID

Password

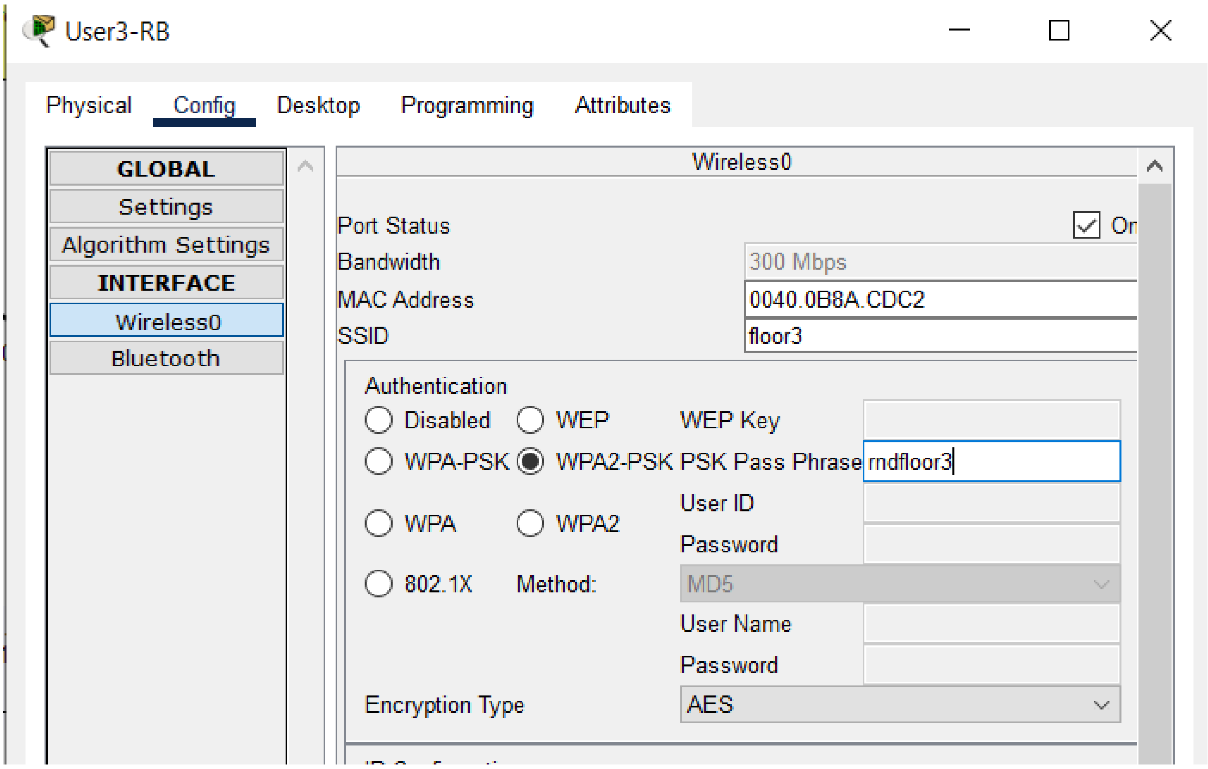
○ 802.1X Method: MD5

User Name

Password

Encryption Type AES

Figure 20 User 3 – Smartphone(1)

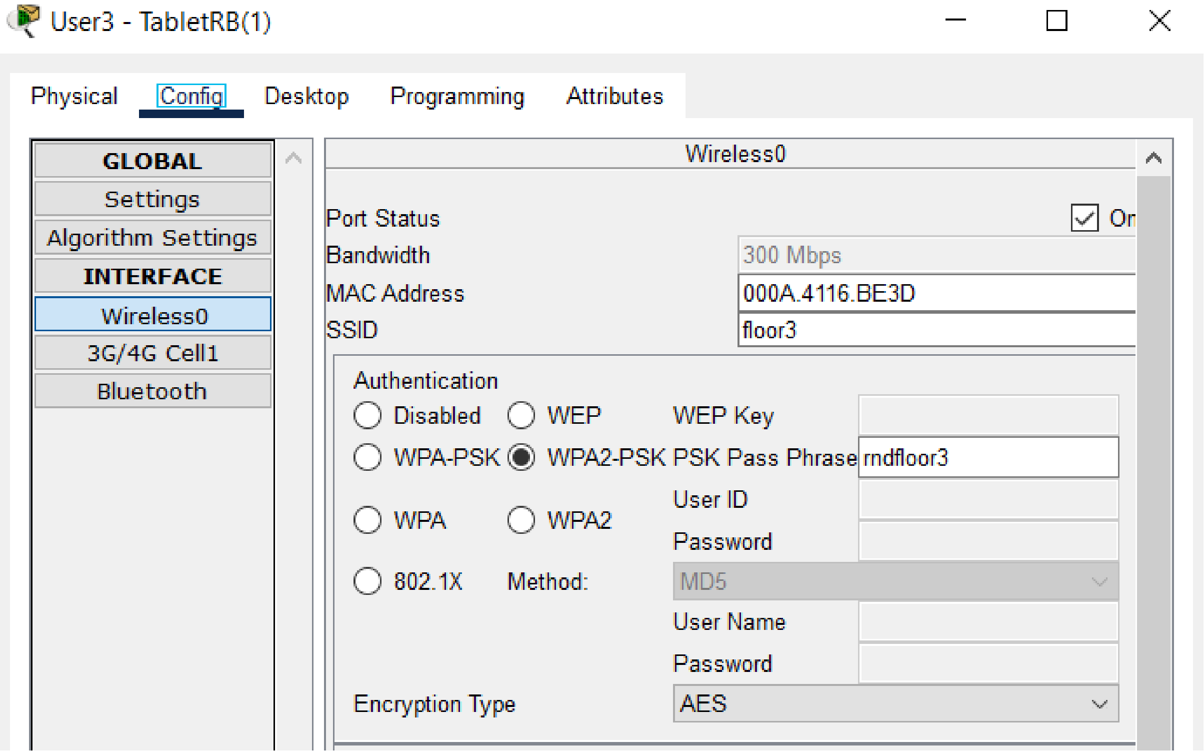


Wireless0

Port Status ☑ On
Bandwidth 300 Mbps
MAC Address 0040.0B8A.CDC2
SSID floor3

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor3
User ID
○ WPA ○ WPA2
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type AES

Figure 21 User 3 – RB



Wireless0

Port Status ☑ On
Bandwidth 300 Mbps
MAC Address 000A.4116.BE3D
SSID floor3

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase rndfloor3
User ID
○ WPA ○ WPA2
Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type AES

Figure 22 User 3 – TabletRB(1)

All the wireless port of the end devices is configured by changing the SSID and giving the pass phrase to the WPA2-PSK authentication and AES encryption type.

2.3.2 Create Account in WLC

The GUI of WLC is accessed with the management PC in HTTP connection and the IP address of the WLC.

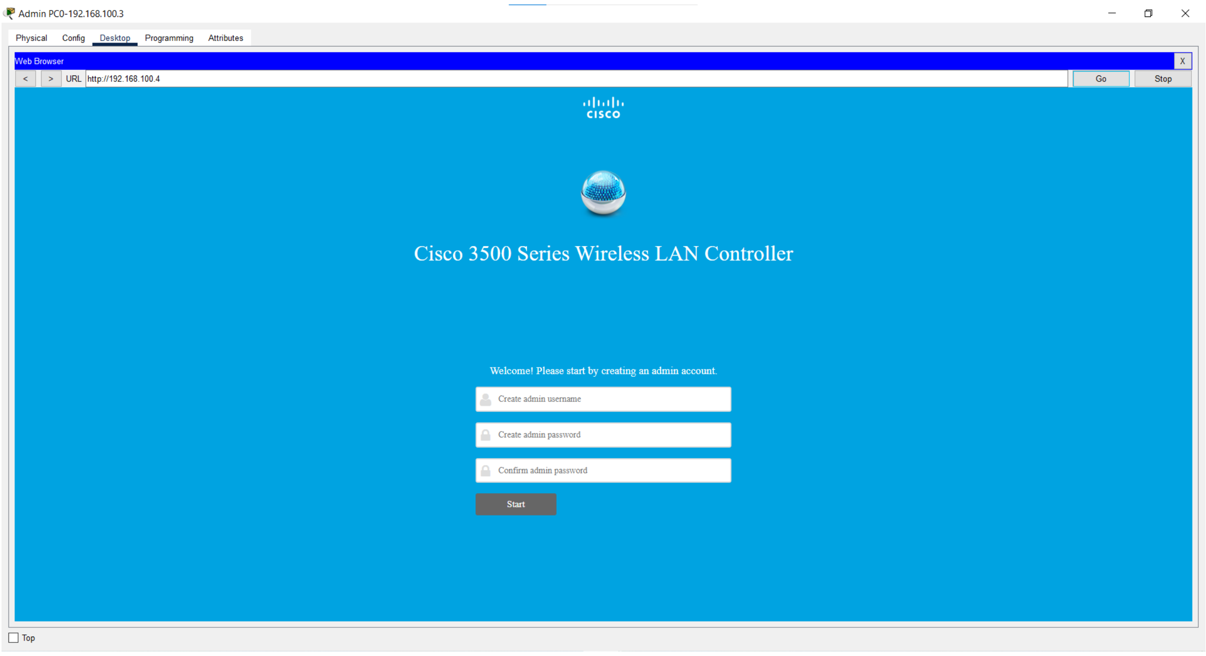
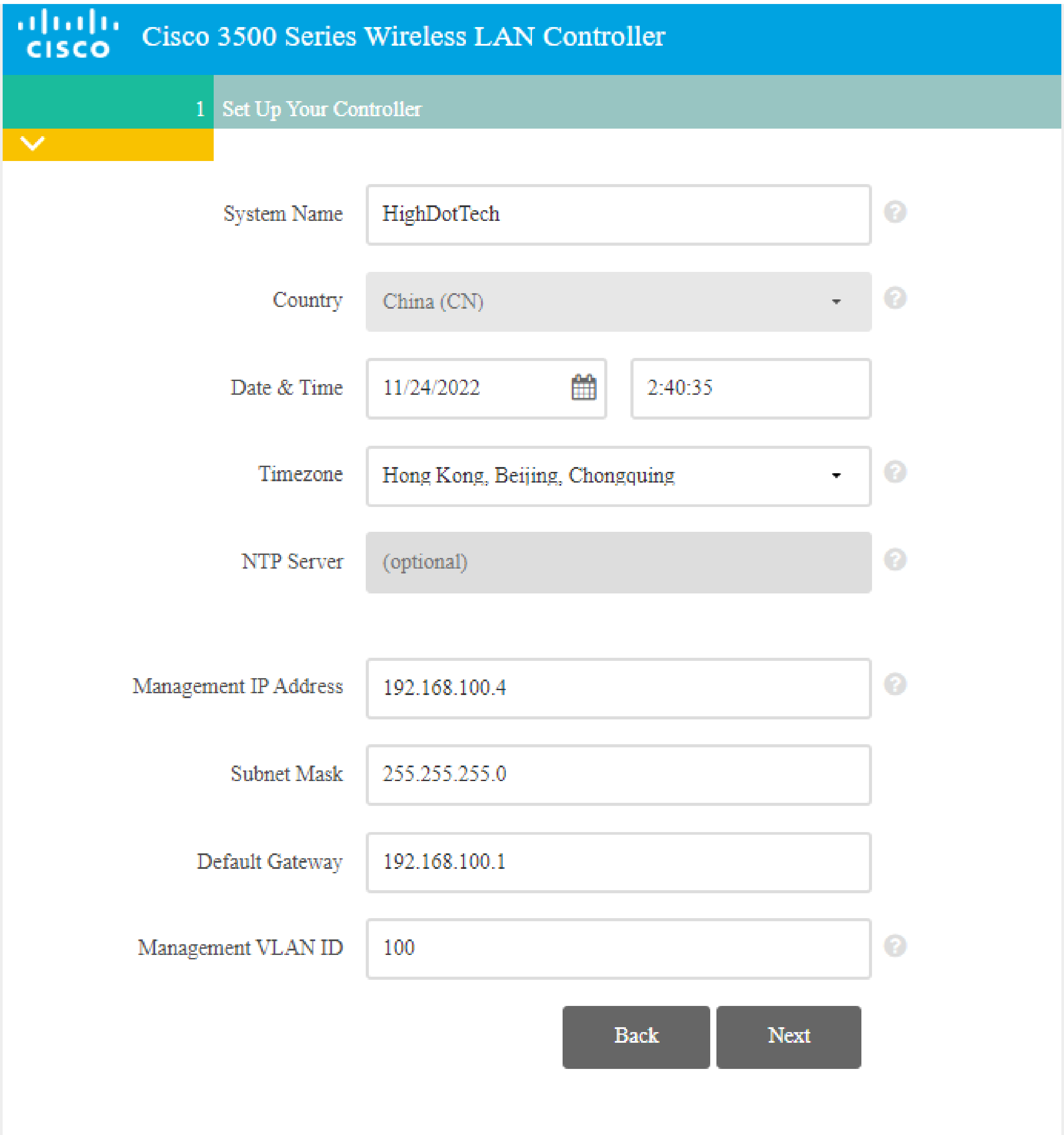


Figure 23 WLC

Username: admin

Password: Tech123

Enter username and password. Click Start.



Cisco 3500 Series Wireless LAN Controller

1 Set Up Your Controller

System Name: HighDotTech

Country: China (CN)

Date & Time: 11/24/2022 2:40:35

Timezone: Hong Kong, Beijing, Chongquing

NTP Server: (optional)

Management IP Address: 192.168.100.4

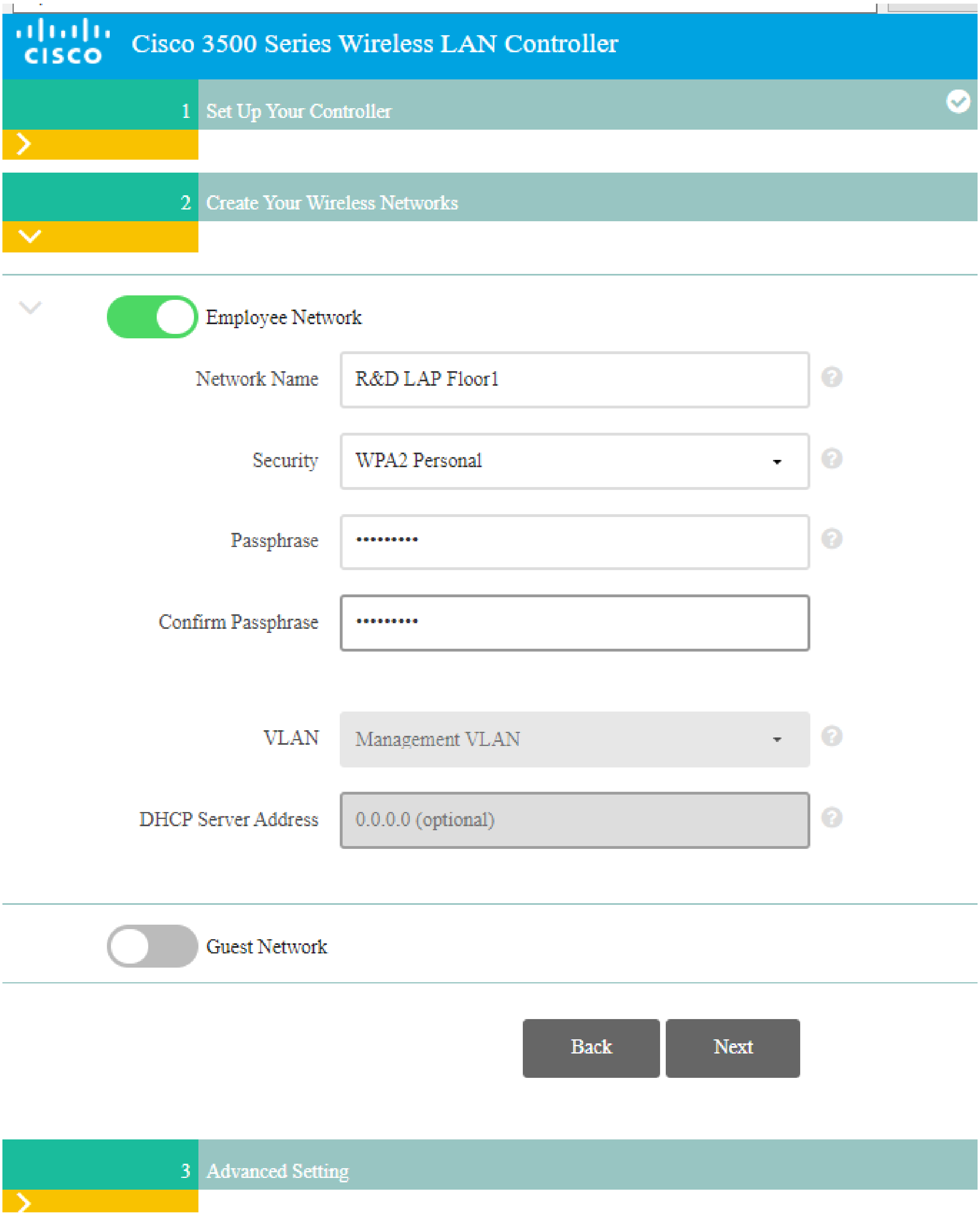
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.100.1

Management VLAN ID: 100

Figure 24 Step 1

All the fields is entered according to the network and click Next.


Cisco 3500 Series Wireless LAN Controller
1 Set Up Your Controller
2 Create Your Wireless Networks

Employee Network

Network Name: R&D LAP Floor1

Security: WPA2 Personal

Passphrase: •••••••••

Confirm Passphrase: •••••••••

VLAN: Management VLAN

DHCP Server Address: 0.0.0.0 (optional)

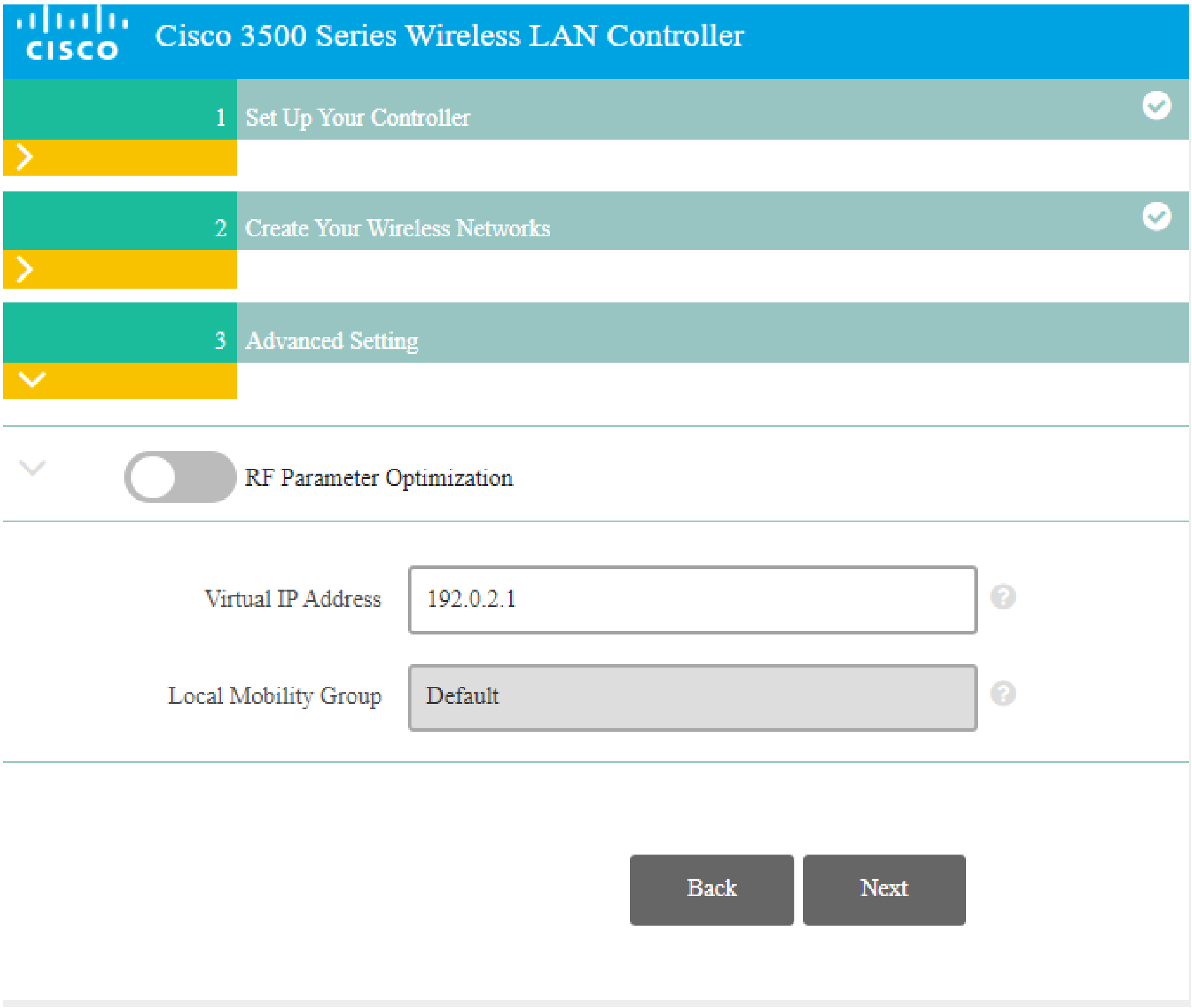
Guest Network

Back
Next
3 Advanced Setting

Figure 25 Step 2

Passphrase: rndfloor1

All the fields is entered and click Next.


Cisco 3500 Series Wireless LAN Controller
1 Set Up Your Controller
2 Create Your Wireless Networks
3 Advanced Setting
Back
Next

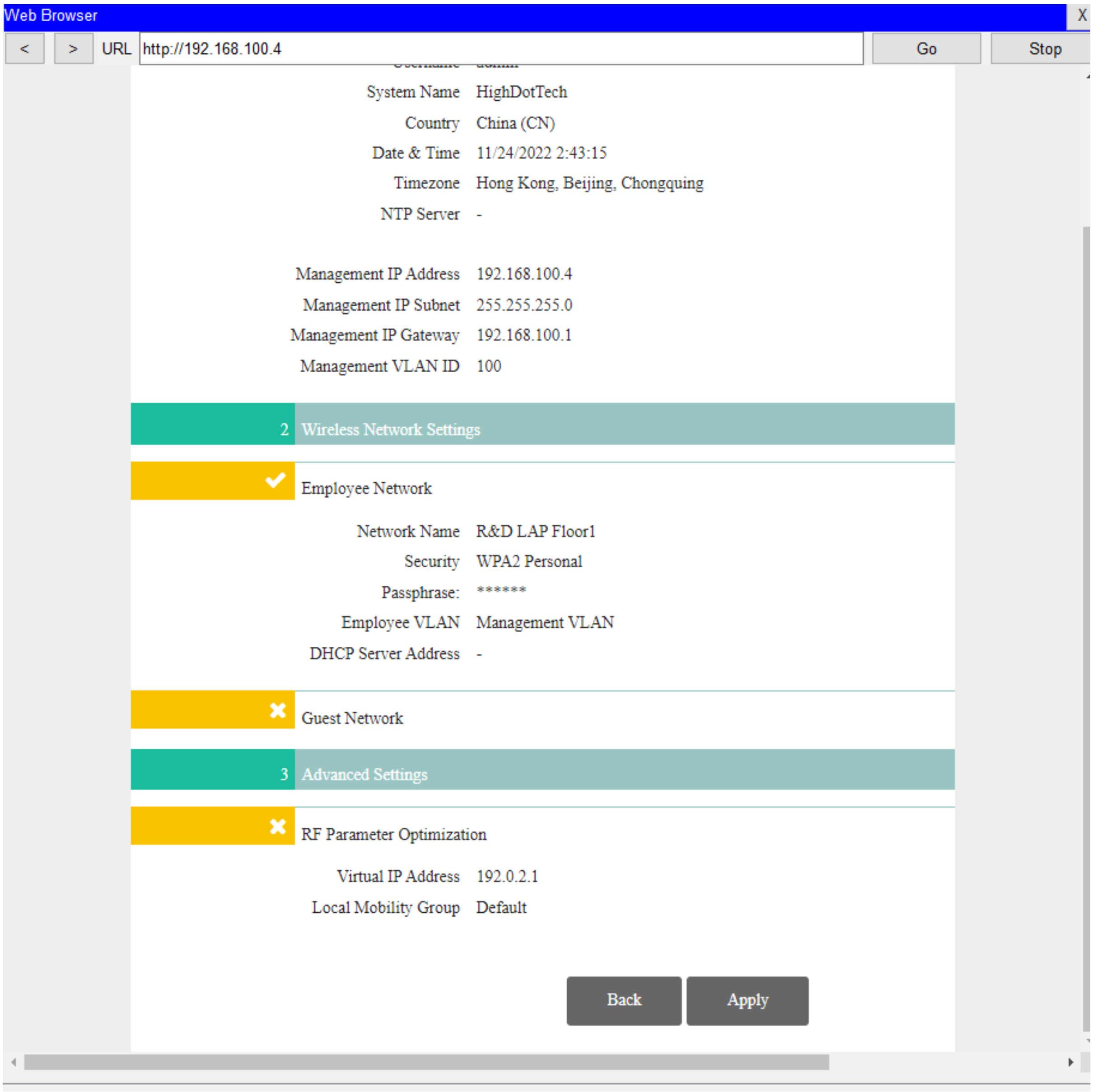
RF Parameter Optimization

Virtual IP Address: 192.0.2.1

Local Mobility Group: Default

Figure 26 Step 3

Leave the Virtual IP Address in default and click Next.



System Name	HighDotTech
Country	China (CN)
Date & Time	11/24/2022 2:43:15
Timezone	Hong Kong, Beijing, Chongquing
NTP Server	-
Management IP Address	192.168.100.4
Management IP Subnet	255.255.255.0
Management IP Gateway	192.168.100.1
Management VLAN ID	100

2 Wireless Network Settings

✓ Employee Network

Network Name	R&D LAP Floor1
Security	WPA2 Personal
Passphrase:	******
Employee VLAN	Management VLAN
DHCP Server Address	-

✗ Guest Network

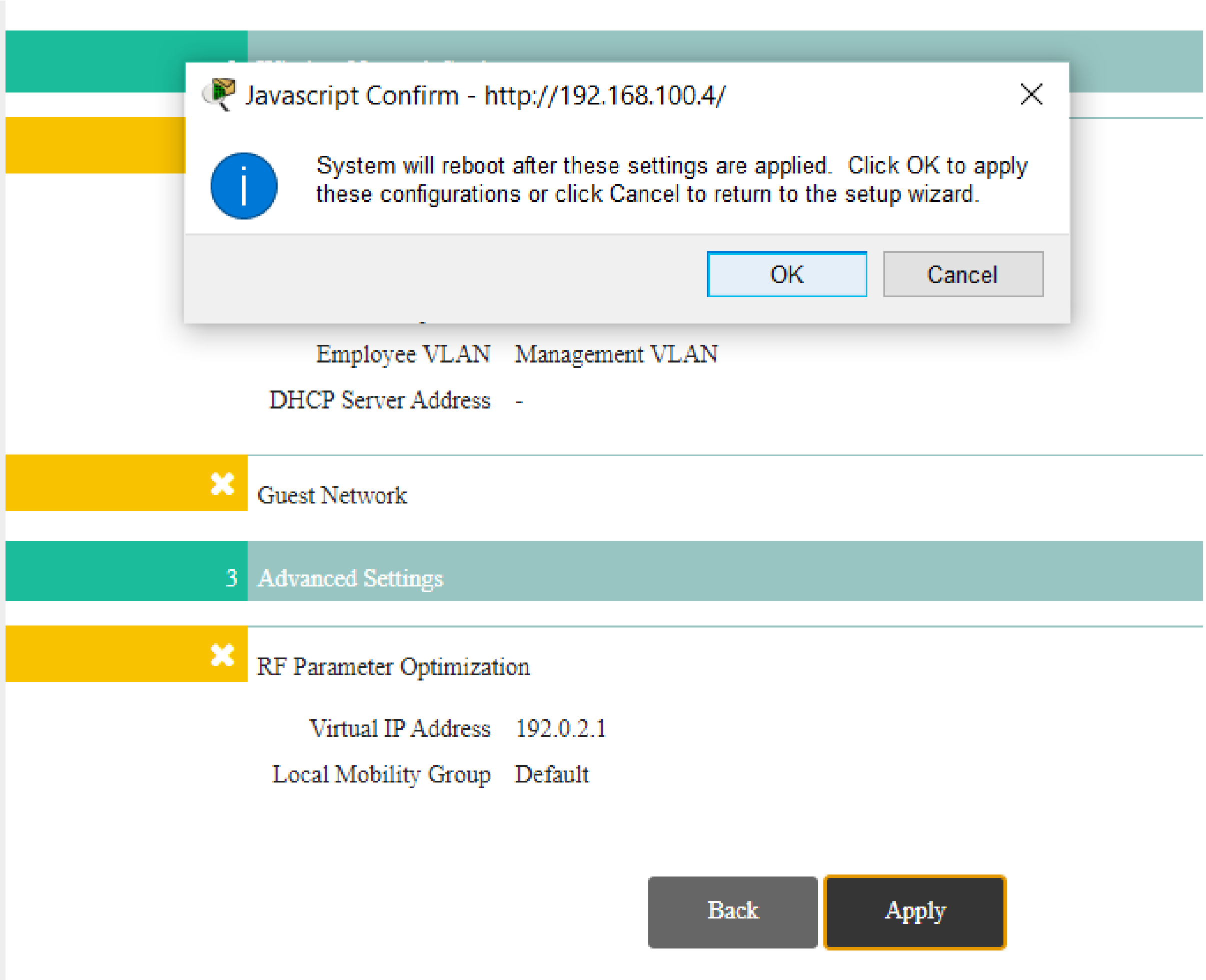
3 Advanced Settings

✗ RF Parameter Optimization

Virtual IP Address	192.0.2.1
Local Mobility Group	Default

Figure 27 Overview

Overview all the settings to create account in WLC. Click Apply to continue create account.



Javascript Confirm - http://192.168.100.4/

System will reboot after these settings are applied. Click OK to apply these configurations or click Cancel to return to the setup wizard.

Employee VLAN Management VLAN

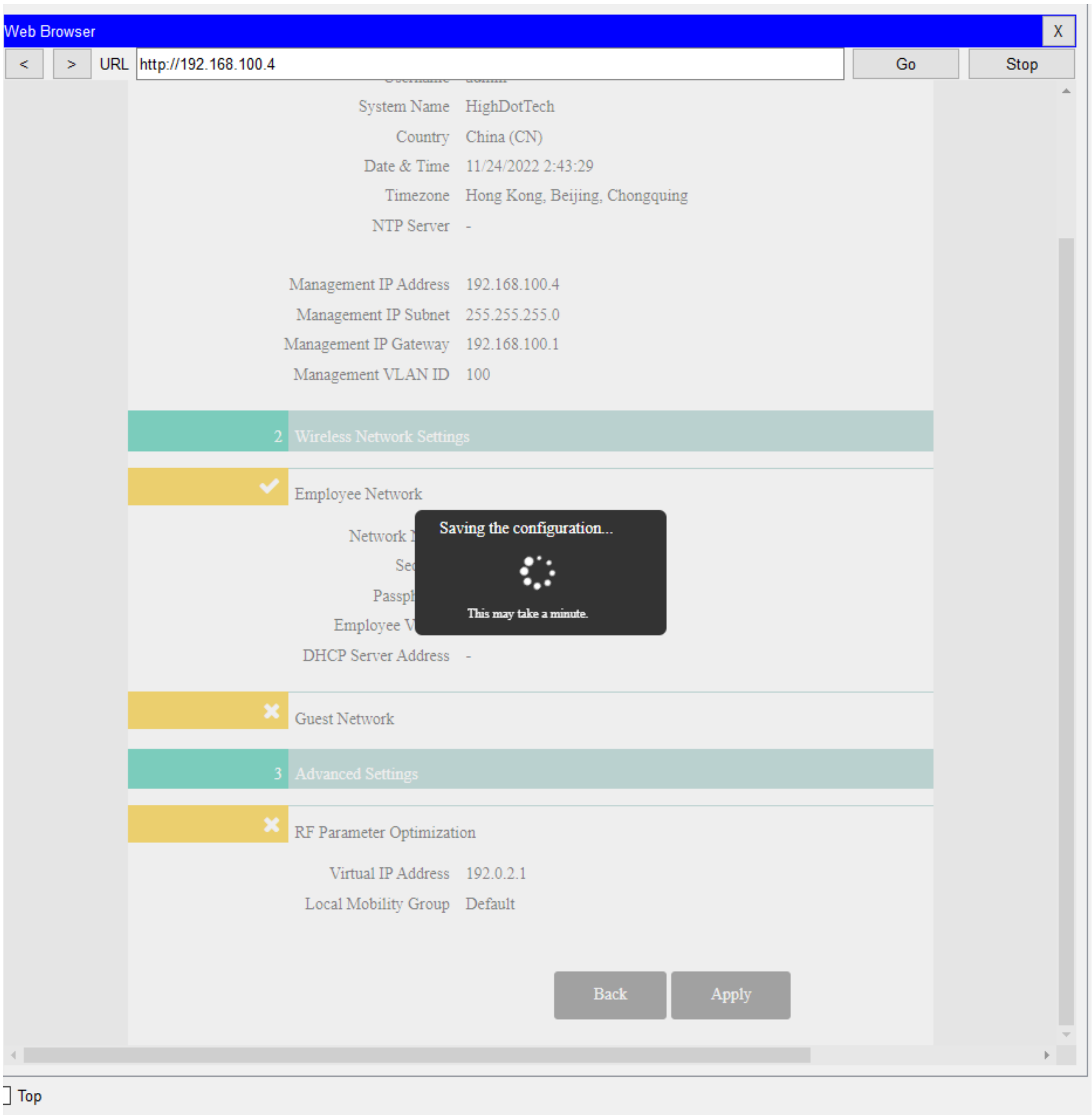
DHCP Server Address -

Virtual IP Address 192.0.2.1

Local Mobility Group Default

Figure 28 Confirm

Click confirm to save the configuration and create account.



System Name HighDotTech
Country China (CN)
Date & Time 11/24/2022 2:43:29
Timezone Hong Kong, Beijing, Chongquing
NTP Server -

Management IP Address 192.168.100.4
Management IP Subnet 255.255.255.0
Management IP Gateway 192.168.100.1
Management VLAN ID 100

2 Wireless Network Settings

✓ Employee Network

Network N
Sec
Passph
Employee V
DHCP Server Address -

Saving the configuration...

This may take a minute.

✖ Guest Network

3 Advanced Settings

✖ RF Parameter Optimization

Virtual IP Address 192.0.2.1
Local Mobility Group Default

Figure 29 Save Configuration

Close the browser after a moment.

3.0 Types of Security Attacks on Layer 2

Security of the Layer 2 is often viewed as the weakest link in the system. This is because LANs have traditionally been administered by a single business. Normal people had a basic level of trust for everyone, and everything linked to LAN. LANs of the High Dot Tech network are now more susceptible to intrusion thanks to BYOD and more sophisticated assaults. Understanding Layer 2's core operations and the risks they present is crucial since doing so will help the network stop attacks on the Layer 2 infrastructure of High Dot Tech networks (Cisco, n.d.).

The security of Layer 2 is often seen as the system's weakest link. This is due to the fact that LANs have often been managed by a single company. The majority of people trusted everyone, and everything connected to LAN on some degree. BYOD and more complex attacks have made the High Dot Tech network's LANs increasingly vulnerable to penetration. The network will be able to prevent assaults on the Layer 2 infrastructure of High Dot Tech networks if it is aware of Layer 2's fundamental functions and the threats they pose (Cisco, n.d.).

3.1 MAC Address Flooding Attack

Switches often incorporate a table structure called the MAC Table that gathers the unique MAC addresses of hosts devices that are connected to network switch ports. Now that they have access to this information, switches may utilise it to tell receivers where to receive data that is leaving ports. Hubs broadcast data to the whole network, enabling it to reach all hosts on the network. While on the other hand, switches carry data to the specific computer or machines to which the data is meant to be transmitted. MAC tables are used to do this (Jithin, 2016).

This MAC Table is destroyed using a MAC Address Flooding Attack. An attack that uses MAC address flooding often includes the attacker delivering a lot of Ethernet packets. The objective of the attacker is to entirely fill the memory of the switch, which will occupy the MAC address database (Jithin, 2016).

The MAC addresses of authorised users will be deleted or removed from the MAC Table which the switch can no longer provide the system with incoming data. As a result, there will be so many incoming frames that all ports will be overloaded. There is no more room in the MAC Address Table to hold any more MAC addresses. The switch will go into fail-open mode as a consequence of the MAC Address table and start acting just like a network hub. All open ports will get a broadcast of the incoming data (Jithin, 2016).

Any data packets intended for the victim PC during network connections would also be intercepted by the attacker. The communications between the victim and other computers will provide the attacker access to sensitive data. Usually, these sensitive data are captured using a packet analyser. The attacker has the option to launch an ARP spoofing attack after a successful MAC Address Flooding Attack. However, the attacker of MAC Address Flooding attack will continue to have access to sensitive data even after the switches under attack have recovered (Jithin, 2016).

3.2 VLAN Hopping Attack

A VLAN hopping attack aims to imitate a switch to trick a real switch into forming a trunking connection between the device of the attacker and the victim switch. A switch and a router or two switches are linked via a trunk connection. The trunk connection maintains the data for the VLANs when traffic is transferred between linked switches or between linked switches and routers (Azad, 1969).

The data packets that go through the trunk connection are tagged with the VLAN to which they belong. Consequently, a trunk connection transports traffic from several VLANs. When the trunk link is established, the attacker will be able to access to every VLAN packet on the network because trunking connections allow for the transmission of all VLAN packets.

The attacker must be connected to a switch interface with either "dynamic requested," "dynamic auto," or "trunk" specified as the configuration setting for this VLAN hopping attack. Trunk links are established between two switches using DTP messages (Azad, 1969).

For this VLAN hopping attack, the attacker must be connected to a switch interface with "dynamic requested," "dynamic auto," or "trunk" chosen as the configuration parameter. DTP messages are used to create trunk linkages between two switches (Azad, 1969).

3.3 DHCP Spoofing Attack

DHCP Spoofing Attack is one type of security attacks on Layer 2. Since DHCP does not provide authentication, it is very vulnerable to spoofing attacks. A network may readily suffer great harm from a spoofing attack (Global, 2022).

Instead of the network's authorised DHCP server, a user may unintentionally start a DHCP connection with an attacker operating a rogue DHCP server on the network. This might easily occur if the malicious DHCP server is located closer to the DHCP client and responds ahead of the real DHCP server (Global, 2022).

The attacker can therefore carry out a man-in-the-middle attack by identifying themselves as a default gateway or DNS server in the DHCP answers sent to the DHCP clients. By doing so, the attacker is able to eavesdrop on IP traffic between the network's configured clients and other clients (Global, 2022).

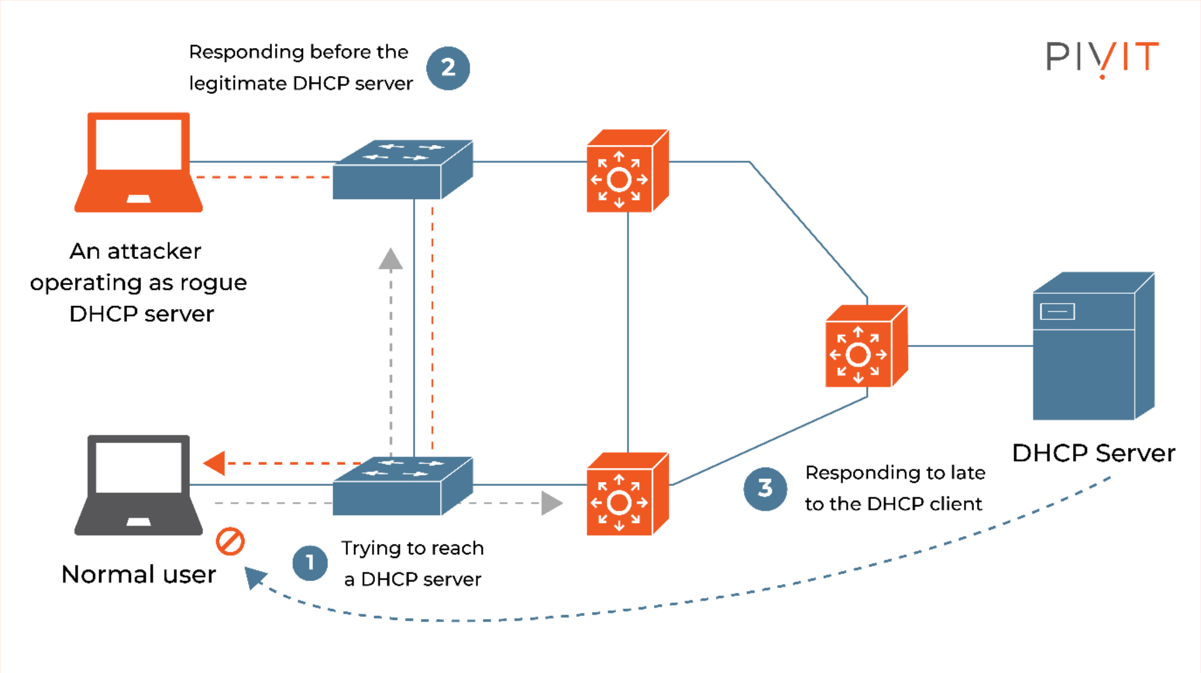

Responding before the legitimate DHCP server
2
PIVIT
An attacker operating as rogue DHCP server
DHCP Server
3
Responding to late to the DHCP client
Normal user
1
Trying to reach a DHCP server

Figure 30 Process of DHCP Spoofing Attack

In order to get IP information, a user first attempts to connect to a DHCP server. The switch will flood the message on all interfaces since this is a broadcast frame, which means that two copies of the message will be sent—one to the genuine DHCP server and the other to the malicious DHCP server (Global, 2022).

Finally, only this server will be used for further DHCP interactions if the attacker's device responds first, and the DHCP Offer message from the regular DHCP server will be denied (Global, 2022).

3.4 STP Attack

STP Attack is one type of security attacks on Layer 2. Attacks against STP are made when an unauthorized user, hacker, or intruder pretends as the root bridge of the topology. The attacker will continue the attack by broadcasting a STP configuration/topology change BPDU in order to make STP recalculation happen. The BPDU signal indicates a lower bridge priority for the attacker's system. The attacker may interrupt the IT service as the frames delivered from other switches is accessible to the attacker. The network may be disrupted when the root bridge changes, which might cause a denial-of-service (DoS) issue. Figure 24: STP Attacks demonstrates how the attacker alters the network topology by using STP to make its host the root bridge (Orbitco, 2022).

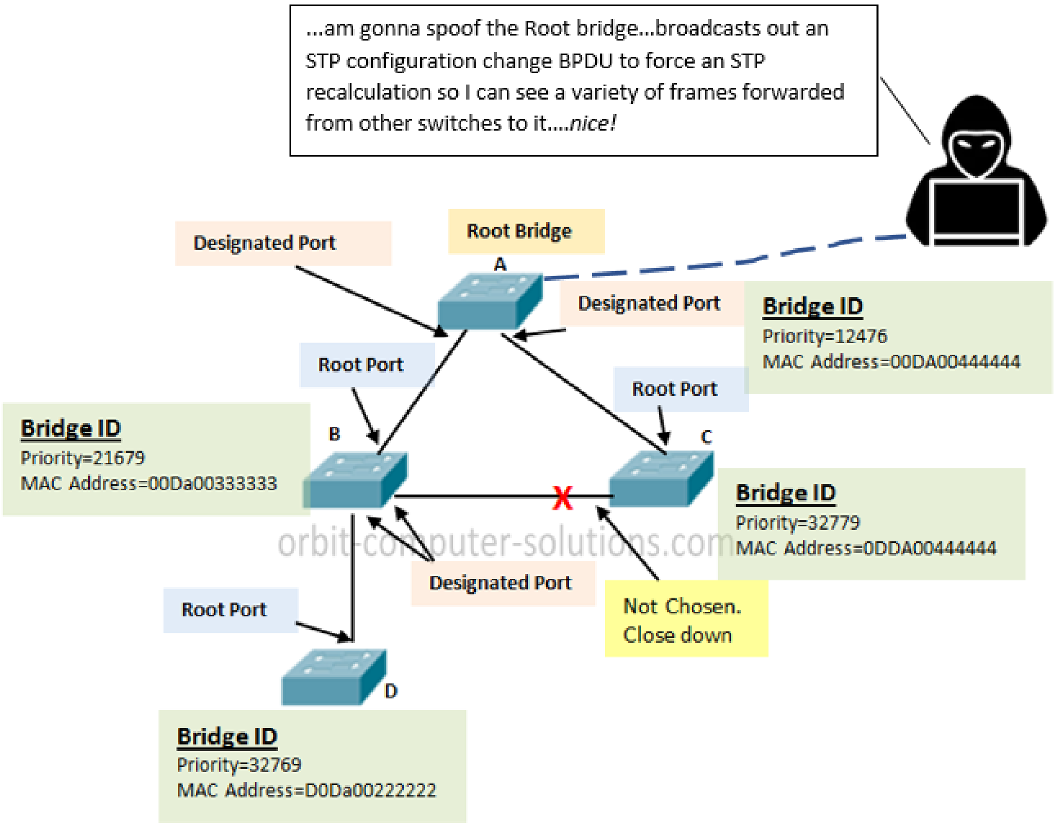


Figure 31 STP Attacks

4.0 Layer 2 Security Deployment to Mitigate the Attacks

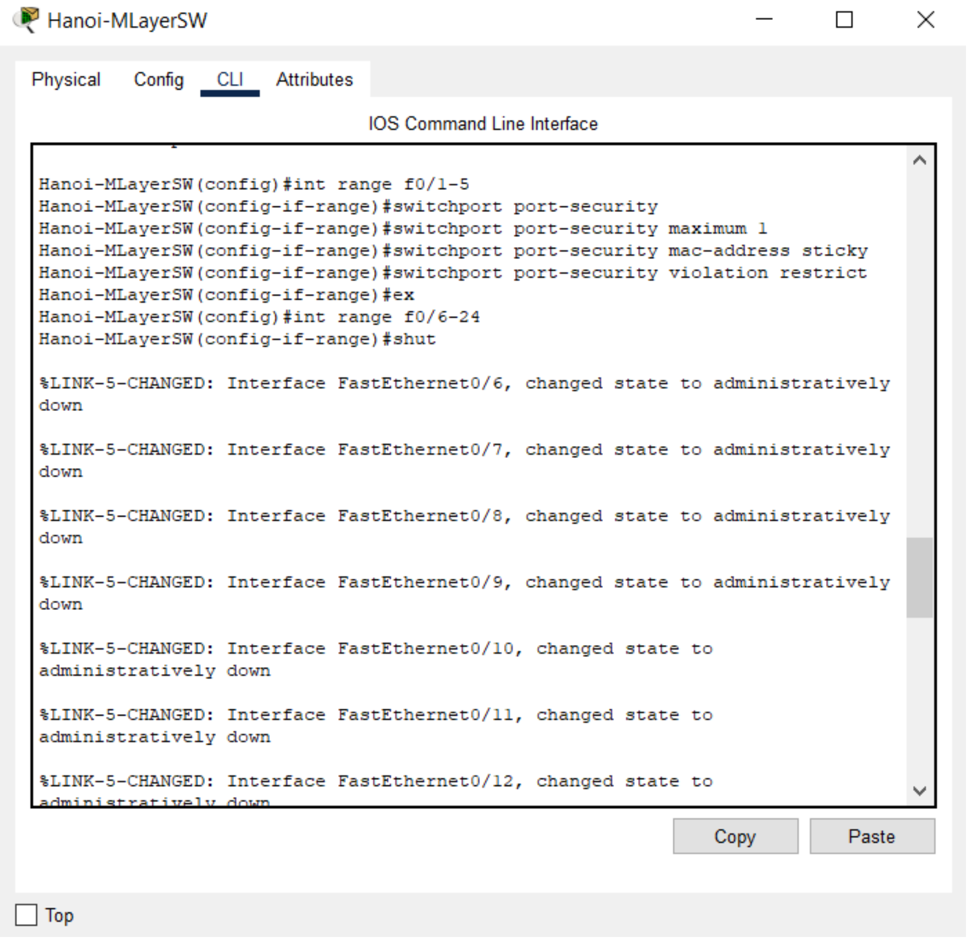
4.1 Solution of MAC Address Flooding Attack

There are several ways to stop the MAC Address Flooding Attack. Here are a few of these techniques.

Port Security

The port security is a typical defense against MAC Flooding Attacks. The end station ports on the switches have a restriction on how many MAC addresses they can detect. The standard MAC address database also contains a small number of "secure" MAC addresses. The MAC address table includes this table as a subset (Jithin, 2016).

4.1.1 Implement Port Security



```
Hanoi-MLayerSW(config)#int range f0/1-5
Hanoi-MLayerSW(config-if-range)#switchport port-security
Hanoi-MLayerSW(config-if-range)#switchport port-security maximum 1
Hanoi-MLayerSW(config-if-range)#switchport port-security mac-address sticky
Hanoi-MLayerSW(config-if-range)#switchport port-security violation restrict
Hanoi-MLayerSW(config-if-range)#ex
Hanoi-MLayerSW(config)#int range f0/6-24
Hanoi-MLayerSW(config-if-range)#shut

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to
administratively down
```

Figure 32 Port Security of Hanoi-MLayerSW

Enable Port Security

In the High Dot Tech network, port security is enabled for all switches' ports with switchport mode access (Cisco, n.d.).

Limit and Learn MAC Addresses

There will be a maximum of 1 MAC address available on each switch port with switchport mode access provided. It is possible to limit the total amount of MAC addresses. All of the switches in the High Dot Tech network will have their switchport mode access ports set up so that they may find MAC addresses on secure ports. Switches may dynamically learn the MAC address and "stick" it to the current configuration (Cisco, n.d.).

Port Security Violation

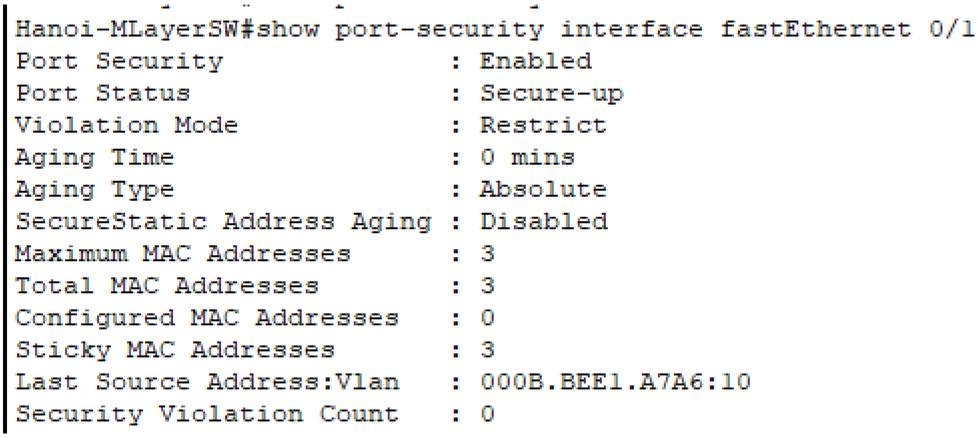
The port rejects packets with unknown source addresses until the number of secure MAC addresses is sufficiently reduced to drop below the maximum value or goes below the maximum value (Cisco, n.d.).

Secure Unused Ports

As a network executive of High Dot Tech company, In order to prevent unauthorised access to the network, I have deactivated. The ***shutdown*** command is used to deactivate the unused ports in the switches (Cisco, n.d.).

I have deactivated the unused ports as a network executive for the High Dot Tech firm to stop unauthorized access to the network. The switches' unused ports are deactivated using the shutdown command (Cisco, n.d.).

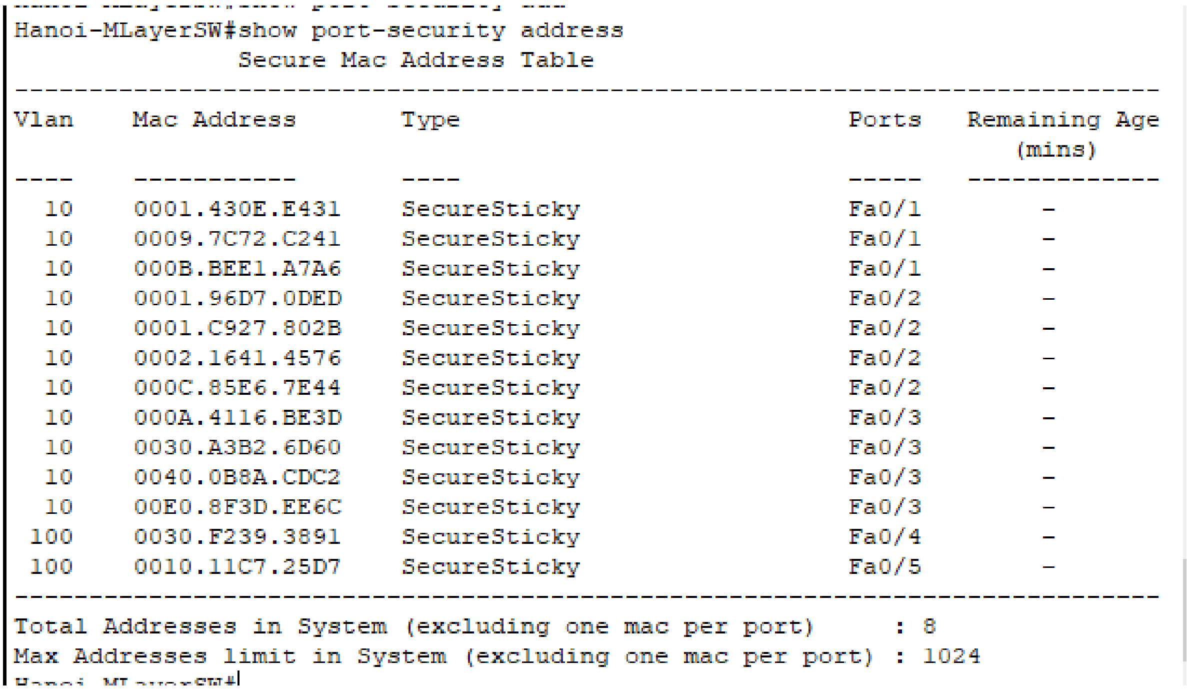
Verification



```
Hanoi-MLayerSW#show port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 3
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 3
Last Source Address:Vlan   : 000B.BEE1.A7A6:10
Security Violation Count   : 0
```

Figure 33 Verify Port Security of Hanoi-MLayerSW

The port security is enabled. Maximum 3 MAC Address is allowed. Sticky MAC address has been configured which the MAC address will be dynamically learned.



```
Hanoi-MLayerSW#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
  10    0001.430E.E431    SecureSticky                  Fa0/1        -
  10    0009.7C72.C241    SecureSticky                  Fa0/1        -
  10    000B.BEE1.A7A6    SecureSticky                  Fa0/1        -
  10    0001.96D7.0DED    SecureSticky                  Fa0/2        -
  10    0001.C927.802B    SecureSticky                  Fa0/2        -
  10    0002.1641.4576    SecureSticky                  Fa0/2        -
  10    000C.85E6.7E44    SecureSticky                  Fa0/2        -
  10    000A.4116.BE3D    SecureSticky                  Fa0/3        -
  10    0030.A3B2.6D60    SecureSticky                  Fa0/3        -
  10    0040.0B8A.CDC2    SecureSticky                  Fa0/3        -
  10    00E0.8F3D.EE6C    SecureSticky                  Fa0/3        -
 100    0030.F239.3891    SecureSticky                  Fa0/4        -
 100    0010.11C7.25D7    SecureSticky                  Fa0/5        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 8
Max Addresses limit in System (excluding one mac per port) : 1024
Hanoi-MLayerSW#
```

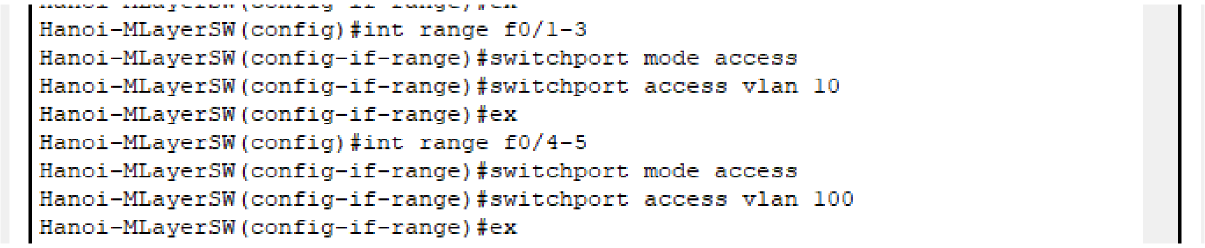
Figure 34 Verify Port Security of Hanoi-MLayerSW

The output shows that each port has different amount of MAC address based on the amount configured and the MAC address sticks to the running configuration.

4.2 Solution of VLAN Hopping Attack

The following modes shouldn't be used for access ports' configuration in High Dot Tech network (Azad, 1969):

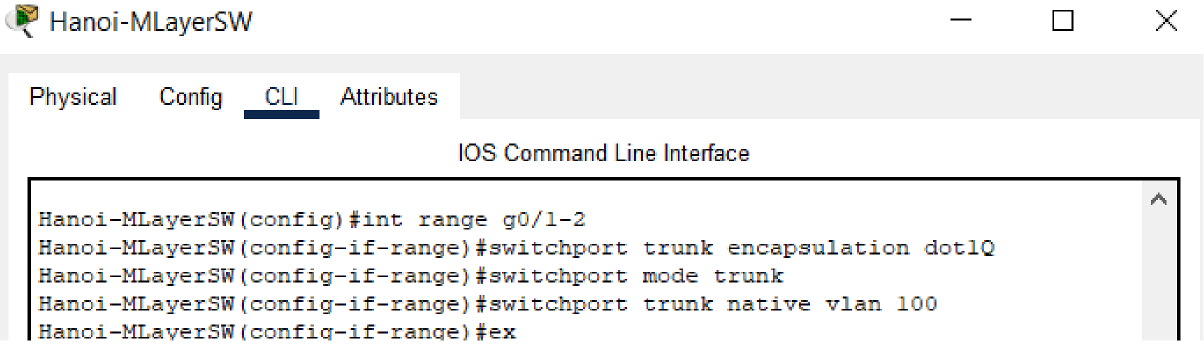
- dynamic desired
- dynamic auto
- trunk



```
Hanoi-MLayerSW(config)#int range f0/1-3
Hanoi-MLayerSW(config-if-range)#switchport mode access
Hanoi-MLayerSW(config-if-range)#switchport access vlan 10
Hanoi-MLayerSW(config-if-range)#ex
Hanoi-MLayerSW(config)#int range f0/4-5
Hanoi-MLayerSW(config-if-range)#switchport mode access
Hanoi-MLayerSW(config-if-range)#switchport access vlan 100
Hanoi-MLayerSW(config-if-range)#ex
```

Figure 35 switchport mode access

As a network executive, I have disabled the dynamic trunking protocol on all access ports by manually configuring them under switchport mode access or switchport negotiation.



```
Hanoi-MLayerSW(config)#int range g0/1-2
Hanoi-MLayerSW(config-if-range)#switchport trunk encapsulation dot1Q
Hanoi-MLayerSW(config-if-range)#switchport mode trunk
Hanoi-MLayerSW(config-if-range)#switchport trunk native vlan 100
Hanoi-MLayerSW(config-if-range)#ex
```

Figure 36 switchport mode trunk

Use the command "***switch port mode trunk***" to manually configure each trunk port and disable the dynamic trunking protocol on each trunk port.

Last but not least, after combining them into a VLAN, switch off any unnecessary interfaces (Azad, 1969).

4.3 Solution of VLAN Double Tagging Attack

On the High Dot Tech network's default VLAN, do not add any hosts. Use a newly created, unused VLAN as the trunk port's native VLAN. Since the selected VLAN is only used by native VLAN, all trunk ports must be set in the same way (Azad, 1969).

4.4 Solution of DHCP Spoofing Attack

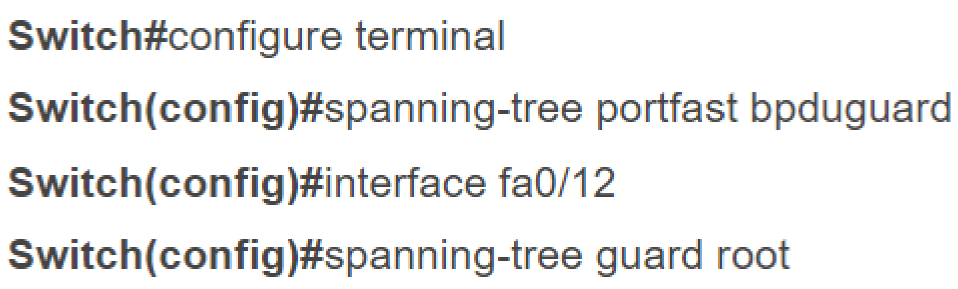
These attacks are mitigated by DHCP snooping. DHCP offers and DHCP ACK messages may be sent via trusted ports during DHCP snooping. As with DHCP, Untrusted ports are not allowed to send messages (Rathore, 2019).

Use the DHCP snooping table to detect the messages arriving from filtered or untrusted ports. The switch rejects all responses coming from untrusted ports and intercepts all requests coming from them (Rathore, 2019).

4.5 Solution of STP Attack

The STP root guard function provides the location of the network's root bridge. The STP BPDU guard maintains the predictability of every operational network topology (Orbitco, 2022). The location of the network's root bridge is made available via the STP root guard function. The STP BPDU guard keeps every operational network topology predictable (Orbitco, 2022).

The configuration shown below explains how to use PortFast with BPDU Guard to use BPDU Guard to disable ports that would otherwise become the root bridge due to their BPDU advertising and to deactivate ports upon BPDU message detection (Orbitco, 2022).



```
Switch#configure terminal
Switch(config)#spanning-tree portfast bpduguard
Switch(config)#interface fa0/12
Switch(config)#spanning-tree guard root
```

Figure 37 Enable BPDU guard

5.0 Conclusion

In this assignment, the proposed WLAN Architecture is Infrastructure mode. This mode has a distribution system which has Ethernet connection to the network infrastructure of High Dot Tech network. There are different types of security attacks can be done on Layer 2 of High Dot Tech network due to its vulnerabilities. Then, Layer 2 security deployment on High Dot Tech network plays an important role to mitigate the Layer 2 attacks.

For Section A, the introduction is briefly explain. As for the Proposed WLAN Architecture part, I have discussed about the WLAN components, Infrastructure WLAN and how to implement WLC WLAN. This part also includes the configurations on the Graphic User Interface (GUI) of the access points on Port 0 and Port 1. Also, I have attached with the screenshot of the steps to create an account in WLC. Next, I have also discussed five types of security attacks on layer 2 which I have also gained a lot of knowledge while completing the research on this section. Along with the type of security attacks, the security deployment to mitigate the attacks is also discussed. Additionally, the solution of the MAC Addressing Flooding Attack is attached with the screenshots and explanations of implementing port security in High Dot Tech network.

As for the next section, the things that would be discussed in Section B will be the ip addressing table which includes few important tables. The entire network will be explained. The LAN and WAN configurations implemented on High Dot Tech network will be included. The security on Layer 2 that has been implemented on the High Dot Tech network is also shown in the next section.

6.0 References

Azad, U. (1969, January 1). *VLAN Hopping Attack and Mitigation*. linuxhint. Retrieved November 27, 2022, from https://linuxhint.com/vlan-hopping-attack-mitigation/

Cisco. (n.d.). *Configure Switch Ports*. Switching, Routing, and Wireless Essentials. Retrieved November 26, 2022, from https://contenthub.netacad.com/srwe-dl/1.2.5

Cisco. (n.d.). *Layer 2 Security Threats*. Switching, Routing, and Wireless Essentials. Retrieved November 26, 2022, from https://contenthub.netacad.com/srwe-dl/10.3.2

Cisco. (n.d.). *WLAN Components*. Switching, Routing, and Wireless Essentials. Retrieved November 26, 2022, from https://contenthub.netacad.com/srwe-dl/12.2.1

Cisco. (n.d.). *WLAN Operation*. Switching, Routing, and Wireless Essentials. Retrieved November 26, 2022, from https://contenthub.netacad.com/srwe-dl/12.3.2

Global, P. I. T. (2022, May 26). *The Ultimate Guide to DHCP spoofing and starvation attacks*. pivit global. Retrieved November 27, 2022, from https://info.pivitglobal.com/resources/dhcp-spoofing-and-starvation-attacks

Jithin. (2016, October 28). *What is Mac flooding? how to prevent it? - interserver tips*. What is MAC Flooding? How to prevent it? Retrieved November 26, 2022, from https://www.interserver.net/tips/kb/mac-flooding-prevent/

Orbitco. (2022, June 30). *Network security - STP manipulation attacks*. Network Security – STP Manipulation Attacks. Retrieved November 27, 2022, from https://www.orbit-computer-solutions.com/network-security-stp-manipulation-attacks/#:~:text=An%20STP%20manipulation%20attack%20is,has%20a%20lower%20bridge%20priority.

Rathore, A. (2019, October 17). *DHCP snooping attack*. Medium. Retrieved November 27, 2022, from https://medium.com/@ayushir/dhcp-snooping-attack-ca728e4dd84