SULTAN QABOOS UNIVERSITY

COLLEGE OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

COMP4515: Mobile Networks

Assignment 2: Design and Configure a Wireless Local Area Networks

Team Members:

Ahmed Al Senaidi

Ahmed Al Khanbshi

November 15, 2024

Contents

1. Introduction

The purpose of this project is to design and configure a secure and scalable Wireless Local Area Network (WLAN)
for a two-floor company, meeting specific requirements such as VLAN separation, RADIUS-based authentication,
and differentiated access through multiple SSIDs. This document details our assumptions, design approach,
configuration steps, and testing methodology.

2. Assumptions

Building Layout: The network is designed for a two-floor building with departments distributed as follows:

- Floor 2: HR Department
- Floor 1: IT Department
- Ground and floor 1: Lobby (for trainees)

Device Count:

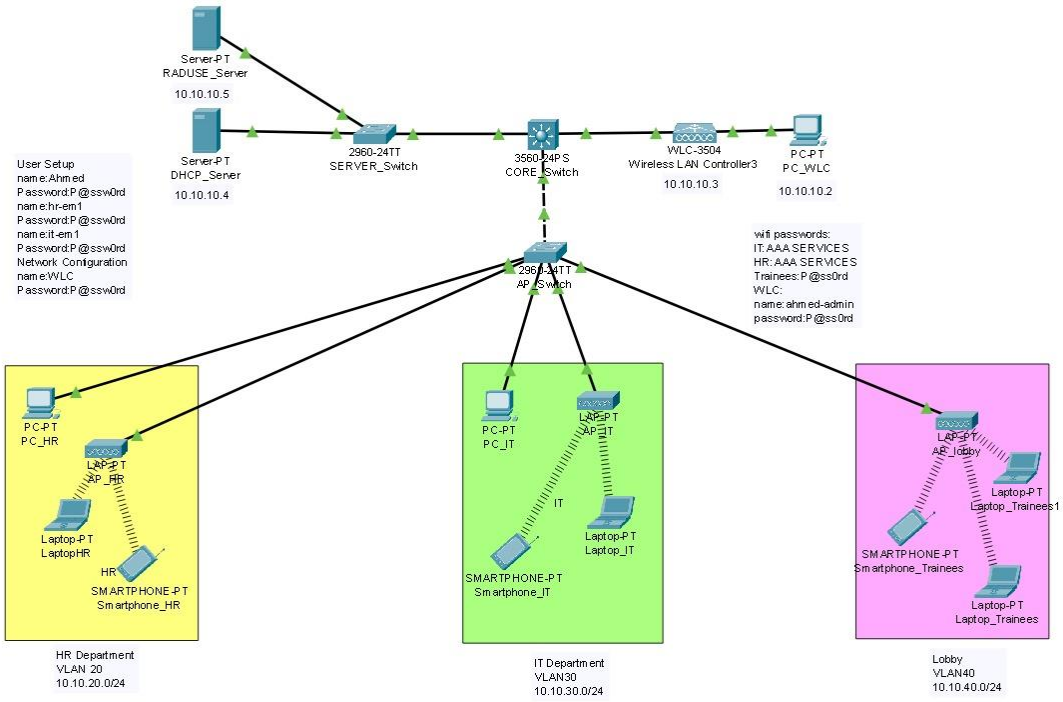
- HR Department: 3 devices (PC, Laptop, Smartphone)
- IT Department: 3 devices (PC, Laptop, Smartphone)
- Lobby (Trainees): 3 devices (2 Laptops, Smartphone)

User Categories and Security Requirements:

- IT Department: VLAN 30, high-security access with RADIUS authentication.
- HR Department: VLAN 20, secure access with RADIUS authentication.
- Trainees (Lobby): VLAN 40, limited access with WPA2-PSK.
- Network Management: VLAN 10 for administrative access to network devices.

```
Switch#show access-lists
Extended IP access list HR_ACL
    10 permit ip 10.10.20.0 0.0.0.255 10.10.20.0 0.0.0.255
    30 deny ip 10.10.20.0 0.0.0.255 10.10.40.0 0.0.0.255 (2 match(es))
    50 permit ip any any (44 match(es))
    60 permit ip 10.10.20.0 0.0.0.255 10.10.30.0 0.0.0.255
Extended IP access list IT_ACL
    10 permit ip 10.10.30.0 0.0.0.255 10.10.30.0 0.0.0.255
    30 deny ip 10.10.30.0 0.0.0.255 10.10.40.0 0.0.0.255 (5 match(es))
    40 permit ip any any (58 match(es))
    50 permit ip 10.10.30.0 0.0.0.255 10.10.20.0 0.0.0.255
Extended IP access list Trainees_ACL
    10 permit ip 10.10.40.0 0.0.0.255 10.10.40.0 0.0.0.255
    20 deny ip 10.10.40.0 0.0.0.255 10.10.20.0 0.0.0.255 (4 match(es))
    30 deny ip 10.10.40.0 0.0.0.255 10.10.30.0 0.0.0.255 (3 match(es))
    40 permit ip any any (72 match(es))

Switch#
```

3. Network Design



3.1 VLANs

Each department and user category is segmented into distinct VLANs to ensure security and manageability.

VLAN ID	Name	IP Subnet	Purpose
10	Management	10.10.10.0/24	Network devices (Native VLAN)
20	HR	10.10.20.0/24	HR Department
30	IT	10.10.30.0/24	IT Department

40	Trainees	10.10.40.0/24	Lobby users

3.2 Connection Types

- AP Switch to Access Points: Trunk links with native VLAN set to VLAN 10 (Management VLAN).
- Core Switch to AP Switch: Trunk links, allowing all VLANs (10, 20, 30, and 40).
- Core Switch to servers Switch: Trunk links, allowing all VLANs (10, 20, 30, and 40).
- Servers Switch to servers (DHCP,RADIUS): Access links VLAN 10.
- Core Switch to WLC: Access links VLAN 10.

- Core Switch to servers: Access links VLAN 10.

4. Device Configuration

4.1 Core Switch (3560-24PS CORE Switch)

The core switch serves as the primary connection point for all VLANs, with trunking configured to allow traffic
across the VLANs.

Core Switch Configuration:
enable

```
configure terminal
# Create VLANs
vlan 10
name Management
vlan 20
name HR
vlan 30
name IT
vlan 40
name Trainees
exit
# Configure VLAN Interfaces with IP addresses
interface Vlan10
 ip address 10.10.10.1 255.255.255.0
 no shutdown
exit
interface Vlan20
 ip address 10.10.20.1 255.255.255.0
 no shutdown
exit
interface Vlan30
 ip address 10.10.30.1 255.255.255.0
 no shutdown
exit
interface Vlan40
 ip address 10.10.40.1 255.255.255.0
 no shutdown
```

```
exit
# Set up trunk ports for VLANs
interface FastEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40
exit
interface FastEthernet0/2
 switchport mode trunk

 switchport trunk allowed vlan 10,20,30,40
exit

interface FastEthernet0/3 #To WLC
switchport mode access

switchport access vlan 10
exit
```

4.2 Access Point (AP) Switch

The AP switch connects to access points and the core switch with trunk ports. Ports connected to APs have native VLAN 10 (for management) and allow traffic from all user VLANs.

```
enable

configure terminal

# Create VLANs

 vlan 10
```

```
name Management
vlan 20
name HR
vlan 30
name IT
vlan 40
name Trainees
exit

# Assign VLANs to ports connected to access points
# Set trunk with native VLAN 10 to allow AP management
interface range FastEthernet0/1 - 4
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk allowed vlan 10,20,30,40
exit

# Set up trunk to connect AP Switch to Core Switch
interface GigabitEthernet0/1
```

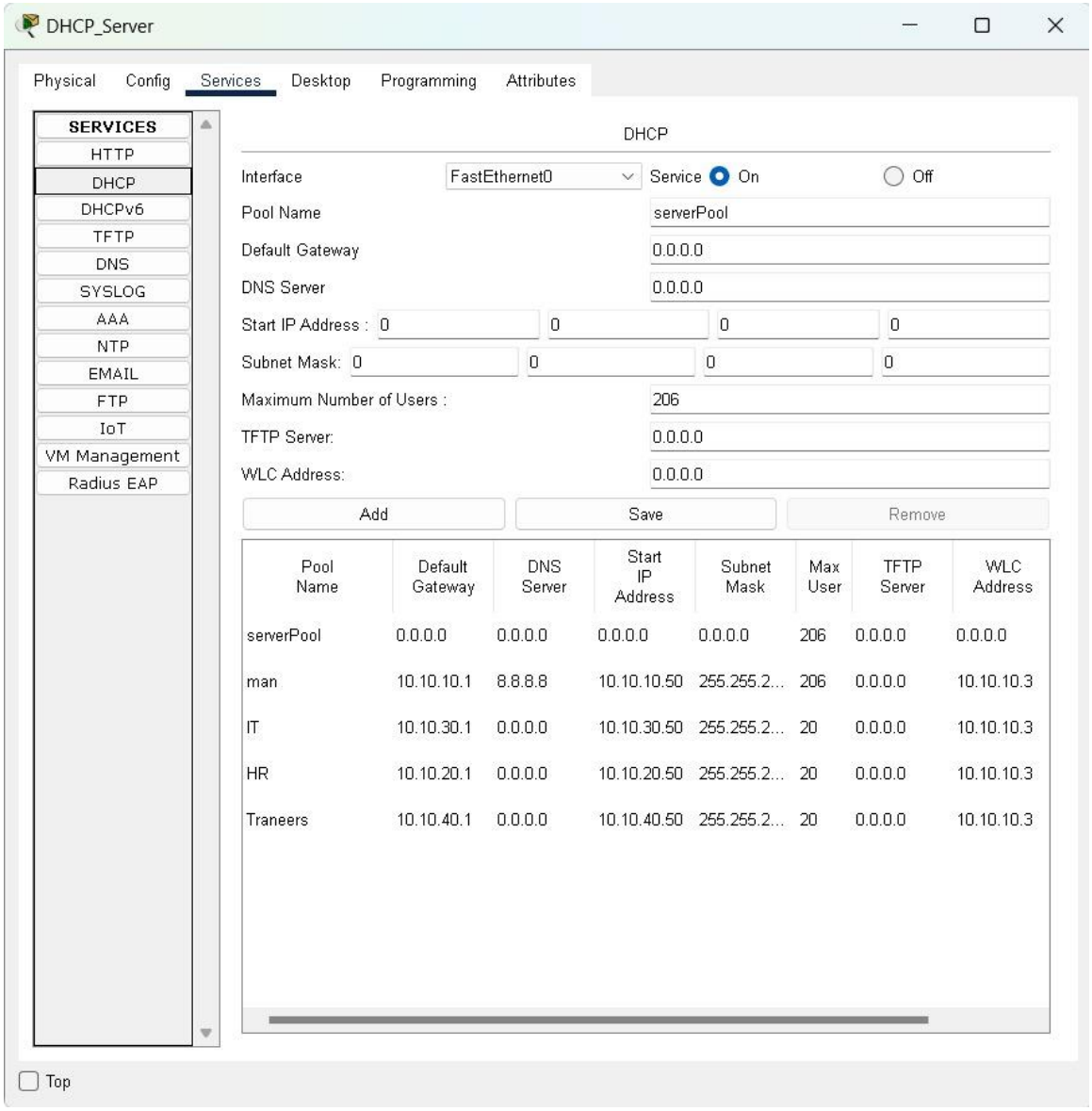
```
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40
exit

# Access ports for HR Department (VLAN 20) - Ports FastEthernet0/6 to 10
interface range FastEthernet0/6 - 10
 switchport mode access
 switchport access vlan 20
exit

# Access ports for IT Department (VLAN 30) - Ports FastEthernet0/11 to 15
interface range FastEthernet0/11 - 15
 switchport mode access
 switchport access vlan 30
exit
```

4.3 Server Switch Configuration (Connecting Core Switch to DHCP and RADIUS Servers)

```
enable

configure terminal


# Create VLANs for server access

vlan 10

name Management

vlan 20

name HR

vlan 30

name IT

vlan 40

name Trainees

exit

# Trunk connection to the Core Switch on GigabitEthernet0/1

interface GigabitEthernet0/1

 switchport mode trunk

 switchport trunk allowed vlan 10,20,30,40
```

```
exit
# Assigning each server to the appropriate VLAN
# DHCP Server - Management VLAN 10
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10
exit
# RADIUS Server - Management VLAN 10
interface FastEthernet0/2
 switchport mode access
 switchport access vlan 10
exit
```

4.4 DHCP server



4.5 RADIUS server

Radius port 1812

User Setup

name:Ahmed

Password:P@ssw0rd

name:hr-em1

Password:P@ssw0rd

name:it-em1

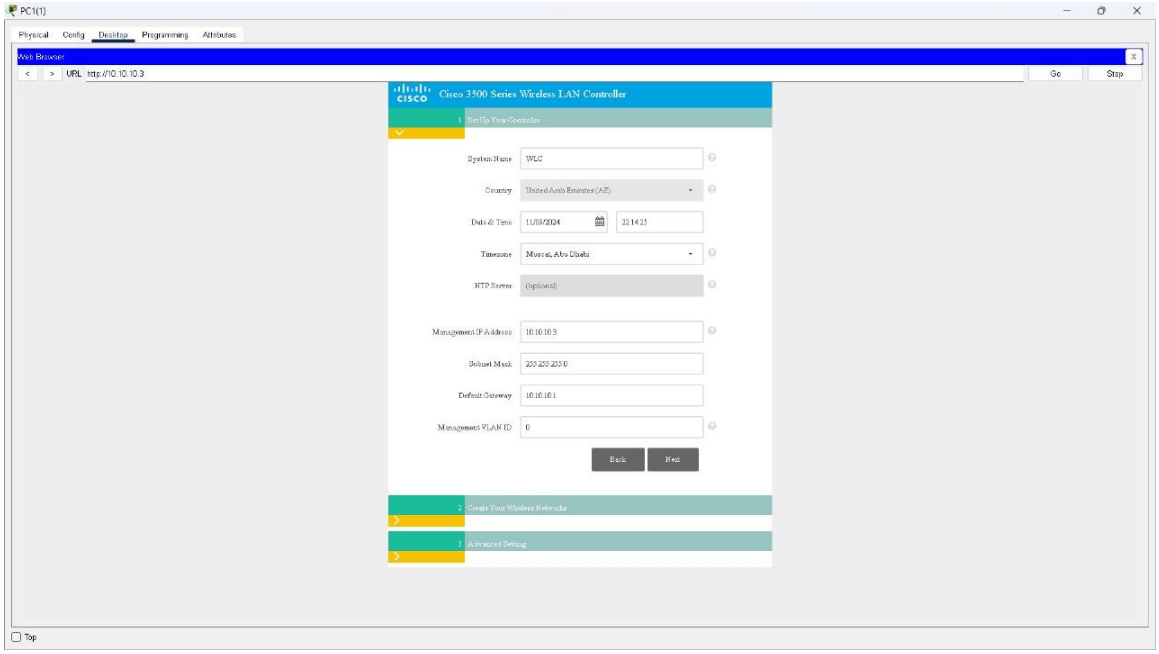
Password:P@ssw0rd

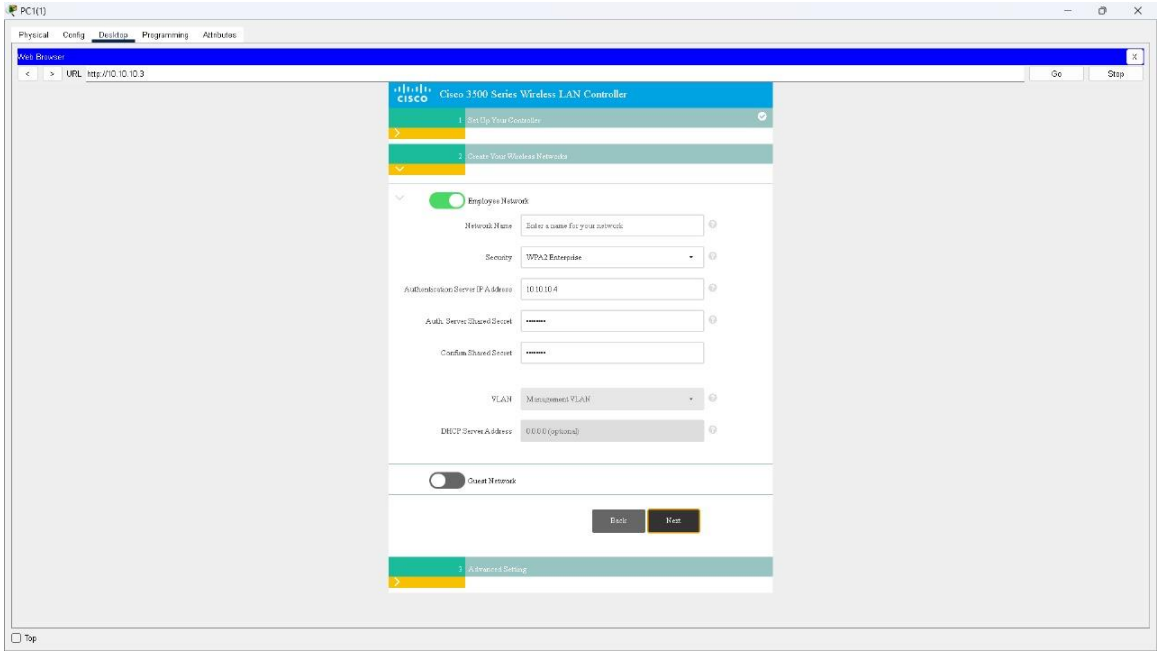
Network Configuration

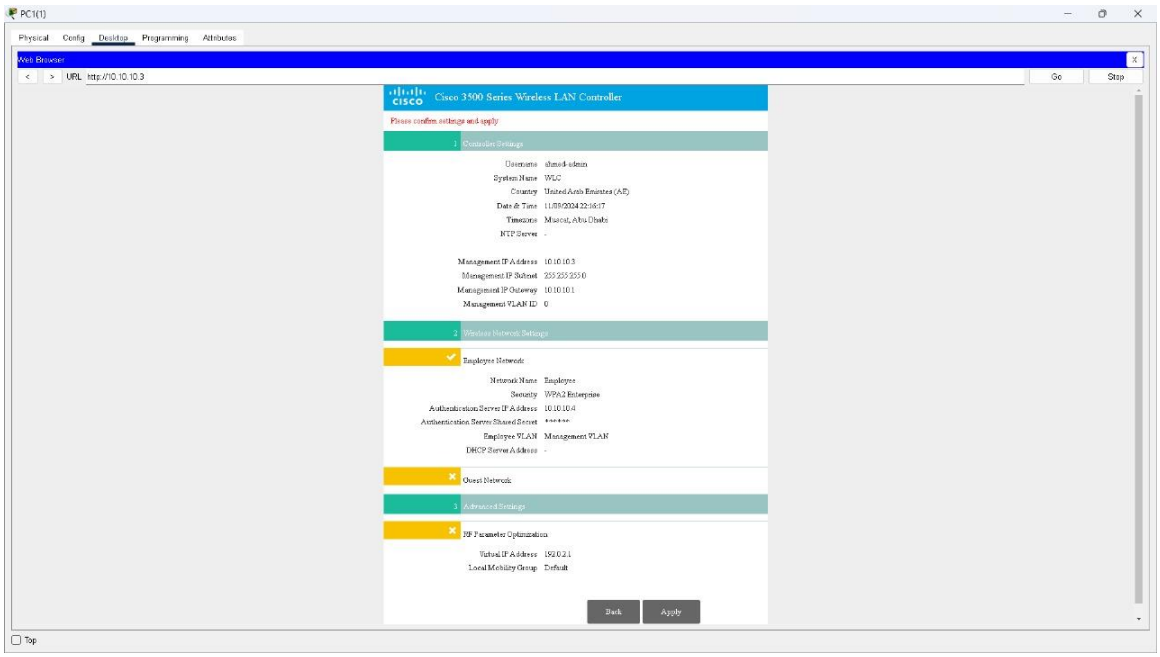
name:WLC

Password:P@ssw0rd

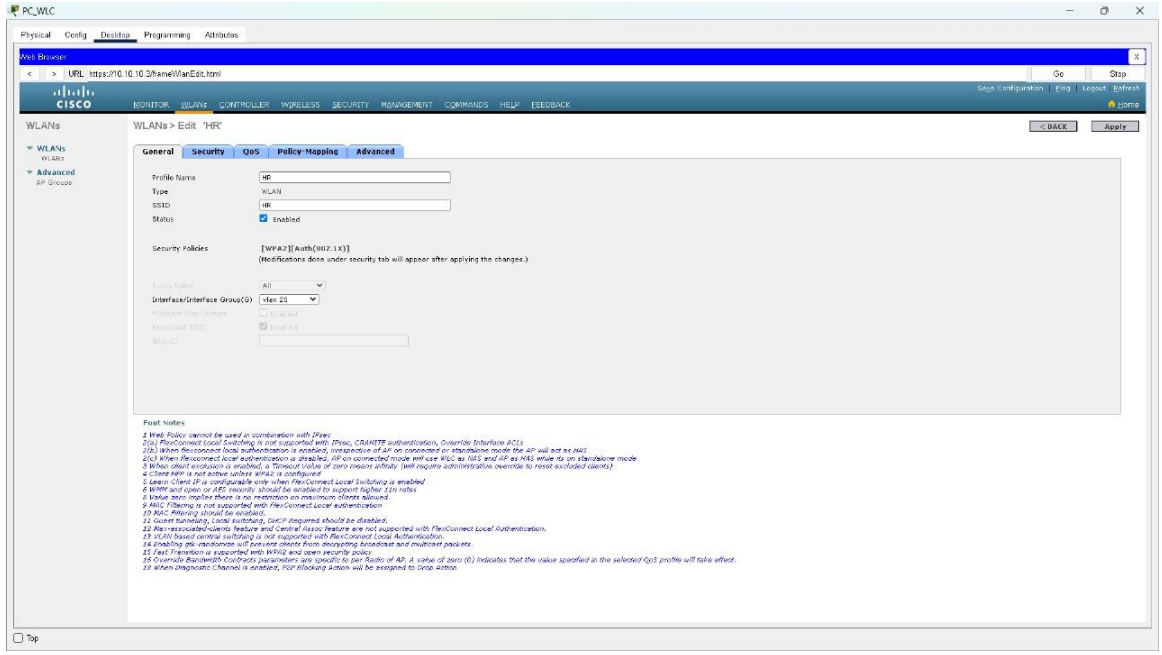
4.6 WLC

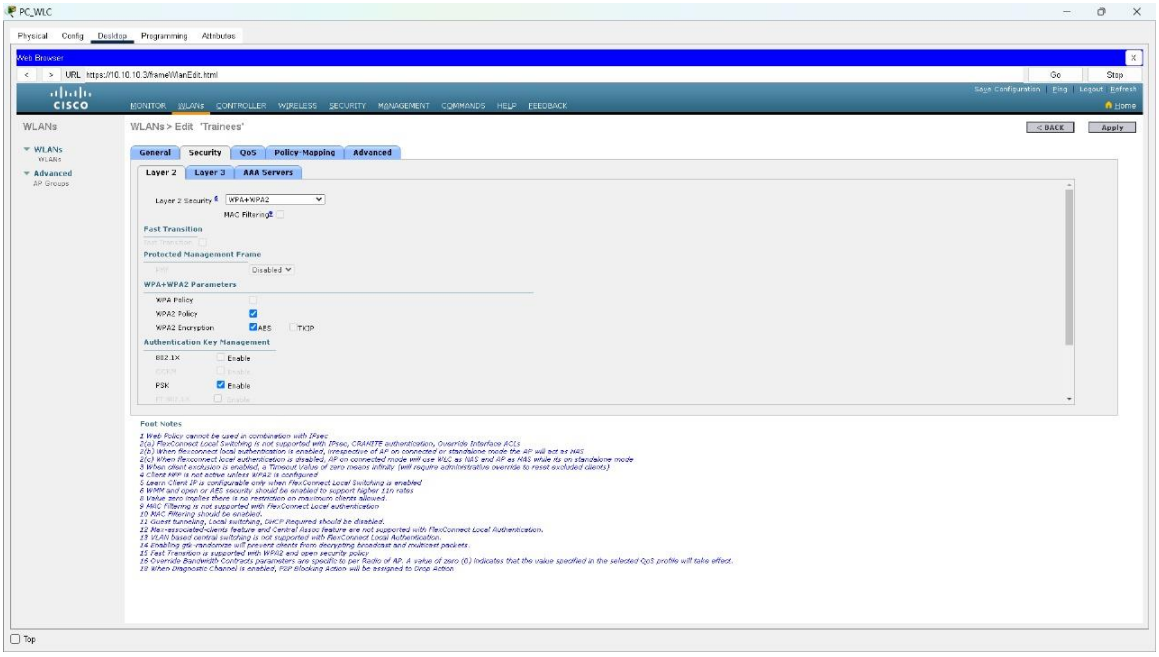

PC1(1)
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL http://10.10.10.3
Go
Stop
Cisco 3500 Series Wireless LAN Controller
1 Set Up Your Controller
System Name WLC
Country United Arab Emirates (AE)
Date & Time 11/09/2024 22:14:25
Timezone Muscat, Abu Dhabi
NTP Server (optional)
Management IP Address 10.10.10.3
Subnet Mask 255.255.255.0
Default Gateway 10.10.10.1
Management VLAN ID 0
Back
Next
2 Create Your Wireless Networks
3 Advanced Setting
Top

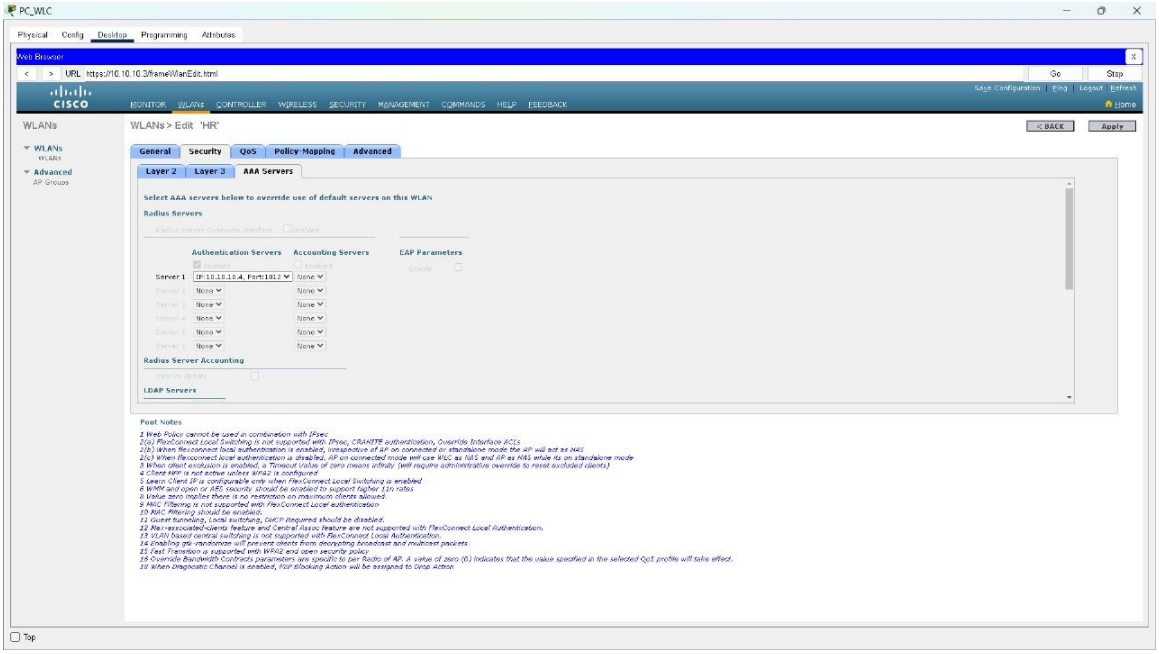

PC1(1)
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL http://10.10.10.3
Go
Stop
Cisco 3500 Series Wireless LAN Controller
1 Set Up Your Controller
2 Create Your Wireless Networks
Employee Network
Network Name Enter a name for your network
Security WPA2 Enterprise
Authentication Server IP Address 10.10.10.4
Auth. Server Shared Secret
Confirm Shared Secret
VLAN Management VLAN
DHCP Server Address 0.0.0.0 (optional)
Guest Network
Back
Next
3 Advanced Setting
Top


PC1(1)
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL http://10.10.10.3
Go
Stop
Cisco 3500 Series Wireless LAN Controller
Please confirm settings and apply
1 Controller Settings
Username ahmed-admin
System Name WLC
Country United Arab Emirates (AE)
Date & Time 11/09/2024 22:16:17
Timezone Muscat, Abu Dhabi
NTP Server -
Management IP Address 10.10.10.3
Management IP Subnet 255.255.255.0
Management IP Gateway 10.10.10.1
Management VLAN ID 0
2 Wireless Network Settings
Employee Network
Network Name Employee
Security WPA2 Enterprise
Authentication Server IP Address 10.10.10.4
Authentication Server Shared Secret ******
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
Top

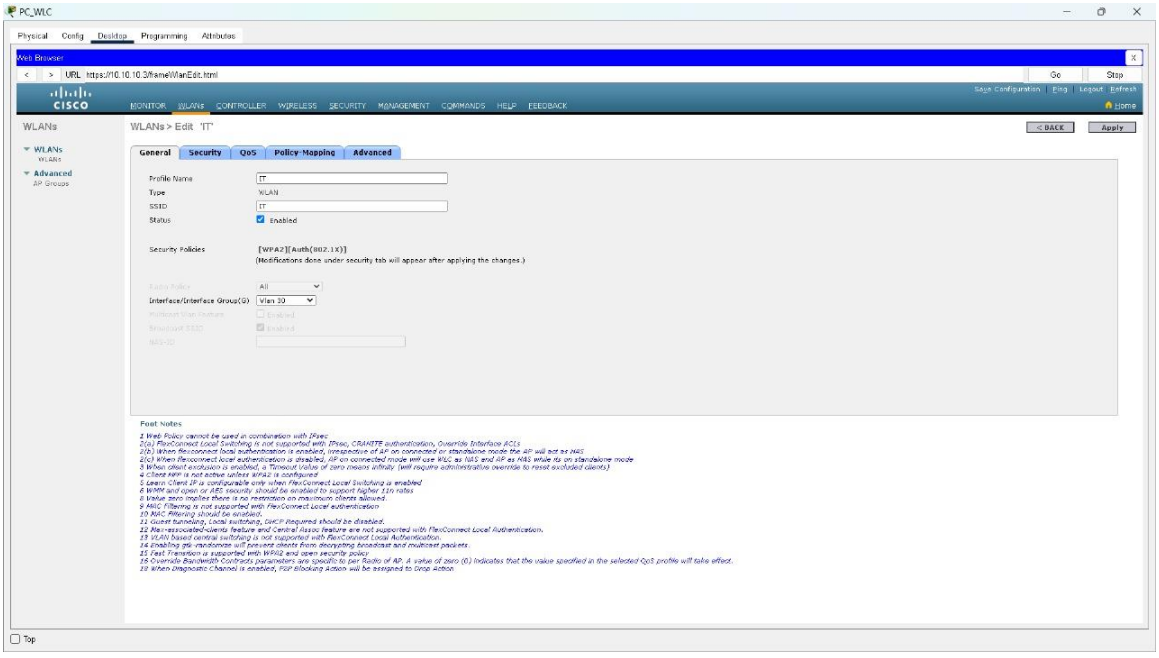
HR

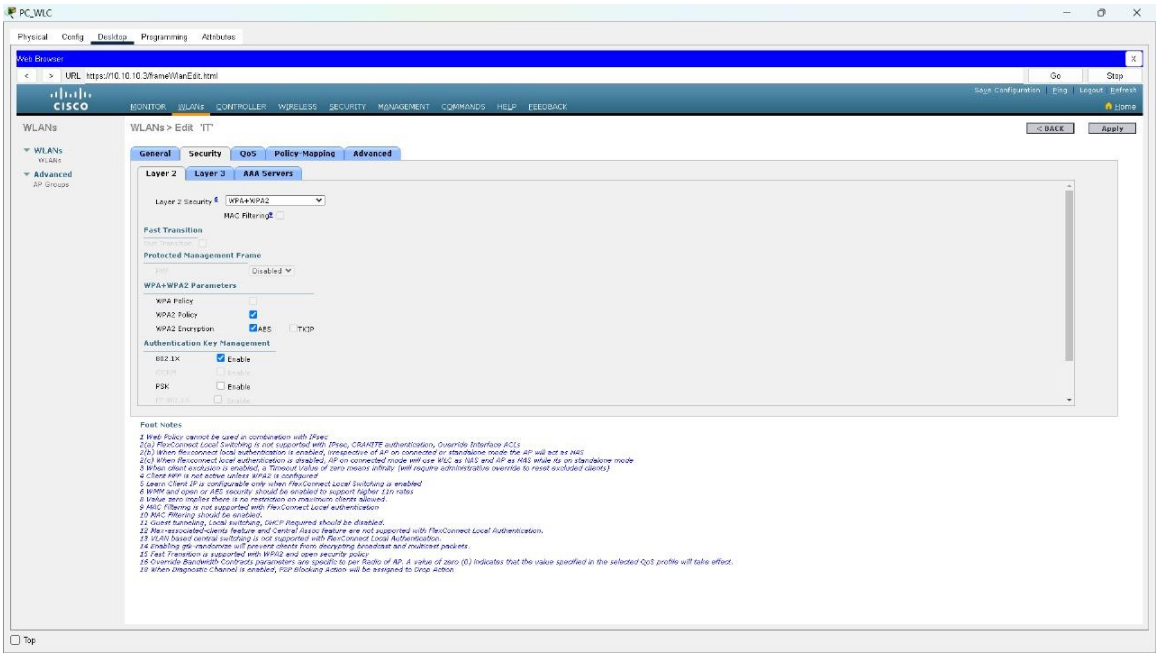

PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameWlanEdit.html
Go
Stop
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs > Edit 'HR'
< BACK
Apply
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
HR
Type
WLAN
SSID
HR
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Interface/Interface Group(G)
vlan 20
Foot Notes
Top

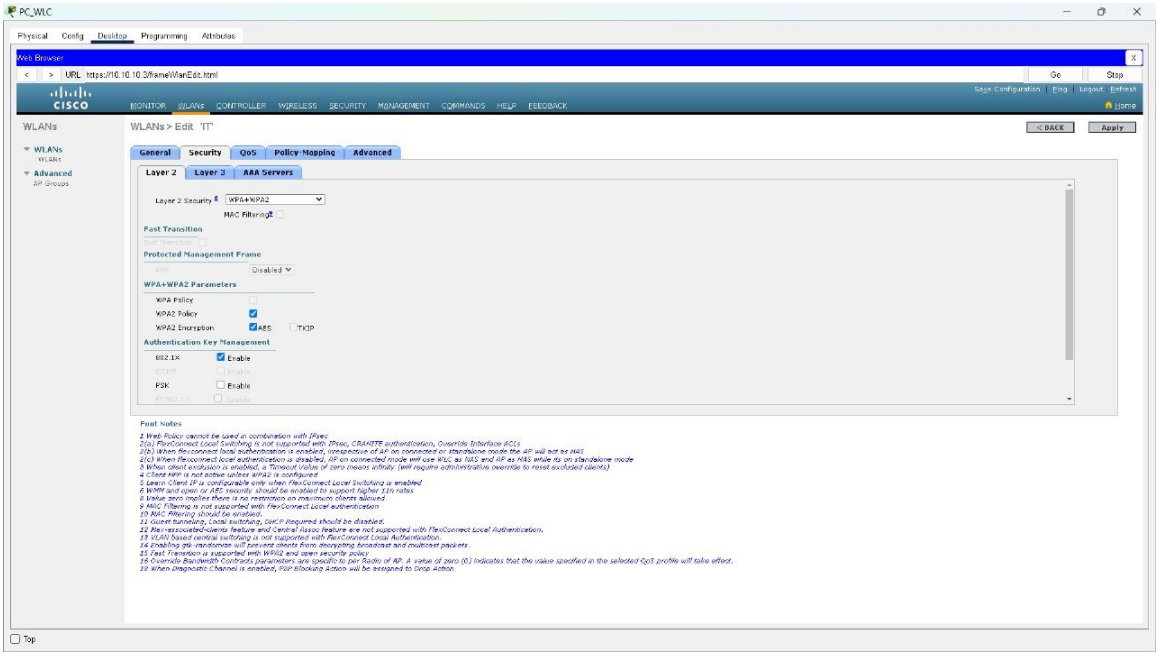

PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameWlanEdit.html
Go
Stop
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs > Edit 'Trainees'
< BACK
Apply
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Protected Management Frame
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Authentication Key Management
802.1X
Enable
PSK
Enable
Foot Notes
Top


PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameWlanEdit.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs > Edit 'HR'
< BACK
Apply
WLANs
WLANs
Advanced
AP Groups
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Select AAA servers below to override use of default servers on this WLAN
Radius Servers
Authentication Servers
Accounting Servers
EAP Parameters
Enabled
Server 1
IP:10.10.10.4, Port:1812
None
Radius Server Accounting
Interim Update
LDAP Servers
Post 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 g96 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, FQF Blocking Action will be assigned to Drop Action
Top

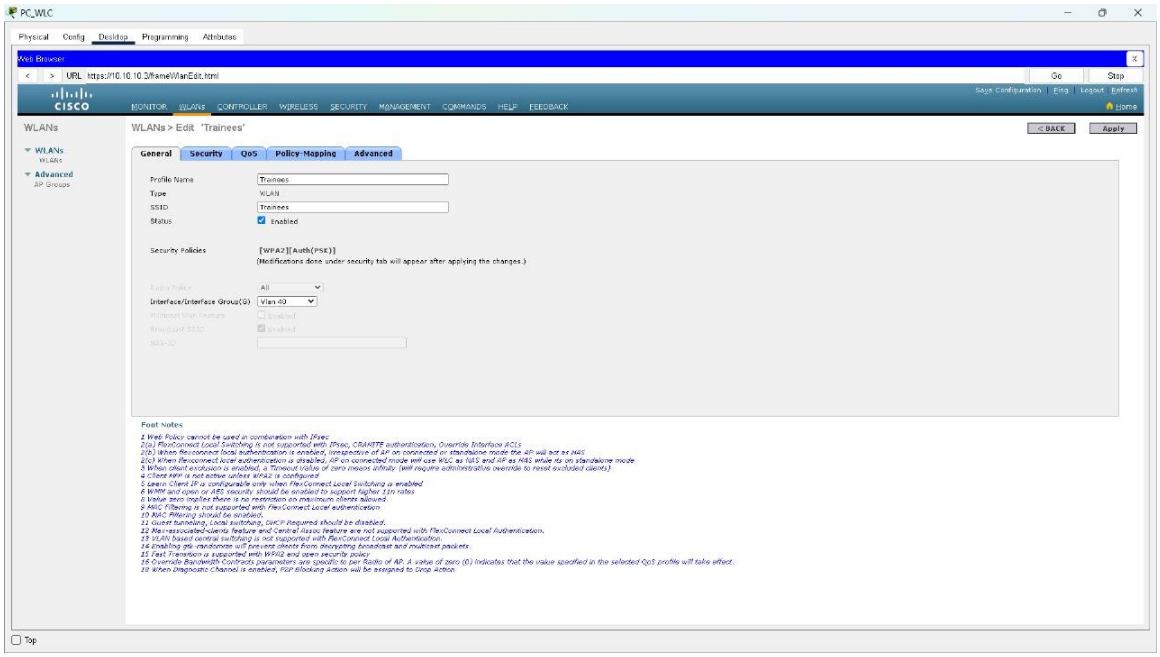
IT

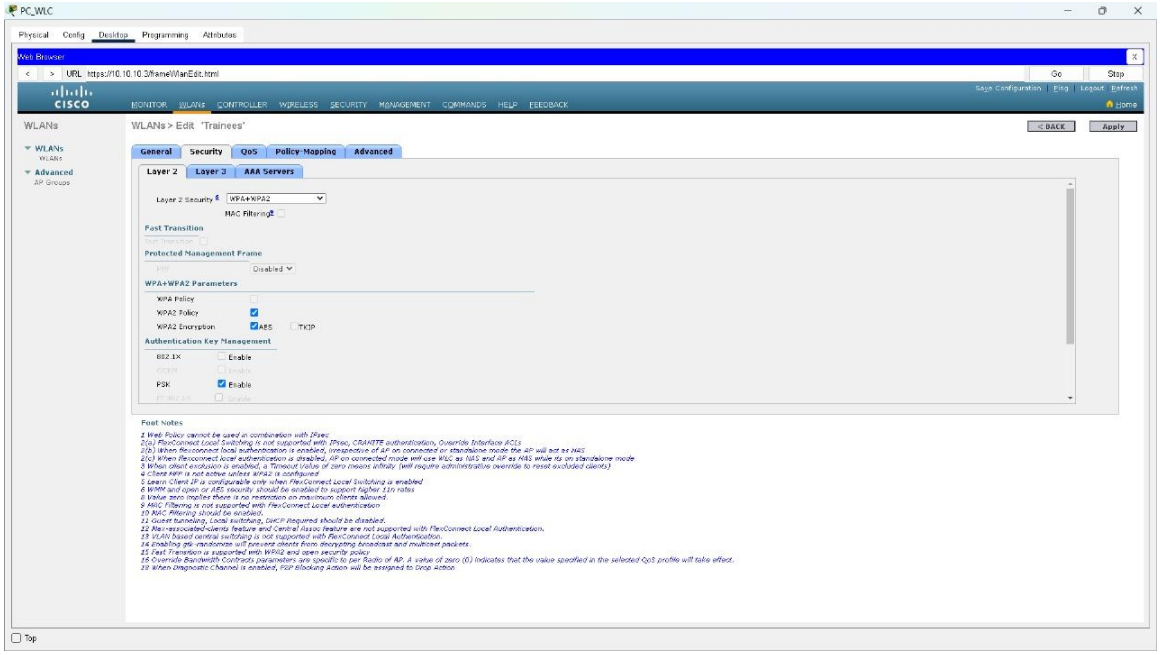

PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameWlanEdit.html
Go
Stop
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs > Edit 'IT'
< BACK
Apply
WLANs
WLANs
Advanced
AP Groups
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
IT
Type
WLAN
SSID
IT
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Interface/Interface Group(G)
Vlan 30
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 Mac-associated-clients feature and Central Assoc feature are not supported with FlexConnect Local Authentication.
13 WLAN based central switching is not supported with FlexConnect Local Authentication.
14 Enabling pbb 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
Top

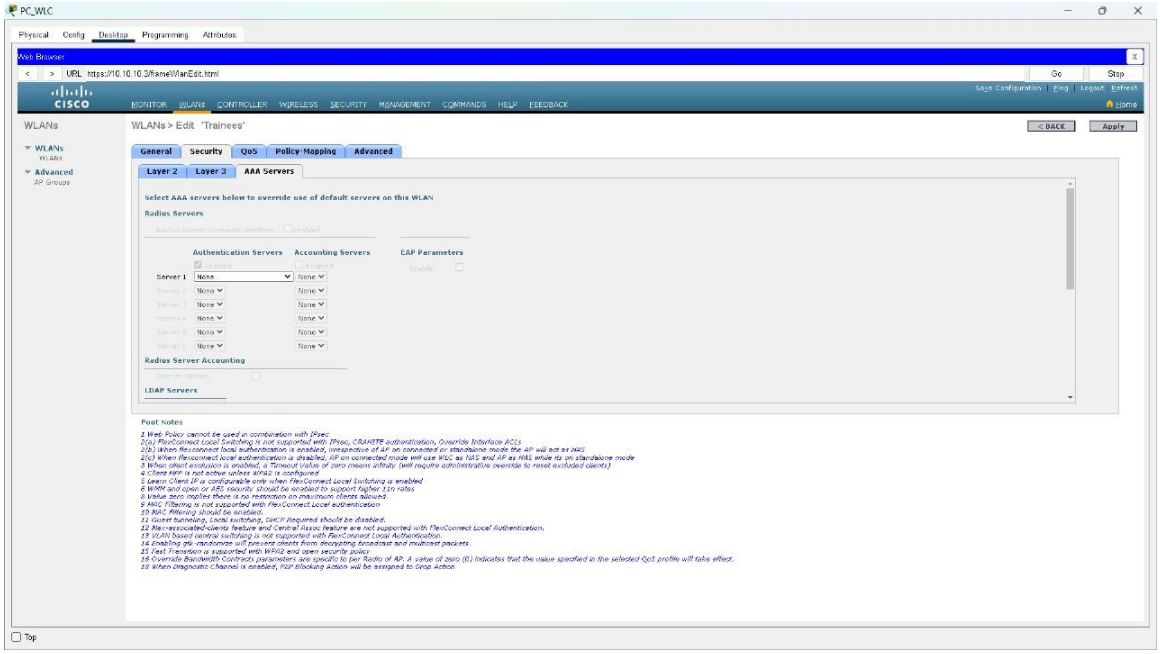

PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameWlanEdit.html
Go
Stop
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
Home
WLANs
WLANs > Edit 'IT'
< BACK
Apply
WLANs
WLANs
Advanced
AP Groups
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Protected Management Frame
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Authentication Key Management
802.1X
Enable
PSK
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)
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 Mac-associated-clients feature and Central Assoc feature are not supported with FlexConnect Local Authentication.
13 WLAN based central switching is not supported with FlexConnect Local Authentication.
14 Enabling pbb 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
Top


PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL: https://10.10.10.3/frameWlanEdit.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
WLANs
Advanced
AP Groups
WLANs > Edit 'IT'
< BACK
Apply
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Protected Management Frame
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Authentication Key Management
802.1X
Enable
PSK
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)
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 pmf -mandatory 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, PSP Blocking Action will be assigned to Drop Action
Top

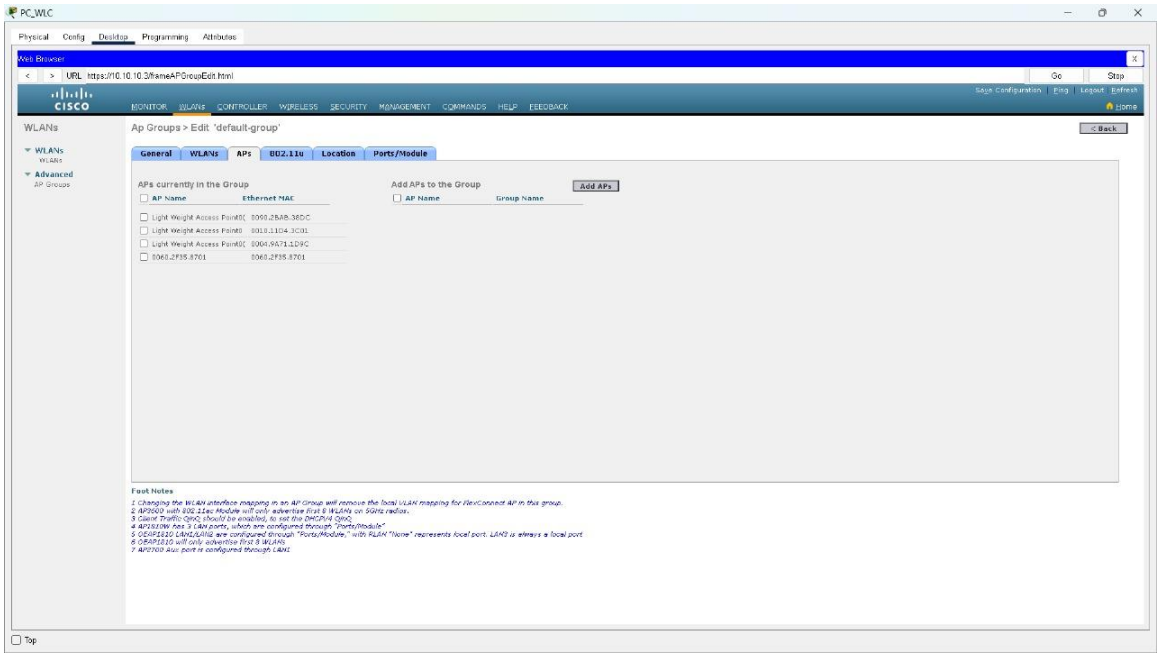
Trainees


PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameWlanEdit.html
Go
Stop
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration
Ping
Logout
Refresh
Home
WLANs
WLANs > Edit 'Trainees'
< BACK
Apply
General
Security
QoS
Policy Mapping
Advanced
Profile Name
Trainees
Type
WLAN
SSID
Trainees
Status
Enabled
Security Policies
[WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)
Interface/Interface Group(G)
Vlan 40
Foot Notes
Top

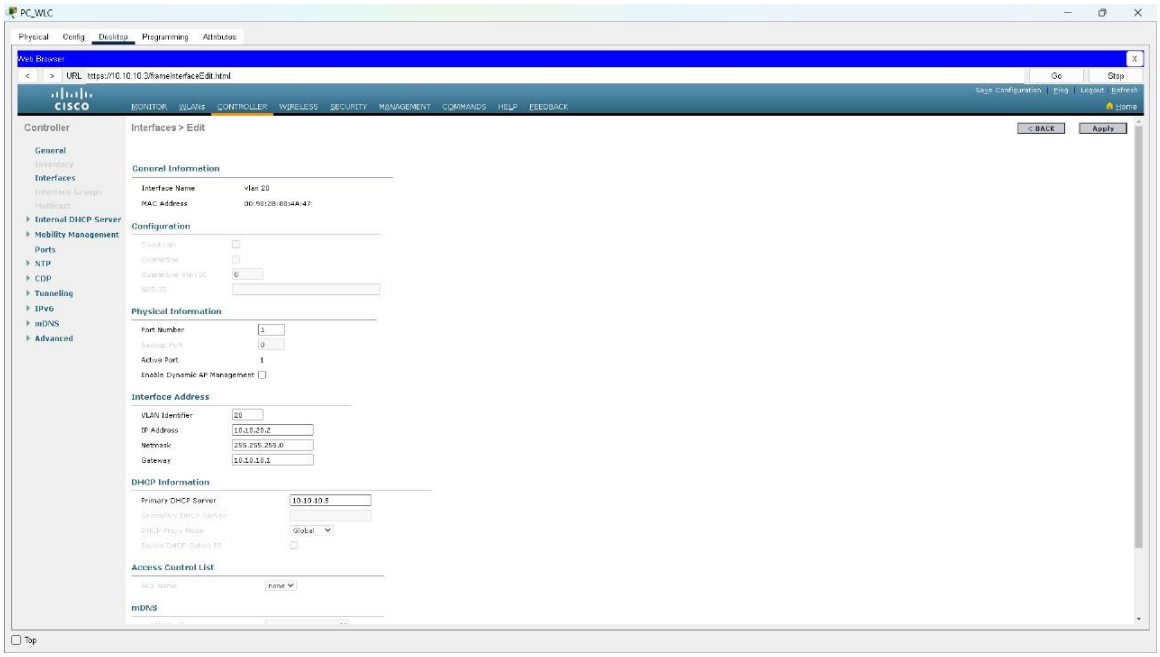

PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameWlanEdit.html
Go
Stop
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration
Ping
Logout
Refresh
Home
WLANs
WLANs > Edit 'Trainees'
< BACK
Apply
General
Security
QoS
Policy Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Protected Management Frame
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Authentication Key Management
802.1X
Enable
PSK
Enable
Foot Notes
Top

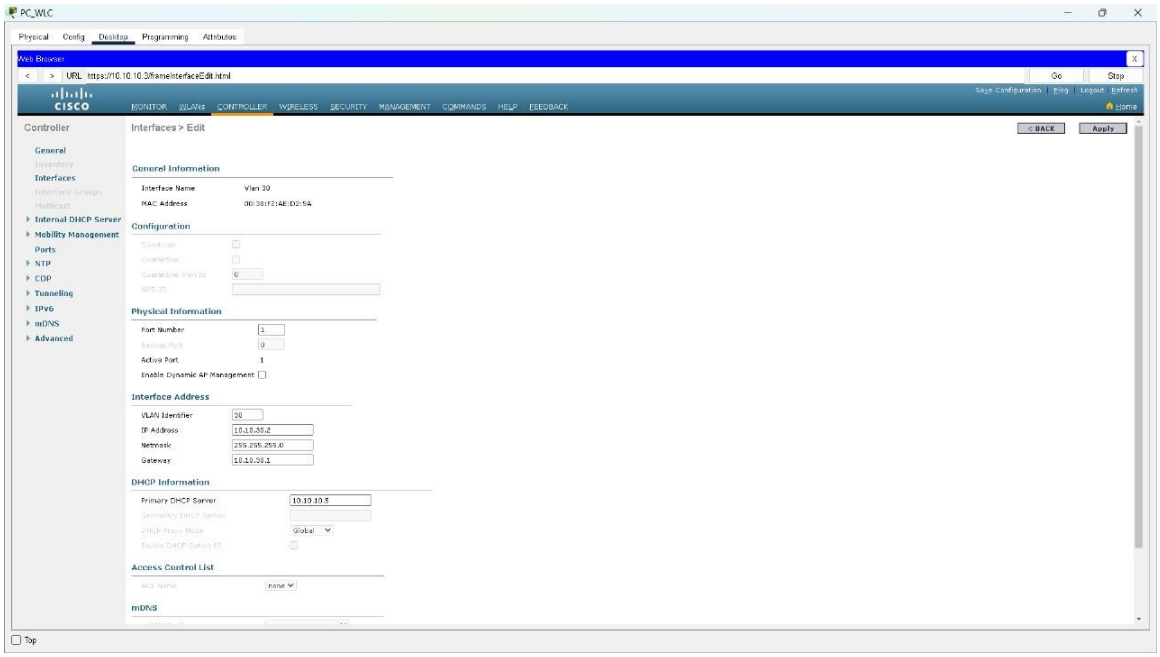

PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameWlanEdit.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs > Edit 'Trainees'
< BACK
Apply
WLANs
WLANs
Advanced
AP Groups
General
Security
QoS
Policy Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Select AAA servers below to override use of default servers on this WLAN
Radius Servers
Authentication Servers
Accounting Servers
EAP Parameters
Enabled
Server 1
None
Radius Server Accounting
LDAP Servers
Post 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 g86 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, Rap Blocking Action will be assigned to Drop Action
Top

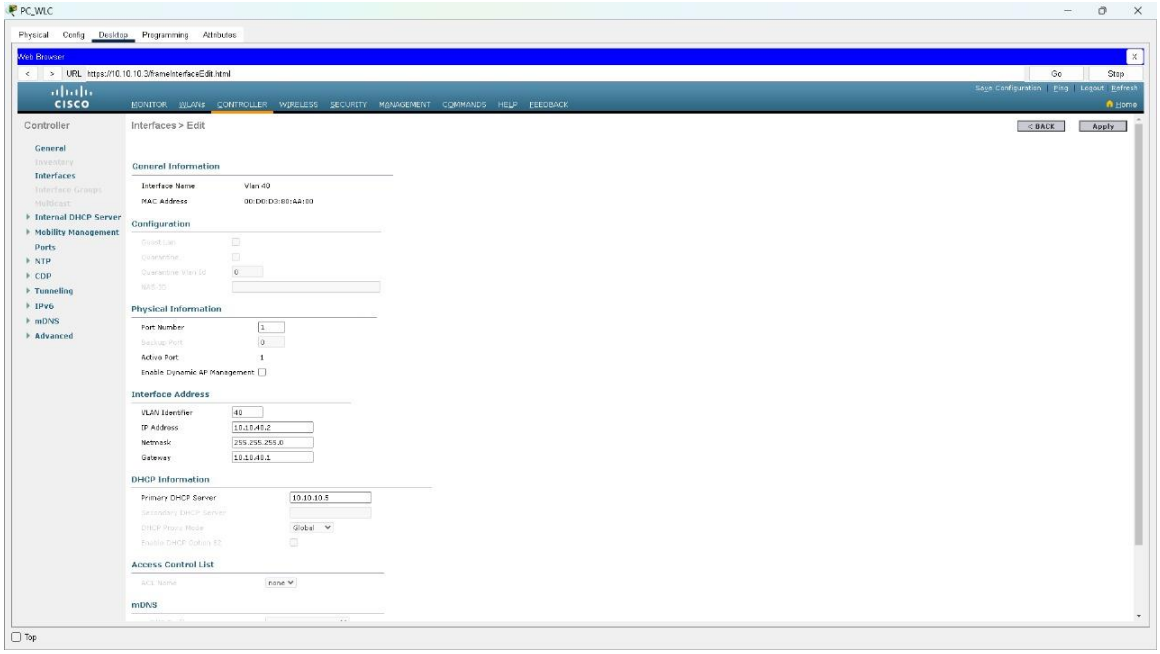
Group:


PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.2/frameAPGroupEdit.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
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
Light Weight Access Point0(0060.2EAB.36DC
Light Weight Access Point0 0010.1104.3C01
Light Weight Access Point0(0004.9A71.1D9C
0060.2F35.8701 0060.2F35.8701
Add APs to the Group
Add APs
AP Name
Group Name
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 not the SVP/M QinQ.
4 AP1810W has 3 LAN ports, which are configured through "Ports/Module".
5 OEAP1810 LAN1/LAN2 are configured through "Ports/Module," with VLAN "None" represents local port. LAN3 is always a local port.
6 OEAP1810 will only advertise first 8 WLANs
7 AP1700 Aux port is configured through LAN1
Top

Interfaces:


PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameInterfaceEdit.html
Go
Stop
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Tunneling
IPv6
mDNS
Advanced
Interfaces > Edit
< BACK
Apply
General Information
Interface Name vlan 20
MAC Address 00:90:2B:B0:AA:47
Configuration
Physical Information
Port Number 1
Backup Port 0
Active Port 1
Enable Dynamic AP Management
Interface Address
VLAN Identifier 20
IP Address 10.10.20.2
Netmask 255.255.255.0
Gateway 10.10.10.1
DHCP Information
Primary DHCP Server 10.10.10.5
Secondary DHCP Server
DHCP Proxy Mode Global
Enable DHCP Option 82
Access Control List
ACL Name none
mDNS
Top


PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameInterfaceEdit.html
Go
Stop
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration Ping Logout Refresh
Home
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Tunneling
IPv6
mDNS
Advanced
Interfaces > Edit
< BACK
Apply
General Information
Interface Name Vlan 30
MAC Address 00:E0:F7:AE:D2:5A
Configuration
Physical Information
Port Number 1
Backup Port 0
Active Port 1
Enable Dynamic AP Management
Interface Address
VLAN Identifier 30
IP Address 10.10.30.2
Netmask 255.255.255.0
Gateway 10.10.30.1
DHCP Information
Primary DHCP Server 10.10.10.5
Secondary DHCP Server
DHCP Proxy Mode Global
Enable DHCP Option 82
Access Control List
ACL Name none
mDNS
Top


PC_WLC
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://10.10.10.3/frameInterfaceEdit.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Tunneling
IPv6
mDNS
Advanced
Interfaces > Edit
< BACK
Apply
General Information
Interface Name
Vlan 40
MAC Address
00:D0:D3:88:AA:80
Configuration
Guest Lan
Quarantine
Quarantine Vlan Id
0
NAS-ID
Physical Information
Port Number
1
Backup Port
0
Active Port
1
Enable Dynamic AP Management
Interface Address
VLAN Identifier
40
IP Address
10.10.40.2
Netmask
255.255.255.0
Gateway
10.10.40.1
DHCP Information
Primary DHCP Server
10.10.10.5
Secondary DHCP Server
DHCP Proxy Mode
Global
Enable DHCP Option 82
Access Control List
ACL Name
none
mDNS
Top