



**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 .....	3
2. Assumptions .....	3
3. Network Design .....	5
3.1 VLANs.....	5
3.2 Connection Types .....	6
4. Device Configuration .....	6
4.1 Core Switch (3560-24PS CORE Switch) .....	6
4.2 Access Point (AP) Switch (2960 IOS15).....	8
4.3 Server Switch Configuration (Connecting Core Switch to DHCP and RADIUS Servers) .....	11
4.4 DHCP server .....	13
4.5 RADIUS server.....	13
4.6 WLC .....	15
HR .....	17
IT .....	19
Trainees.....	21
Group: .....	23
Interfaces: .....	24

# 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)

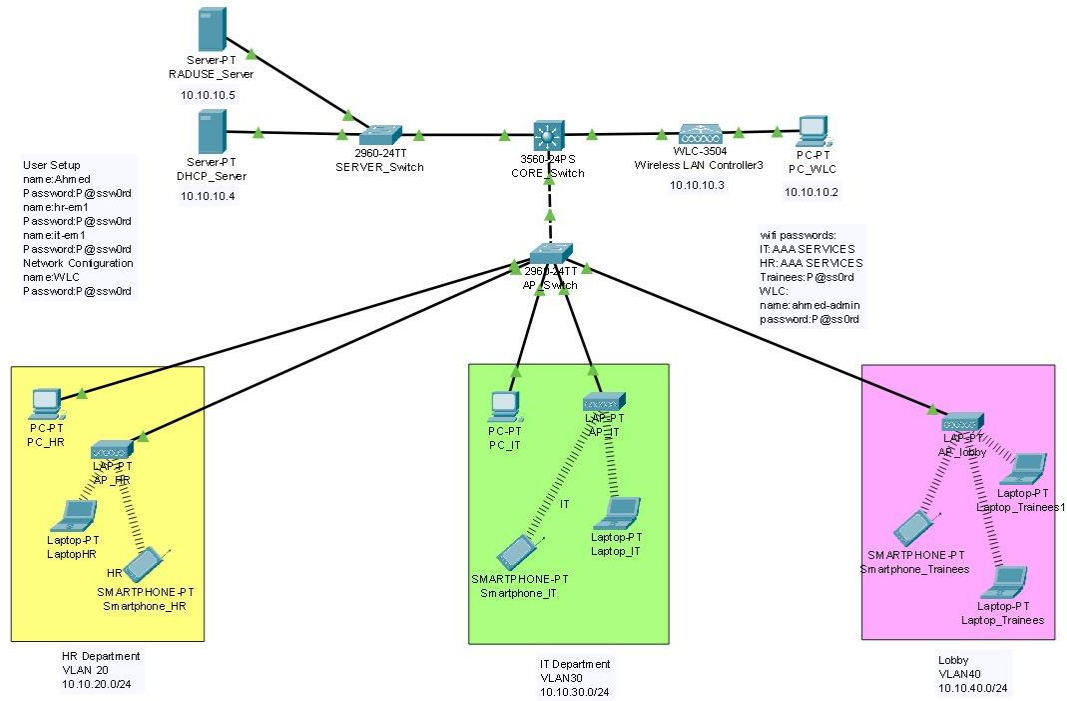
## User Categories and Security Requirements:

- 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

The screenshot shows the 'DHCP\_Server' configuration window. The 'Services' tab is selected, and the 'DHCP' service is highlighted in the left sidebar. The main configuration area is titled 'DHCP' and includes the following fields:

- Interface: FastEthernet0
- Service: ☒ On ☐ Off
- Pool Name: serverPool
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0
- Start IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Maximum Number of Users: 206
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

Below these fields are three buttons: 'Add', 'Save', and 'Remove'. A table below these buttons lists the configured DHCP pools:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	206	0.0.0.0	0.0.0.0
man	10.10.10.1	8.8.8.8	10.10.10.50	255.255.2...	206	0.0.0.0	10.10.10.3
IT	10.10.30.1	0.0.0.0	10.10.30.50	255.255.2...	20	0.0.0.0	10.10.10.3
HR	10.10.20.1	0.0.0.0	10.10.20.50	255.255.2...	20	0.0.0.0	10.10.10.3
Traneers	10.10.40.1	0.0.0.0	10.10.40.50	255.255.2...	20	0.0.0.0	10.10.10.3

At the bottom left of the window, there is a 'Top' button.

## 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 3400 Series Wireless LAN Controller

1. Set Up Your Controller

System Name: WLC

Country: United Arab Emirates (AE)

Date & Time: 11/09/2024 22:14:35

Timezone: Muscat, Abu Dhabi

NTP Server: (optional)

Management IP Address: 10.10.10.3

Default Mask: 255.255.255.0

Default Gateway: 10.10.10.1

Management VLAN ID: 0

Back Next

2. Create Your Wireless Network

3. Advanced Setting

Top

PC1(1)

Physical Config **Desktop** Programming Attributes

Web Browser

< > URL http://10.10.10.3

Go Stop

### Cisco 3400 Series Wireless LAN Controller

1. Set Up Your Controller

2. Create Your Wireless Network

3. Advanced Setting

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: \*\*\*\*\*

Ctrl-Pln Shared Secret: \*\*\*\*\*

VLAN: Management VLAN

DECT Service Address: 00000 (optional)

Grant Network

Back Next

3. Advanced Setting

Top

PC1(1)

Physical Config **Devices** Programming Attributes

Web Browser

URL: http://10.10.10.3

Go Stop

**CISCO** Cisco 3500 Series Wireless LAN Controller

Please confirm settings and apply

1 System Settings

Username: admin4-admin  
System Name: WLC  
Country: United Arab Emirates (AE)  
Date & Time: 11/09/2024 22:16:17  
Timezone: Manual, 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: Employees  
Security: WPA2 Enterprise  
Authentication Server IP Address: 10.10.10.4  
Authentication Server Shared Secret: secret  
Employee VLAN: Management VLAN  
RADIUS Server Address: -

☒ Guest Network

3 Advanced Settings

☒ RF Parameter Optimization

Radio 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://10.10.3/ane/WarEdit.html

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs > Edit 'HR'

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.)

Layer 2 Security: All

Interface/Interface Group(s): lan 23

Protected Management Frame: ☐ Enabled ☒ Disabled

WPA2 Parameters: WPA2 Policy: ☒ WPA2 Encryption: ☒ AES ☐ TKIP

Authentication Key Management: IEEE 802.1X: ☐ Enable ☒ Disable PSK: ☒ Enable ☐ Disable

Post Notes:

- 1 Web Policy cannot be used in combination with 2Pacs.
- 2) FlexConnect Local Switching is not supported with 3Pacs, CSMA/CA authentication, Override Interface ACLs.
- 3) When Reconnect Local Authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS.
- 4) When Reconnect Local Authentication is disabled, AP on connected mode will use WLC as RADIUS and AP as NAS while AP on standalone mode.
- 5 When client exclusion is enabled, a Timeout value of zero means infinity. (will require administrative override to reset excluded clients).
- 6 When client IP is not active within WPA2 is configured.
- 7 When client IP is configurable only when FlexConnect Local Switching is enabled.
- 8 WPA2 and open or AES security should be enabled to support higher 11n rates.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering should be disabled.
- 11 Guest Network, Local Authentication, CAPWAP required should be disabled.
- 12 Non-associated clients feature and Central Authentication feature are not supported with FlexConnect Local Authentication.
- 13 VLAN based central switching is not supported with FlexConnect Local Authentication.
- 14 Enabling psk authentication will prevent clients from encrypting broadcast and multicast packets.
- 15 Fast Transition is supported with WPA2 and open security policy.
- 16 Override Bandwidth Constraints parameters are specific to per Rates of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.
- 17 When Diagnostic Channel is enabled, RFP blocking action will be assigned to drop action.

PC\_WLC

Physical Config **Desktop** Programming Attributes

Web Browser

URL: https://10.10.3/ane/WarEdit.html

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs > Edit 'Trainees'

General Security QoS Policy Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: WPA2/WPA3

MAC Filtering: ☐

Post Transition: ☐

Protected Management Frame: Disabled

WPA2/WPA3 Parameters: WPA2 Policy: ☐ WPA2 Encryption: ☒ AES ☐ TKIP

Authentication Key Management: IEEE 802.1X: ☐ Enable ☒ Disable PSK: ☒ Enable ☐ Disable

Post Notes:

- 1 Web Policy cannot be used in combination with 2Pacs.
- 2) FlexConnect Local Switching is not supported with 3Pacs, CSMA/CA authentication, Override Interface ACLs.
- 3) When Reconnect Local Authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS.
- 4) When Reconnect Local Authentication is disabled, AP on connected mode will use WLC as RADIUS and AP as NAS while AP on standalone mode.
- 5 When client exclusion is enabled, a Timeout value of zero means infinity. (will require administrative override to reset excluded clients).
- 6 When client IP is not active within WPA2 is configured.
- 7 When client IP is configurable only when FlexConnect Local Switching is enabled.
- 8 WPA2 and open or AES security should be enabled to support higher 11n rates.
- 9 Value zero implies there is no restriction on maximum clients allowed.
- 10 MAC Filtering should be disabled.
- 11 Guest Network, Local Authentication, CAPWAP required should be disabled.
- 12 Non-associated clients feature and Central Authentication feature are not supported with FlexConnect Local Authentication.
- 13 VLAN based central switching is not supported with FlexConnect Local Authentication.
- 14 Enabling psk authentication will prevent clients from encrypting broadcast and multicast packets.
- 15 Fast Transition is supported with WPA2 and open security policy.
- 16 Override Bandwidth Constraints parameters are specific to per Rates of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.
- 17 When Diagnostic Channel is enabled, RFP blocking action will be assigned to drop action.

PC:WLC

Physical Config **Devices** Programming Attributes

Web Browser

URL: https://10.10.10.3/ane/ViewEdit.html

Go Stop

Back Configuration Exit Logout Refresh

Home

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > EdgR 'HR'

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

Radius Server Discovery Interface: ☒ Enabled ☐ Disabled

Authentication Servers	Accounting Servers	EAP Parameters
<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled	<input type="checkbox"/> Enabled <input type="checkbox"/> Disabled	<input type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Server 1: IP: 10.10.10.4, Port: 1812	None	None
Server 2: None	None	None
Server 3: None	None	None
Server 4: None	None	None
Server 5: None	None	None
Server 6: None	None	None

Radius Server Accounting

Interim Updates: ☐

LDAP Servers

Post Notes

1. Host Policy cannot be used in combination with Flex.
- 2(a) FlexConnect Local Switching is not supported with Flex, Cisco ISE authentication, Onboard Interface ACS.
- 2(b) When FlexConnect Local Authentication is enabled, irrespective of AP or connected to, 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 oversight to reset excluded clients).
4. Client KPI is not active unless WPA2 is configured.
5. Guest Client ID is configurable only when FlexConnect Local Switching is enabled.
6. WPA2 and open or AES security should be enabled to support higher 15m rates.
7. Some new modes there is no restriction on maximum clients allowed.
8. ALC Filtering is not supported with FlexConnect Local Authentication.
9. RADIUS Accounting should be enabled.
10. Guest roaming, Local Switching, Cisco ISE required should be disabled.
11. FlexConnect Local Switching is not supported with Flex, Cisco ISE authentication, Onboard Interface ACS.
12. FlexConnect Local Authentication is not supported with Flex, Cisco ISE authentication, Onboard Interface ACS.
13. FlexConnect Local Authentication is not supported with FlexConnect Local Authentication.
14. Enabling pki operations will prevent clients from connecting to standalone mode.
15. Flex Transition is supported with WPA2 and open security policy.
16. Override the switch control 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.
17. When diagnostic channel is enabled, RADIUS Accounting will be assigned to Cong action.

☐ Top

IT

PC\_WLC

Physical Config **Desktop** Programming Attributes

Web Browser

< > URL https://10.10.10.3/#name=WlanEdit.html

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs

Advanced

AP Groups

WLANs > Edit: IT

General Security QoS Policy Mapping Advanced

Profile Name: IT

Type: WLAN

SSID: IT

Status: ☒ Enabled

Security Policies: [WPA2][Auth(WPA2,1X)]  
(Modifications done under security tab will appear after applying the changes.)

Auth Policy: All

Interface/Interface Group(s): Vlan 22

Portfast Span Protection: ☐ Enabled

Portfast SSID: ☒ Enabled

AP ID:

Post Notes:

1 WPA Policy cannot be used in combination with Flex.  
2(1) FlexConnect Local Switching is not supported with Flex, CHAP/NTL 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.  
3(1) When FlexConnect Local Authentication is disabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
3(2) When client authentication is enabled, a Timeout value of zero means infinite. (will require authentication repeatedly to reveal excluded identity).  
4 Client APN is not active unless WPA2 is configured.  
5 Leave Client IP as configurable only when FlexConnect Local Switching is enabled.  
6 WPA and open or AES security should be enabled to support higher 11n rates.  
7 Leave zero implies there is no restriction on maximum clients allowed.  
8 MAC Filtering is not supported with FlexConnect Local Authentication.  
9 MAC Filtering should be disabled.  
10 Guest functionality, Local authentication, CAPWAP required should be disabled.  
11 All unsupported features, features and Central Issues feature are not supported with FlexConnect Local Authentication.  
12 VLAN based central switching is not supported with FlexConnect Local Authentication.  
13 Enabling ps, mechanisms will prevent clients from connecting broadcast and multicast packets.  
14 Fast Transition is supported with WPA2 and open security policy.  
15 Override Broadcast Control 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.  
16 When diagnostic channel is enabled, Port Blocking Action will be assigned to drop action.

Top

PC\_WLC

Physical Config **Desktop** Programming Attributes

Web Browser

< > URL https://10.10.10.3/#name=WlanEdit.html

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs

Advanced

AP Groups

WLANs > Edit: IT

General Security QoS Policy Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: WPA+WPA2

MAC Filtering: ☐

Post Transition:

Protected Management Frame: Disabled

WPA+WPA2 Parameters

WPA Policy: ☐

WPA2 Policy: ☒

WPA2 Encryption: ☒ AES ☐ TKIP

Authentication Key Management

802.1X: ☒ Enable

PSK: ☐ Enable

IT WPA2: ☐ Supply

Post Notes:

1 WPA Policy cannot be used in combination with Flex.  
2(1) FlexConnect Local Switching is not supported with Flex, CHAP/NTL 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.  
3(1) When FlexConnect Local Authentication is disabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
3(2) When client authentication is enabled, a Timeout value of zero means infinite. (will require authentication repeatedly to reveal excluded identity).  
4 Client APN is not active unless WPA2 is configured.  
5 Leave Client IP as configurable only when FlexConnect Local Switching is enabled.  
6 WPA and open or AES security should be enabled to support higher 11n rates.  
7 Leave zero implies there is no restriction on maximum clients allowed.  
8 MAC Filtering is not supported with FlexConnect Local Authentication.  
9 MAC Filtering should be disabled.  
10 Guest functionality, Local authentication, CAPWAP required should be disabled.  
11 All unsupported features, features and Central Issues feature are not supported with FlexConnect Local Authentication.  
12 VLAN based central switching is not supported with FlexConnect Local Authentication.  
13 Enabling ps, mechanisms will prevent clients from connecting broadcast and multicast packets.  
14 Fast Transition is supported with WPA2 and open security policy.  
15 Override Broadcast Control 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.  
16 When diagnostic channel is enabled, Port Blocking Action will be assigned to drop action.

Top

PC\_WLC

Physical Config **Desktop** Programming Attributes

Web Browser

< > URL: https://10.10.3/pane/WanEdt.html

Save Configuration Exit Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit TT

WLANs WLANs Advanced AP Groups

General Security **QoS** Policy-Mapping Advanced

Layer 2 Layer 3 **AAA Servers**

Layer 2 Security 8 WPA4/WPA2

HAC Filtering ☐

Fast Transition

Protected Management Frame

PMF Disabled

WPA/WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☒

WPA2 Encryption ☒ AES ☐ TKIP

Authentication Key Management

802.1X ☒ Enable

PSK ☐ Enable

WPA2 ☐ Enable

Post Notes

1 Web Proxy cannot be used in combination with PMF.  
2 WPA/WPA2 Local Switching is not supported with IPv6, CHAP/HTTP authentication, Overload Interface ACS.  
3 WPA/WPA2 Local Switching is not supported with IPv6, CHAP/HTTP authentication, Overload Interface ACS.  
4 When WPA/WPA2 Local Switching is enabled, regardless of AP or connected or standalone mode the AP will act as MAC.  
5 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
6 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
7 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
8 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
9 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
10 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
11 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
12 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
13 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
14 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
15 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
16 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
17 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
18 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
19 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.  
20 When WPA/WPA2 Local Switching is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while its on standalone mode.

☐ Top

# Trainees

PC-WLC

Physical Config **Desktop** Programming Attributes

Web Browser  
URL: https://10.10.10.3/wire/VarEdit.html

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit "Trainees"

WLANs  
WLANs  
Advanced  
AP Groups

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.)

Apply Policy: All  
Interface/Interface Group(s): Vlan 40  
Multicast Scan Method: ☐ Enabled  
Broadcast SSID: ☒ Enabled  
MBO-20:

Foot Notes

- 1 Web Policy cannot be used in combination with Flex.
- 2 FlexConnect Local Switching is not supported with Flex, CDA/TE authentication, Override Interface ACLs.
- 3 When FlexConnect Local Authentication is enabled, irrespective of AP or standalone mode the AP will act as NAS.
- 4 When FlexConnect Local Authentication is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while in on-standalone mode.
- 5 When client authentication is enabled, a Timeout value of zero means infinity (will require administrative override to reset excluded clients).
- 6 Client APN is not active unless WPA2 is configured.
- 7 Guest Client AP is configurable only when FlexConnect Local Switching is enabled.
- 8 WMM and open or AES security should be selected to support higher TX rates.
- 9 When more than one channel is in operation on maximum clients allowed.
- 10 MAC Filtering is not supported with FlexConnect Local Authentication.
- 11 MAC Filtering should be disabled.
- 12 Guest forwarding, Local switching, GPOC programs should be disabled.
- 13 FlexConnect Local Authentication and Central Access feature are not supported with FlexConnect Local Authentication.
- 14 WLAN based central switching is not supported with FlexConnect Local Authentication.
- 15 Enabling the authentication will prevent clients from connecting. Associated and unassociated packets.
- 16 Fast Transition is supported with WPA2 and open security policy.
- 17 Override Broadcast Control 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, RRM blocking action will be assigned to Group action.

☐ Top

PC-WLC

Physical Config **Desktop** Programming Attributes

Web Browser  
URL: https://10.10.10.3/wire/VarEdit.html

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit "Trainees"

WLANs  
WLANs  
Advanced  
AP Groups

General Security **QoS** Policy-Mapping Advanced

Layer 2 Layer 3 **AAA Servers**

Layer 2 Security: [WPA2+WPA3]  
MAC Filtering: ☐

Fast Transition

Protected Management Frame  
PMF: Disabled

WPA+WPA2 Parameters  
WPA Policy: ☒  
WPA2 Policy: ☒  
WPA2 Encryption: ☒ AES ☐ TKIP

Authentication Key Management  
BSS TX: ☐ Enable  
PSK: ☒ Enable

Foot Notes

- 1 Web Policy cannot be used in combination with Flex.
- 2 FlexConnect Local Switching is not supported with Flex, CDA/TE authentication, Override Interface ACLs.
- 3 When FlexConnect Local Authentication is enabled, irrespective of AP or standalone mode the AP will act as NAS.
- 4 When FlexConnect Local Authentication is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while in on-standalone mode.
- 5 When client authentication is enabled, a Timeout value of zero means infinity (will require administrative override to reset excluded clients).
- 6 Client APN is not active unless WPA2 is configured.
- 7 Guest Client AP is configurable only when FlexConnect Local Switching is enabled.
- 8 WMM and open or AES security should be selected to support higher TX rates.
- 9 When more than one channel is in operation on maximum clients allowed.
- 10 MAC Filtering is not supported with FlexConnect Local Authentication.
- 11 MAC Filtering should be disabled.
- 12 Guest forwarding, Local switching, GPOC programs should be disabled.
- 13 FlexConnect Local Authentication and Central Access feature are not supported with FlexConnect Local Authentication.
- 14 WLAN based central switching is not supported with FlexConnect Local Authentication.
- 15 Enabling the authentication will prevent clients from connecting. Associated and unassociated packets.
- 16 Fast Transition is supported with WPA2 and open security policy.
- 17 Override Broadcast Control 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, RRM blocking action will be assigned to Group action.

☐ Top

PC-WLC

Physical Config **Devices** Programming Attributes

Web Browser

URL: https://10.10.3/pane/WarEdit.html

Go Stop

Save configuration Log Logout Refresh

Home

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs

Advanced

AP Groups

WLANs > Edit "Trainees"

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

Radius Server Discovery Interface Disabled

	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	None	None	Secure
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	
Server 7	None	None	
Server 8	None	None	
Server 9	None	None	
Server 10	None	None	

Radius Server Accounting

Radius Defaults

LDAP Servers

Post-Notes

1 Real-IPsec cannot be used in combination with Flex.  
2 Flex/Connect Local Switching is not supported with Flex, CBA/ATP authentication, Onboard Interface ACLs.  
3(1) When FlexConnect local authentication is enabled, regardless of AP or connected or standalone mode the AP will act as NAS.  
2(1) When FlexConnect local authentication is enabled, AP on connected mode will use WLC as RADIUS and AP as NAS while it is on standalone mode.  
3 When client authentication is enabled, a Timeout of zero means infinity. (will require administrative oversight to reset excluded clients).  
4 Client AP is not active unless WPA2 is configured.  
5 Green Client IP is configurable only when FlexConnect Local Switching is enabled.  
6 WPA2 and open or AES security should be selected to support higher 11n rates.  
7 When WPA2 is selected there is no restriction on maximum clients allowed.  
8 RADIUS filtering is not supported with FlexConnect Local authentication.  
9 RADIUS filtering should be disabled.  
10 Client forwarding, local switching, DHCP required should be disabled.  
11 Max recommended clients per AP and Central Access feature are not supported with FlexConnect Local Authentication.  
12 WLAN based central switching is not supported with FlexConnect Local Authentication.  
13 Enabling the authentication will prevent clients from connecting, disconnect and re-authenticate.  
14 Fast Transition is supported with WPA2 and open security policy.  
15 Override the switch control parameters are specific to per basis of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.  
16 When diagnostic channel is enabled, port blocking action will be assigned to drop action.

Top

## Group:

PC:WLC

Physical Config Desktop Programming Airhouse

Web Browser  
URL: https://10.10.10.2/aaaAPGroupEdit.html

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration | Exit | Logout | Refresh

WLANs

▼ WLANs  
▼ Advanced  
2P Groups

Ap Groups > Edit "default-group"

General | **WLANs** | APs | 802.11n | Location | Ports/Module

APs currently in the Group

AP Name	Ethernet MAC
<input type="checkbox"/> Light Weight Access Point01	1000.2BAA.3E0C
<input type="checkbox"/> Light Weight Access Point01	0013.1104.3C9E
<input type="checkbox"/> Light Weight Access Point02	1000.9A71.1D9C
<input type="checkbox"/> 1065.2F55.8761	1065.2F55.8761

Add APs to the Group

☐ AP Name Group Name

Fast Notes

1 Changing the WLAN interface mapping in an AP Group will remove the local WLAN mapping for disconnected AP in this group.  
2 AP7000 with 802.11n Module will only advertise 802.11n if 802.11n is selected.  
3 Guest Traffic QoS should be enabled, to set the QoS QoS.  
4 AP7000 has 3 LAN ports, which are configured through "Ports/Module".  
5 OSPF110 LAN/LAN2 are configured through "Ports/Module", with WLAN "None" represents local port. LAN2 is always a local port.  
6 OSPF110 will only advertise Port 0 (LAN0).  
7 AP7000 Aux port is configured through LAN0.

☐ Top

## Interfaces:

PC\_WLC

Physical Config Desktop Programming Attributes

Web Browser

URL: https://10.10.20.1/ame/interface50.html

Go Stop

Save Configuration Log Logout Refresh Home

MONITOR VLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Controller

General

Inventory

Interfaces

Interface Groups

Mobilecast

Internal DHCP Server

Mobility Management

Ports

NTP

CDP

Tunneling

IPv6

mDNS

Advanced

Interfaces > Edit

General Information

Interface Name: Vlan 20

MAC Address: 00:50:0B:8D:44:47

Configuration

Speed/Link: ☐

Coastdown: ☐

Overloadable Vlan ID: 0

WNT-20:

Physical Information

Port Number: 1

Access 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: 10.10.20.1

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:

mDNS

Top

PC\_WLC

Physical Config Desktop Programming Attributes

Web Browser

URL: https://10.10.20.1/ame/interface50.html

Go Stop

Save Configuration Log Logout Refresh Home

MONITOR VLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Controller

General

Inventory

Interfaces

Interface Groups

Mobilecast

Internal DHCP Server

Mobility Management

Ports

NTP

CDP

Tunneling

IPv6

mDNS

Advanced

Interfaces > Edit

General Information

Interface Name: Vlan 20

MAC Address: 00:30:17:14E:D2:54

Configuration

Speed/Link: ☐

Coastdown: ☐

Overloadable Vlan ID: 0

WNT-20:

Physical Information

Port Number: 1

Access 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: 10.10.20.1

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:

mDNS

Top



PC\_WLC

PhysicalConfigDesktopProgrammingAttributes

Web Browser

<>URL: https://10.10.10.3/laninterfaceEdit.html

GoStop

Save ConfigurationEngLogoutRefreshHome

CISCO

MONITORVLANSCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHelpFeedback

Controller

General

Interfaces

Interface Groups

Multicast

Internal DHCP Server

Mobility Management

Ports

NTP

CDP

Tunneling

IPv6

mDNS

Advanced

Interfaces > Edit

General Information

Interface NameVlan 40

MAC Address00:00:00:00:00:00

Configuration

Bridge Mode☐

Overlapping☐

Overlapping VLAN ID6

VLAN ID

Physical Information

Port Number1

Backup Port0

Active Port1

Enable Dynamic AP Management☐

Interface Address

VLAN Identifier40

IP Address10.10.10.1

Netmask255.255.255.0

Gateway10.10.10.1

DHCP Information

Primary DHCP Server10.10.10.1

Secondary DHCP Server

DHCP Proxy ModeGlobal

Enable DHCP Option 82☐

Access Control List

ACL Name

mDNS

Top