

1. Cấu hình Core Switch

configure terminal

Switch(config)#hostname Core

Core# vlan database

vlan 10 name Management

vlan 11 name Corporate

vlan 12 name Guest

vlan 13 name Smartphone

exit

Core#configure terminal

interface range g1/0/1-10

switchport mode trunk

switchport trunk native vlan 10

interface range g1/0/21-24

switchport mode access

switchport access vlan 10

spanning-tree portfast

2. Cấu hình Router

```
interface g0/0  
no shutdown
```

```
interface GigabitEthernet0/0.10  
encapsulation dot1Q 10 native  
ip address 192.168.10.1 255.255.255.0
```

```
interface GigabitEthernet0/0.11  
encapsulation dot1Q 11  
ip address 192.168.11.1 255.255.255.0
```

```
interface GigabitEthernet0/0.12  
encapsulation dot1Q 12  
ip address 192.168.12.1 255.255.255.0
```

```
interface GigabitEthernet0/0.13  
encapsulation dot1Q 13  
ip address 192.168.13.1 255.255.255.0
```

Router cấu hình DHCP cấp IP cho wireless client

```
ip dhcp excluded-address 192.168.11.1 192.168.11.100  
ip dhcp pool Corporate  
network 192.168.11.0 255.255.255.0  
default-router 192.168.11.1
```

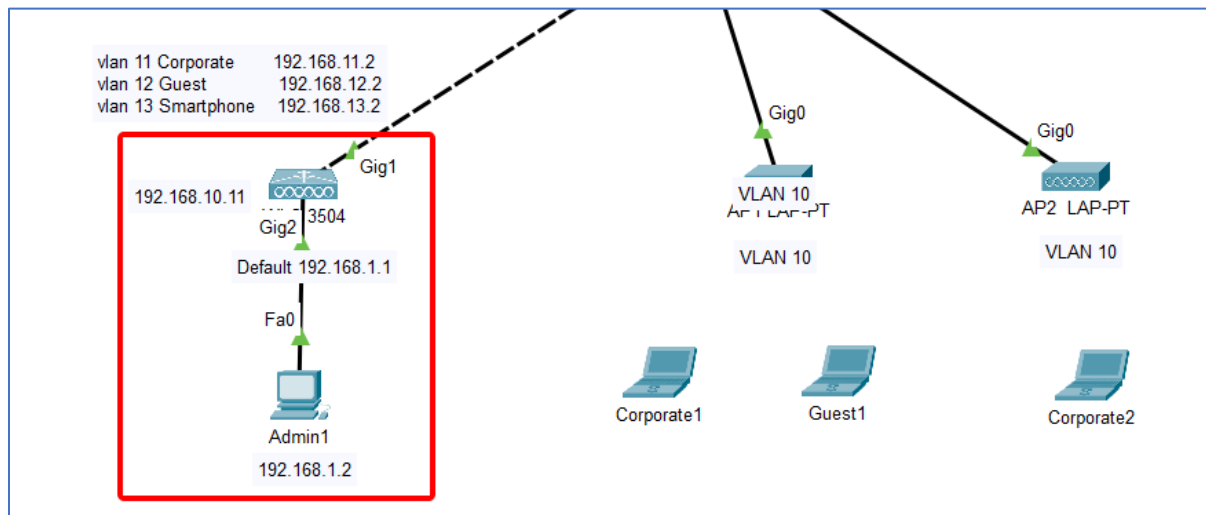
```
ip dhcp excluded-address 192.168.12.1 192.168.12.100  
ip dhcp pool Guest  
network 192.168.12.0 255.255.255.0  
default-router 192.168.12.1
```

```
ip dhcp excluded-address 192.168.13.1 192.168.13.100  
ip dhcp pool Smartphone
```

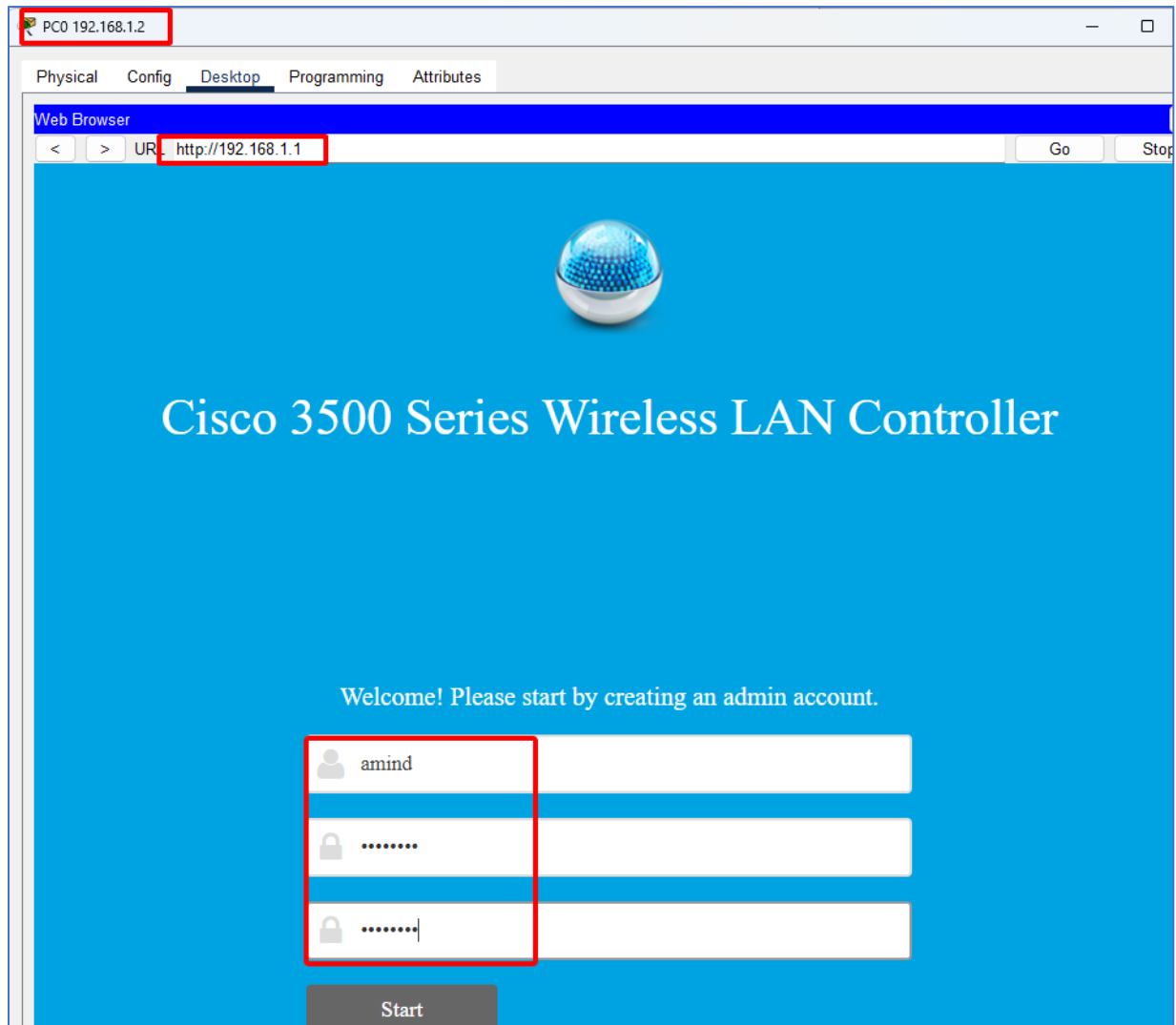
network 192.168.13.0 255.255.255.0
 default-router 192.168.13.1

3. Cấu hình WLC


B1. Nối PC0 Admin1 trực tiếp với WLC, ping kiểm tra



B2. Mở <http://192.168.1.1> trong cửa sổ trình duyệt web trên máy tính xách tay của Admin1 mở Giao diện người dùng quản trị Wireless LAN Controller. Đăng nhập bằng tên **admin** và mật khẩu **P@ssword**. Nếu bạn nhận được thông báo lỗi 'Host Name Unresolved' thì hãy đóng cửa sổ trình duyệt web, sau đó mở lại và thử lại.



B3. Nhập các thông tin quản lý WLC



Cisco 3500 Series Wireless LAN Controller

1

Set Up Your Controller

System Name

MasterLH

?

Country

Thailand (TH)

?

Date & Time

10/15/2024

16:04:29

Timezone

Saigon, Hanoi, Bangkok, Jakarta

?

NTP Server

(optional)

?

Management IP Address

192.168.10.11

?

Subnet Mask

255.255.255.0

Default Gateway

192.168.10.1

Management VLAN ID

1

?

Back

Next

B4. Next, Next, Apply

> URL <http://192.168.1.1> Go

2 Create Your Wireless Networks

Employee Network ☒

Network Name

Security

Passphrase

Confirm Passphrase

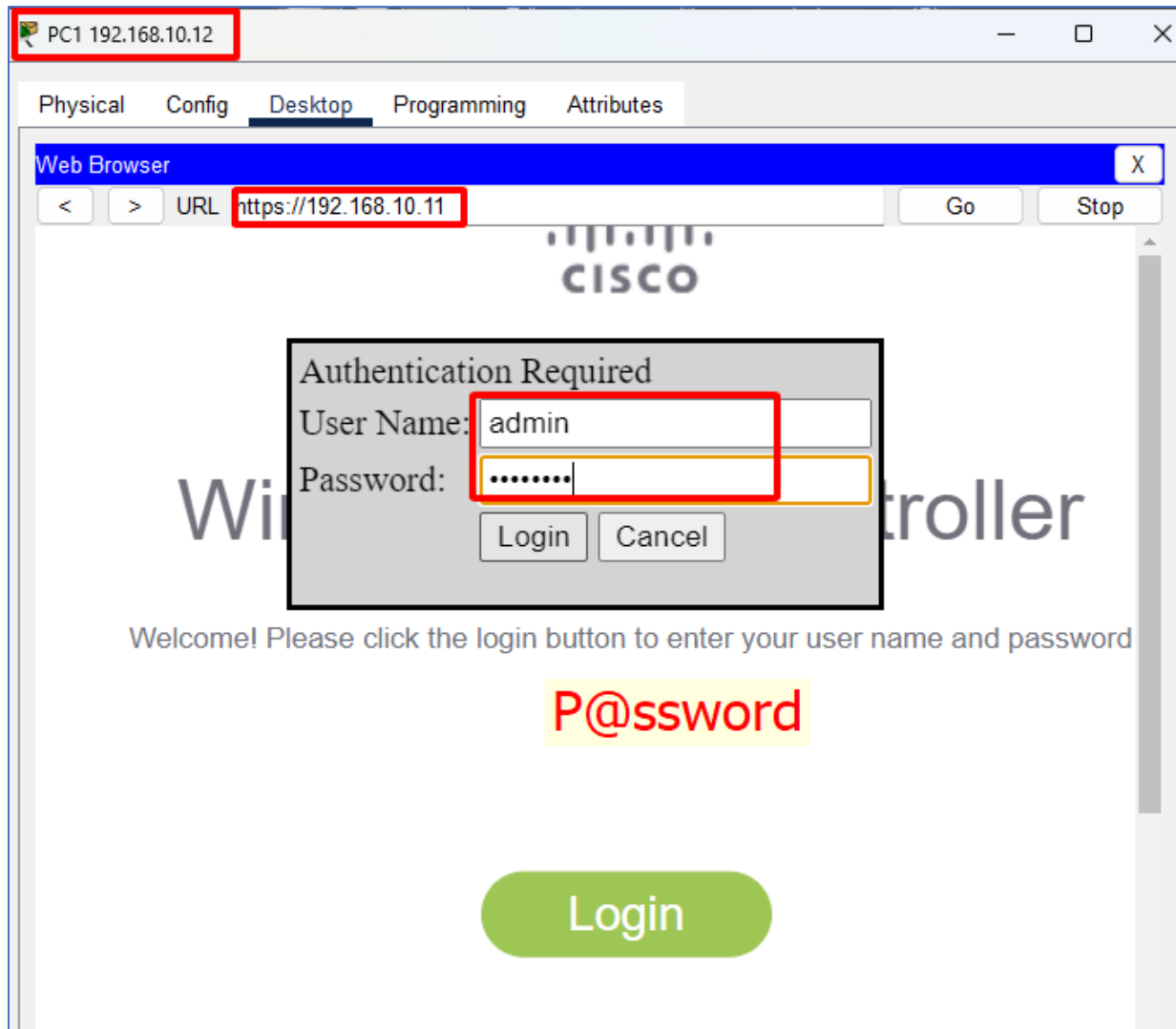
VLAN

DHCP Server Address

Guest Network ☐

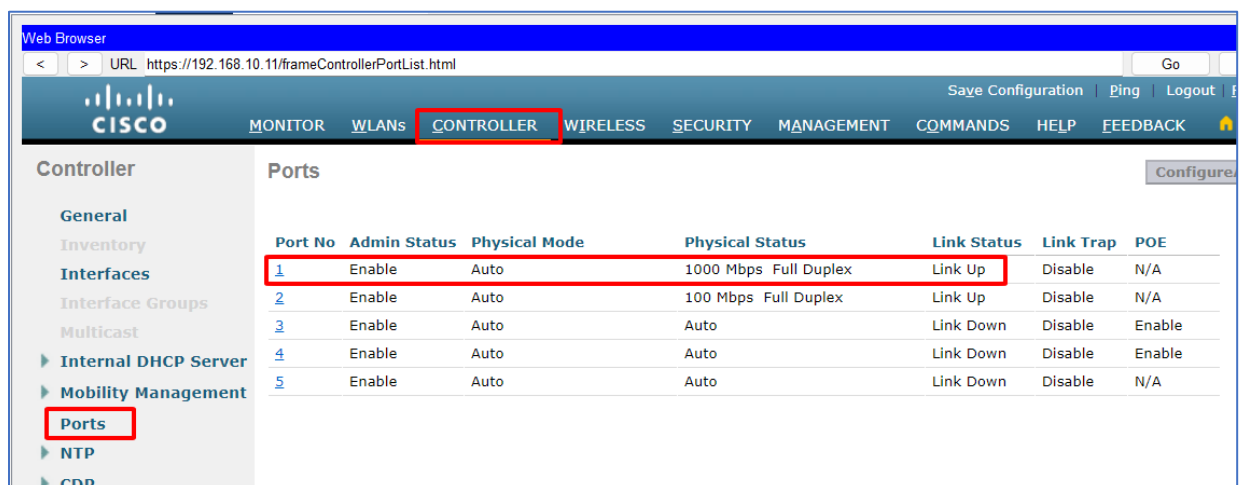
Back Next

B5. Từ PC1 admin2 truy cập vào WLC

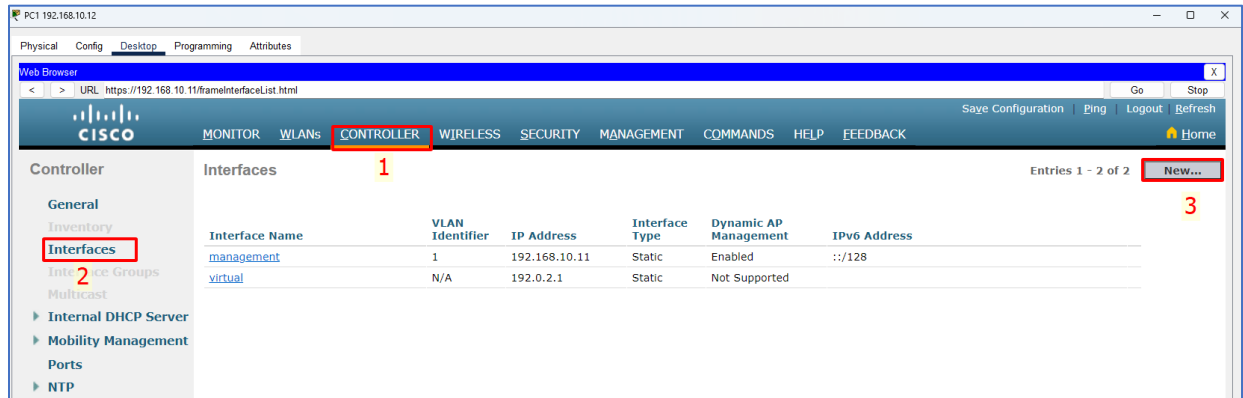


4. Logical Interfaces on the Wireless LAN Controller

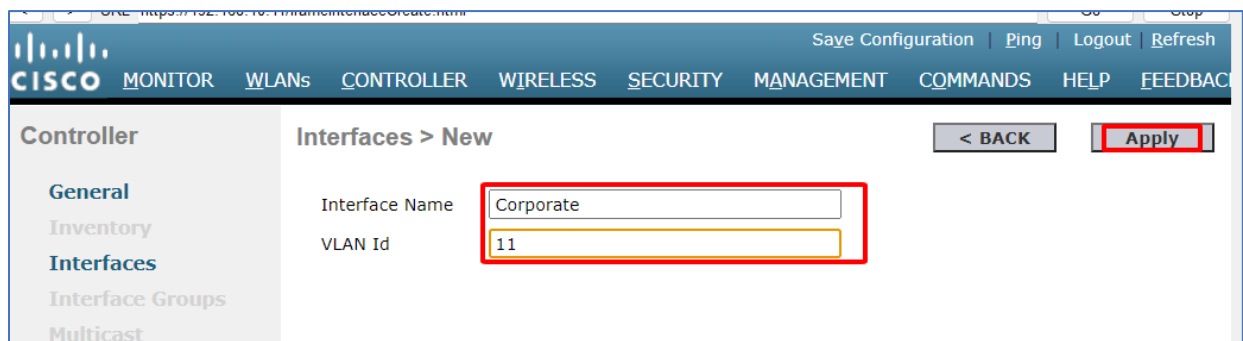
B1. Quan sát port WLC đang kết nối vào switch L3- port 1



B2. Tạo một logical interface Corporate trên Wireless LAN Controller trong Corporate VLAN, với địa chỉ IP là 192.168.11.2.



Tạo interface Corporate



Nhập các thông tin và nhấn **Apply**

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Ping Logout Refresh Home

Interfaces > Edit < BACK Apply

General Information

Interface Name Corporate
MAC Address 00:E0:F9:17:2E:66

Configuration

Guest Lan ☐
Quarantine ☐
Quarantine Vlan Id 0
NAS-ID

Physical Information

Port Number 1
Backup Port 0
Active Port 0
Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier 11
IP Address 192.168.11.2
Netmask 255.255.255.0
Gateway 192.168.11.1

DHCP Information

Primary DHCP Server 0.0.0.0
Secondary DHCP Server

B3. Tạo một logical interface Guest trên Wireless LAN Controller trong Guest VLAN, với địa chỉ IP là 192.168.12.2.

tps://192.168.10.11/frameInterfaceList.html Go Stop

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Ping Logout Refresh Home

Interfaces Entries 1 - 3 of 3 New...

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
Corporate	11	192.168.11.2	Dynamic	Disabled	
management	1	192.168.10.11	Static	Enabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

Remove

Nhập các thông tin và nhấn **Apply**

eb Browser

URL https://192.168.10.11/frameInterfaceCreate.html

Go Stop

Save Configuration | Ping | Logout | Refresh

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

Controller

General

Inventory

Interfaces

Interface Groups

Multicast

Internal DHCP Server

Mobility Management

Interfaces > New

< BACK Apply

Interface Name Guest

VLAN Id 12

Nhập các thông tin và nhấn **Apply**

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

Interfaces > Edit

< BACK Apply

General Information

Interface Name Guest

MAC Address 00:0A:F3:81:89:CC

Configuration

Guest Lan ☐

Quarantine ☐

Quarantine Vlan Id 0

NAS-ID

Physical Information

Port Number 1

Backup Port 0

Active Port 0

Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier 12

IP Address 192.168.12.2

Netmask 255.255.255.0

Gateway 192.168.12.1

DHCP Information

Primary DHCP Server 0.0.0.0

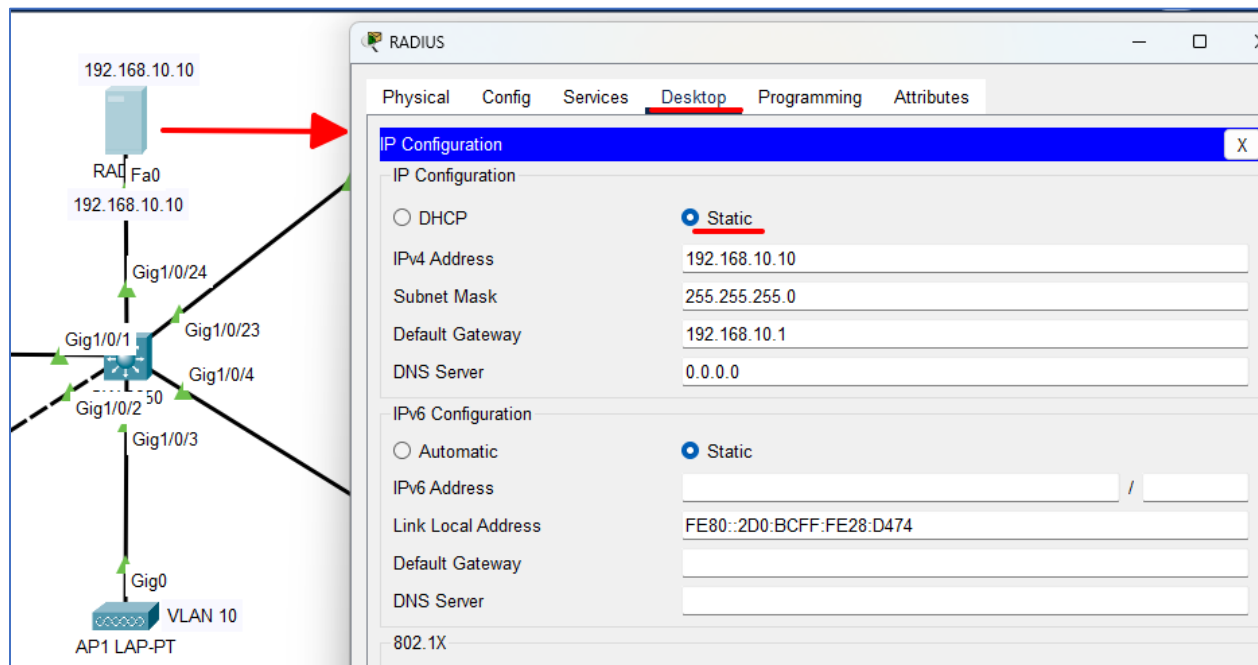
Secondary DHCP Server

DHCP Proxy Mode Global

5. Radius server

B1. Cấu hình Radius server

Nhập IP



Nhập thông tin Radius server

The screenshot shows a network topology on the left and the RADIUS configuration interface on the right. The topology includes a RADIUS server (192.168.10.10) connected to a switch (192.168.10.10) via Fa0. The switch has interfaces Gig1/0/24, Gig1/0/23, Gig1/0/1, Gig1/0/2, Gig1/0/3, and Gig1/0/4. A laptop (Corporate1) is connected to Gig1/0/2, and another (Guest1) is connected to Gig1/0/3. The RADIUS configuration interface has tabs: Physical, Config, **Services**, Desktop, Programming, Attributes. The **SERVICES** tab is active, showing a list of services. The **AAA** service is highlighted. The **AAA** configuration section shows: Service: ☒ On, Radius Port: 1812. The **Network Configuration** section shows: Client Name: WLC, Client IP: 192.168.10.11, Secret: master123, ServerType: Radius. The **User Setup** section shows: Username: nv2, Password: 12345678. A table lists users: nv1 and nv2, both with password 12345678.

B2. Khai báo WLC kết nối và chứng thực từ Radius server

The screenshot shows the Cisco WLC configuration interface. The **SECURITY** tab is active. The **RADIUS Authentication Servers** section is visible. The **Auth Called Station ID Type** is set to **IP Address**. The **Use AES Key Wrap** checkbox is unchecked. The **MAC Delimiter** is set to **Hyphen**. The **Framed MTU** is set to **1300**. The **Network User** table is empty. The **Apply** button is highlighted, and the **New...** button is also highlighted.

Nhập các thông tin về RADIUS server và nhấn **Apply**

Web Browser URL: https://192.168.10.11/frameRadiusCreate.html

Navigation: MONITOR | **WLANs** | CONTROLLER | WIRELESS | **SECURITY** | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Left Menu: AAA (General, RADIUS, Authentication, Accounting, Fallback, DNS, Downloaded AVP), TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies, Local EAP, Advanced EAP, Priority Order, Certificate, Access Control Lists

Section: RADIUS Authentication Servers > New

Fields:

- Server Index (Priority): 1
- Server IP Address(Ipv4/Ipv6): 192.168.10.10
- Shared Secret Format: ASCII
- Shared Secret: master123
- Confirm Shared Secret: master123
- Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for CoA: Disabled
- Server Timeout: 2 seconds
- Network User: ☒ Enable
- Management: ☒ Enable
- Management Retransmit Timeout: 2 seconds
- IPSec: ☐ Enable

Buttons: < BACK, Apply

6. Tạo wireless network cho nhân viên

Tạo mạng LAN không dây có tên là 'Corporate'. Các Clients phải được xác thực bởi máy chủ RADIUS 192.168.10.10 mà bạn đã thêm trước đó và mã hóa WPA2 AES phải được sử dụng.

B1. Xóa WLAN mặc định

Web Browser URL: https://192.168.10.11/frameWlan.html

Navigation: MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Left Menu: WLANs (WLANs, Advanced, AP Groups)

Section: WLANs

Current Filter: [Change Filter] [Clear Filter]

Buttons: Create New, Go

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

B2. Nhấp vào 'WLANs', chọn 'Create New' trong danh sách thả xuống rồi nhấp vào 'Go'

Web Browser URL: https://192.168.10.11/frameWlan.html

Navigation: MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Left Menu: WLANs (WLANs, Advanced, AP Groups)

Section: WLANs

Current Filter: [Change Filter] [Clear Filter]

Buttons: Create New, Go

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
---------	------	--------------	-----------	--------------	-------------------

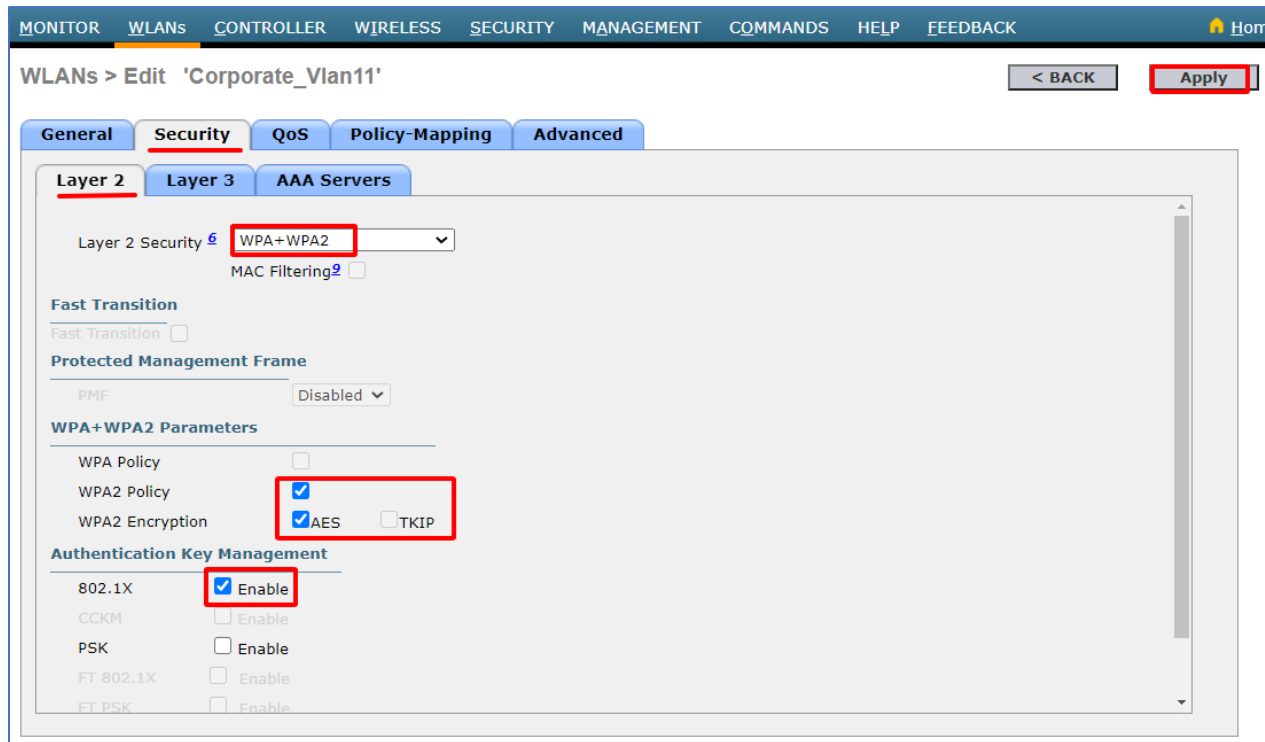
B3. Nhập thông tin chi tiết sau đó nhấp vào 'Apply'

The screenshot shows the Cisco WLAN configuration interface. The 'WLANs > New' form is displayed with the following fields: Type (WLAN), Profile Name (Corporate_Vlan11), SSID (Corporate), and ID (1). The 'Apply' button is highlighted with a red box.

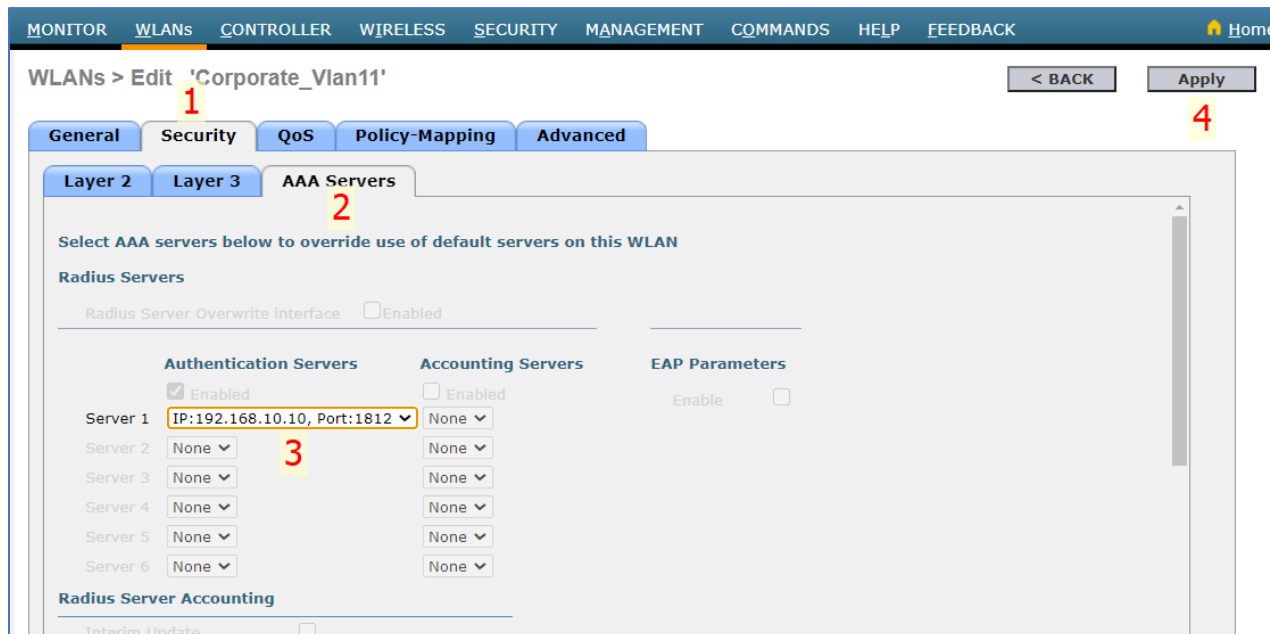
B4. Liên kết WLAN với giao diện '**Corporate**'. Không bật trạng thái vì bạn chưa cấu hình cài đặt bảo mật. Nhấp vào '**Apply**'.

The screenshot shows the Cisco WLAN configuration interface for editing 'Corporate_Vlan11'. The 'General' tab is selected, and the 'Status' checkbox is checked. The 'Interface/Interface Group(G)' dropdown is set to 'Corporate'. The 'Apply' button is highlighted with a red box.

B5. Nhấp vào tab '**Security**' và đảm bảo Layer 2 Security là '**WPA + WPA2**', Chính sách WPA2 được áp dụng với mã hóa AES và Authentication Key Management là 802.1X, sau đó nhấp vào '**Apply**'



B6. Nhấp vào tab 'Security' rồi 'AAA Servers', chọn máy chủ RADIUS mà bạn đã thêm trước đó 'IP:192.168.10.10, Cổng:1812' làm Server 1 và nhấp vào 'Apply'.

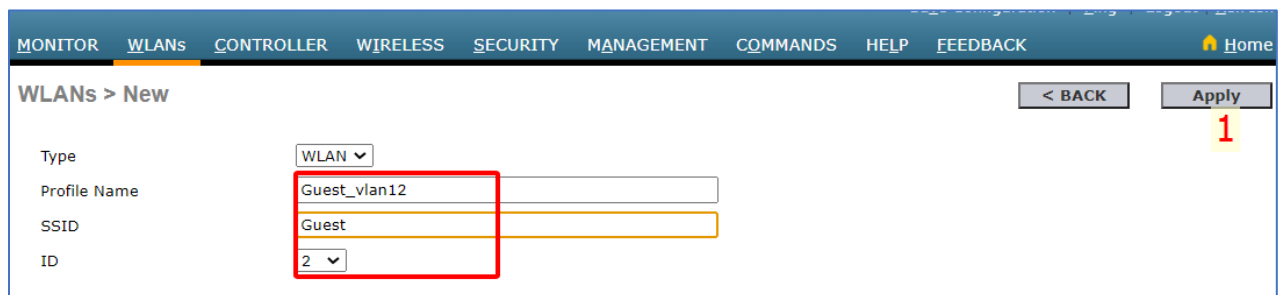


7. Tạo wireless network cho khách – Guest

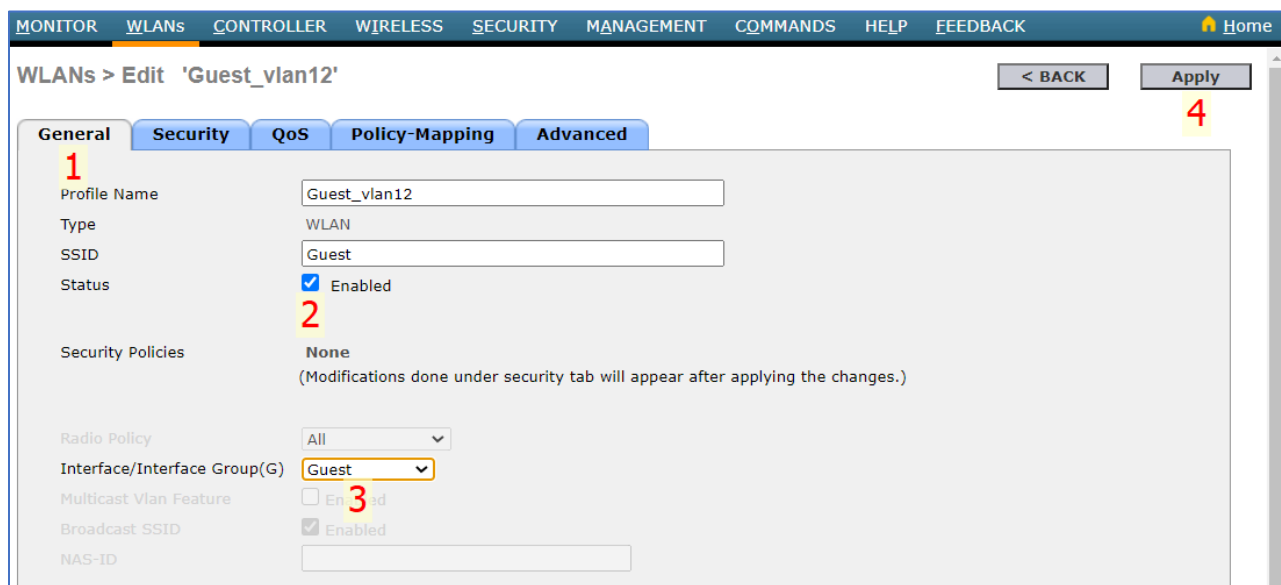
B1. Nhấp vào 'WLANs', chọn 'Create New' trong danh sách thả xuống rồi nhấp vào 'Go'



B2. Nhập thông tin chi tiết sau đó nhấn vào 'Apply'



B3. Liên kết WLAN với giao diện 'Guest'. Không bật trạng thái vì bạn chưa cấu hình cài đặt bảo mật. Nhấn vào 'Apply'.



B4. Nhấn vào tab 'Security' và đảm bảo Layer 2 Security là 'WPA + WPA2', Chính sách WPA2 được áp dụng với mã hóa AES và Authentication Key Management là 802.1X, sau đó nhấn vào 'Apply'

WLANs > Edit 'Guest_vlan12'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security **3** WPA+WPA2

MAC Filtering ☐

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy **4** ☒

WPA2 Encryption **5** ☒ AES ☐ TKIP

Authentication Key Management

802.1X ☐ Enable

CKM ☐ Enable

PSK **5** ☒ Enable

FT PSK ☐ Enable

PSK Format ASCII **6** master123

WPA gtk-randomize State Disabled

7 Apply

B5. Chọn như hình sau đó nhấn vào 'Apply'

WLANs > Edit 'Guest_vlan12'

General Security QoS Policy-Mapping **Advanced**

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching **2** ☒ Enabled

FlexConnect Local Auth **12** ☒ Enabled

Learn Client IP Address **5** ☒ Enabled

Vlan based Central Switching **13** ☐ Enabled

Central DHCP Processing ☐ Enabled

Override DNS ☐ Enabled

NAT-PAT ☐ Enabled

Central Assoc ☐ Enabled

Passive Client ☐

Voice

Media Session Snooping ☐ Enabled

Re-anchor Roamed Voice Clients ☐ Enabled

KTS based CAC Policy ☐ Enabled

Radius Client Profiling

DHCP Profiling ☐

HTTP Profiling ☐

Local Client Profiling

DHCP Profiling ☐

HTTP Profiling ☐

Universal AP Admin Support

Universal AP Admin ☐

11v BSS Transition Support

BSS Transition ☐

Apply

B6. Kết quả

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Corporate_vlan11	Corporate	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Guest_vlan12	Guest	Enabled	[WPA2][Auth(PSK)]

8. Cấu hình DHCP cấp ip cho Vlan 10 – management

B1. CONTROLLER, Internal DHCP Server, DHCP Scope

Xóa scope mặc định và tạo scope mới

Scope Name	Address Pool	Lease Time	Status
day0-dhcp-mgmt	192.168.1.3 - 192.168.1.14		Enabled

B2. Nhập tên scope, nhấn Apply

Scope Name:

B3. Nhấp tên scope

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

DHCP Scopes

New...

Scope Name	Address Pool	Lease Time	Status
DHCP_vlan10_management	0.0.0.0 - 0.0.0.0		Enabled Remove

1

B4. Nhập các thông tin, nhấn Apply

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

DHCP Scope > Edit

< Back Apply 1

Scope Name: DHCP_vlan10_management

Pool Start Address: 192.168.10.101

Pool End Address: 192.168.10.200

Network: 192.168.10.0

Netmask: 255.255.255.0

Lease Time (seconds): 86400

Default Routers: 192.168.10.1 0.0.0.0 0.0.0.0

DNS Domain Name: Not Supported

DNS Servers: 8.8.8.8 0.0.0.0 0.0.0.0

Netbios Name Servers: 0.0.0.0 0.0.0.0 0.0.0.0

Status: Enabled

B5. Chỉ định nguồn cấp IP cho các AP

URL: https://192.168.10.11/frameInterfaceList.html

CISCO

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Controller

General
Inventory
Interfaces 2
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports

Interfaces

1

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
Corporate	11	192.168.11.2	Dynamic	Disabled	
Guest	12	192.168.12.2	Dynamic	Disabled	
management	1	192.168.10.11	Static	Enabled	::/128
virtual 3	N/A	192.0.2.1	Static	Not Supported	

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK [Home](#)

Interfaces > Edit [< BACK](#) [Apply](#)

General Information

Interface Name: management
MAC Address: 00:01:97:96:AA:AD

Configuration

Guest Lan: ☐
NAS-ID:

NAT Address

Enable NAT Address: ☐

Physical Information

Port Number:
Backup Port:
Active Port:
Enable Dynamic AP Management: ☒

Interface Address

VLAN Identifier:
IP Address:
Netmask:
Gateway:

DHCP Information

Primary DHCP Server:
Secondary DHCP Server:

B6. Chỉ định nguồn cấp IP cho các client Corporate

URL: https://192.168.10.11/frameInterfaceEdit.html

Go Stop

Save Configuration Ping Logout Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

Controller

General

Inventory

Interfaces

Interface Groups

Multicast

Internal DHCP Server

Mobility Management

Ports

NTP

CDP

Tunneling

IPv6

mDNS

Advanced

Interfaces > Edit

< BACK Apply

General Information

Interface Name corporate

MAC Address 00:04:9A:59:94:93

Configuration

Guest Lan ☐

Quarantine ☐

Quarantine Vlan Id 0

NAS-ID

Physical Information

Port Number 1

Backup Port 0

Active Port 1

Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier 11

IP Address 192.168.11.2

Netmask 255.255.255.0

Gateway 192.168.11.1

DHCP Information

Primary DHCP Server 192.168.11.1

Secondary DHCP Server

cisco router

B7. Chỉ định nguồn cấp IP cho các client Guest

The screenshot shows the Cisco Meraki Controller web interface. The left sidebar has a menu with 'Interfaces' highlighted. The main content area is titled 'Interfaces > Edit' and contains several sections for configuring a new interface named 'Guest'.

General Information

- Interface Name: Guest
- MAC Address: 00:30:F2:EC:7A:60

Configuration

- Guest Lan: ☐
- Quarantine: ☐
- Quarantine Vlan Id: 0
- NAS-ID:

Physical Information

- Port Number: 1
- Backup Port: 0
- Active Port: 1
- Enable Dynamic AP Management: ☐

Interface Address

- VLAN Identifier: 12
- IP Address: 192.168.12.2
- Netmask: 255.255.255.0
- Gateway: 192.168.12.1

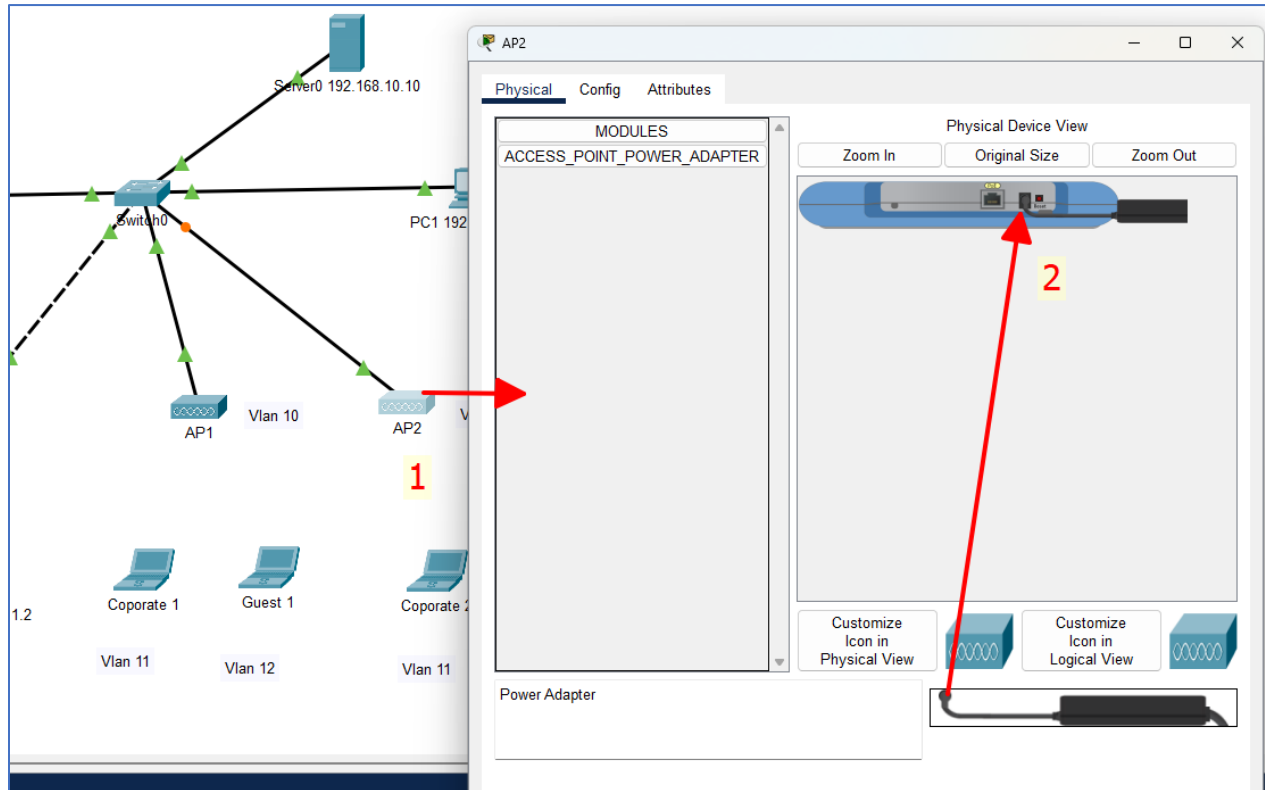
DHCP Information

- Primary DHCP Server: 192.168.12.1
- Secondary DHCP Server:
- DHCP Proxy Mode: Global

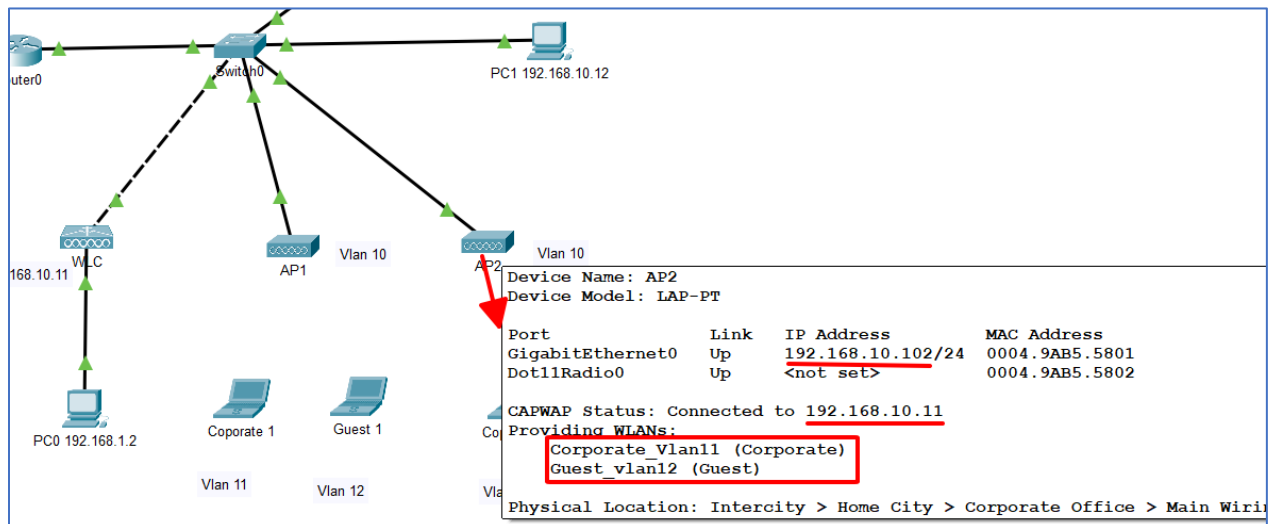
Buttons at the top right include '< BACK' and 'Apply'. A yellow box with the text 'cisco router' is placed next to the Primary DHCP Server field.

9. client kết nối vào mạng không dây

B1. Cấp nguồn cho các AP



B2. Kiểm tra IP đã nhận từ WLC



B3. Client Guest1, Guest2

