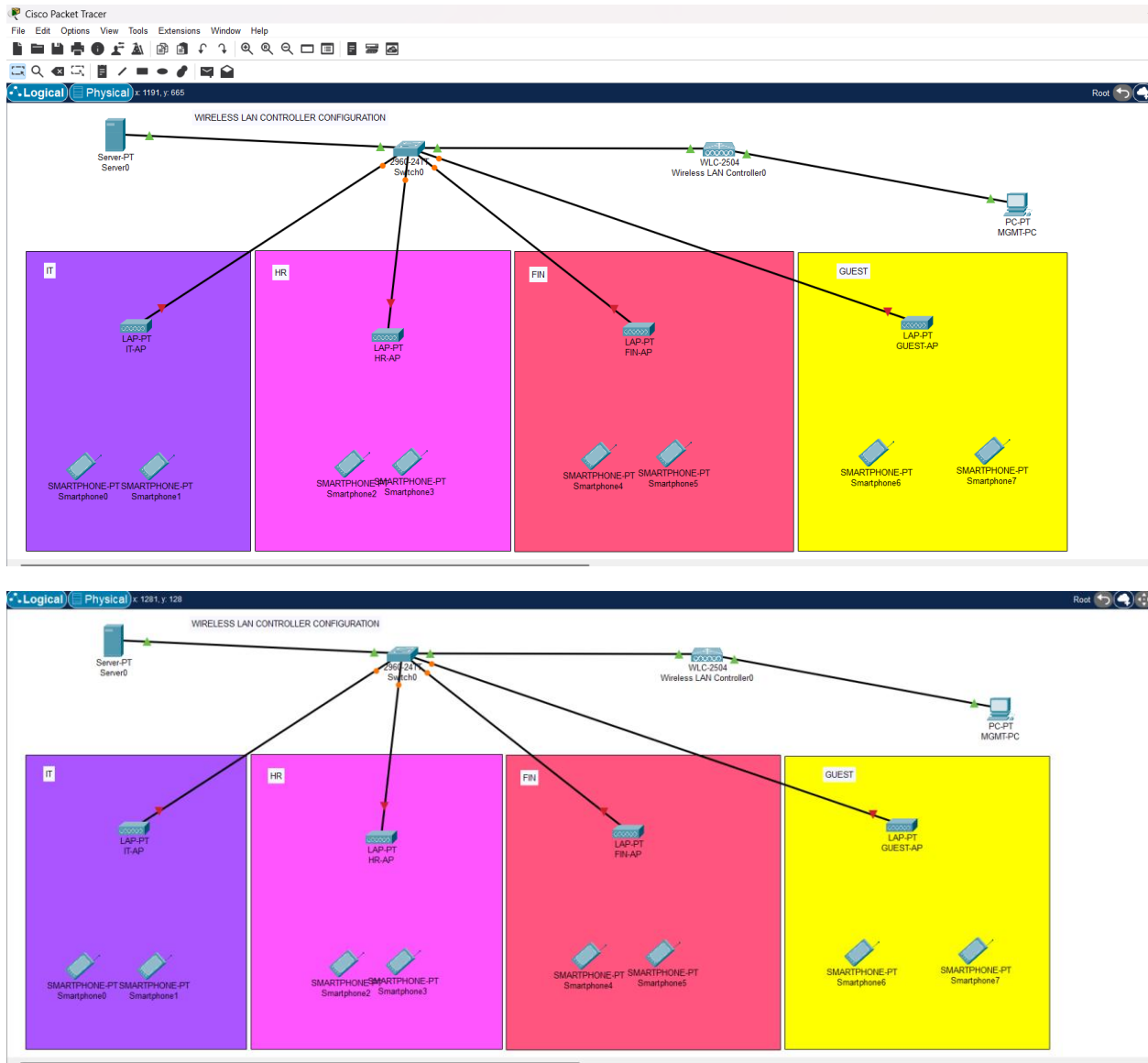
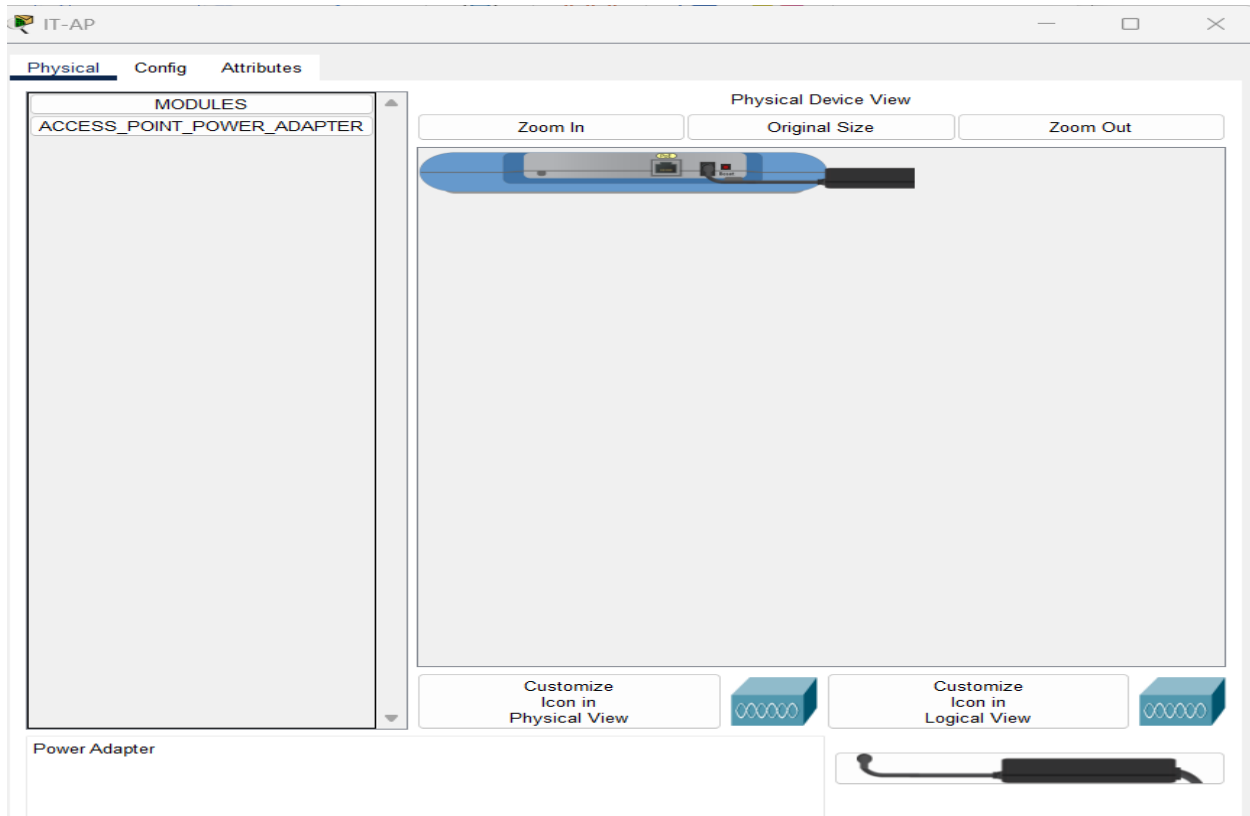


## Wireless LAN Controller (WLC) Using Cisco Packet Tracer

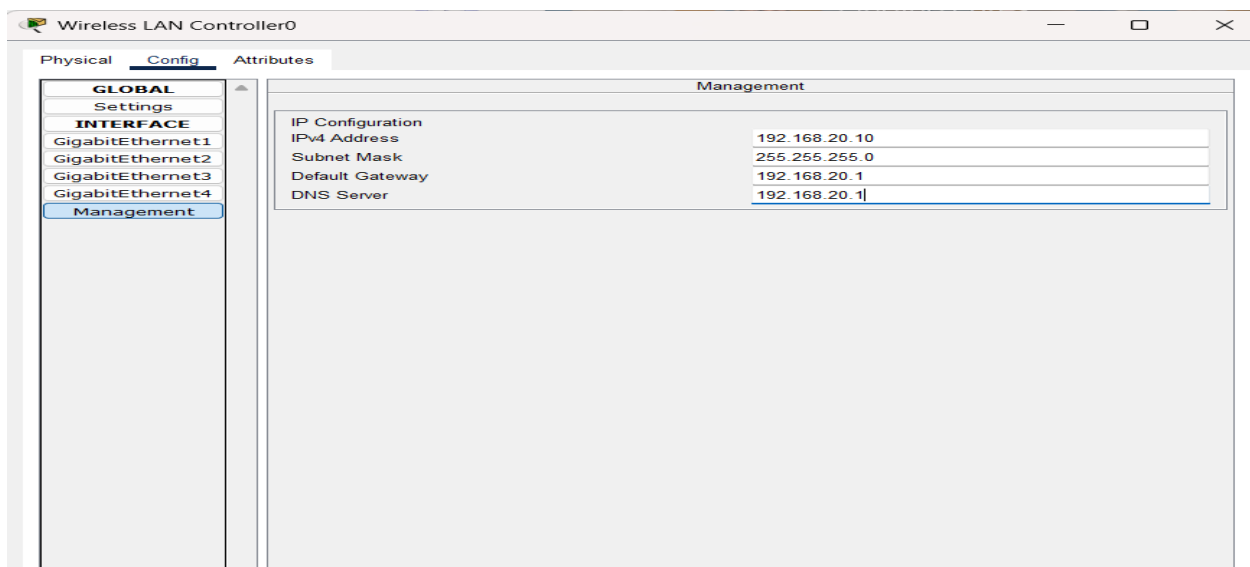


**Power on the Access Point**



We will configure IP address to the server, Wireless LAN Controller and Management PC

### Configuration of IP Address on Wireless LAN Controller



## IP Configuration for Management PC

The screenshot shows a window titled "MGMT-PC" with a standard Windows-style title bar (minimize, maximize, close buttons). Below the title bar is a tabbed interface with four tabs: "Physical", "Config", "Desktop", and "Attributes". The "Config" tab is active, and within it, the "Desktop" sub-tab is selected. The main content area is titled "IP Configuration" with a blue header bar and a close button (X) on the right. Below the header, there is a dropdown menu for "Interface" set to "FastEthernet0". The configuration is divided into three sections: "IP Configuration", "IPv6 Configuration", and "802.1X". In the "IP Configuration" section, the "Static" radio button is selected, and the fields for IPv4 Address (192.168.20.7), Subnet Mask (255.255.255.0), Default Gateway (192.168.20.1), and DNS Server (192.168.20.1) are filled. In the "IPv6 Configuration" section, the "Static" radio button is also selected, and the "Link Local Address" field is filled with "FE80::2E0:F7FF:FE9B:C07D". The "802.1X" section has the "Use 802.1X Security" checkbox unchecked, and the "Authentication" dropdown is set to "MD5". The "Username" and "Password" fields are empty.

MGMT-PC

Physical Config **Desktop** Programming Attributes

**IP Configuration** X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.20.7

Subnet Mask 255.255.255.0

Default Gateway 192.168.20.1

DNS Server 192.168.20.1

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:F7FF:FE9B:C07D

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

## IP Configuration for Server

Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.20.5

Subnet Mask 255.255.255.0

Default Gateway 192.168.20.1

DNS Server 192.168.20.1

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:A3FF:FE8B:270D

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

Lets create a pool. The purpose of this server is to create a pool, a pool that will be able to provide ip addressing to the Wireless Devices

Services for the wireless LAN controller

Server0

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

Interface

FastEthernet0

Service

On

Off

Pool Name

serverPool

Default Gateway

192.168.20.1

DNS Server

192.168.20.1

Start IP Address :

192

168

20

101

Subnet Mask:

255

255

255

0

Maximum Number of Users :

120

TFTP Server:

0.0.0.0

WLC Address:

192.168.20.10

Add

Save

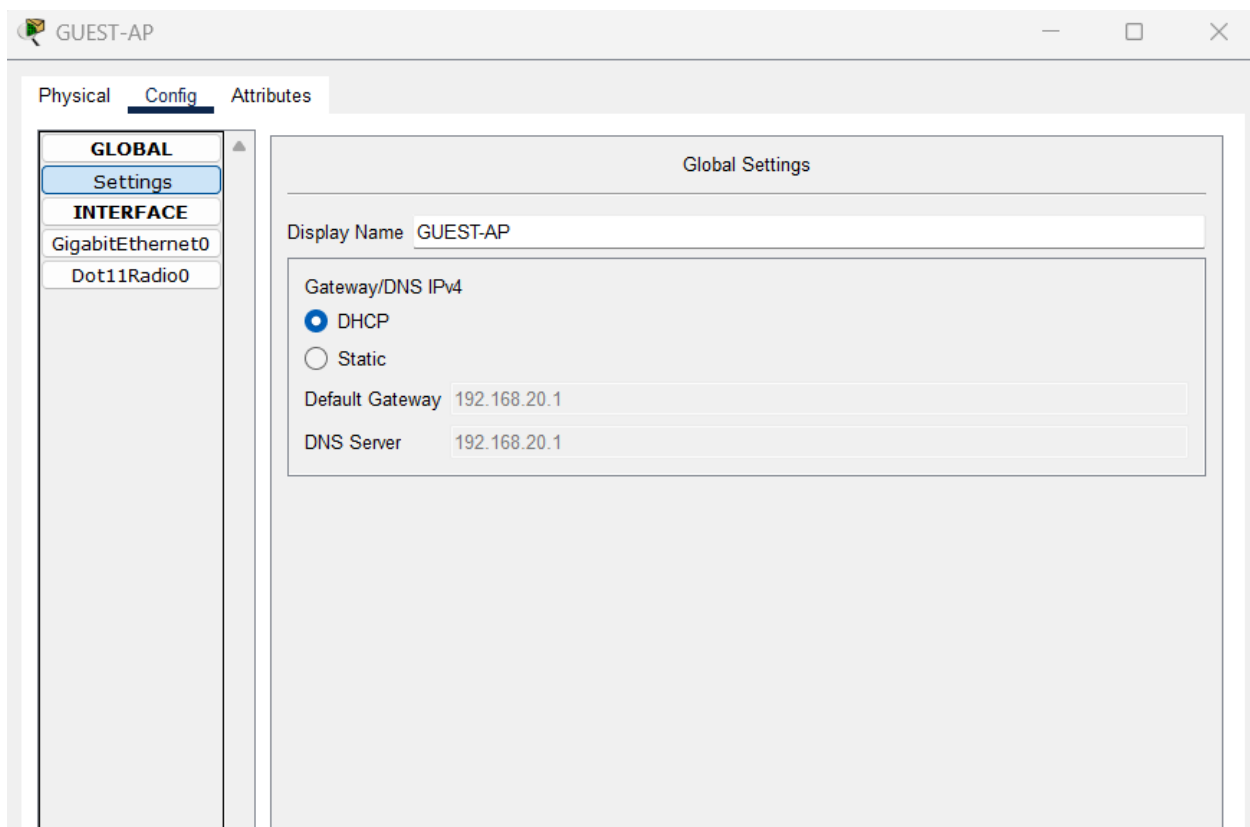
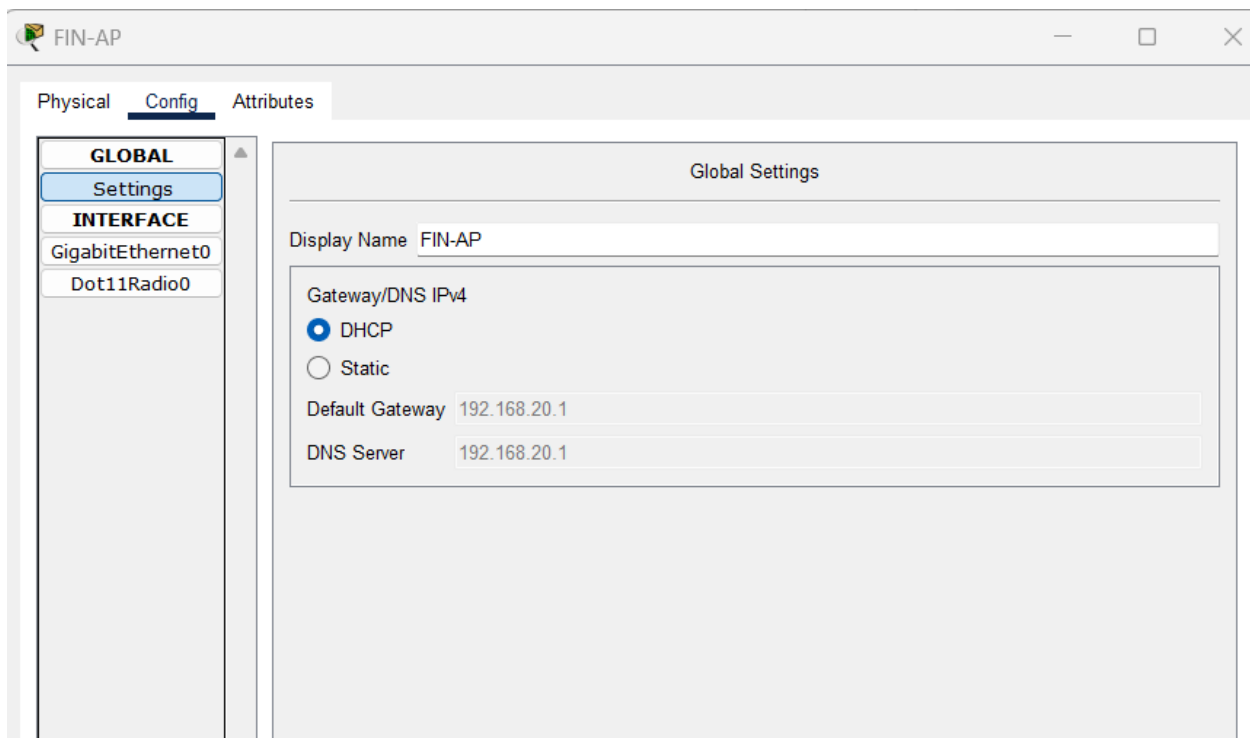
Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.20.1	192.168.20.1	192.168.2...	255.255.2...	120	0.0.0.0	192.168.2...

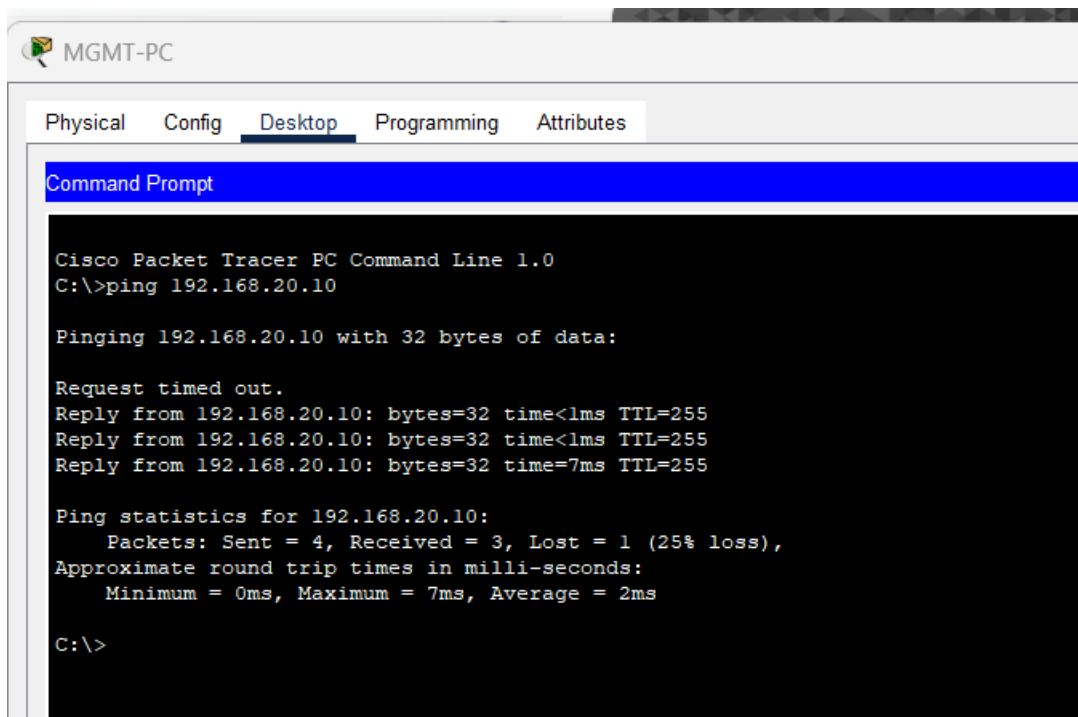
The IP address will be the ip address of the Wireless LAN Controller

The 3 rd step is to turn on the DHCP option of the connecting interface of the access point.



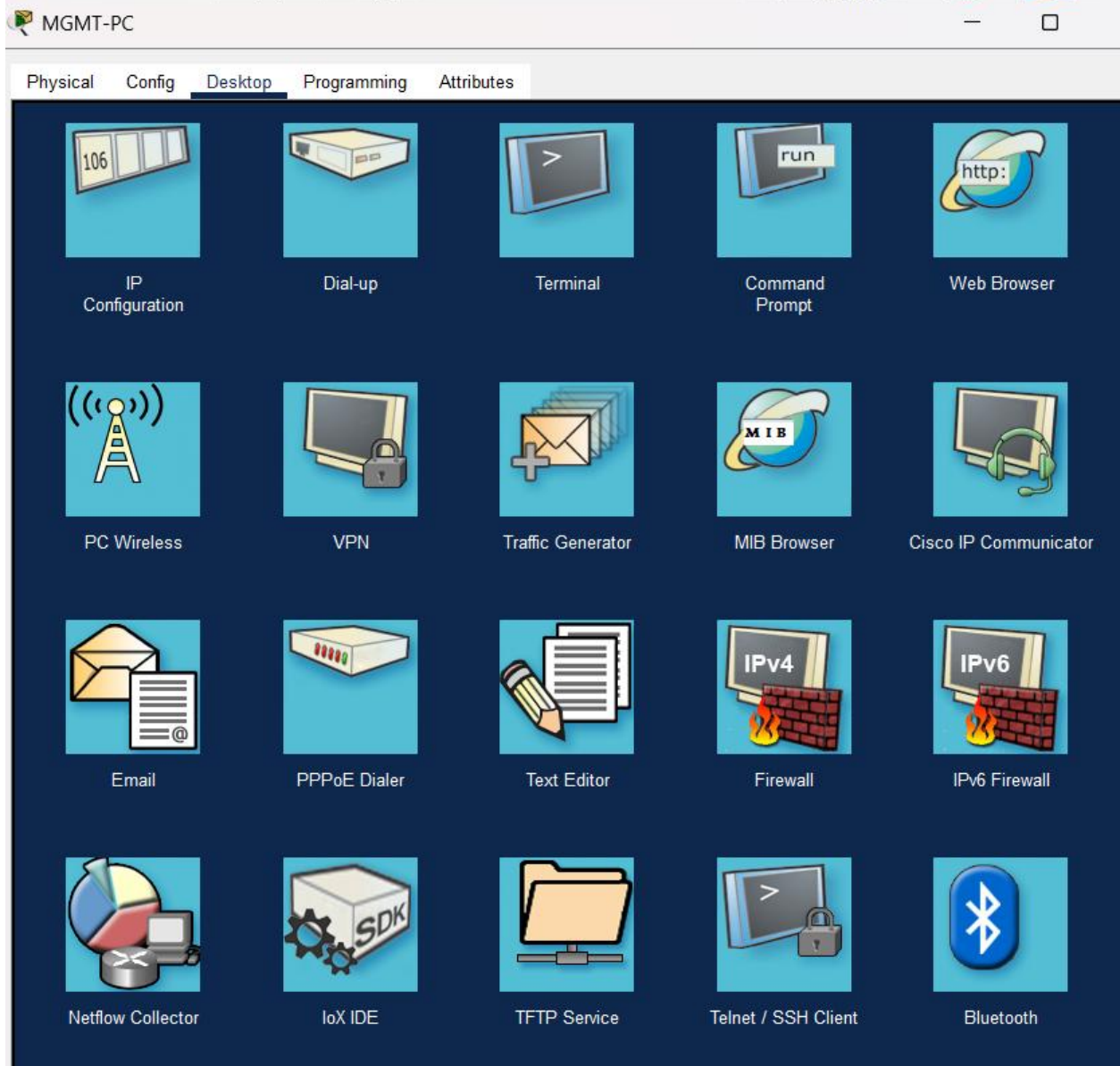


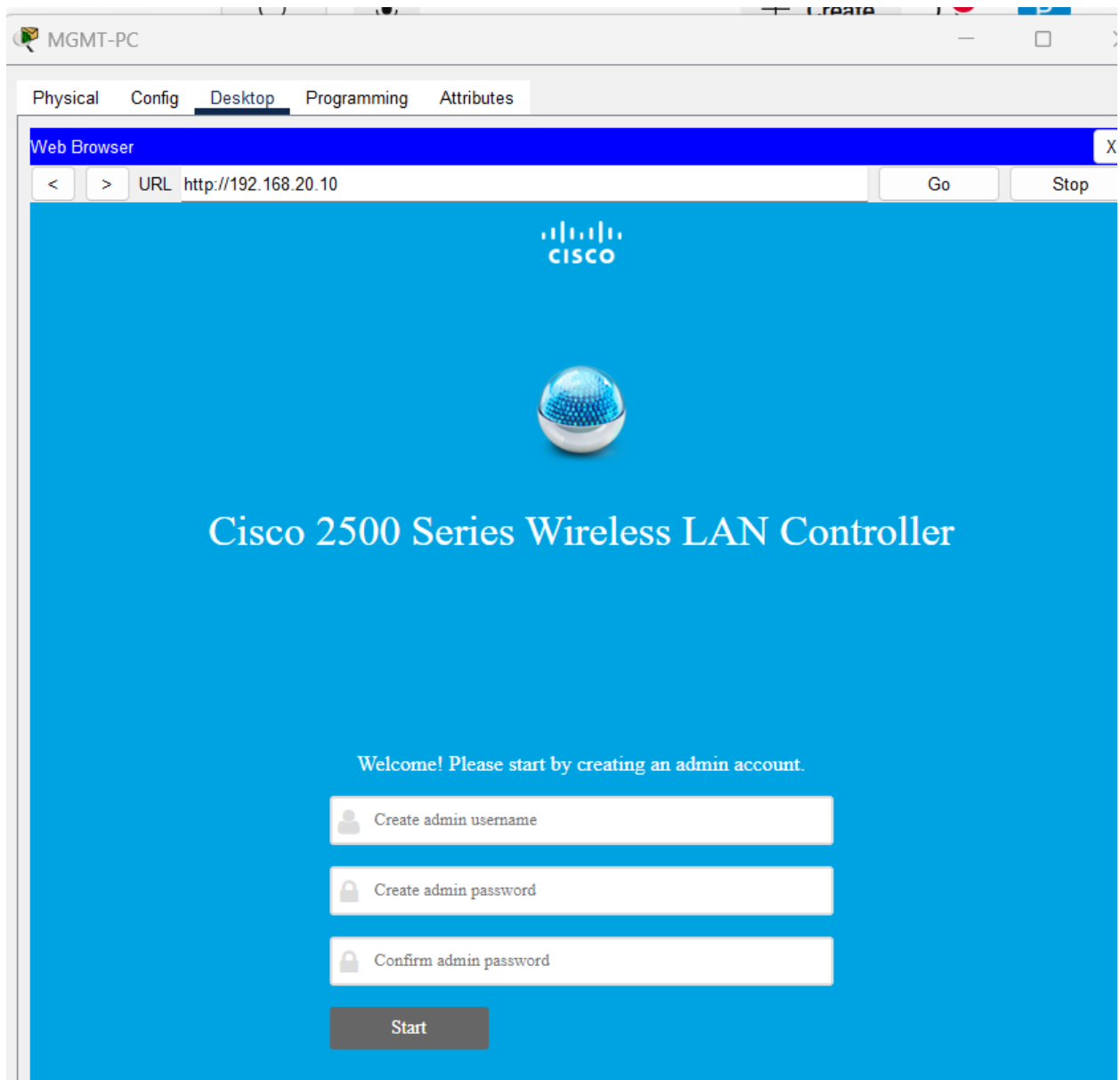
Now we can manage them remotely



Go to Management PC







Username : GTech


Password : GTech123

MGMT-PC

PhysicalConfigDesktopProgrammingAttributes

Web Browser

<>URLhttp://192.168.20.10GoStop

Cisco 2500 Series Wireless LAN Controller

1 Set Up Your Controller

▼

System Name

GTECHWLC?

Country

United States (US)?

Date & Time

07/11/202520:26:06

Timezone

Eastern Time (US and Canada)?

NTP Server

(optional)?

Management IP Address

192.168.20.10?

Subnet Mask

255.255.255.0

Default Gateway

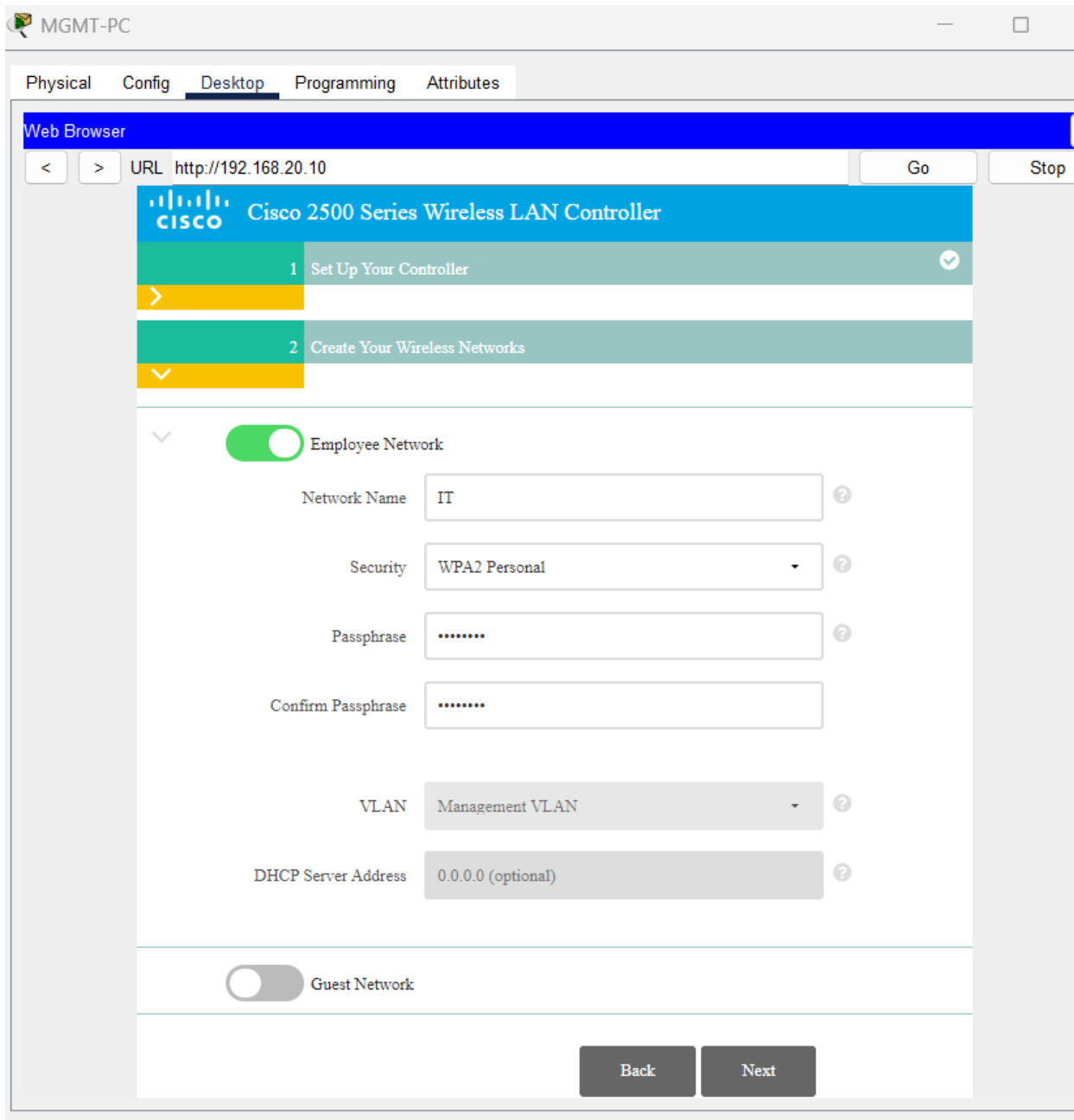
192.168.20.1

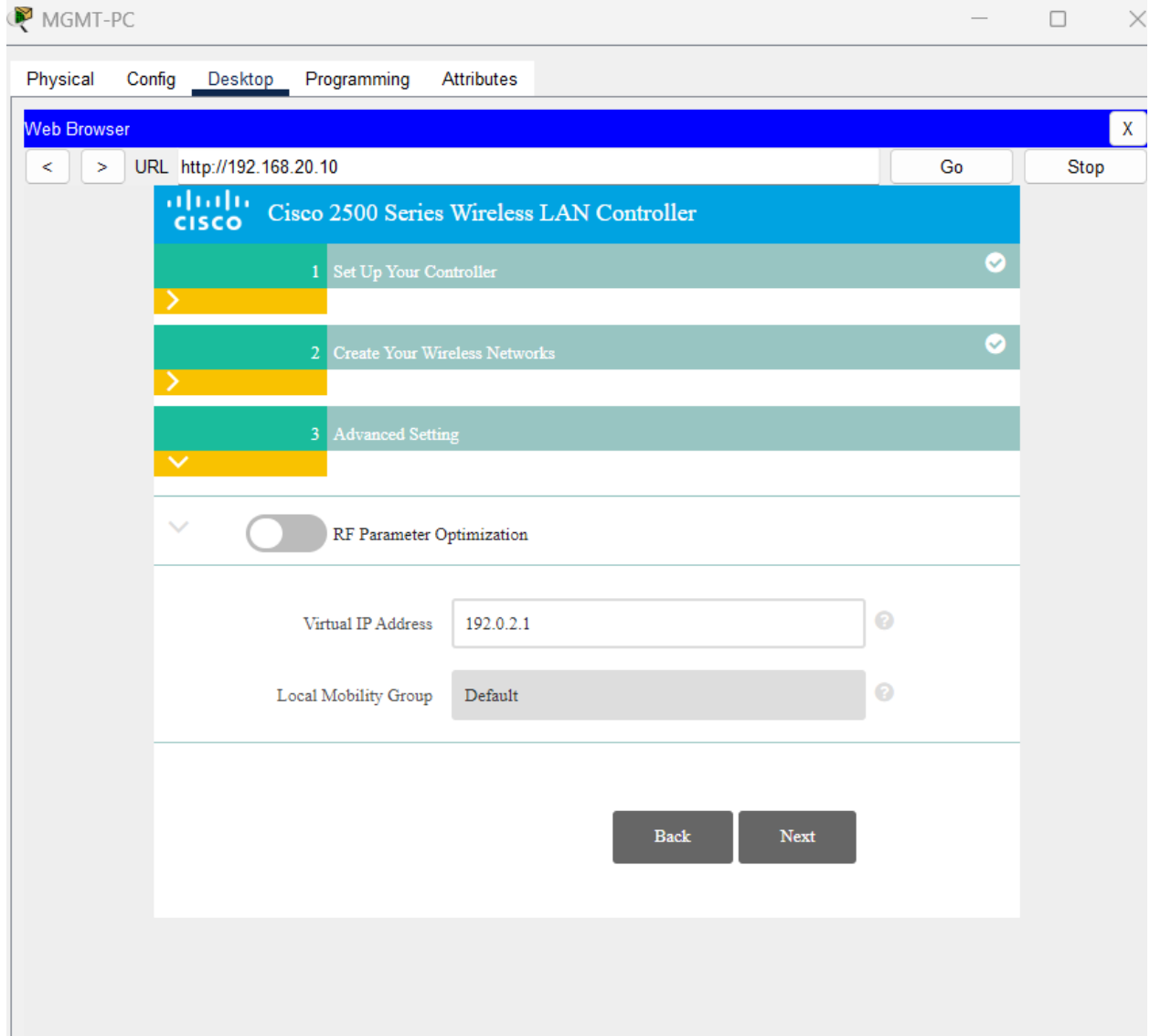
Management VLAN ID

0?

Back

Next





MGMT-PC

Physical

Config

Desktop

Programming

Attributes

Web Browser

< > | URL: http://192.168.20.10

Go

Cisco

Cisco 2500 Series Wireless LAN Controller

Please confirm settings and apply

1

Controller Settings

Username

GTech

System Name

GTECHWLC

Country

United States (US)

Date & Time

07/11/2025 20:28:42

Timezone

Eastern Time (US and Canada)

NTP Server

-

Management IP Address

192.168.20.10

Management IP Subnet

255.255.255.0

Management IP Gateway

192.168.20.1

Management VLAN ID

0

2

Wireless Network Settings

✓

Employee Network

Network Name

IT

Security

WPA2 Personal

Passphrase

\*\*\*\*\*

Employee VLAN

Management VLAN

DHCP Server Address

-

✗

Guest Network

3

Advanced Settings

✗

RF Parameter Optimization

Virtual IP Address


192.0.2.1

Local Mobility Group

Default

Web Browser

< > URL http://192.168.20.10 Go St

 Cisco 2500 Series Wireless LAN Controller

Please confirm settings and apply

1 Controller Settings

Username

GTech

System Name

GTECHWLC

Country

United States (US)

Date & Time

07/11/2025 20:29:01

Timezone

Eastern Time (US and Canada)

NTP Server

-

Management IP Address

192.168.20.10

Management IP Subnet

255.255.255.0

Management IP Gateway

192.168.20.1

Management VLAN ID

0

2 Wireless Network Settings

✓ Employee Network

Network Name

IT

Security

WPA2 Personal

Passphrase:

\*\*\*\*\*

Employee VLAN

Management VLAN

DHCP Server Address

-

✗ Guest Network

MGMT-PC

PhysicalConfigDesktopProgrammingAttributes

Web Browser

<>URLhttp://192.168.20.10GoStop

TimezoneEastern Time (US and Canada)

NTP Server-

Management IP Address192.168.20.10

Management IP Subnet255.255.255.0

Management IP Gateway192.168.20.1

Management VLAN ID0

2Wireless Network Settings

✓Employee Network

Network NameIT

SecurityWPA2 Personal

Passphrase:\*\*\*\*\*

Employee VLANManagement VLAN

DHCP Server Address-

✗Guest Network

3Advanced Settings

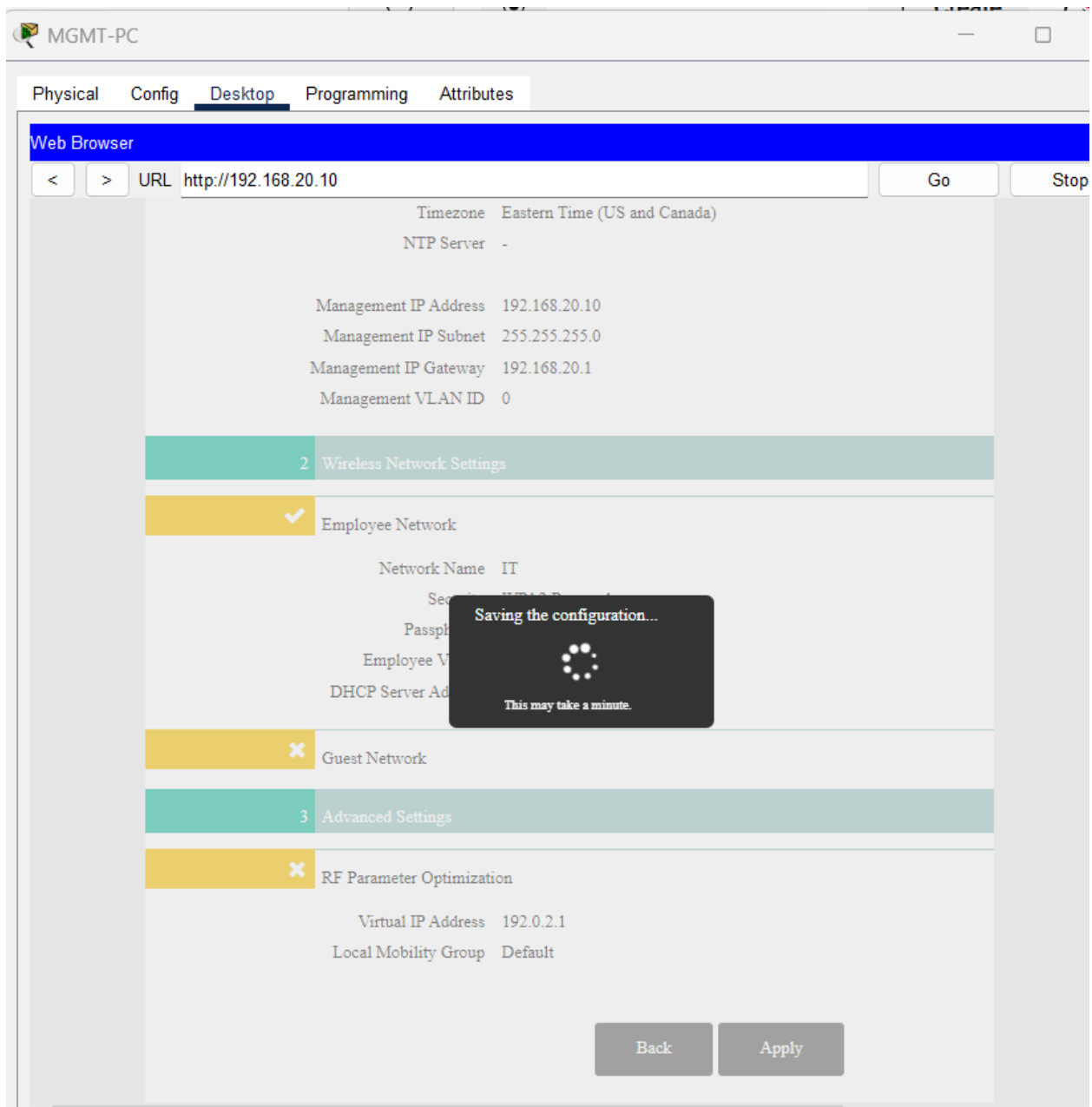
✗RF Parameter Optimization

Virtual IP Address192.0.2.1

Local Mobility GroupDefault

BackApply





Close the Web Browser and come to command prompt and ping again

By going back again to browser we again get this error

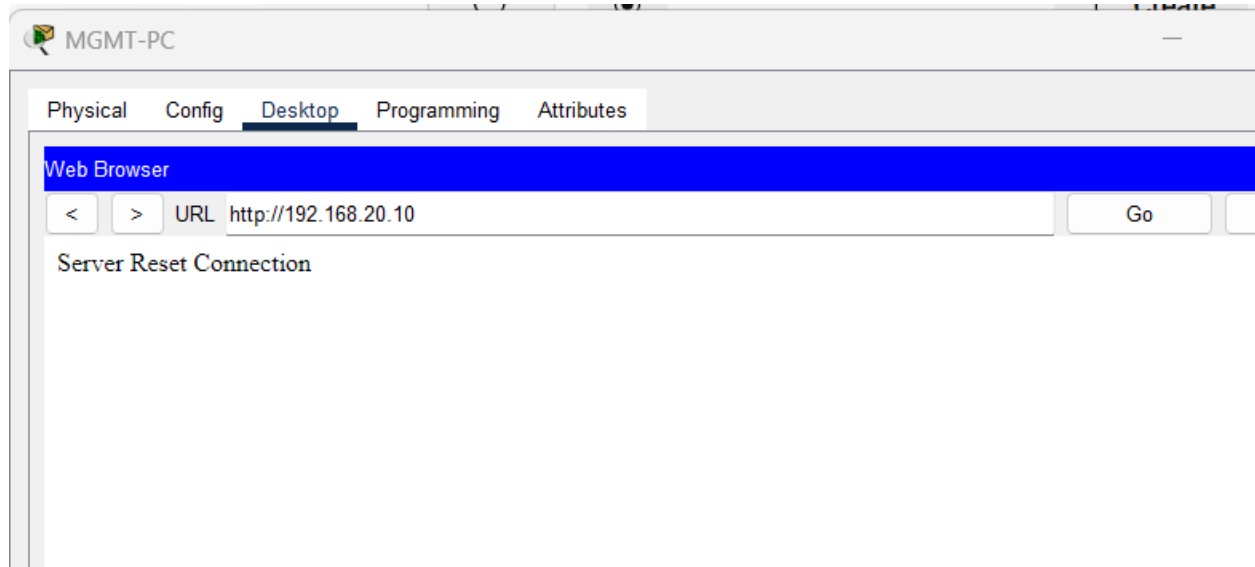
```
C:\>ping 192.16820.10
Ping request could not find host 192.16820.10. Please check the name and try again.
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.10: bytes=32 time<1ms TTL=255
Reply from 192.168.20.10: bytes=32 time<1ms TTL=255
Reply from 192.168.20.10: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



Change it to https



MGMT-PC

Physical

Config

Desktop

Programming

Attributes

Web Browser

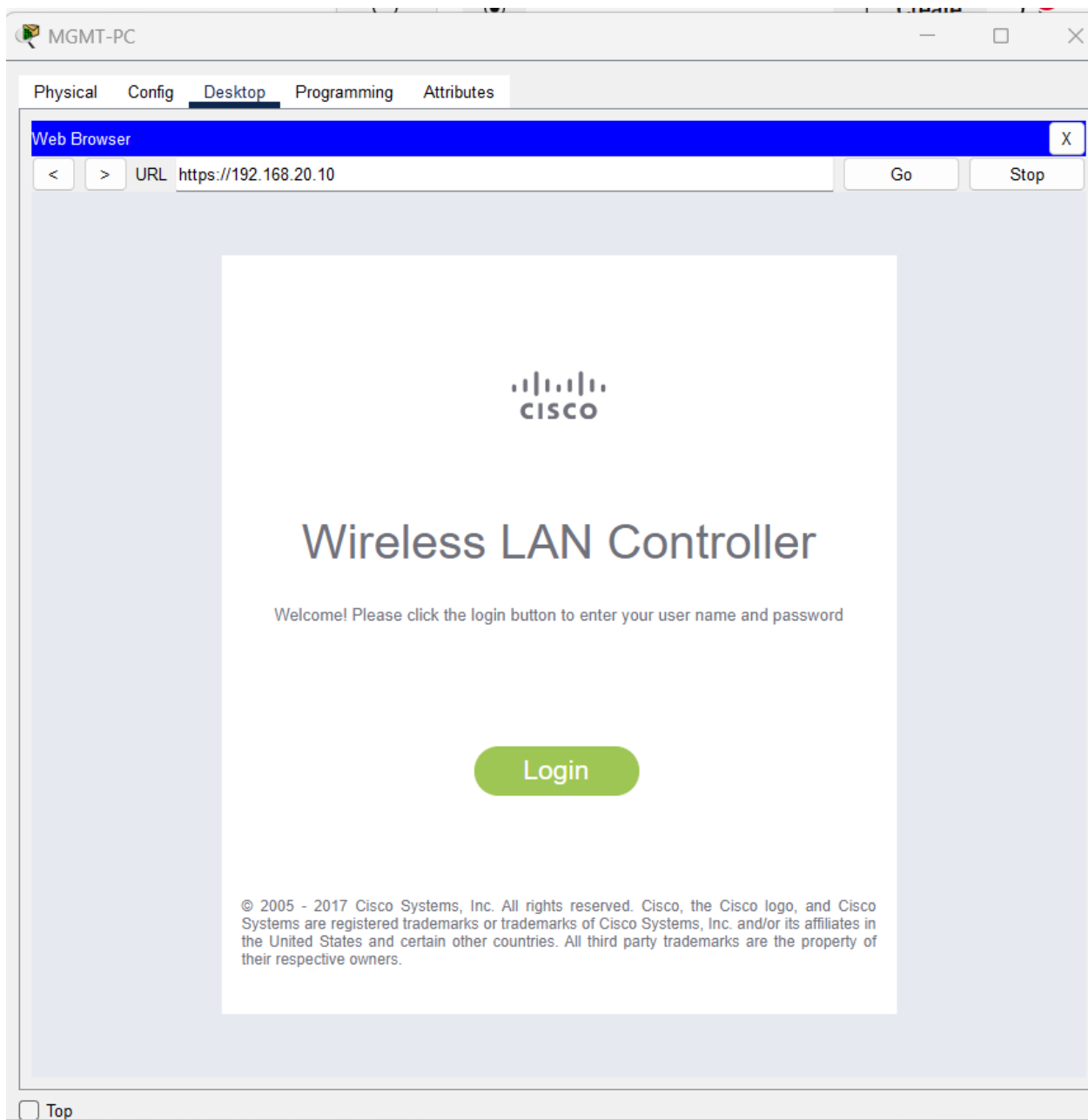
<

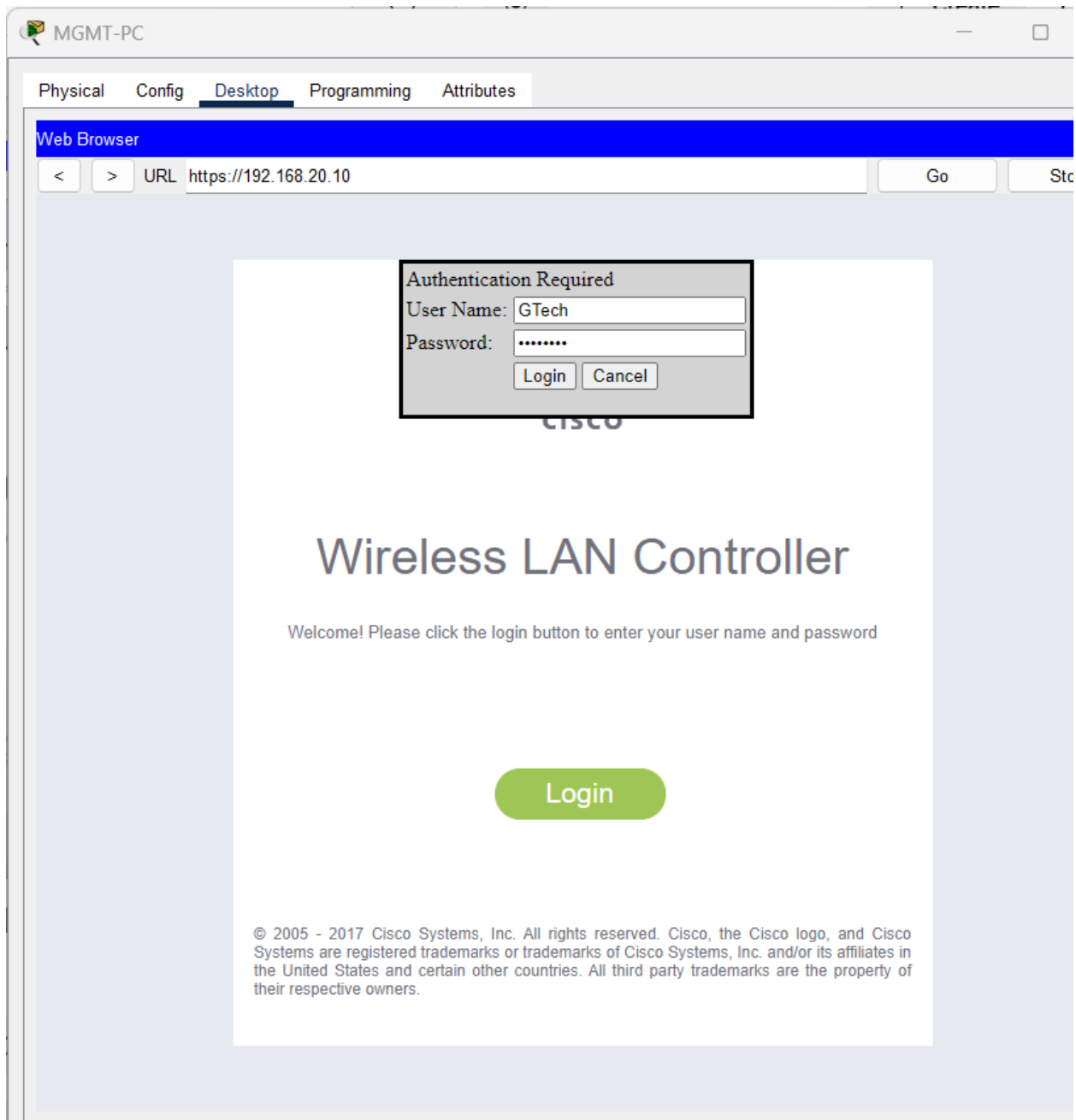
>

URL <http://192.168.20.10>

Go

Server Reset Connection





Physical port of Wireless LAN Controller

**Monitor** | Summary

25 Access Points Supported

**Controller Summary**

Management IP Address	192.168.20.10 , ::1/128
Software Version	8.3.111.0
Field Recovery Image Version	7.6.101.1
System Name	QTECHWLC
Up Time	12 minutes, 23 seconds
System Time	Fri Jul 11 20:42:49 2025
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	4	4	0	<a href="#">Detail</a>
802.11b/g/n Radios	4	4	0	<a href="#">Detail</a>
Dual-Band Radios	0	0	0	<a href="#">Detail</a>
All APs	4	4	0	<a href="#">Detail</a>

**Client Summary**

**Rogue Summary**

Active Rogue APs	0	<a href="#">Detail</a>
Active Rogue Clients	0	<a href="#">Detail</a>
Adhoc Rogues	0	<a href="#">Detail</a>
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](#)

Lets check the status of Wireless LAN Access Point

We are able to see the number of Acces Points in the network

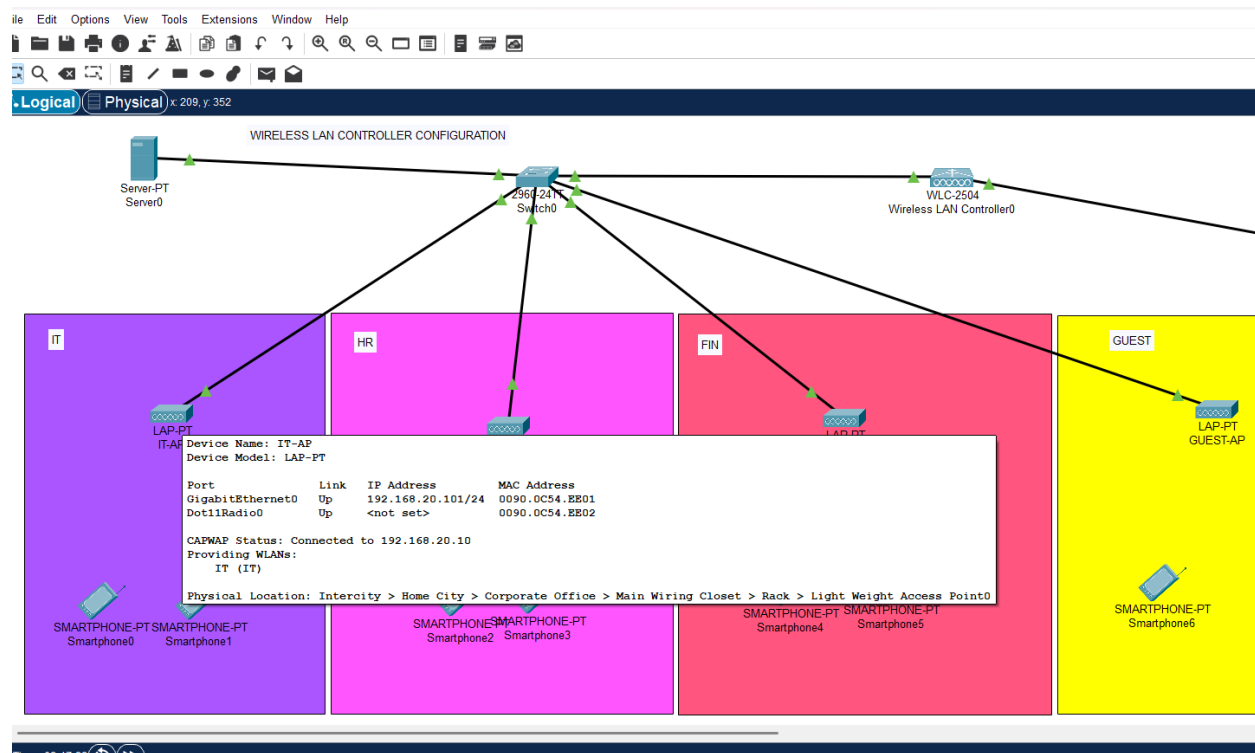
**Wireless** | All APs

Current Filter: [\[Choose Filter\]](#) [\[Clear Filter\]](#)

Number of APs: 4

AP Name	IP Address (IPv4/IPv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	PoE Status	Sp
<a href="#">GUEST-AP</a>	192.168.20.104	PT-AIR-CAP10001-A-K9	00:30:A3:2E:49:01	0 d, 2 h 24 m 1 s	Enabled	REG	-	10
<a href="#">HS-AP</a>	192.168.20.102	PT-AIR-CAP10001-A-K9	00:40:0B:8A:6B:01	0 d, 2 h 24 m 25 s	Enabled	REG	-	10
<a href="#">FIN-AP</a>	192.168.20.103	PT-AIR-CAP10001-A-K9	00:E0:P9:0E:81:01	0 d, 2 h 24 m 9 s	Enabled	REG	-	10
<a href="#">IT-AP</a>	192.168.20.101	PT-AIR-CAP10001-A-K9	00:90:0C:54:EE:01	0 d, 2 h 24 m 40 s	Enabled	REG	-	10

Entries 1 - 4 of 4



We are able to see the CAPWAP status. The CAPWAP status maintains the relationship between the access point and the wireless lan controller.

Now we need to come to WLAN and create Wi-Fi names

MGMT-PC

Physical Config Desktop Programming Attributes

Web Browser X

< > URL https://192.168.20.10/frameWlanCreate.html Go Stop

Save Configuration Ping Logout Refresh

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANS

WLANS > New

< BACK Apply

▼ WLANS  
WLANS

▼ Advanced  
AP Groups

Type WLAN ▼

Profile Name HR

SSID HR

ID 2 ▼

MGMT-PC

Physical Config Desktop Programming Attributes

Web Browser X

< > URL https://192.168.20.10/frameWlanEdit.html Go Stop

Save Configuration Ping Logout Refresh

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANS

WLANS > Edit 'HR'

< BACK Apply

▼ WLANS  
WLANS

▼ Advanced  
AP Groups

General Security QoS Policy-Mapping Advanced

Profile Name HR

Type WLAN

SSID HR

Status ☐ Enabled

Security Policies None  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy AS

Interface/Interface Group(G) management ▼

Multicast VLAN Feature ☐ Enabled

Broadcast SSID ☒ Enabled

WMM-ID

Foot Notes

1 Web Policy cannot be used in combination with IPsec  
2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs  
2(b) When Flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS  
2(c) When Flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode  
3 When client exclusion is enabled, a Timeout (value of zero means infinity (will require administrative override to reset excluded clients))  
4 Client MFP is not active unless WPA2 is configured  
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled  
6 WMM and open or AES security should be enabled to support higher 11n rates  
8 Value zero implies there is no restriction on maximum clients allowed.  
9 MAC Filtering is not supported with FlexConnect Local authentication  
10 MAC Filtering should be enabled.  
11 Guest Tunneling, Local switching, DHCP Required should be disabled.  
12 Max-associated-clients feature and Central Assoc feature are not supported with FlexConnect Local Authentication.  
13 VLAN based central switching is not supported with FlexConnect Local Authentication.  
14 Enabling gls-randomize will prevent clients from decrypting broadcast and multicast packets.  
15 Fast Transition is supported with WPA2 and open security policy  
16 Override Bandwidth Contracts parameters are specific to per Radio of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.  
18 When Diagnostic Channel is enabled, P2P Blocking Action will be assigned to Drop Action



MGMT-PC

Physical

Config

Desktop

Programming

Attributes

Web Browser

<

>

URL

https://192.168.20.10/frameWlanEdit.html

Go

Stop

CISCO

MONITOR

WLANs

CONTROLLER

WIRELESS

SECURITY

MANAGEMENT

COMMANDS

HELP

FEEDBACK

Save Configuration

Ping

Logout

Refresh

WLANs

▼ WLANs

WLANs

▼ Advanced

AP Groups

WLANs > Edit 'HR'

< BACK

Apply

General

Security

QoS

Policy-Mapping

Advanced

Profile Name

HR

Type

WLAN

SSID

HR

Status

☒ Enabled

Security Policies

None

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

Radio Policy

All

Interface/Interface Group(G)

management

Multicast Vlan Feature

☐ Enabled

Broadcast SSID

☒ Enabled

NAS-ID

Foot Notes

1 Web Policy cannot be used in combination with IPsec

2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs

2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS

2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode

MGMT-PC

Physical Config Desktop Programming Attributes

Web Browser

URL: https://192.168.20.10/frameWlanEdit.html

Go Stop

Save Configuration Logout Refresh Home

WLANs

WLANs > Edit 'HR'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security WPA+WPA2

HAC Filtering

Protected Management Frame

WPA+WPA2 Parameters

WPA Policy WPA Encryption WPA2 Policy

Authentication Key Management

802.1X CCMP PSK Format

WPA gtk-randomize Status

Foot Notes

1 Web Policy cannot be used in combination with Flex  
2(1) FlexConnect Local Switching is not supported with IPsec, CRANTTE authentication, Override Interface ACLs  
2(2) When Flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS  
2(3) When Flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode  
3 When client exclusion is enabled, a Timeout value of zero means infinity (will require administrative override to reset excluded clients)  
4 Client WPA is not active unless WPA2 is configured  
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled  
6 WPM and open or AES security should be enabled to support higher 11n rates  
8 Value zero implies there is no restriction on maximum clients allowed.  
9 MAC Filtering is not supported with FlexConnect Local authentication  
10 MAC Filtering should be enabled.  
11 Guest tunneling, Local switching, DHCP Required should be disabled.  
12 Max-associated-clients feature and Central Assoc. feature are not supported with FlexConnect Local Authentication.  
13 VLAN based central switching is not supported with FlexConnect Local Authentication.  
14 Enabling gtk-randomize will prevent clients from decrypting broadcast and multicast packets.  
15 Fast Transition is supported with WPA2 and open security policy  
16 Override Bandwidth Constraints parameters are specific to per Radio of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.  
18 When Diagnostic Channel is enabled, P2P Blocking Action will be assigned to Drop Action

MGMT-PC

Physical Config **Desktop** Programming Attributes

Web Browser X

< > URL <https://192.168.20.10/frameWlanEdit.html> Go Stop

Save Configuration Ping Logout Refresh

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

**WLANs**

- WLANs
- Advanced**
  - AP Groups

**WLANs > Edit 'HR'** < BACK Apply


**General** Security QoS Policy-Mapping Advanced

Profile Name

Type

SSID

JavaScript Confirm - <https://192.168.20.10/frameWlanEdit.html> X

 Changing WLAN parameters while it is enabled will cause the WLAN to be momentarily disabled and thus may result in loss of connectivity for some clients. Press OK to continue. (Applying the changes.)

OK Cancel

Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☒ Enabled

NAS-ID

**Foot Notes**

1 Web Policy cannot be used in combination with IPsec

2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs

2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS

MGMT-PC

PhysicalConfigDesktopProgrammingAttributes

Web Browser

<>URLhttps://192.168.20.10/frameWlanCreate.htmlGoStop

CISCO

MONITORWLANsCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHELPFEEDBACK

Save Configuration | Ping | Logout | Refresh

WLANs

WLANs

Advanced

AP Groups

WLANs > New

< BACKApply

Type

WLAN

Profile Name

FIN

SSID

FIN

ID

3

MGMT-PC

Physical Config Desktop Programming Attributes

Web Browser

< > URL https://192.168.20.10/frameWlanEdit.html Go Stop

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Ping Logout Refresh

WLANs

WLANs

Advanced

AP Groups

WLANs > Edit 'FIN'

< BACK Apply

General Security QoS Policy-Mapping Advanced

Profile Name FIN

Type WLAN

SSID FIN

Status ☒ Enabled

Security Policies None

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

Radio Policy All

Interface/Interface Group(G) management

Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☒ Enabled

NAS-ID

Foot Notes

1 Web Policy cannot be used in combination with IPsec

2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs

2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS

2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode

3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)

MGMT-PC

Physical Config **Desktop** Programming Attributes

Web Browser X

URL https://192.168.20.10/frameWlanEdit.html Go Stop

Save Configuration Ping Logout Refresh

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

**WLANS**

- WLANS
- Advanced
  - AP Groups

**WLANS > Edit 'FIN'** < BACK Apply

General Security **QoS** Policy-Mapping Advanced

Layer 2 Layer 3 **AAA Servers**

MAC Filtering ☐

**Protected Management Frame**

PMF Disabled

**WPA+WPA2 Parameters**

WPA Policy ☒

WPA Encryption ☒ AES ☐ TKIP

WPA2 Policy ☐

**Authentication Key Management**

802.1X ☐ Enable

CKM ☐ Enable

PSK ☒ Enable

PSK Format ASCII

WPA gtk-randomize State ☐ Disable

**Foot Notes**

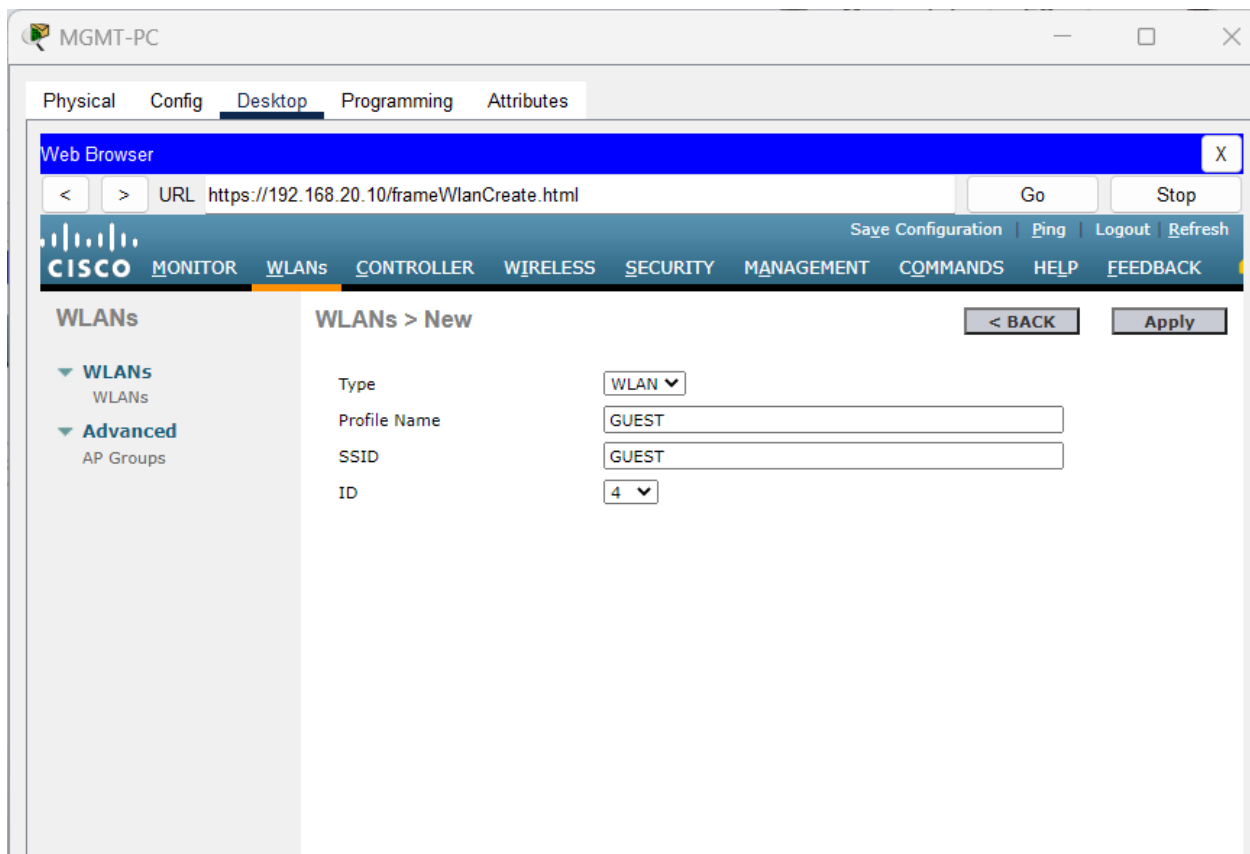
1 Web Policy cannot be used in combination with IPsec

2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs

2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS

2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode

3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)



MGMT-PC

Physical Config **Desktop** Programming Attributes

Web Browser X

< > URL https://192.168.20.10/frameWlanEdit.html Go Stop

Save Configuration Ping Logout Refresh

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

**WLANS**

- ▼ **WLANS**
  - WLANS
- ▼ **Advanced**
  - AP Groups

**WLANS > Edit 'GUEST'** < BACK Apply

**General** Security QoS Policy-Mapping Advanced

**Layer 2** Layer 3 AAA Servers

Layer 2 Security <sup>6</sup> WPA+WPA2 ▼

MAC Filtering <sup>9</sup> ☐

**Fast Transition**

Fast Transition ☐

**Protected Management Frame**

PMF Disabled ▼

**WPA+WPA2 Parameters**

WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/> AES <input type="checkbox"/> TKIP

**Authentication Key Management**

802.1X	<input type="checkbox"/> Enable
CCKM	<input type="checkbox"/> Enable
PSK	<input checked="" type="checkbox"/> Enable
FT 802.1X	<input type="checkbox"/> Enable

**Foot Notes**

<sup>1</sup> Web Policy cannot be used in combination with IPsec  
<sup>2(a)</sup> FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs  
<sup>2(b)</sup> When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS  
<sup>2(c)</sup> When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode  
<sup>3</sup> When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)



MGMT-PC

Physical Config **Desktop** Programming Attributes

Web Browser X

< > URL <https://192.168.20.10/frameWlanEdit.html> Go Stop

Save Configuration Ping Logout Refresh

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

WLANs

- WLANs
- Advanced
  - AP Groups

WLANs > Edit 'GUEST' < BACK Apply

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 **AAA Servers**

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

WPA gtk-randomize State Disable

Foot Notes

1 Web Policy cannot be used in combination with IPsec

2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs

2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS

2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode

Number of created Wi-Fi network

MGMT-PC

Physical Config **Desktop** Programming Attributes

Web Browser X

< > URL <https://192.168.20.10/frameWlan.html> Go Stop

Save Configuration | Ping | Logout | Refresh

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

**WLANs**

- ▼ **WLANs**
  - WLANs
- ▼ **Advanced**
  - AP Groups

**WLANs** Entries 1 - 4 of 4

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

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID
<input type="checkbox"/>	<a href="#">1</a>	WLAN	IT	IT
<input type="checkbox"/>	<a href="#">2</a>	WLAN	HR	HR
<input type="checkbox"/>	<a href="#">3</a>	WLAN	FIN	FIN
<input type="checkbox"/>	<a href="#">4</a>	WLAN	GUEST	GUEST

Go to Advanced and click on Default groups. All access points belong to default groups

Click on Access Points you will see

MGMT-PC

Physical Config **Desktop** Programming Attributes

Web Browser X

< > URL https://192.168.20.10/frameAPGroupEdit.html Go Stop

Save Configuration | Ping | Logout | Refresh

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

WLANs

- ▼ WLANsWLANs
- ▼ AdvancedAP Groups

Ap Groups > Edit 'default-group' < Back

General **WLANs** APs 802.11u Location Ports/Module

WLAN ID	WLAN SSID <sup>(2)(6)</sup>	Interface/Interface Group(G)
1	IT	management
2	HR	management
3	FIN	management
4	GUEST	management

Click on WLANs you will see her

MGMT-PC

PhysicalConfigDesktopProgrammingAttributes

Web Browser

<>URLhttps://192.168.20.10/frameAPGroupEdit.htmlGoStop

Save ConfigurationPingLogoutRefresh

CISCO

MONITORWLANsCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHelpFEEDBACK

WLANs

WLANsWLANsAdvancedAP Groups

Ap Groups > Edit 'default-group'

< Back

GeneralWLANsAPs802.11uLocationPorts/Module

APs currently in the Group

<input type="checkbox"/> AP Name	Ethernet MAC
<input type="checkbox"/> GUEST-AP	0030.A32E.4901
<input type="checkbox"/> HR-AP	0040.0BBA.6B01
<input type="checkbox"/> FIN-AP	00E0.F90E.8101
<input type="checkbox"/> IT-AP	0090.0C54.EE01

Add APs to the Group

☐ AP Name

MGMT-PC

Physical

Config

Desktop

Programming

Attributes

Web Browser

<

>

URL

https://192.168.20.10/frameAPGroupList.html

Go

Stop

CISCO

MONITOR

WLANs

CONTROLLER

WIRELESS

SECURITY

MANAGEMENT

COMMANDS

HELP

FEEDBACK

WLANs

▼

WLANs

WLANs

▼

Advanced

AP Groups

AP Groups

Entries 1 - 1 of 1

Add Group

Add New AP Group

AP Group Name

IT

Description

IT WIFI USERS

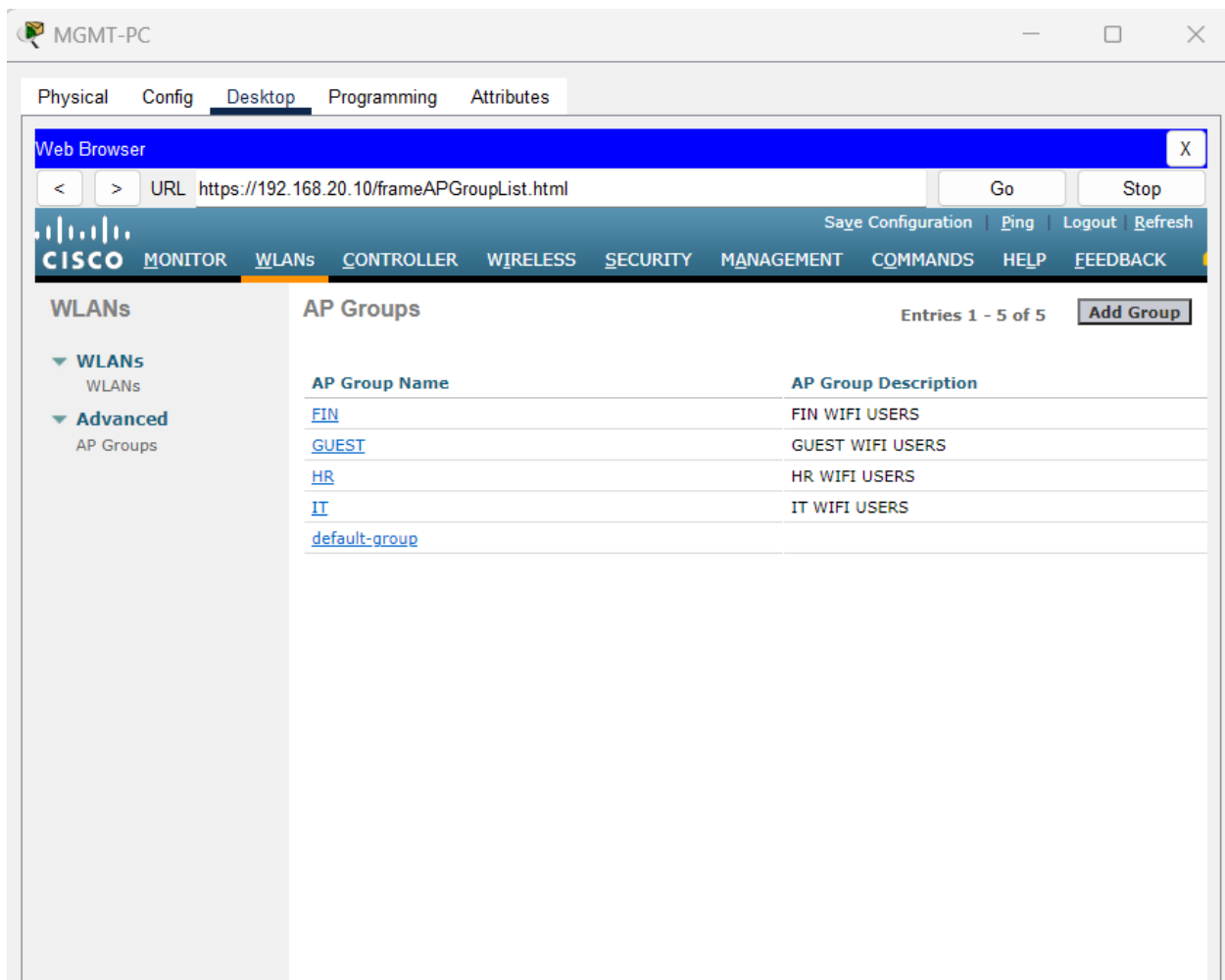
Add

Cancel

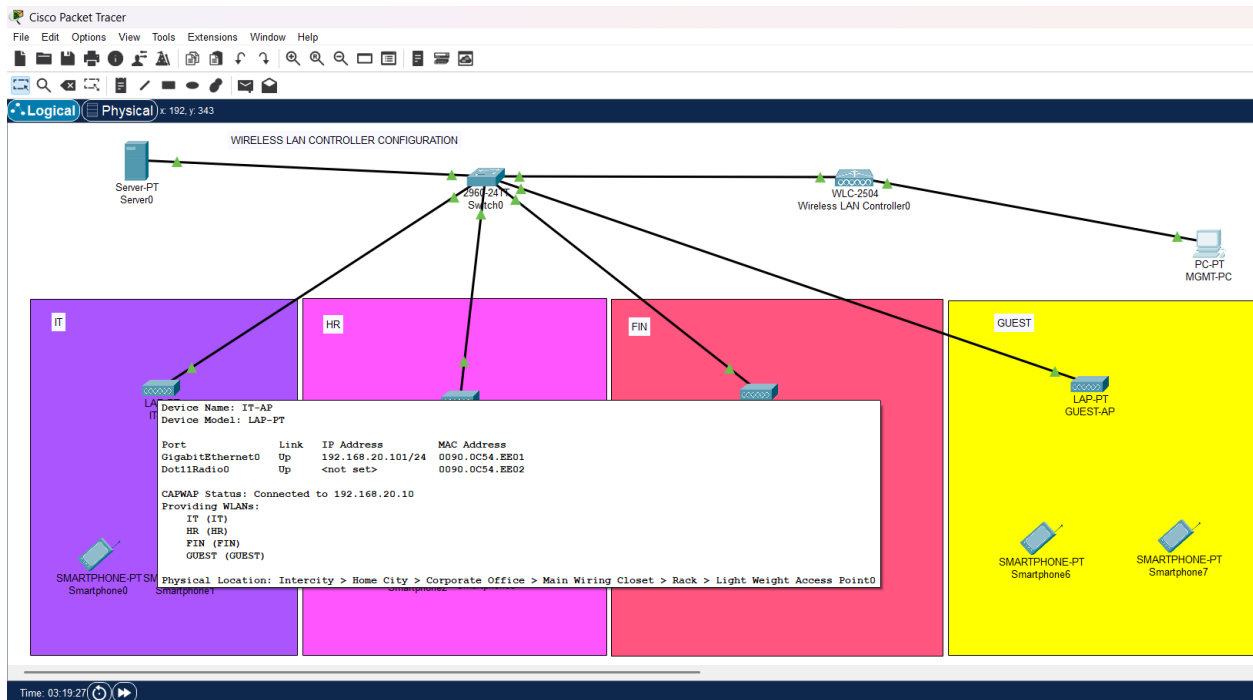
AP Group Name

AP Group Description

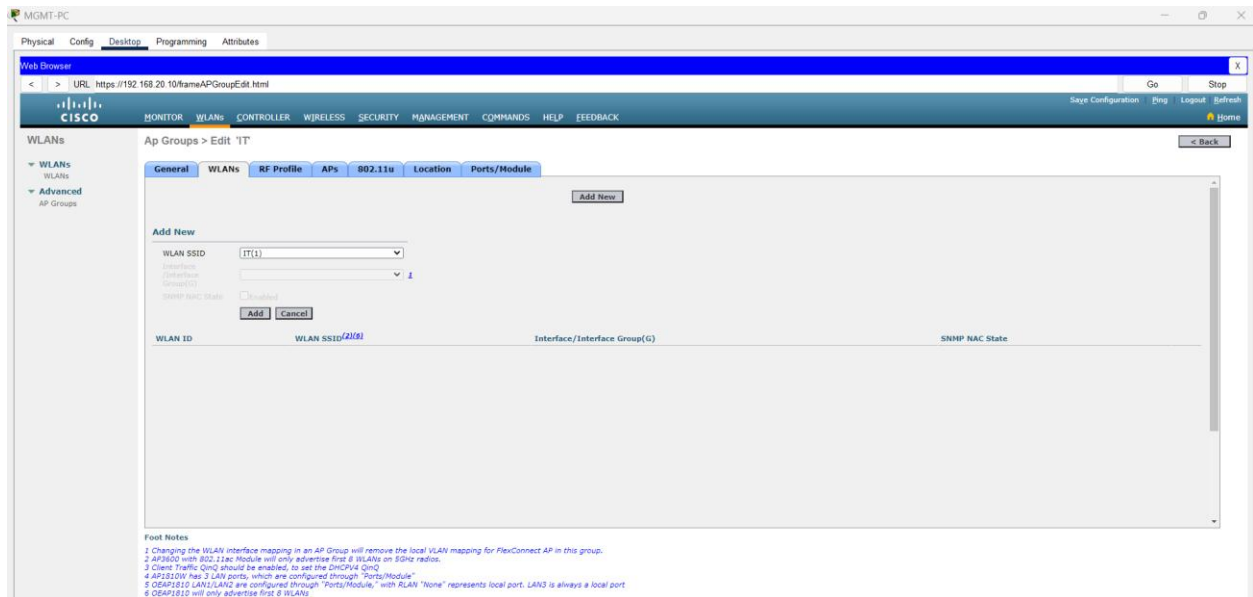
default-group



After creating each group enable specific WiFi and access point



## Now on Management PC



After clicking Add we get this

MGMT-PC

Physical Config **Desktop** Programming Attributes

Web Browser X

< > URL <https://192.168.20.10/frameAPGroupEdit.html> Go Stop

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

**WLANs**

- ▼ **WLANs**  
WLANs
- ▼ **Advanced**  
AP Groups

**Ap Groups > Edit 'IT'** < Back

**General** **WLANs** RF Profile APs 802.11u Location

**Ports/Module** Apply

AP Group Name IT

AP Group Description

NAS-ID

Enable Client Traffic QinQ ☐

Enable DHCPv4 QinQ [3](#) ☐

QinQ Service Vlan Id

CAPWAP Preferred Mode ☐ Not-Configured



MGMT-PC

PhysicalConfigDesktopProgrammingAttributes

Web BrowserX

<>URLhttps://192.168.20.10/frameAPGroupEdit.htmlGoStop

Save ConfigurationPingLogoutRefresh

CISCO

MONITORWLANsCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHELPFEEDBACK

WLANs

▼ WLANsWLANs

▼ AdvancedAP Groups

Ap Groups > Edit 'IT'

< Back

GeneralWLANsRF ProfileAPs802.11uLocation

Ports/Module

WLAN ID	WLAN SSID(2)(6)	Interface/Interface Group(G)
1	IT	management

MGMT-PC

Physical

Config

Desktop

Programming

Attributes

Web Browser

< > URL https://192.168.20.10/frameAPGroupEdit.html

CISCO

MONITOR

WLANs

CONTROLLER

WIRELESS

SECURITY

MANAGEMENT

COMMANDS

HELP

FEEDBACK

WLANs

▼ WLANs

WLANs

▼ Advanced

AP Groups

Ap Groups > Edit 'IT'

General

WLANs

RF Profile

APs

802.11u

Location

Ports/Module

APs currently in the Group

Remove APs

Add APs to the Group

Add APs

<input type="checkbox"/> AP Name	Ethernet MAC	<input type="checkbox"/> AP Name	Group Name
		<input type="checkbox"/> GUEST-AP	default-group
		<input type="checkbox"/> HR-AP	default-group
		<input type="checkbox"/> FIN-AP	default-group
		<input checked="" type="checkbox"/> IT-AP	default-group

Foot Notes

1 Changing the WLAN interface mapping in an AP Group will remove the local VLAN mapping for FlexConnect AP in this group.

2 AP3600 with 802.11ac Module will only advertise first 8 WLANs on 5GHz radios.

3 Client Traffic QmQ should be enabled, to set the DHCPV4 QmQ

4 AP1810W has 3 LAN ports, which are configured through "Ports/Module"

5 DEAP1810 LAN1/LAN2 are configured through "Ports/Module," with LAN "None" represents local port. LAN3 is always a local port

6 DEAP1810 will only advertise first 8 WLANs

7 AP2700 Aux port is configured through LAN1

MGMT-PC

Physical Config **Desktop** Programming Attributes

Web Browser X

< > URL https://192.168.20.10/frameAPGroupEdit.html Go Stop

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

Save Configuration | Ping | Logout | Refresh

**WLANS**

- ▼ **WLANS**  
WLANS
- ▼ **Advanced**  
AP Groups

**Ap Groups > Edit 'IT'** < Back

**General** **WLANS** RF Profile APs 802.11u Location

**Ports/Module** Apply

AP Group Name IT

AP Group Description IT WIFI USERS

NAS-ID none

Enable Client Traffic QinQ ☐

Enable DHCPv4 QinQ [3](#) ☐

QinQ Service Vlan Id 0

CAPWAP Preferred Mode ☐ Not-Configured