

37 Wireless Fundamentals Configuration - Answer Key

In this lab you will configure Corporate and Guest WLANs in a company campus. VLANs and IP subnets have already been set up for the company servers and IT administrators to connect via wired connections:

VLAN Name	VLAN Number	IP Subnet	Gateway (on switch)
Server	11	192.168.11.0/24	192.168.11.1
Admin	21	192.168.21.0/24	192.168.21.1

The IT administrators are restricted to wired connections for security reasons, an 'Admin' WLAN will not be created.

A new Wireless LAN Controller has been added to the network. Your colleague has already performed the initial setup at the command line to give the device IP address 192.168.10.1/24

Two Lightweight Wireless Access Points have just been unboxed and cabled to the Multilayer Switch.

Your job is to configure the new Corporate and Guest WLANs.

You can ignore the MGMT_NET router, it has been added to the lab because Packet Tracer does not support trunk ports on the WLC.

Switch Configuration

- 1) On the multilayer switch, create a new VLAN for management of the wireless infrastructure devices. Use VLAN number 10 and name the VLAN 'Management'.

```
Switch(config)#vlan 10
Switch(config-vlan)#name Management
```

- 2) Create a VLAN interface on the multilayer switch to be used as the default gateway for the Management VLAN. Use IP address 192.168.10.1/24

```
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
```

- 3) On the 'Services > DNS' tab of the RADIUS/DNS/Web server, create a DNS A record which resolves the hostname 'cisco-capwap-controller' to the WLC's IP address 192.168.10.11.
This will allow the Lightweight Access Points to resolve the IP address of the WLC during the Zero Touch Provisioning process.

Fill in the details and click the 'Add' button to add the A record.

The screenshot shows the 'RADIUS/DNS/Web Server' configuration window. The 'Services' tab is selected, and the 'DNS' service is highlighted in the left sidebar. The main area shows the 'DNS' configuration with the 'DNS Service' toggle set to 'On'. Under 'Resource Records', a new A record is being added with the name 'cisco-capwap-controller' and the address '192.168.10.11'. The 'Add' button is highlighted.

Services

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name **cisco-capwap-controller** Type **A Record**

Address **192.168.10.11**

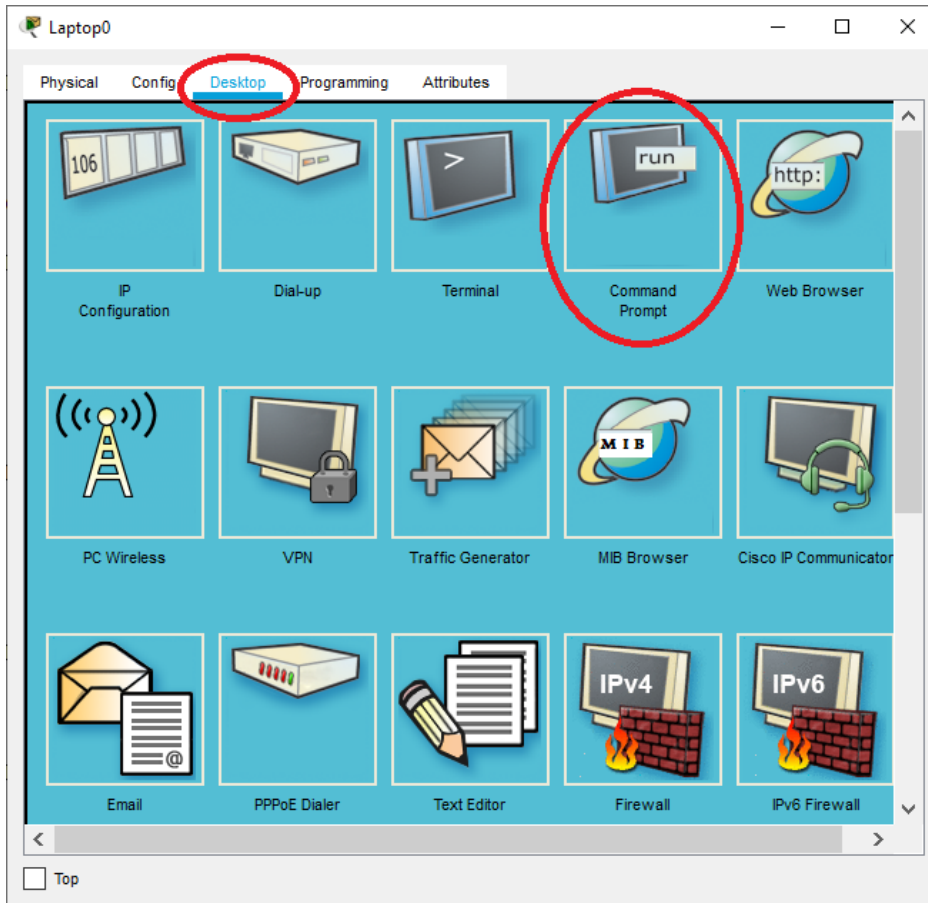
Add Save Remove

No.	Name	Type	Detail
-----	------	------	--------

DNS Cache

☐ Top

- 4) On the Admin laptop, open a Command Prompt and test the DNS entry using the 'nslookup' command. After a pause, it should resolve the name cisco-capwap-controller to 192.168.10.11. (Note that you cannot ping the WLC yet.)



```
C:\>nslookup cisco-capwap-controller
```

```
Server: [192.168.11.10]  
Address: 192.168.11.10
```

```
Non-authoritative answer:
```

```
Name: cisco-capwap-controller  
Address: 192.168.10.11
```

- 5) You will create a WLAN for Corporate users (staff members) later in this lab exercise. Create a new VLAN for the staff users on the multilayer switch. Use VLAN number 22 and name the VLAN 'Corporate'.

```
Switch(config)#vlan 22  
Switch(config-vlan)#name Corporate
```

- 6) Create a VLAN interface on the multilayer switch to be used as the default gateway for the Corporate VLAN. Use IP address 192.168.22.1/24

```
Switch(config)#interface vlan 22  
Switch(config-if)#ip address 192.168.22.1 255.255.255.0
```

- 7) You will also create a WLAN for guest users (non-staff members) later in this lab exercise. Create a new VLAN for the guest users. Use VLAN number 23 and name the VLAN 'Guest'.

```
Switch(config)#vlan 23  
Switch(config-vlan)#name Guest
```

- 8) Create a VLAN interface on the multilayer switch to be used as the default gateway for the Guest VLAN. Use IP address 192.168.23.1/24

```
Switch(config)#interface vlan 23  
Switch(config-if)#ip address 192.168.23.1 255.255.255.0
```

9) Verify you now have these VLANs and VLAN interfaces configured:

VLAN Name	VLAN Number	IP Subnet	Gateway (on switch)
Management	10	192.168.10.0/24	192.168.10.1
Server	11	192.168.11.0/24	192.168.11.1
Admin	21	192.168.21.0/24	192.168.21.1
Corporate	22	192.168.22.0/24	192.168.22.1
Guest	23	192.168.23.0/24	192.168.23.1

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Gig1/0/3, Gig1/0/4, Gig1/0/5, Gig1/0/8 Gig1/0/9, Gig1/0/10, Gig1/0/11, Gig1/0/12 Gig1/0/13, Gig1/0/14, Gig1/0/15, Gig1/0/16 Gig1/0/17, Gig1/0/18, Gig1/0/19, Gig1/0/20 Gig1/0/21, Gig1/0/22, Gig1/0/23, Gig1/0/24 Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
10 Management	active	
11 Server	active	Gig1/0/2
21 Admin	active	Gig1/0/1
22 Corporate	active	
23 Guest	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch#show ip interface brief | include Vlan
```

Vlan1	unassigned	YES unset	administratively down	down
Vlan10	192.168.10.1	YES manual	up	up
Vlan11	192.168.11.1	YES manual	up	up
Vlan21	192.168.21.1	YES manual	up	up
Vlan22	192.168.22.1	YES manual	up	up
Vlan23	192.168.23.1	YES manual	up	up

- 10) Port GigabitEthernet1/0/5 on the multilayer switch is connected to the WLC Wireless LAN Controller.
Configure the port to support the Corporate and Guest WLANs and management of the Wireless Access Points.
The spanning tree protocol should not check for possible layer 2 loops on the port.

The switchport connected to the WLC should be configured as a trunk which carries the AP management and WLAN traffic.

```
Switch(config)#interface GigabitEthernet1/0/5
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,22,23
Switch(config-if)#spanning-tree portfast trunk
```

Caution: The “switchport trunk encapsulation command” will be rejected on a C3650 switch, as discussed in Section 21 “VLAN Trunk Ports”. The C3650 switch supports only Dot1q encapsulation, there is no option to change it.

- 11) Port GigabitEthernet1/0/3 and GigabitEthernet1/0/4 on the multilayer switch are connected to the Lightweight Access Points.
Configure the ports to support the Corporate and Guest WLANs and management of the Wireless Access Points.
The spanning tree protocol should not check for possible layer 2 loops on the port.

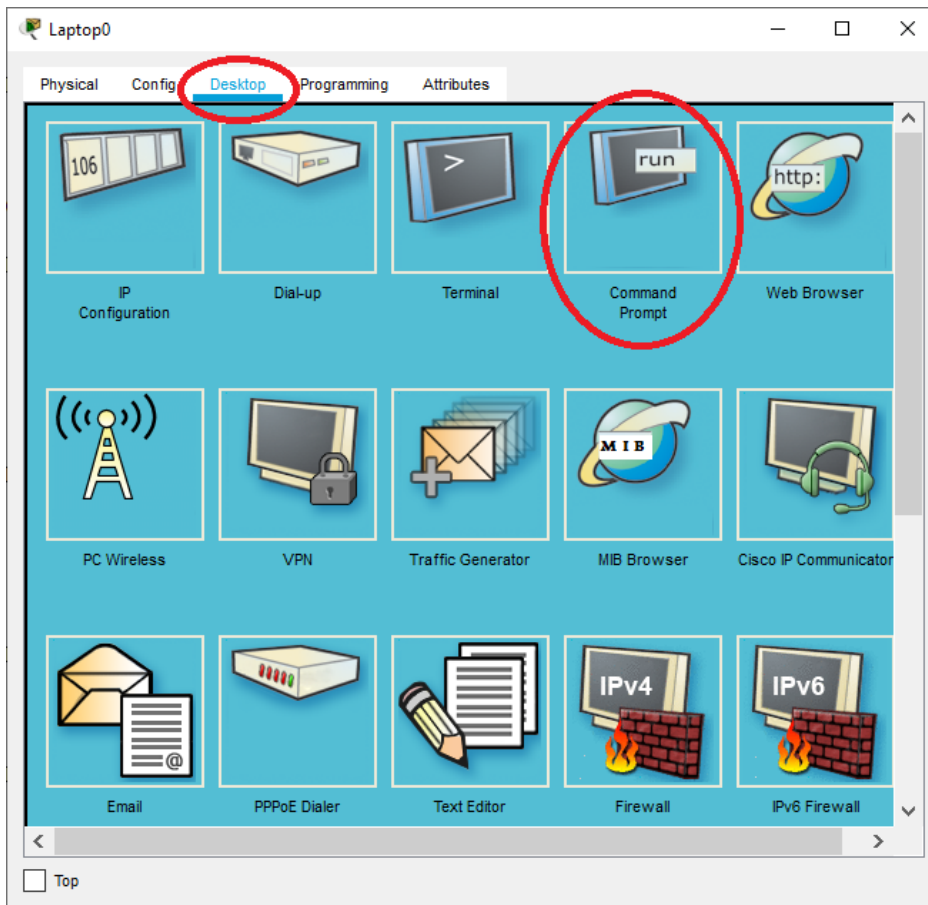
The switchports connected to the Access Points should be configured as access ports for the AP management VLAN. Traffic will be carried inside a CAPWAP tunnel to the WLC.

```
Switch(config)#interface range GigabitEthernet1/0/3 - 4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#spanning-tree portfast
```

Wireless LAN Controller and RADIUS Server Integration

12) Check you can ping the Wireless LAN Controller at 192.168.10.11 from the Admin laptop.

Open a command prompt on the Admin laptop.

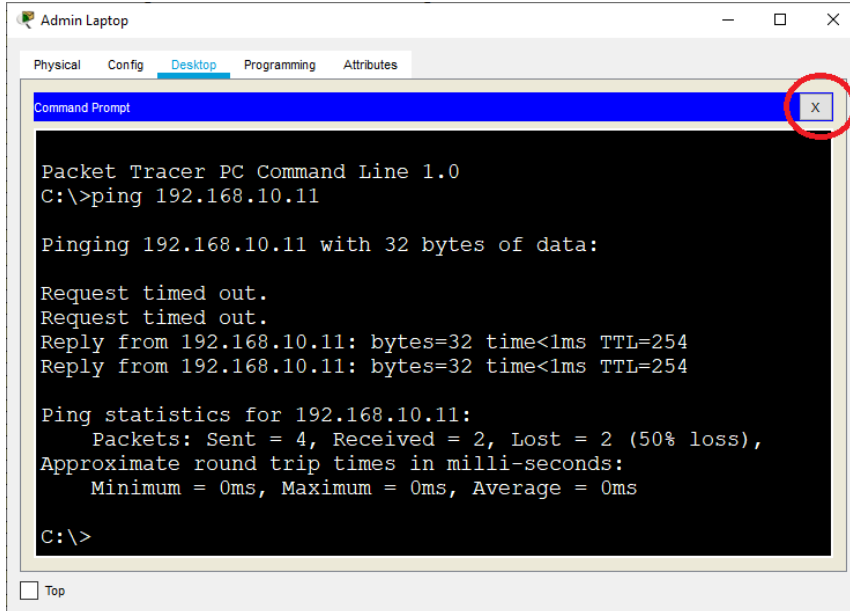


```
C:\>ping 192.168.10.11
Pinging 192.168.10.11 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Reply from 192.168.10.11: bytes=32 time<1ms TTL=254
Reply from 192.168.10.11: bytes=32 time<1ms TTL=254
```

```
Ping statistics for 192.168.10.11:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

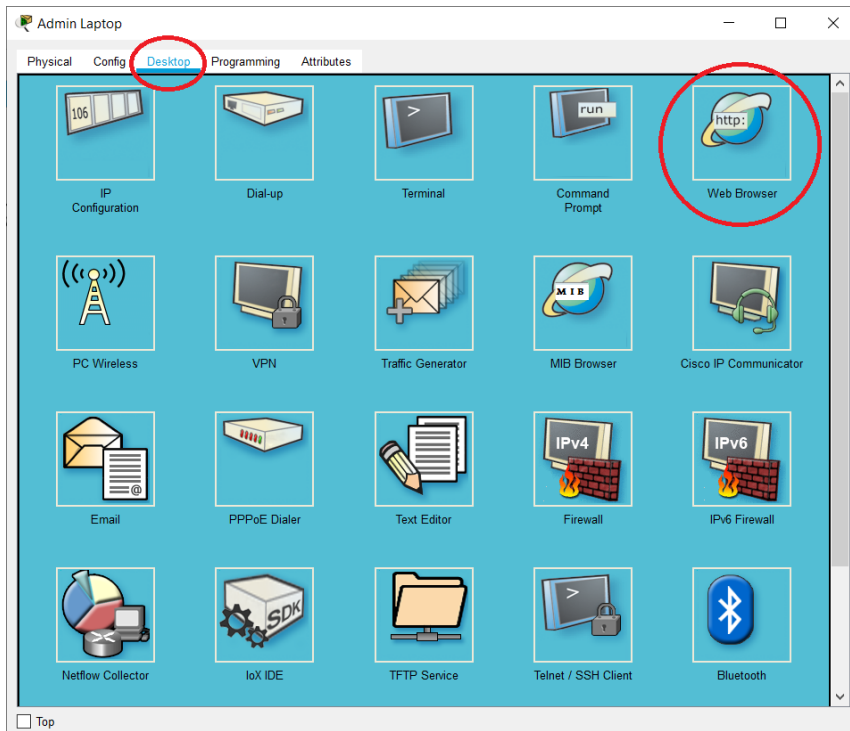
Close the command prompt window.

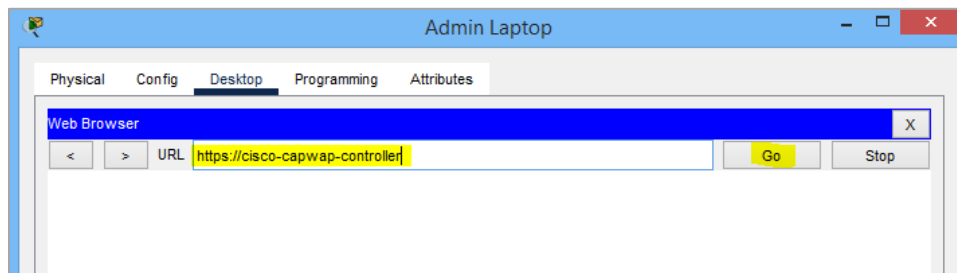


- 13) Open <https://cisco-capwap-controller> (use https, not http) in a web browser window on the Admin laptop to open the Wireless LAN Controller administration GUI.

Login with username **admin** and password **Flackbox1**

If you get a 'Host Name Unresolved' error message then close the web browser window, then reopen it and try again.






Authentication Required

User Name: admin

Password:

Login Cancel



Wireless LAN Controller

Welcome! Please click the login button to enter your user name and password

Login

© 2005 - 2017 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

- 14) On the dashboard Summary page and the Wireless page, verify the two Access Points have registered with the WLC. (You can ignore it if you see two extra APs, this is a Packet Tracer glitch.)

Admin Laptop

Physical Config Desktop Programming Attributes

Web Browser

URL: <https://cisco-capwap-controller/frameMonitor.html> Go Stop

Save Configuration Ping Logout Refresh

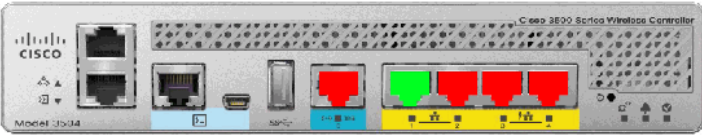
CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients
- Sleeping Clients
- Multicast
- Applications
- Local Profiling

Summary

150 Access Points Supported



Controller Summary

Management IP Address	192.168.10.11 , ::/128
Software Version	8.3.111.0
Field Recovery Image Version	7.6.101.1
System Name	WLC
Up Time	39 minutes, 36 seconds
System Time	Di Jan 17 01:32:05 2023
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/0%
Memory Usage	46%
Fan Status	3800 rpm

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Top WLANs

Profile Name	# of Clients
--------------	--------------

Most Recent Traps

[View All](#)

Top Applications

Application Name	Packet Count	Byte Count
------------------	--------------	------------

[View All](#)

Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	2	2	0	Detail
802.11b/g/n Radios	2	2	0	Detail
Dual-Band Radios	0	0	0	Detail
All APs	2	2	0	Detail

☐ Top

Admin Laptop

Physical Config Desktop Programming Attributes

Web Browser

URL: https://cisco-capwap-controller/frameWireless.html

Go Stop

Save Configuration Ping Logout Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

Wireless

Access Points

All APs

Radios

802.11a/n/ac

802.11b/g/n

Dual-Band Radios

Global Configuration

Advanced

Mesh

ATF

RF Profiles

FlexConnect Groups

FlexConnect ACLs

FlexConnect VLAN Templates

OEAP ACLs

Network Lists

802.11a/n/ac

802.11b/g/n

Media Stream

All APs

Entries 1 - 2 of 2

Current Filter [Change Filter] [Clear Filter]

Number of APs 2

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC
AP2	192.168.10.102	PT-AIR-CAP1000I-A-K9	00:01:C9:42:!!
AP1	192.168.10.101	PT-AIR-CAP1000I-A-K9	00:90:0C:5C:I

Top

- 15) Add the RADIUS AAA server at 192.168.11.10 to the Wireless LAN Controller.
Your colleague has already added the Wireless LAN Controller as a client on the RADIUS server with shared secret **Flackbox1**.

Click 'Security' > 'AAA' > 'RADIUS' > 'Authentication' then 'New'

The screenshot shows the Cisco WLC configuration interface. The 'Security' tab is selected in the top navigation bar. In the left sidebar, the 'Authentication' option under the 'RADIUS' section is highlighted. The main content area shows the 'RADIUS Authentication Servers' configuration page. At the top right of this page, the 'New...' button is highlighted. Below the configuration fields, there is a table with columns: Network User, Management, Server Index, Server Address(Ipv4/Ipv6), Port, IPsec, and Admin Status. The table is currently empty.

Enter the IP address 192.168.11.10 and password Flackbox1 for the RADIUS server then click 'Apply'.

The screenshot shows the Cisco Admin Laptop interface with the 'RADIUS Authentication Servers > New' configuration page. The 'Server IP Address' field is set to 192.168.11.10, and the 'Shared Secret' field is set to Flackbox1. The 'Apply' button is highlighted.

Web Browser: <https://cisco-capwap-controller/frameRadiusCreate.html>

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

Security > RADIUS Authentication Servers > New

Server Index (Priority): 1

Server IP Address(Ipv4/Ipv6): 192.168.11.10

Shared Secret Format: ASCII

Shared Secret: Flackbox1

Confirm Shared Secret: Flackbox1

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**

Verify the RADIUS server is added.

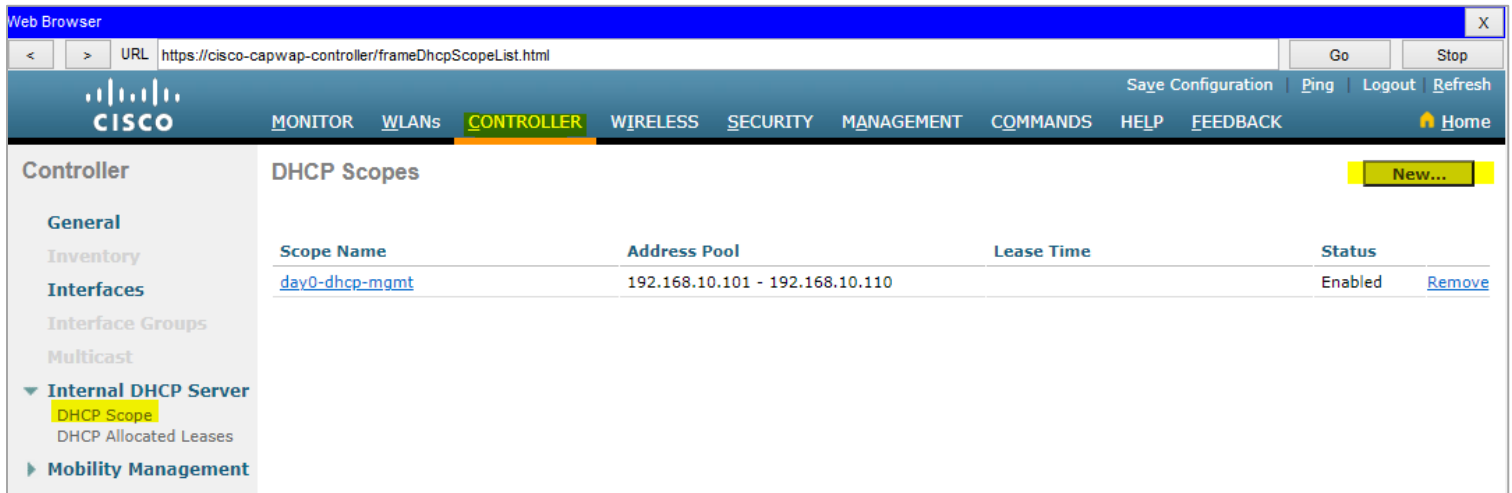
RADIUS Authentication Servers							Apply	New...
Auth Called Station ID Type		IP Address						
Use AES Key Wrap		<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)						
MAC Delimiter		Hyphen						
Framed MTU		1300						
Network User	Management	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	192.168.11.10	1812	Disabled	Enabled	Remove	

DHCP on Wireless LAN Controller

In Packet Tracer, the WLC automatically creates a DHCP scope with the name 'day0-dhcp-mgmt' which is used for the Lightweight Access Points to retrieve their IP address and DNS server info through the Zero Touch Provisioning process. On real hardware this DHCP scope will not exist by default.

- 16) Wireless DHCP clients can receive their IP address from an external DHCP server or from the Wireless LAN Controller.
Configure a DHCP scope on the WLC for Corporate wireless clients with the address range 192.168.22.101 to 192.168.22.254.
Configure a DNS server with IP address 192.168.11.10.
Enter all other relevant details.

Click 'Controller' > 'Internal DHCP Server' > 'DHCP Scope' then 'New'



Web Browser

URL: https://cisco-capwap-controller/frameDhcpScopeList.html

Go Stop

Save Configuration Ping Logout Refresh

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

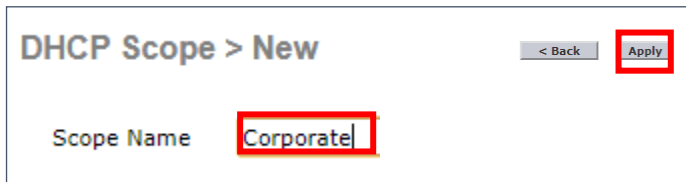
Controller

General
Inventory
Interfaces
Interface Groups
Multicast
▼ Internal DHCP Server
 DHCP Scope
 DHCP Allocated Leases
► Mobility Management

DHCP Scopes New...

Scope Name	Address Pool	Lease Time	Status
day0-dhcp-mgmt	192.168.10.101 - 192.168.10.110		Enabled Remove

Name the scope 'Corporate' then click 'Apply'.



DHCP Scope > New < Back Apply

Scope Name Corporate

Click on the Corporate DHCP scope to configure it.

Scope Name	Address Pool	Lease Time	Status
Corporate	0.0.0.0 - 0.0.0.0		Enabled Remove
day0-dhcp-mgmt	192.168.10.101 - 192.168.10.110		Enabled Remove

Enter the details then click 'Apply'

DHCP Scope > Edit

< BackApply

Scope Name	Corporate		
Pool Start Address	<input type="text" value="192.168.22.101"/>		
Pool End Address	<input type="text" value="192.168.22.254"/>		
Network	<input type="text" value="192.168.22.0"/>		
Netmask	<input type="text" value="255.255.255.0"/>		
Lease Time (seconds)	<input type="text" value="86400"/>		
Default Routers	<input type="text" value="192.168.22.1"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
DNS Domain Name	<input type="text" value="Not Supported"/>		
DNS Servers	<input type="text" value="192.168.11.10"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Netbios Name Servers	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Status	<input type="text" value="Enabled"/>		

- 17) Configure a DHCP scope on the WLC for Guest wireless clients with the address range 192.168.23.101 to 192.168.23.254.
Configure a DNS server with IP address 192.168.11.10.
Enter all other relevant details.

Click 'Controller' > 'Internal DHCP Server' > 'DHCP Scope' then 'New'

Web Browser

URL https://cisco-capwap-controller/frameDhcpScopeList.html

GoStop

CISCO

MONITORWLANSCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHELPFEEDBACK

Save ConfigurationPingLogoutRefreshHome

Controller

General

Inventory

Interfaces

Interface Groups

Multicast

Internal DHCP Server

DHCP Scope

DHCP Allocated Leases

Mobility Management

DHCP Scopes

New...

Scope Name	Address Pool	Lease Time	Status
Corporate	192.168.22.101 - 192.168.22.254		Enabled Remove
day0-dhcp-mgmt	192.168.10.101 - 192.168.10.110		Enabled Remove

Name the scope 'Guest' then click 'Apply'.

DHCP Scope > New

< BackApply

Scope NameGuest

Click on the Guest DHCP scope to configure it.

DHCP Scopes				New...
Scope Name	Address Pool	Lease Time	Status	
Guest	0.0.0.0 - 0.0.0.0		Enabled	Remove
Corporate	192.168.22.101 - 192.168.22.254		Enabled	Remove
day0-dhcp-mgmt	192.168.10.101 - 192.168.10.110		Enabled	Remove

Enter the details then click 'Apply'

DHCP Scope > Edit

< BackApply

Scope NameGuest

Pool Start Address192.168.23.101

Pool End Address192.168.23.254

Network192.168.23.0

Netmask255.255.255.0

Lease Time (seconds)86400

Default Routers192.168.23.10.0.0.00.0.0.0

DNS Domain NameNot Supported

DNS Servers192.168.11.100.0.0.00.0.0.0

Netbios Name Servers0.0.0.00.0.0.00.0.0.0

StatusEnabled

Verify all scopes are enabled.

DHCP Scopes				New...
Scope Name	Address Pool	Lease Time	Status	
Guest	192.168.23.101 - 192.168.23.254		Enabled	Remove
Corporate	192.168.22.101 - 192.168.22.254		Enabled	Remove
day0-dhcp-mgmt	192.168.10.101 - 192.168.10.110		Enabled	Remove

Logical Interfaces on the Wireless LAN Controller

The management interface is preconfigured to be untagged because the Packet Tracer WLC does not support trunk ports.

Admin Laptop

Physical Config **Desktop** Programming Attributes

Web Browser

< > URL <https://cisco-capwap-controller/frameInterfaceList.html>

CISCO MONITOR WLANS **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Controller

General
Inventory
Interfaces
Interface Groups
Multicast

Interfaces

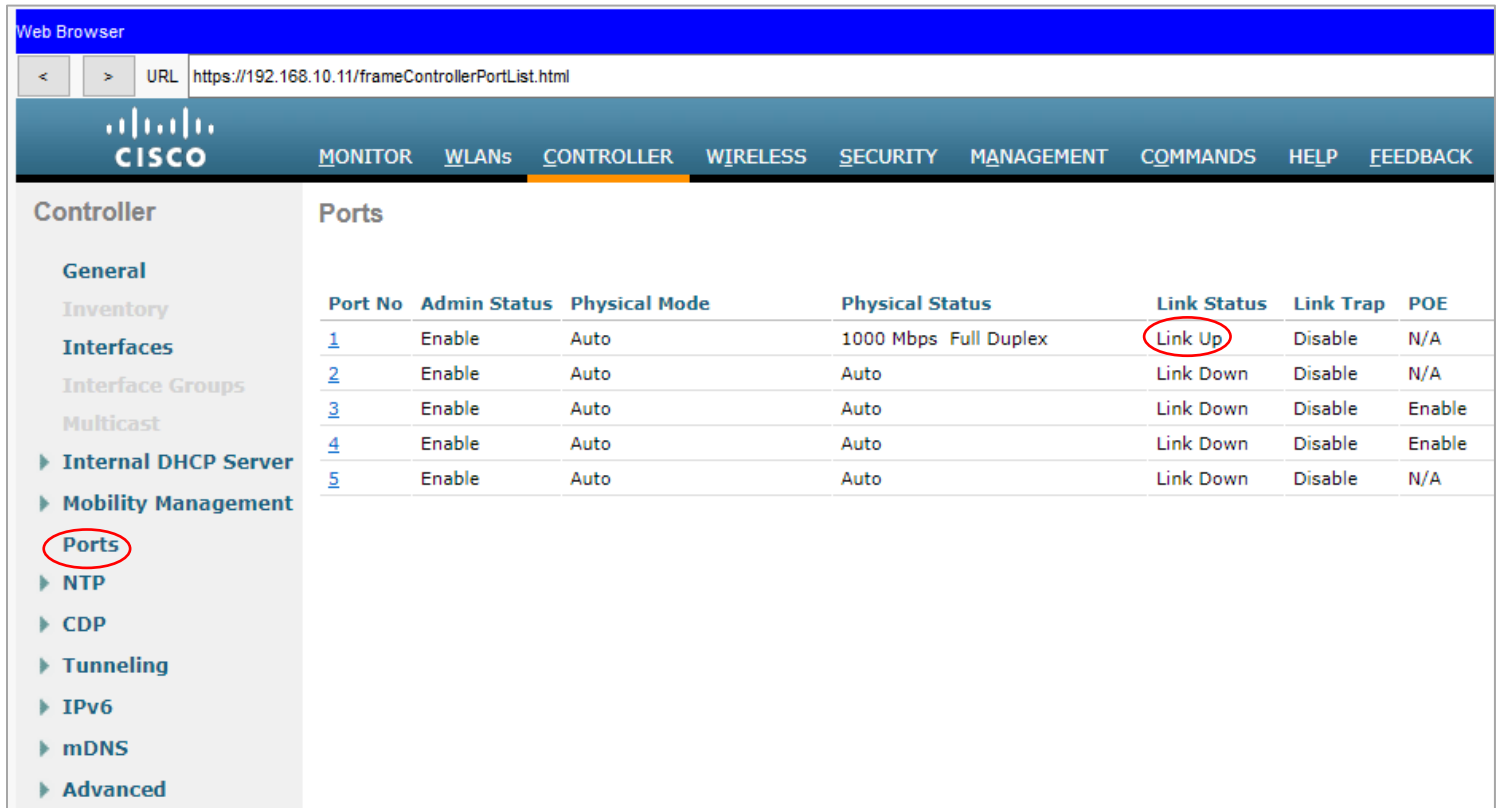
Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	192.168.10.11	Static	Enabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

On the Multilayer switch the native VLAN for the port is already set to the management VLAN 10.

```
Switch#show run
! truncated
interface GigabitEthernet1/0/5
description WLC
switchport trunk native vlan 10
switchport trunk allowed vlan 10,22-23
switchport trunk encapsulation dot1q
switchport mode trunk
spanning-tree portfast trunk
```

- 18) Create a logical interface on the Wireless LAN Controller in the Corporate VLAN, with IP address 192.168.22.11 and gateway 192.168.22.1.
Wireless clients on the Corporate VLAN should get an IP address from the management interface of the Wireless LAN Controller.

Click 'Ports' to check which physical interface is connected to the switch.



Web Browser

URL: https://192.168.10.11/frameControllerPortList.html

CISCO

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

Controller

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Internal DHCP Server
- Mobility Management
- Ports**
- NTP
- CDP
- Tunneling
- IPv6
- mDNS
- Advanced

Ports

Port No	Admin Status	Physical Mode	Physical Status	Link Status	Link Trap	POE
1	Enable	Auto	1000 Mbps Full Duplex	Link Up	Disable	N/A
2	Enable	Auto	Auto	Link Down	Disable	N/A
3	Enable	Auto	Auto	Link Down	Disable	Enable
4	Enable	Auto	Auto	Link Down	Disable	Enable
5	Enable	Auto	Auto	Link Down	Disable	N/A

Port 1 is connected.

Click 'Controller' > 'Interfaces' then 'New'



Web Browser

URL: https://cisco-capwap-controller/frameinterfaceList.html

CISCO

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

Controller

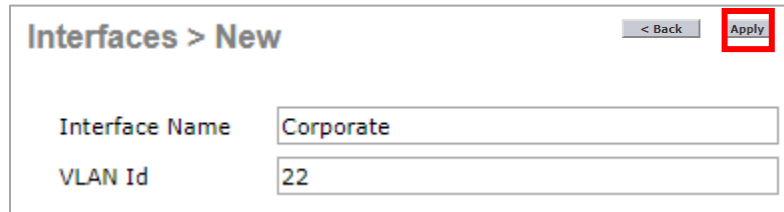
- General
- Inventory
- Interfaces**
- Interface Groups
- Multicast
- Internal DHCP Server

Interfaces

Entries 1 - 2 of 2 [New...](#)

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

Enter Interface Name 'Corporate' and VLAN ID '22' then click 'Apply'

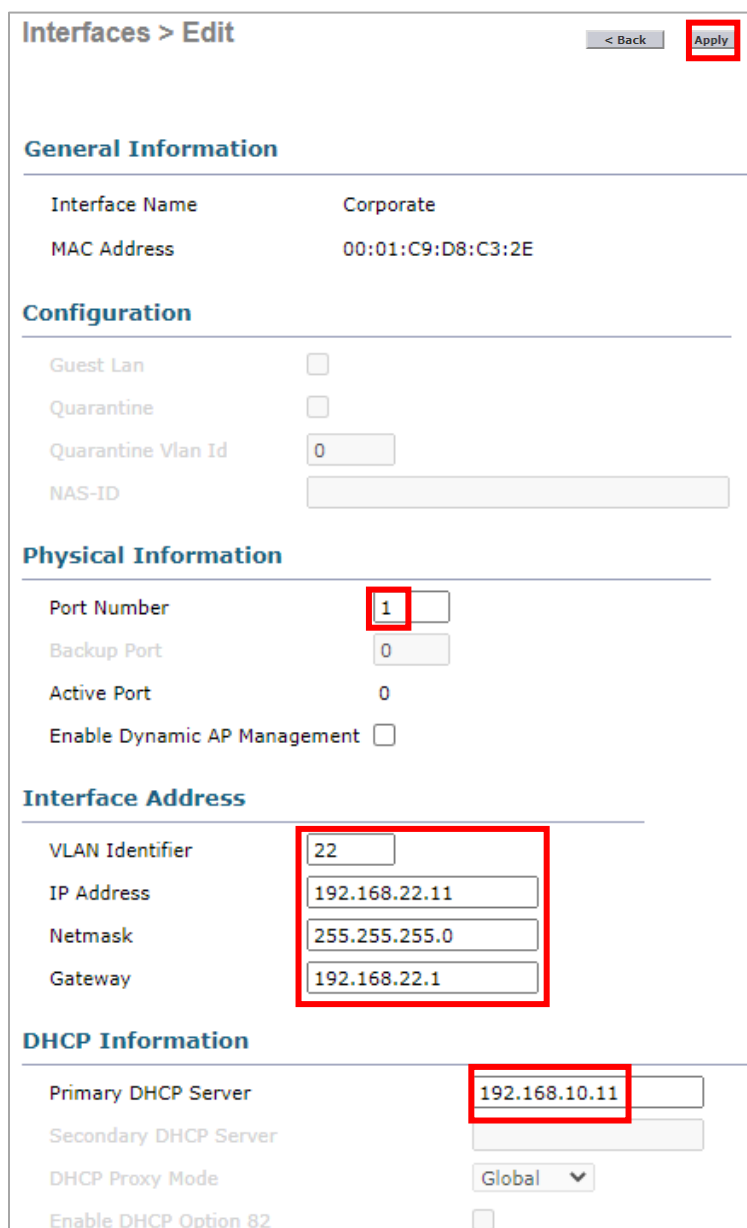


Interfaces > New < Back Apply

Interface Name

VLAN Id

Enter the details for the VLAN interface. It should be associated with Port Number 1, and the 192.168.10.11 management address of the WLC should be configured as the DHCP server.



Interfaces > Edit < Back Apply

General Information

Interface Name Corporate

MAC Address 00:01:C9:D8:C3:2E

Configuration

Guest Lan ☐

Quarantine ☐

Quarantine Vlan Id

NAS-ID

Physical Information

Port Number

Backup Port

Active Port 0

Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

DHCP Information

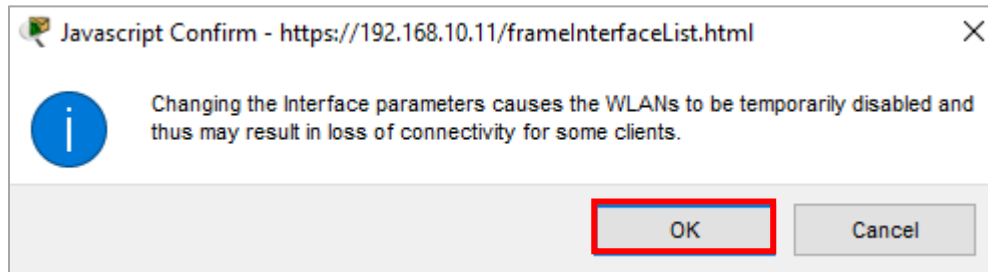
Primary DHCP Server

Secondary DHCP Server

DHCP Proxy Mode Global ▼

Enable DHCP Option 82 ☐

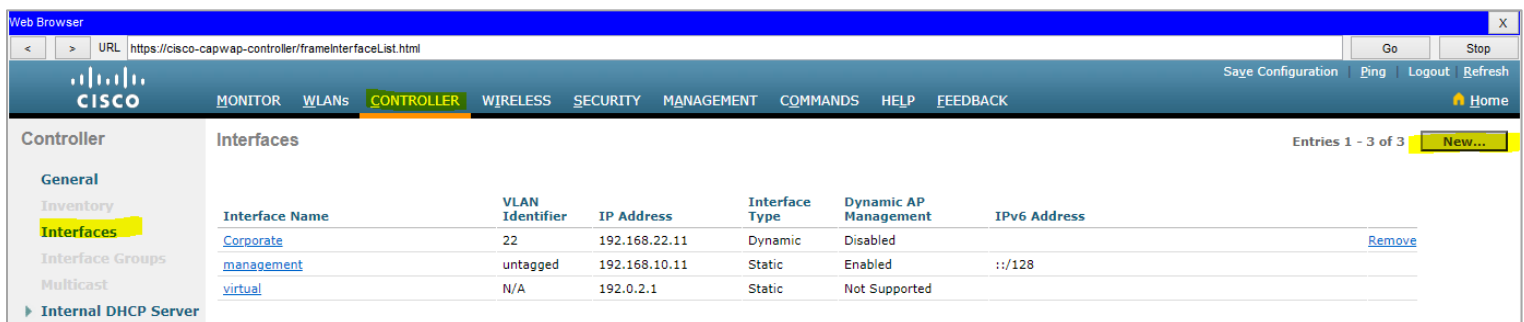
Click on Apply and then on 'OK' on the warning message. No wireless clients are connected yet so there will be no disruption.



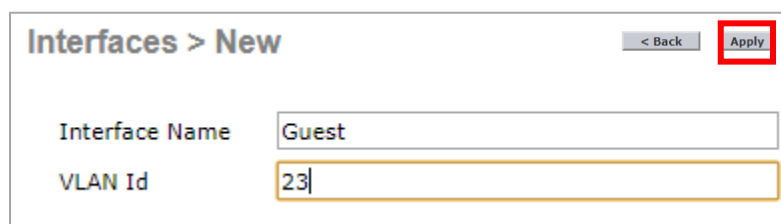
Go back to the interfaces page.

- 19) Create a logical interface in the Guest VLAN with IP address 192.168.23.11 and gateway 192.168.23.1.
Wireless clients on the Guest VLAN should get an IP address from the management interface of the Wireless LAN Controller.

Click 'Controller' > 'Interfaces' then 'New'



Enter Interface Name 'Guest' and VLAN ID '23' then click 'Apply'

A form titled "Interfaces > New". It has a "< Back" button and an "Apply" button (highlighted with a red rectangle). The form contains two input fields: "Interface Name" with the value "Guest" and "VLAN Id" with the value "23".

Enter the details for the VLAN interface. It should be associated with Port Number 1, and the 192.168.10.11 management address of the WLC should be configured as the DHCP server.

Interfaces > Edit

< BackApply

General Information

Interface Name	Guest
MAC Address	00:04:9A:A2:80:2D

Configuration

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	

Physical Information

Port Number	1
Backup Port	0
Active Port	0
Enable Dynamic AP Management	<input type="checkbox"/>

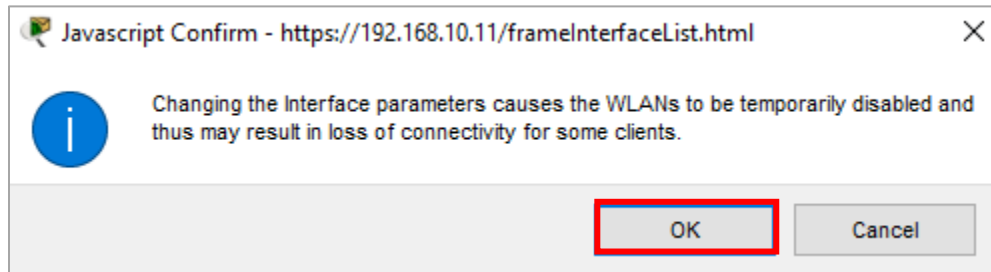
Interface Address

VLAN Identifier	23
IP Address	192.168.23.11
Netmask	255.255.255.0
Gateway	192.168.23.1

DHCP Information

Primary DHCP Server	192.168.10.11
Secondary DHCP Server	
DHCP Proxy Mode	Global
Enable DHCP Option 82	<input type="checkbox"/>

Click on Apply and then on 'OK' on the warning message. No wireless clients are connected yet so there will be no disruption.



Verify both interfaces have been created.

Interfaces				
Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
Corporate	22	192.168.22.11	Dynamic	Disabled
Guest	23	192.168.23.11	Dynamic	Disabled
management	untagged	192.168.10.11	Static	Enabled
virtual	N/A	192.0.2.1	Static	Not Supported

Wireless LANs

- 20) Create the wireless LAN named 'Corporate'. Clients should be authenticated by the 192.168.10.11 RADIUS server you added earlier, and WPA2 AES encryption should be used.

Click on 'WLANs', select 'Create New' in the drop-down then click 'Go'

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

CISCO

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

WLANs

▼ WLANs
WLANs

▼ Advanced
AP Groups

WLANs

Current Filter: [Change Filter] [Clear Filter]

Create New Go

WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies

Enter the details then click 'Apply'

WLANs > New

< Back Apply

Type WLAN ▼

Profile Name Corporate

SSID Corporate

ID 1 ▼

Associate the WLAN with the 'Corporate' interface. Do not enable the status as you haven't configured the security settings yet. Click 'Apply'.

WLANs > Edit 'Corporate'

< BackApply

GeneralSecurityQoSPolicy-MappingAdvanced

Profile NameCorporate

TypeWLAN

SSIDCorporate

☐ Enabled

Security PoliciesNone
(Modifications done under security tab will appear after applying the changes.)

Radio PolicyAll

Interface/Interface Group(G)Corporate

Multicast Vlan Feature☐ Enabled

Broadcast SSID☒ Enabled

NAS-ID

Click on the 'Security' tab and ensure Layer 2 Security is 'WPA + WPA2', the WPA2 Policy is applied with AES encryption, and Authentication Key Management is 802.1X then click 'Apply'.

WLANs > Edit 'Corporate' [< Back](#) [Apply](#)

General **Security** **QoS** **Policy-Mapping** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Layer 2 Security [6](#) WPA+WPA2 ▼

MAC Filtering [9](#) ☐

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled ▼

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☒

WPA2 Encryption ☒ AES ☐ TKIP

Authentication Key Management

802.1X ☒ Enable

CCKM ☐ Enable

PSK ☐ Enable

Click on the 'Security' then 'AAA Servers' tabs, select the RADIUS server you added earlier 'IP:192.168.10.11, Port:1812' as Server 1, and click 'Apply'.

WLANs > Edit 'Corporate' < Back Apply

General **Security** **QoS** **Policy-Mapping** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface ☐ Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	<input checked="" type="checkbox"/> Enabled IP:192.168.11.10, Port:1812 ▼	<input type="checkbox"/> Enabled None ▼	Enable <input type="checkbox"/>
Server 2	None ▼	None ▼	
Server 3	None ▼	None ▼	
Server 4	None ▼	None ▼	
Server 5	None ▼	None ▼	
Server 6	None ▼	None ▼	

On the 'General' tab, tick the 'Enabled' checkbox to enable the WLAN and click 'Apply'.

WLANs > Edit 'Corporate'

< Back **Apply**

General Security QoS Policy-Mapping Advanced

Profile Name

Type

SSID

Status ☒ Enabled

Security Policies **[WPA2][Auth(802.1X)]**
(Modifications done under security tab will appear after applying the changes.)

Radio Policy

Interface/Interface Group(G)

Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☒ Enabled

NAS-ID

21) Create the wireless LAN named 'Guest'. WPA2 AES encryption should be used, and clients should authenticate with the pre-shared key **Flackbox3**.

Click on 'WLANs', select 'Create New' in the drop-down then click 'Go'

Web Browser

< > URL <https://192.168.10.11/frameWlan.html>

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

WLANs

▼ WLANs
WLANs
▼ Advanced
AP Groups

WLANs

Current Filter: [\[Change Filter\]](#) [\[Clear Filter\]](#) **Create New** **Go**

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
<input type="checkbox"/>	1	WLAN	Corporate	Corporate	Disabled	[WPA2][Auth(802.1X)]	Remove

Enter the details then click 'Apply'

WLANs > New < Back Apply

Type	WLAN ▼
Profile Name	Guest
SSID	Guest
ID	2 ▼

Associate the WLAN with the 'Guest' interface and click 'Apply'. Do not enable the status as you haven't configured the security settings yet.

WLANs > Edit 'Guest' < Back Apply

General **Security** **QoS** **Policy-Mapping** **Advanced**

Profile Name	Guest
Type	WLAN
SSID	Guest
Status	<input type="checkbox"/> Enabled
Security Policies	None (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All ▼
Interface/Interface Group(G)	Guest ▼
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	

Click on the 'Security' tab and ensure Layer 2 Security is 'WPA + WPA2', the WPA2 Policy is applied with AES encryption, Authentication Key Management is PSK and enter the pre-shared key **Flackbox3**, then click 'Apply'. You may need to scroll down to see the field to enter the pre-shared key in.

The screenshot shows the 'WLANs > Edit 'Guest'' configuration page. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Fast Transition' section has 'Fast Transition' disabled. The 'Protected Management Frame' section has 'PMF' set to 'Disabled'. The 'WPA+WPA2 Parameters' section shows 'WPA Policy' disabled, 'WPA2 Policy' checked, 'WPA2 Encryption' set to 'AES' (checked), and 'TKIP' disabled. The 'Authentication Key Management' section shows '802.1X', 'CCKM', 'FT 802.1X', and 'FT PSK' all disabled, while 'PSK' is checked and enabled. The 'PSK Format' is set to 'ASCII', and the 'PSK' field contains the pre-shared key 'Flackbox3' (represented by dots).

WLANs > Edit 'Guest' < Back Apply

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☒

WPA2 Encryption ☒ AES ☐ TKIP

Authentication Key Management

802.1X ☐ Enable

CCKM ☐ Enable

PSK ☒ Enable

FT 802.1X ☐ Enable

FT PSK ☐ Enable

PSK Format ASCII

PSK

On the 'General' tab, tick the 'Enabled' checkbox to enable the WLAN and click 'Apply'.

WLANs > Edit 'Guest' [< Back](#) [Apply](#)

General Security QoS Policy-Mapping Advanced

Profile Name

Type

SSID

Status ☒ Enabled

Security Policies **[WPA2][Auth(PSK)]**
(Modifications done under security tab will appear after applying the changes.)

Radio Policy

Interface/Interface Group(G)

Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☒ Enabled

NAS-ID

Click 'WLANs' to verify both WLANs are enabled.

Web Browser

URL: https://192.168.10.11/frameWlan.html

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

WLANs

▼ **WLANs**
WLANs

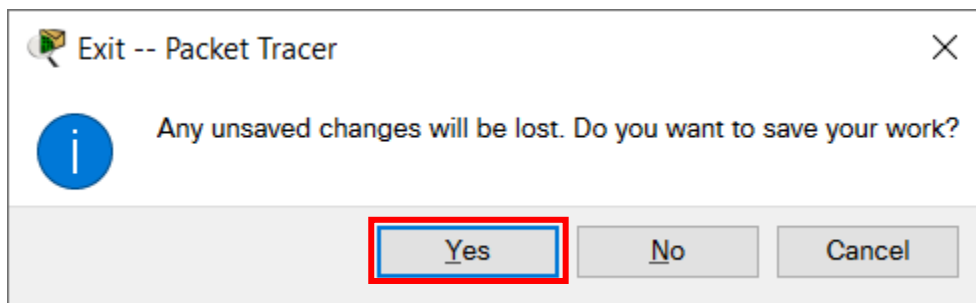
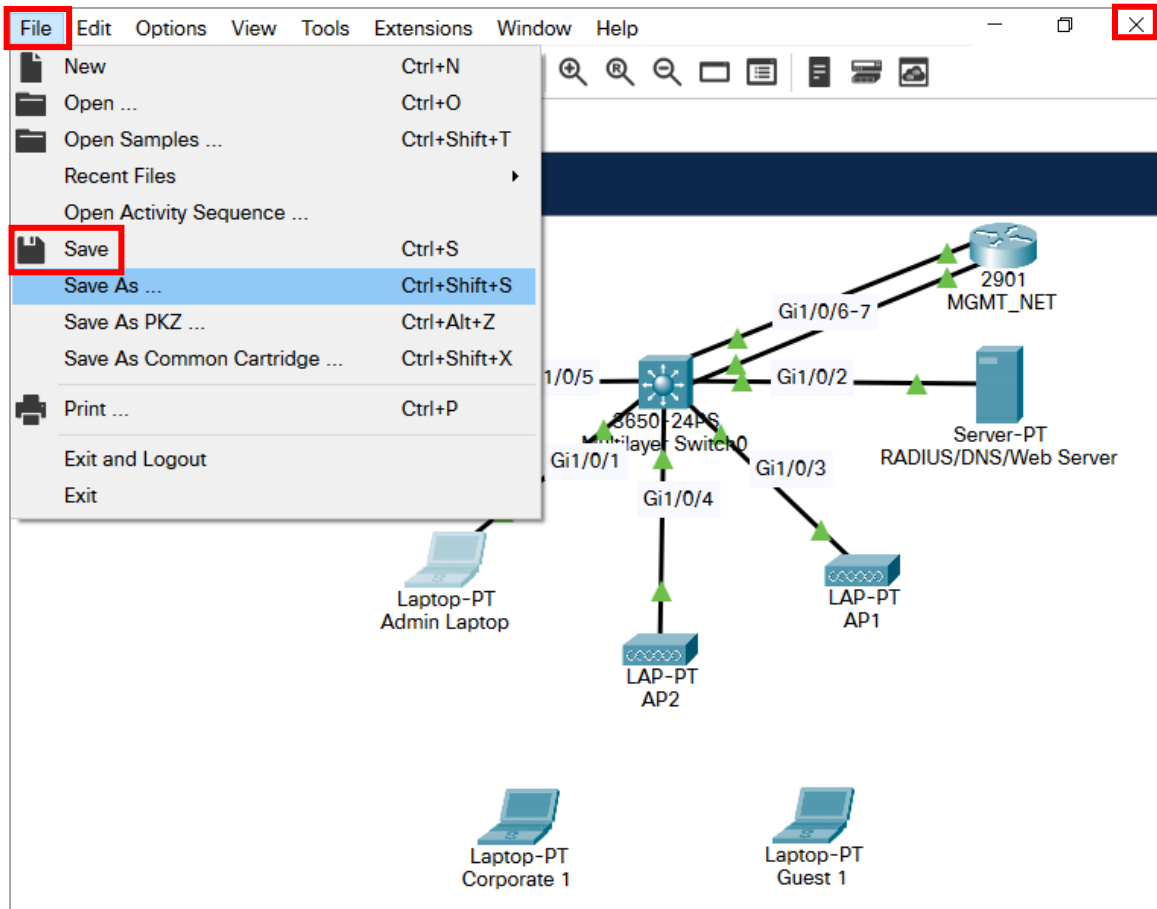
▼ **Advanced**
AP Groups

WLANs

Current Filter: [\[Change Filter\]](#) [\[Clear Filter\]](#) Create New

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
<input type="checkbox"/>	1	WLAN	Corporate	Corporate	Enabled	[WPA2][Auth(802.1X)]	Remove
<input type="checkbox"/>	2	WLAN	Guest	Guest	Enabled	[WPA2][Auth(PSK)]	Remove

22) Save the configuration of the Wireless LAN Controller Packet Tracer lab, close Packet Tracer, and then open the lab exercise again. (Otherwise the WLAN clients will probably get no IP from their DHCP server.)



Join Clients to the Wireless LANs

23) A username **Flackbox** with password **Flackbox2** has been configured on the RADIUS server.

Connect to the 'Corporate' WLAN from the Corporate1 laptop using this username.

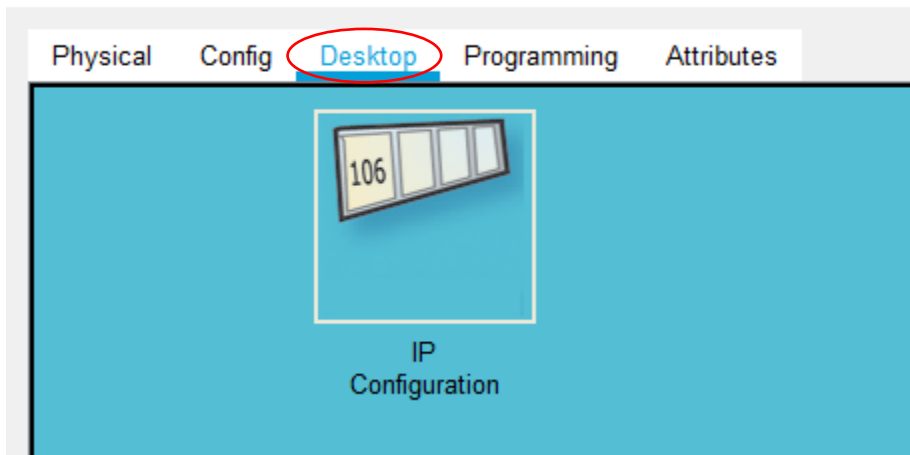
Click on the Corporate1 laptop in the Packet Tracer main window, then 'Config' and 'Wireless0'. Enter the SSID 'Corporate', select WPA2 authentication then enter the user ID Flackbox and password Flackbox2. Do not change the encryption type, it's AES by default.

The screenshot shows the configuration window for the Corporate1 laptop in Packet Tracer. The 'Config' tab is selected, and the 'Wireless0' interface is highlighted in the left sidebar. The configuration details are as follows:

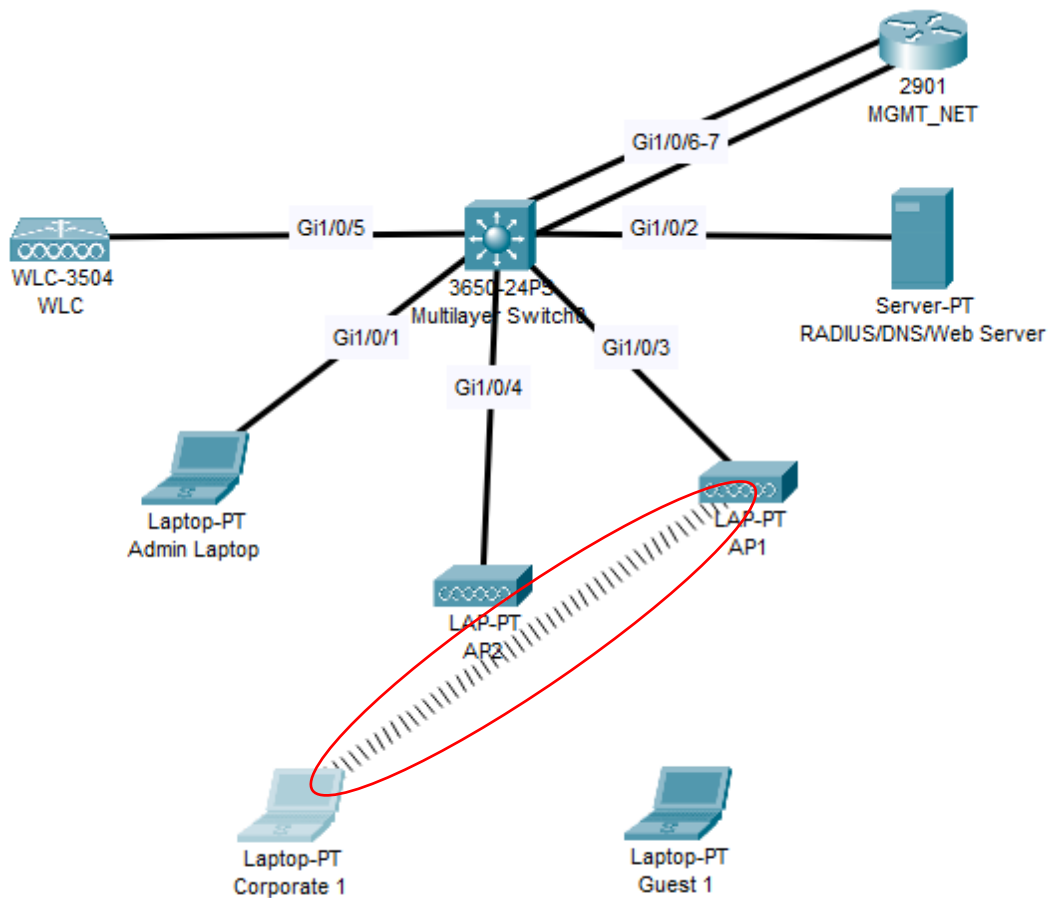
Wireless0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	11 Mbps
MAC Address	00D0.BAA5.C193
SSID	Corporate
Authentication	
<input type="radio"/> Disabled	<input type="radio"/> WEP
<input type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK
<input type="radio"/> WPA	<input checked="" type="radio"/> WPA2
<input type="radio"/> 802.1X	Method: MD5
WEP Key	
PSK Pass Phrase	
User ID	Flackbox
Password	Flackbox2
User Name	
Password	
Encryption Type	AES
IP Configuration	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static	
IPv4 Address	192.168.22.101
Subnet Mask	255.255.255.0
IPv6 Configuration	
<input type="radio"/> Automatic	
<input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::2D0:BAFF:FEA5:C193

Click out of the 'Config' tab to ensure the changes take effect.

Corporate 1



Verify the laptop connects in the Packet Tracer main window.



24) Connect to the 'Guest' WLAN from the Guest1 laptop.

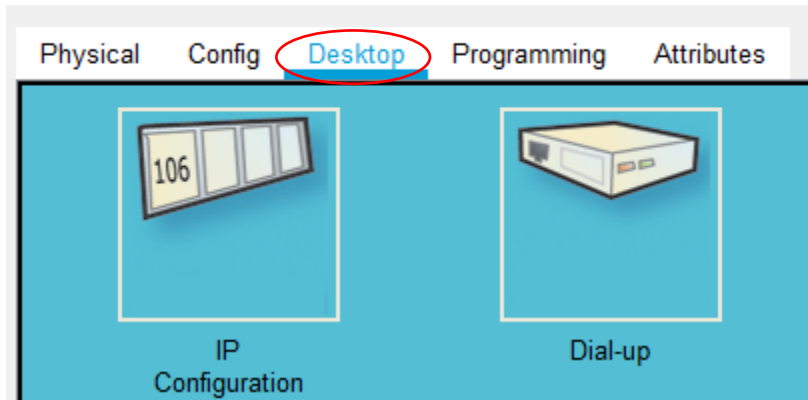
Click on the Guest1 laptop in the Packet Tracer main window, then 'Config' and 'Wireless0'. Enter the SSID 'Guest', select WPA2-PSK authentication then enter the pre-shared key **Flackbox3**. Do not change the encryption type, it's AES by default.

The screenshot shows the configuration window for 'Guest 1' in Packet Tracer. The 'Config' tab is selected, and the 'Wireless0' interface is highlighted in the left sidebar. The main configuration area is divided into several sections:

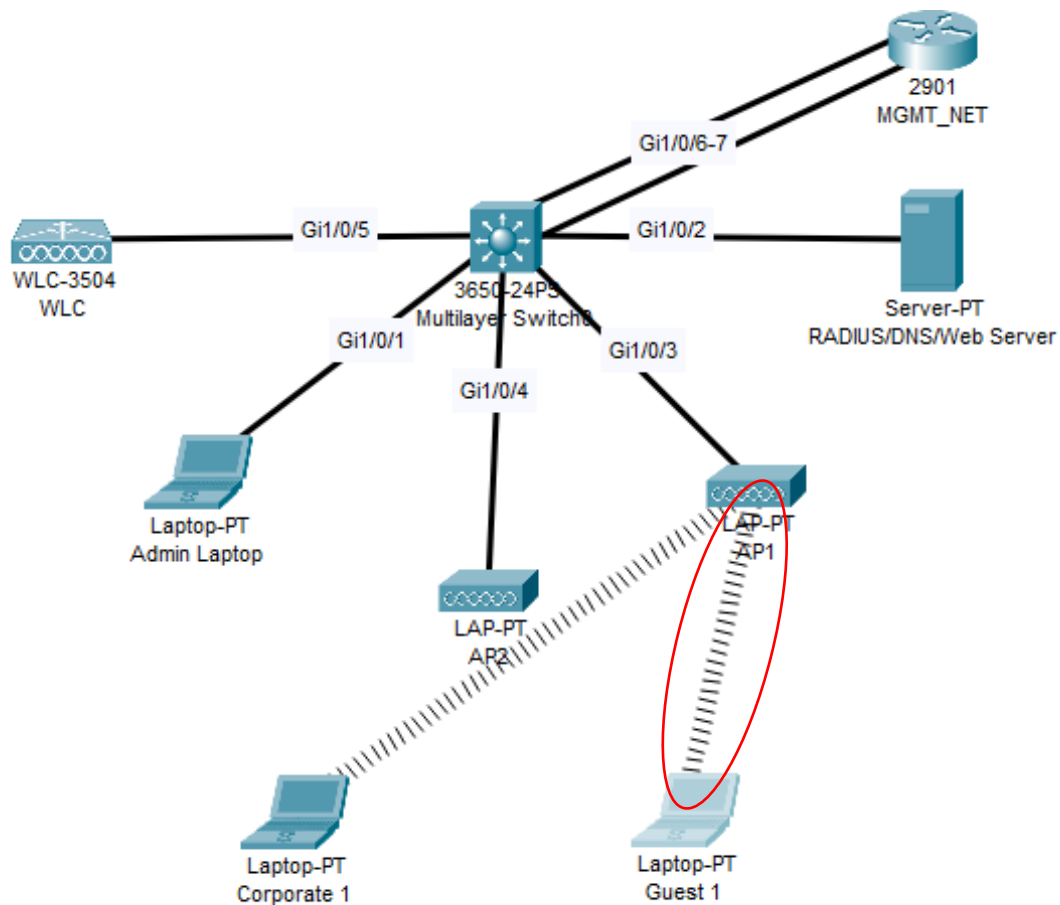
- Wireless0** (Interface Name)
- Port Status**: ☒ On
- Bandwidth**: 11 Mbps
- MAC Address**: 0040.0BE2.6AC4
- SSID**: Guest
- Authentication**:
 - ☐ Disabled
 - ☐ WEP
 - ☒ WPA2-PSK
 - ☐ WPA
 - ☐ WPA2
 - ☐ 802.1X
- WEP Key**: (Empty field)
- PSK Pass Phrase**: Flackbox3
- User ID**: (Empty field)
- Password**: (Empty field)
- Method**: MD5
- User Name**: (Empty field)
- Password**: (Empty field)
- Encryption Type**: AES
- IP Configuration**:
 - ☒ DHCP
 - ☐ Static
- IPv4 Address**: 192.168.23.101
- Subnet Mask**: 255.255.255.0
- IPv6 Configuration**:
 - ☐ Automatic
 - ☒ Static
- IPv6 Address**: (Empty field)
- Link Local Address**: FE80::240:BFF:FEE2:6AC4

Click out of the 'Config' tab to ensure the changes take effect.

Guest 1

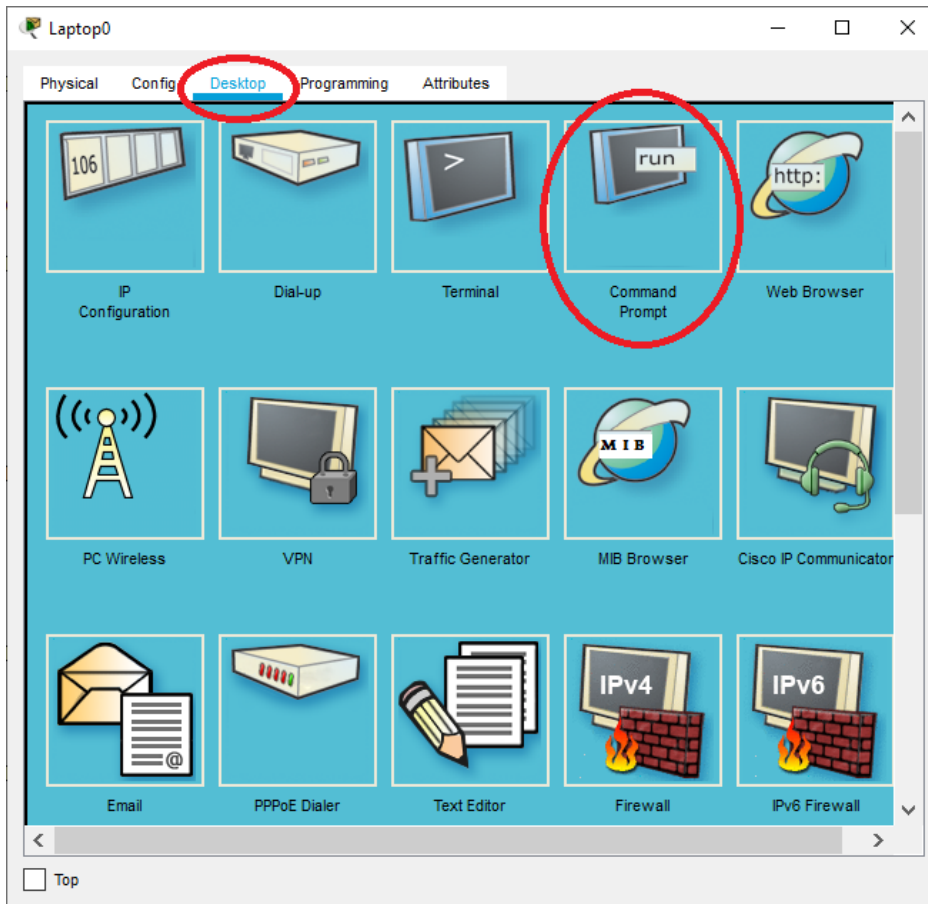


Verify the laptop connects in the Packet Tracer main window.



25) Verify connectivity by pinging the Corporate1 laptop from the Guest1 laptop.

Open a Command Prompt on the Corporate1 laptop then enter the command 'ipconfig' to check its IP address.



```
C:\>ipconfig
```

```
Wireless0 Connection:(default port)
```

```
Connection-specific DNS Suffix...:
```

```
Link-local IPv6 Address.....: FE80::230:A3FF:FE30:3DEE
```

```
IPv6 Address.....: ::
```

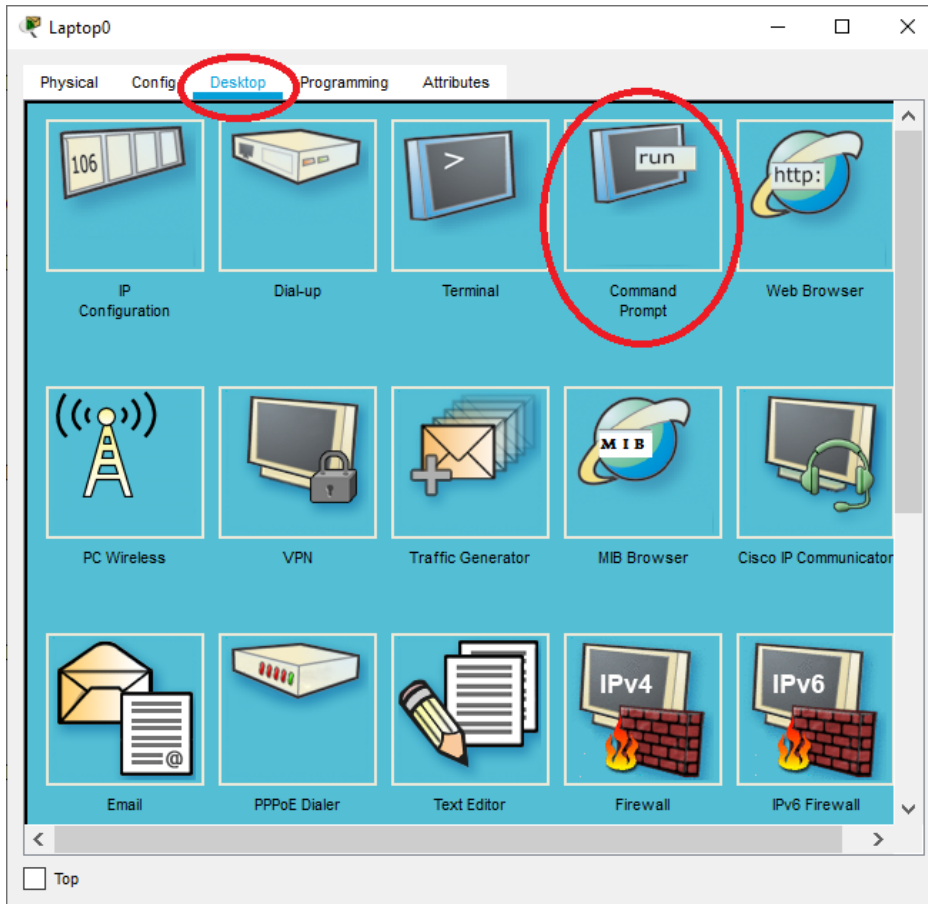
```
IPv4 Address.....: 192.168.22.101
```

```
Subnet Mask.....: 255.255.255.0
```

```
Default Gateway.....: ::
```

```
192.168.22.1
```

Open a Command Prompt on the Guest1 laptop then ping Corporate1.



```
C:\>ping 192.168.22.101
```

Pinging 192.168.22.101 with 32 bytes of data:

```
Reply from 192.168.22.101: bytes=32 time=35ms TTL=127
Reply from 192.168.22.101: bytes=32 time=39ms TTL=127
Reply from 192.168.22.101: bytes=32 time=16ms TTL=127
Reply from 192.168.22.101: bytes=32 time=31ms TTL=127
Reply from 192.168.22.101: bytes=32 time=22ms TTL=127
```

Ping statistics for 192.168.22.101:

```
Packets: Sent = 4, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 39ms, Average = 28ms
```