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.

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'.

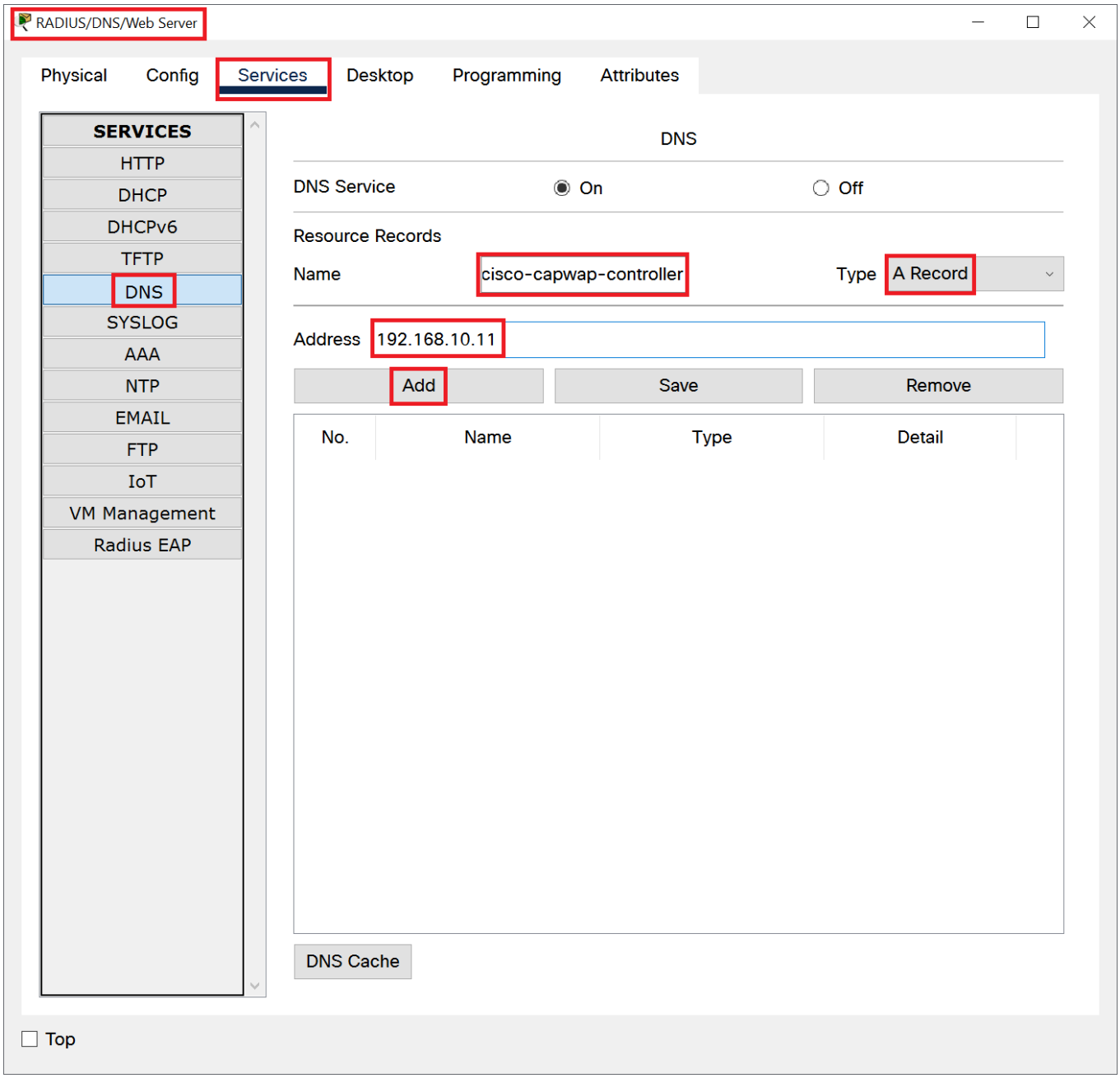
```
Switch(config)#vlan 10
Switch(config-vlan)#name Management
```

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

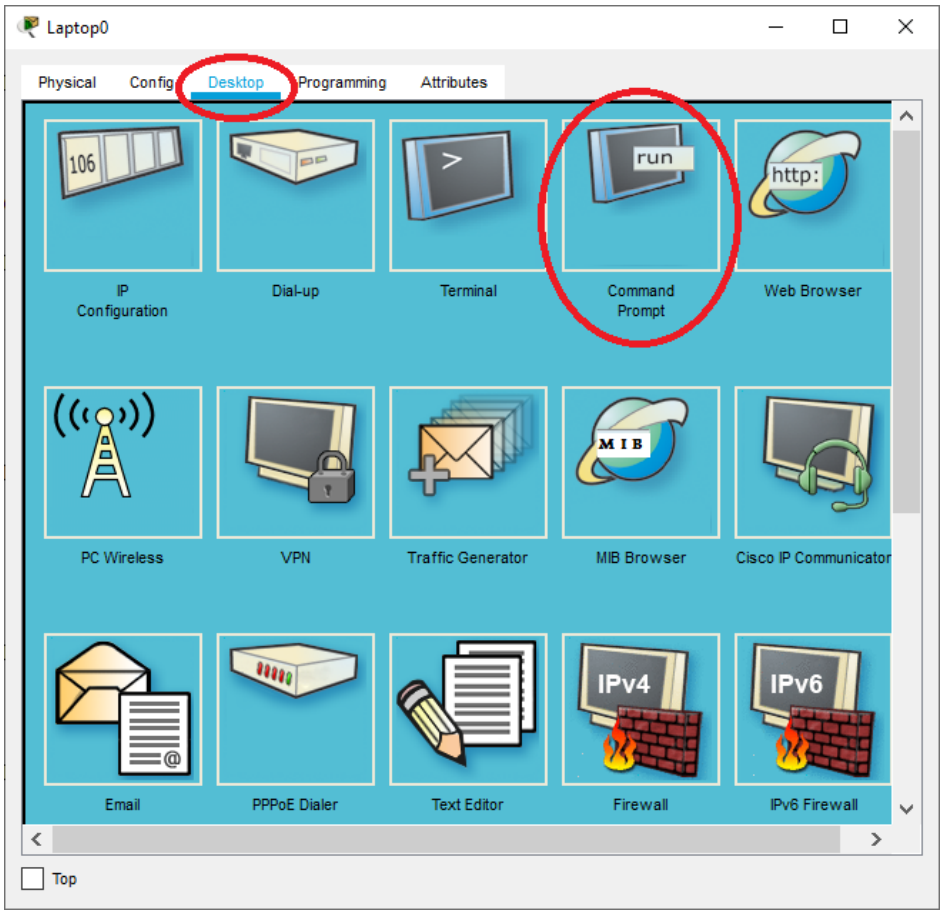
```
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
```

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.



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
```

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.

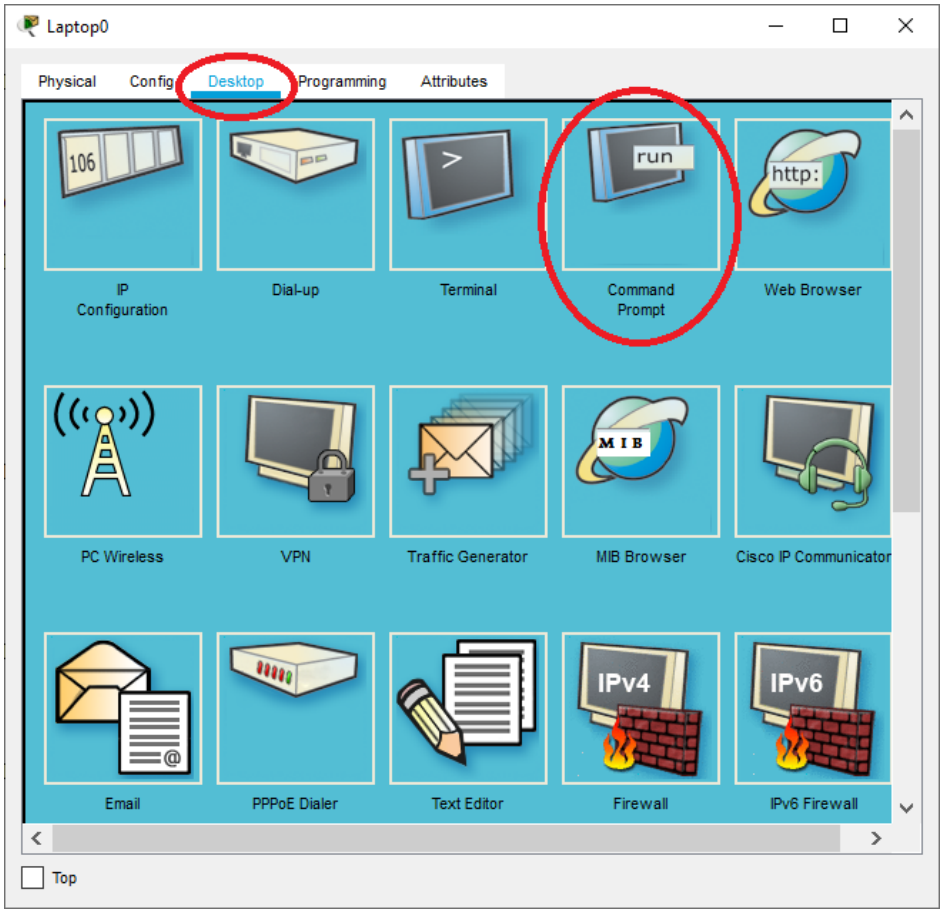
The switchports connected to the Access Points should be configured as access ports for the AP management VLAN. Traffic will be carried inside a CAPWAP tunnel to the WLC.

```
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

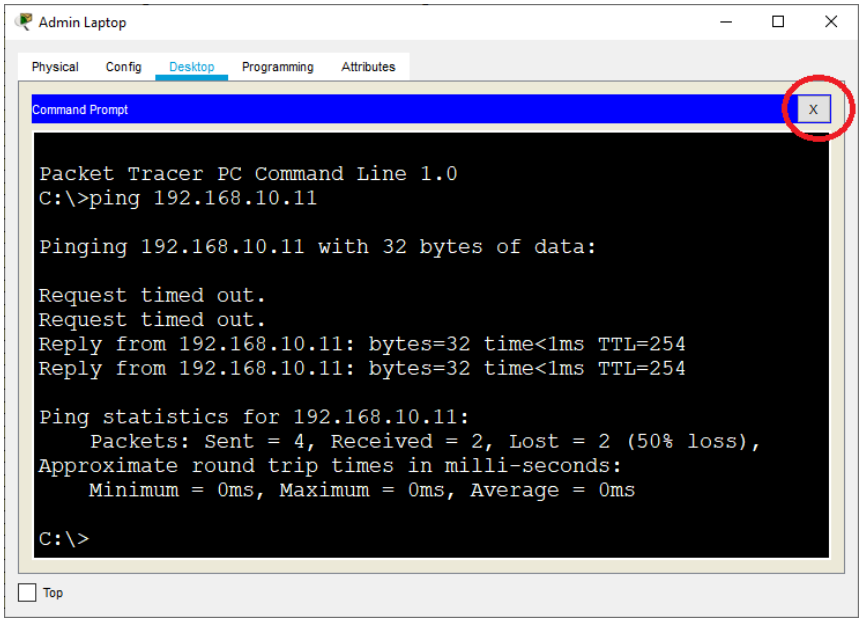
12) Check you can ping the Wireless LAN Controller at 192.168.10.11 from the Admin laptop.

Open a command prompt on the Admin laptop.

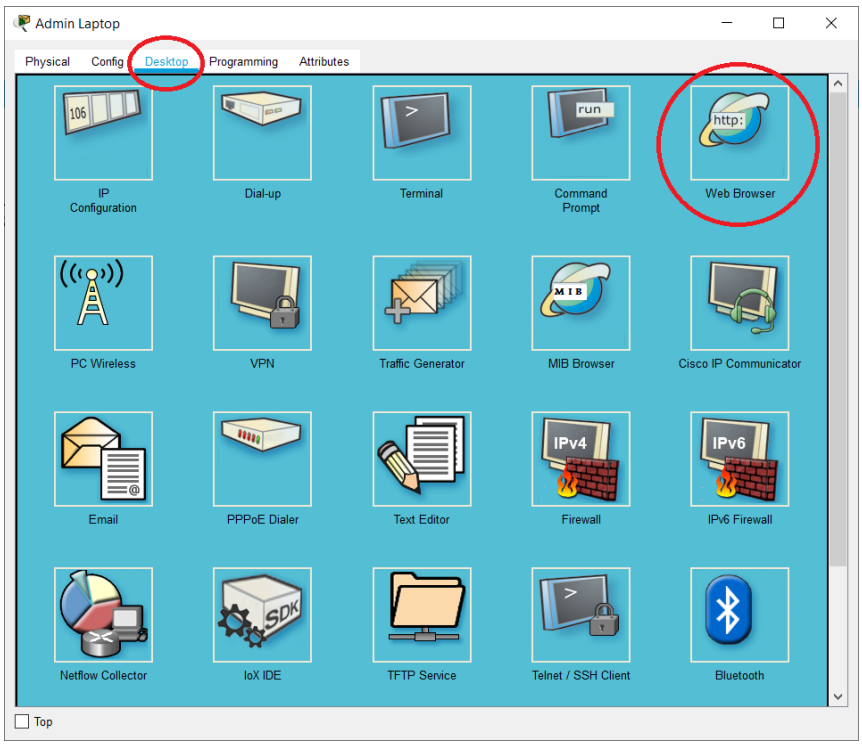


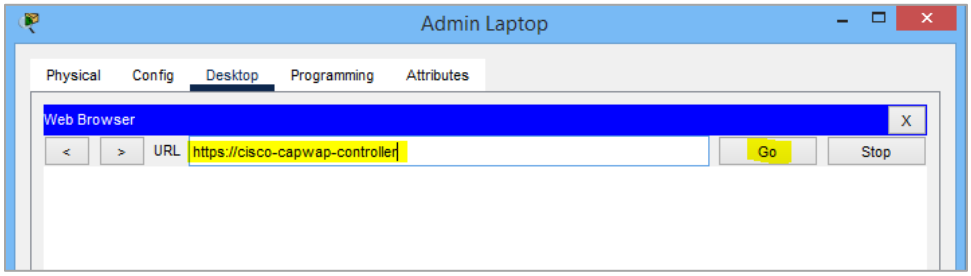

```
C:\>ping 192.168.10.11
Pinging 192.168.10.11 with 32 bytes of data:

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
```

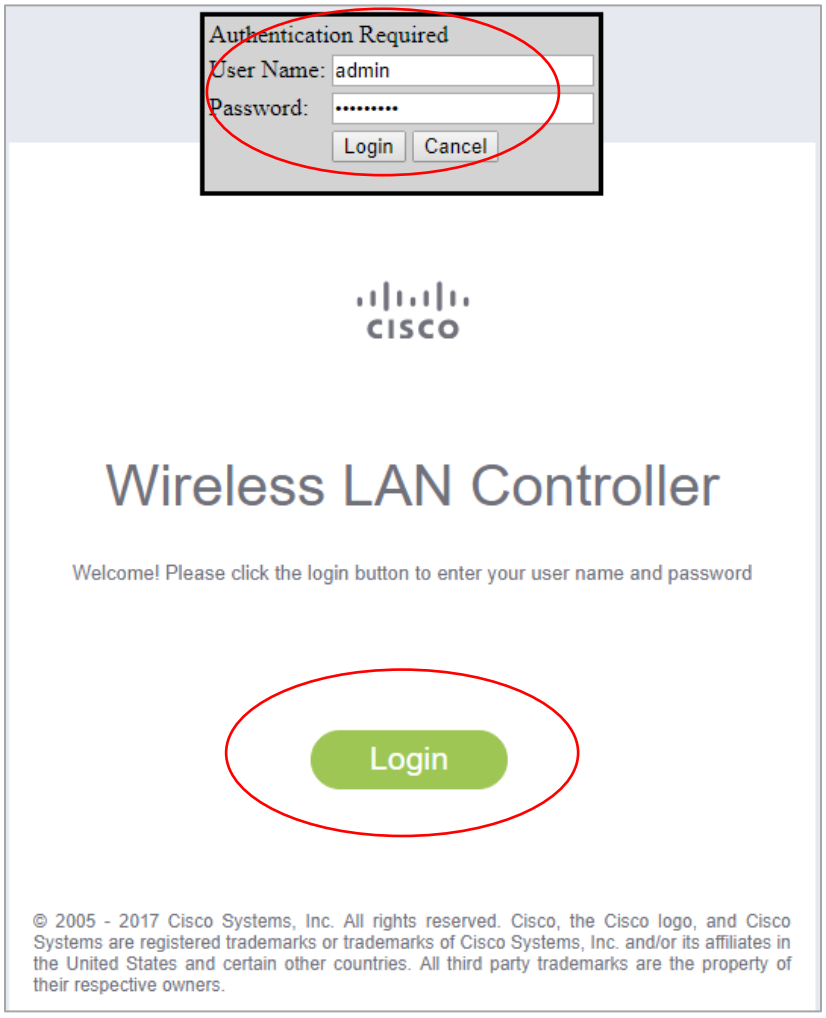
Close the command prompt window.



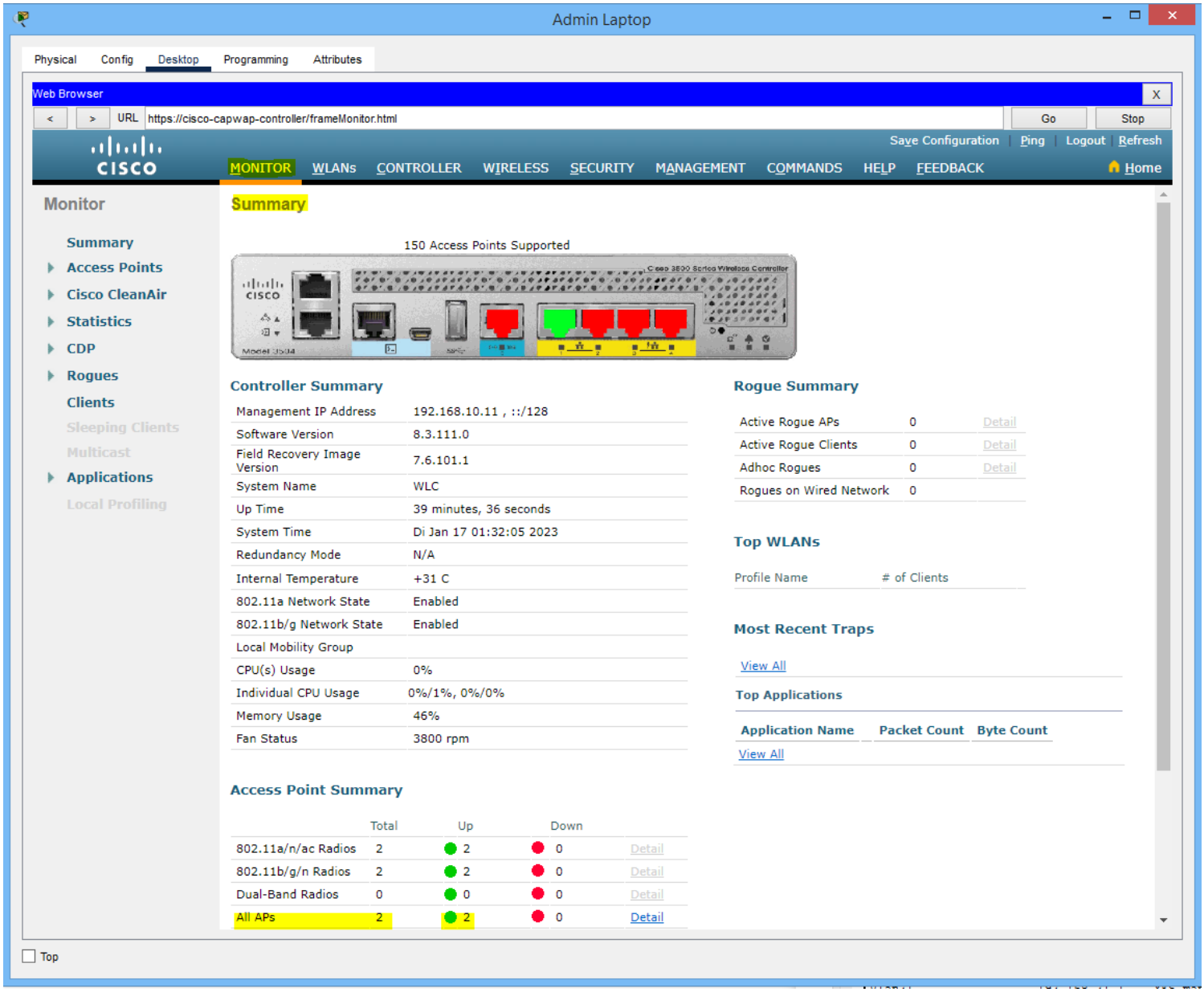
13) Open https://cisco-capwap-controller (use https, not http) in a web browser window on the Admin laptop to open the Wireless LAN Controller administration GUI.
Login with username **admin** and password **Flackbox1**
If you get a 'Host Name Unresolved' error message then close the web browser window, then reopen it and try again.

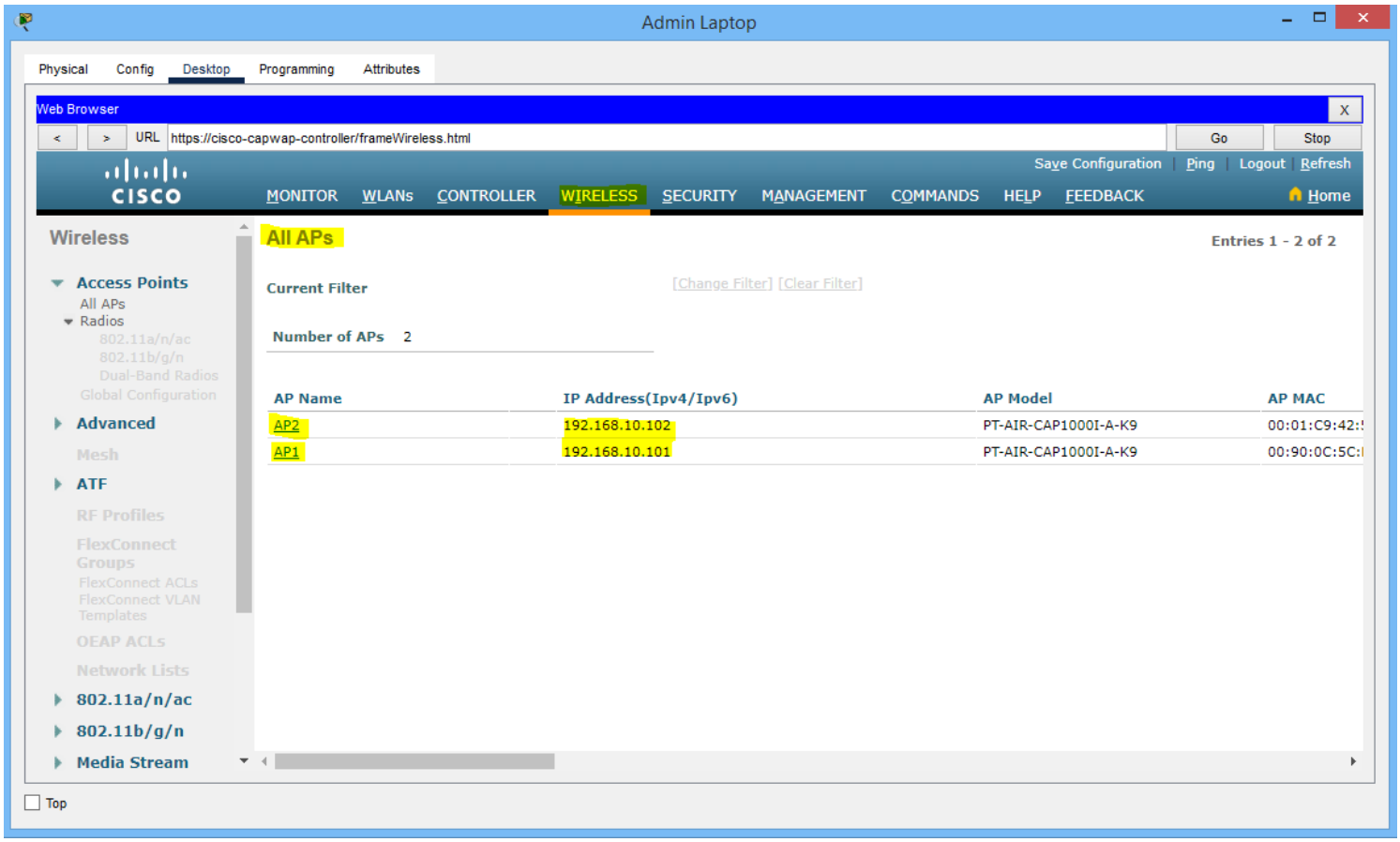



Admin Laptop
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
https://cisco-capwap-controller
Go
Stop


Authentication Required
User Name: admin
Password: ••••••••
Login
Cancel
cisco
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.

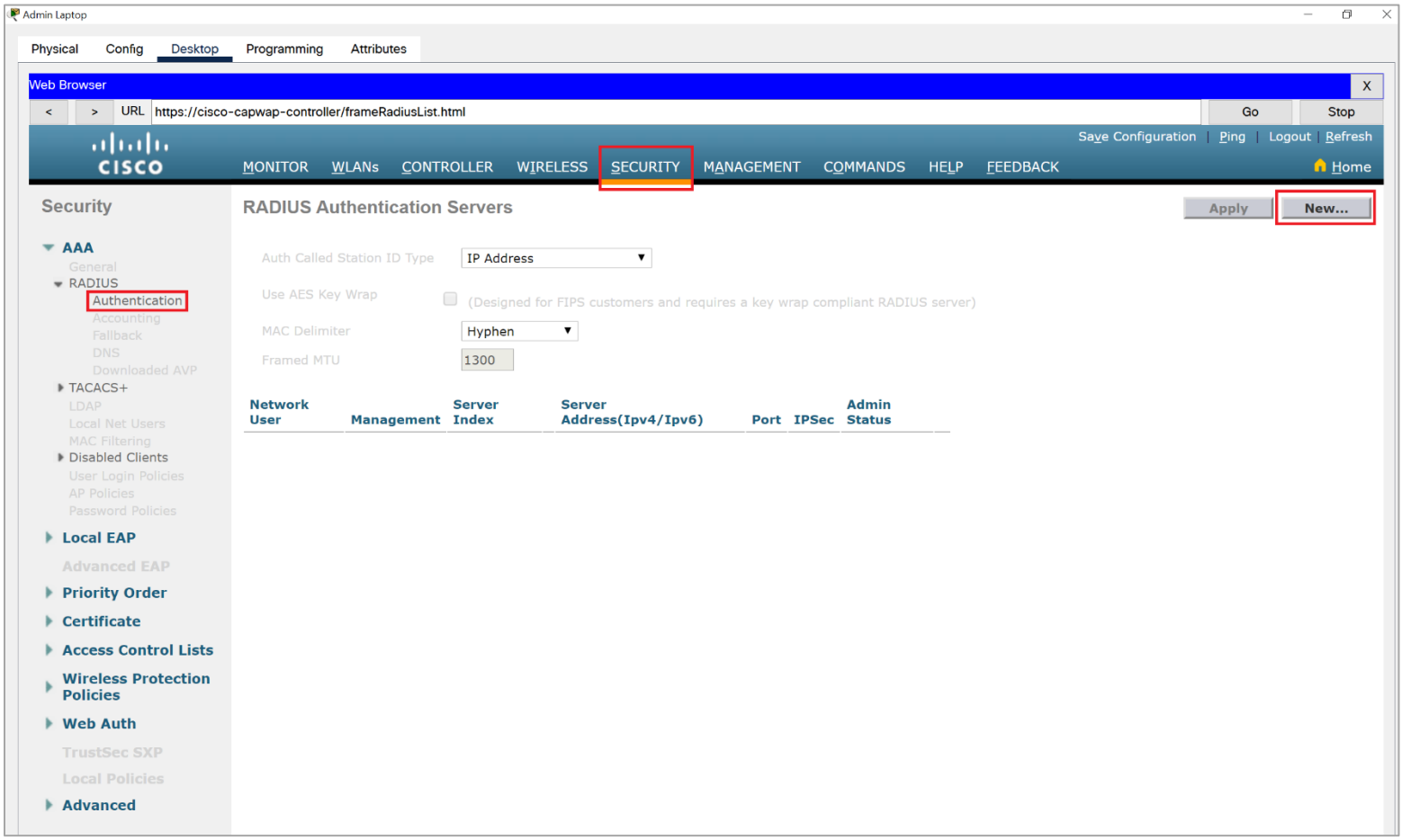
14) On the dashboard Summary page and the Wireless page, verify the two Access Points have registered with the WLC. (You can ignore it if you see two extra APs, this is a Packet Tracer glitch.)



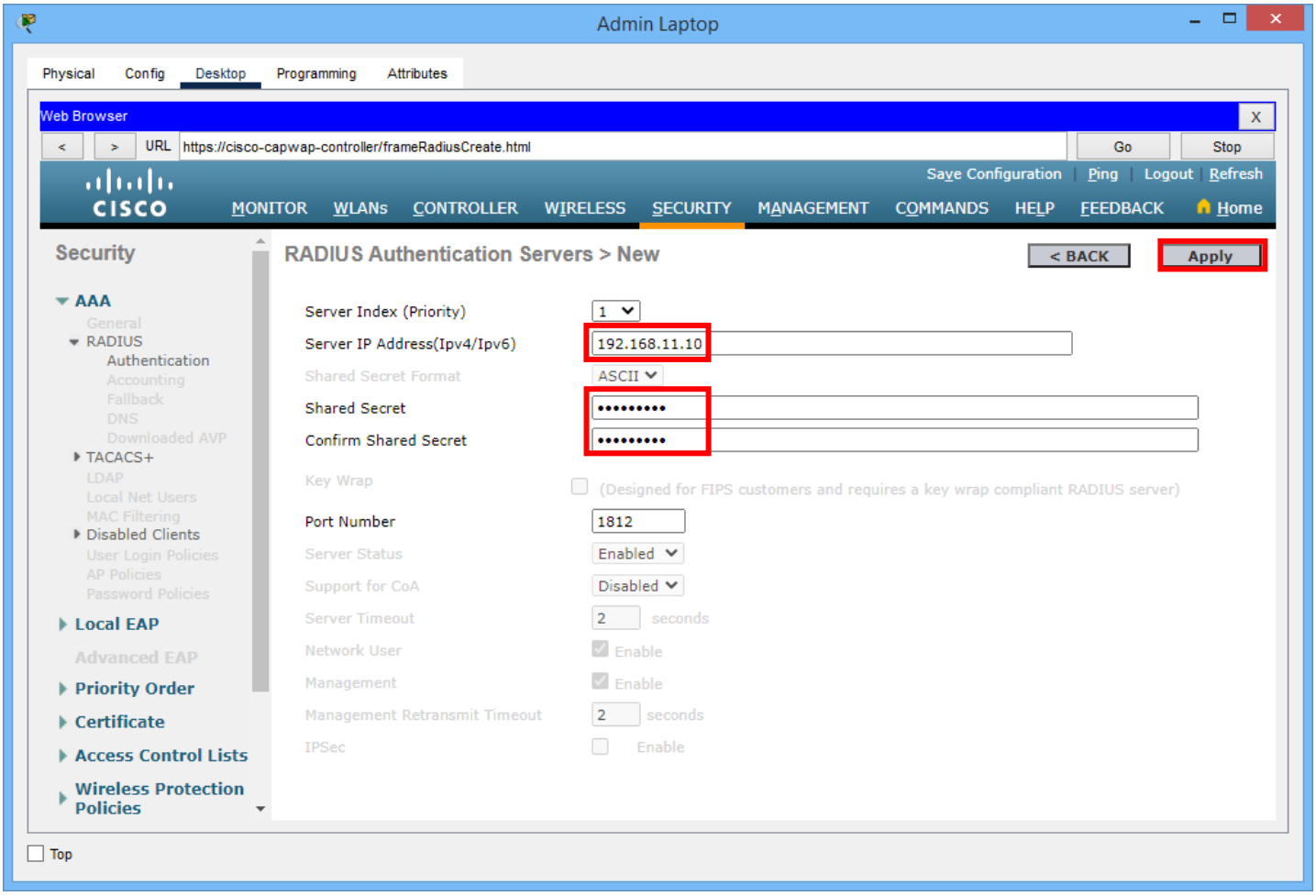

Admin Laptop
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
https://cisco-capwap-controller/frameWireless.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
Wireless
Access Points
All APs
Radios
802.11a/n/ac
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
AP1
192.168.10.101
PT-AIR-CAP1000I-A-K9
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**.

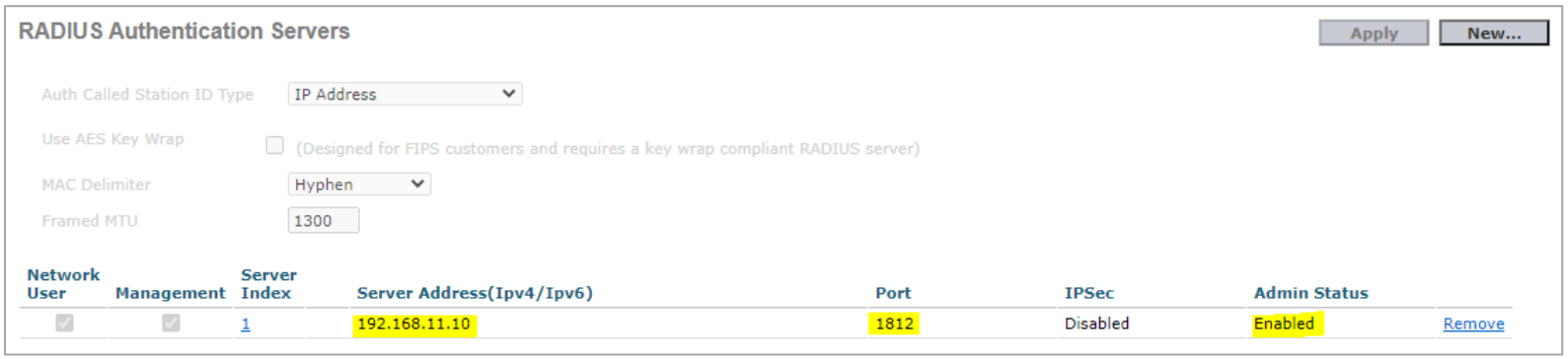
Click ‘Security’ > ‘AAA’ > ‘RADIUS’ > ‘Authentication’ then ‘New’



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



Verify the RADIUS server is added.

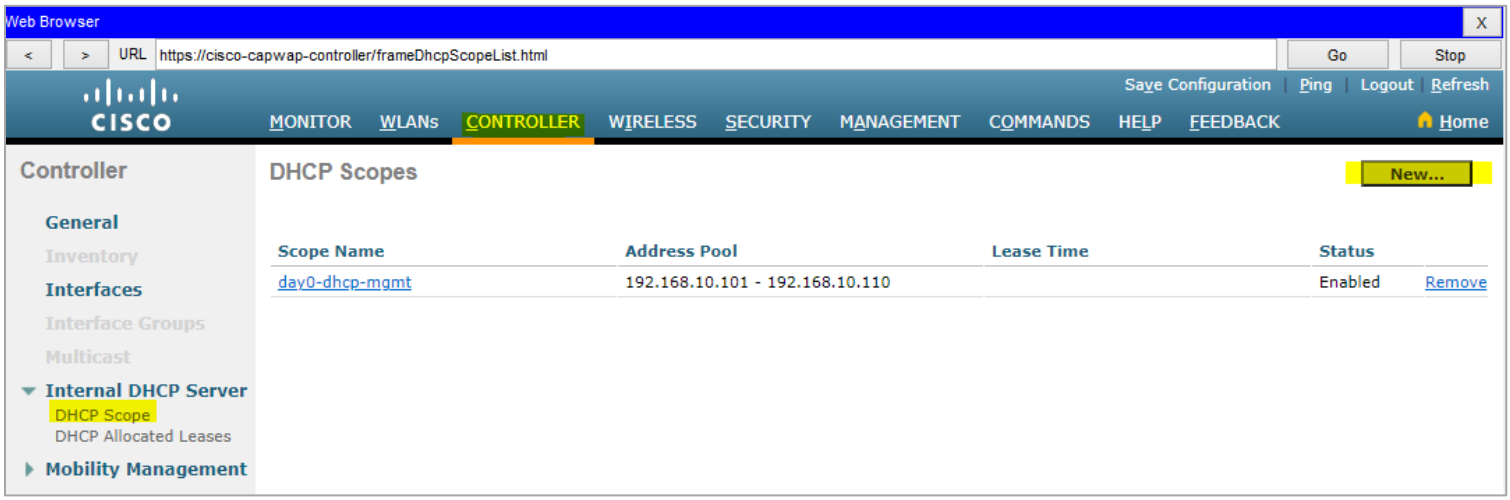


DHCP on Wireless LAN Controller

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.

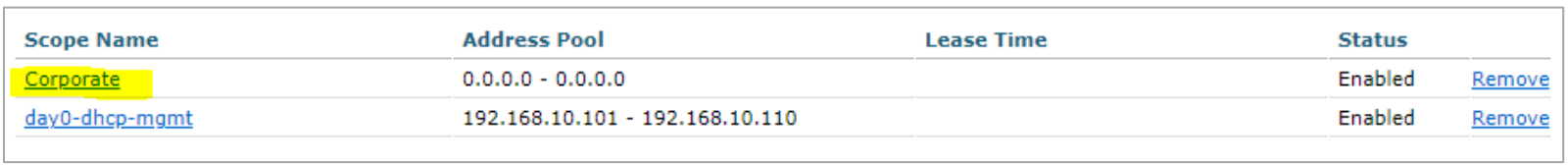
16) Wireless DHCP clients can receive their IP address from an external DHCP server or from the Wireless LAN Controller.
Configure a DHCP scope on the WLC for Corporate wireless clients with the address range 192.168.22.101 to 192.168.22.254.
Configure a DNS server with IP address 192.168.11.10.
Enter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

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

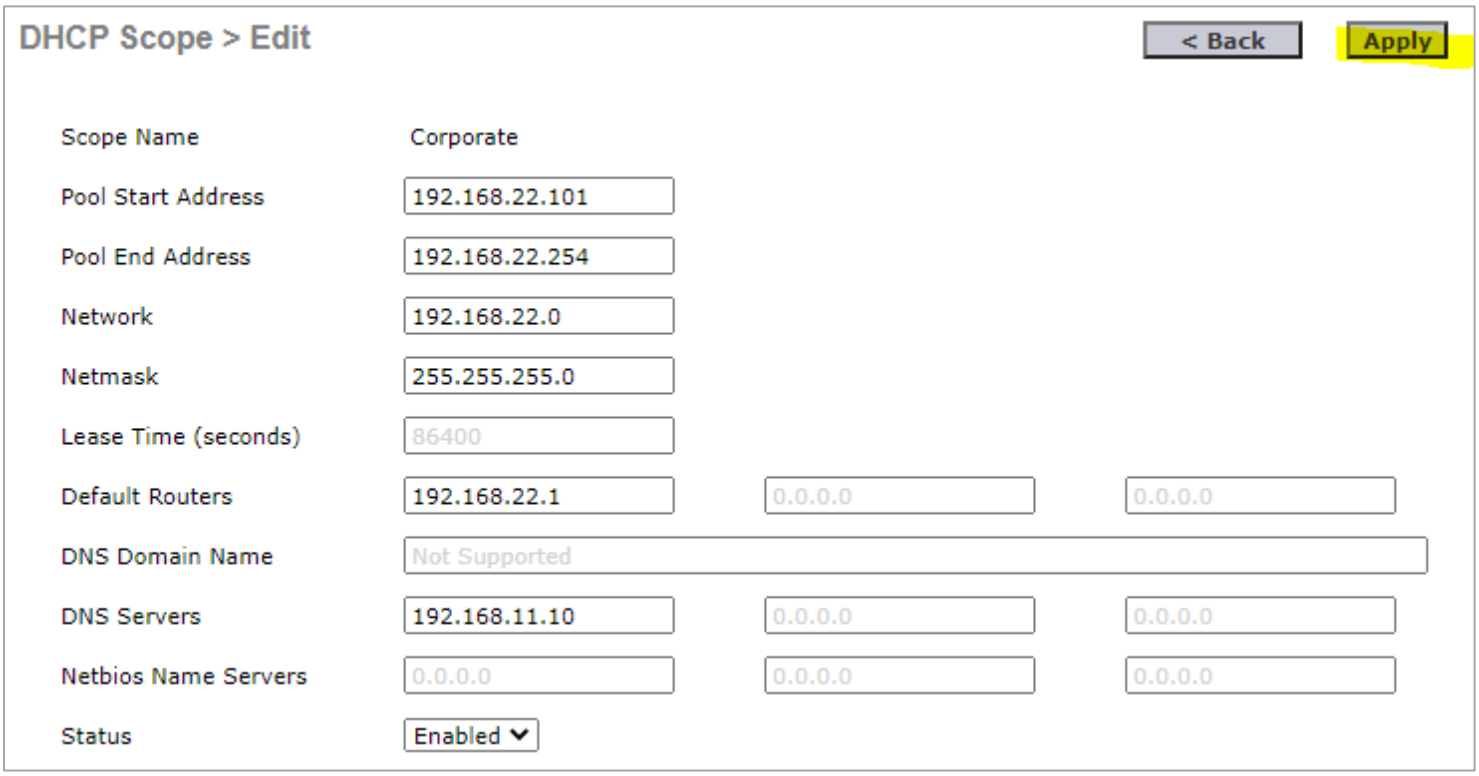


Name the scope 'Corporate' then click 'Apply'.

Click on the Corporate DHCP scope to configure it.



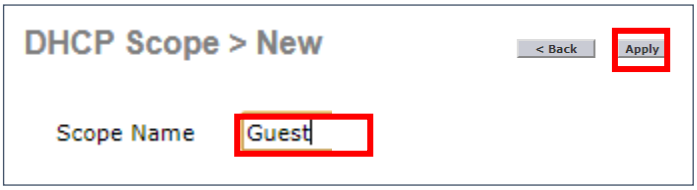
Enter the details then click ‘Apply’



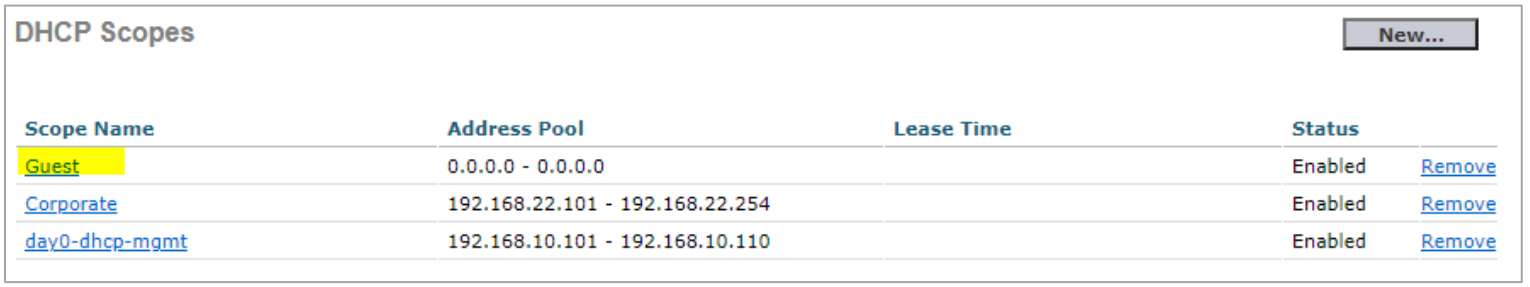
17) Configure a DHCP scope on the WLC for Guest wireless clients with the address range 192.168.23.101 to 192.168.23.254.
Configure a DNS server with IP address 192.168.11.10.
Enter all other relevant details.

Click ‘Controller’ > ‘Internal DHCP Server’ > ‘DHCP Scope’ then ‘New’

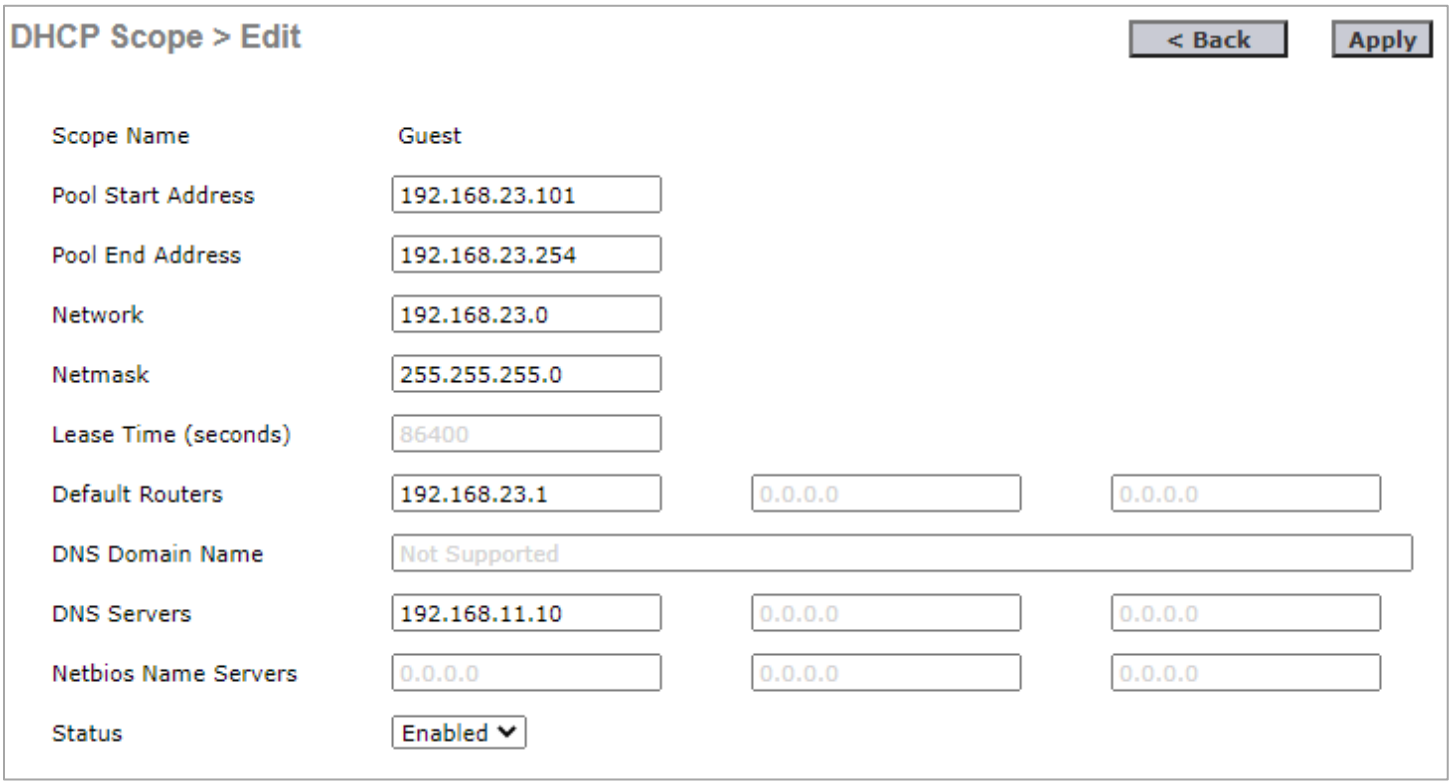
Name the scope ‘Guest’ then click ‘Apply’.



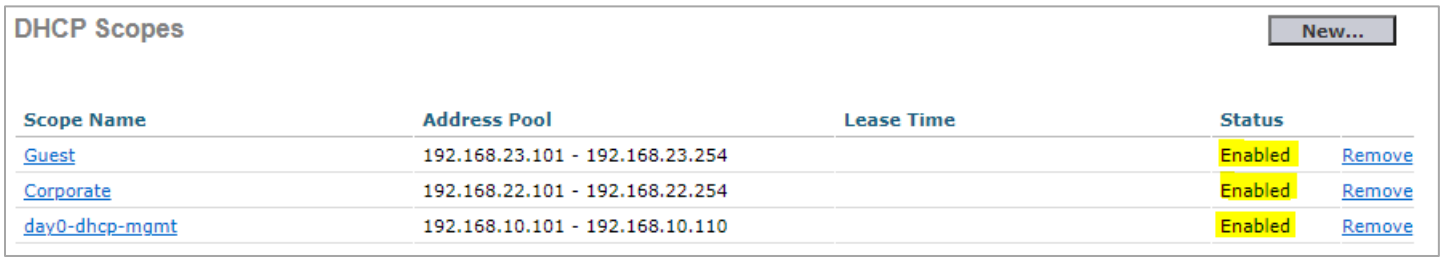
Click on the Guest DHCP scope to configure it.



Enter the details then click ‘Apply’

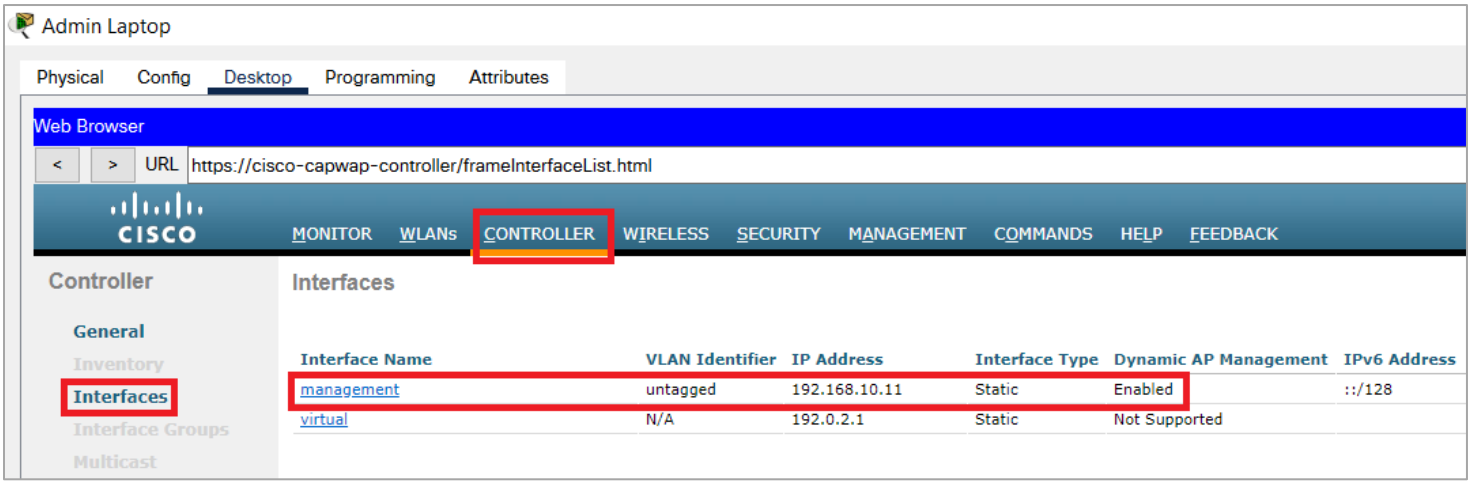


Verify all scopes are enabled.



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.

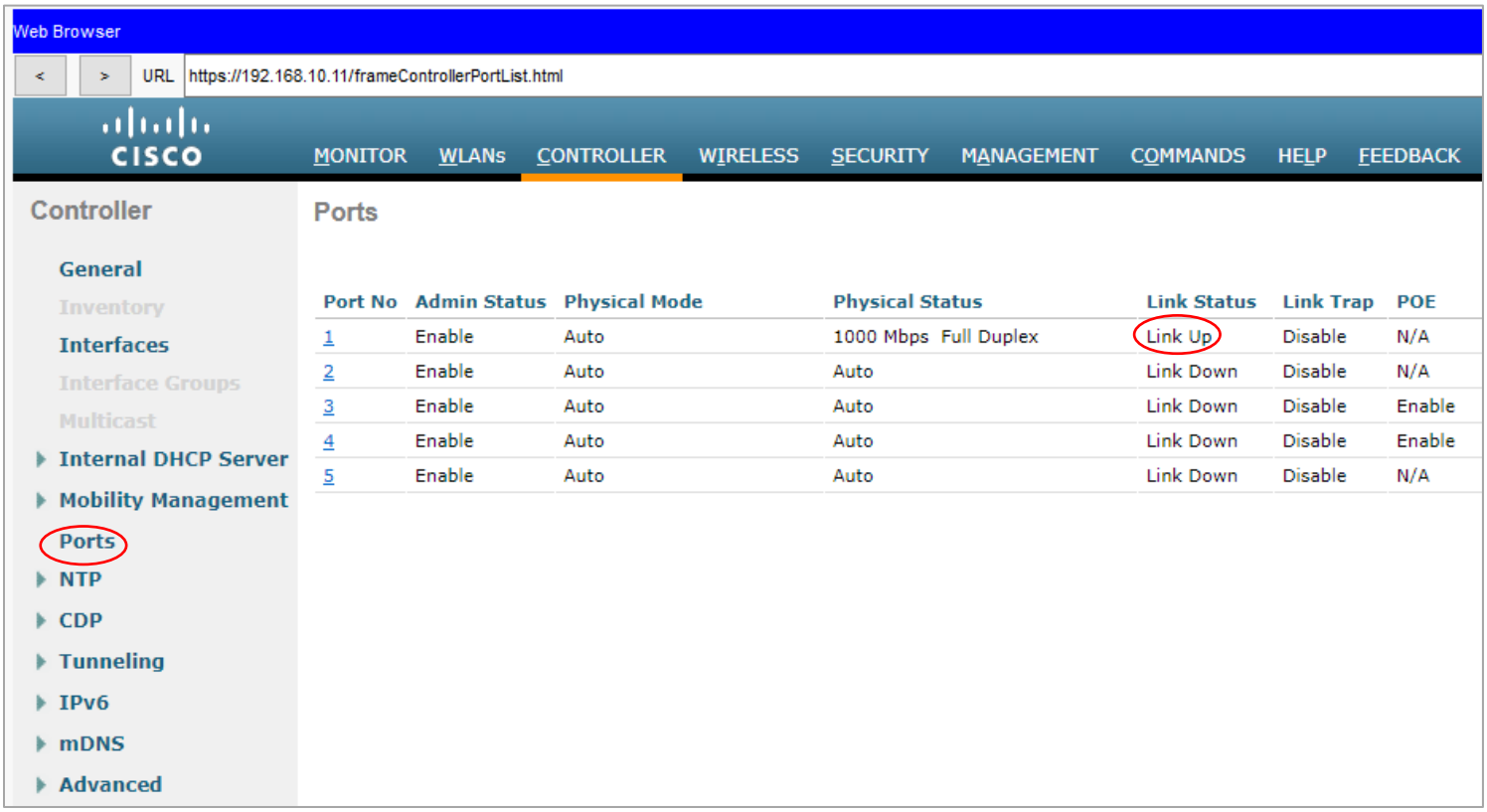


On the Multilayer switch the native VLAN for the port is already set to the management VLAN 10.

```
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
```

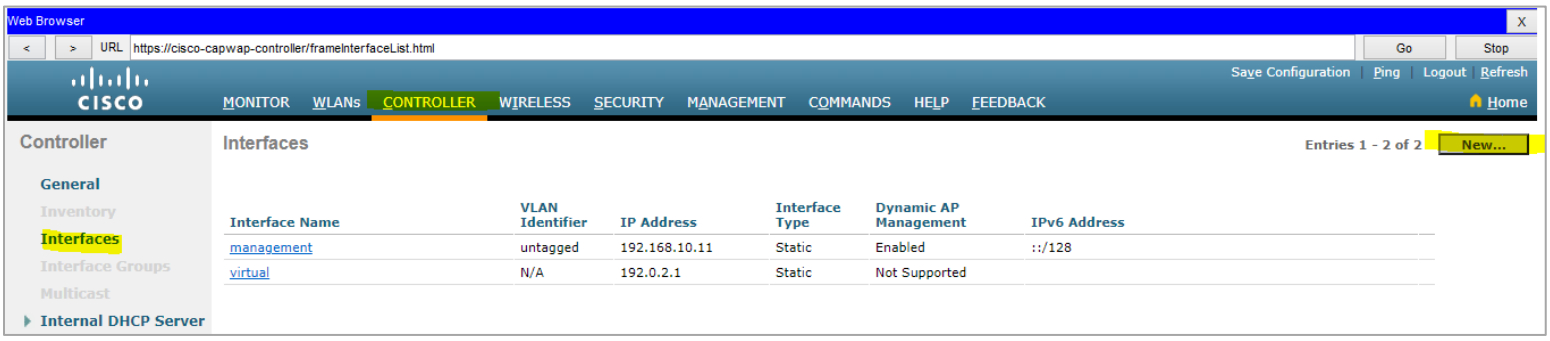
18) Create a logical interface on the Wireless LAN Controller in the Corporate VLAN, with IP address 192.168.22.11 and gateway 192.168.22.1. Wireless clients on the Corporate VLAN should get an IP address from the management interface of the Wireless LAN Controller.

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

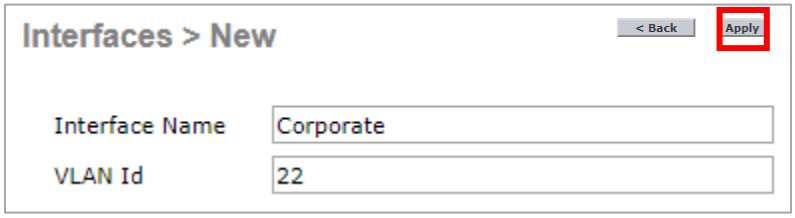


Port 1 is connected.

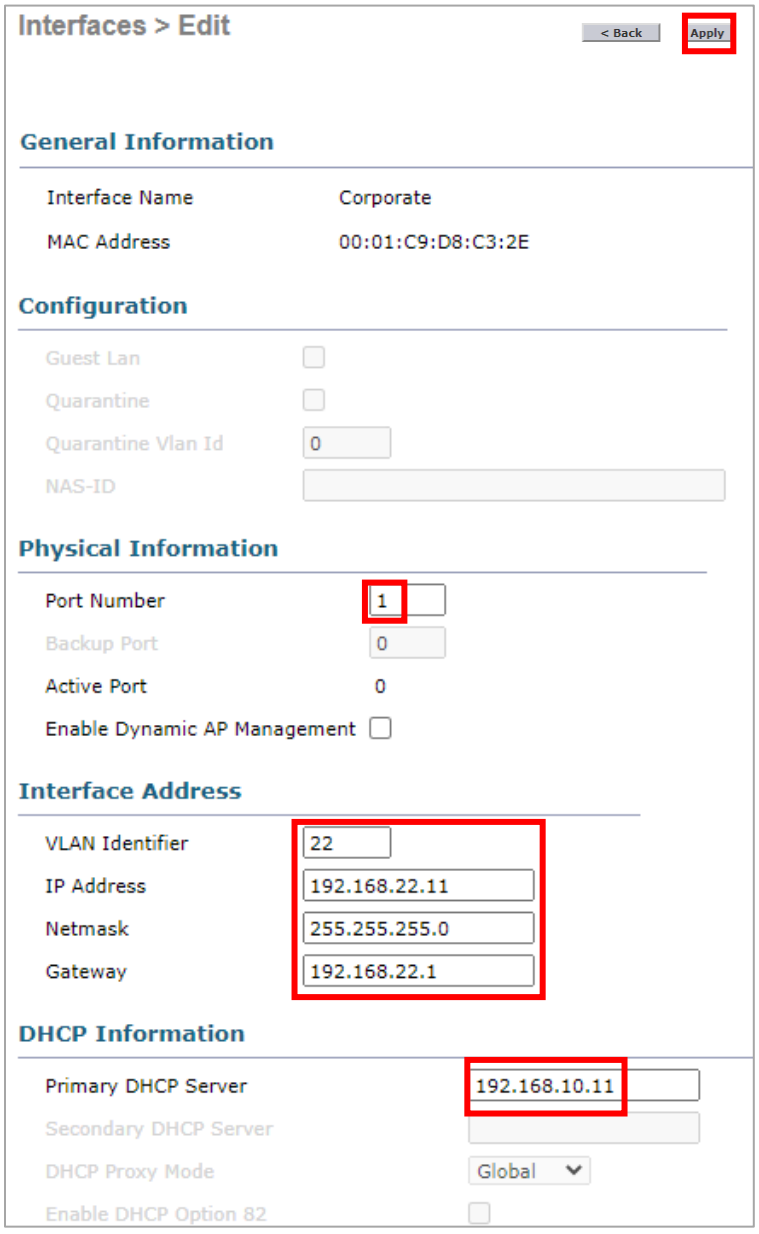
Click ‘Controller’ > ‘Interfaces’ then ‘New’



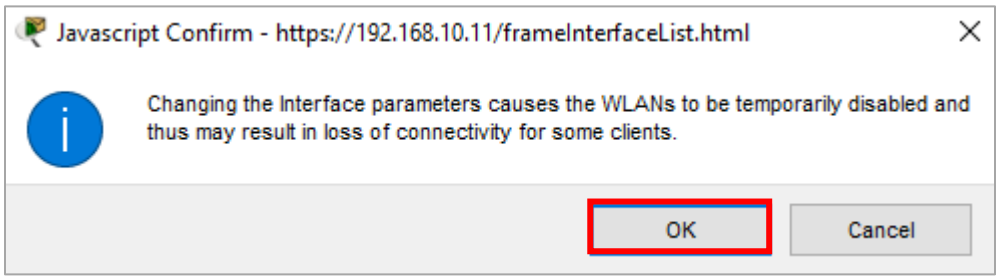
Enter Interface Name ‘Corporate’ and VLAN ID ‘22’ then click ‘Apply’



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.



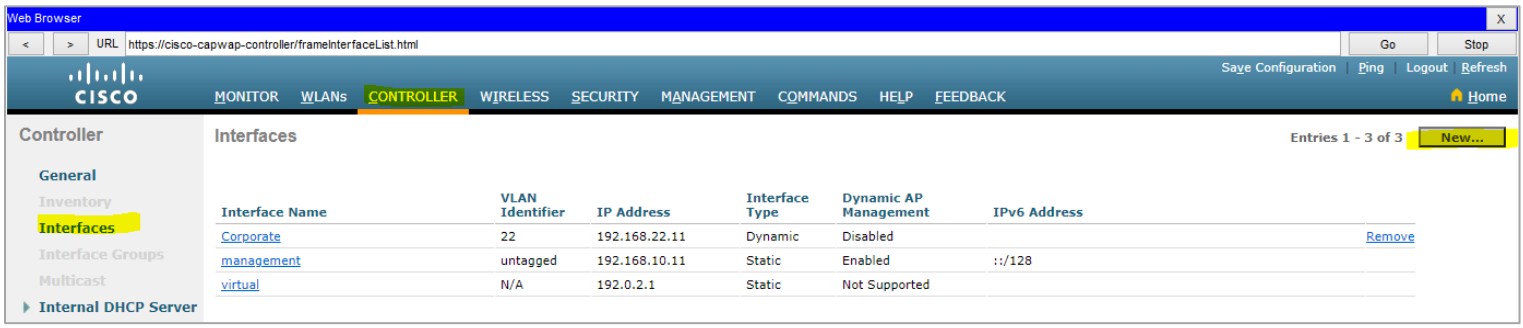
Click on Apply and then on ‘OK’ on the warning message. No wireless clients are connected yet so there will be no disruption.



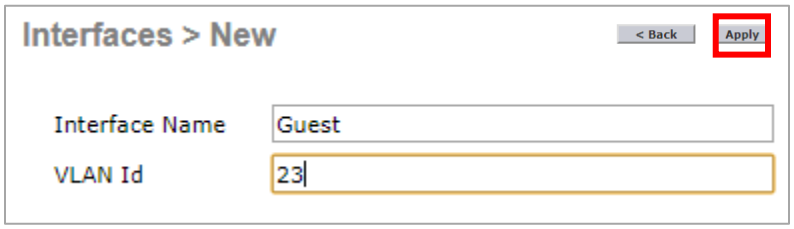
Go back to the interfaces page.

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.

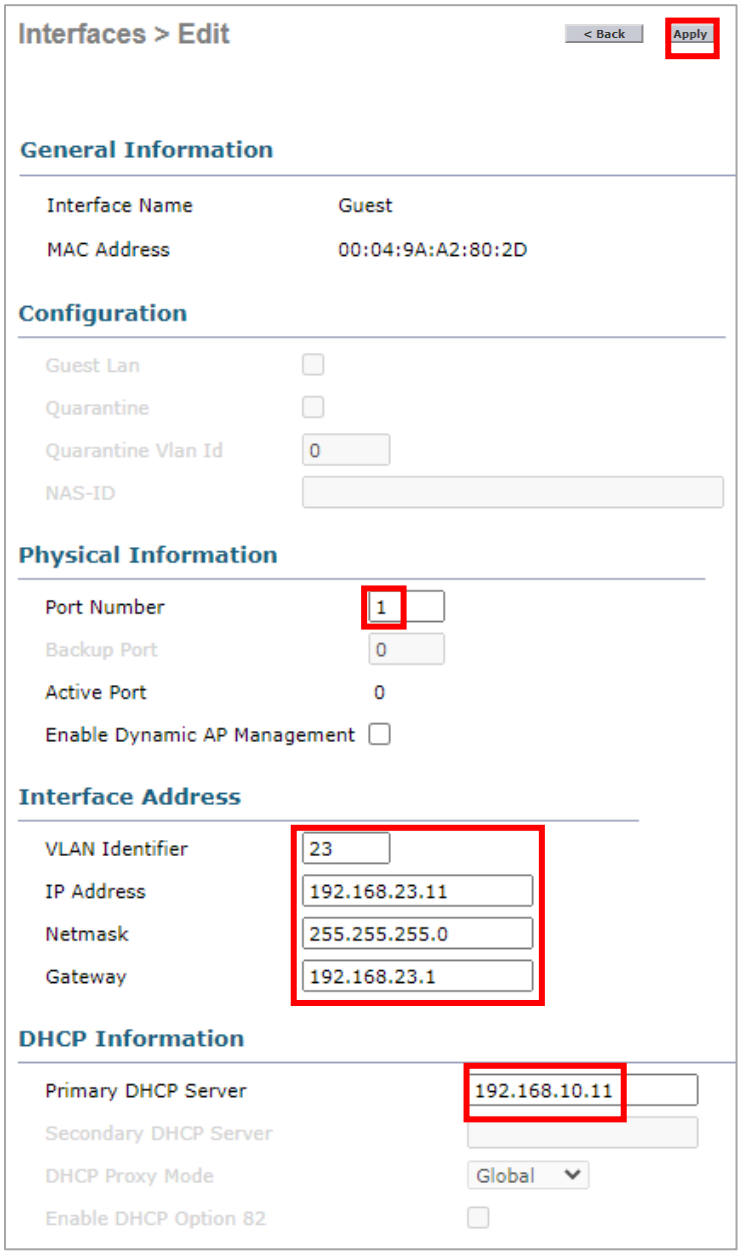
Click ‘Controller’ > ‘Interfaces’ then ‘New’



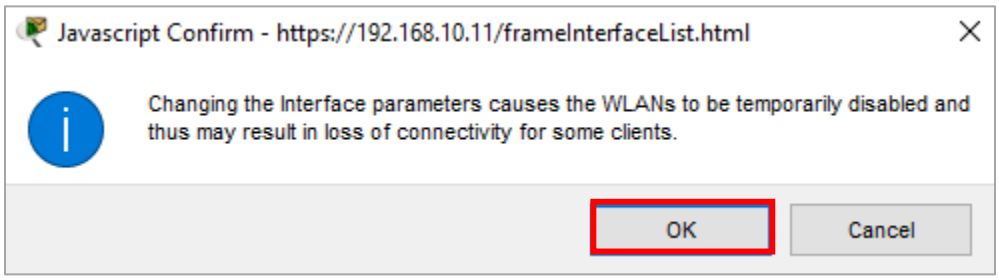
Enter Interface Name ‘Guest and VLAN ID ‘23’ then click ‘Apply’



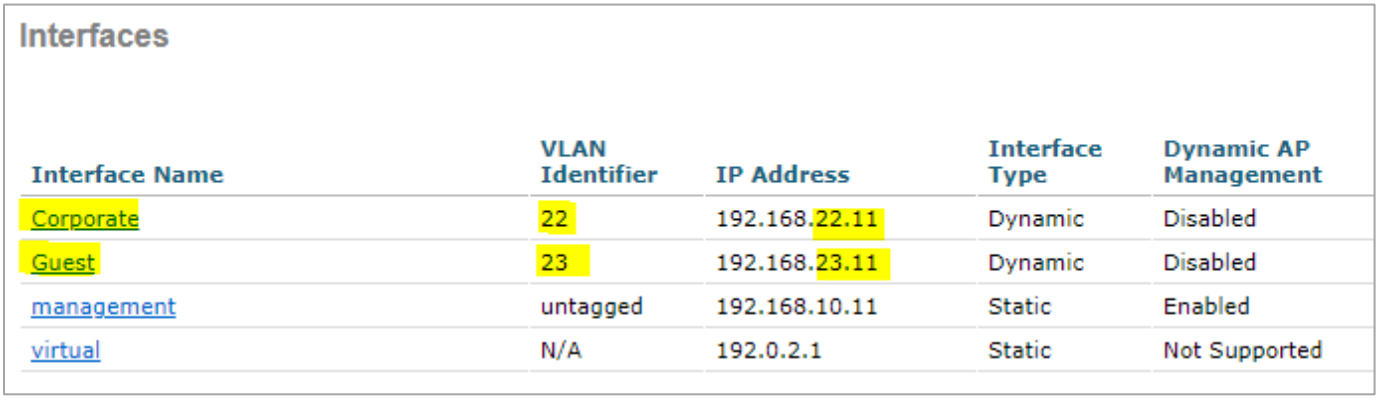
Enter the details for the VLAN interface. It should be associated with Port Number 1, and the 192.168.10.11 management address of the WLC should be configured as the DHCP server.



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

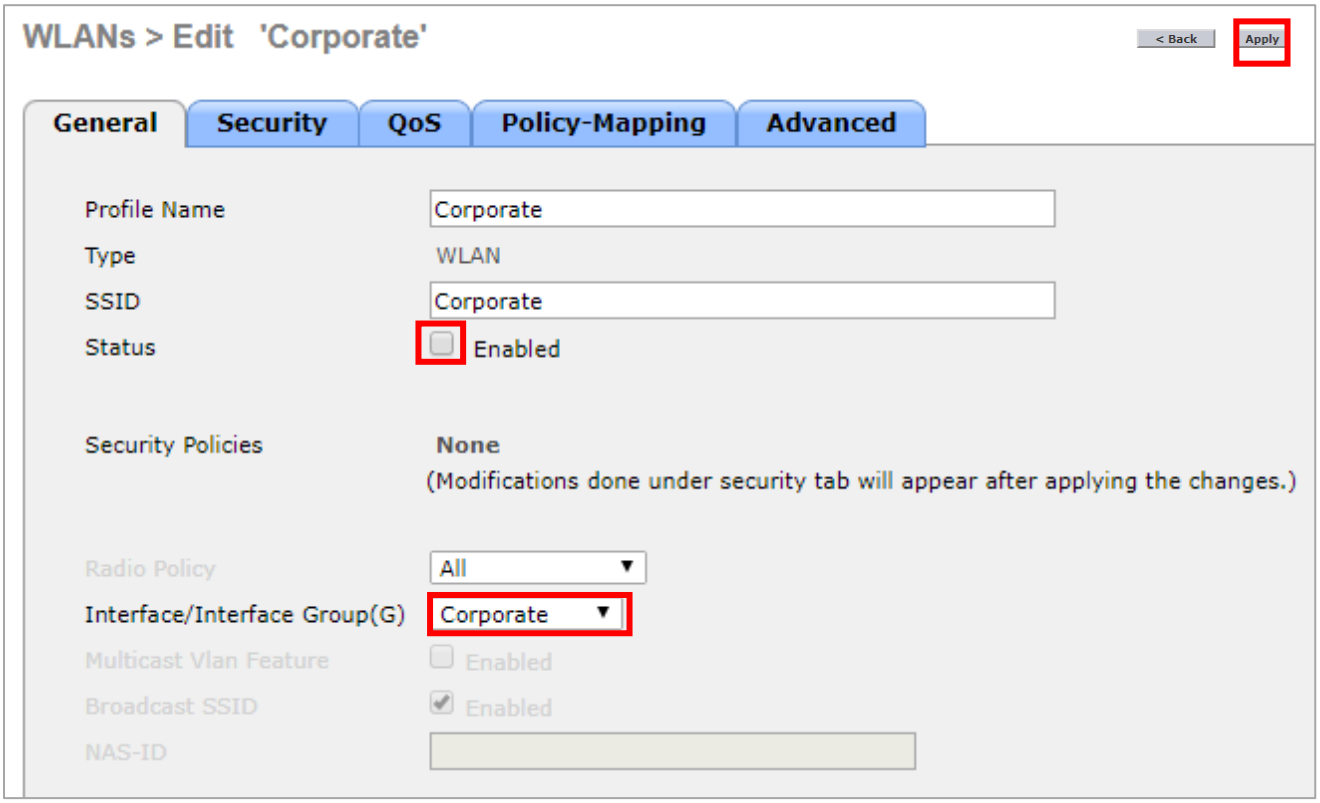
Wireless LANs

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.

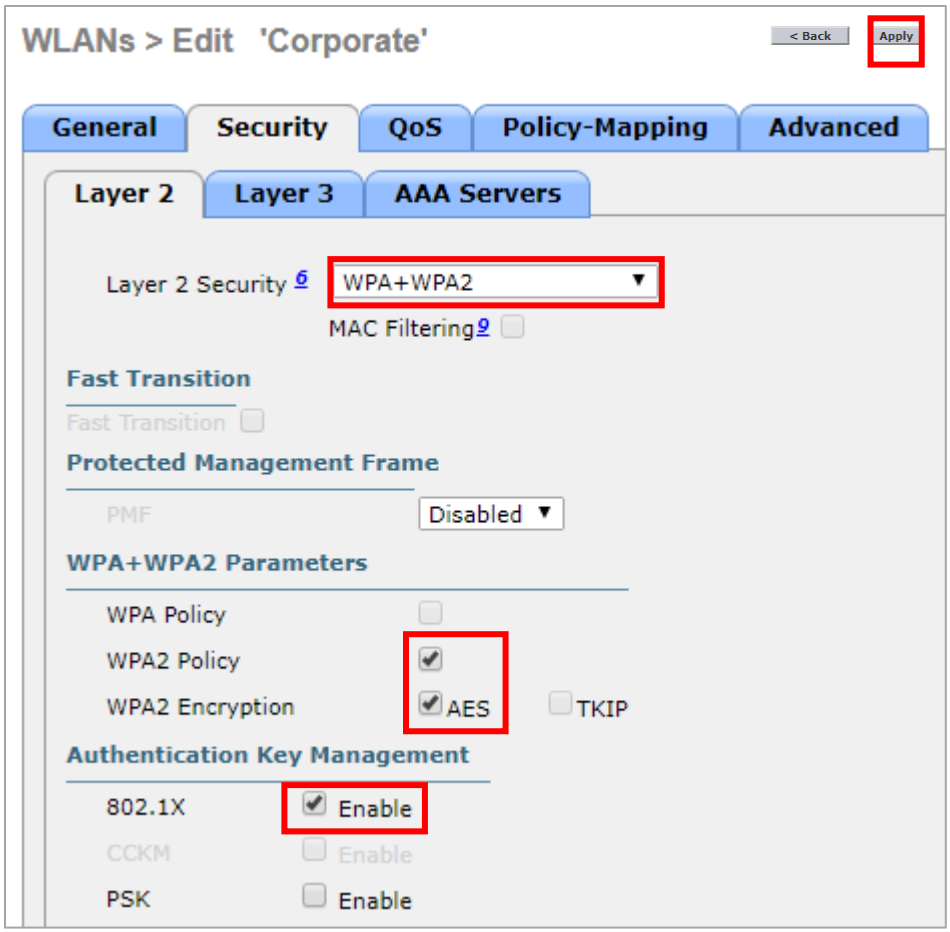
Click on ‘WLANs’, select ‘Create New’ in the drop-down then click ‘Go’

Enter the details then click ‘Apply’

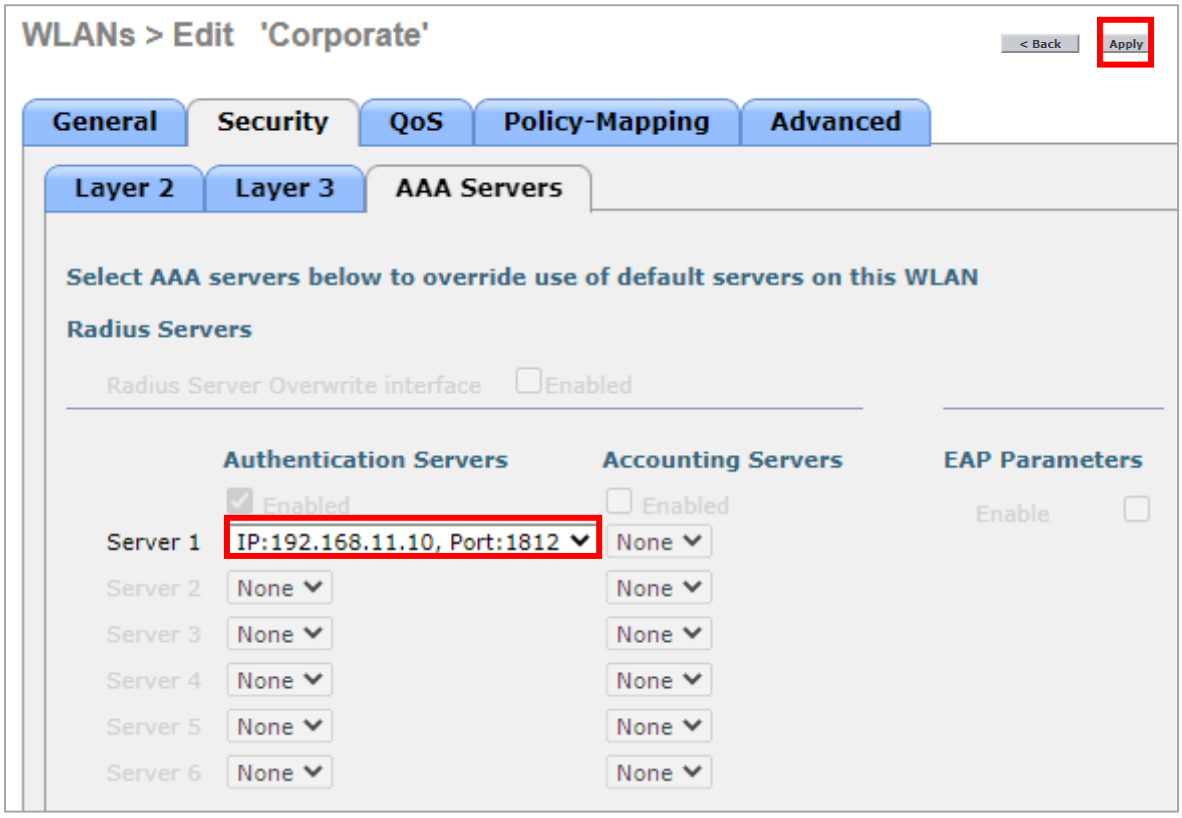
Associate the WLAN with the ‘Corporate’ interface. Do not enable the status as you haven’t configured the security settings yet. Click ‘Apply’.



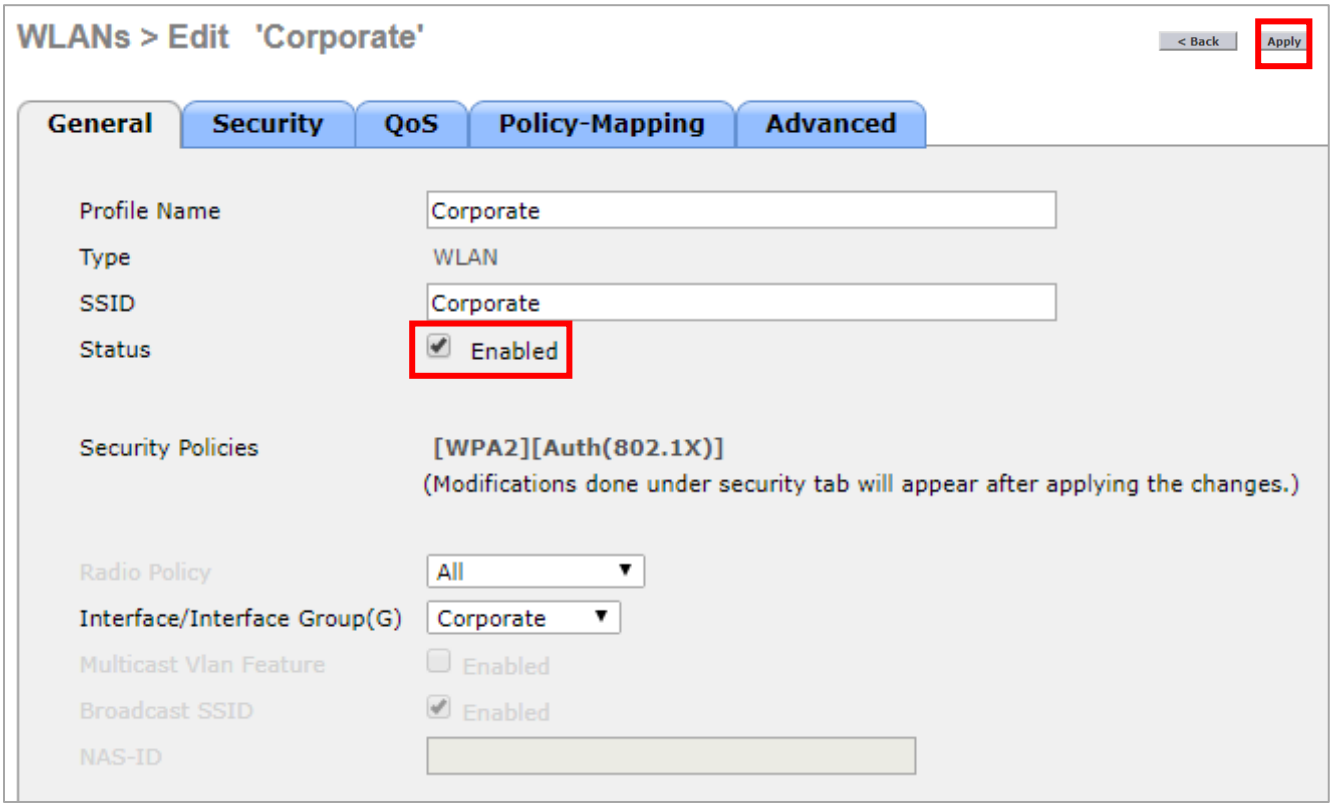
Click on the ‘Security’ tab and ensure Layer 2 Security is ‘WPA + WPA2’, the WPA2 Policy is applied with AES encryption, and Authentication Key Management is 802.1X then click ‘Apply’.



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’.



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

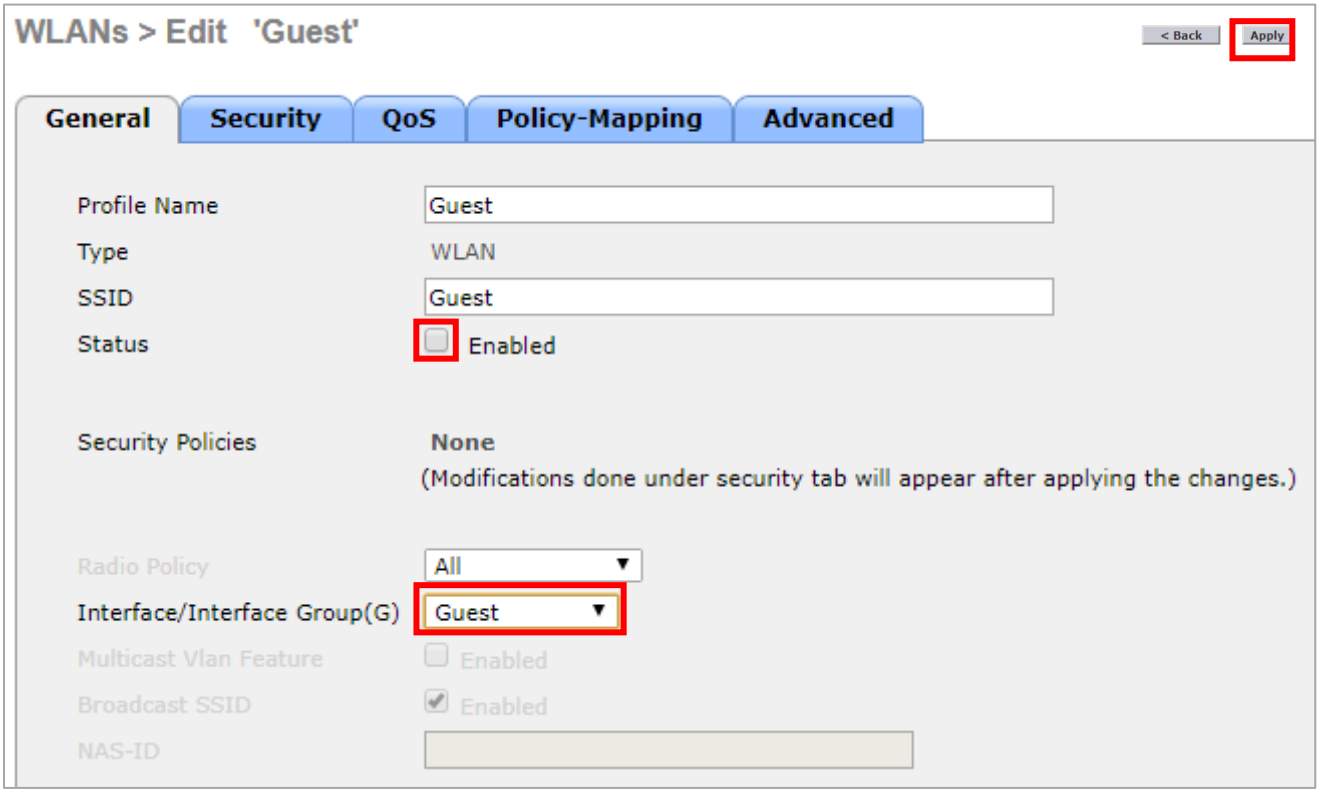


21) Create the wireless LAN named ‘Guest’. WPA2 AES encryption should be used, and clients should authenticate with the pre-shared key **Flackbox3**.

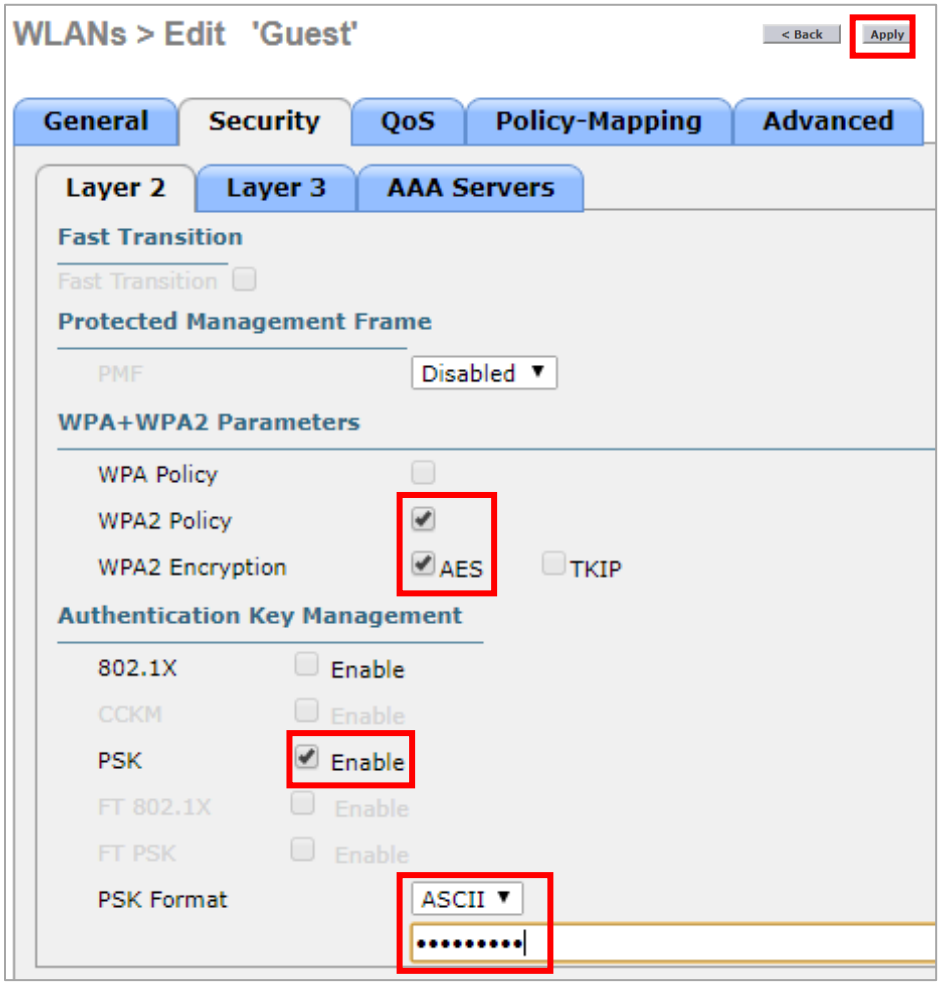
Click on ‘WLANs’, select ‘Create New’ in the drop-down then click ‘Go’

Enter the details then click ‘Apply’

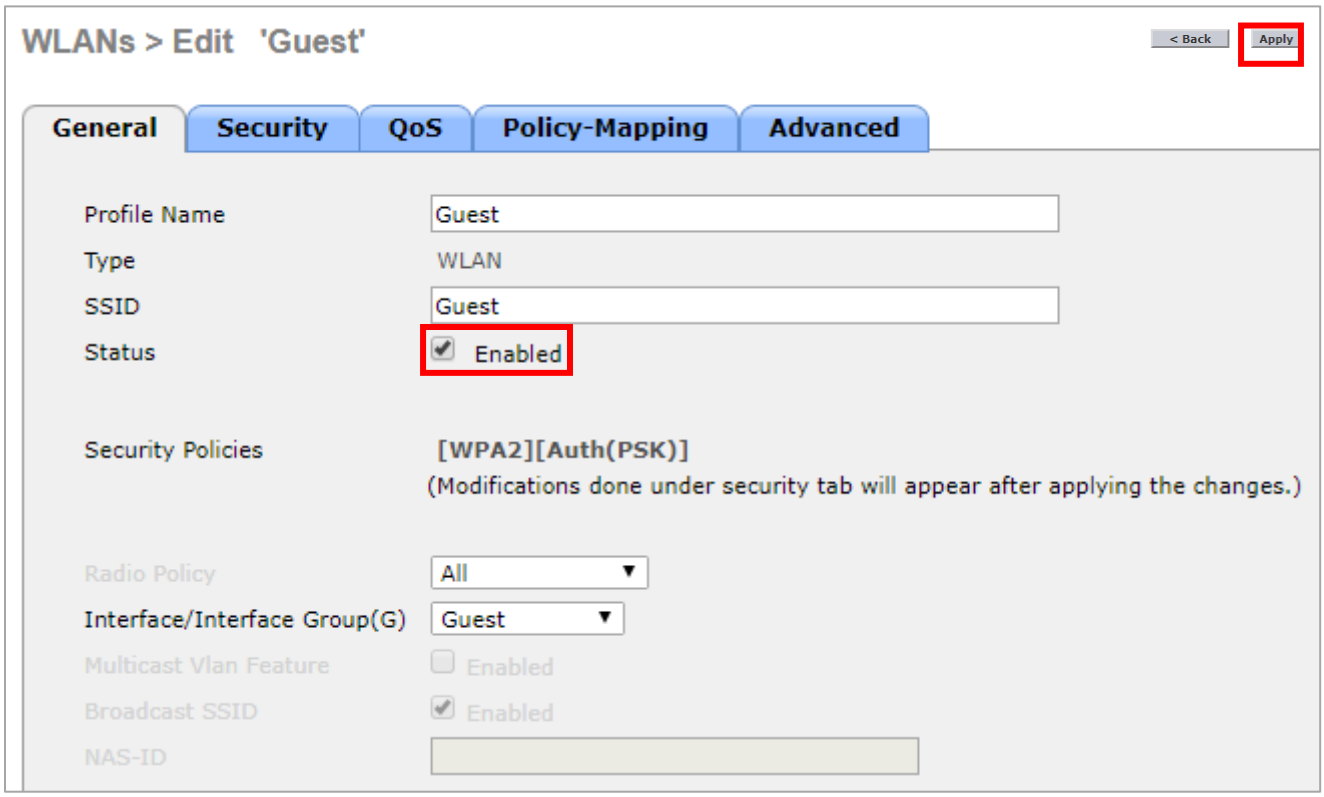
Associate the WLAN with the ‘Guest’ interface and click ‘Apply’. Do not enable the status as you haven’t configured the security settings yet.



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.

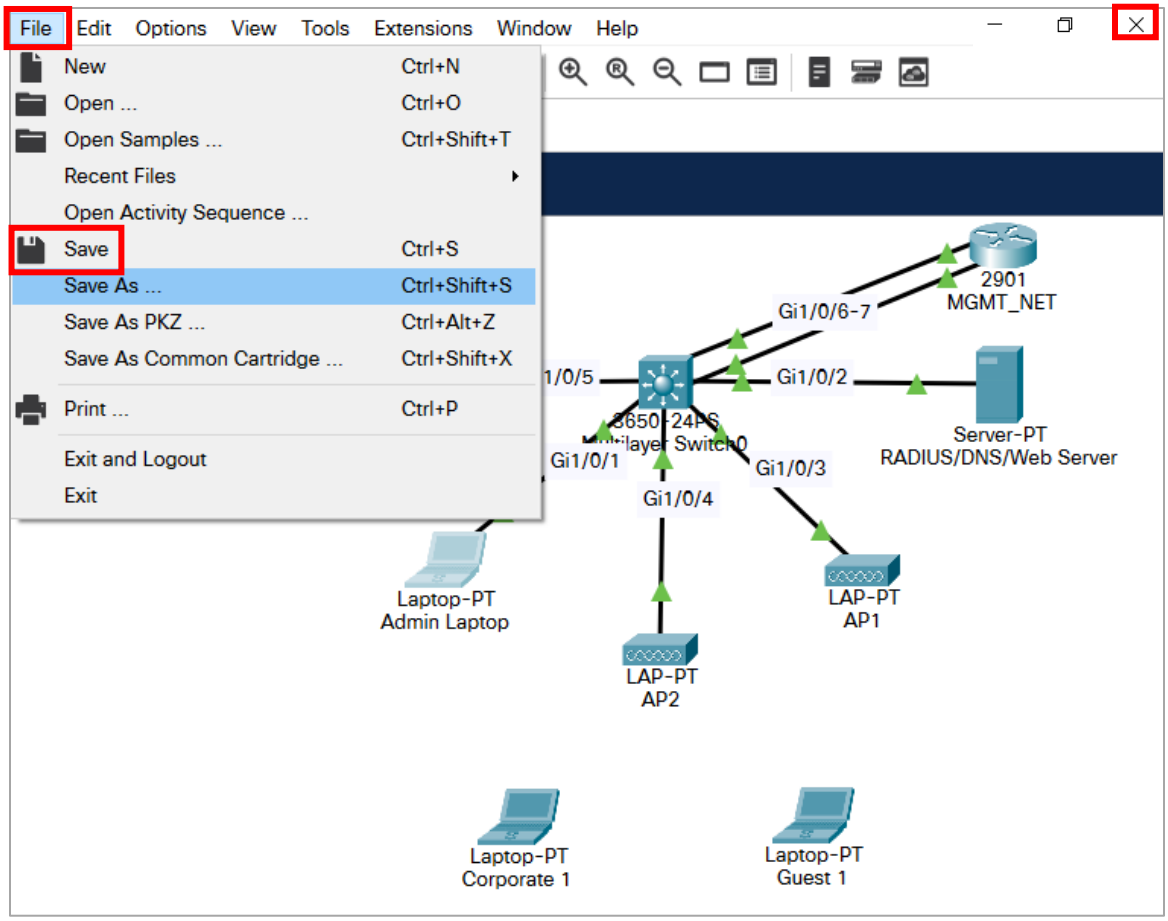


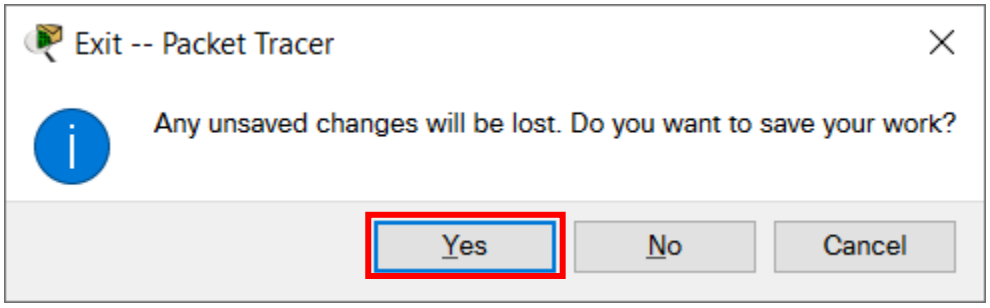
On the ‘General’ tab, tick the ‘Enabled’ checkbox to enable the WLAN and click ‘Apply’.



Click ‘WLANs’ to verify both WLANs are enabled.

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.)

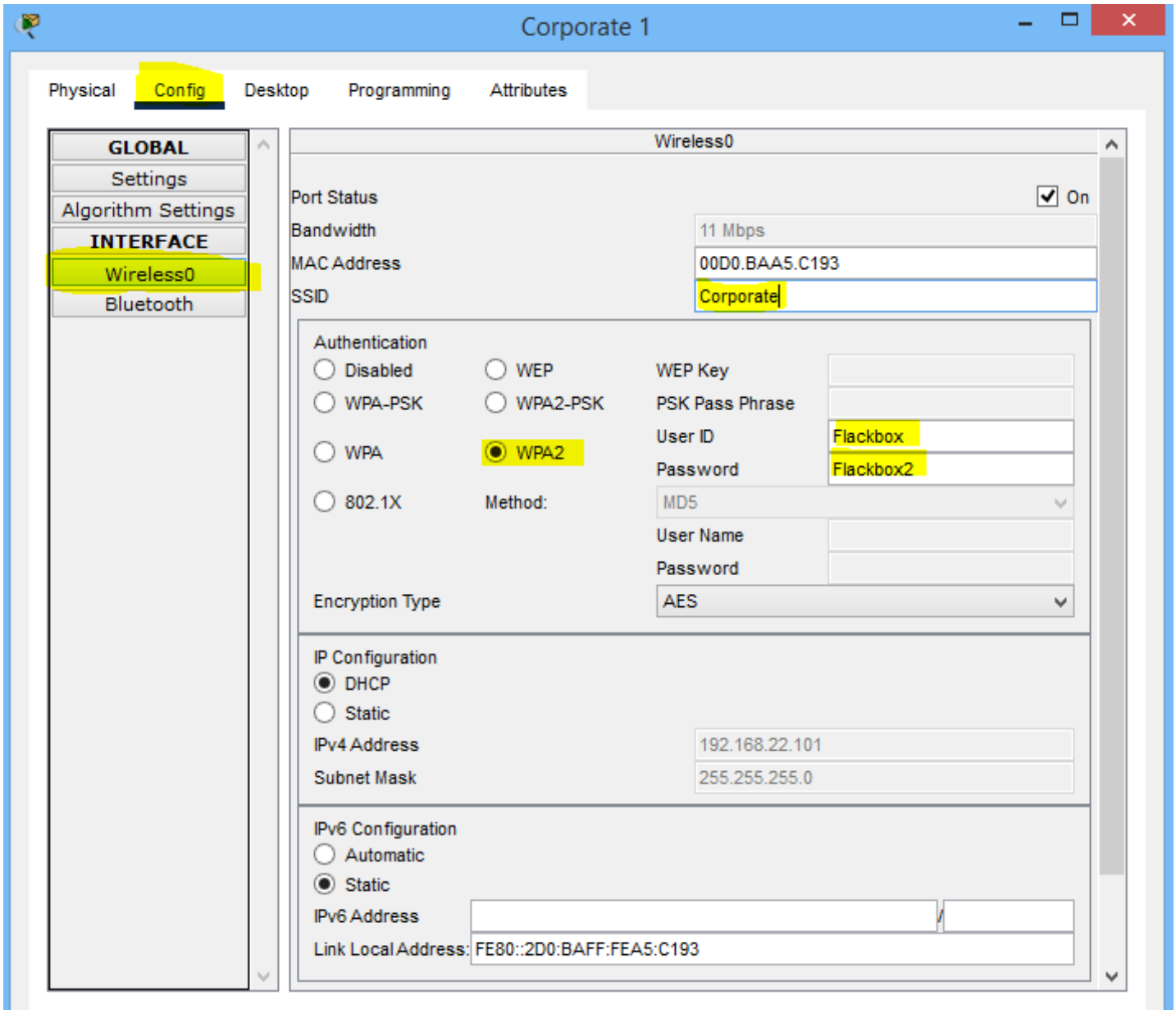




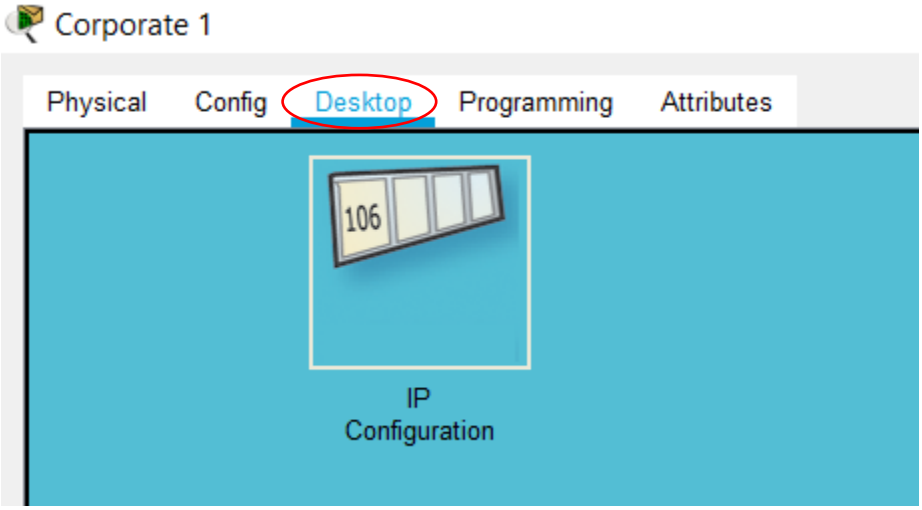
Join Clients to the Wireless LANs

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.

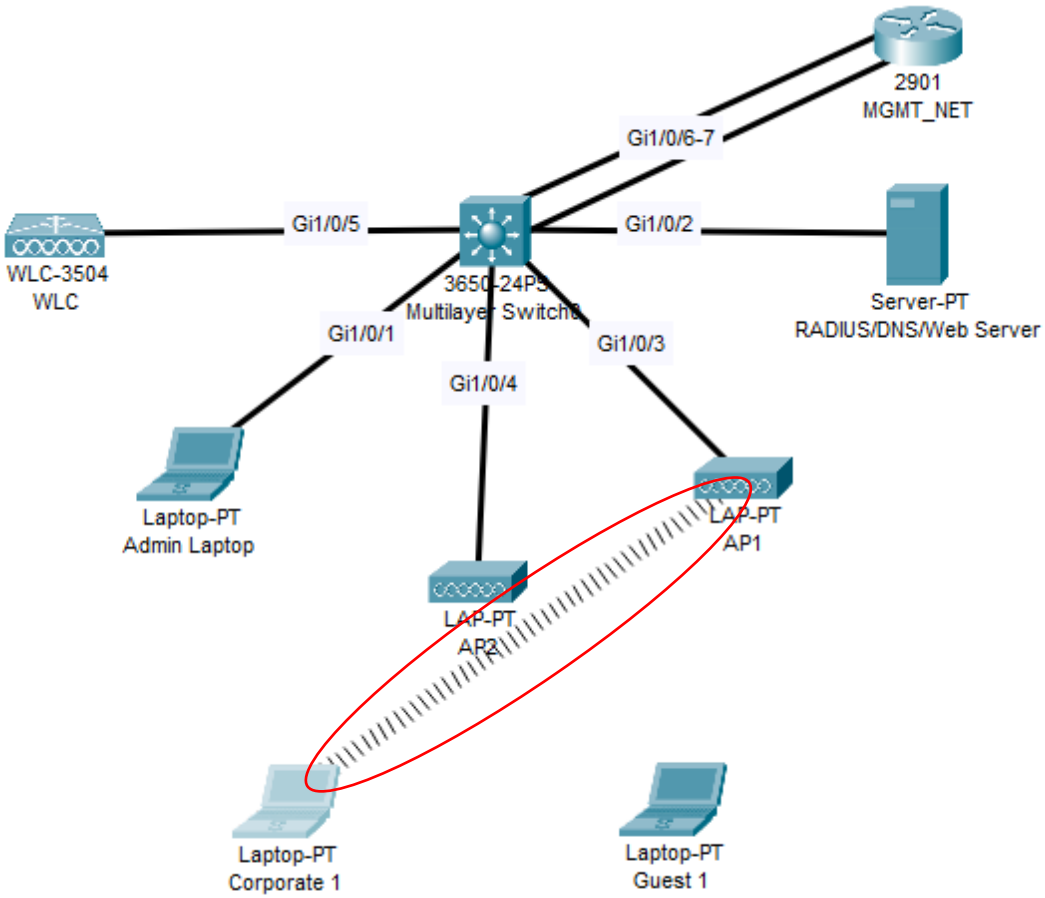
Click on the Corporate1 laptop in the Packet Tracer main window, then 'Config' and 'Wireless0'. Enter the SSID 'Corporate', select WPA2 authentication then enter the user ID Flackbox and password Flackbox2. Do not change the encryption type, it's AES by default.



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

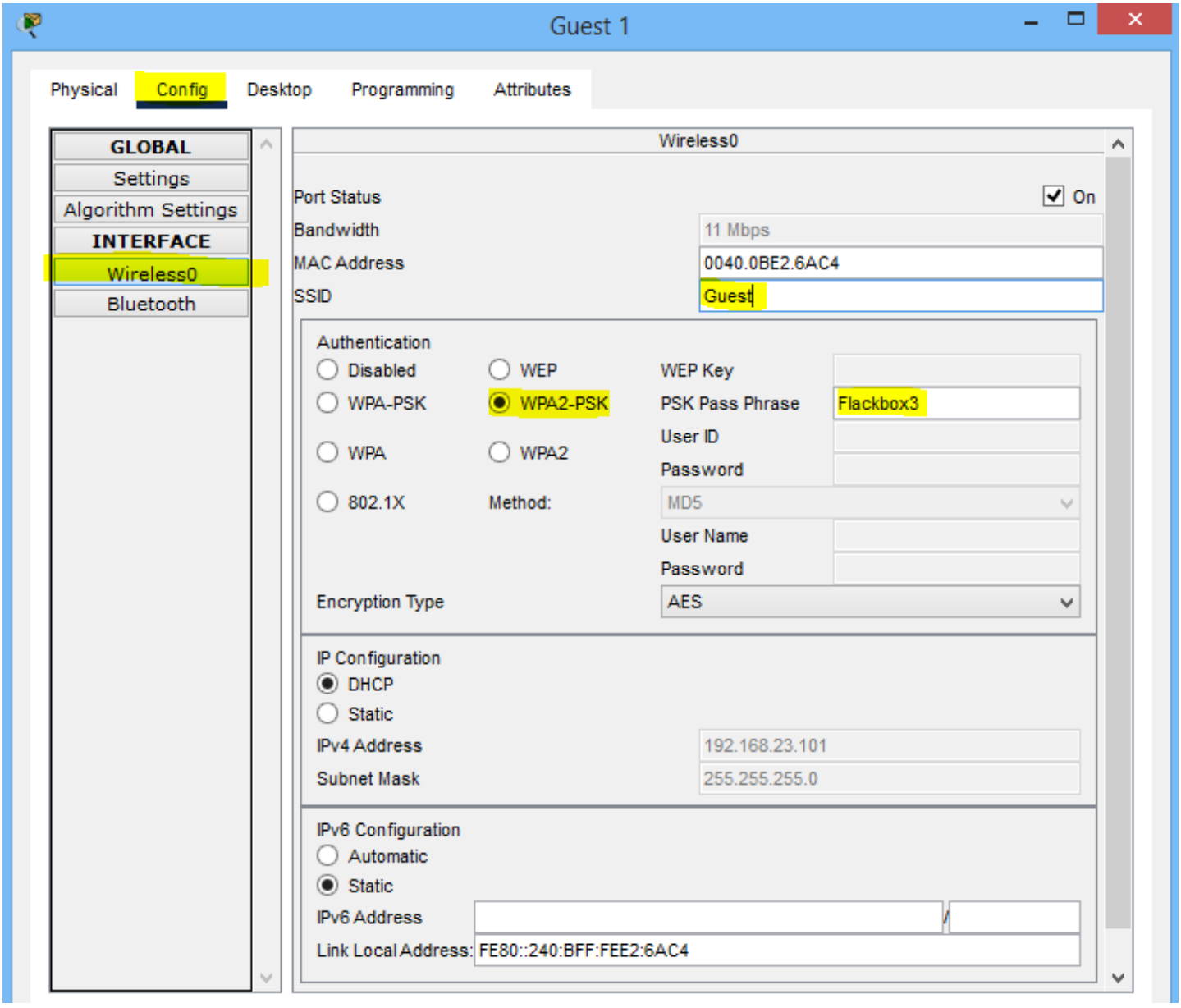


Verify the laptop connects in the Packet Tracer main window.

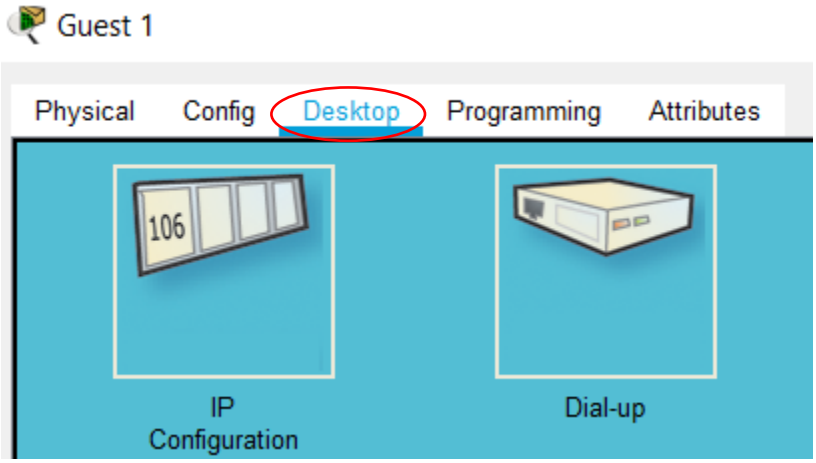


24) Connect to the ‘Guest’ WLAN from the Guest1 laptop.

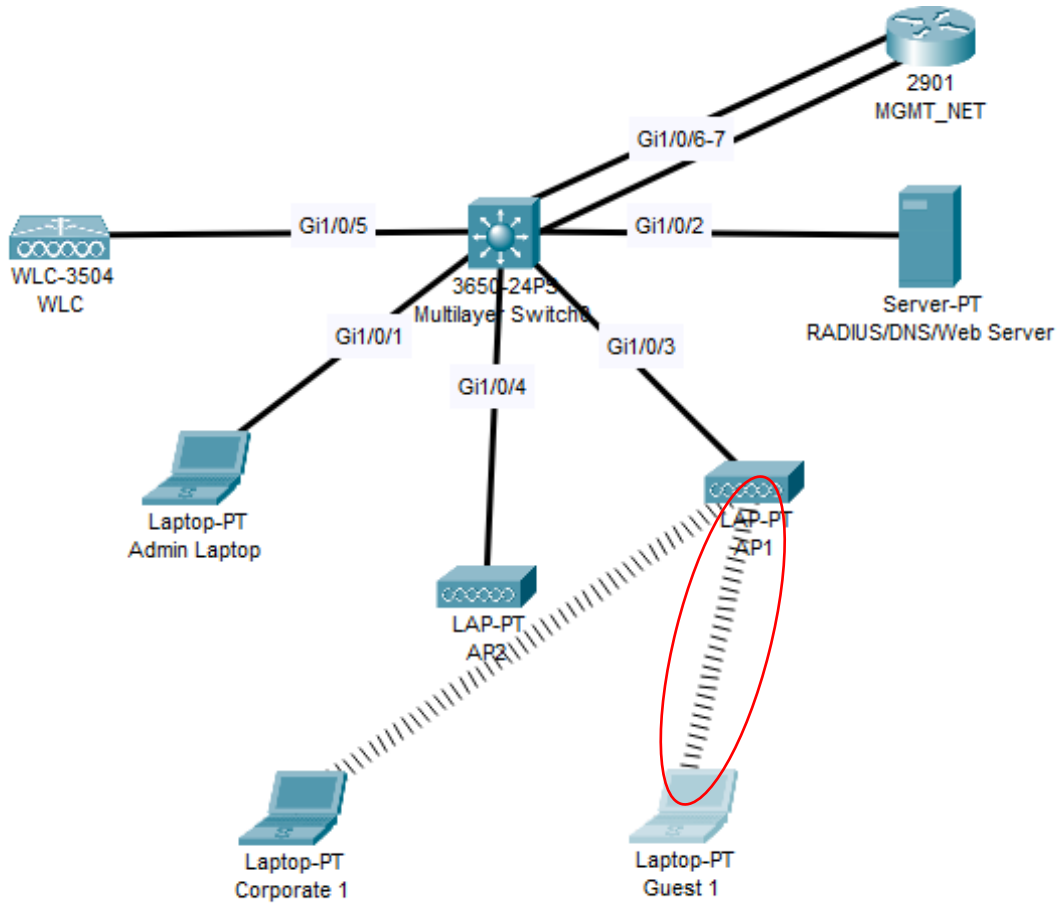
Click on the Guest1 laptop in the Packet Tracer main window, then ‘Config’ and ‘Wireless0’. Enter the SSID ‘Guest’, select WPA2-PSK authentication then enter the pre-shared key **Flackbox3**. Do not change the encryption type, it’s AES by default.



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

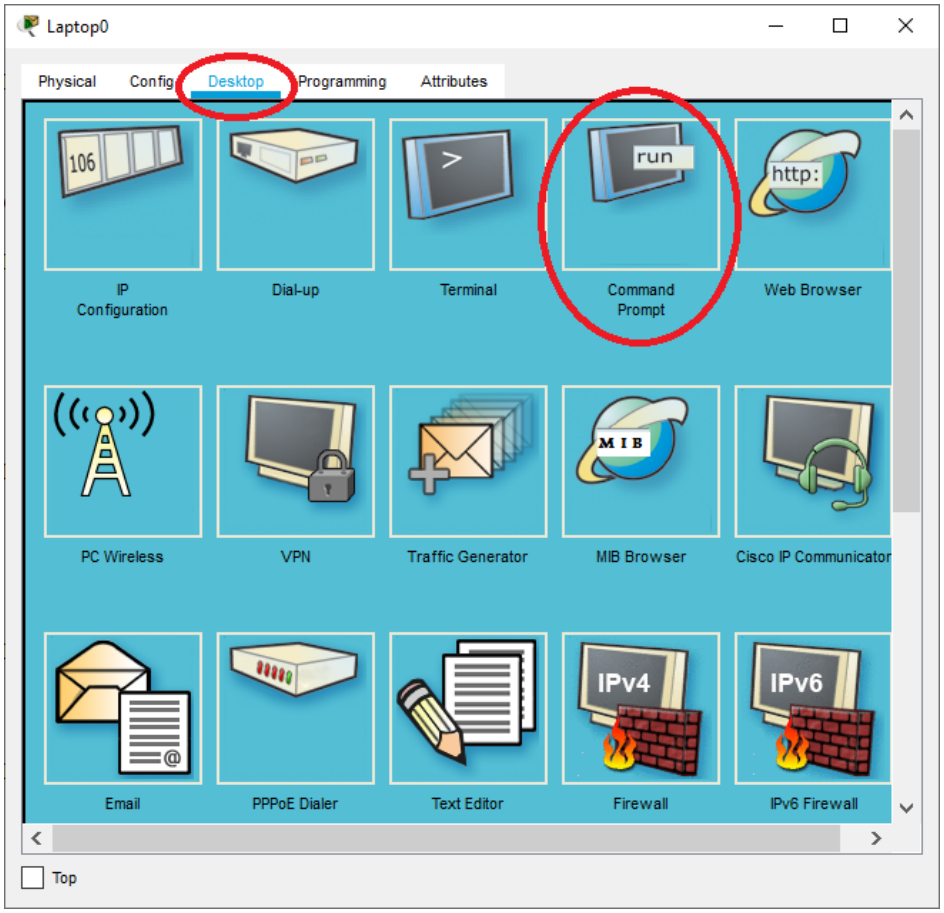


Verify the laptop connects in the Packet Tracer main window.



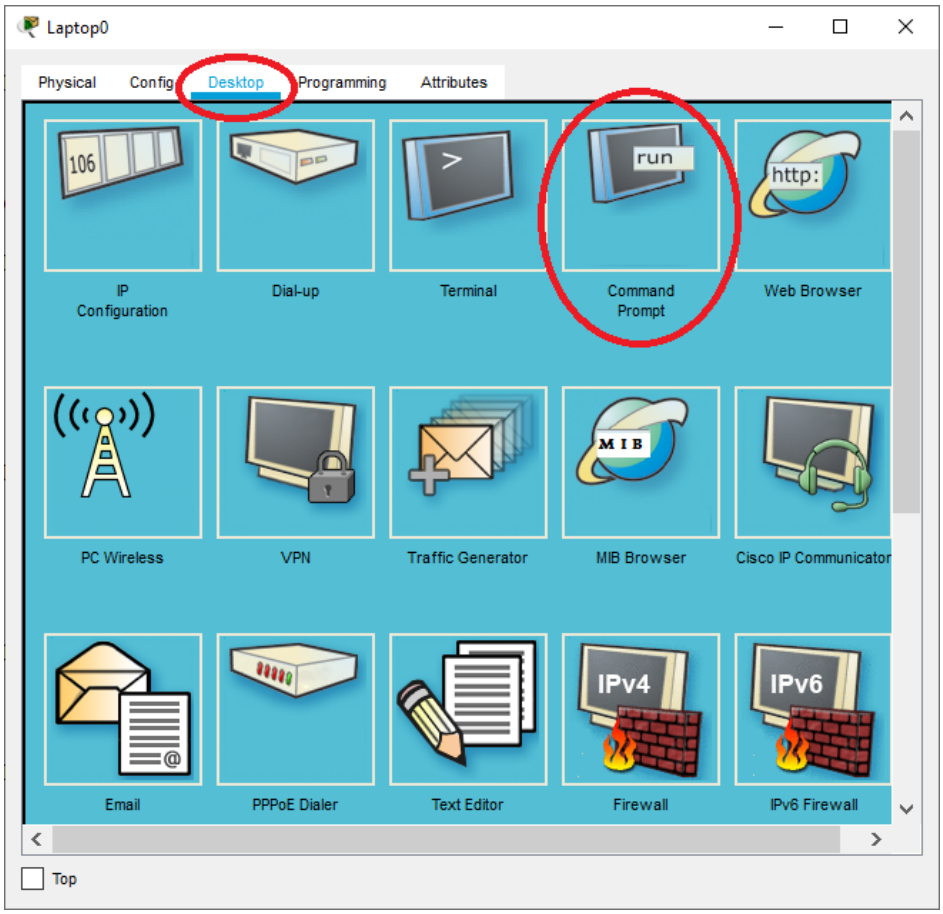
25) Verify connectivity by pinging the Corporate1 laptop from the Guest1 laptop.

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
```