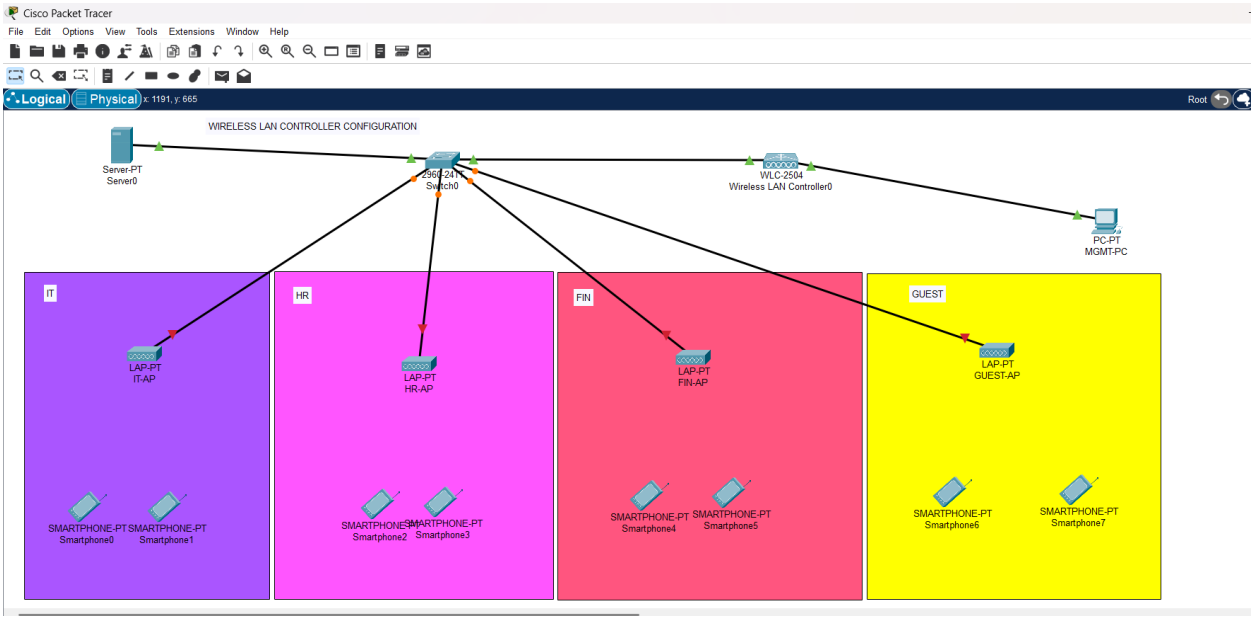
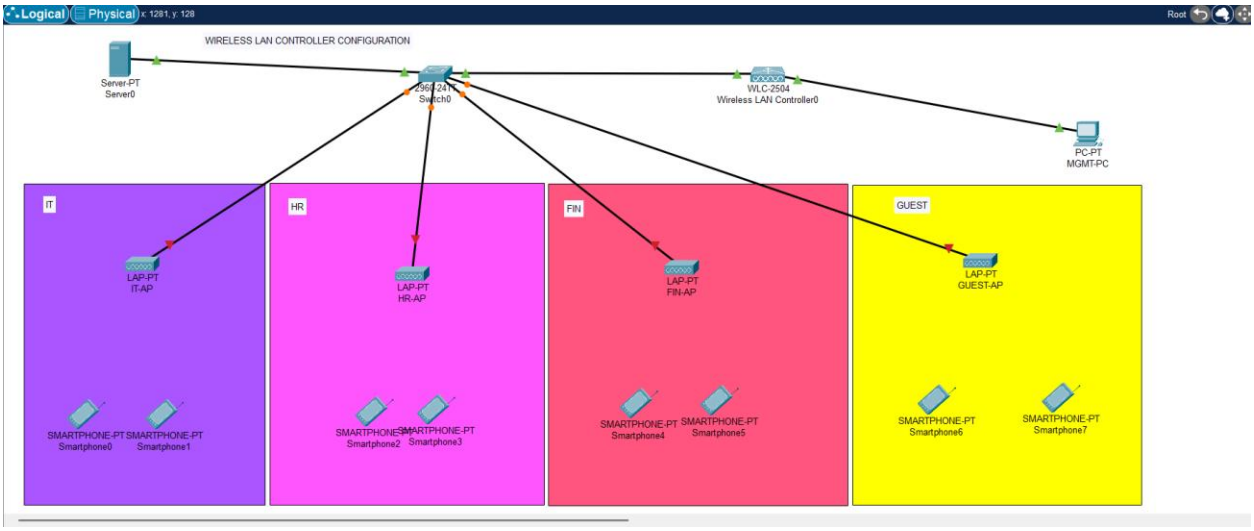
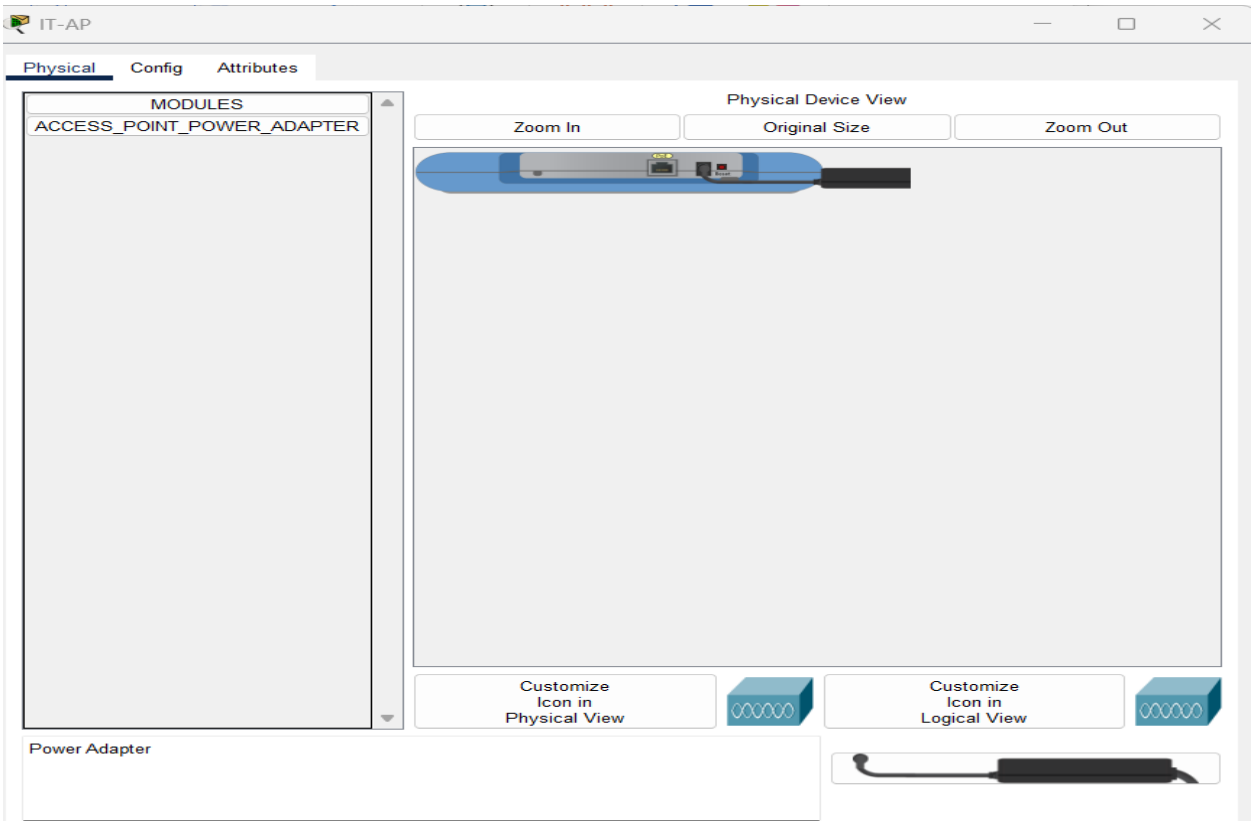
Wireless LAN Controller (WLC) Using Cisco Packet Tracer



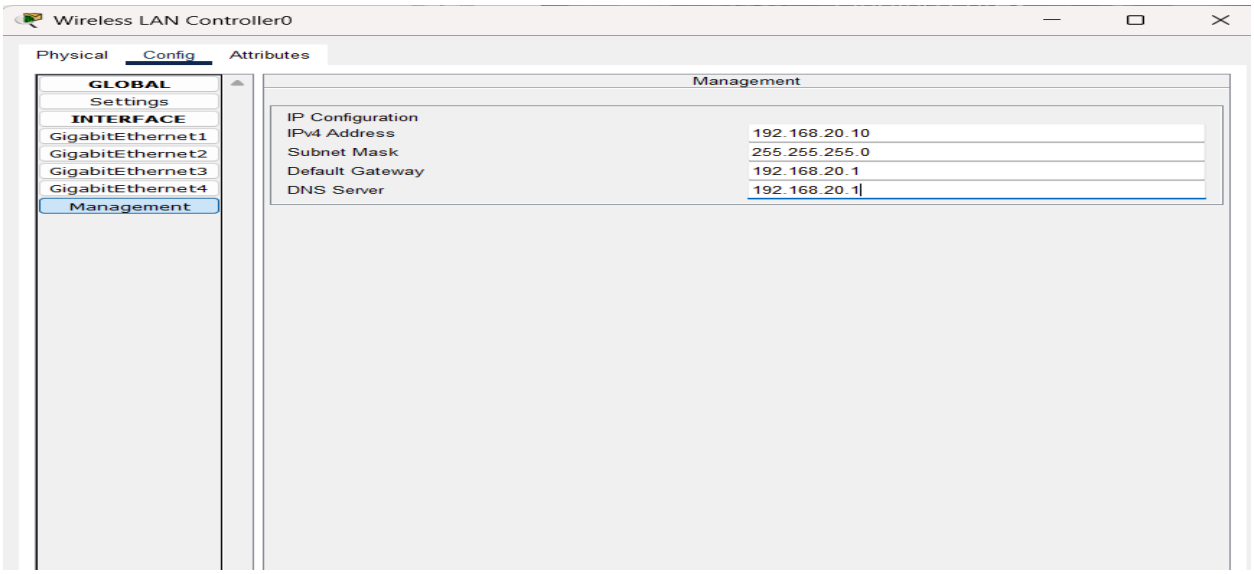


Power on the Access Point

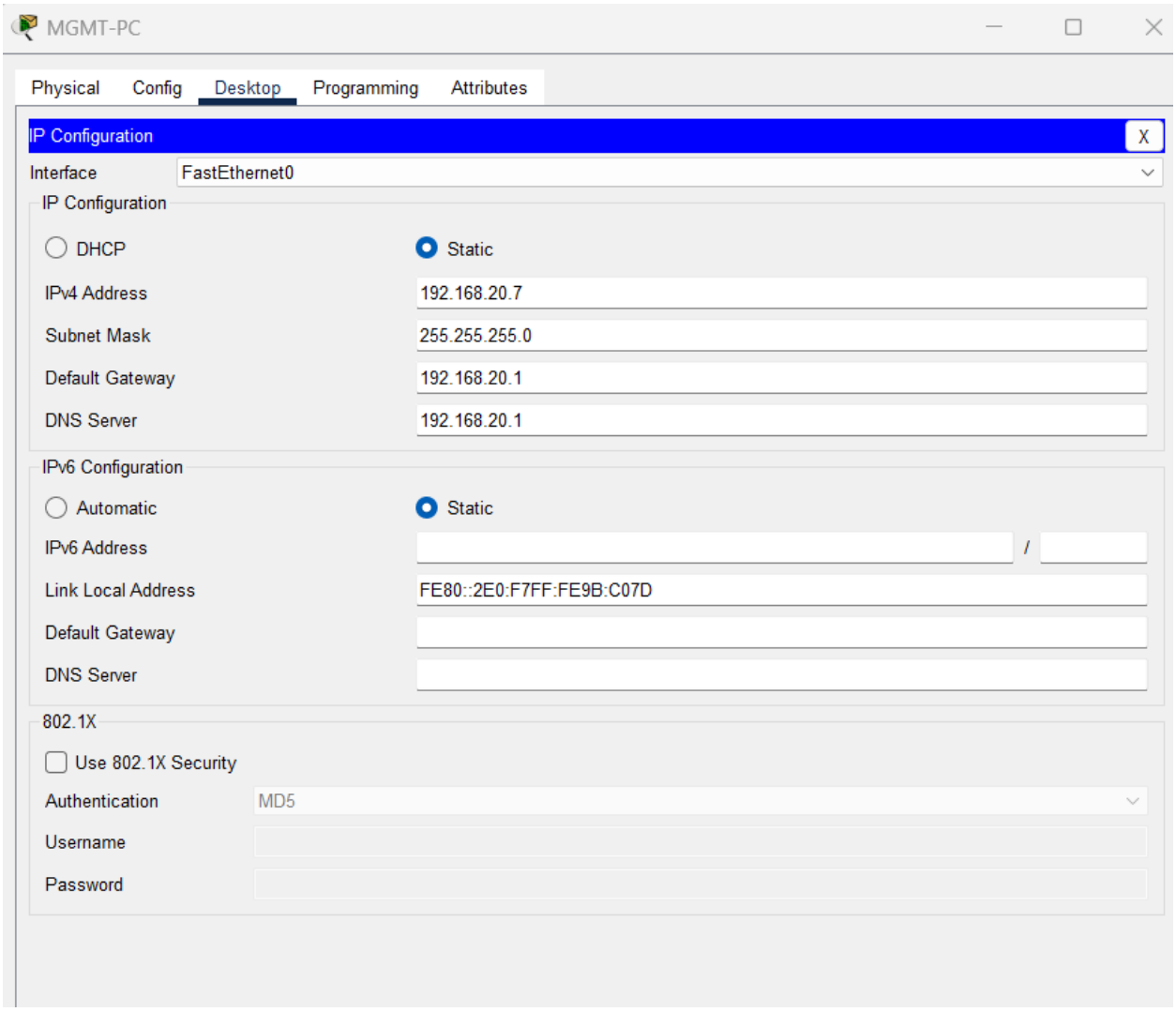


We will configure IP address to the server, Wireless LAN Controller and Management PC

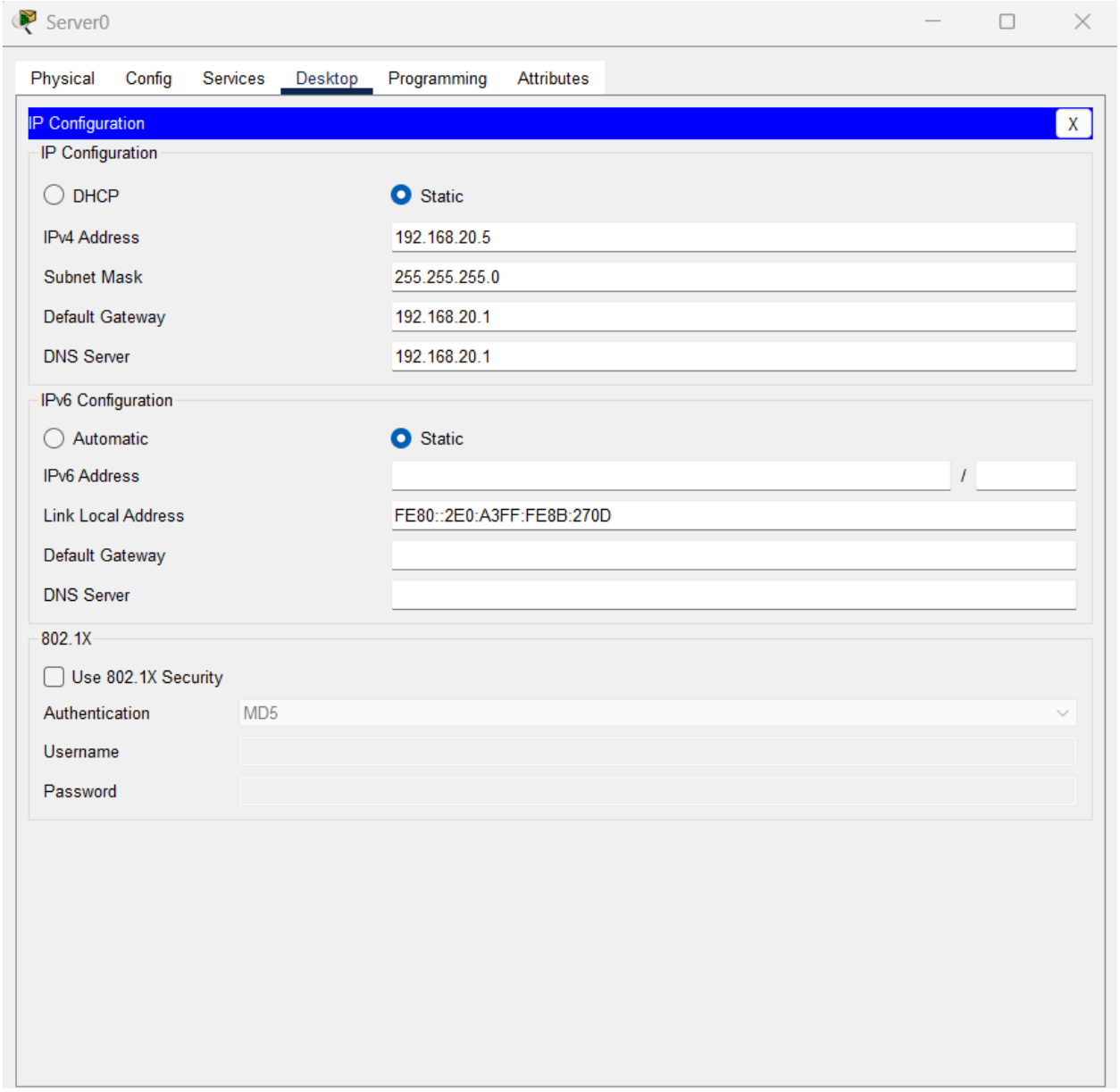
Configuration of IP Address on Wireless LAN Controller



IP Configuration for Management PC

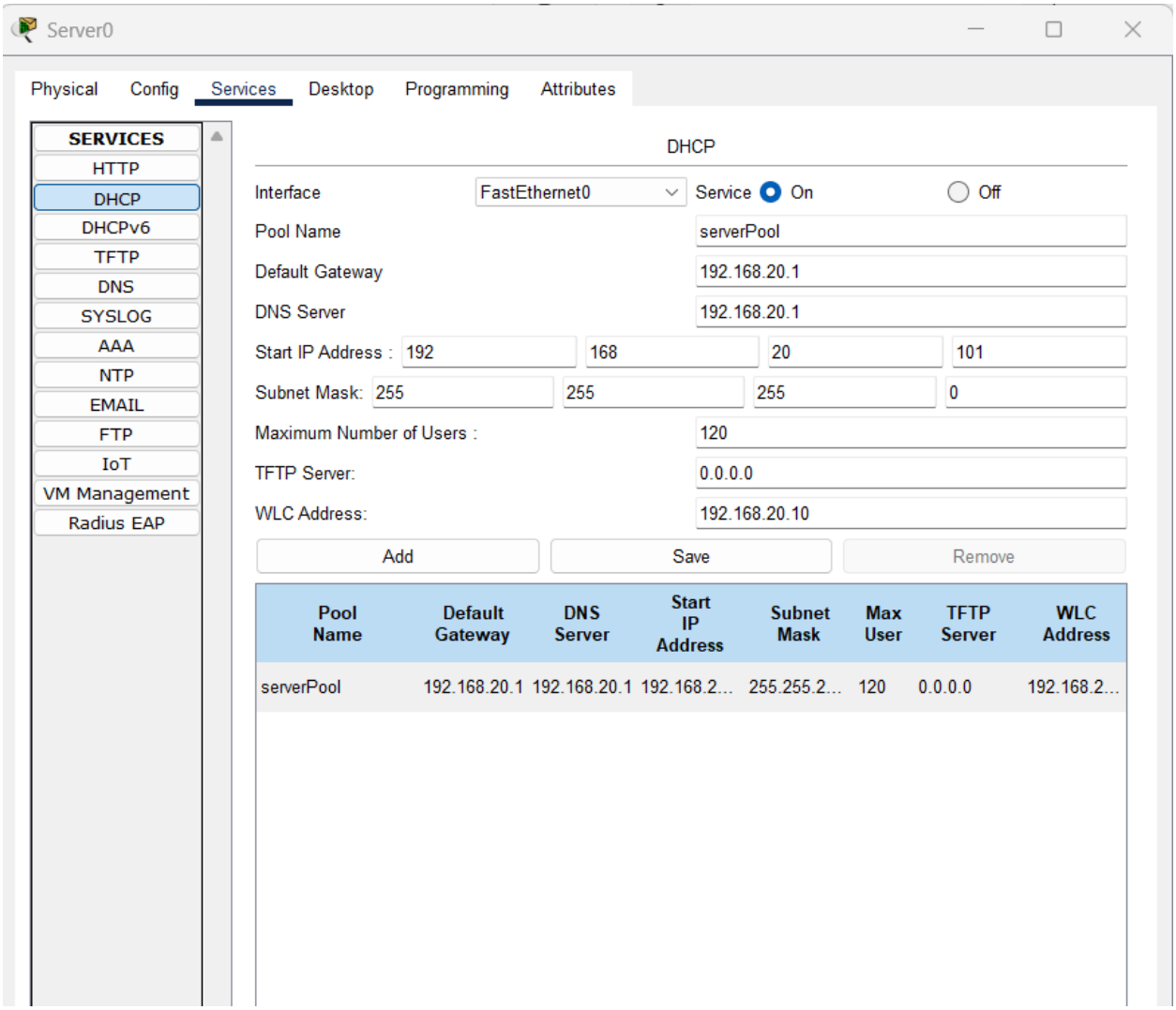


IP Configuration for Server



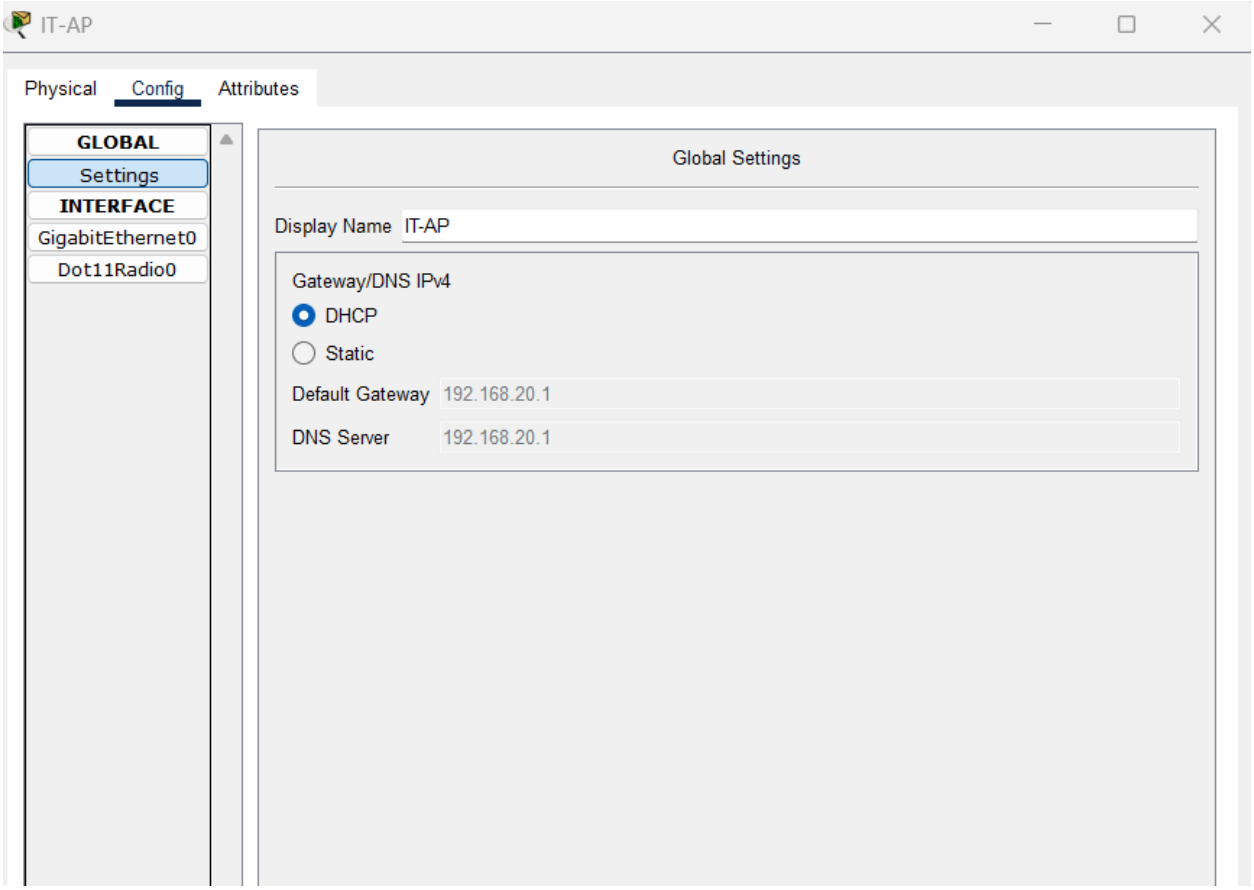
Lets create a pool. The purpose of this server is to create a pool, a pool that will be able to provide ip addressing to the Wireless Devices

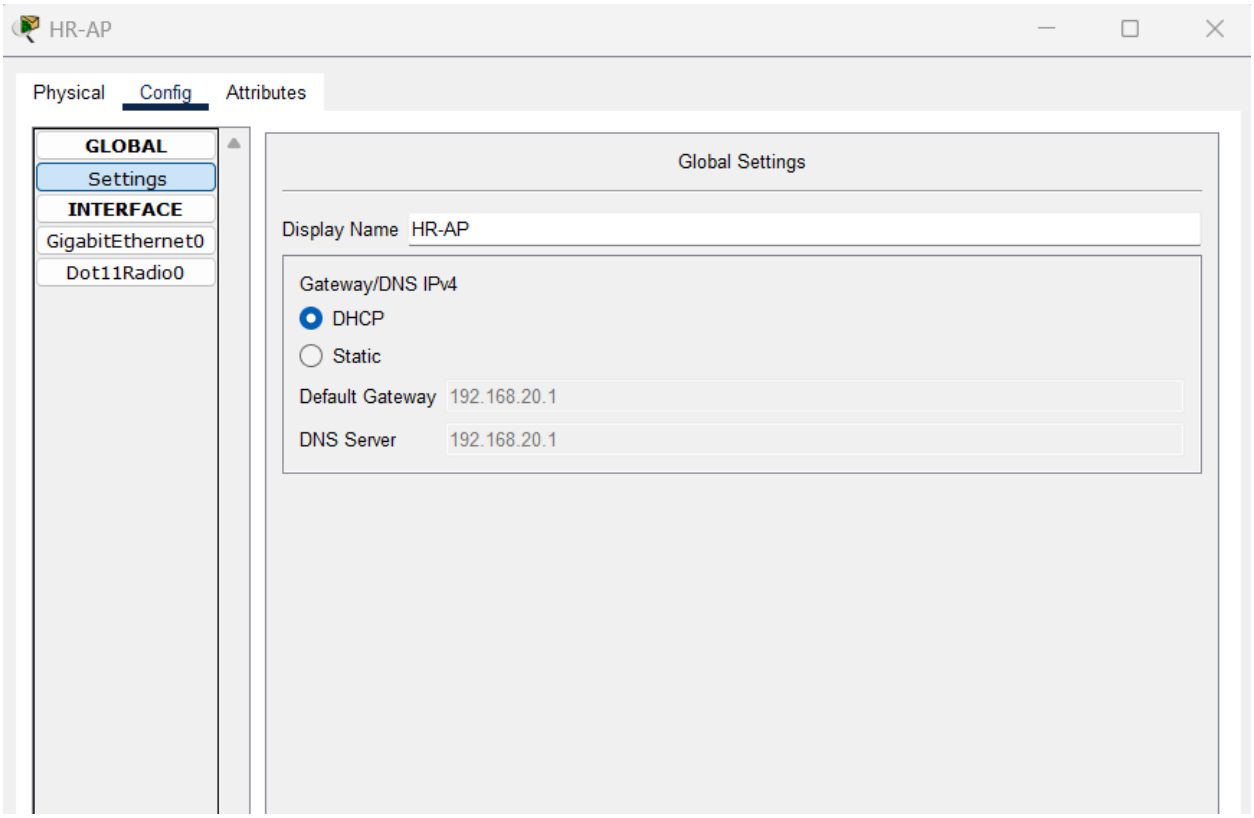
Services for the wirless LAN controller

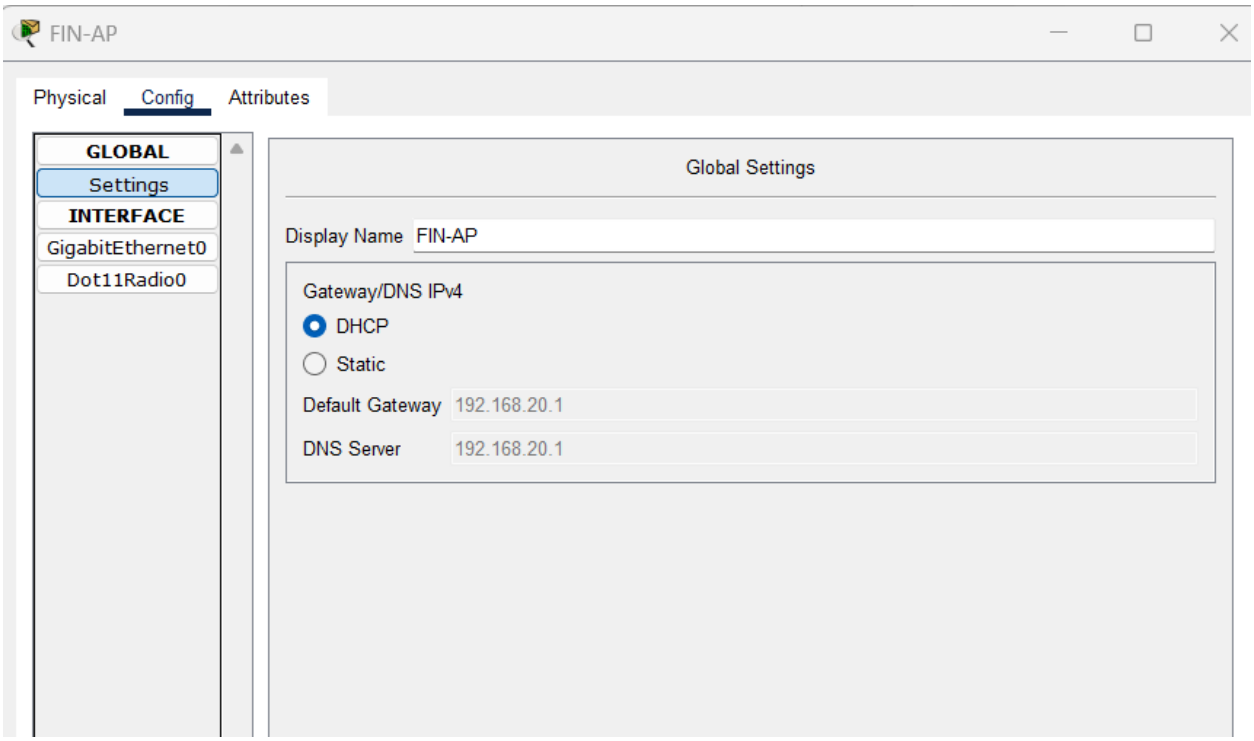


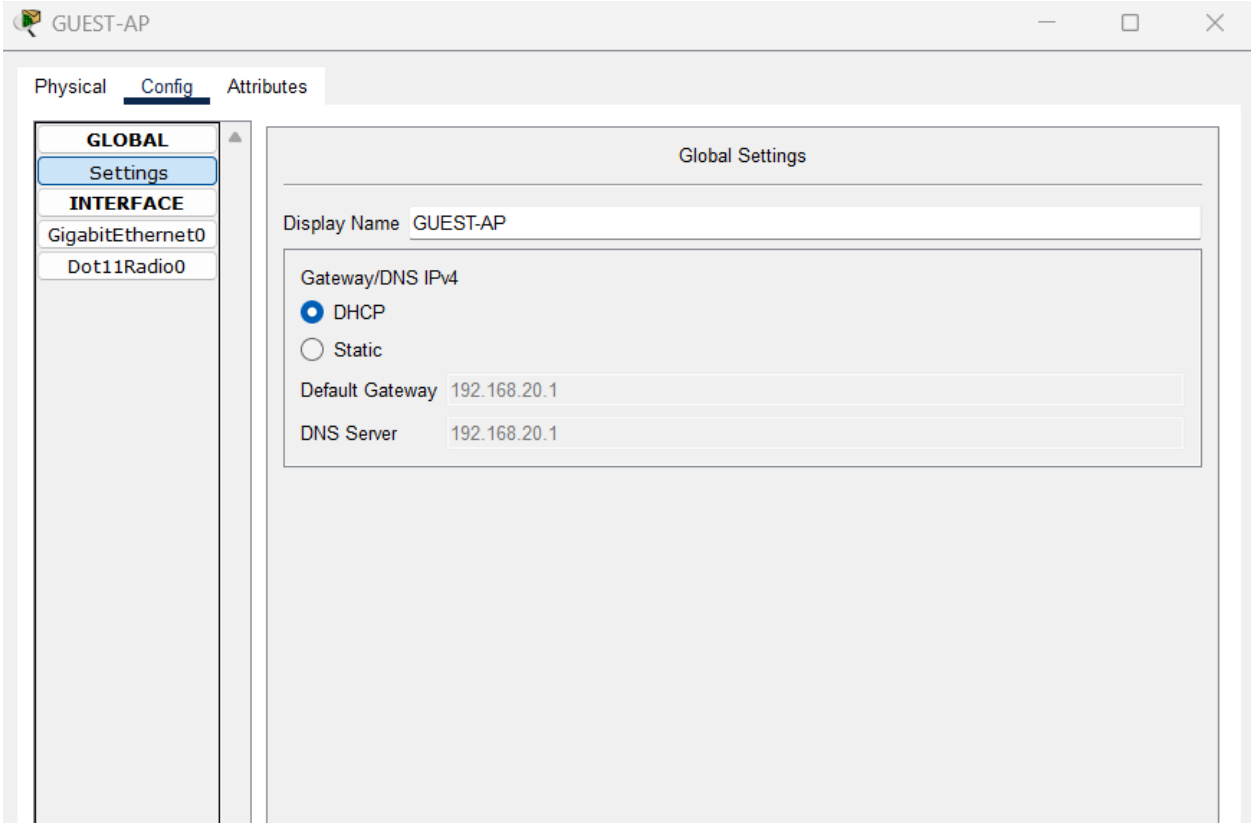
The IP address will be the ip address of the Wireless LAN Controller

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

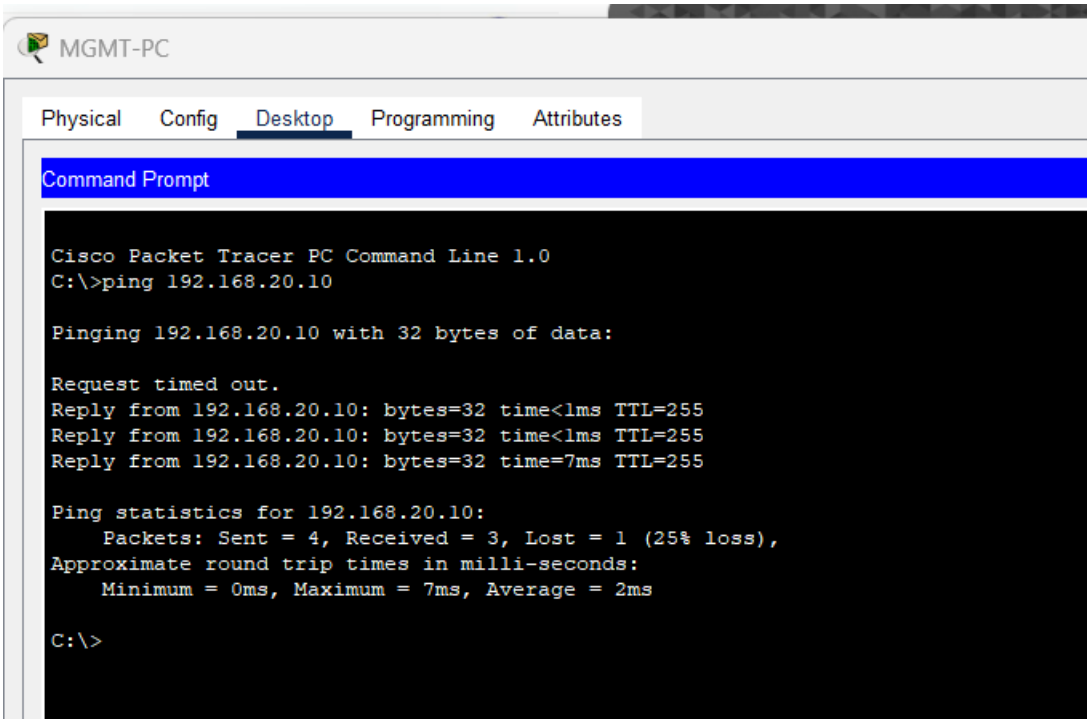

IT-AP
Physical
Config
Attributes
GLOBAL
Settings
INTERFACE
GigabitEthernet0
Dot11Radio0
Global Settings
Display Name
IT-AP
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.20.1
DNS Server
192.168.20.1


HR-AP
Physical
Config
Attributes
GLOBAL
Settings
INTERFACE
GigabitEthernet0
Dot11Radio0
Global Settings
Display Name
HR-AP
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.20.1
DNS Server
192.168.20.1

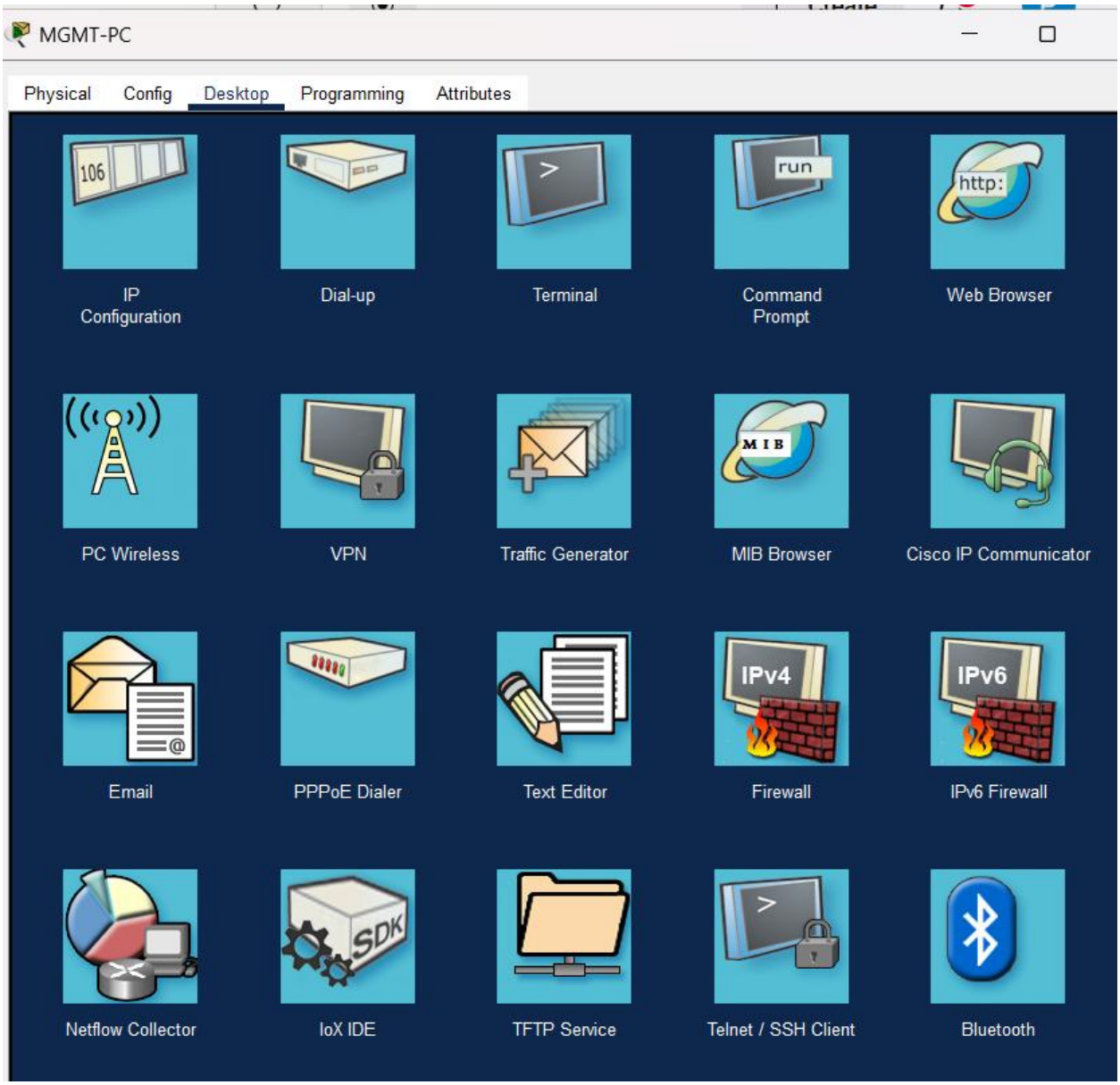


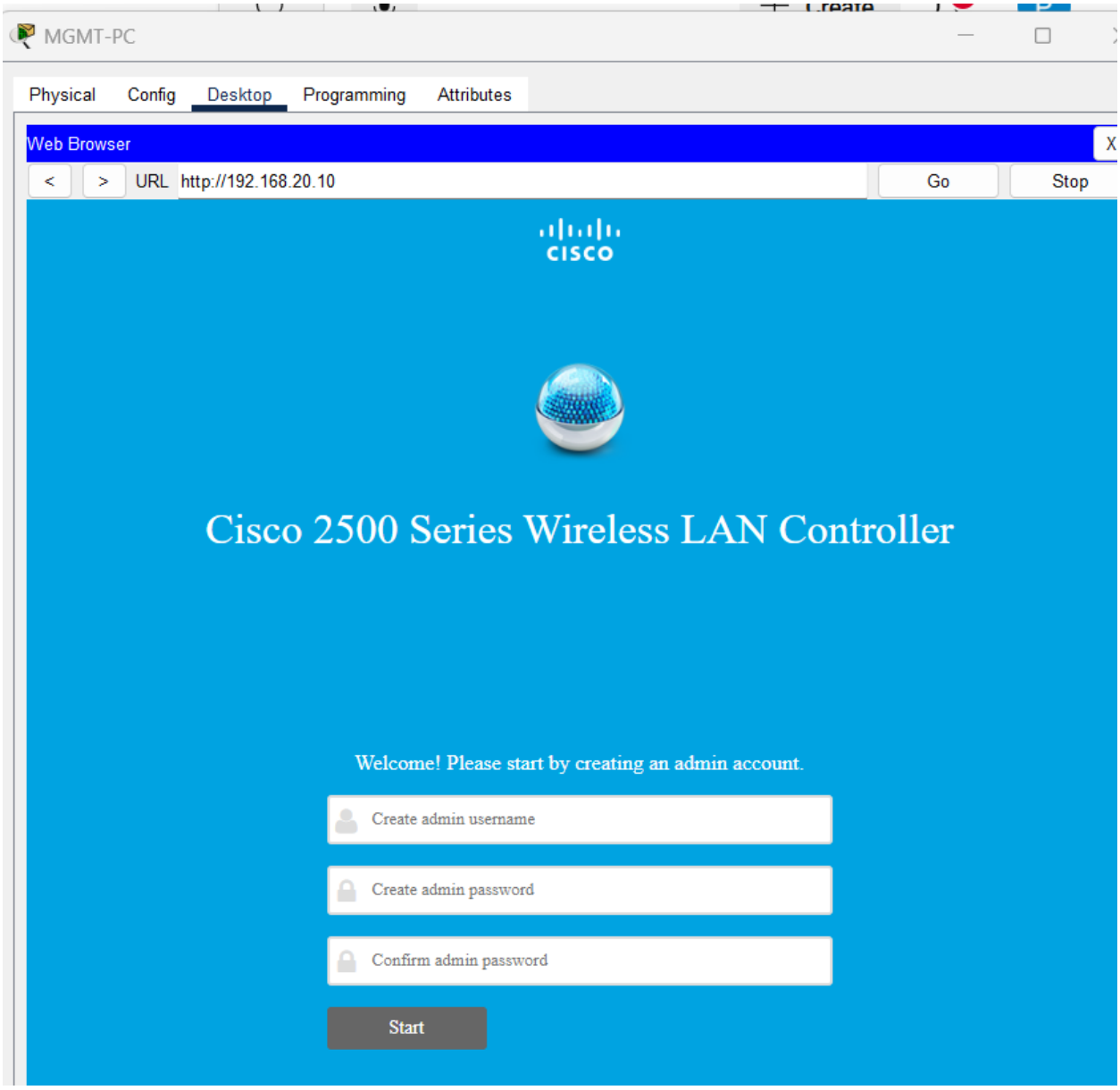


Now we can manage them remotely



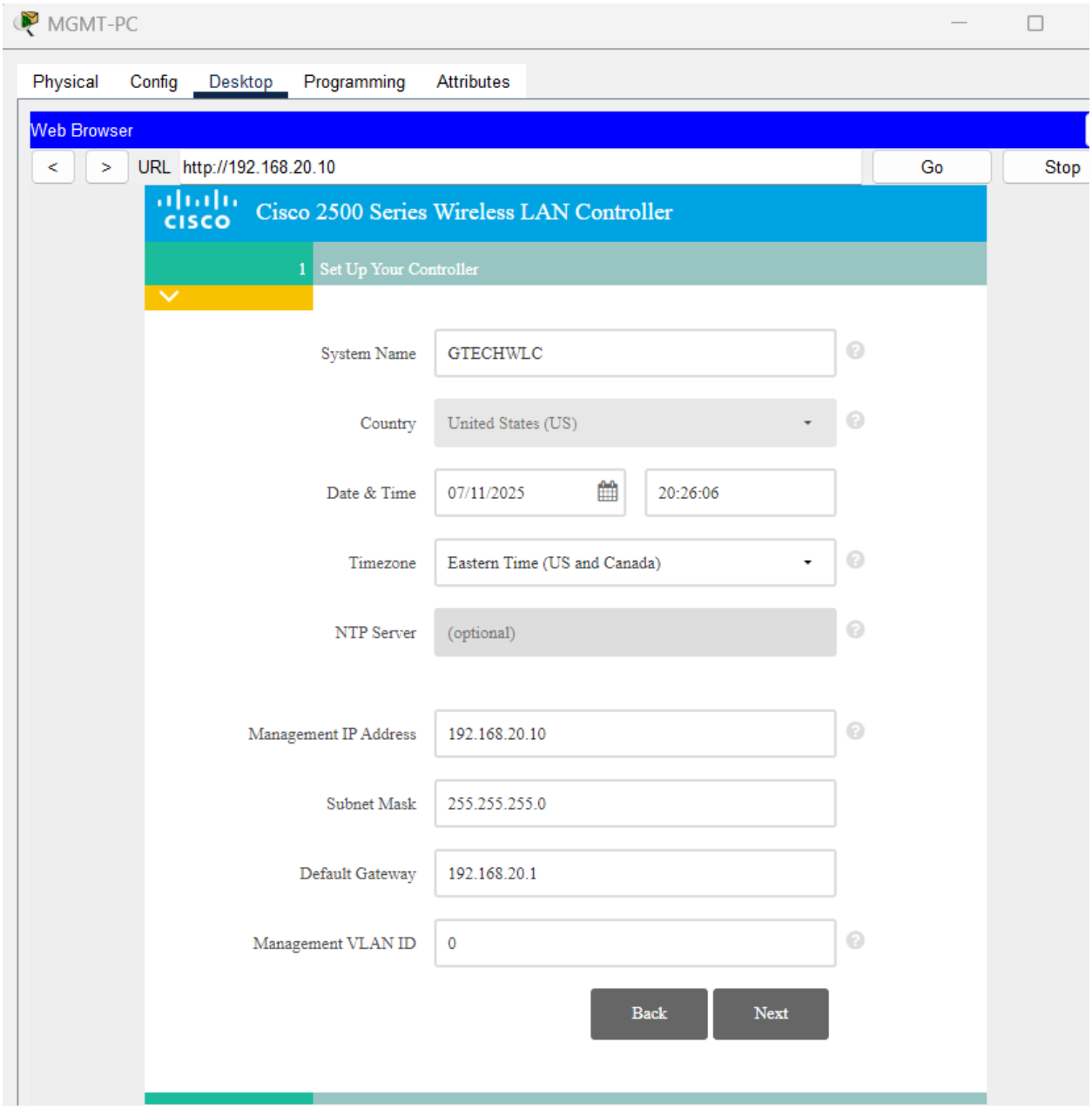
Go to Management PC

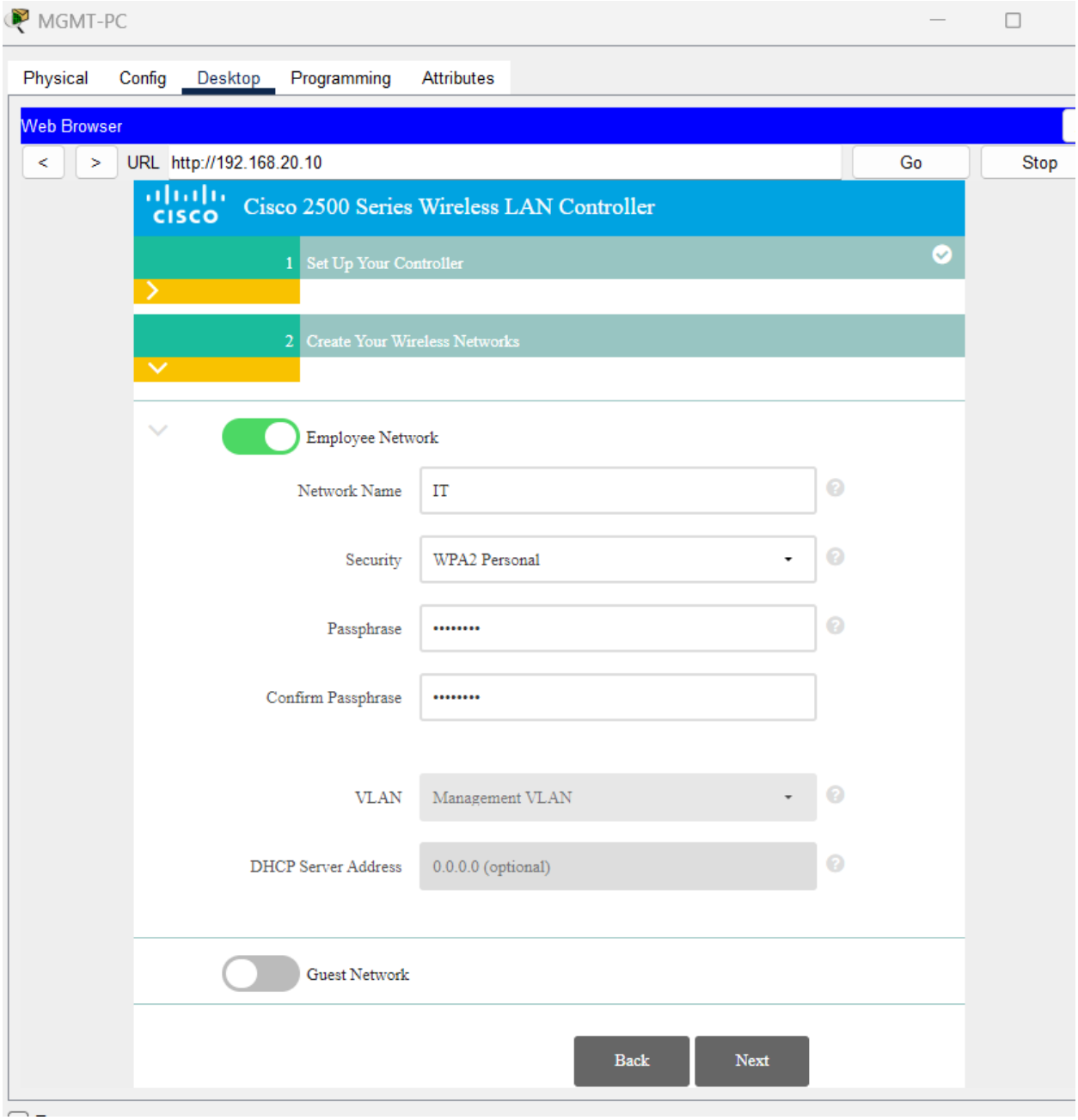

MGMT-PC
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Dial-up
Terminal
Command Prompt
Web Browser
PC Wireless
VPN
Traffic Generator
MIB Browser
Cisco IP Communicator
Email
PPPoE Dialer
Text Editor
Firewall
IPv6 Firewall
Netflow Collector
IoX IDE
TFTP Service
Telnet / SSH Client
Bluetooth

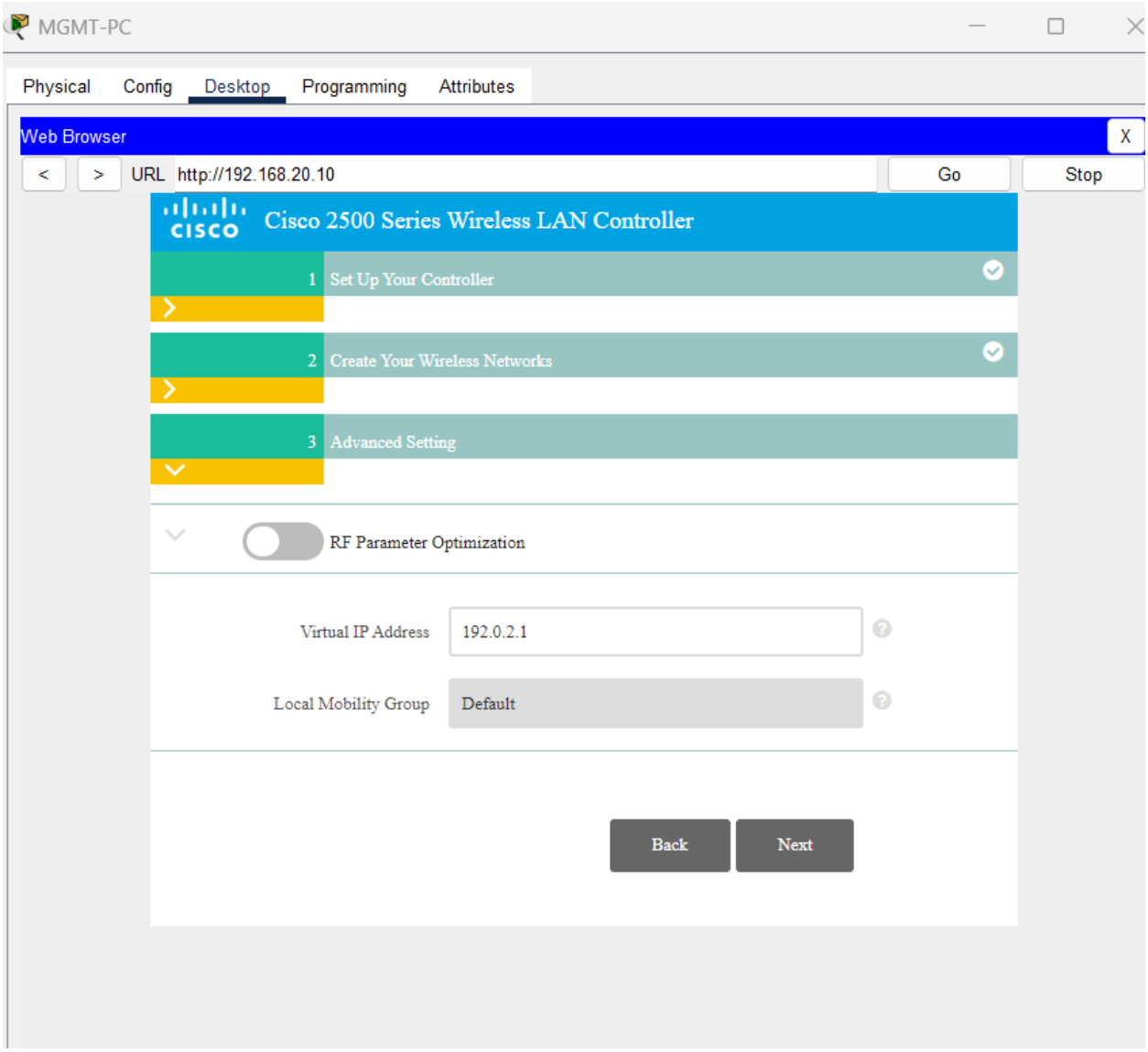


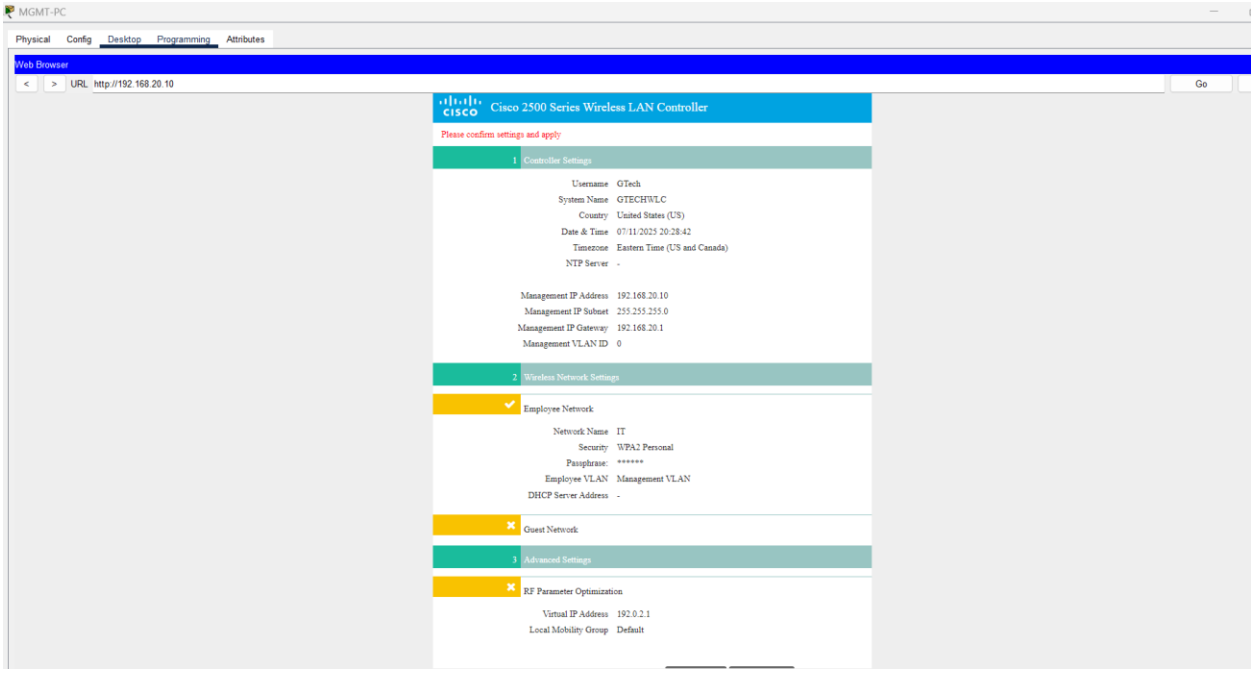
Username : GTech

Password : GTech123


MGMT-PC
Physical
Config
Desktop
Programming
Attributes
Web Browser
<
>
URL
http://192.168.20.10
Go
Stop
Cisco 2500 Series Wireless LAN Controller
1
Set Up Your Controller
System Name
GTECHWLC
Country
United States (US)
Date & Time
07/11/2025
20:26:06
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
Stop
Cisco 2500 Series Wireless LAN Controller
1 Set Up Your Controller
2 Create Your Wireless Networks
Employee Network
Network Name
IT
Security
WPA2 Personal
Passphrase
Confirm Passphrase
VLAN
Management VLAN
DHCP Server Address
0.0.0.0 (optional)
Guest Network
Back
Next


MGMT-PC
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.20.10
Go
Stop
Cisco 2500 Series Wireless LAN Controller
1 Set Up Your Controller
2 Create Your Wireless Networks
3 Advanced Setting
RF Parameter Optimization
Virtual IP Address
192.0.2.1
Local Mobility Group
Default
Back
Next


MGMT-PC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL http://192.168.20.10
Go
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

Physical | Config | Desktop | Programming | Attributes

Web Browser

< > URL http://192.168.20.10 Go Stop

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	-

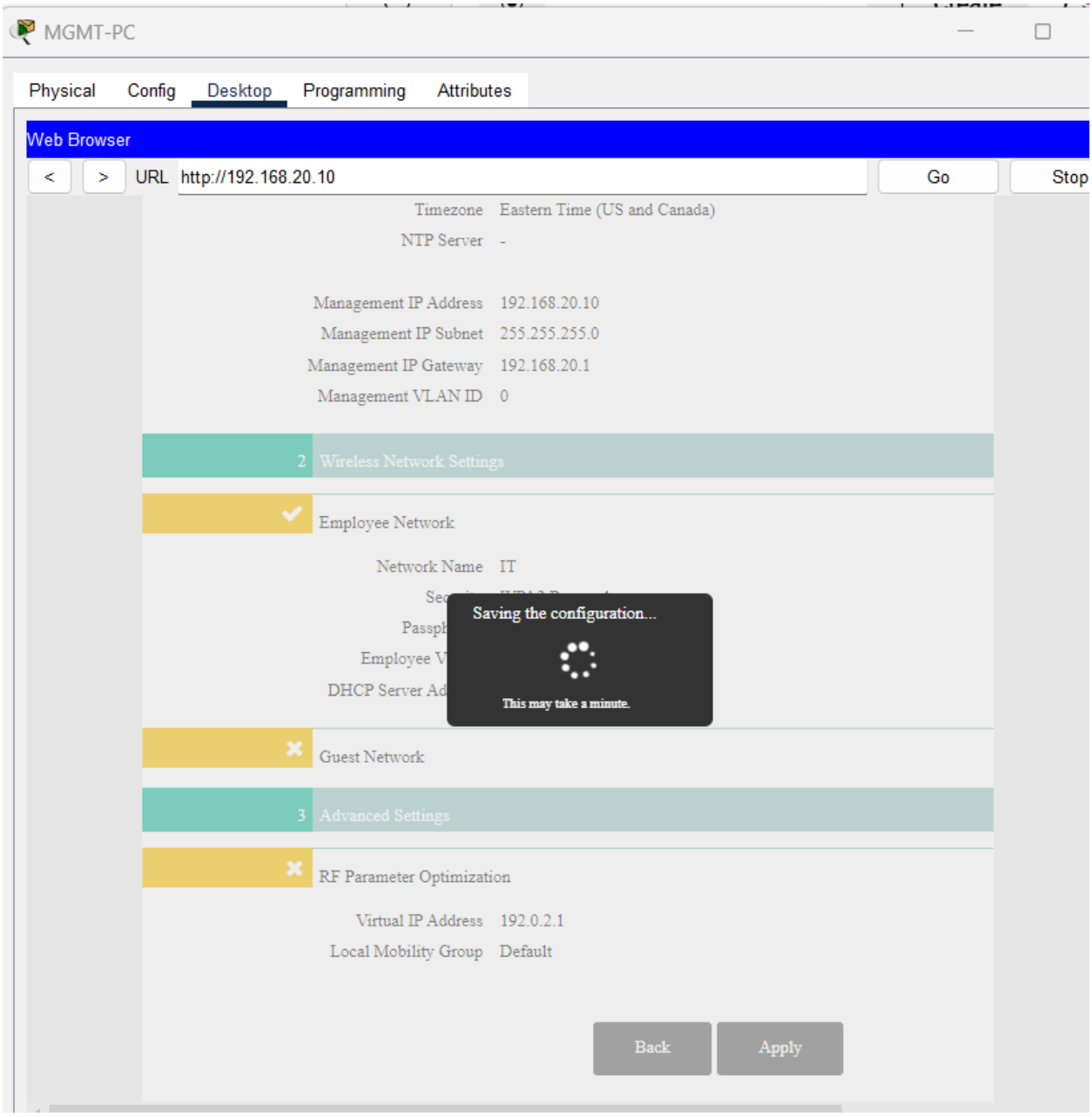
✖ Guest Network

3 Advanced Settings

✖ RF Parameter Optimization

Virtual IP Address	192.0.2.1
Local Mobility Group	Default

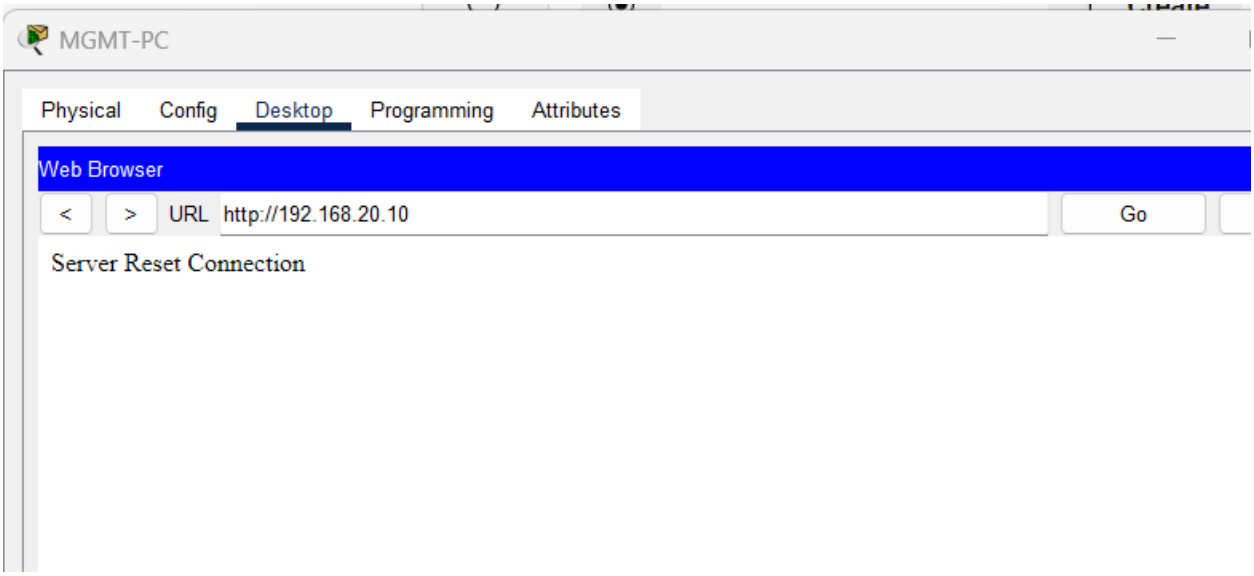
Back Apply



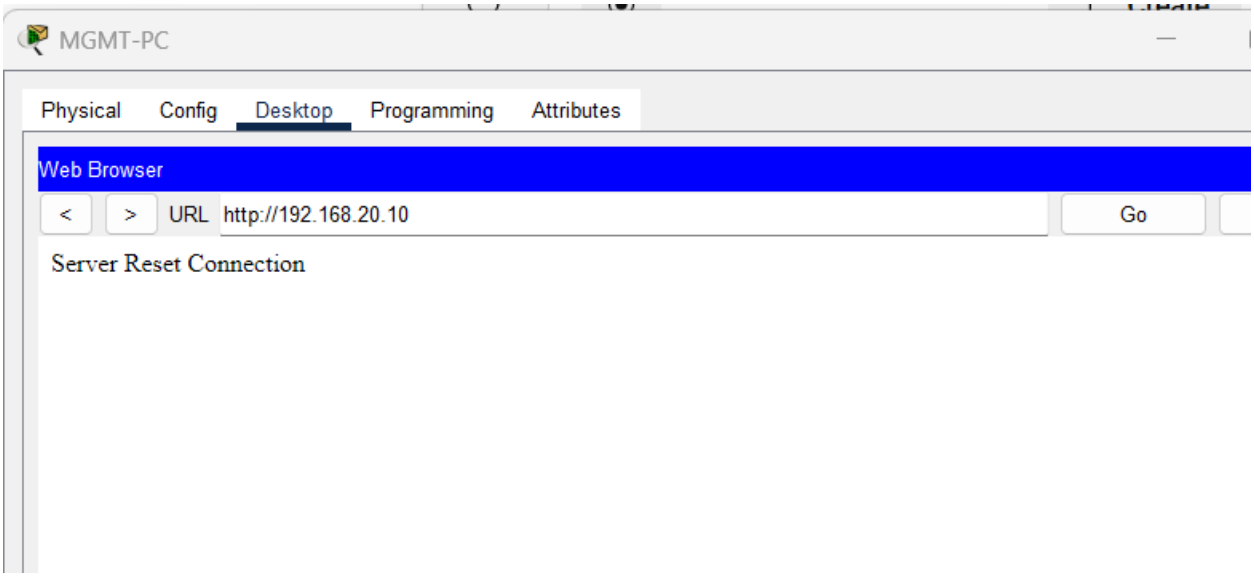
Close the Web Browser and come to command prompt and ping again

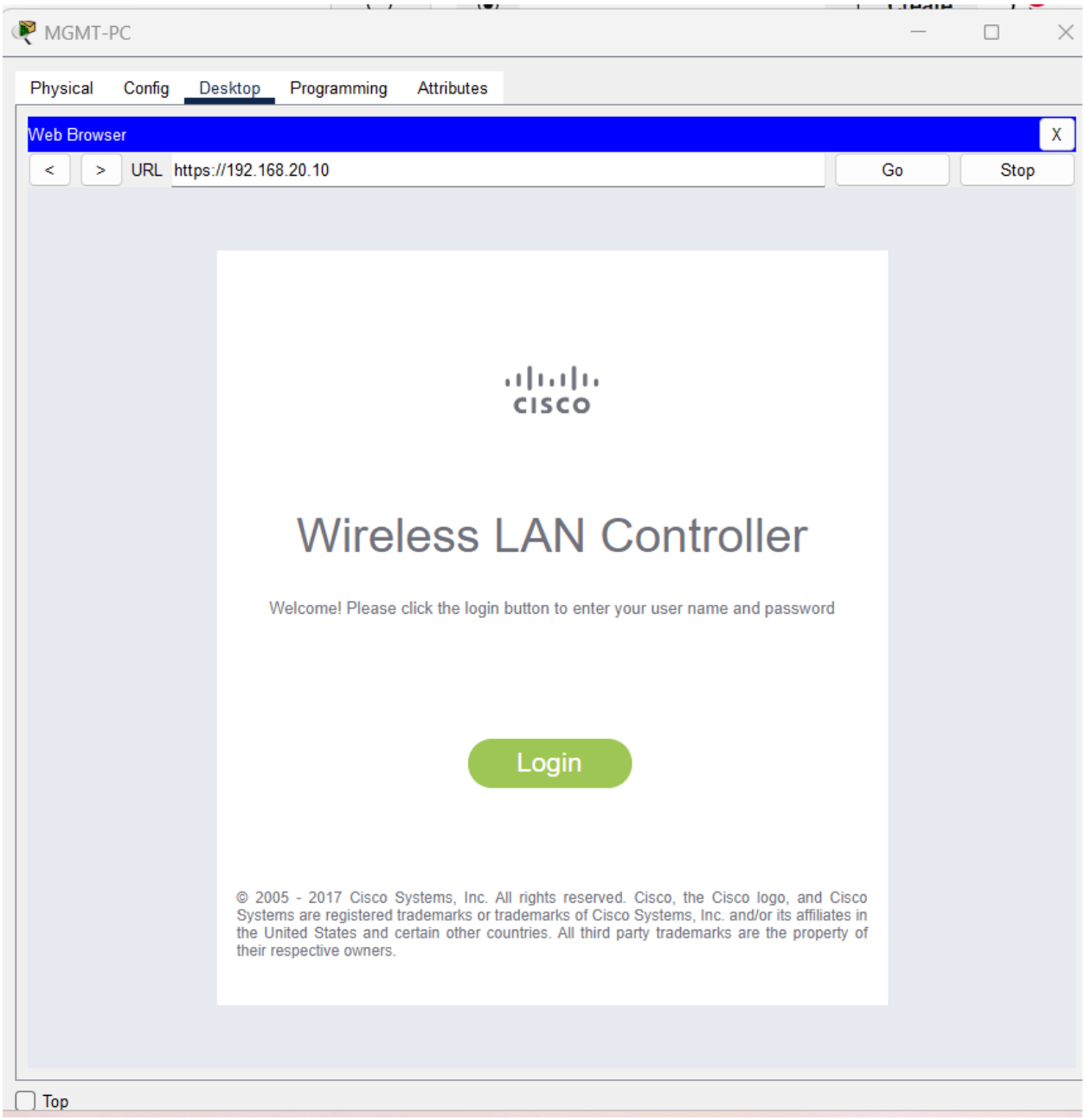
By going back again to browser we again get this error

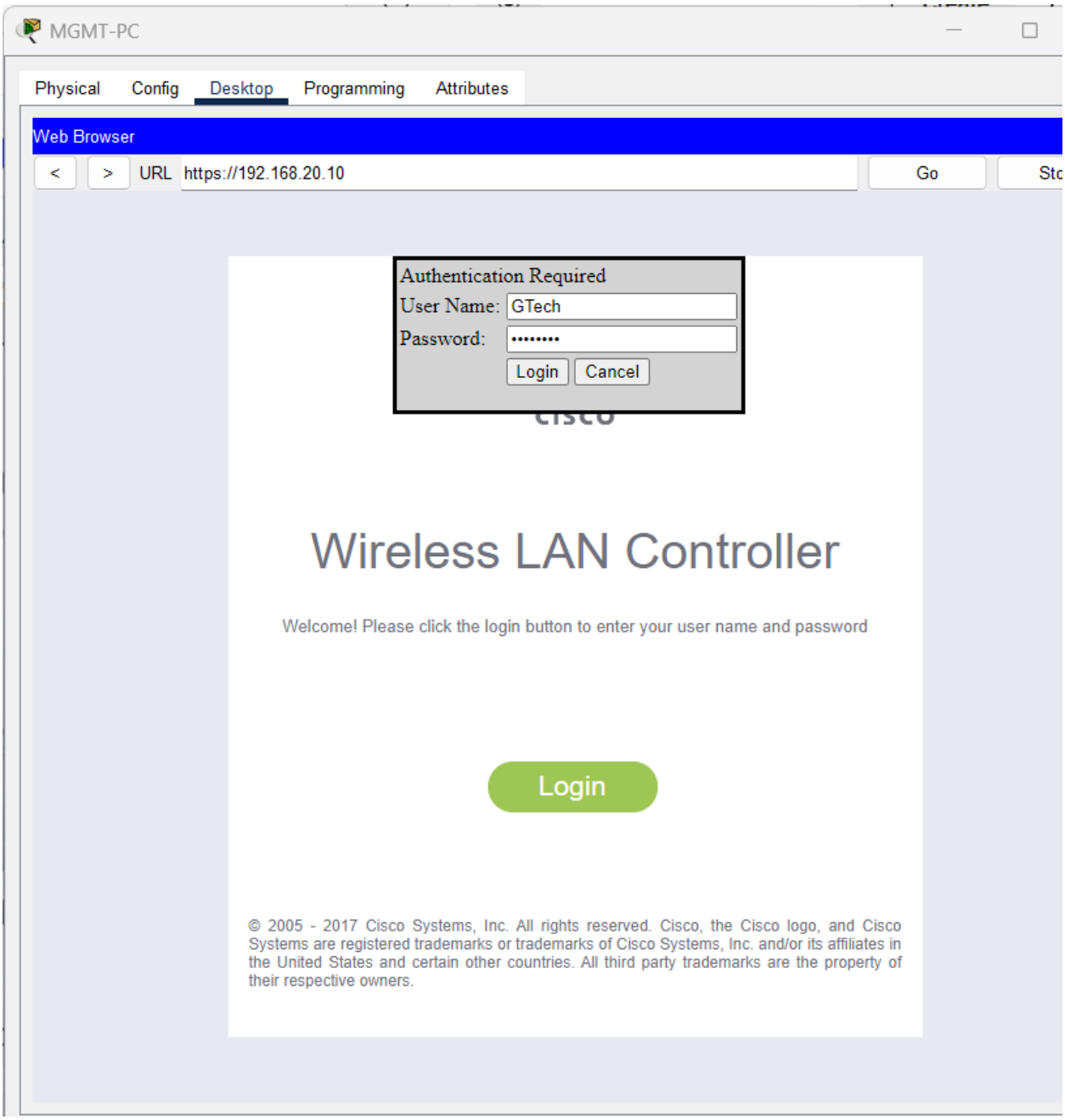
```
C:\>ping 192.16820.10
Ping request could not find host 192.16820.10. Please check the name and try again.
C:\>ping 192.168.20.10

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:\>
```



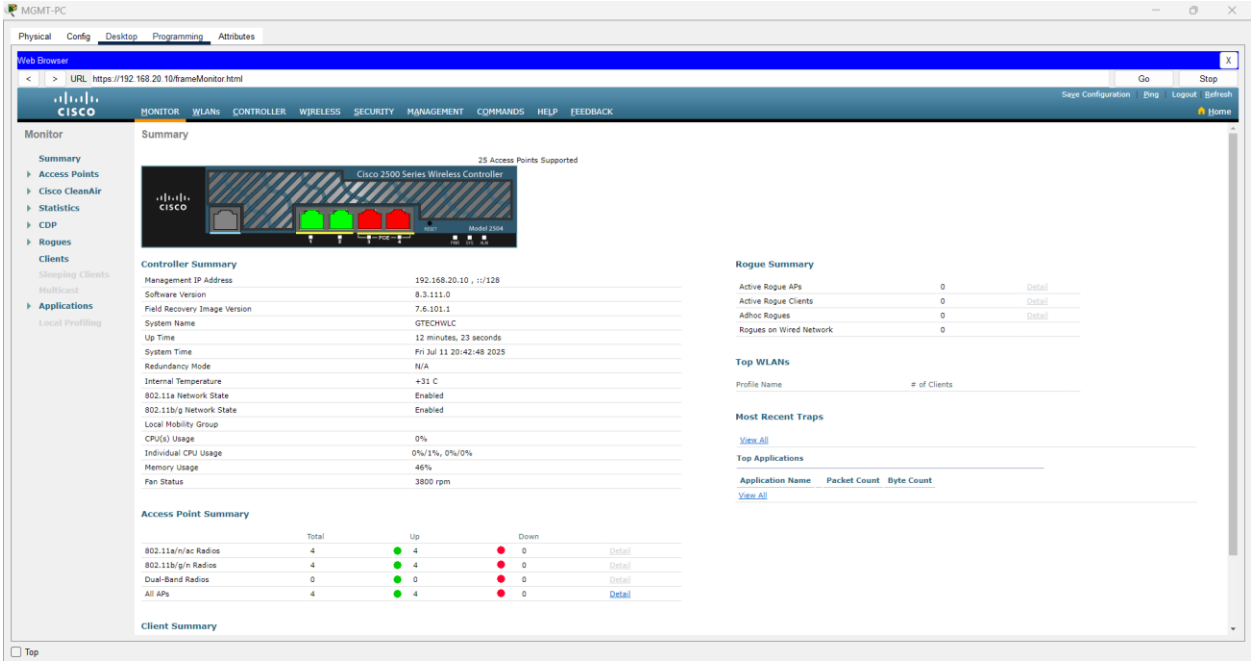
Change it to https


MGMT-PC
Physical
Config
Desktop
Programming
Attributes
Web Browser
<
>
URL
http://192.168.20.10
Go
Server Reset Connection


MGMT-PC
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
https://192.168.20.10
Go
Stop
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.
Top

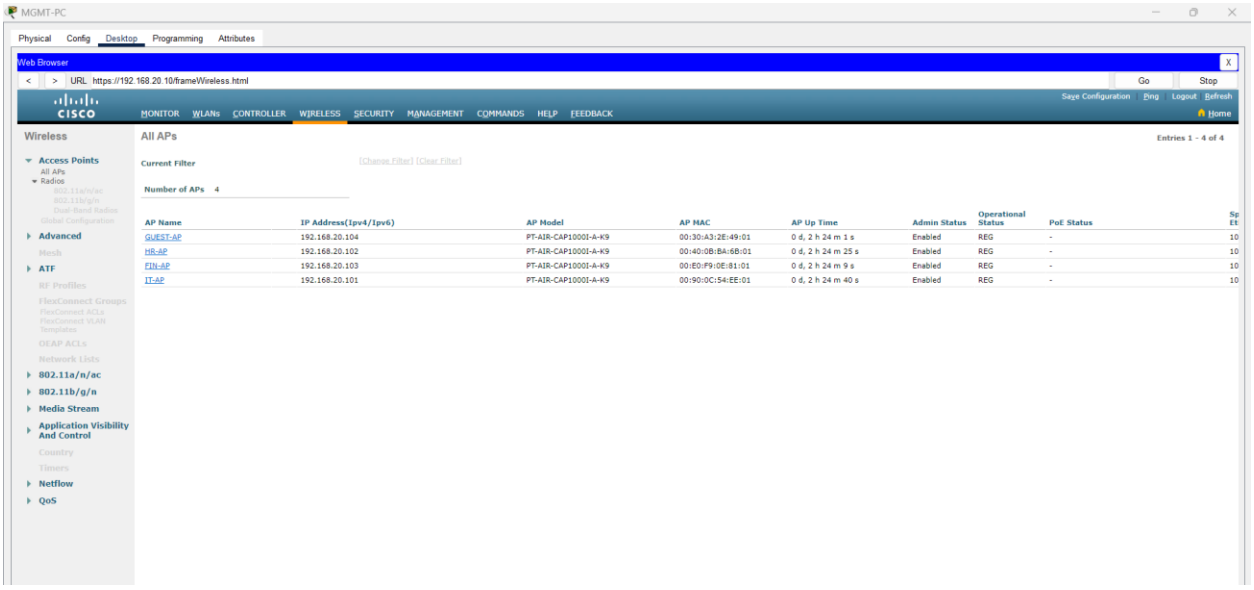


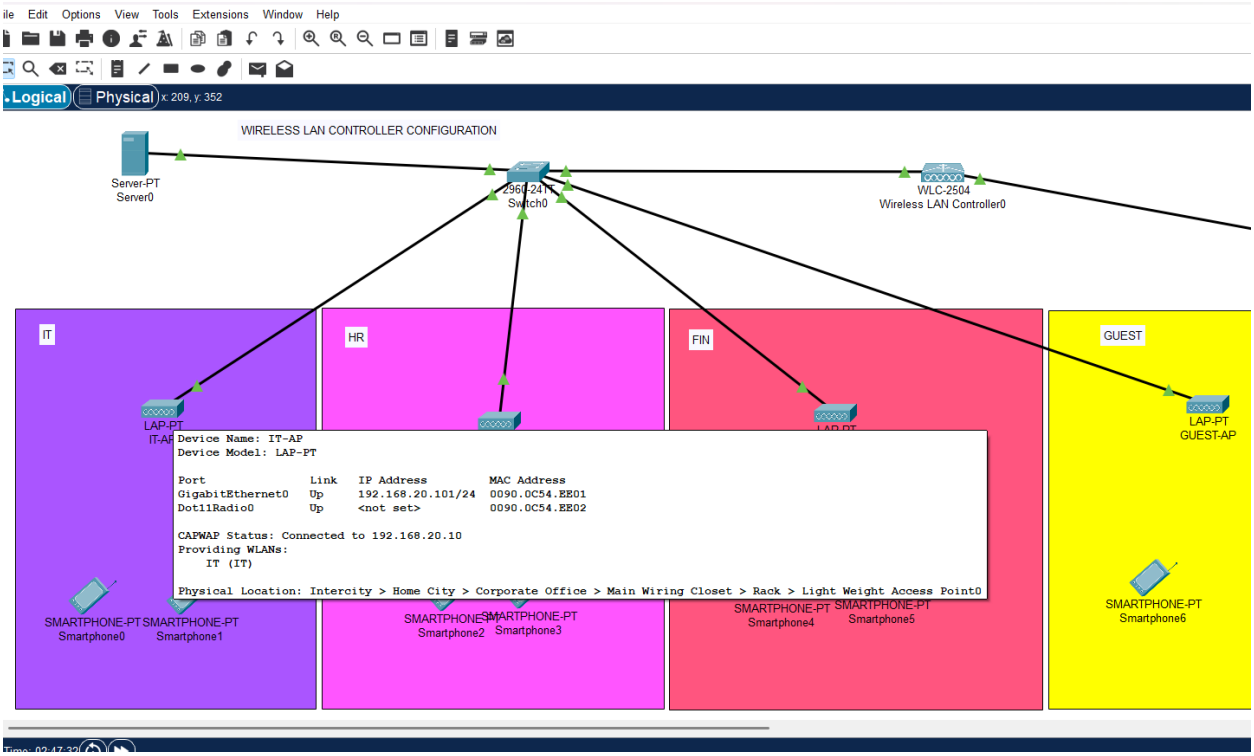
Pysical port of Wireless LAN Controller



Lets check the status of Wireless LAN Access Point

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





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

< > 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
  - WLANs
- Advanced
  - AP Groups

WLANs > New

< BACK Apply

Type	WLAN
Profile Name	HR
SSID	HR
ID	2

MGMT-PC

Physical Config Desktop Programming Attributes

Web Browser

< > 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

Home

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
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 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 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

Save Configuration | Ping | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

- WLANs
  - WLANs
- Advanced
  - AP Groups

WLANs > Edit 'HR'

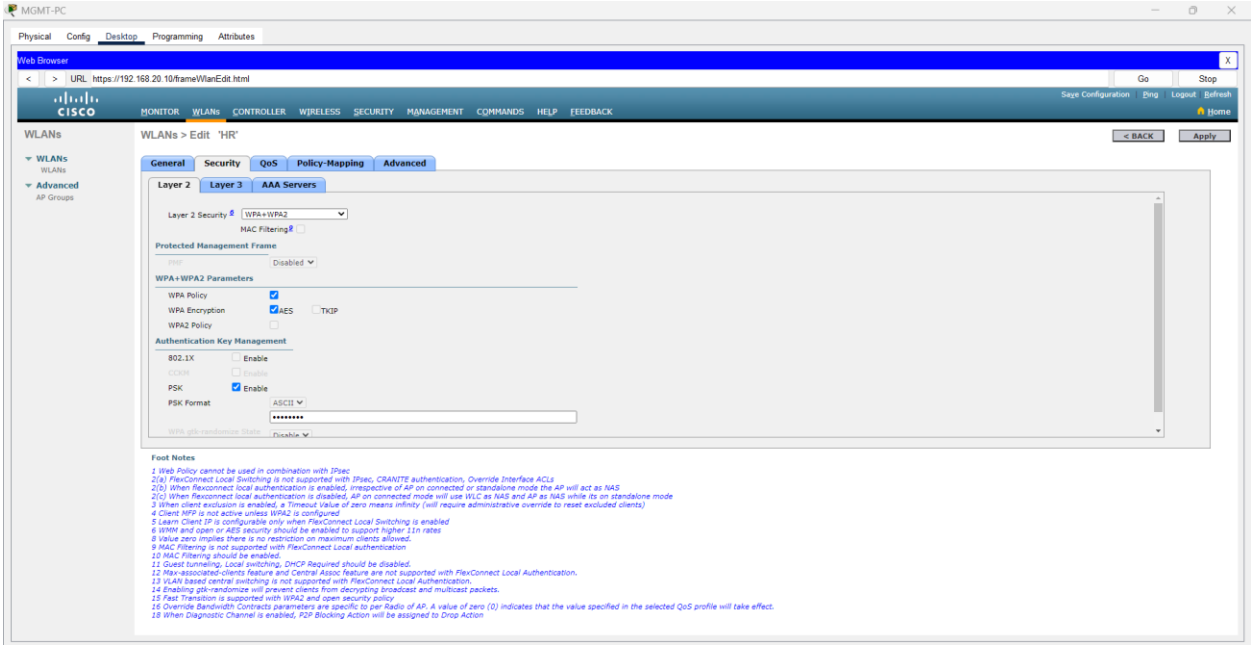
< BACK Apply

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
Ping
Logout
Refresh
Home
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
WLANs
WLANs > Edit 'HR'
< BACK
Apply
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA Encryption
AES
TKIP
WPA2 Policy
Authentication Key Management
802.1X
Enable
CCKM
Enable
PSK
Enable
PSK Format
ASCII
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 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 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

Save Configuration | Ping | Logout | Refresh

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

WLANs

- WLANs
  - WLANs
- Advanced
  - AP Groups

WLANs > Edit 'HR'

< BACK | Apply

General | Security | QoS | Policy-Mapping | Advanced

Profile Name: HR

Type: WLAN

SSID: HR

Javascript Confirm - https://192.168.20.10/frameWlanEdit.html

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.

OK | Cancel

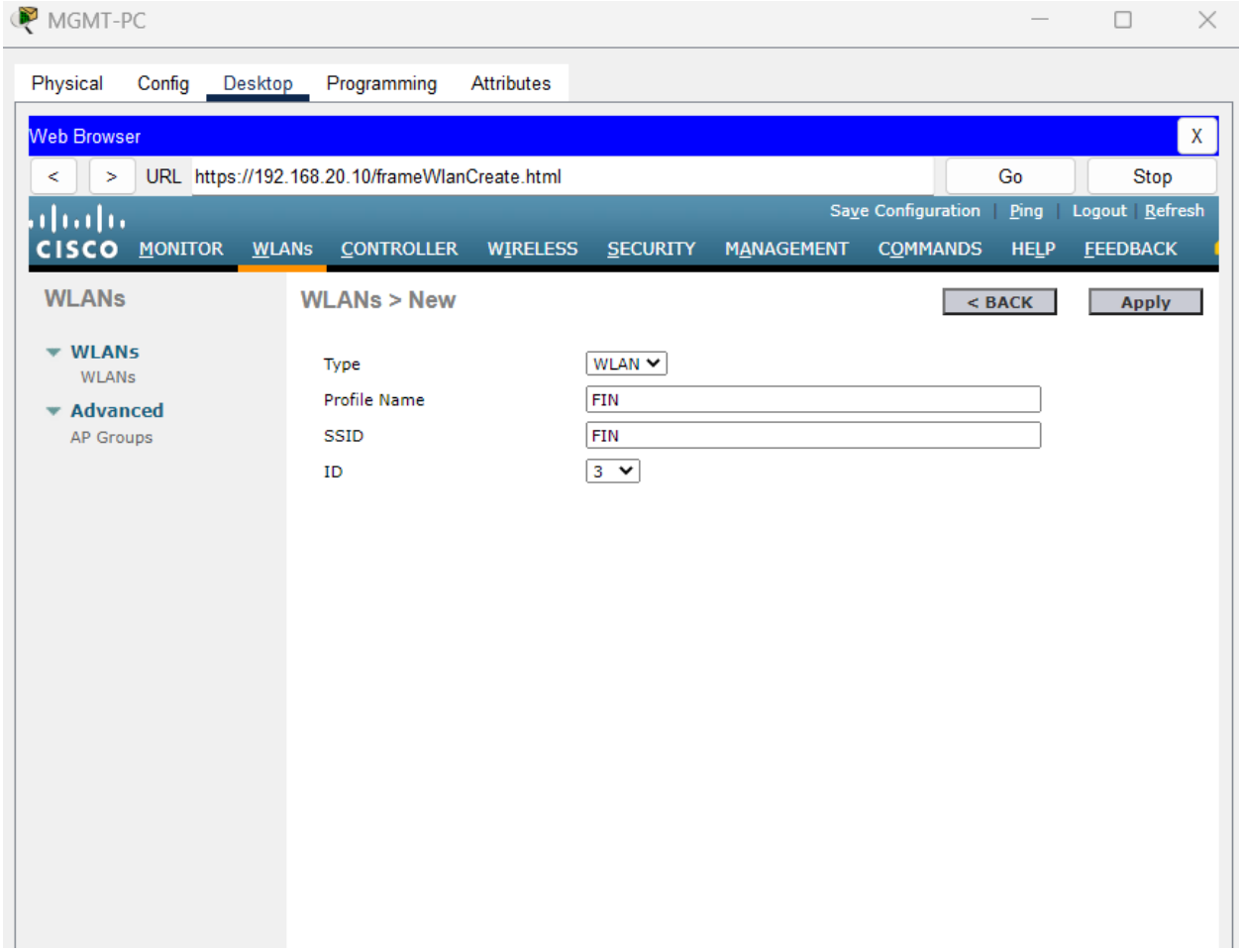
Multicast Vlan Feature: Enabled

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
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
FIN
SSID
FIN
ID
3

MGMT-PC

Physical | Config | Desktop | Programming | Attributes

Web Browser

< > 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 '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

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 'FIN'

< BACK | Apply

General | Security | QoS | Policy-Mapping | Advanced

Layer 2 | Layer 3 | AAA Servers

MAC Filtering[9]

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy: [x]

WPA Encryption: [x] AES [ ] TKIP

WPA2 Policy: [ ]

Authentication Key Management

802.1X: [ ] Enable

CCKM: [ ] Enable

PSK: [x] Enable

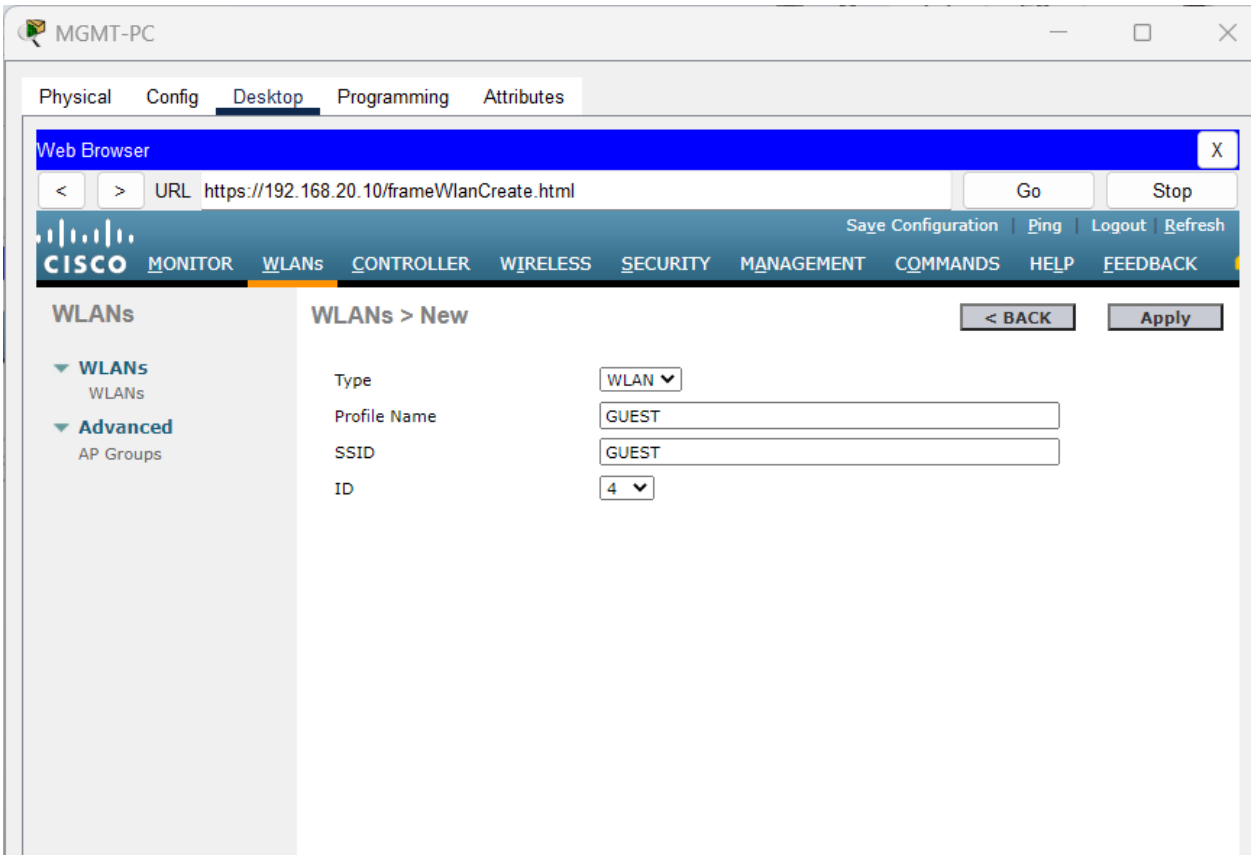
PSK Format: ASCII

••••••••

WPA gtk-randomize State[14]: 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/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
GUEST
SSID
GUEST
ID
4

MGMT-PC

Physical | Config | Desktop | Programming | Attributes

Web Browser

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 [6] WPA+WPA2

MAC Filtering [9] ☐

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☑

WPA2 Encryption ☑ AES ☐ TKIP

Authentication Key Management

802.1X ☐ Enable

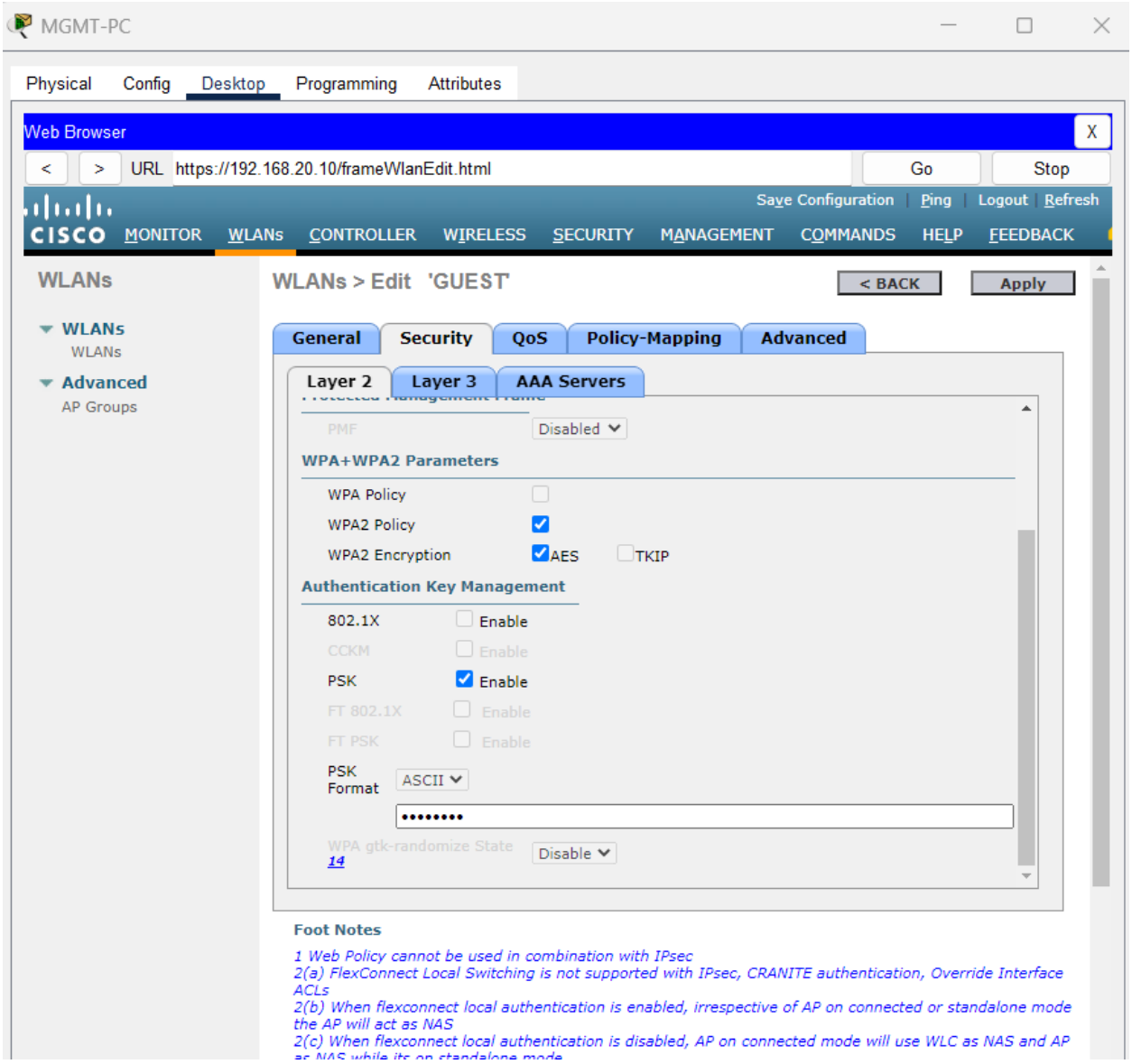
CCKM ☐ Enable

PSK ☑ Enable

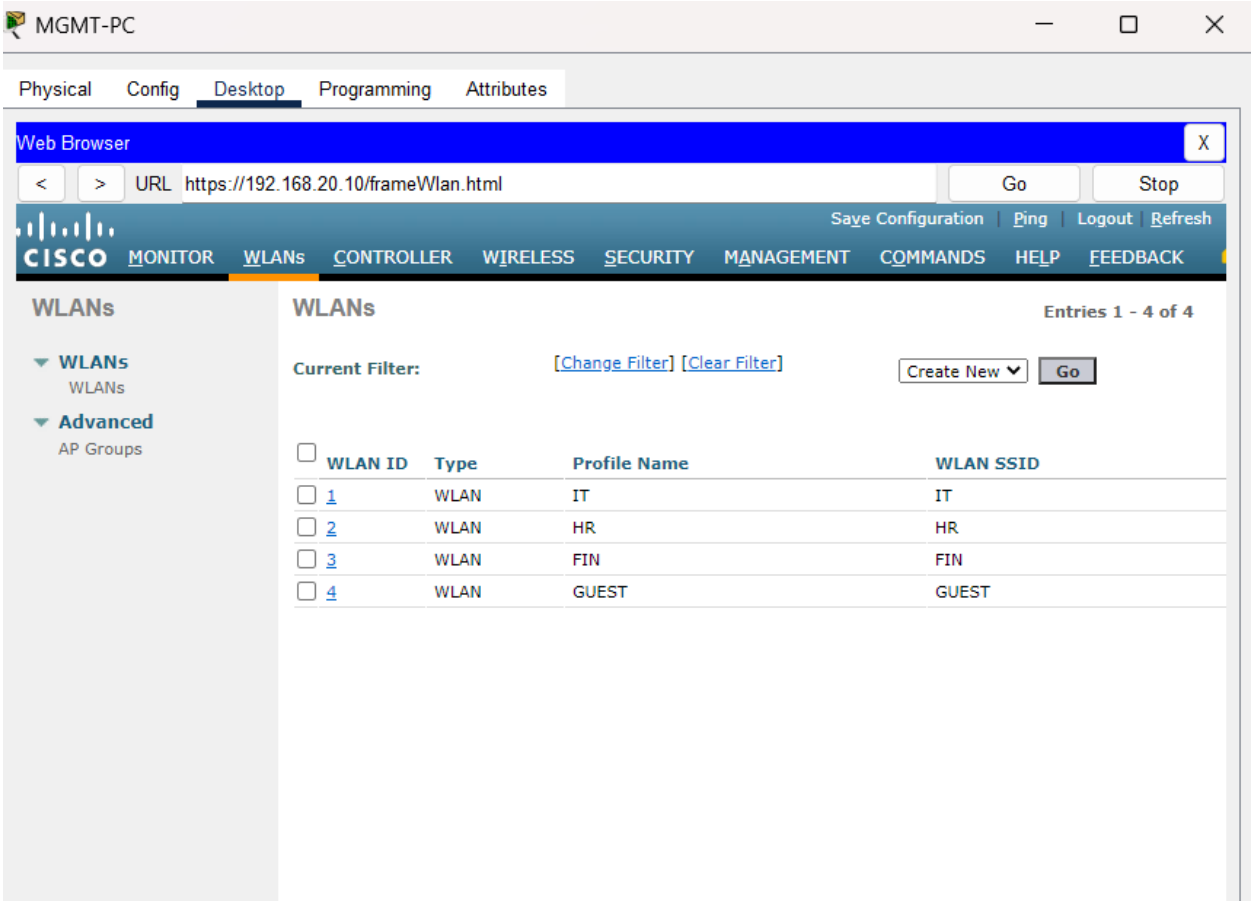
FT 802.1X ☐ Enable

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)

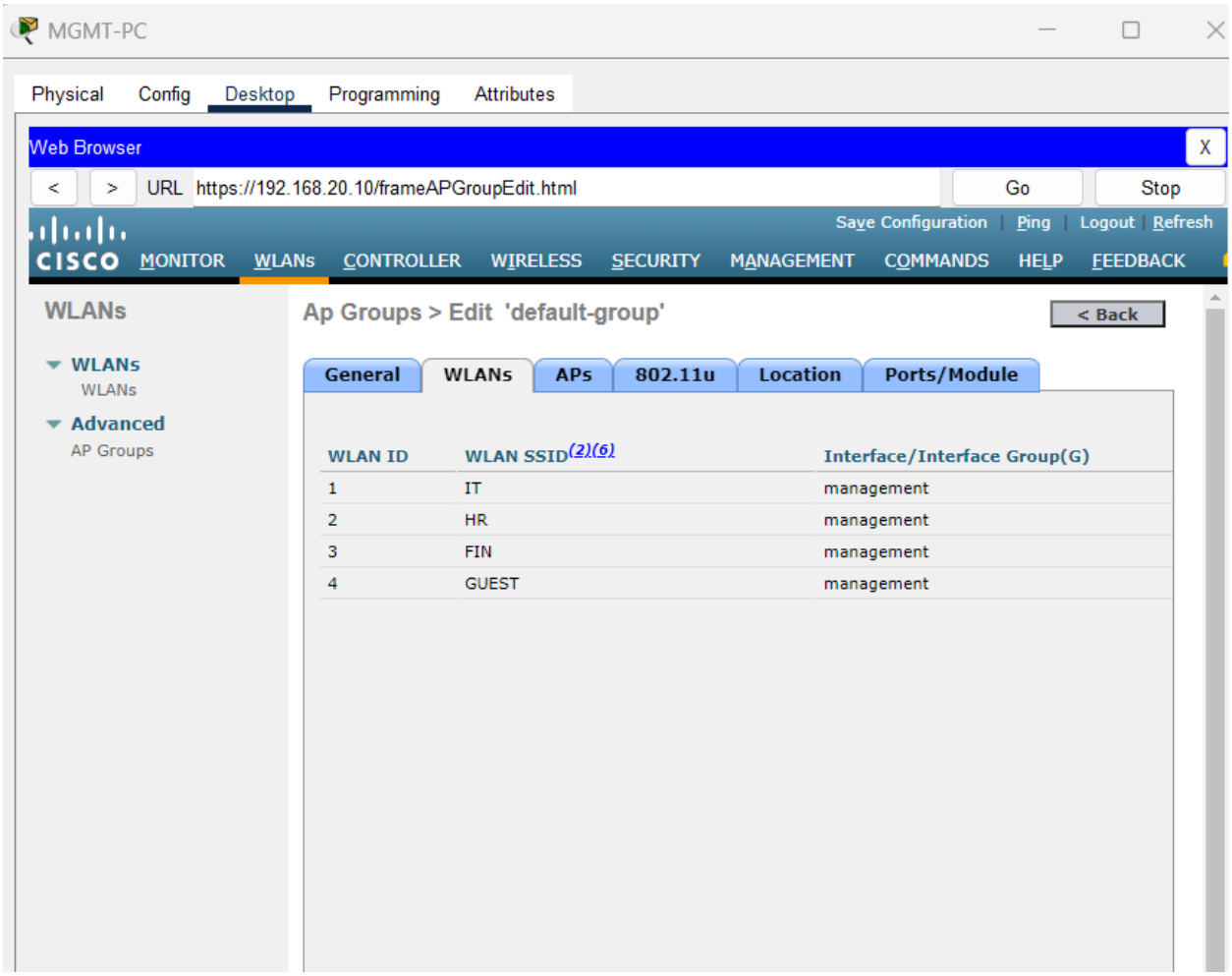


Number of created Wi-Fi network



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

Click on Access Points you will see



Click on WLANs you will see her

MGMT-PC

Physical | Config | Desktop | Programming | Attributes

Web Browser

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

- WLANs
  - WLANs
- Advanced
  - AP Groups

Ap Groups > Edit 'default-group'

< Back

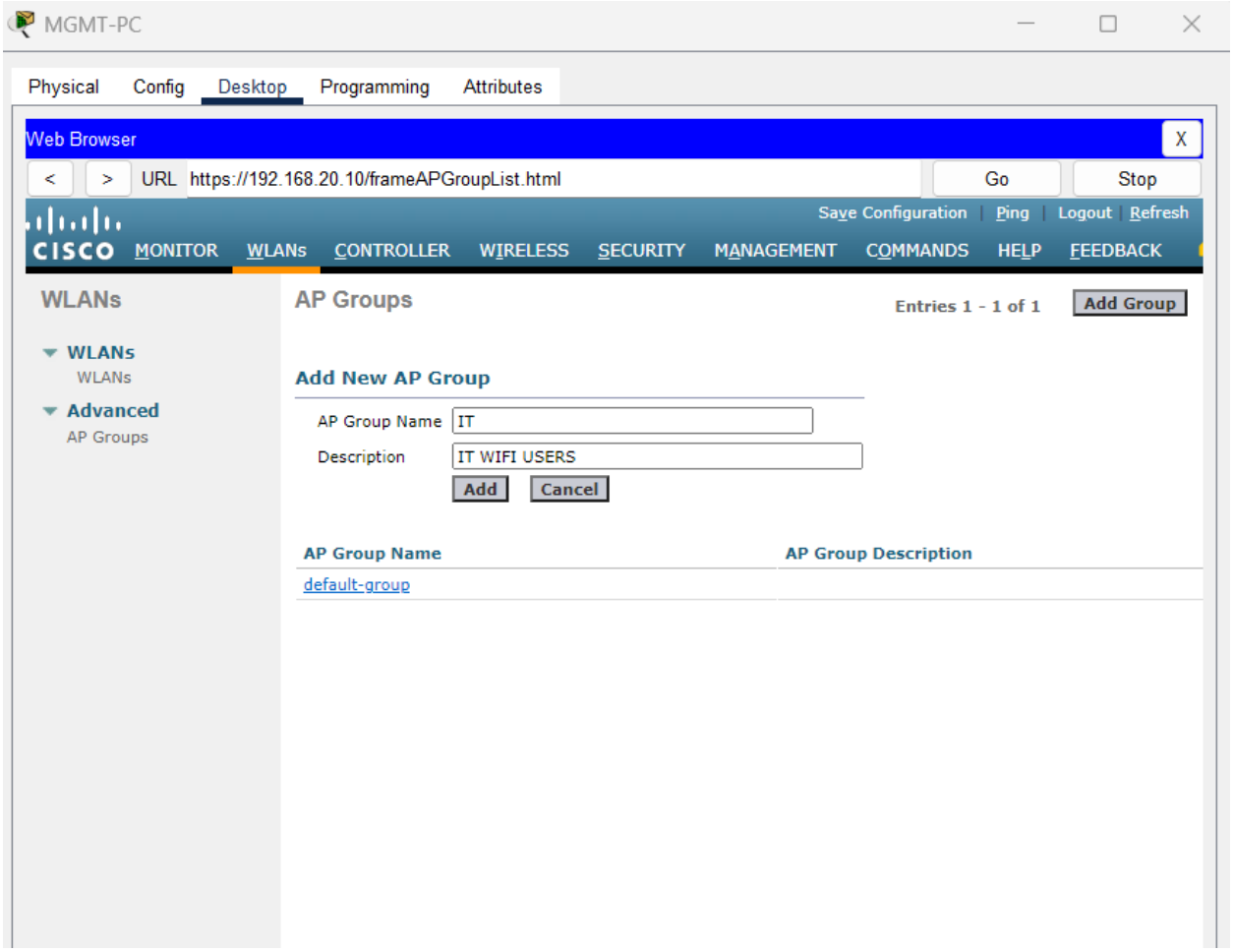
General | WLANs | APs | 802.11u | Location | Ports/Module

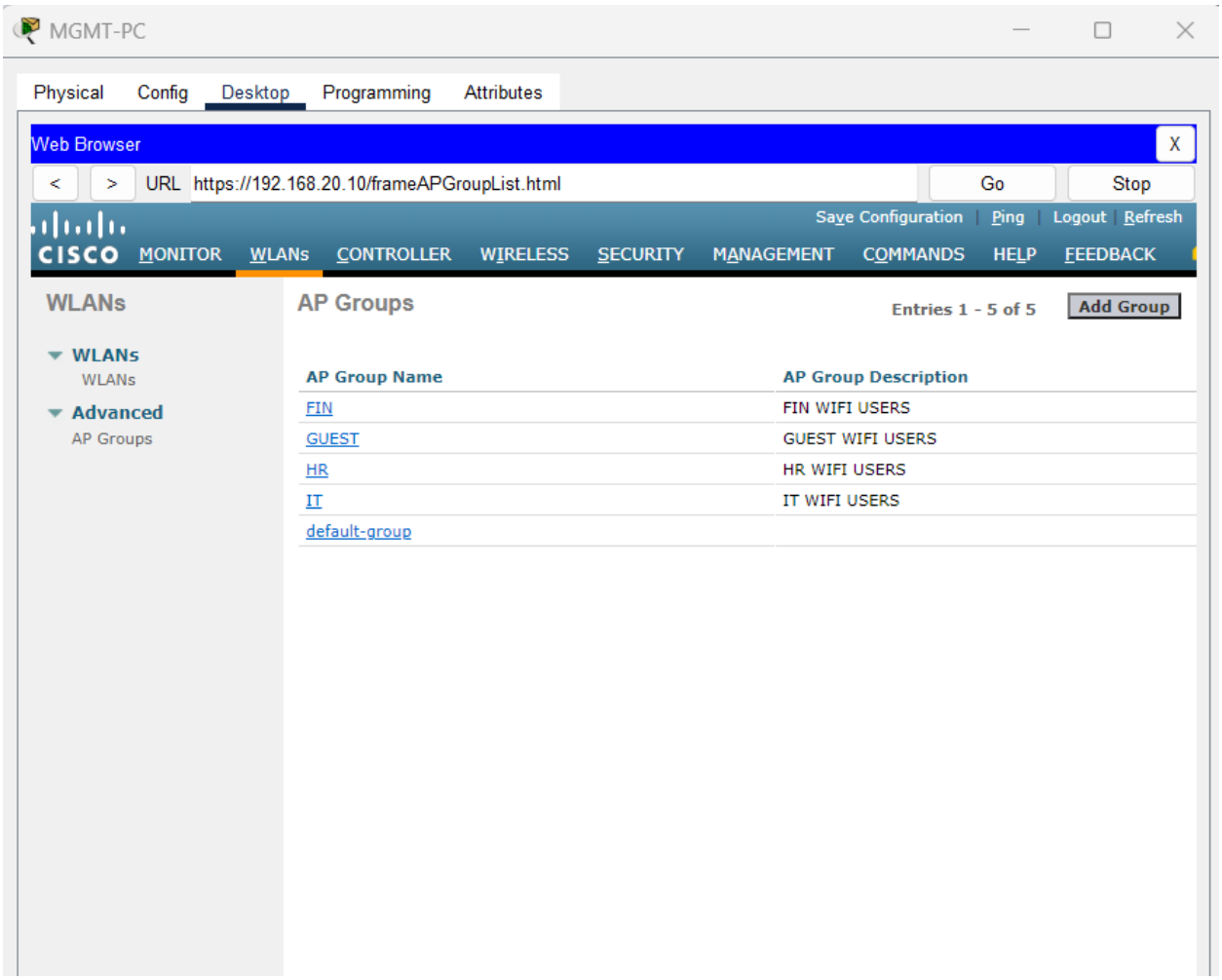
APs currently in the Group

AP Name	Ethernet MAC
GUEST-AP	0030.A32E.4901
HR-AP	0040.0BBA.6B01
FIN-AP	00E0.F90E.8101
IT-AP	0090.0C54.EE01

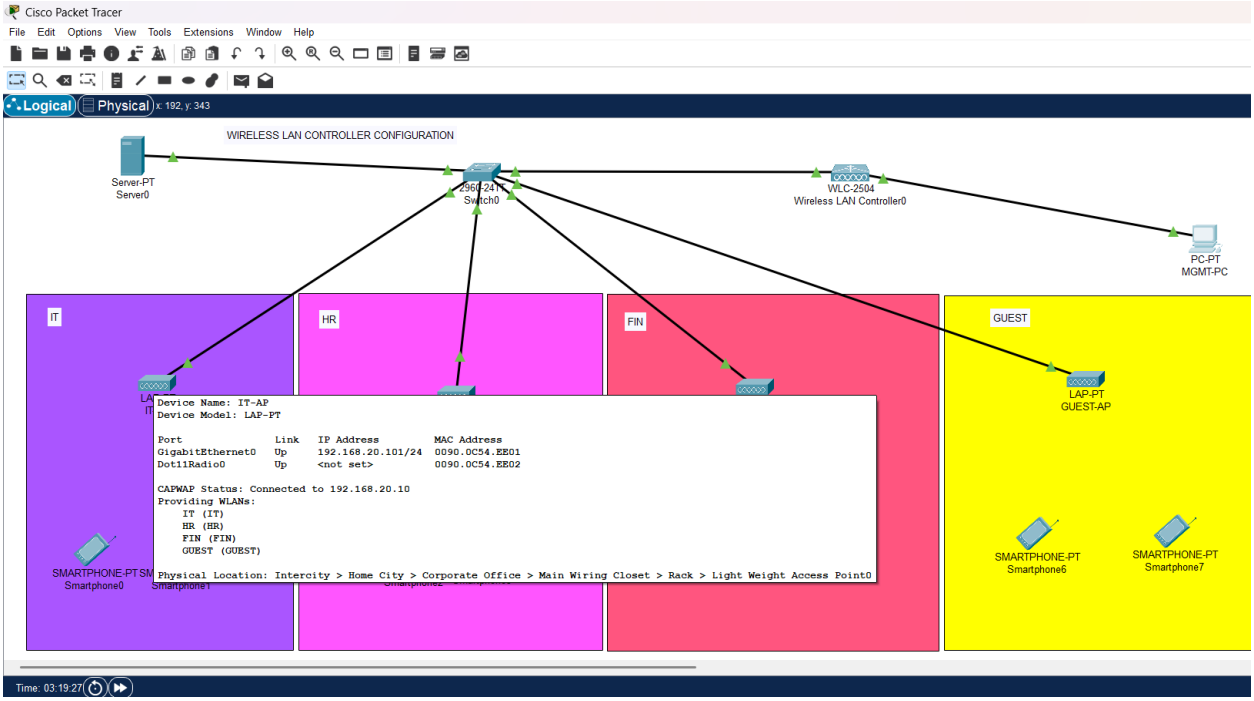
Add APs to the Group

AP Name

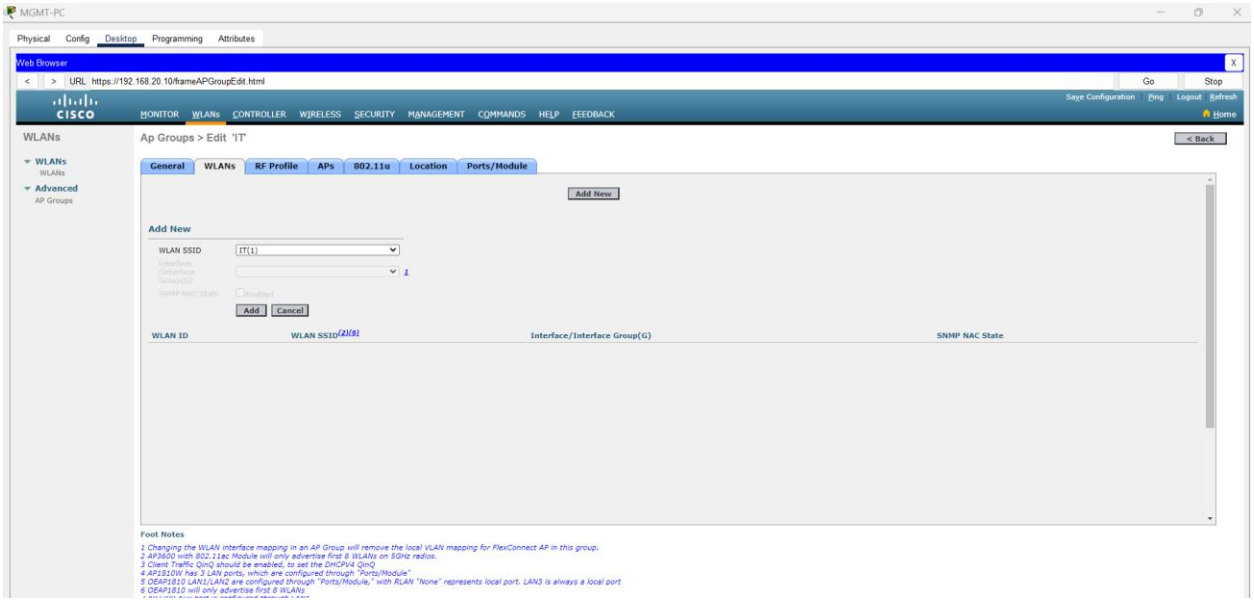

MGMT-PC
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
https://192.168.20.10/frameAPGroupList.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
WLANs
WLANs
WLANs
Advanced
AP Groups
AP Groups
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



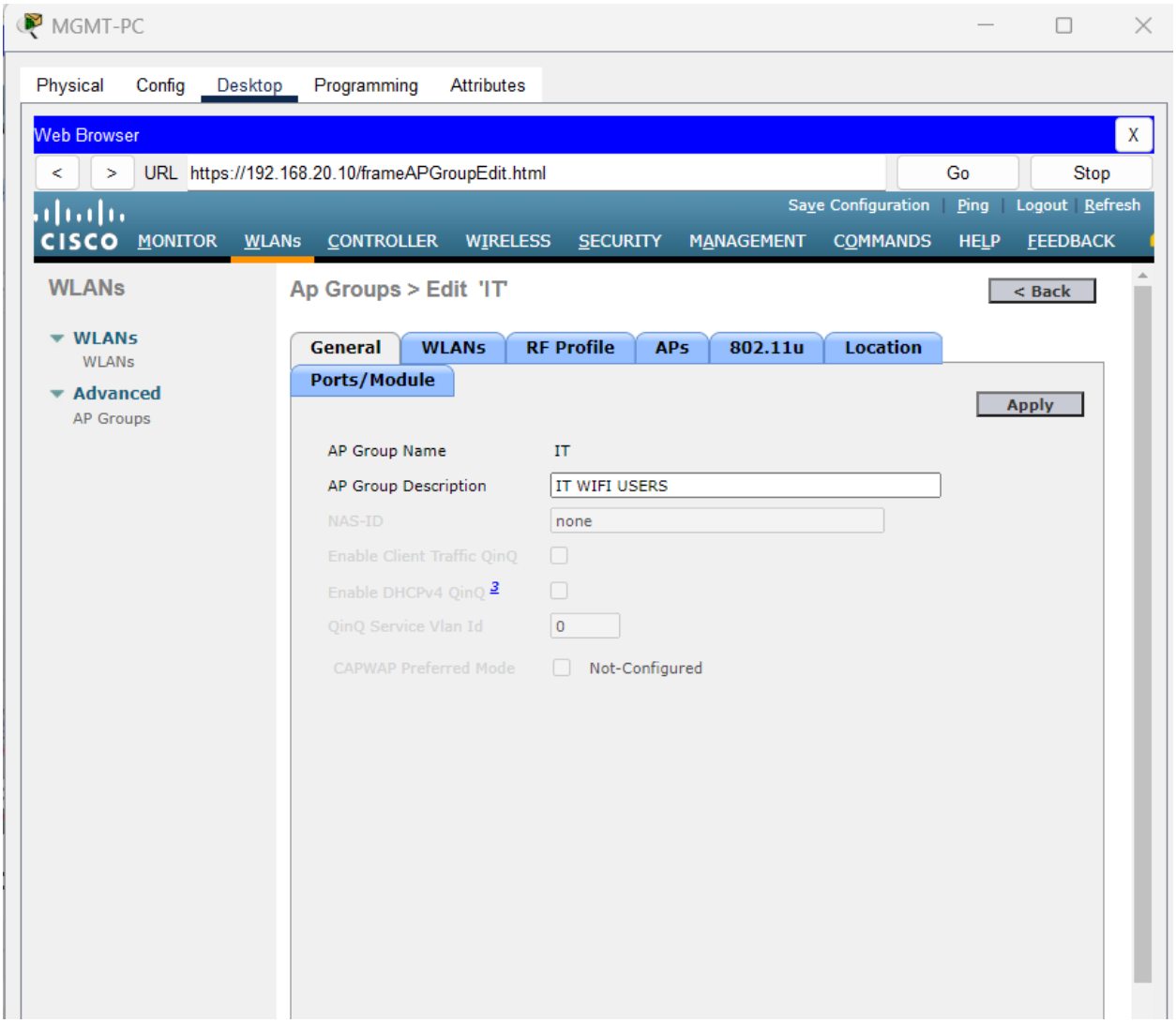
After creating each group enable specific WiFi and access point

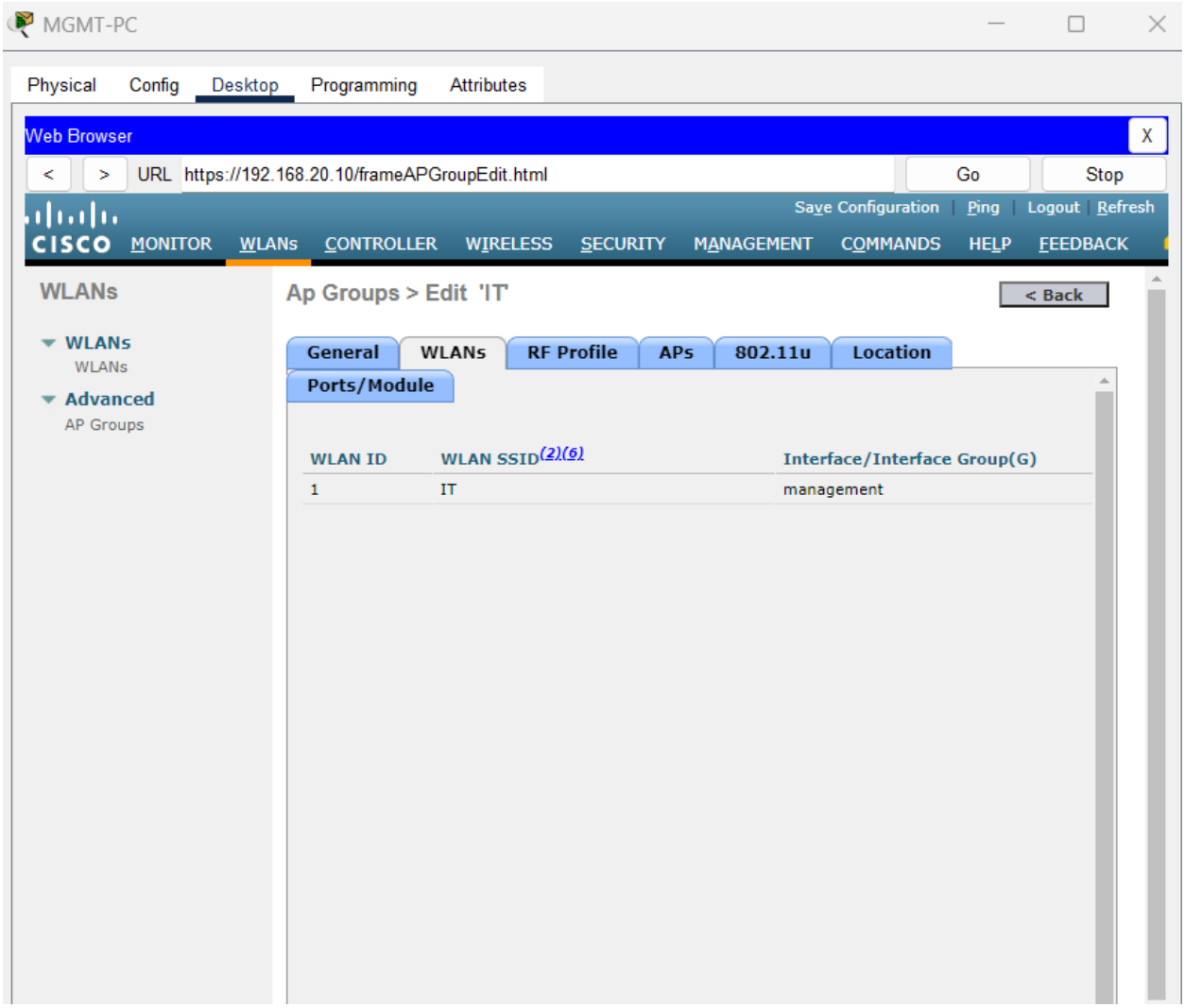


Now on Management PC



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
Save Configuration | Ping | Logout | Refresh
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
IT WIFI USERS
NAS-ID
none
Enable Client Traffic QinQ
Enable DHCPv4 QinQ
QinQ Service Vlan Id
0
CAPWAP Preferred Mode
Not-Configured


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
WLANs
WLANs
Advanced
AP Groups
Ap Groups > Edit 'IT'
< Back
General
WLANs
RF Profile
APs
802.11u
Location
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

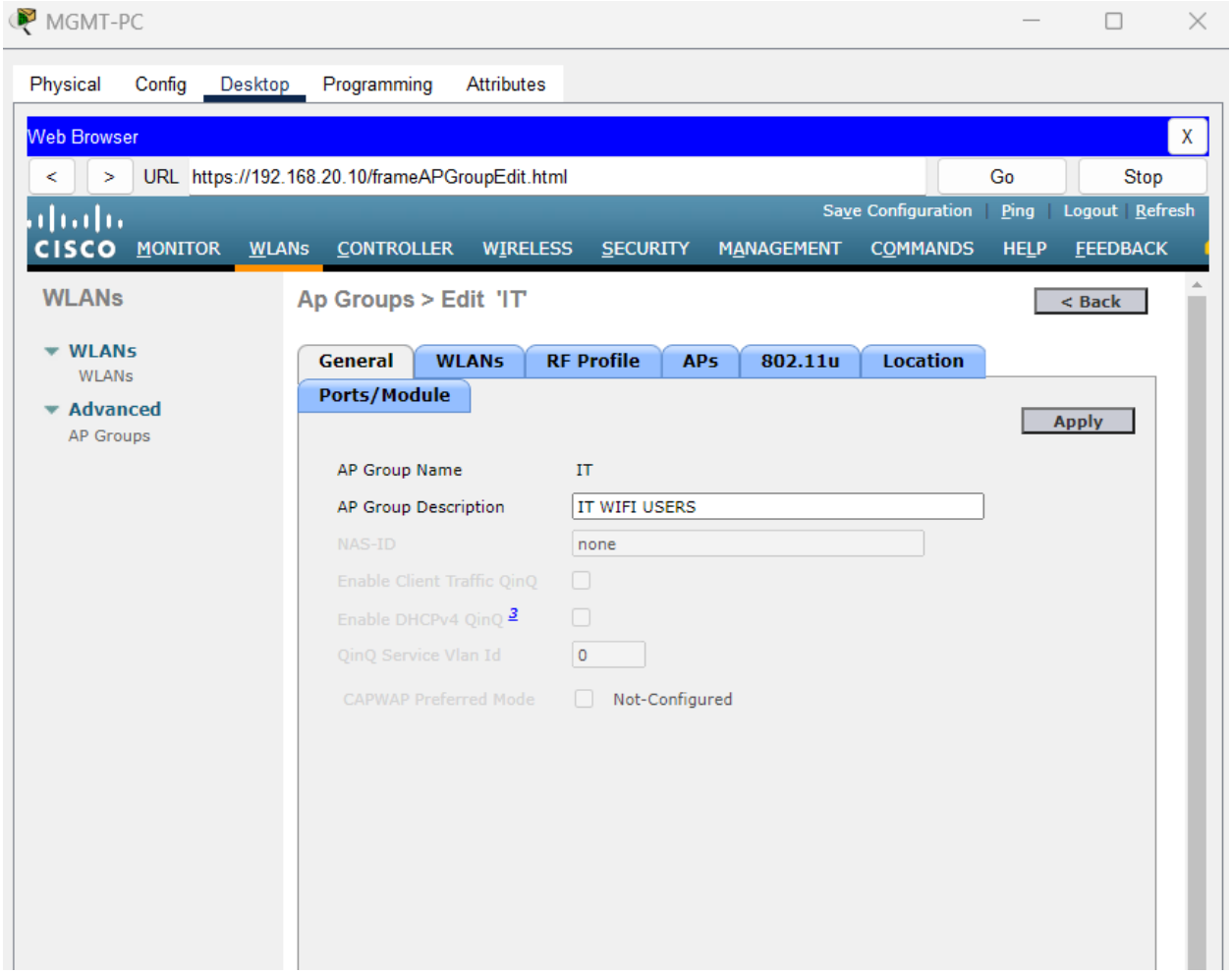
AP Name	Ethernet MAC

Add APs to the Group — Add APs

AP Name	Group Name
GUEST-AP	default-group
HR-AP	default-group
FIN-AP	default-group
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 QinQ should be enabled, to set the DHCPv4 QinQ
4 AP1810W has 3 LAN ports, which are configured through "Ports/Module"
5 OEAP1810 LAN1/LAN2 are configured through "Ports/Module," with RLAN "None" represents local port. LAN3 is always a local port
6 OEAP1810 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
Save Configuration | Ping | Logout | Refresh
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
IT WIFI USERS
NAS-ID
none
Enable Client Traffic QinQ
Enable DHCPv4 QinQ
QinQ Service Vlan Id
0
CAPWAP Preferred Mode
Not-Configured