

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 192.168.10.11/24

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.

Note: Packet Tracer does not support a trunk port to the WLC so you will configure the VLAN information on 'dummy' ports on the switch. The devices are really connected to interfaces GigabitEthernet1/0/11 – 15. Do not change this.

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) Create a DHCP scope on the multilayer switch to allocate IP addresses to Wireless Access Points on the Management VLAN.
Use an address range of 192.168.10.101 to 192.168.10.254.
The default gateway is 192.168.10.1 and the Wireless APs should learn the address of the Wireless LAN Controller.
(A DNS server is not required in this lab environment.)

```
Switch(config)#ip dhcp excluded-address 192.168.10.1  
192.168.10.100  
Switch(config)#ip dhcp pool Management  
Switch(dhcp-config)# network 192.168.10.0 255.255.255.0  
Switch(dhcp-config)# default-router 192.168.10.1  
Switch(dhcp-config)# option 43 ip 192.168.10.11
```

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

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

- 5) 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
```

- 6) 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
```

- 7) 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
```

- 8) Verify you now have these VLANs and VLAN interfaces configured (do not worry about the VLAN interface status being up/down, that is expected in this lab environment):

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

VLAN	Name	Status	Ports
1	default	active	Gig1/0/3, Gig1/0/4, Gig1/0/5, Gig1/0/6 Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10 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	Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14 Gig1/0/15
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
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1/0/1	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/2	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/3	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/4	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/5	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/6	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/7	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/8	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/9	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/10	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/11	unassigned	YES	NVRAM	up	up
GigabitEthernet1/0/12	unassigned	YES	NVRAM	up	up
GigabitEthernet1/0/13	unassigned	YES	NVRAM	up	up
GigabitEthernet1/0/14	unassigned	YES	NVRAM	up	up
GigabitEthernet1/0/15	unassigned	YES	NVRAM	up	up
GigabitEthernet1/0/16	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/17	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/18	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/19	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/20	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/21	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/22	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/23	unassigned	YES	NVRAM	down	down
GigabitEthernet1/0/24	unassigned	YES	NVRAM	down	down
GigabitEthernet1/1/1	unassigned	YES	NVRAM	down	down
GigabitEthernet1/1/2	unassigned	YES	NVRAM	down	down
GigabitEthernet1/1/3	unassigned	YES	NVRAM	down	down
GigabitEthernet1/1/4	unassigned	YES	NVRAM	down	down
Vlan1	unassigned	YES	unset	administratively down	down
Vlan10	192.168.10.1	YES	manual	up	up
Vlan11	192.168.11.1	YES	manual	up	down
Vlan22	192.168.22.1	YES	manual	up	down
Vlan23	192.168.23.1	YES	manual	up	down

- 9) Port GigabitEthernet1/0/5 on the multilayer switch is connected to the Wireless LAN Controller.
 Configure the switchport 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
```

- 10) Port GigabitEthernet1/0/3 and GigabitEthernet1/0/4 on the multilayer switch are connected to the Lightweight Access Points.
Configure the switchports 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.

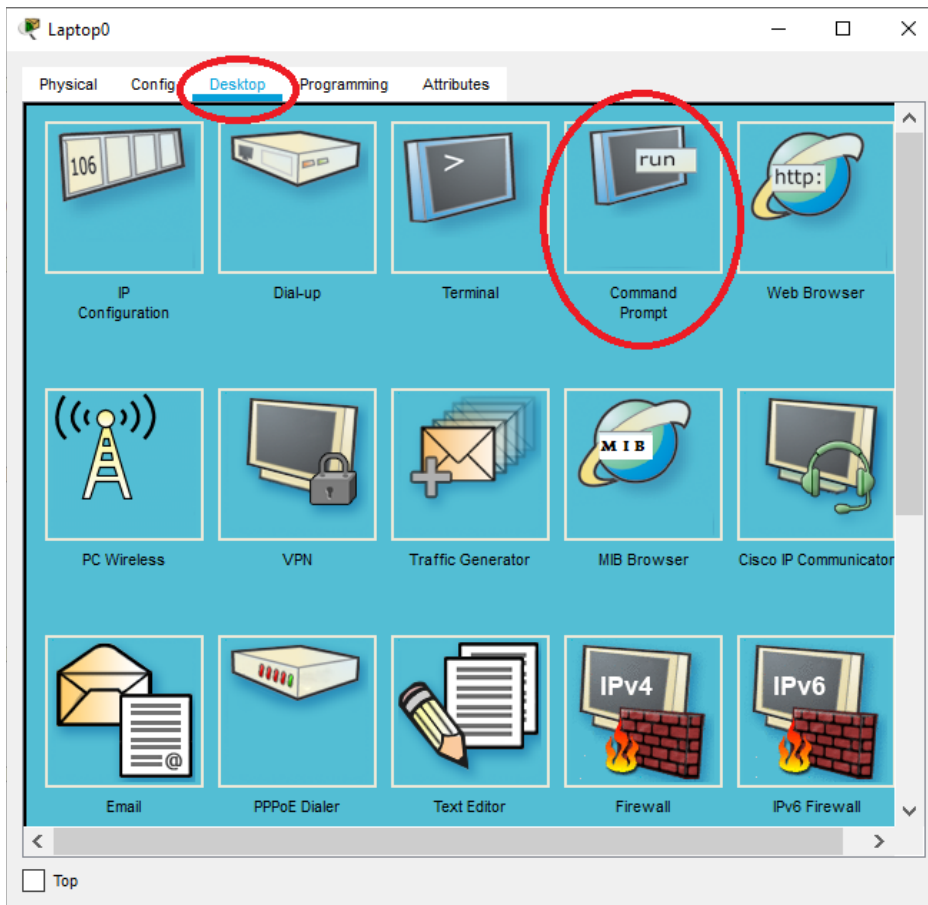
The switchports connected to the Access Points should be configured as access ports for the AP management VLAN. Traffic will be carried inside a CAPWAP tunnel to the WLC.

```
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

- 11) 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
```

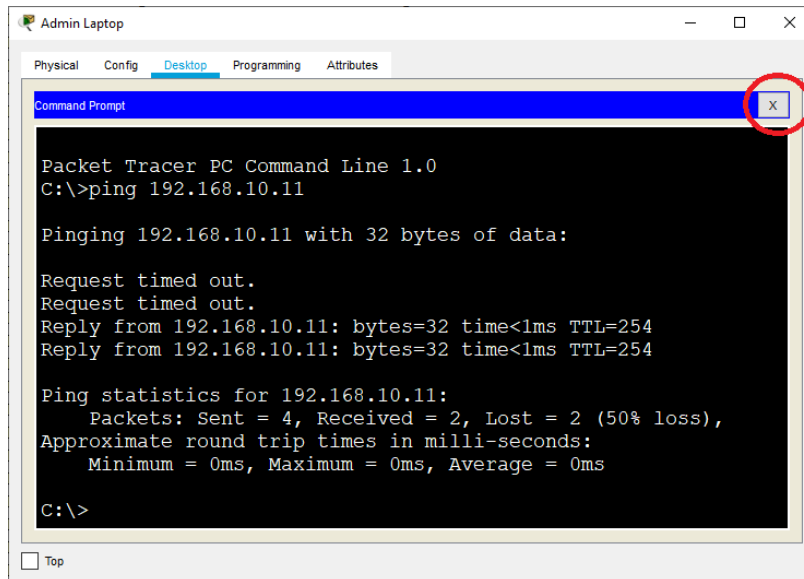
```
Ping statistics for 192.168.10.11:
```

```
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

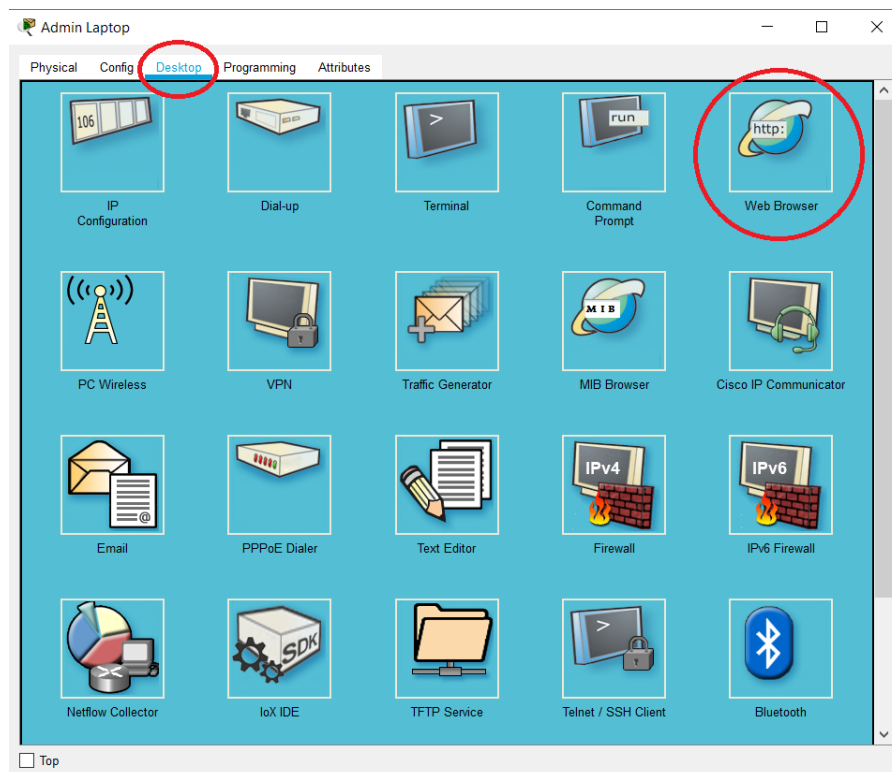
Close the command prompt window.

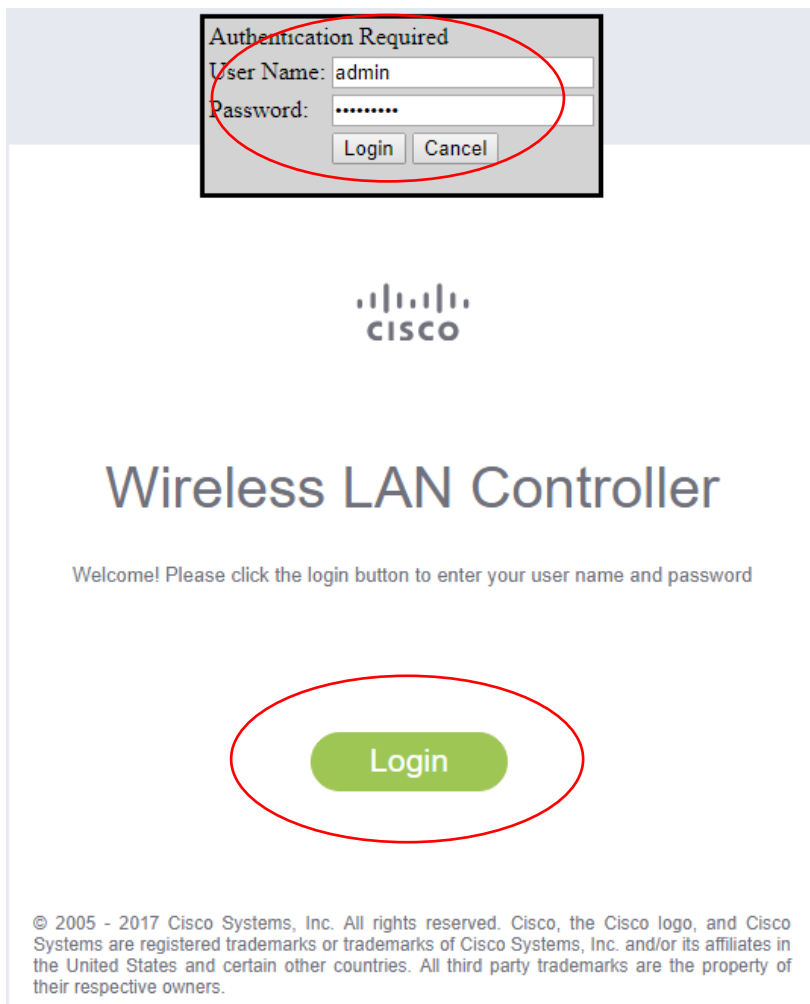
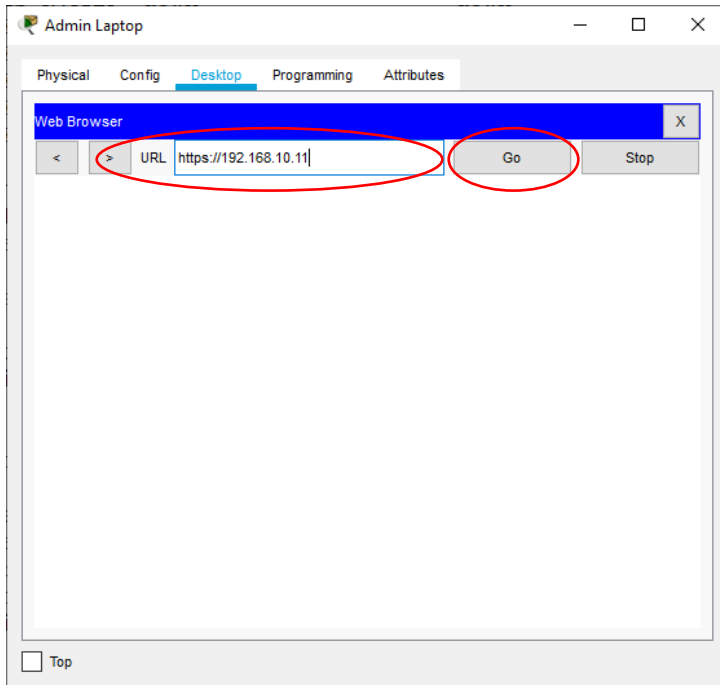


- 12) Open <https://192.168.10.11> (use https, not http) in a web browser window on the Admin laptop to open the Wireless LAN Controller administration GUI.

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.





- 13) On the dashboard Summary page, verify the two Access Points have registered with the WLC.

Web Browser

URL: https://192.168.10.11/frameMonitor.html

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Monitor

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	WLC1
Up Time	18 minutes, 19 seconds
System Time	Fri Feb 21 00:10:49 2020
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

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

- 14) Add the RADIUS AAA server at 192.168.10.10 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'

Web Browser

URL: https://192.168.10.11/frameMonitor.html

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

AAA

RADIUS Authentication

RADIUS Authentication Servers

Network	User	Management	Server Index	Server Address (IPv4/IPv6)	Port	IPSec	Admin Status
---------	------	------------	--------------	----------------------------	------	-------	--------------

Enter the details for the RADIUS server then click 'Apply'.

RADIUS Authentication Servers > New

Server Index (Priority)	<input type="text" value="1"/>
Server IP Address(Ipv4/Ipv6)	<input type="text" value="192.168.10.10"/>
Shared Secret Format	<input type="text" value="ASCII"/>
Shared Secret	<input type="password" value="....."/>
Confirm Shared Secret	<input type="password" value="....."/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	<input type="text" value="1812"/>
Server Status	<input type="text" value="Enabled"/>
Support for CoA	<input type="text" value="Disabled"/>
Server Timeout	<input type="text" value="2"/> seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	<input type="text" value="2"/> seconds
IPSec	<input type="checkbox"/> Enable

Verify the RADIUS server is added.

RADIUS Authentication Servers

Auth Called Station ID Type	<input type="text" value="IP Address"/>
Use AES Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Delimiter	<input type="text" value="Hyphen"/>
Framed MTU	<input type="text" value="1300"/>

Network User	Management	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	192.168.10.10	1812	Disabled	Enabled	Remove

DHCP on Wireless LAN Controller

- 15) 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.
Enter all other relevant details (a DNS server is not required in this lab environment.)

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

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

CISCO

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

Controller

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

DHCP Scopes

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

New...

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

DHCP Scope > New

Scope Name

Click on the Corporate DHCP scope to configure it.

DHCP Scopes

Scope Name	Address Pool	Lease Time	Status
Corporate	0.0.0.0 - 0.0.0.0		Enabled Remove
day0-dhcp-mgmt	192.168.1.3 - 192.168.1.14		Enabled Remove

New...

Enter the details then click 'Apply'

DHCP Scope > Edit

Scope Name	Corporate
Pool Start Address	192.168.22.101
Pool End Address	192.168.22.254
Network	192.168.22.0
Netmask	255.255.255.0
Lease Time (seconds)	86400
Default Routers	192.168.22.1
DNS Domain Name	Not Supported
DNS Servers	0.0.0.0
Netbios Name Servers	0.0.0.0
Status	Enabled ▼

- 16) Configure a DHCP scope on the WLC for Guest wireless clients with the address range 192.168.23.101 to 192.168.23.254.
Enter all other relevant details (a DNS server is not required in this lab environment.)

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

Web Browser

URL: https://192.168.10.11/frameDhcpScopeList.html

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

Controller

DHCP Scopes

[New...](#)

Scope Name	Address Pool	Lease Time	Status
Corporate	192.168.22.101 - 192.168.22.254		Enabled Remove
day0-dhcp-mgmt	192.168.1.3 - 192.168.1.14		Enabled Remove

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

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

DHCP Scope > New

Scope Name

Click on the Corporate 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	192.168.1.3 - 192.168.1.14		Enabled Remove

Enter the details then click 'Apply'

DHCP Scope > Edit

Scope Name	Guest		
Pool Start Address	<input type="text" value="192.168.23.101"/>		
Pool End Address	<input type="text" value="192.168.23.254"/>		
Network	<input type="text" value="192.168.23.0"/>		
Netmask	<input type="text" value="255.255.255.0"/>		
Lease Time (seconds)	<input type="text" value="86400"/>		
Default Routers	<input type="text" value="192.168.23.1"/>	<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="0.0.0.0"/>	<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"/>		

Verify both scopes are enabled.

DHCP Scopes

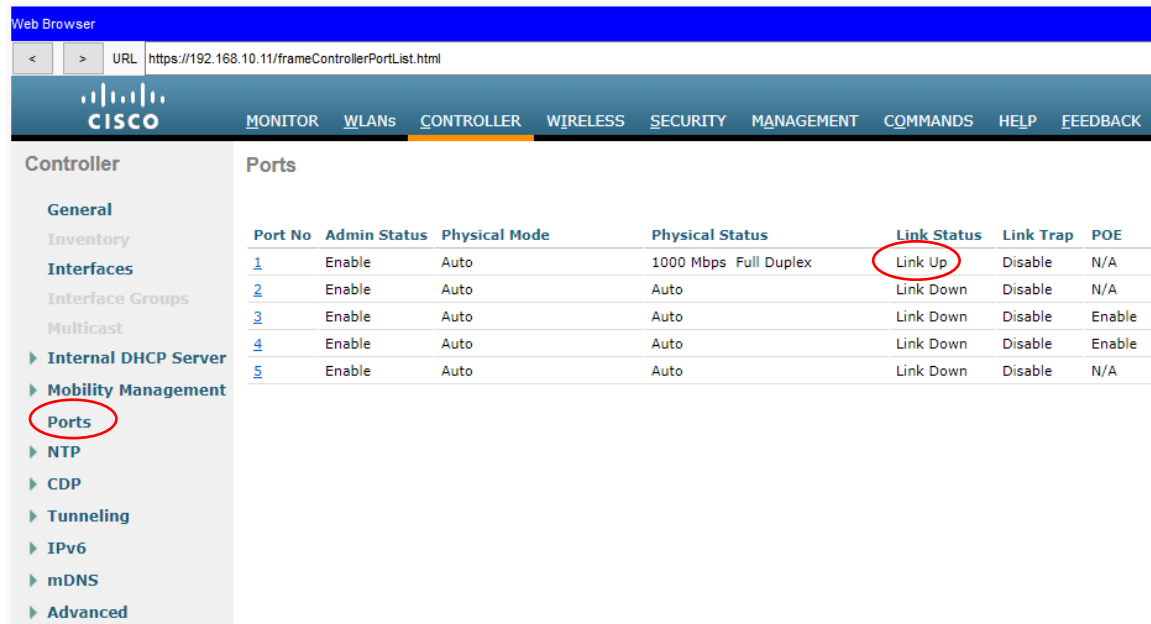
[New...](#)

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	192.168.1.3 - 192.168.1.14		Enabled Remove

Logical Interfaces on the Wireless LAN Controller

- 17) Create a logical interface on the Wireless LAN Controller in the Corporate VLAN, with IP address 192.168.22.2.
Wireless clients on the Corporate VLAN should get an IP address from the Wireless LAN Controller.

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

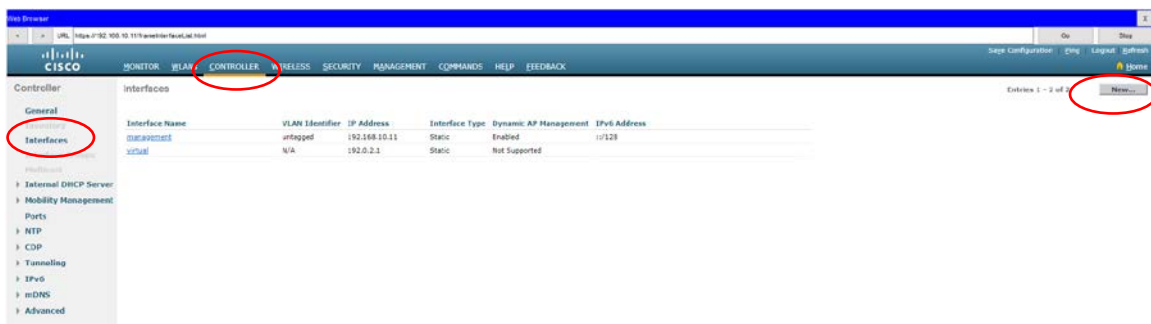


The screenshot shows the Cisco WLC web interface. The 'CONTROLLER' tab is selected. In the left sidebar, 'Ports' is highlighted with a red circle. The main content area displays a table of ports:

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'



The screenshot shows the Cisco WLC web interface. The 'CONTROLLER' tab is selected. In the left sidebar, 'Interfaces' is highlighted with a red circle. The main content area displays a table of interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
DMZ-PORTS	unassigned	192.168.10.11	Static	Enabled	10129
WLAN	N/A	192.0.2.1	Static	Not Supported	

The 'New' button in the top right corner is highlighted with a red circle.

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

Interfaces > New

Interface Name	<input type="text" value="Corporate"/>
VLAN Id	<input type="text" value="22"/>

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

General Information

Interface Name	Corporate
MAC Address	00:D0:BC:6E:BD:49

Configuration

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

Physical Information

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

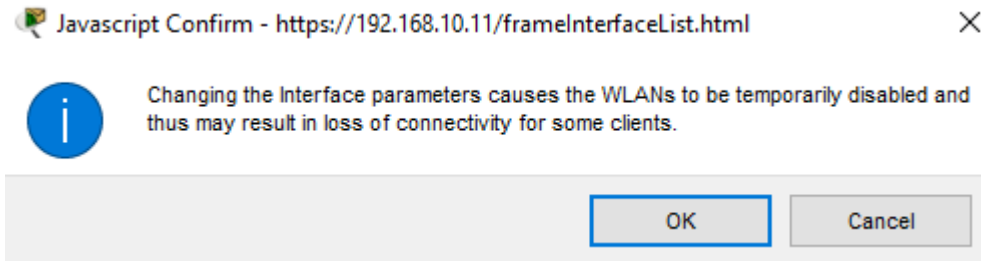
Interface Address

VLAN Identifier	<input type="text" value="22"/>
IP Address	<input type="text" value="192.168.22.2"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.22.1"/>

DHCP Information

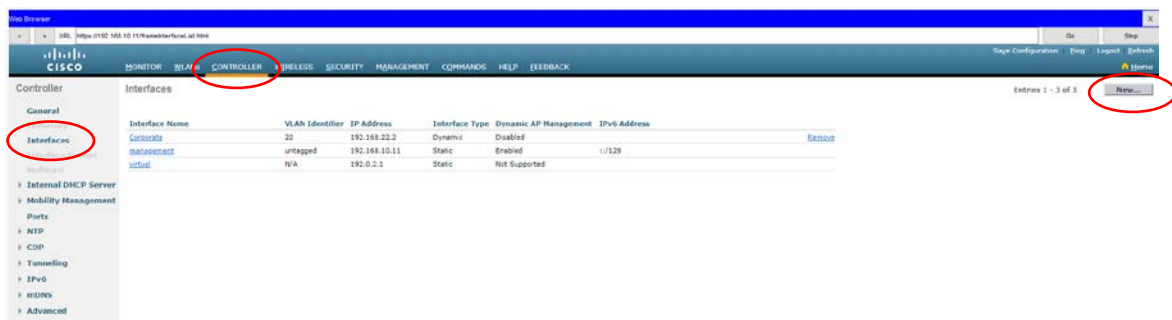
Primary DHCP Server	<input type="text" value="192.168.10.11"/>
Secondary DHCP Server	<input type="text"/>
DHCP Proxy Mode	<input type="text" value="Global"/>
Enable DHCP Option 82	<input type="checkbox"/>

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



- 18) Create a logical interface in the Guest VLAN with IP address 192.168.23.2.
Wireless clients on the Guest VLAN should get an IP address from the Wireless LAN Controller.

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



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

Interfaces > New

Interface Name	<input type="text" value="Guest"/>
VLAN Id	<input type="text" 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

General Information

Interface Name	Guest
MAC Address	00:04:9A:CE:DD:26

Configuration

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

Physical Information

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

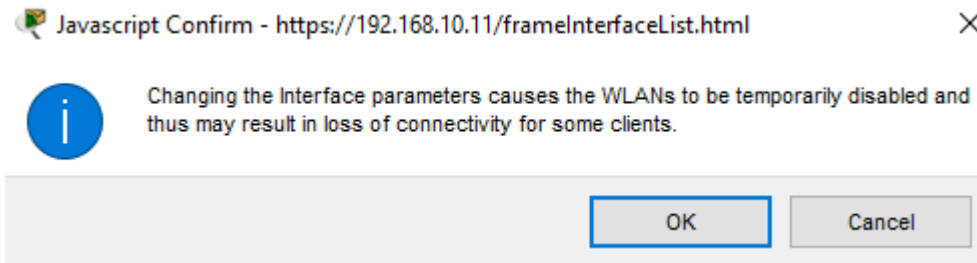
Interface Address

VLAN Identifier	<input type="text" value="23"/>
IP Address	<input type="text" value="192.168.23.2"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.23.1"/>

DHCP Information

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

Click '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	IPv6 Address	
Corporate	22	192.168.22.2	Dynamic	Disabled		Remove
Guest	23	192.168.23.2	Dynamic	Disabled		Remove
management	untagged	192.168.10.11	Static	Enabled	::/128	
virtual	N/A	192.0.2.1	Static	Not Supported		

Wireless LANs

- 19) Create the wireless LAN named 'Corporate'. Clients should be authenticated by the 192.168.10.10 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'



Enter the details then click 'Apply'

WLANs > New

Type	WLAN ▼
Profile Name	Corporate
SSID	Corporate
ID	1 ▼

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

WLANs > Edit 'Corporate'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	Corporate			
Type	WLAN			
SSID	Corporate			
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)	Corporate ▼			
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, and Authentication Key Management is 802.1X then click 'Apply'.

WLANs > Edit 'Corporate'

The screenshot shows the 'Security' tab of the WLAN configuration interface. The 'Layer 2' sub-tab is selected. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'MAC Filtering' checkbox is unchecked. Under 'Fast Transition', the 'Fast Transition' checkbox is unchecked. Under 'Protected Management Frame', the 'PMF' dropdown is set to 'Disabled'. Under 'WPA+WPA2 Parameters', the 'WPA Policy' checkbox is unchecked, the 'WPA2 Policy' checkbox is checked, and the 'WPA2 Encryption' dropdown is set to 'AES'. Under 'Authentication Key Management', the '802.1X' checkbox is checked and labeled 'Enable', while 'CCKM' and 'PSK' are unchecked.

Click on the 'Security' then 'AAA Servers' tabs, select the RADIUS server you added earlier 'IP:192.168.10.10, Port:1812' as Server 1, and click 'Apply'.

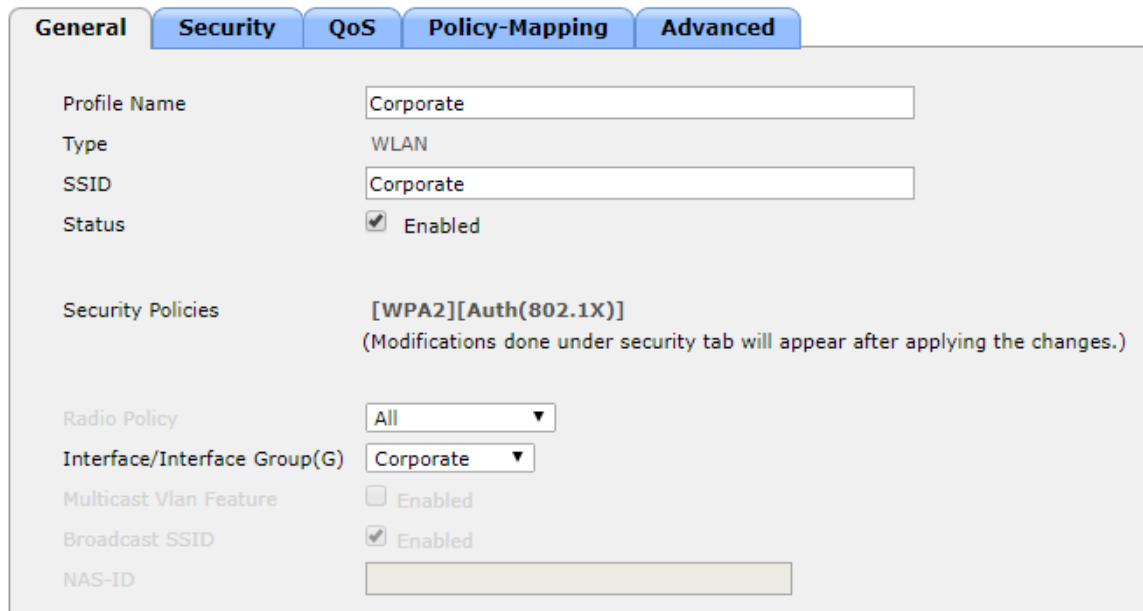
WLANs > Edit 'Corporate'

The screenshot shows the 'AAA Servers' tab of the WLAN configuration interface. The 'Select AAA servers below to override use of default servers on this WLAN' instruction is at the top. Under 'Radius Servers', the 'Radius Server Overwrite interface' checkbox is unchecked. The 'Authentication Servers' section has a table with 6 servers. Server 1 is selected with the value 'IP:192.168.10.10, Port:1812'. Servers 2 through 6 are set to 'None'. The 'Accounting Servers' section has a table with 6 servers, all set to 'None'. The 'EAP Parameters' section has an 'Enable' checkbox which is unchecked. At the bottom, the 'Radius Server Accounting' section has an 'Interim Update' checkbox which is unchecked.

Authentication Servers		Accounting Servers		EAP Parameters	
Server 1	IP:192.168.10.10, Port:1812	Server 1	None	Enable	<input type="checkbox"/>
Server 2	None	Server 2	None		
Server 3	None	Server 3	None		
Server 4	None	Server 4	None		
Server 5	None	Server 5	None		
Server 6	None	Server 6	None		

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

WLANs > Edit 'Corporate'



General Security QoS Policy-Mapping Advanced

Profile Name: Corporate

Type: WLAN

SSID: Corporate

Status: ☒ Enabled

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

Radio Policy: All

Interface/Interface Group(G): Corporate

Multicast Vlan Feature: ☐ Enabled

Broadcast SSID: ☒ Enabled

NAS-ID:

20) 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: https://192.168.10.11/frameWlan.html

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

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
1	WLAN	Corporate	Corporate	Disabled	[WPA2][Auth(802.1X)]

Remove

Enter the details then click 'Apply'

WLANs > New

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'

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.

WLANs > Edit 'Guest'

The screenshot shows the 'Security' tab of the WLAN configuration interface. The 'Layer 2' sub-tab is selected. Under 'Protected Management Frame', the PMF is set to 'Disabled'. In the 'WPA+WPA2 Parameters' section, 'WPA2 Policy' is checked, and 'WPA2 Encryption' is set to 'AES'. Under 'Authentication Key Management', 'PSK' is checked and 'Enable' is selected. The 'PSK Format' is set to 'ASCII', and a pre-shared key field contains ten dots, representing the key 'Flackbox3'.

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

WLANs > Edit 'Guest'

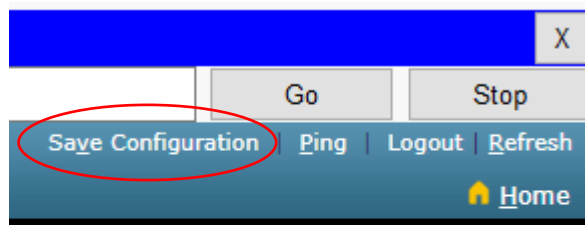
The screenshot shows the 'General' tab of the WLAN configuration interface. The 'Profile Name' is 'Guest', 'Type' is 'WLAN', and 'SSID' is 'Guest'. The 'Status' checkbox is checked and labeled 'Enabled'. The 'Security Policies' field shows '[WPA2][Auth(PSK)]' with a note that modifications will appear after applying changes. The 'Radio Policy' is set to 'All', and the 'Interface/Interface Group(G)' is 'Guest'. The 'Multicast Vlan Feature' is unchecked, and 'Broadcast SSID' is checked and labeled 'Enabled'. The 'NAS-ID' field is empty.

Click 'WLANS' to verify both WLANS are enabled.

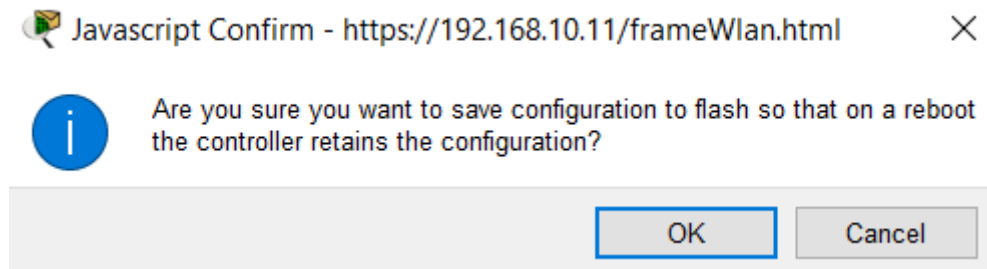


21) Save the configuration on the Wireless LAN Controller.

Click 'Save Configuration' near the top-right corner.



Click 'OK' when you see the warning message (this does NOT reboot the controller).



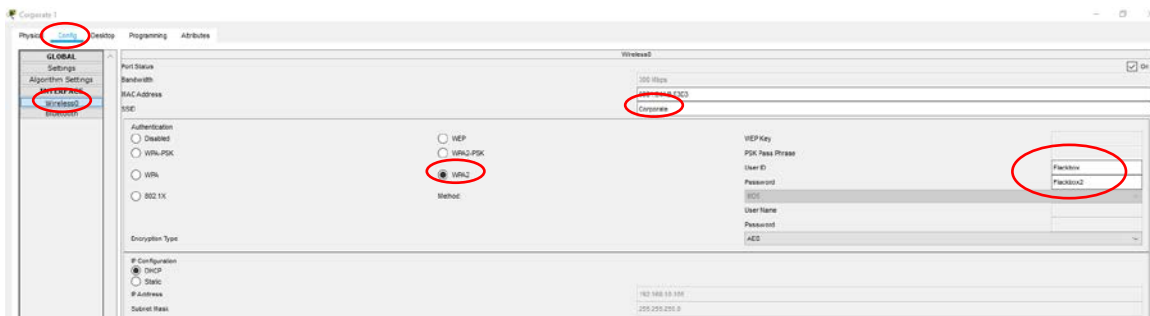
Join Clients to the Wireless LANs

Note that the wireless clients will be assigned IP addresses from the 192.168.10.0/24 subnet in this Packet Tracer lab, rather than the Corporate and Guest DHCP scopes as would happen in a real world environment.

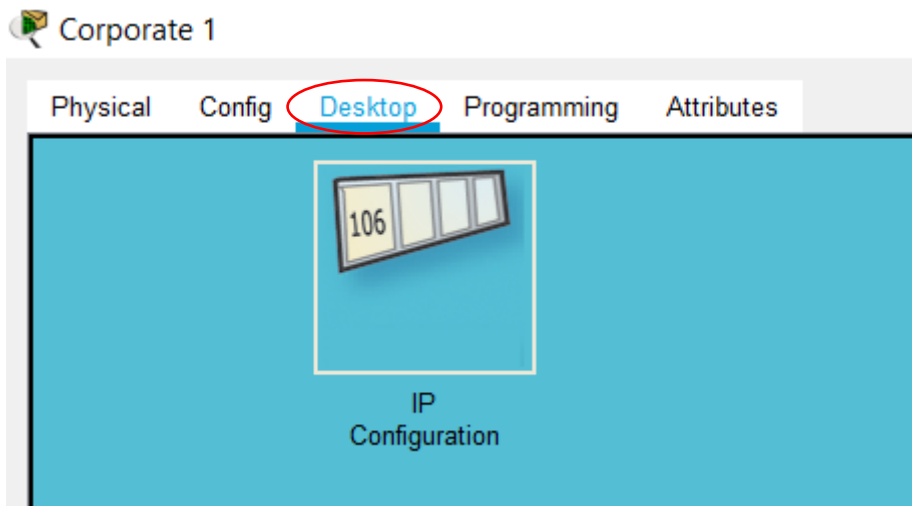
22) A username **Flackbox** with password **Flackbox2** has been configured on the RADIUS server.

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

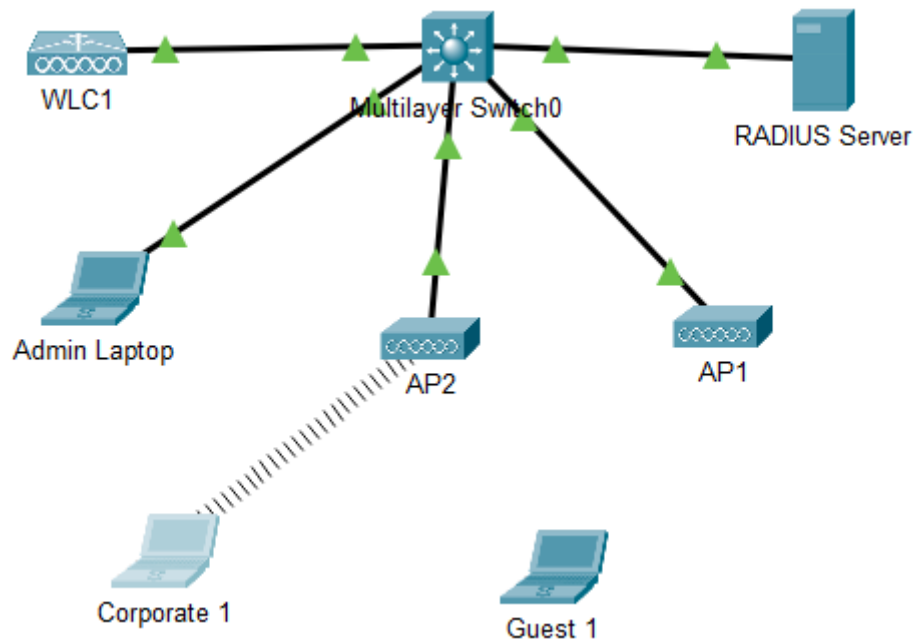
Click on the Corporate1 laptop in the Packet Tracer main window, then 'Config' and 'Wireless0'. Enter the SSID 'Corporate', select WPA2 authentication then enter the user ID Flackbox and password Flackbox2.



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

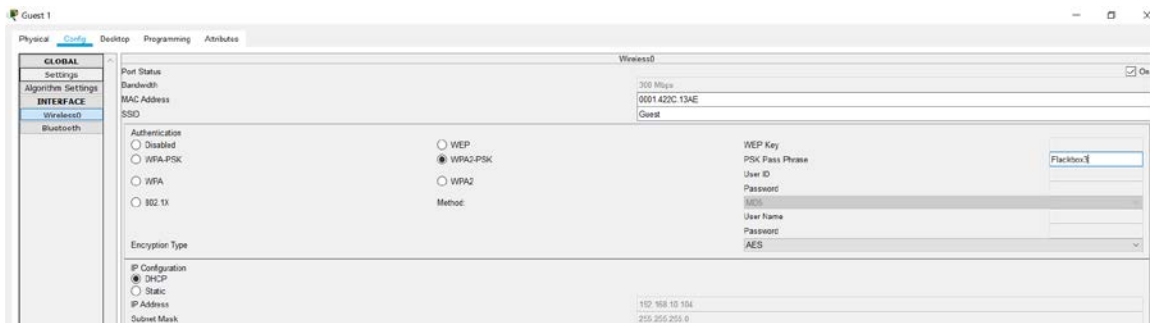


Verify the laptop connects in the Packet Tracer main window.




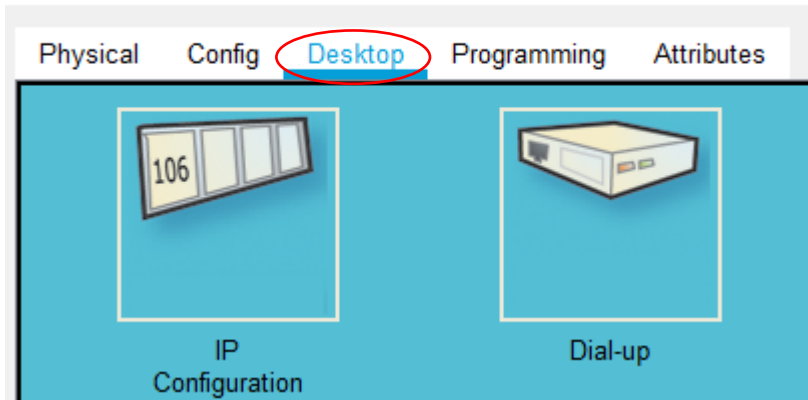
23) Connect to the 'Guest' WLAN from the Guest1 laptop.

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**



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

 Guest 1



Verify the laptop connects in the Packet Tracer main window.

