

# **Implementing Cisco Wireless Network Fundamentals**

---

**Version 1.0**

## **Fast Lane Lab Guide**

**Version 1.0.4**



---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

**DISCLAIMER WARRANTY:** THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

# Table of Contents

<b><u>Lab Introduction .....</u></b>	<b>1</b>
<b><u>Hardware Lab 1: Configure Windows 7 Client Access.....</u></b>	<b>3</b>
Overview .....	3
Visual Objective .....	4
Job Aids .....	4
Task 1: Establish an Open WLAN Connection.....	5
Task 2: Establish a PSK WLAN Connection .....	7
Task 3: Establish a PEAP WLAN Connection.....	9
Task 4: Establish a Web Authentication WLAN Connection.....	16
<b><u>Hardware Lab 2: Configuring the Wired Infrastructure.....</u></b>	<b>19</b>
Overview .....	19
Visual Objective .....	20
Job Aids .....	20
Task 1: Initialize the 3650 Switch.....	21
Task 2: Configure Layer 2 Operations .....	22
Task 3: Configure Layer 3 IPv4 Operations .....	26
<b><u>Hardware Lab 3: Configuring the Centralized WLAN Deployment.....</u></b>	<b>33</b>
Overview .....	33
Visual Objective .....	34
Job Aids .....	34
Task 1: Review and Modify Management Access.....	35
Task 2: Review AP Status.....	38
Task 3: Configure RF Power and Channel .....	40
Task 4: Configure a WLAN .....	44
Task 5: Enable Additional Features .....	48
Task 6: Associate the Client .....	52
Task 7: Review CleanAir.....	54
Task 8: Disassociate the Client.....	56
<b><u>Hardware Lab 4: Configuring IPv6 Operation in a Centralized WLAN Deployment .</u></b>	<b>57</b>
Overview .....	57
Visual Objective .....	58
Job Aids .....	58
Task 1: Review Client Association before IPv6 Configuration .....	59
Task 2: Enable IPv6 Infrastructure .....	62
Task 3: Associate the Client after IPv6 Configuration.....	66
<b><u>Hardware Lab 5: Configuring Security in a Centralized WLAN Deployment .....</u></b>	<b>69</b>
Visual Objective .....	70
Job Aids .....	70
Task 1: Implement WPA PSK Authentication.....	71
Task 2: Implement Local EAP Authentication .....	73
Task 3: Implement EAP with RADIUS Authentication.....	79
Task 4: Implement WebAuth Authentication .....	84
<b><u>Hardware Lab 6: Configuring Guest Access Using the Anchor WLC.....</u></b>	<b>87</b>
Overview .....	87
Visual Objective .....	88
Job Aids .....	88
Task 1: Add Foreign WLC on Anchor WLC .....	89
Task 2: Add Anchor WLC on Foreign WLC.....	92
Task 3: Configure the Guest WLAN on the Foreign WLC .....	94
Task 4: Configure the Guest WLAN on the Anchor WLC.....	98
Task 5: Create Local User on the Anchor WLC .....	101

Task 6: Associate the Client using WLC Credentials .....	102
Task 7: Associate the Client using ISE Credentials .....	105
Task 8: Lab Cleanup.....	110

## **Hardware Lab 7: Deploying a Converged Access WLAN..... 112**

Overview .....	112
Visual Objective .....	113
Job Aids .....	113
Task 1: Verify the Catalyst 3650 Status .....	114
Task 2: Initialize the Cat3650 Wireless Controller and AP .....	117
Task 3: Adjust RF Power and Channel .....	125
Task 4: Configure a WLAN .....	127
Task 5: Enable Additional Features .....	129
Task 6: Associate the Client .....	133
Task 7: Review CleanAir .....	135
Task 8: Disassociate the Client.....	137

## **Hardware Lab 8: Configuring Security on a Converged WLAN Deployment..... 138**

Overview .....	138
Visual Objective .....	139
Job Aids .....	139
Task 1: Implement WPA2 PSK Authentication .....	140
Task 2: Implement Local EAP Authentication.....	143
Task 3: Implement RADIUS Authentication .....	155
Task 4: Implement WebAuth Passthrough.....	162
Task 5: Implement Local WebAuth .....	168

## **Hardware Lab 9: Implement a FlexConnect WLAN Deployment..... 176**

Overview .....	176
Visual Objective .....	177
Job Aids .....	177
Task 1: Configure the Switch for FlexConnect Connectivity.....	178
Task 2: Add a New WLAN for FlexConnect Testing .....	180
Task 3: Adjust the AP Mode of Operation .....	181
Task 4: Test Client Access for FlexConnect .....	185
Task 5: Implement a FlexConnect Group .....	187
Task 6: Test Client Access for FlexConnect Group .....	193
Task 7: Switch Configuration Example .....	196
This section presents the switch configuration for Podx as an example. ....	196

## **Hardware Lab 10: Initialize an Autonomous WLAN Deployment..... 198**

Visual Objective .....	199
Job Aids .....	199
Task 1: Initialize and Configure the Autonomous AP .....	200
Task 2: Test Client Access to the Autonomous AP .....	209

## **Hardware Lab 11: Configure Security on an Autonomous AP WLAN Deployment . 212**

Visual Objective .....	213
Job Aids .....	213
Task 1: Implement PSK Authentication on an Autonomous AP .....	214
Task 2: Implement RADIUS Authentication on an Autonomous AP.....	218
Task 3: Autonomous Lab Cleanup.....	221

## **Hardware Lab 12: Configure Security on a Cloud WLAN Deployment..... 224**

Visual Objective .....	225
Job Aids .....	225
Task 1: Implement PSK Authentication on a Cloud WLAN Deployment .....	227
Task 2: Implement Local EAP-PEAP on a Cloud WLAN Deployment .....	232
Task 3: Implement WebAuth on a Cloud WLAN Deployment .....	236

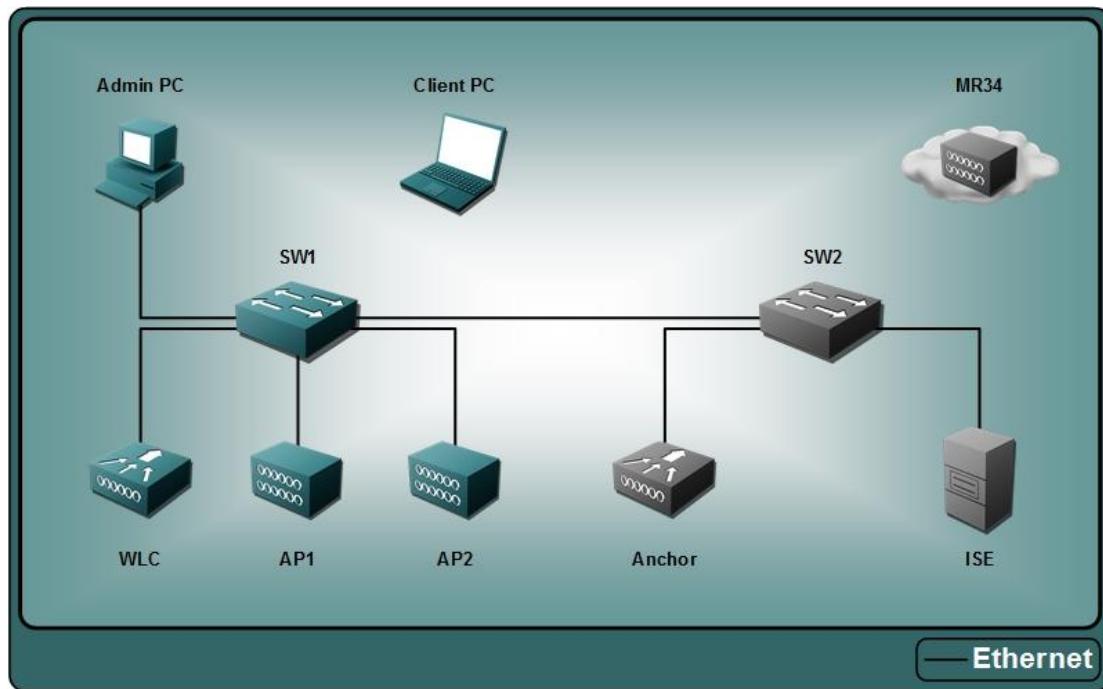
Task 4: Disable SSIDs on the Cloud WLAN Deployment .....	241
<b><u>Hardware Lab 13: Perform Centralized Controller Maintenance.....</u></b>	<b><u>244</u></b>
Visual Objective .....	245
Job Aids .....	245
Task 1: Backup the WLC Configuration .....	246
Task 2: Optional—Perform an AireOS Upgrade to the WLC.....	249
<b><u>Hardware Lab 14: Perform WiFi Scanning .....</u></b>	<b><u>252</u></b>
Visual Objective .....	253
Job Aids .....	253
Task 1: Enable Metageek inSSIDer .....	254
Task 2: Review 2.4 GHz Activity.....	257
Task 3: Review 5 GHz Activity .....	259
<b><u>Hardware Lab 15: Challenge—Various Trouble Tickets .....</u></b>	<b><u>260</u></b>
Visual Objective .....	262
Job Aids .....	262
Task 1: Challenge Ticket #1.....	263
Task 2: Challenge Ticket #2.....	266
Task 3: Answer Key .....	269
<b><u>Hardware Lab 16: Perform a Predictive WLAN Design .....</u></b>	<b><u>273</u></b>
Visual Objective .....	274
Job Aids .....	274
Task 1: Familiarization with Ekahau Site Survey Pro + Planner.....	275
Task 2: Perform a basic predictive WLAN design using a single floor layout.....	278
<b><u>Hardware Lab 17: Perform Passive Site Survey.....</u></b>	<b><u>285</u></b>
<b><u>Analysis .....</u></b>	<b><u>285</u></b>
Visual Objective .....	286
Job Aids .....	286
Task 1: Configure AP for Spectrum Expert AP mode of operation .....	287
Task 2: Configure Metageek Chanalyzer - spectrum analyzer software.....	289
Task 3: Load RF capture information into metageek Chanalyzer - spectrum analyzer software.....	292
Task 4: Analyze RF capture information into Metageek Chanalyzer - spectrum analyzer software.	293
<b><u>Glossary .....</u></b>	<b><u>300</u></b>



# Lab Introduction

---

This lab guide provides you with the opportunity put into practice the knowledge and skills you have acquired from this course. These labs focus on skills required to successfully implement and troubleshoot wireless technologies.





# **Hardware Lab 1: Configure Windows 7 Client Access**

---

## **Overview**

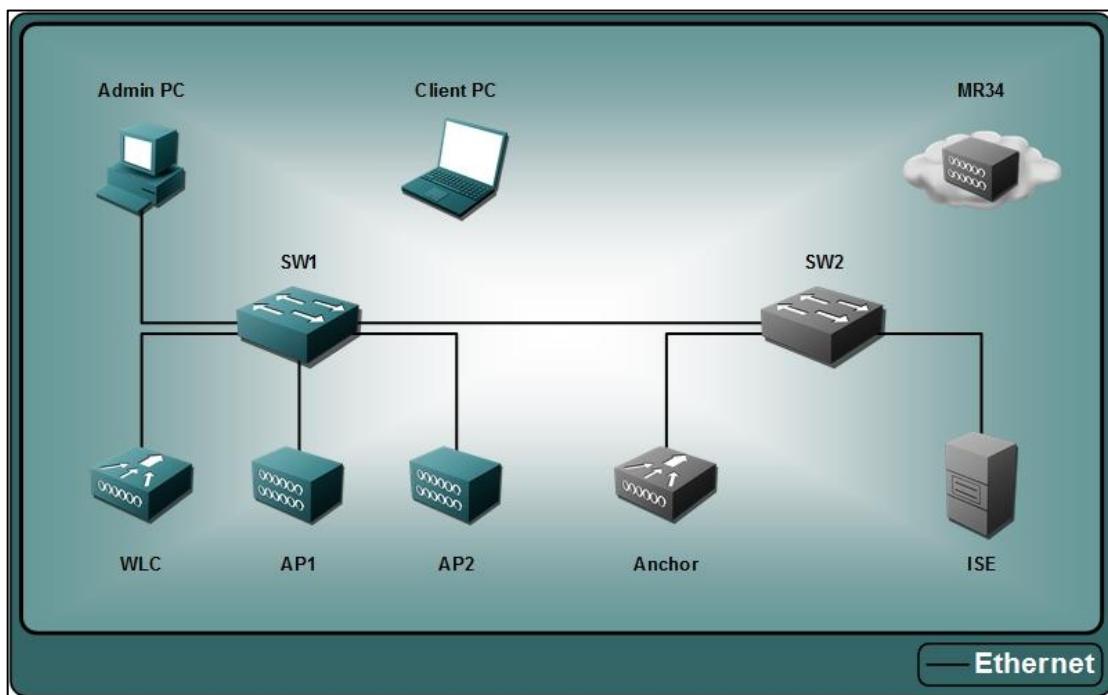
Complete this lab activity to practice what you learned in the related module.

In this activity, you will work with a Windows 7 client using native wireless configuration tools. After completing this activity, you will be able to meet these objectives:

- Establish an Open WLAN connection
- Establish a PSK WLAN connection
- Establish an EAP WLAN connection
- Establish a Web Authentication WLAN connection

# Visual Objective

The figure illustrates the topology for this lab.



## Job Aids

Here are the resources and equipment that are required to complete this activity:

- A Windows 7 PC with a wireless USB client adapter
- Meraki Access Point

# Task 1: Establish an Open WLAN Connection

## **Activity Procedure**

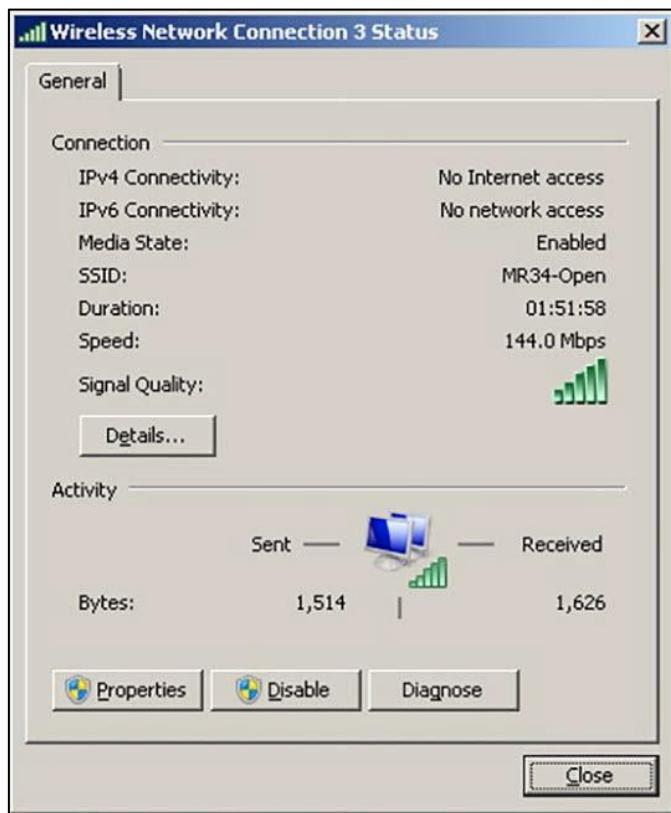
In this task, you will configure a connection to an open WLAN using the Windows 7 WLAN AutoConfig service.

- Step 1** Connect to the Client PC and log in with **Administrator / 1234QWer**.
- Step 2** Click the WLAN tray.
- Step 3** Click the **MR34-L-Open** (where L is your lab number as stated in the Student Notes) network, and then click **Connect**. (Do Not check the box for Connect automatically, you do not want to create a profile yet).



- Step 4** Click the WLAN tray.
- Step 5** Hover over the **MR34-L-Open** network. Check the status and the icon display.

**Step 6** Right-click the **MR34-L-Open** network and select **Status**.



**Step 7** Review the information that is displayed and the **Details**.

**Step 8** Verify IP connectivity by pinging the Gateway from the Details section.

**Step 9** Click the WLAN tray and then click the **MR34-L-Open** network and click “Disconnect”.



### ***Activity Verification***

You have successfully completed this task when you attain this result:

- You connected to the open network and verified IP connectivity.

## **Task 2: Establish a PSK WLAN Connection**

### ***Activity Procedure***

In this task, you will configure a connection to a PSK WLAN using the Windows 7 WLAN AutoConfig service.

Complete these steps:

**Step 1** Connect to the Client PC.

**Step 2** Click the WLAN tray.



- Step 3** Click the **MR34-L-PSK** (where L is your lab number as stated in the Student Notes) network, and then click **Connect**. (Do Not check the box for Connect automatically, you do not want to create a profile yet.)
- Step 4** Enter **Cisco123** for the Security Key and click **OK**.



- Step 5** Click the WLAN tray.
- Step 6** Hover over the **MR34-L-PSK** network. Check the status and the icon display.
- Step 7** Right-click the **MR34-L-PSK** network and select **Status**.
- Step 8** Review the information that is displayed and the **Details**.
- Step 9** Verify IP connectivity by pinging the Gateway from the Details section.
- Step 10** Click the WLAN tray and then click the **MR34-L-PSK** network and click **Disconnect**.

## **Activity Verification**

You have successfully completed this task when you attain this result:

- You connected to the PSK network and verified IP connectivity.

## **Task 3: Establish a PEAP WLAN Connection**

### **Activity Procedure**

In this task, you will configure a connection to a PEAP WLAN using the Windows 7 WLAN AutoConfig service.

Complete these steps:

- Step 1** Connect to the Client PC.



- Step 2** Click the WLAN tray.

- Step 3** Click the **MR34-L-PEAP** (where L is your lab number ad stated in the Student Notes) network, and then click **Connect**. (Do Not check the box for Connect automatically, you do not want to create a profile yet.)

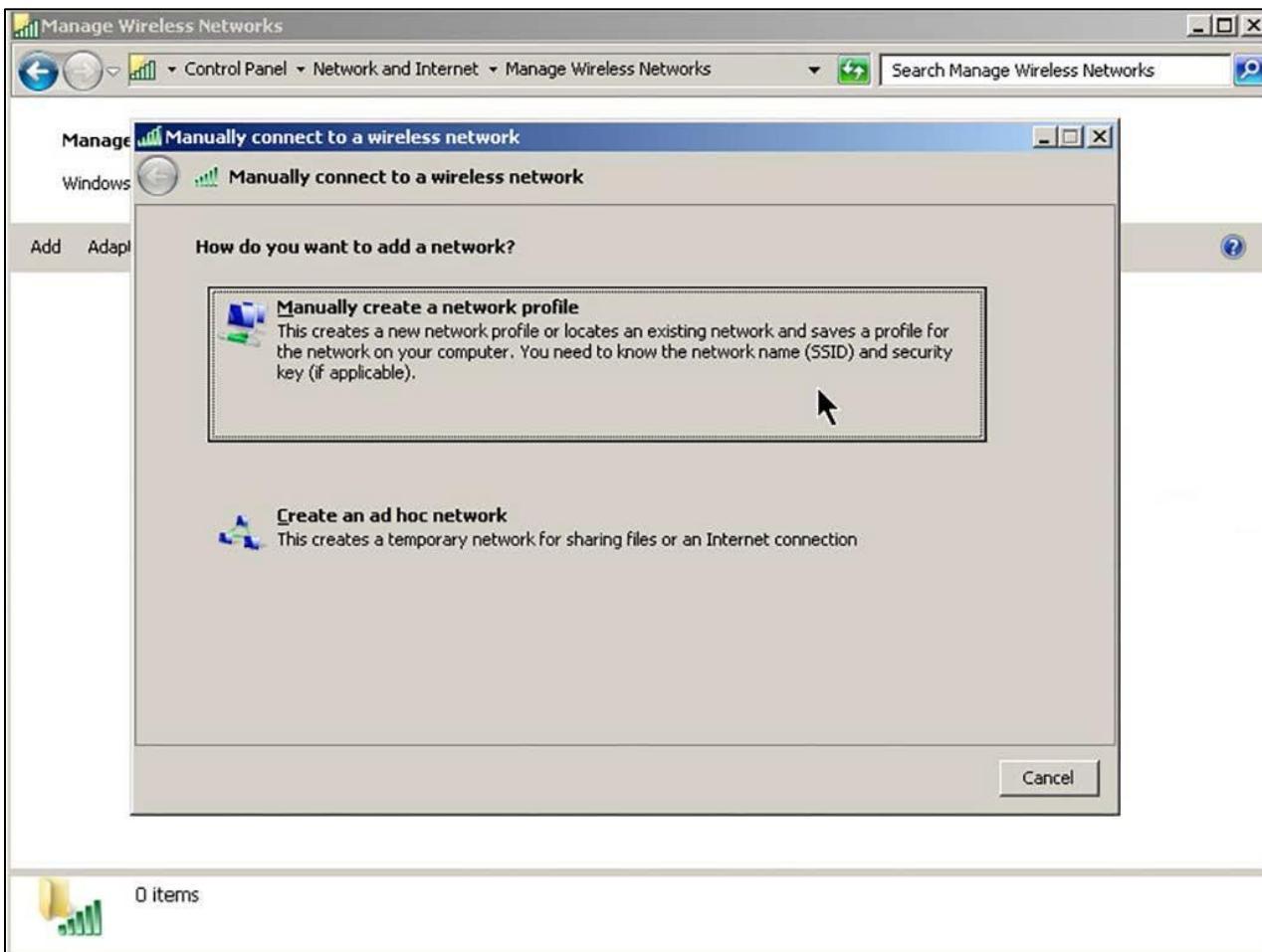


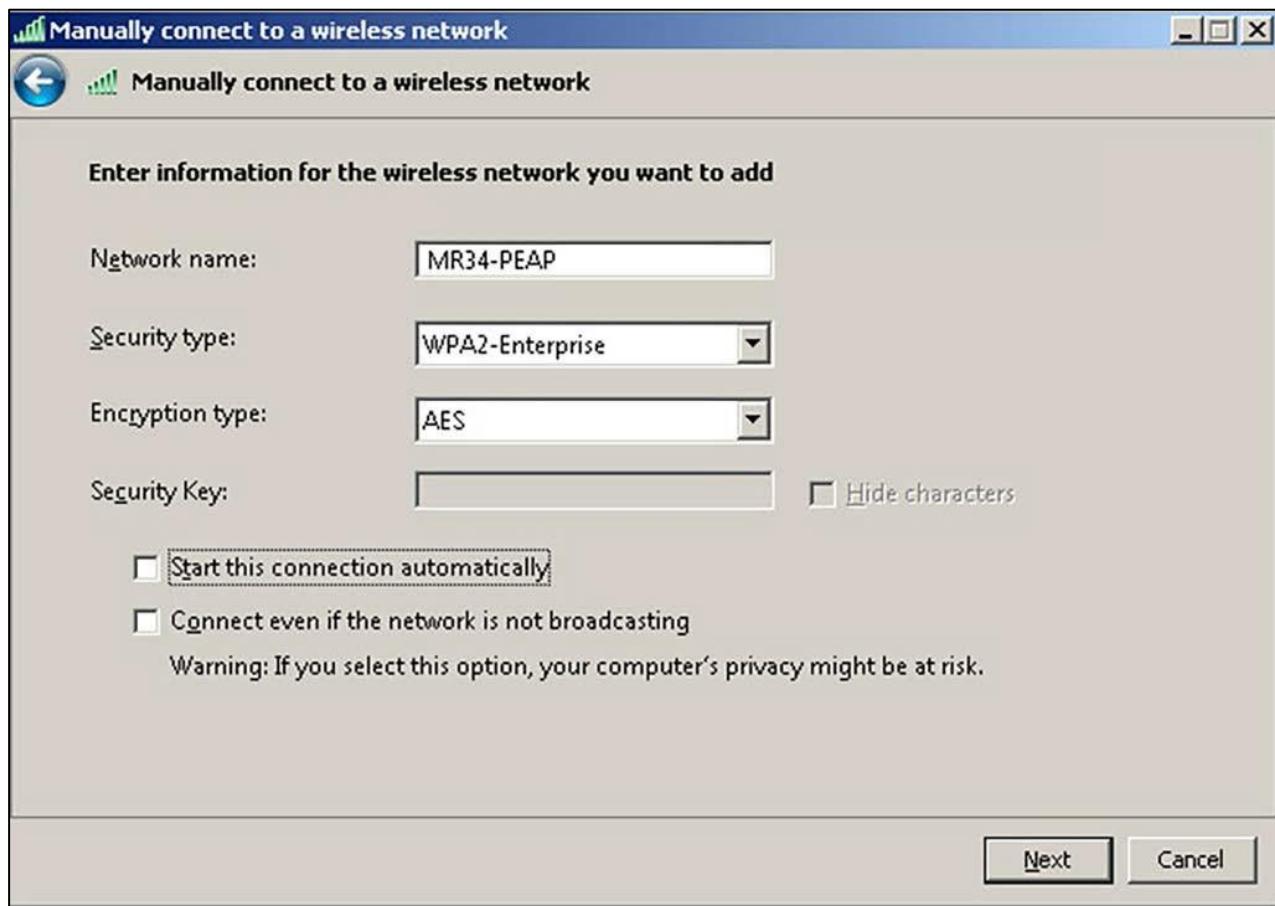
- Step 4** At the Windows Security pop-up screen, enter [lab@domain.com](#) on the first line and **Cisco123** on the second line and click **OK**.



- Step 5** At the next Windows Security Alert pop-up, click the **Connect** button to continue.  
Normally you would not accept untrusted certificates or certificate authorities, but in this lab example the risk is controlled.
- Step 6** Click the WLAN tray.
- Step 7** Hover over the **MR34-L-PEAP** network. Check the status and the icon display.
- Step 8** Right-click the **MR34-L-PEAP** network and select **Status**.
- Step 9** Review the information that is displayed and the **Details**.
- Step 10** Verify IP connectivity by pinging the Gateway from the Details section.

- Step 11** Click the WLAN tray and then click the **MR34-L-PEAP** network and click **Disconnect**.
- Step 12** Click the WLAN tray and select **Open Network and Sharing Center**.
- Step 13** Select **Manage wireless networks**.
- Step 14** Remove any saved profiles
- Step 15** On the **Manage wireless networks** page, click **Add** to add a network.
- Step 16** Select **Manually create a network profile**.





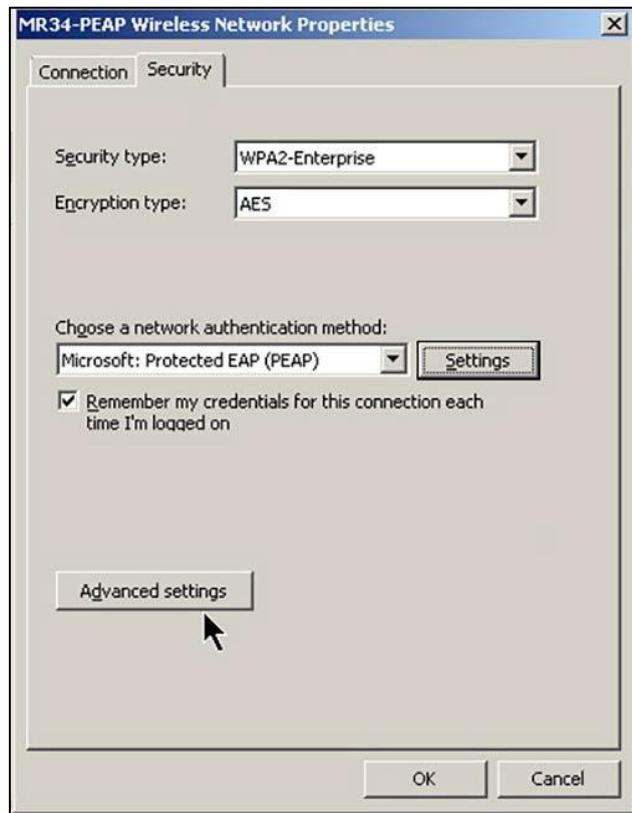
**Step 17** Enter in the following for the network:

- Network name: **MR34-L-PEAP** (where L is your lab number ad stated in the Student Notes)
- Security type: **WPA2-Enterprise**
- Encryption type: **AES**
- Unselect the **Start this connection automatically**

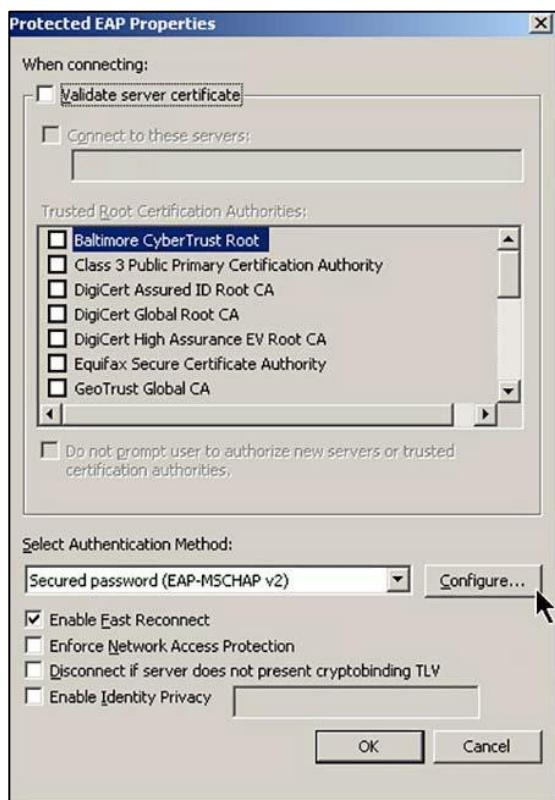
**Step 18** Click **Next** and then click **Close**.

**Step 19** Double-click the new profile.

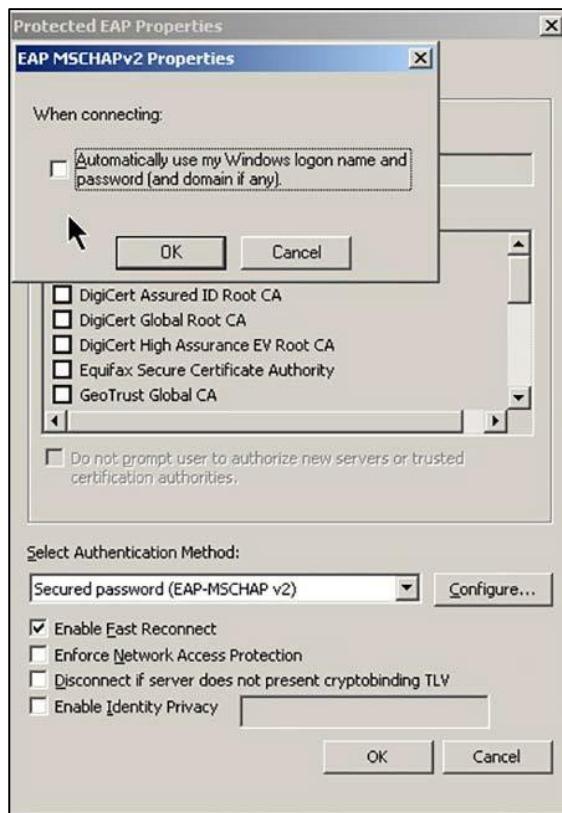
**Step 20** Select the **Security** tab.



**Step 21** Select **Settings** and then unselect **Validate server certificate**.

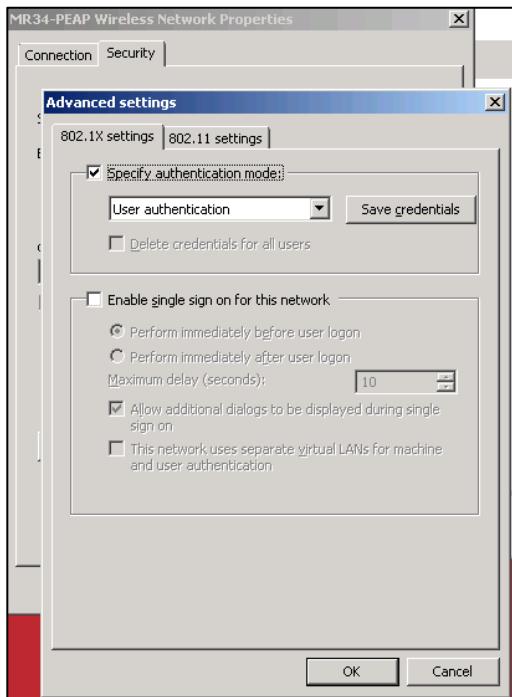


**Step 22** Click **Configure** and then on the pop-up, unselect **Automatically use my Windows logon name and password**. Then click **OK** and **OK**.



**Step 23** On the **Security** tab, click **Advanced settings**.

**Step 24** Select the **802.1X settings**.



**Step 25** Check the box for **Specify authentication mode**.

**Step 26** Change the drop-down selection to **User authentication**.

**Step 27** Then click **OK**, and **OK**, and **OK**.

**Step 28** Click **Close** on Profile Wizard

**Step 29** Click the WLAN tray.

**Step 30** Click the **MR34-L-PEAP** network, and then click **Connect**.

**Step 31** At the Windows Security pop-up screen, enter **podox@podox.com** (where x = pod number) on the first line and **Cisco123** on the second line.

**Step 32** Verify IP connectivity by pinging the gateway IP address (`ipconfig /all`).

**Step 33** Click the WLAN tray and then click the **MR34-L-PEAP** network and click **Disconnect**.

## **Activity Verification**

You have successfully completed this task when you attain this result:

- You connected to the PEAP network and verified IP connectivity.
- You created a PEAP profile with saved credentials.

# Task 4: Establish a Web Authentication WLAN Connection

## Activity Procedure

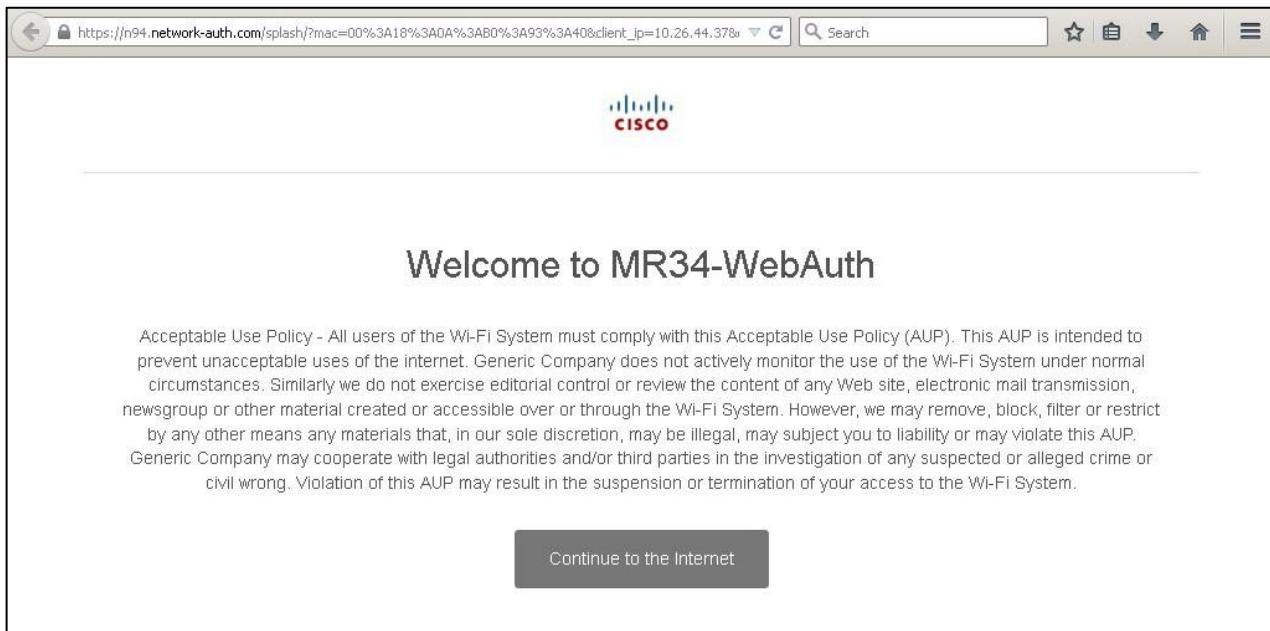
In this task, you will configure a connection to a web authentication WLAN using the Windows 7 WLAN AutoConfig service.

Complete these steps:

- Step 1** Connect to the Client PC.
- Step 2** Click the WLAN tray.
- Step 3** Click the **MR34-L-WebAuth** (where L is your lab number ad stated in the Student Notes) network, and then click **Connect**. (Do Not check the box for Connect automatically, you do not want to create a profile yet.)
- Step 4** Click the WLAN tray.



- Step 5** Hover over the **MR34-L- WebAuth** network. Check the status and the icon display.
- Step 6** Right-click the **MR34-L- WebAuth** network and select **Status**.
- Step 7** Review the information that is displayed and optionally the **Details**.
- Step 8** Open a browser and go to <http://www.cisco.com> (or <http://172.16.0.2> -switch web GUI)



**Step 9** You should be redirected to the Web Authentication page. Click **Continue to the internet**.

**Step 10** You will now be redirected back to your original URL of **http://www.cisco.com** (or to switch **http://172.16.0.2** and be prompted for login)



**Step 11** Click the WLAN tray and then click the **MR34-L-WebAuth** network and click **Disconnect**.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- You connected to the web authentication network and verified IP connectivity.
- You were redirected to an authentication page and upon acceptance, back to your original target URL.



# **Hardware Lab 2: Configuring the Wired Infrastructure**

---

## **Overview**

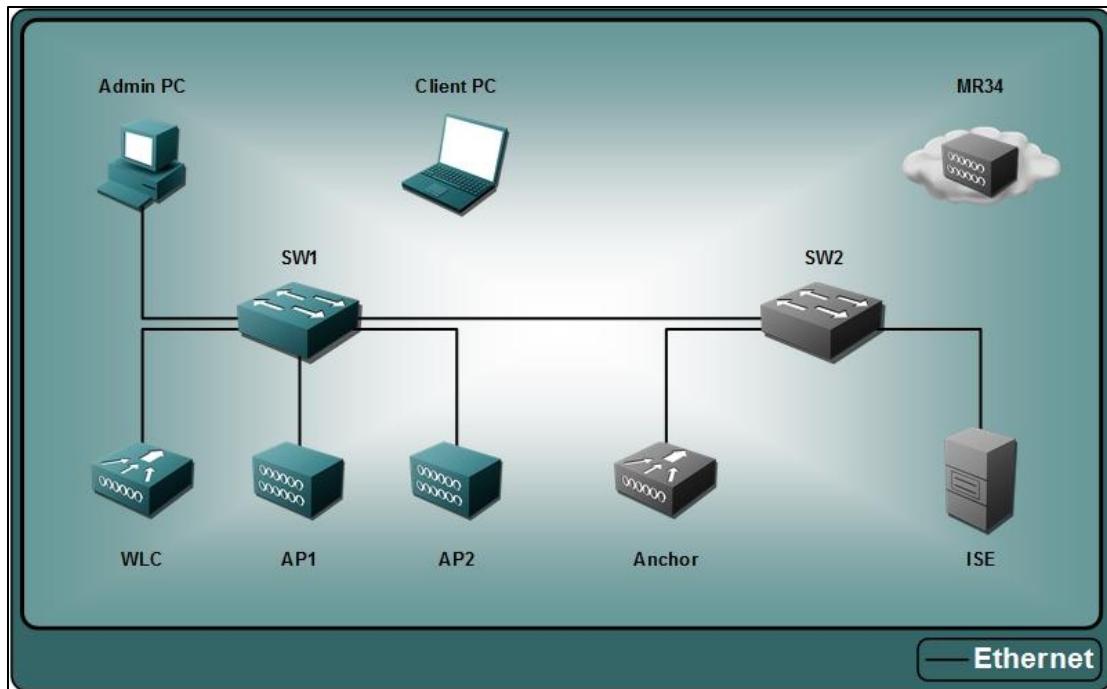
In this activity, you configure the wired infrastructure Layer 2 and Layer 3 operations.

Upon completing this guided lab, you will be able to:

- Initialize the 3650
- Configure Layer 2 Operations
- Configure Layer 3 IPv4 Operations

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 3650 switch

### VLANs and IP Ranges

#### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

# Task 1: Initialize the 3650 Switch

## **Activity Procedure**

In the following steps, you will connect to the “un-initialized” switch and run the Initial Configuration Dialog wizard to setup basic configuration for the switch.

Complete these steps:

**Step 1** Connect to the SW1 switch Console port

**Step 2** Power On the switch

**Step 3** You are now connected to the switch console port and can see the power up sequence.

**Note:** The switch should be in a factory reset state, if not, contact your instructor

**Step 4** When switch is done reloading, press Enter until you see this prompt:

Would you like to enter the initial configuration dialog?

**Step 5** Type yes and press **Enter**

Would you like to enter basic setup instead of extended setup?

**Step 6** Type yes and press **Enter**

**Step 7** Type the entries at indicated for each prompt and press **Enter**

- Enter host name: **SW1**
- Enter enable secret: **cisco**
- Enter enable password: **enablecisco**
- Enter virtual terminal password: **Cisco123**
- Do you want to configure country code: **yes**
- Enter the country code [US]: **DE**
  - Note: There will be a slight pause before next prompt
- Setup account for accessing HTTP server?: **yes**
- User: **admin**
- Password: **Cisco123**
- Configure SNMP network management? **no**

**Step 8** The interfaces will then be listed:

Press **space** to see more

- Step 9** This next step will set our management interface IP address and VLAN association. Enter the information given for each prompt and press **Enter**.
- Enter interface name used to connect to the management network from the above interface summary: **vlan1**
  - Configure IP on this interface?: **yes**
  - IP address for this interface: **192.168.11.254**
  - Subnet mask for this interface [255.255.255.0]: **255.255.255.0**
- Step 10** Display will show “The following configuration command script was created:” (Basically a Show Run)
- Press **space** for **More** and until command shows **end**
- Step 11** At the “Enter your selection [2]” prompt, type **2** and press **Enter**
- Type **Y** and press **Enter** to continue
- Step 12** At the “press RETURN to get started:”, press **Enter**
- Step 13** At the SW1 prompt, type **enable** and press **Enter**
- Step 14** Type the password of **cisco**.
- Step 15** Type: **copy run start** and press **Enter**
- Step 16** At “Destination filename [startup-config]? Press **Enter**

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- You have initialized the 3650 switch with the correct values.
- You have saved the configuration to startup-config.

## **Task 2: Configure Layer 2 Operations**

### ***Activity Procedure***

In this task, you will configure the Layer 2 operations for the switch, as well as some basic console connectivity settings.

Complete these steps:

**Step 1** Connect to the SW1 switch Console port

**Step 2** Press enter until SW1 prompt appears

**Step 3** Type: **enable** and press **Enter**

**Step 4** Enter password of **cisco** and press **Enter**

**Step 5** Type: **config term** and press **Enter** to enter global configuration mode

**Note:** Press **Enter** after every command (ex: type: **interface vlan1**)

**First, we need to setup console and virtual terminal access parameters.**

**Step 6** Buffer log messages:

```
SW1(config)# line con 0
SW1(config-line)# logging synchronous
SW1(config-line)# exec-timeout 30
SW1(config-line)# line vty 0 5
SW1(config-line)# logging synchronous
SW1(config-line)# exec-timeout 30
```

**The VTP mode will be set to off as we do not want to send or forward VTP updates.**

**Step 7** Turn off VLAN Trunking Protocol advertisement

```
SW1(config)# vtp mode off
```

**The WLC will need a management VLAN, AP VLAN and a Client VLAN.**

**Step 8** Create Management VLAN

```
SW1(config)# vlan 11
SW1(config-vlan)# name mgt
```

**Step 9** Create Access Point VLAN

```
SW1(config-vlan)# vlan 12
SW1(config-vlan)# name AP
```

**Step 10** Create Client VLAN

```
SW1(config-vlan)# vlan 14
SW1(config-vlan)# name Client
```

---

**Note** Verify VLANs by typing “show vlan brief” from the EXEC mode.

---

**The switch ports will need to be configured for the proper operation (access vs. trunk) and the correct VLANs.**

**Step 11** Configure DC switch port as an access port with mgt VLAN to allow communication between the WLC, ISE and other devices.

```
SW1(config)# interface GigabitEthernet1/0/24
SW1(config-if)# description To DC Switch
SW1(config-if)# switchport access vlan 11
SW1(config-if)# switchport mode access
SW1(config-if)# spanning-tree portfast
```

---

<b>Note</b>	Note warning regarding STP. We can use this command as this is a host connection
-------------	--

---

**Step 12** Configure AP1 switch port. Configured for Access mode and needs Vlan 12 for DHCP.

```
SW1(config)# interface GigabitEthernet1/0/1
SW1(config-if)# description AP1
SW1(config-if)# switchport access vlan 12
SW1(config-if)# switchport mode access
SW1(config-if)# spanning-tree portfast
```

**Step 13** Configure AP2 switch port. Configured for Trunk Access and will be used in a later lab.

```
SW1(config)# interface GigabitEthernet1/0/2
SW1(config-if)# description AP2
SW1(config-if)# switchport access vlan 12
SW1(config-if)# switchport trunk native vlan 12
SW1(config-if)# switchport mode trunk
SW1(config-if)# shut
```

**Step 14** Configure WLC switch port. Configured as a Trunk Port to allow multiple VLANS (mgt, AP and Client).

```
SW1(config)# interface GigabitEthernet1/0/12
SW1(config-if)# description WLC
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport nonegotiate
```

---

<b>Note</b>	“Switchport nonegotiate” disables DTP (Dynamic Trunking Protocol) and puts the interface into trunk mode immediately.
-------------	---

---

**Step 15** Configure switch port. This goes to the SW2 switch and requires a trunk port with all pod VLANs that may need to be routed.

```
SW1(config)# interface GigabitEthernet1/0/22
SW1(config-if)# description to SW2
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 11-14,111
```

---

<b>Note</b>	Verify interfaces by typing “show run interface G1/0/x” from the EXEC mode for each interface.
-------------	--

---

**Step 16** Type: **CTRL-z** to exit global configuration mode.

**Step 17** Type: **copy run start** and press **Enter**

**Step 18** At “Destination filename [startup-config]? Press **Enter**

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- You have entered the Layer 2 commands with the correct values.
- You have saved the configuration to startup-config.

# Task 3: Configure Layer 3 IPv4 Operations

## Activity Procedure

In this task, you will configure the Layer 3 operations for the switch necessary for DHCP and routing. You will need separate subnets for Management, APs and Clients. This will segment our traffic for security, control and routing.

Complete these steps:

**Step 1** Connect to the SW1 switch Console port

**Step 2** Press enter until SW1 prompt appears

**Step 3** Type: **enable** and press **Enter**

**Step 4** Type: in password of **cisco** and press **Enter**

**Step 5** Type: **config term** and press **Enter** to enter global configuration mode

**Note:** Press **Enter** after every command (ex: type: **interface vlan1**)

**Step 6** Remove IP address from vlan1 (we originally configured this in the setup with an IP address, but we are not going to use the default VLAN of 1).

```
SW1(config)# interface vlan1  
SW1(config-if)# no ip address
```

**Step 7** Add management IP address to vlan11. This is the mgt Vlan 11 and you will assign it an IP subnet.

```
SW1(config)# interface vlan11  
SW1(config-if)# ip address 192.168.11.254 255.255.255.0
```

**Step 8** Add IP address to Access Point vlan12. This is the AP Vlan 12 and you will assign it an IP subnet.

```
SW1(config)# interface vlan12  
SW1(config-if)# ip address 192.168.12.254 255.255.255.0
```

**Step 9** Add IP address to Client vlan14. This is the Client Vlan 14 and you will assign it an IP subnet.

```
SW1(config)# interface vlan14  
SW1(config-if)# ip address 192.168.14.254 255.255.255.0
```

---

**Note** Verify VLANs by typing “show run interface vlan 1x” from the EXEC mode for each interface.

---

**Step 10** Enable IP Routing

```
SW1(config)# ip routing
```

**Step 11** Disable IP domain lookups

```
SW1(config)# no ip domain lookup
```

**Step 12** Set a gateway of last resort to go to the **mgt** VLAN address of 192.168.11.1

```
SW1(config)# ip route 0.0.0.0 0.0.0.0 192.168.11.1
```

**Step 13** Define Core Switch as NTP server (need NTP for certificate validation, proper logging timestamps and etc.).

```
SW1(config)# ntp server 172.16.0.2
```

**Step 14** Set excluded DHCP IP addresses (excluding address for DHCP, as some will be statically assigned. Ex: WLC is 192.168.11.5)

```
SW1(config)# ip dhcp excluded-address 192.168.11.1 192.168.11.25
SW1(config)# ip dhcp excluded-address 192.168.12.1 192.168.12.10
SW1(config)# ip dhcp excluded-address 192.168.14.1 192.168.14.10
```

**Step 15** Set management DHCP scope (IP addresses for devices in the mgt VLAN). Default gateway is .254

```
SW1(config)# ip dhcp pool mgt
SW1(dhcp-config)# network 192.168.11.0 255.255.255.0
SW1(dhcp-config)# default-router 192.168.11.254
```

**Step 16** Set Access Point (AP) DHCP scope (IP addresses for devices in the AP VLAN). Default gateway is .254

```
SW1(config)# ip dhcp pool ap
SW1(dhcp-config)# network 192.168.12.0 255.255.255.0
SW1(dhcp-config)# default-router 192.168.12.254
SW1(dhcp-config)# option 43 hex f104.c0a8.0b05
```

---

<b>Note</b>	When DHCP servers are programmed to offer WLAN Controller IP addresses as Option 43 for current Cisco Aironet LAPs, the sub-option TLV (type-length-value) block is defined in this way: <ul style="list-style-type: none"><li>· Type – 0xf1 (decimal 241)</li><li>· Length – Number of controller IP addresses * 4</li><li>· Value – List of the WLC management interfaces,</li></ul>
-------------	--

All values are typically translated to hexadecimal values

Therefore the formula break down for our controller is:

f1 = controller TLV

04 = Length (number of controllers \* 4) (in our case: 1 \* 4 = 4)

c0a8.0b05 = Controller IP address (192.168.11.5 in hex)

---

**Step 17** Set client DHCP scope (IP addresses for devices in the Client VLAN). Default gateway is .254

```
SW1(config)# ip dhcp pool client
SW1(dhcp-config)# network 192.168.14.0 255.255.255.0
SW1(dhcp-config)# default-router 192.168.14.254
```

---

<b>Note</b>	Verify interfaces by typing “show run ip dhcp pool” from the EXEC mode for each interface.
-------------	--

---

**Step 18** Type: **CTRL-z** to exit global configuration mode.

**Step 19** Type: **copy run start** and press **Enter**

**Step 20** At “Destination filename [startup-config]? Press **Enter**

## **Activity Verification**

You have successfully completed this task when you attain this result:

- You have entered the Layer 3 commands with the correct values.
- You have saved the configuration to startup-config.

## **Switch Configuration Example**

This section presents the switch configuration for Pod1 as an example.

### **Lab 3-1 Pod1 – Running Configuration**

**show run brief**

```
Building configuration...

Current configuration : 4062 bytes
!
! Last configuration change at
10:33:32 UTC Fri Jan 8 2016
!
version 15.2
no service pad
service timestamps debug datetime
msec
service timestamps log datetime
msec
no service password-encryption
service compress-config
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-vrf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
```

```

!
enable secret 5
$1$ZXxE$CzU64Pil.6Jj7WRBmHee2/
enable password enablecisco
!
username Cisco123 privilege 15
password 0 Cisco123
no aaa new-model
switch 1 provision ws-c3650-24ps
!
!
!
!
ip routing
!
no ip domain-lookup
ip dhcp excluded-address
192.168.11.1 192.168.11.25
ip dhcp excluded-address
192.168.12.1 192.168.12.10
ip dhcp excluded-address
192.168.14.1 192.168.14.10
!
ip dhcp pool mgt
  network 192.168.11.0
  255.255.255.0
    default-router 192.168.11.254
!
ip dhcp pool ap
  network 192.168.12.0
  255.255.255.0
    default-router 192.168.12.254
    option 43 hex f104.c0a8.0b05
!
ip dhcp pool client
  network 192.168.14.0
  255.255.255.0
    default-router 192.168.14.254
!
!
qos queue-softmax-multiplier 100
vtp mode off
!
!
diagnostic bootup level minimal
spanning-tree mode pvst
spanning-tree extend system-id
hw-switch switch 1 logging onboard
message level 3
!
redundancy
  mode sso
!
!
vlan 11
  name mgt
!
vlan 12
  name AP
!
```

```

vlan 14
  name Client
!
!
class-map match-any non-client-
nrt-class
!
policy-map port_child_policy
  class non-client-nrt-class
    bandwidth remaining ratio 10
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```

interface GigabitEthernet1/0/12
description WLC
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
description to SW2
switchport trunk allowed vlan 11-
14,111
switchport mode trunk
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
description To DC Switch
switchport access vlan 11
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
!
interface Vlan11
ip address 192.168.11.254
255.255.255.0
!
interface Vlan12
ip address 192.168.12.254
255.255.255.0
!
interface Vlan14
ip address 192.168.14.254
255.255.255.0
!
ip forward-protocol nd

```

```
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0
192.168.11.1
!
!
!
!
!
line con 0
exec-timeout 30 0
logging synchronous
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 30 0
password Cisco123
logging synchronous
login
line vty 5
exec-timeout 30 0
password Cisco123
logging synchronous
login
line vty 6 15
password Cisco123
login
!
ntp server 172.16.0.2
wsma agent exec
profile httplistener
profile httpslistener
!
wsma agent config
profile httplistener
profile httpslistener
!
wsma agent filesys
profile httplistener
profile httpslistener
!
wsma agent notify
profile httplistener
profile httpslistener
!
!
wsma profile listener httplistener
transport http
!
wsma profile listener
httpslistener
transport https
!
ap country DE
ap group default-group
end
```

# **Hardware Lab 3: Configuring the Centralized WLAN Deployment**

---

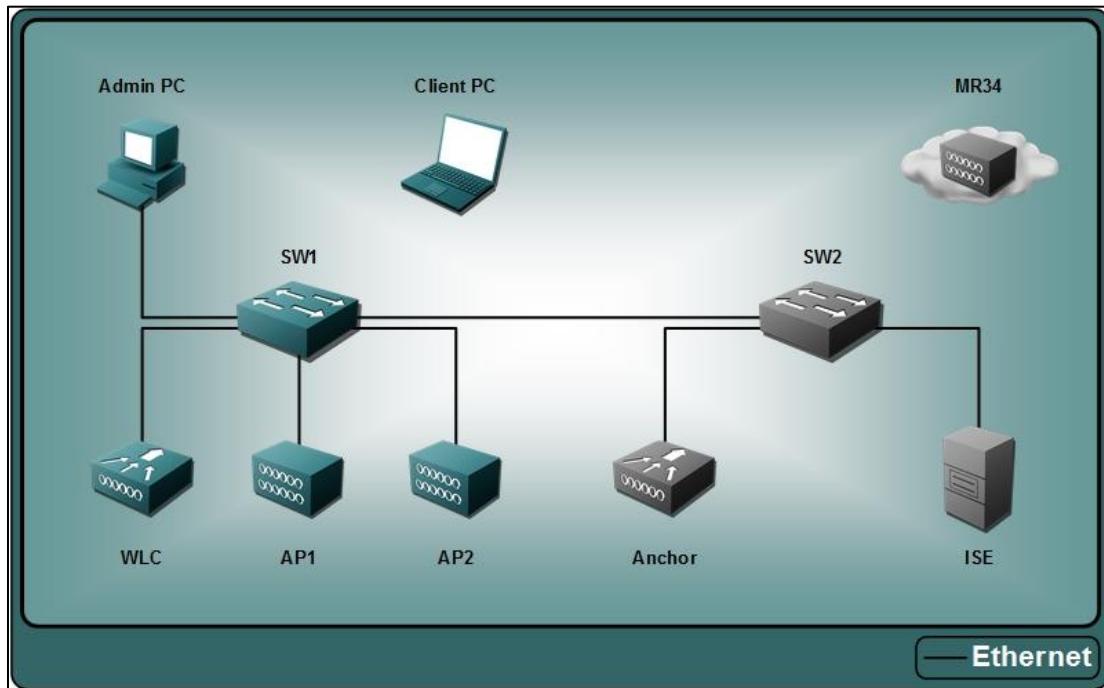
## **Overview**

In this activity, you configure the 2504 WLC to enable centralized WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Login and review basic status information
- Configure the APs and radios
- Create a WLAN and connect a wireless client to it
- Modify additional features for the WLAN
- Verify feature operation

# Visual Objective



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 2504 WLC
- AP 3700i (Centralized AP)

## Device Information

### VLANs and IP Ranges

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

### Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
WLC 2504	192.168.11.5	admin	Cisco123	
Pod 3650 Switch	192.168.11.254	admin	Cisco123	cisco

## RF Channels

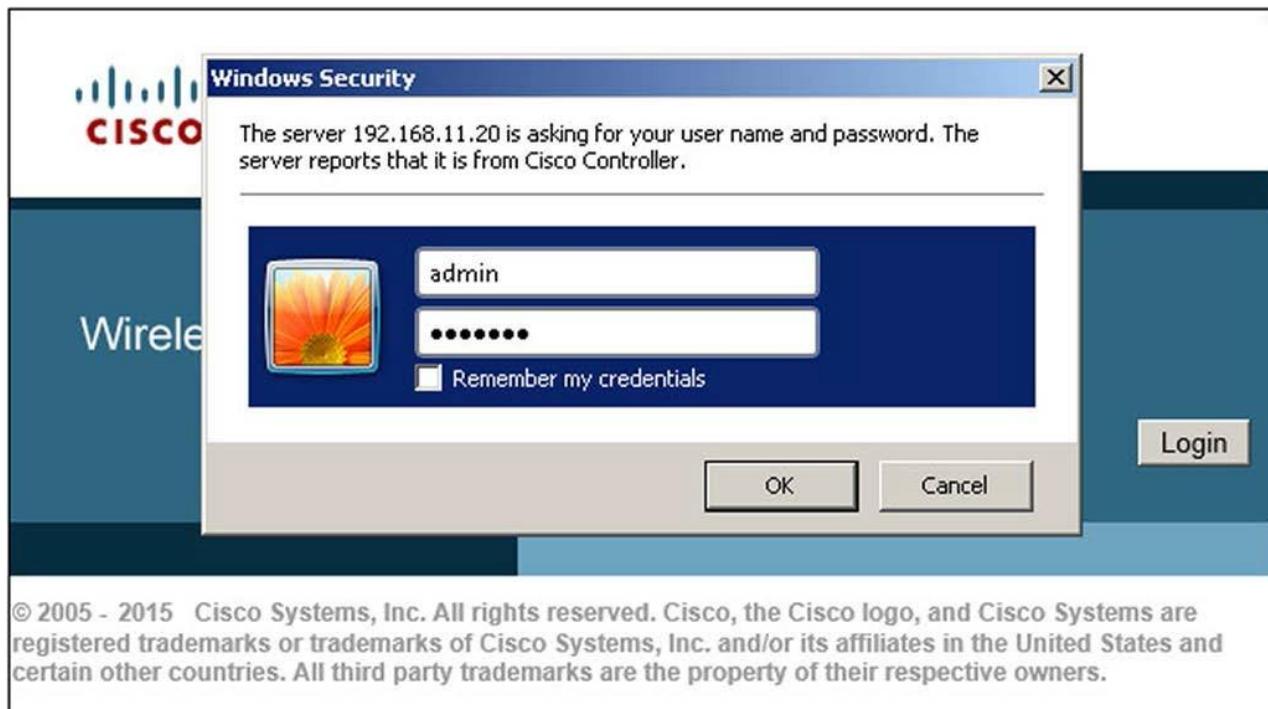
Pod	RF Channel 802.11b/g/n	RF Channel 802.11a/n/ac
1, 9, 17	1	36
2, 10, 18	6	40
3, 11, 19	11	44
4, 12, 20	1	48
5, 13, 21	6	52
6, 14, 22	11	56
7, 15, 23	1	60
8, 16, 24	6	64

## Task 1: Review and Modify Management Access

### ***Activity Procedure***

In this task, you will review and modify management access for the WLC. Complete these steps:

- Step 1** Connect to the Admin PC using the login Administrator / 1234QWer .
- Step 2** Open a web browser (IE or FF)
- Step 3** Type in the address field: **http://192.168.11.5** and press **enter**



**Step 4** Click **Login**.

**Step 5** At the login screen, enter the user name of **admin** and password of **Cisco123** and click **OK**. You will now be at the WES home screen.

**Step 6** Go to the Advanced screen on your next login, click the Gear icon on the top right and from the **Landing Page** drop-down, choose **Monitor Summary**.

The screenshot shows the Cisco 2500 Series Wireless Controller's Monitor Summary dashboard. The top navigation bar includes links for 'Dashboard', 'Logs', 'Statistics', 'Reports', and 'Advanced'. A 'Logout' link is also present. The dashboard features several summary cards: 'Wireless Networks' (1), 'Access Points' (1), 'Active Client Devices' (0 2.4GHz, 0 5GHz), 'Rogues' (0 APs, 0 Clients), and 'Interferers' (0 2.4GHz, 0 5GHz). Below these are sections for 'Top Access Points' (with columns for Description, Volume, and Clients) and 'Top Applications' (empty). Further down are sections for 'Top Operating Systems' and 'Top Client Devices' (with columns for Description, Volume, and % Usage).

---

<b>Note</b>	This new :"Dashboard" allows for quick information and links to the following: Wireless Networks (WLANS menu), Access Points (All AP menu), Active Clients by radio (Monitor Client menu) Rogues (Monitor Rogue AP or Clients) and Interferers by radio (Monitor Interferers menu)
-------------	--

---

**Step 7** Click **Advanced** to go to the **Advanced** screen and **Monitor** menu.



**Step 8** Click on the **Management** menu

- On the left navigation menu – Click **Telnet-SSH**
- Change the drop-down beside **Allow New Telnet Sessions** to **Yes**
  - For security purposes your enterprise, you would probably leave this to “No.”
- Click **Apply** in right corner
  - Apply saves the configuration change as the “running-config”
- Click **Save Configuration** in the top menu and Click **OK** to confirm and then Click **OK** on the Success pop-up.

---

<b>Note</b>	“Save Configuration” saves the running-config to the startup-config. If you use “Apply” and don’t use “Save Configuration”, you will lose any changes on a reset or reboot.
-------------	---

---

**Step 9** On the **Management** menu, select the following:

- On the left navigation menu, click **HTTP-HTTPS**
- Change the **Web Session Timeout** to **60** minutes
- Click **Apply** in right corner

- Click **Save Configuration** in the top menu and Click **OK** to confirm and then Click **OK** on the Success pop-up.

**Note** You will always need to click “Apply” to save the configuration, but you do not have to click “Save Configuration” until you want all changes saved to startup Flash. Just don’t forget to do it.

**Step 10** Click on the **Monitor** menu

- Scroll down to the Access Point Summary section
- You should see one access point

<b>Access Point Summary</b>				
	Total	Up	Down	
802.11a/n/ac Radios	1	● 1	● 0	<a href="#">Detail</a>
802.11b/g/n Radios	1	● 1	● 0	<a href="#">Detail</a>
Dual-Band Radios	0	● 0	● 0	<a href="#">Detail</a>
All APs	1	● 1	● 0	<a href="#">Detail</a>

**Activity Verification**

You have successfully completed this task when you attain this result:

- You have logged on to the GUI interface and made changes
- You have verified that one access point is online.

## Task 2: Review AP Status

### **Activity Procedure**

In this task, you will review the AP status for the 2504 WLC.

Complete these steps:

**Step 1** Connect to the Admin PC

- Step 2** Open an web browser (Internet Explorer or Firefox)
- Step 3** Type in the address field: **http://192.168.11.5** and press **enter**.
- Step 4** Click **Login**.
- Step 5** At the login screen, enter the username of **admin** and password of **Cisco123** and click **OK**.  
You will now be at the **Advanced Monitor Summary** screen
- Step 6** Click on the **Wireless** menu  
You should see one access point and verify:
- IP address is in the **192.168.12.0** range per the switch DHCP
  - PoE Status PoE/Full Power (using 802.3at, this would be 16.8W – below is switch configuration for power)

Interface	Admin	Oper	Power	Device	Class	Max
			(Watts)			
G1/0/1	auto	on	16.0	AIR-CAP3702I-A-K9	4	30.0
G1/0/2	auto	on	16.8	AIR-CAP3702I-A-K9	4	30.0
G1/0/3	auto	on	16.0	AIR-CAP3702I-A-K9	4	30.0
G1/0/4	auto	off	0.0	n/a	n/a	30.0

You can also connect to the Pod Switch and enter the “show cdp neighbor” to verify that the AP is connected to port G1/0/1 and its status.

- Step 7** Click on the **AP name** (MAC address) and view the **General** tab information and verify:
- AP Mode = **Local** and AP Sub Mode = **None**
  - Change AP Name (to easily identify it) to **AP1** and click **Apply** (and **Save Configuration**)
  - Explore the other AP tabs

General	Versions
AP Name: AP1	Primary Software Version: 8.0.120.0
Location: default location	Backup Software Version: 0.0.0.0
AP MAC Address: e4:aa:5d:a0:0e:44	Predownload Status: None
Base Radio MAC: e4:aa:5d:ad:76:50	Predownloaded Version: None
Admin Status: Enable	Predownload Next Retry Time: NA
AP Mode: local	Predownload Retry Count: NA
AP Sub Mode: None	Boot Version: 15.2.4.0
	TOS Version: 15.2(2)1A4#

- Step 8** Take time to explore some of the other menus tabs
- Step 9** Find the following and record the Menu that they were under:

**1** WLAN: Podx\_Open:

---

---

**2** Wireless Clients:

---

---

**3** CDP Interface Neighbors:

---

---

**4** Management Interface:

---

---

**Note** Don't make any configuration changes, unless instructed to do so.

---

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- You have verified that the AP is in Local Mode
- The AP Name is now **AP1**.

## **Task 3: Configure RF Power and Channel**

### ***Activity Procedure***

In this task, you will configure the RF power and channel information for the AP.

**Step 1** Connect to the WLC from the Admin PC

#### **Network Radio Management**

In this section you will modify radios settings (per band) for all APs

**Step 2** Click on the **Wireless** menu and on the left vertical side click on the **arrow** beside the **802.11b/g/n** selection.

- Underneath the **802.11b/g/n** heading, Click **Network**.
- Disable the Data Rates of **1, 2, 5.5, 6, 9, 11** and set **12** to **Mandatory** to improve cell coverage and roaming and click **Apply**.

Wireless

**802.11b/g Global Parameters**

**General**

802.11b/g Network Status	<input checked="" type="checkbox"/> Enabled
802.11g Support	<input checked="" type="checkbox"/> Enabled
Beacon Period (millisecs)	100
Short Preamble	<input checked="" type="checkbox"/> Enabled
Fragmentation Threshold (bytes)	2346
DTPC Support.	<input checked="" type="checkbox"/> Enabled
Maximum Allowed Clients	200
RSSI Low Check	<input type="checkbox"/> Enabled
RSSI Threshold (-60 to -90 dBm)	-80

**CCX Location Measurement**

Mode	<input type="checkbox"/> Enabled
------	----------------------------------

**Data Rates\*\***

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Disabled
11 Mbps	Disabled
12 Mbps	Supported
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

**Apply**

## AP Radio Management

In this section you will modify radios settings (per band) per AP.

- Step 3** Click on the **Wireless** menu and on the left side under **Access Points > Radios**, click on **802.11b/g/n** radio. Scroll to the far right and hover mouse over the blue drop-down arrow.

Wireless

**802.11b/g/n Radios**

Entries 1 - 1 of 1

**Current Filter:** None [Change Filter] [Clear Filter]

AP Name	Radio Slot#	Base Radio MAC	Admin Status	Operational Status	Channel	CleanAir Admin Status	CleanAir Oper Status	Power Level	Antenna
Centralized_AP	0	f0:7f:06:e0:22:a0	Enable	DOWN	1 *	Enable	DOWN	1 *	Internal

- Step 4** Click **Configure**. Under **RF Channel Assignment** click on the **Custom** radio button and manually assign a channel from the drop down, as stated in the Job Aids table .

- Step 5** Under **Tx Power Level Assignment** click on the **Custom** radio button and manually assign the power (5 - lowest) from the drop down.

- 
- Note** The **Current Tx Power Level** setting of "1" represents the maximum conducted power setting for the access point. Each subsequent power level (for example, 2, 3, 4 and so on) represents approximately a 50% (or 3 dBm) reduction in the transmit power from the previous power level. The power will not be allowed to exceed country level regulations.
-

The screenshot shows the Cisco Wireless Configuration interface for AP1. The left sidebar has a tree view with 'Access Points' expanded, showing 'All APs', 'Radios' (with '802.11a/n/ac' and '802.11b/g/n' selected), 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', 'OEAP ACLs', 'Network Lists', '802.11a/n/ac' (selected), 'Network', 'RRM' (with 'RF Grouping', 'TPC', 'DCA', 'Coverage', 'General', 'Client Roaming', 'Media', 'EDCA Parameters', 'DFS (802.11h)', 'High Throughput (802.11n/ac)', 'CleanAir'), and 'Dual-Band Radios'. The main panel has tabs for 'General', 'RF Channel Assignment', '11n Parameters', 'Tx Power Level Assignment', 'CleanAir', 'Antenna Parameters', and 'Performance Profile'. Under 'General', 'AP Name' is AP1, 'Admin Status' is 'Enable', 'Operational Status' is 'UP', and 'Slot #' is 0. Under 'RF Channel Assignment', 'Current Channel' is 6, 'Channel Width' is '20 MHz', 'Assignment Method' is 'Custom', and 'Note' says 'Only Channels 1,6 and 11 are nonoverlapping'. Under 'Tx Power Level Assignment', 'Current Tx Power Level' is 1, 'Assignment Method' is 'Custom', and 'Note' says 'Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients'. Under 'CleanAir', 'CleanAir Capable' is Yes, 'CleanAir Admin Status' is 'Enable', and 'Number of Spectrum Expert connections' is 0. Under 'Antenna Parameters', 'Antenna Type' is 'Internal', and 'Antenna' options A, B, C, and D are checked.

**Step 6** Click **Apply** and confirm with **OK**.

**Step 7** Click on the **Wireless** menu and on the left vertical side click on the **arrow** beside the **802.11a/n/ac** selection.

Underneath the **802.11a/n/ac** heading, Click **Network**.

- You will again verify that the **802.11a/n/ac Network Status** is enabled.
- If you also see under **802.11a Band Status**, that the **Low, Mid and High** bands are enabled.

The screenshot shows the Cisco Wireless Configuration interface for '802.11a Global Parameters'. The left sidebar has a tree view with 'Access Points' expanded, showing 'All APs', 'Radios' (with '802.11a/n/ac' and '802.11b/g/n' selected), 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', 'OEAP ACLs', 'Network Lists', and '802.11a/n/ac' (selected). The main panel has tabs for 'General', 'Data Rates\*\*', '802.11a Band Status', and 'CCX Location Measurement'. Under 'General', '802.11a Network Status' is 'Enabled', 'Beacon Period (millisecs)' is 100, 'Fragmentation Threshold (bytes)' is 2346, 'DTPC Support.' is 'Enabled', 'Maximum Allowed Clients' is 200, 'RSSI Low Check' is 'Enabled', and 'RSSI Threshold (-60 to -90 dBm)' is -80. Under 'Data Rates\*\*', rates 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps have their 'Supported' checkboxes checked. Under '802.11a Band Status', 'Low Band', 'Mid Band', and 'High Band' are all 'Enabled'. Under 'CCX Location Measurement', 'Mode' is 'Enabled'.

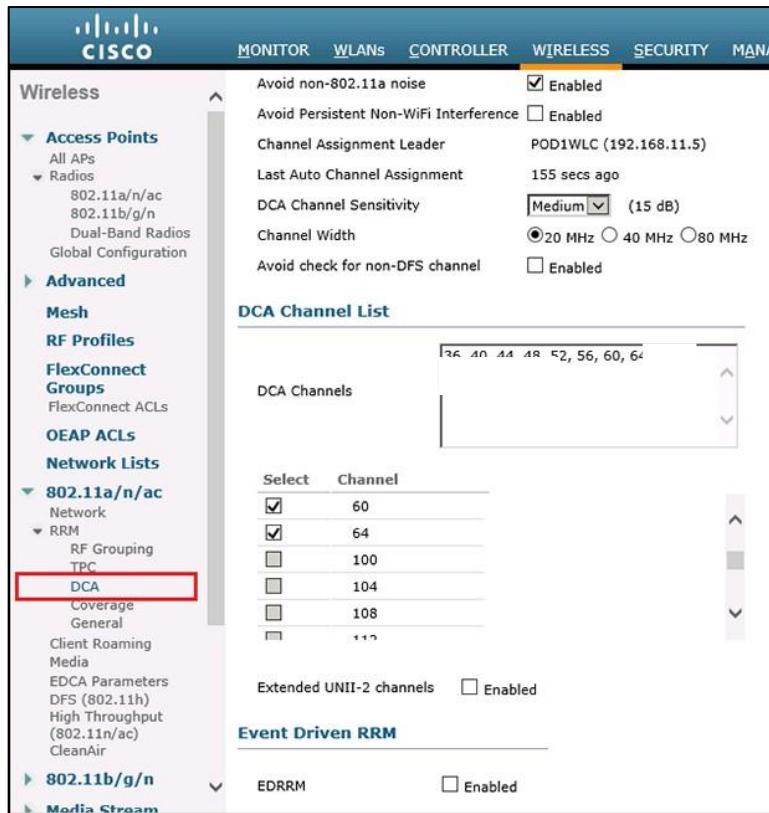
## Network Radio Management

In this section you will again modify radios settings (per band) for all APs.

**Step 8** Click on the **Wireless** menu and on the left side under **802.11a/n/ac > RRM > DCA**.

Notice under Dynamic Channel Assign Algorithm, the default channel width of 20MHz. Also notice under DCA Channel List, the channels that are available for DCA. A little further down, you will notice that the UNII-2 channels are not enabled by default.

- 
- |             |   |
|-------------|---|
| <b>Note</b> | With 802.11ac you could increase the channel width from 20MHz to 40MHz or even 80MHz, as long as you allow for channel spacing. You are not using UNII-2, as it has FCC DFS requirements. |
|-------------|---|
- 



## AP Radio Management

In this section you will again modify radios settings (per band) per AP.

**Step 9** Click on the **Wireless** menu and on the left side under **Access Points > Radios**, click on **802.11a/n/ac** radio. Scroll to the far right and hover mouse over the blue drop-down arrow.

**Step 10** Click **Configure**. Under **RF Channel Assignment** you can click on the **Custom** radio button and manually assign the channel width (20, 40 80 MHz) and the channels from the drop down. This would normally left at **Global** to allow Radio resource management (RRM) to control the channel.

- 
- |             |  |
|-------------|--|
| <b>Note</b> | Notice that channels 120-128 Dynamic frequency Selection (DFS) channels and are unusable. Also note, by using 20 MHz channels, you increase our channel density. |
|-------------|--|
-

The screenshot shows the Cisco Wireless Controller (WLC) configuration interface for a 802.11a/n/ac AP. The left sidebar lists various configuration categories like Access Points, RF Profiles, and Network Lists. The main configuration page has tabs for General, RF Channel Assignment, Tx Power Level Assignment, and Performance Profile. Under RF Channel Assignment, the 'Current Channel' is set to 64 and 'Channel Width' is set to 20 MHz. Under Tx Power Level Assignment, the 'Current Tx Power Level' is 1 and 'Assignment Method' is set to 'Custom'. A note in the Performance Profile section states: 'Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.'

- Step 11** Under **RF Channel Assignment**, click on the **Custom** radio button and manually assign the channel from the drop down as stated in the Job Aids table. Click **Apply** and **OK**.
- Step 12** Under **Tx Power Level Assignment**, click on the **Custom** radio button and manually assign the power to the highest number available from the drop down (lowering the TX power). This would normally left at **Global** to allow Radio resource management (RRM) to control the channel.
- Step 13** Click **Apply** and then **Save Configuration**.

## Activity Verification

You have successfully completed this task when you attain this result:

- You have configured the 2.4 GHz radio channel and power setting according to the instructions.
- You have configured the 5 GHz radio channel and power setting according to the instructions.

## Task 4: Configure a WLAN

### Activity Procedure

In this task, you will configure WLAN for the AP.

Complete these steps:

- Step 1** Connect to the WLC from the Admin PC.

- Step 2** Click on the **Controller** menu.

#### Add a Dynamic Interface

You will add a dynamic interface for the Clients to get an IP address.

**Step 3** On the left side, click on **Interfaces**.

Controller							Save Config
General		Interfaces					
Inventory	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address	
Interfaces	management	11	192.168.11.5	Static	Enabled	::/128	
Interface Groups	virtual	N/A	192.0.2.1	Static	Not Supported		
Multicast							

**Step 4** On the top right side, click **New**.

**Step 5** For the **Interface Name**, enter **Client** and for the **VLAN Id**, enter **14**.

Controller

Interfaces > New

General	Interface Name	Client
Inventory	VLAN Id	14
Interfaces		x
Interface Groups		

**Step 6** Click **Apply**.

**Step 7** On the next page, under **Physical Information**, enter the following:

- Port Number: **1** (port connected to switch)
- Enabled Dynamic AP Management: **Unchecked**

**Step 8** Under **Interface Address**, enter the following:

- IP Address: **192.168.14.5**
- Netmask: **255.255.255.0**
- Gateway: **192.168.14.254**

**Step 9** Under DHCP Information, enter the following:

- Primary DHCP Server: **192.168.14.254**

---

**Note** DHCP configured on switch for client VLAN

---

<b>Physical Information</b>	
Port Number	<input type="text" value="1"/>
Backup Port	<input type="text" value="0"/>
Active Port	0
Enable Dynamic AP Management <input type="checkbox"/>	
<b>Interface Address</b>	
VLAN Identifier	<input type="text" value="14"/>
IP Address	<input type="text" value="192.168.14.5"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.14.254"/>
<b>DHCP Information</b>	
Primary DHCP Server	<input type="text" value="192.168.14.254"/> <input type="button" value="X"/>
Secondary DHCP Server	<input type="text"/>
DHCP Proxy Mode	<input type="button" value="Global"/> <input checked="" type="checkbox"/>
Enable DHCP Option 82 <input type="checkbox"/>	
<b>Access Control List</b>	
ACL Name	<input type="text" value="none"/> <input type="button" value="▼"/>
<b>mDNS</b>	
mDNS Profile	<input type="text" value="none"/> <input type="button" value="▼"/>

**Step 10** Click **Apply** and **OK**.

**Step 11** Click **Back** at the top right and view the newly created interface.

### Modify the WLAN

You will modify the WLAN of Podx\_Open.

The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar includes links for MONITOR, WLANs (which is highlighted in orange), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the far right, there is a 'Save Configuration' button. The left sidebar has a tree view with 'WLANS' expanded, showing 'WLANS' and 'Advanced'. The main content area is titled 'WLANS' and displays a table with one row. The table columns are: WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. The single entry is: WLAN ID 1, Type WLAN, Profile Name Pod1\_Open, WLAN SSID Pod1\_Open, Admin Status Enabled, and Security Policies [WPA2][Auth(802.1X)]. There are also 'Change Filter' and 'Clear Filter' buttons above the table, and a 'Create New' button with a dropdown and a 'Go' button to its right.

**Step 12** Click on the top menu of WLANs.

---

**Note** Notice the default security is WPA2Auth /802.1X.

---

**Step 13** Click on the **WLAN ID (1)** that was created at the time of install.

**Step 14** Verify the following under the General tab:

- Profile name: **Podx\_Open** (naming convention is Pod number and security type)
- Status: **Enabled**

- Radio Policy is set to all by default; you could specify this WLAN for specific radios (802.11a only, 802.11a/g only and etc.)
- Broadcast SSID: **Enabled**
- Change the **Interface/Interface Group** dropdown to **Client** to match the dynamic interface that was just created to segment our traffic and get the proper DHCP scope

The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar includes links for MONITOR, WLANS (which is highlighted), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a sidebar under 'WLANS' shows 'WLANS' and 'Advanced'. The main content area is titled 'WLANS > Edit 'Pod1\_Open''. Below this, there are tabs for General, Security (which is selected), QoS, Policy-Mapping, and Advanced. The 'General' tab displays fields for Profile Name (Pod1\_Open), Type (WLAN), SSID (Pod1\_Open), and Status (Enabled). The 'Security' tab displays Security Policies ([WPA2][Auth(802.1X)]), a note about modifications appearing after applying changes, and settings for Radio Policy (All), Interface/Interface Group (client), Multicast Vlan Feature (Enabled), Broadcast SSID (Enabled), and NAS-ID (POD1WLC).

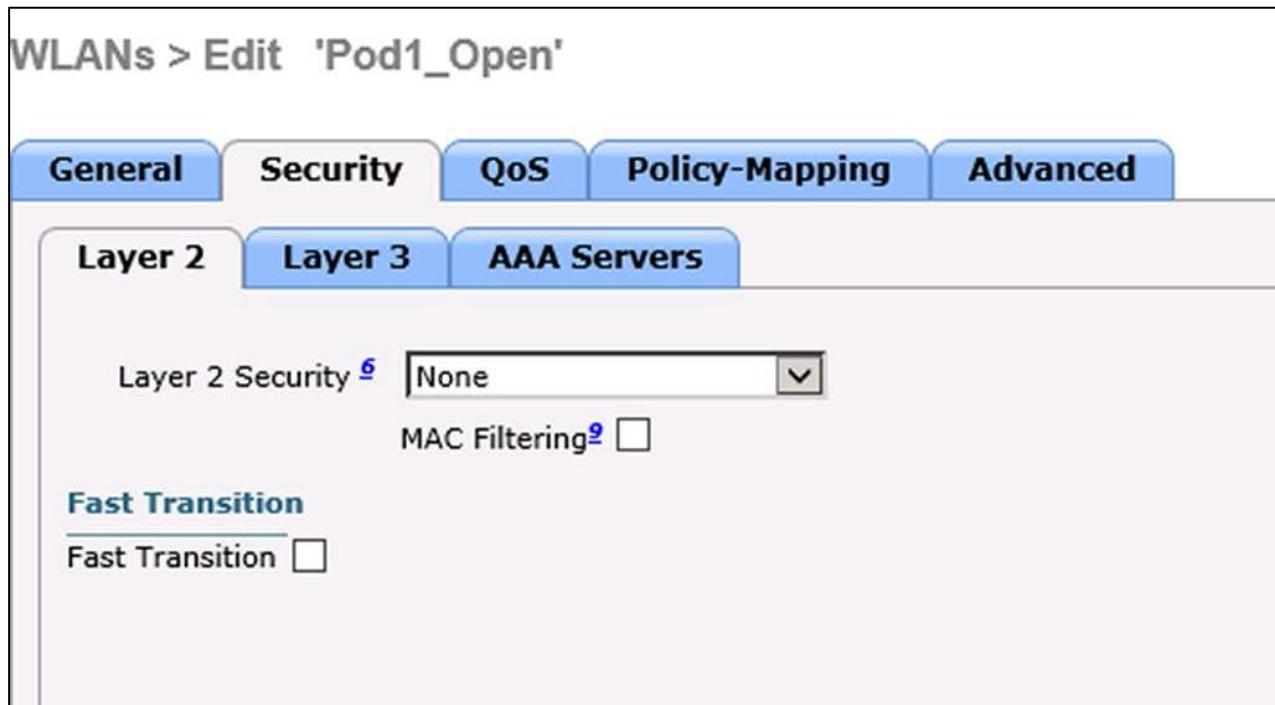
### Set Security for Open Authentication

This SSID is “open” and will have no layer 2 security (like WPA2-PSK) or layer 3 security (like Web-Auth).

**Step 15** Change the following under the **Security** tab:

- **Layer 2 > Layer 2 Security** on dropdown is **None** (open)
- **Layer 3 > Layer 3 Security** on dropdown is **None** (open)

**Step 16** Click **Apply** and **Save configuration**.



## Activity Verification

You have successfully completed this task when you attain this result:

- Created a new Client interface with the specified settings.
- Modified the existing Podx\_Open WLAN to use the new interface and have Open authentication.
- Disabled Aironet IE for the WLAN to lessen compatibility issues with the wireless clients for this WLAN.

## Task 5: Enable Additional Features

### Activity Procedure

In this task, you will configure the WLC for additional features. Complete these steps:

**Step 1** Connect to the WLC from the Admin PC

#### Enable Band Select

Since our client and AP have dual band radios, we are going to enable Band Select to “move the client to 5 GHz band.

**Step 2** Click on the top menu for **Wireless**.

**Step 3** On the left side Click on the arrow beside **Advanced** and then choose **Band Select**.

The screenshot shows the Cisco Wireless Controller interface. The top navigation bar includes icons for MONITOR, WLANs, CONTROLLER, and WIRELESS. The WIRELESS tab is selected. On the left, a sidebar under 'Wireless' has sections for 'Access Points' (All APs, Radios, 802.11a/n/ac, 802.11b/g/n, Dual-Band Radios, Global Configuration) and 'Advanced' (Load Balancing, Band Select). The 'Band Select' section is currently active. The main content area displays configuration parameters: Probe Cycle Count, Scan Cycle Period Threshold (1-1000 milliseconds), Age Out Suppression (10-200 seconds), Age Out Dual Band (10-300 seconds), Acceptable Client RSSI (dBm), and Acceptable Client Mid RSSI (dBm). A note at the bottom states: *\* Band Select is configurable per WLAN.*

Parameter	Description
Probe Cycle Count	Not explicitly listed in the table, implied by Scan Cycle Period Threshold.
Scan Cycle Period Threshold (1-1000 milliseconds)	Scan cycle period threshold.
Age Out Suppression (10-200 seconds)	Age out suppression time.
Age Out Dual Band (10-300 seconds)	Age out dual band time.
Acceptable Client RSSI (dBm)	Acceptable client RSSI range.
Acceptable Client Mid RSSI (dBm)	Acceptable client mid RSSI range.

**Step 4** Here you can observe the global timing parameters that affect **Band Select**.

**Enable Band Select on the WLAN**

Band Select is enabled per WLAN.

**Step 5** Click on top menu for **WLANs** and then Click on the **WLAN ID** of the newly created WLAN (Podx\_Open).

**Step 6** Click on the **Advanced** tab and then under **Load Balancing and Band Select**, check the box for **Client Band Select**.

WLANS > Edit 'Pod1\_Open'

General	Security	QoS	Policy-Mapping	Advanced
Layer2 Acl	None			
P2P Blocking Action	Disabled			
Client Exclusion <sup>3</sup>	<input checked="" type="checkbox"/> Enabled <input type="text" value="60"/> Timeout Value (secs)			
Maximum Allowed Clients <sup>8</sup>	<input type="text" value="0"/>			
Static IP Tunneling <sup>11</sup>	<input type="checkbox"/> Enabled			
Wi-Fi Direct Clients Policy	Disabled			
Maximum Allowed Clients Per AP Radio	<input type="text" value="200"/>			
Clear HotSpot Configuration	<input type="checkbox"/> Enabled			
Client user idle timeout(15-1000000)	<input type="checkbox"/>			
Client user idle threshold (0-10000000)	<input type="text" value="0"/> Bytes			
Radius NAI-Realm	<input type="checkbox"/>			
<b>Off Channel Scanning Defer</b>	Scan Defer Priority <b>0 1 2 3 4 5 6 7</b> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>			
<b>Management Frame Protection (MFP)</b> MFP Client Protection <sup>4</sup> <input type="checkbox"/> Optional				
<b>DTIM Period (in beacon intervals)</b> 802.11a/n (1 - 255) <input type="text" value="1"/> 802.11b/g/n (1 - 255) <input type="text" value="1"/>				
<b>NAC</b> NAC State <input type="checkbox"/> None				
<b>Load Balancing and Band Select</b> Client Load Balancing <input type="checkbox"/> Client Band Select <input checked="" type="checkbox"/>				
<b>Passive Client</b> Passive Client <input type="checkbox"/>				
<b>Voice</b> Media Session Snooping <input type="checkbox"/> Enabled Re-anchor Roamed Voice Clients <input type="checkbox"/> Enabled				

**Step 7** Click Apply and OK and OK.

**Enable CleanAir on the WLAN for 5GHz**

CleanAir is enabled globally per radio band.

**Step 8** Click on top menu for Wireless.

**Step 9** On the left side, click on the arrow beside **802.11/a/n/ac** and then select CleanAir. Here you will enable the **CleanAir** feature for our network.

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The WIRELESS tab is selected. On the left, a sidebar menu lists various wireless categories like Access Points, Advanced, Mesh, RF Profiles, FlexConnect Groups, and OEAP ACLS. The main panel title is "802.11a > CleanAir". Under "CleanAir Parameters", the "CleanAir" checkbox is checked. Other options include "Report Interferers" (checked) and "Persistent Device Propagation" (unchecked). The "Interferences to Ignore" section is empty. The "Interferences to Detect" section lists "TDD Transmitter", "Jammer", "Continuous Transmitter", "DECT-like Phone", and "Video Camera". In the "Trap Configurations" section, "Enable AQI(Air Quality Index) Trap" is checked with a threshold of 35. "Enable trap for Unclassified Interferences" is unchecked with a threshold of 20. "Enable Interference For Security Alarm" is checked. The "Do not trap on these types" section lists "TDD Transmitter", "Continuous Transmitter", "DECT-like Phone", "Video Camera", and "SuperAG". The "Trap on these types" section lists "Jammer", "WiFi Inverted", and "WiFi Invalid Channel".

- Step 10** Under CleanAir parameters, check the **Enabled** box beside **CleanAir** to enable it.
- Step 11** The **Report Interferers** should already be checked (to report any detected sources of interference).
- Step 12** Observe the list of **Interferences to Detect** to see a list of what can be detected.
- Step 13** Also view the trap conditions for the **Air Quality Index (AQI)**.
- Step 14** Click **Apply**.

The screenshot shows the Cisco Wireless configuration interface for AP configuration. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The WIRELESS tab is selected. The left sidebar menu lists Access Points, Advanced, Mesh, RF Profiles, FlexConnect Groups, OEAP ACLS, Network Lists, 802.11a/n/ac, 802.11b/g/n, Media Stream, and Application Visibility. The main panel title is "802.11a/n Cisco APs > Configure". The "General" section includes fields for AP Name (Centralized\_AP), Admin Status (Enable), Operational Status (UP), and Slot # (1). The "11n Parameters" section includes "11n Supported" (Yes). The "CleanAir" section includes "CleanAir Capable" (Yes) and "CleanAir Admin Status" (Enable). A note states: "\* CleanAir enable will take effect only if it is enabled on this band." The "RF Channel Assignment" section shows Current Channel (36) and Channel Width (20 MHz). A note says: "\* Channel width can be configured only when channel configuration is in custom mode." The "Tx Power Level Assignment" section shows Current Tx Power Level (5) and Assignment Method (Custom, value 5). The "Performance Profile" section is partially visible.

- Step 15** CleanAir will be automatically enabled for APs that support it. To verify this, go to **Wireless > Access Points > Radios > 802.11a/n/ac** (or 802.11b/g/n) and click **Configure** on the drop down for that AP's radio. Under CleanAir, you will see if it is capable and its status.

## **Verify CleanAir on the WLAN for 2.4GHz**

Make the same changes for the 2.4GHz radio as you did for the 5GHz radio

**Step 16** Go to **Wireless > 802.11b/g/n > CleanAir** and repeat the steps 10 – 14.

## **Enable Profiling on the WLAN**

Profiling is enabled pre WLAN. You will do this to see the client types when they connect.

**Step 17** Click on top menu for **WLANs** and then Click on the **WLAN ID** of the newly created WLAN (Podx\_Open).

**Step 18** Click on the **Advanced** tab and then under **Local Client Profiling**, check the box for:

- **DHCP Profiling** and read the pop-up and click **OK**
- **HTTP Profiling**

**Step 19** Click **Apply** and **OK** and then **Save Configuration**.

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- Verified Band Select global settings
- Enabled Band Select on the WLAN (Podx\_Open).
- Enabled CleanAir for each radio band.
- Enabled Local Profiling on the WLAN (Podx\_Open).

# **Task 6: Associate the Client**

## ***Activity Procedure***

In this task, you will configure the Client PC to connect to the WLAN.

Complete these steps:

**Step 1** Connect to the Client PC.

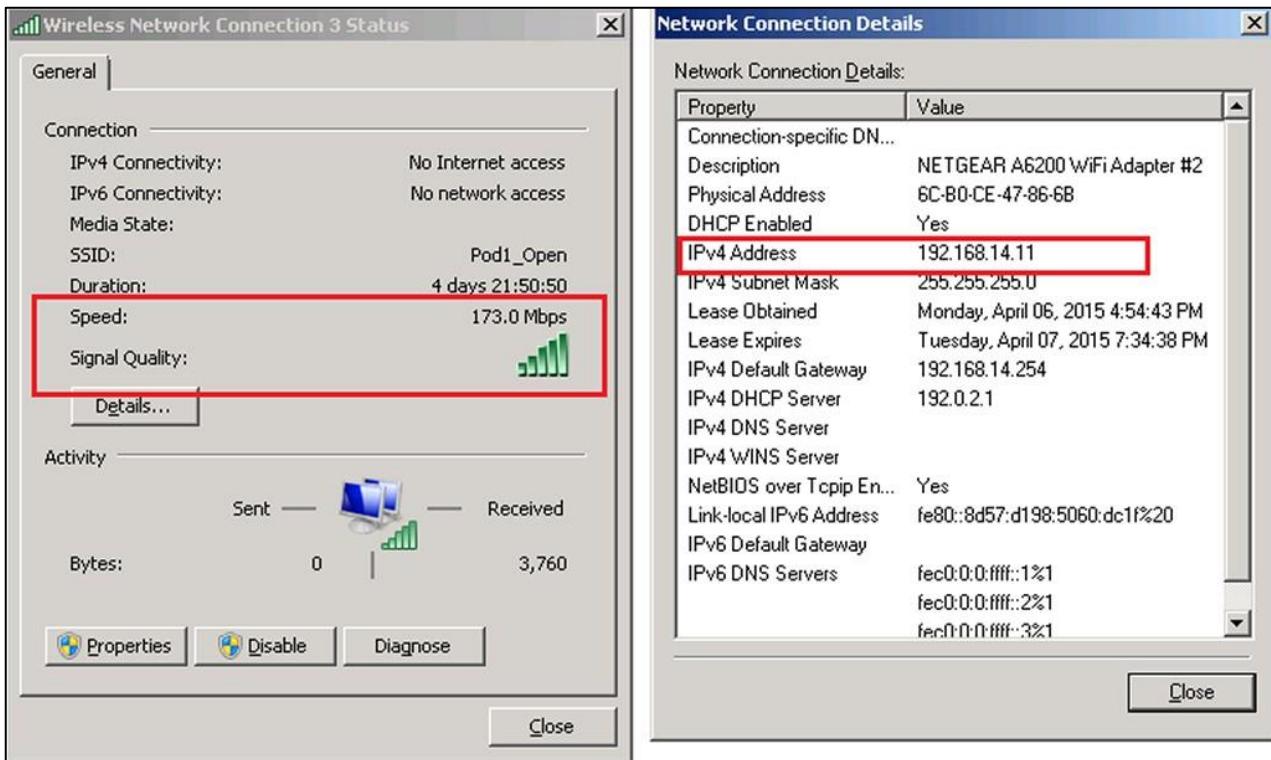
**Step 2** Click on the **Wireless** icon in the bottom right tray.

**Step 3** Click on **Podx\_Open** and then click **Connect**.

**Step 4** After connection (there may not be internet connectivity at this time), Click on the **Wireless** icon in the tray again.

**Step 5** Right click on the **Podx\_Open** WLAN and choose **Status**.

**Step 6** Observe your **Speed** and **Signal Quality**.



- Step 7** Click on the **Details** button ion the **Status** screen.
- Step 8** You should have an IP address in the **192.168.14.0** network. You have an IP in this subnet because the Podx\_Open WLAN Interface was “Client”
- Step 9** Connect to the WLC from the Admin PC
- Step 10** Click on top menu for **Monitor**.
- Step 11** On the left side, click **Clients**.

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	WGB	Device Type
6c:b0:ce:47:86:6b	192.168.14.11	Centralized_AP	Podx_Open	Podx_Open	Unknown	802.11ac	Associated	Yes	1	1	No	Microsoft-Workstation

Here is some of the information that can be seen: Client MAC, IP Address, WLAN Profile, Protocol, Status, and Device Type.

- Step 12** Click on the Client’s **MAC address** to see the information for the **General** tab.
- Step 13** Click on **Link Test** and view the results.
- Step 14** Click **Back** to return to the **Monitor > Clients** screen
- Step 15** You should have noticed on the far right under Device Type, that your client type was detected (Microsoft Workstation). This is available because Local Profiling was turned on. Go back to the left side (still on Monitor menu) and click on **Local Profiling** to see the **Device Stats**.

## Activity Verification

You have successfully completed this task when you attain this result:

- Associated the wireless client with the new WLAN.
- Verified on the client on PC side (IP address, signal and speed).

- Verified on the WLC side, the detailed information about the client, including their device type.

## Task 7: Review CleanAir

### Activity Procedure

In this task, you will review the CleanAir reports.

- Step 1** Connect to the WLC from the Admin PC.
- Step 2** Click on top menu for **Monitor**.
- Step 3** On the left side, click on the arrow beside **Cisco CleanAir**.
- Step 4** Under **802.11b/g/n** (or 802.11a/n/ac), click on **Interference Devices**.

AP Name	Radio Slot#	Device Type	Affected Channel	Detected Time	Severity	Duty Cycle (%)	RSSI	DevID	ClusterID
Centralized_AP	0	Continuous TX	1	Mon Apr 6 22:50:05 2015	12	100	-85	0x3001	b0:3c:20:00:00:00

- 
- Note** Optionally, the instructor may turn on an interfering device to display information in the report. It will show up in the 2.4GHz space.
- 

- Step 5** Hover the cursor over the **blue arrow** on the right side and choose **AQ Graph**.

The screenshot shows the Cisco CleanAir Radio Monitoring Rapid Update interface. The left sidebar has a tree view with nodes like 'Summary', 'Access Points', 'Cisco CleanAir' (expanded to show '802.11a/n/ac' and '802.11b/g/n' sub-nodes), 'Statistics', 'CDP', 'Rogues', 'Clients', 'Sleeping Clients', 'Multicast', 'Applications', and 'Local Profiling'. The main content area has a title '802.11b > Centralized\_AP > CleanAir > Radio Monitoring Rapid Update'. Below it, there's a table titled 'Active Interferers' with columns: Interferer Type, Affected Channel, Detected Time, Severity, Duty Cycle(%), RSSI(dBm), DevID, and ClusterID. The table lists three entries: 'Continuous TX' on channel 1 at Mon Apr 6 22:50:05 2015 with severity 12, duty cycle 100, RSSI -85, DevID 0x3001, ClusterID b0:3c:20:00:00:c; and two 'BLE Beacon' entries on unknown channels at Mon Apr 6 22:54:57 2015 and Mon Apr 6 22:55:01 2015, both with severity 0, duty cycle 0, RSSI -70/-71, DevID 0x3002/0x3003, and ClusterID b0:3c:20:00:00:c. Below the table is a chart titled '1. Air Quality' showing air quality levels from 40 to 100, with a large blue bar indicating a value around 60.

**Step 6** You will see the **Active Interferers** and **Air Quality** graphs. Click **Back** at the top right of the page.

The screenshot shows the Cisco CleanAir Air Quality Report interface. The left sidebar has a tree view with nodes like 'Summary', 'Access Points', 'Cisco CleanAir' (expanded to show '802.11a/n/ac' and '802.11b/g/n' sub-nodes), 'Statistics', 'CDP', 'Rogues', 'Clients', 'Sleeping Clients', 'Multicast', 'Applications', and 'Local Profiling'. The main content area has a title '802.11b/g/n Cisco APs > Air Quality Report'. It shows a table with columns: AP Name, Radio Slot#, Channel, Average AQ, Minimum AQ, Interferer, and DFS. There is one entry for 'Centralized\_AP' on channel 1 with average AQ 64, minimum AQ 64, 1 interferer, and DFS No.

**Step 7** Under **802.11b/g/n** (or 802.11a/n/ac), click on **Air Quality Report**.

**Step 8** Hover the cursor over the **blue arrow** on the right side and choose **AQ Graph** to view the Air Quality graphs.

**Step 9** To see the **Worst Air Quality Report**, go to **Monitor > Cisco CleanAir > Worst Air Quality Report**. This will show the Air Quality of both bands.

**Step 10** Notice that the 5GHz band has less interference

## Activity Verification

You have successfully completed this task when you attain this result:

- Review the CleanAir interfering devices and CleanAir AQ reports.

## Task 8: Disassociate the Client

### ***Activity Procedure***

In this task, you will configure the Client PC to disconnect from the WLAN.

Complete these steps:

**Step 1** Connect to the Client PC.

**Step 2** Click on the **Wireless** icon in the bottom right tray.

**Step 3** Right click on **Podx\_Open** and choose **Disconnect**.

**Step 4** Click on the **Wireless** icon in the bottom right tray.

**Step 5** At the bottom, click on **Open Network and Sharing Center**.

**Step 6** On the left side, click on **Manage Wireless Networks**.

**Step 7** Delete any network profiles and close all open dialog windows.

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- Disconnected the wireless client from the WLAN

# **Hardware Lab 4: Configuring IPv6 Operation in a Centralized WLAN Deployment**

---

## **Overview**

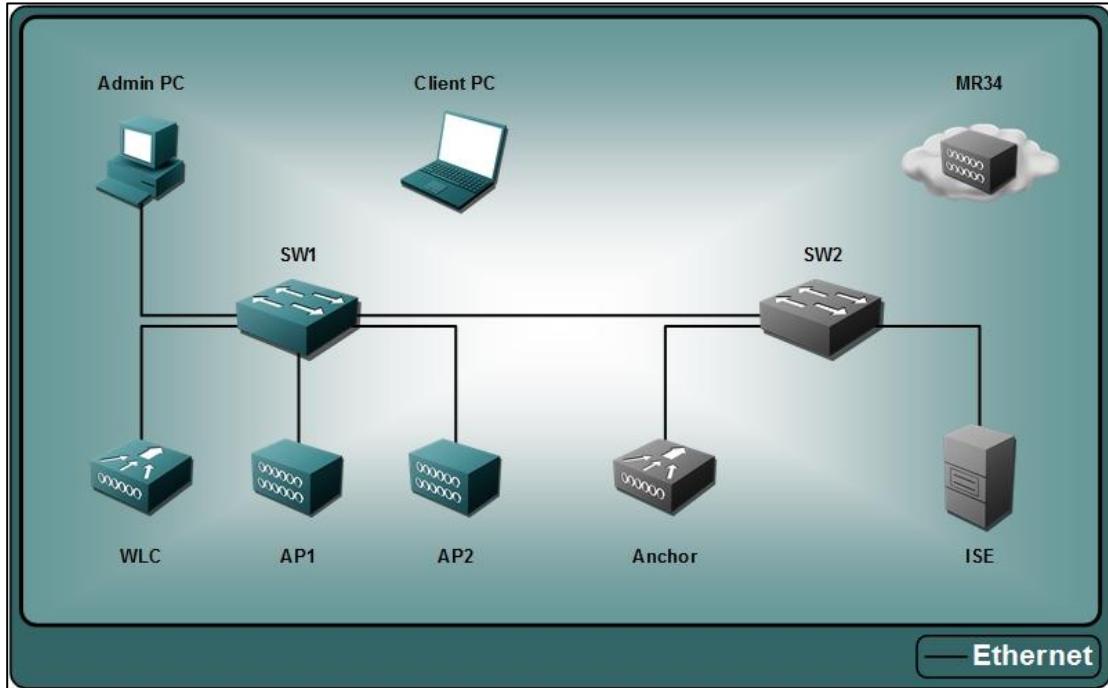
In this activity, you configure IPv6 in a centralized WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Enable the WLC and Switch for IPv6
- Verify IPv6 operation for wired and wireless operation

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 3650 switch
- Pod 2504 WLC
- AP 3700i (Centralized AP)

## VLANs and IP Ranges

### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## IPv6 Addresses

Interface	IPv6 Address	Mask	Link Local
Vlan 11	2001:0db8::1:a::1	/64	fe80::1
Vlan 14	2001:0db8:1:e::1	/64	fe80::1
WLC 2504 Management	2001:0db8:1:a::2	/64	fe80::1
AP Multicast Group	ff1e::239:100:100:94	/16	none

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
WLC 2504	192.168.11.5	admin	Cisco123	
Pod 3650 Switch	192.168.11.254	admin	Cisco123	cisco

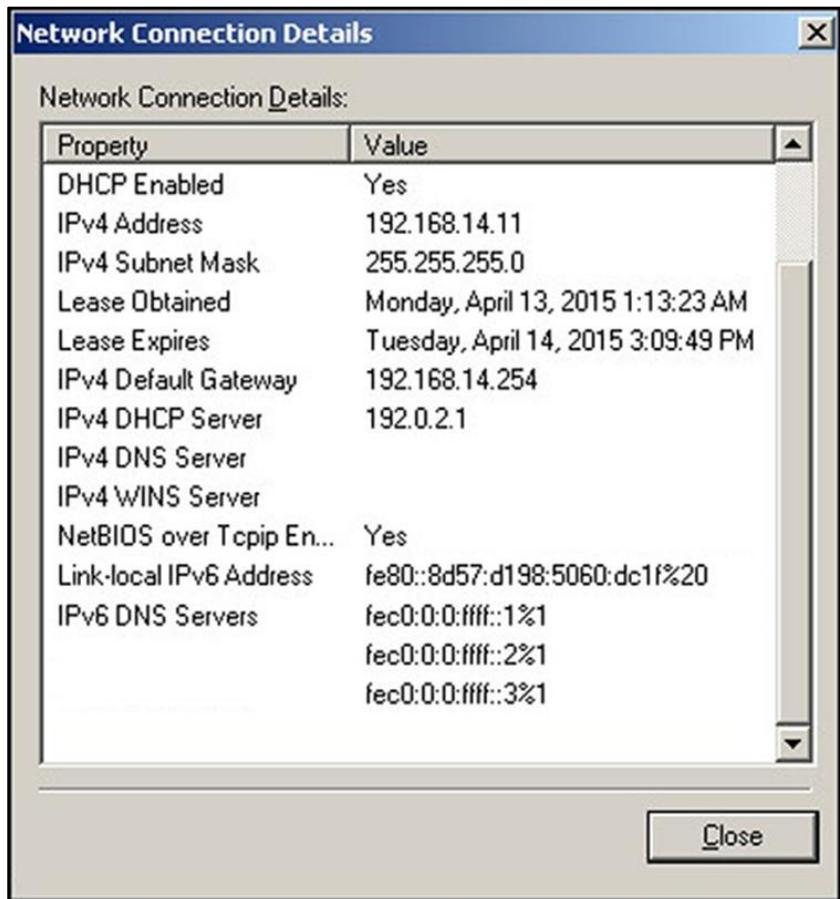
## Task 1: Review Client Association before IPv6 Configuration

### ***Activity Procedure***

In this task, you will review the client's association and IP connectivity before the IPv6 configuration.

Complete these steps:

- Step 1** Connect to the Client PC.
- Step 2** Click on the **Wireless** icon in the bottom right tray.
- Step 3** Click on **Podx\_Open** and then click **Connect**.
- Step 4** After connection (there may not be internet connectivity at this time), Click on the **Wireless** icon in the tray again.
- Step 5** Right Click on the **Podx\_Open** WLAN and choose **Status**.
- Step 6** Click on the **Details** button on the **Status** screen.
- Step 7** You should have an IPv4 address in the **192.168.14.0** network.
- Step 8** You should also have a **link-local IPv6 address** listed (remember the link-local is self-assigned and the prefix is **FE80:** and no unique global address has been defined yet).



#### Verify IPv6 from the WLC 2504

- Step 9** Connect to the WLC from the Admin PC.
- Step 10** Click on the top menu for **Monitor**.
- Step 11** On the left side, click **Clients**.
- Step 12** Notice under the **IP Address** column that your client only has an IPv4 address.
- Step 13** Click on the **MAC address** of your client.
- Step 14** Here you will see the IPv4 address (matches client PC) and the link-local IPv6 address (matches client PC).

**Clients > Detail**

**Max Number of Records**

**General** **AVC Statistics**

**Client Properties**

MAC Address	6c:b0:ce:47:86:6b
IPv4 Address	192.168.14.13
IPv6 Address	fe80::8d57:d198:5060:dc1f,

**Step 15** No Global IPv6 addresses are available for the client, as the IPv6 configuration has not been implemented yet.

---

**Note** The link-local address is assigned by the client adapter because the IPv6 protocol was enabled on the client PC.

---

**Step 16** Go to the client PC and disconnect the client from the WLAN Podx\_Open. (right click on WLAN and select Disconnect).

**Step 17** Go to the Admin PC and remove the client (**Monitor > Client** and **Remove** from the dropdown).

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Associated the wireless client with the WLAN and verified the wireless client's IP connectivity on the client and on the WLC.
- Disconnected the wireless client from the WLAN and removed them from the WLC.

# Task 2: Enable IPv6 Infrastructure

## Activity Procedure

In this task, you will enable the IPv6 Infrastructure on the SW1 and the 2504 WLC.

Complete these steps:

- Step 1** Connect to the SW1 console port.
- Step 2** Press **Enter** until prompt appears.
- Step 3** Login with the enable password of **cisco**.
- Step 4** Go to global configuration by typing **config term** and **Enter**.
- Step 5** The switch is not going to use DHCPv6 for IPv6 addresses, but SLAAC.
- Step 6** First you need to assign a global unicast IPv6 address and a link-local address for the management VLAN (enables SLAAC for the management VLAN). Type each command followed by **Enter**:
  - **int vlan 11**
  - **ipv6 address 2001:0db8:1:a::1/64** (1:a hex subnet could be used to match decimal IPv4 subnet (.11))
  - **ipv6 address fe80::1 link-local** (easy static address assignment)
- Step 7** Now you need to assign a global unicast IPv6 address and a link-local address for the client VLAN (enables SLAAC for the client VLAN). Type each command followed by **Enter**:
  - **int vlan 14** (where x=pod)
  - **ipv6 address 2001:0db8:1:e::1/64** (1:e hex subnet could be used to match decimal IPv4 subnet .14)
  - **ipv6 address fe80::1 link-local** (easy static address assignment)
- Step 8** Type: **Control-c** to return to the enable prompt.
- Step 9** Verify that the addresses for the VLANS are correct, by entering the following:
  - **show run interface vlan 11**
  - **show run interface vlan 14**
- Step 10** Go to global configuration by typing **config term** and **Enter**.
- Step 11** Finally, you need to configure the switch for IPv6 Unicast Routing to enable the forwarding of IPv6 unicast data packets. Configure the switch for unicast routing, by typing, **ipv6 unicast-routing**.
- Step 12** Enter **Control-c** to return to the enable prompt.
- Step 13** Verify the switch configuration, by typing the **show run brief** command.

```
!
!
ipv6 unicast-routing
vtp mode off
!
!
interface Vlan11
 ip address 192.168.11.254 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:1:A::1/64
!
interface Vlan12
 ip address 192.168.12.254 255.255.255.0
!
interface Vlan14
 ip address 192.168.14.254 255.255.255.0
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:1:E::1/64
!
```

**Step 14** Type Write and Enter to save the configuration.

#### Configure IPv6 on the WLC 2504

Here you will enable the WLC for IPv6 Infrastructure mode.

**Step 15** Connect to the WLC from the Admin PC to make IPv6 changes to the WLC

**Step 16** Go to the **Controller > Interfaces**.

**Step 17** Click on the **Management** interface and enter the following:

- IPv6 Address: **2001:0db8:1:a::2**
- Prefix Length: **64**
- IPv6 Gateway: **fe80::1**
- Click **Apply** and **OK** to PI warning pop-up.
- Click **OK** to WLAN disruption warning pop-up.

Interface Address	
VLAN Identifier	<input type="text" value="11"/>
IP Address	<input type="text" value="192.168.11.5"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.11.254"/>
IPv6 Address	<input type="text" value="2001:db8:1:a::2"/>
Prefix Length	<input type="text" value="64"/>
IPv6 Gateway	<input type="text" value="fe80::1"/>
Link Local IPv6 Address	<input type="text" value="fe80::1ede:a7ff:fe06:3c20/64"/>

**Step 18** Verify on the **Controller > Interfaces** that the management VLAN has an IPv6 address.

**Step 19** Click on the **Controller > Interface > client interface** and you will notice that there is not a place for an IPv6 address because it is a Dynamic Interface.

You now need to set some Global IPv6 configurations.

---

<b>Note</b>	Unlike previous versions of releases, IPv6 Unicast traffic support does not mandate that “Global Multicast Mode” be enabled on the controller. IPv6 Unicast traffic support is enabled automatically.
-------------	---

---

**Step 20** It is important to perform the following steps for IPv6 Multicast for configuring the 2500 Series Wireless Controller. To enable efficient multicast transmission, perform this step on all wireless controllers.

**Step 21** Go to the **Controller > General** and do the following:

- The AP Multicast Mode is already set for Multicast and has an IPv4 Multicast Group Address that you entered on POD 2504 WLC setup.
- AP IPv6 Multicast Mode dropdown: **Multicast**
- In Multicast Group Address text box, enter: **ff1e::239:100:100:94**
- Click **Apply**

---

<b>Note</b>	The IPv6 multicast group address must be in the FFXX::/16 range which is scoped for IPv6 multicast applications.
-------------	--

---

<b>General</b>		
Name	POD1WLC	
802.3x Flow Control Mode	Disabled	
LAG Mode on next reboot	Disabled	(LAG Mode is currently disabled).
Broadcast Forwarding	Disabled	
AP Multicast Mode <a href="#">1</a>	Multicast	239.0.1.1 Multicast Group Address
AP IPv6 Multicast Mode <a href="#">1</a>	Multicast	ff1e::239:100:100:94 IPv6 Multicast Group Address
AP Fallback	Enabled	
CAPWAP Preferred Mode	ipv4	

**Step 22** Go to Controller > **IPv6** > **RA Throttle Policy** and select the following:

- Enable RA Throttle Policy: **Checked**
- Interval Option dropdown: **Passthrough**
- Click **Apply** and **Save Configuration**.

---

<b>Note</b>	The Router Advertisement (RA) Policy must be turned on for IPv6 clients to see the RA to obtain their SLAAC IPv6 address. The Passthrough option allows any RAs with an interval option to go through without throttling.
-------------	---

---

## RA Throttle Policy > Edit

Enable RA Throttle Policy	<input checked="" type="checkbox"/>
Throttle Period (10-86400 seconds)	<input type="text" value="600"/>
Max Through (0-256)	<input type="text" value="10"/> No Limit <input type="checkbox"/>
Interval Option	<input type="button" value="Passthrough"/>
Allow At-least (0-32)	<input type="text" value="1"/>
Allow At-most (0-256)	<input type="text" value="1"/> No Limit <input type="checkbox"/>

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- Configured the 3650 switch with IPv6 Global and Link-Local addresses for the management and client VLANs for SLAAC addressing.
- Configured the 3650 for IPv6 unicast routing.
- Configured the WLC Management interface with an IPv6 address.
- Enabled IPv6 multicast and anIPv6 multicast address.
- Enabled the IPv6 RA throttle policy.

## **Task 3: Associate the Client after IPv6 Configuration**

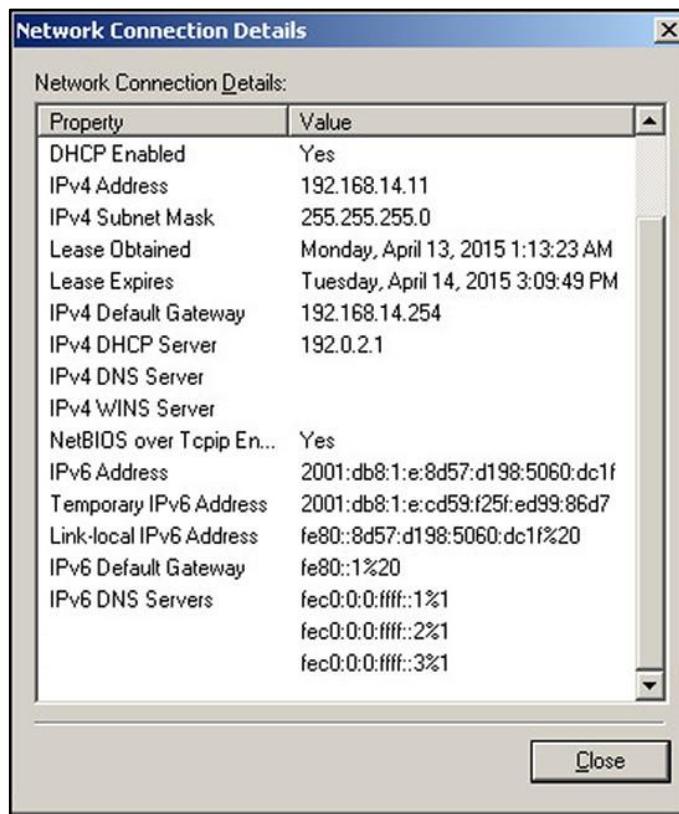
### ***Activity Procedure***

In this task, you will verify that the wireless client obtains an IPv6 address in the correct range.

Complete these steps:

- Step 1** Connect to the Client PC.

- Step 2** Verify that the client is not connected to any WLAN (from wireless tray).
- Step 3** Click on the **Wireless** icon in the tray again.
- Step 4** Connect to **Podx\_Open** WLAN and choose **Status**.
- Step 5** Click on the **Details** button on the **Status** screen.
- Step 6** You should have an IPv4 address in the **192.168.14.0** network.
- Step 7** You should also have an IPv6 address in the **2001:db8:1:e** network.



- 
- Note** You will have three IPv6 addresses:
1. IPv6 Address: Same network prefix as client VLAN and derived from Link-Local address
  2. Temporary IPv6 Address: Windows 7/8 use this as an alternative address to provide anonymity and it is randomly generated and changes over time.
  3. Link-Local IPv6 Address: Self-assigned address
- 

- Step 8** Open a Command Prompt and perform the following:
- Ping the Client VLAN interface of **2001:db8:1:e::1**
  - Ping the default gateway of **fe80::1**
- Step 9** Connect to the WLC from the Admin PC.
- Step 10** Go to **Monitor > Clients**. Notice under the IP Address column that your client only has an IPv4 address.
- Step 11** Click on the **MAC address** of your client. You will see the following addresses:

- IPv4 (192.168.14.0 network)
- IPv6 (**2001:db8:1:e** network) – Assigned address via SLAAC
- IPv6 (**2001:db8:1:e** network) – Temporary via Windows
- IPv6 (**fe80:** network) – Link-Local address

**Step 12** Now, verify they **Management** interface IPv6 address.

**Step 13** On the Client PC, open the Firefox browser and enter the URL: **http://[2001:db8:1:a::2]**

---

<b>Note</b>	You must enter the IPv6 address in brackets [] for the browser to know that you aren't looking up a host (unique to current AireOS WLC)
-------------	---

---

**Step 14** You should now see the WLC login page.

This verifies that the wired client is also using IPv6 and you can confirm this by opening a command prompt and typing IPCONFIG.

**Step 15** Go to the client PC and disconnect the client from the WLAN **Poxd\_Open**. (right click on WLAN and select Disconnect).

**Step 16** Go to the Admin PC and remove the client (**Monitor > Client** and **Remove** from the dropdown).

**Step 17** Close all open dialogue windows.

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- Associated the wireless client with the WLAN and verified the wireless client's IPv6 connectivity on the client and on the WLC.
- Verified that the wired client had IPv6 connectivity and the management interface's IPv6 address could be accessed.
- Disconnected the wireless client from the WLAN and removed them from the WLC

# **Hardware Lab 5: Configuring Security in a Centralized WLAN Deployment**

---

## **Overview**

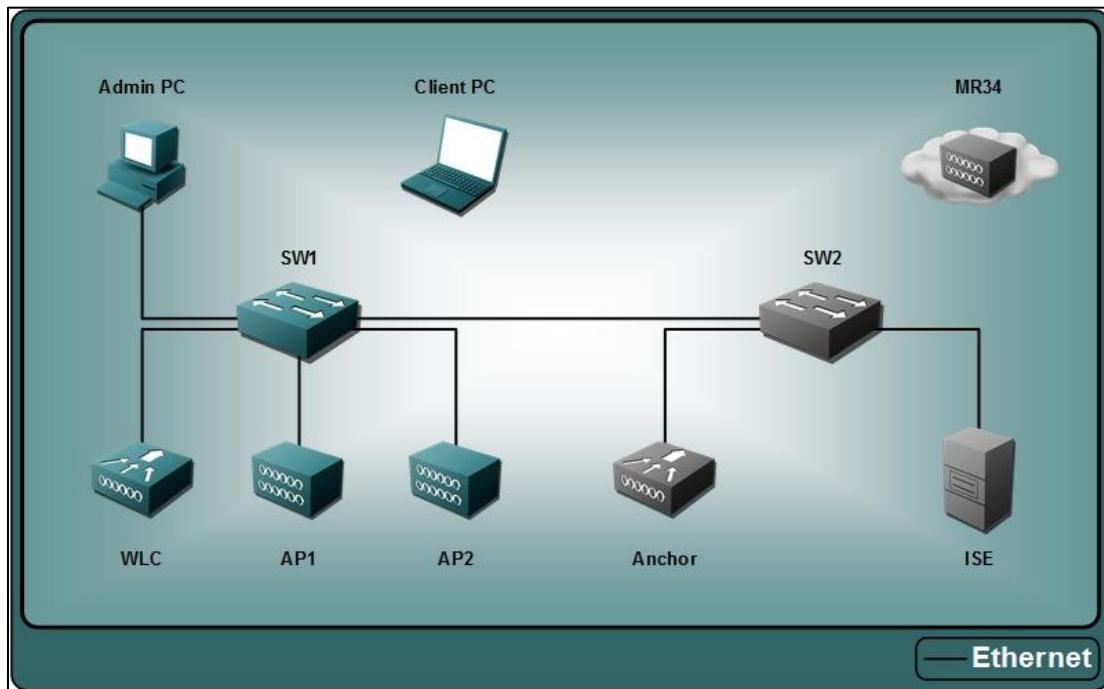
In this activity, you configure the WLC provide security on the WLAN centralized WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Implement and test WPA2-PSK security
- Implement test Local-EAP security
- Implement and test EAP with RADIUS security
- Implement and test WebAuth security

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 3650 switch
- Pod 2504 WLC
- AP 3700i (Centralized AP)
- Cisco ISE

### VLANs and IP Ranges

#### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
WLC 2504	192.168.11.5	admin	Cisco123	
Pod 3650 Switch	192.168.11.254	admin	Cisco123	cisco
ISE (RADIUS)	192.168.11.21	admin	1234QWer	

## Task 1: Implement WPA PSK Authentication

### Activity Procedure

In this task, you will implement WPA PSK authentication on the WLC and test with a wireless client.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

**Step 1** Connect to the Admin PC.

**Step 2** Open a browser and connect to the WLC from the Admin PC.

**Step 3** From the WLAN menu, choose **WLANS > WLANS**.

---

**Note** To help keep the number of broadcasting SSID to a minimum, you will keep re-using the existing WLAN and modifying it for each authentication type.

---

**Step 4** Click on the ID for the **Podx\_Open** WLAN and select the following:

- Profile Name: **Podx\_PSK** (x=pod)

- SSID: **Podx\_PSK** (x=pod)
- Status: **Enabled** (checked)
- Interface/Interface Group(G) dropdown: **client** (our client access VLAN)
- Broadcast SSID: **Enabled** (checked)

**Step 5** Go to the **Security** tab and select the following under Layer 2:

- Layer 2 Security: **WPA + WPA2**
- WPA + WPA2 Parameters: **WPA2 Policy-AES** (checked – all others unchecked)
- Authentication Key Management: **PSK** (checked)
- For the PSK Format, use ASCII and enter a key in of: **Cisco123** (ok for labs – not production)

---

<b>Note</b>	You are choosing the more secure policy of WPA2. If you choose WPA, you will see it uses AES by default and TKIP (deprecated) is not used by default.
-------------	---

---

**Step 6** Click **Apply** and **OK** to any pop-up warnings (remember, changing a WLAN that is in use, could cause a momentary loss of connectivity for clients).

**Step 7** Click **Back** and verify that the WLAN shows **[WPA2][Auth(PSK)]**

#### Verify PSK operation with the Client

**Step 8** Connect to the Client PC.

**Step 9** You are now connected to the Client PC.

**Step 10** On the desktop, right-click on **Network** and choose **Properties** to go to the **Network and Sharing Center**.

**Step 11** Click **Manage Wireless Networks** and right-click and delete all profiles that may exist.

**Step 12** Click the WLAN tray.

**Step 13** Click on the **Podx\_PSK** network, and then click **Connect**. (Uncheck the box for “Connect automatically”, you don’t want to create a profile).

**Step 14** You will be prompted for the Network Security Key, type **Cisco123** and click **OK**.

**Step 15** Click the WLAN tray.

**Step 16** Right click the **Podx\_PSK** network and select **Status**.

**Step 17** On the **General** tab of the Status window, click the **Details** button.

**Step 18** You will now see your IP address (network 192.168.14.0)

**Step 19** Open a Command Prompt and ping your gateway (192.168.14.254).

**Step 20** Verify your client connection on the WLC Monitor menu.

**Step 21** Close all dialogue windows.

## **Activity Verification**

You have successfully completed this task when you attain this result:

- Created a WLAN with PSK authentication.
- Connected your wireless client to the PSK WLAN
- Client got an IP address in the proper range and could ping the gateway.

## **Task 2: Implement Local EAP Authentication**

### **Activity Procedure**

In this task, you will implement Local EAP authentication on the WLC and test with a wireless client.

---

<b>Note</b>	The lower case “x” in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

Complete these steps:

**Step 1** Open a browser and connect to the WLC from the Admin PC.

**Step 2** First, create a local user account for EAP authentication. Go to the **Security** menu and on the left side, choose **AAA > Local Net Users**. Click **New** and enter the following:

- User Name: **wlcuser** (naming convention for local user)
- Password: **Cisco123**
- For the WLAN Profile, choose: **Any WLAN** (you could restrict this user to a specific WLAN for these credentials)
- Click **Apply**

### **Create a Local EAP Profile**

A profile must be created for the WLAN to know which Local EAP types are supported. You will also only enable the type of “PEAP”, because we can easily test without certificates needed.

**Step 3** Next, create a security profile for the authentication method to be used. Go to the **Security** menu and on the left side, choose **Local EAP > Profiles**. Click **New** and enter the following:

- Profile Name: **WLC\_Local\_EAP**
- Click **Apply**
- On the next screen, check the EAP type(s) to be used: **PEAP**
- Click **Apply**

### **Modify the WLAN for EAP**

**Step 4** Open the **WLANS** menu.

**Step 5** Click on the ID for the **Podx\_PSK** WLAN and on the **General** tab and enter the following:

- Profile Name: **Podx\_EAP** (x=pod)
- SSID: **Podx\_EAP** (x=pod)

- Step 6** Go to the **Security** tab and enter the following for Layer 2:
- Layer 2 Security: **WPA + WPA2**
  - WPA + WPA2 Parameters: **WPA2 Policy-AES** (checked – all others unchecked)
  - Authentication Key Management: **Uncheck PSK** and then **Check 802.1X**
  - For **AAA Servers** unselect the **Enabled** check boxes for **Radius Authentication Servers** and **Accounting Servers** to disable RADIUS accounting and authentication for this WLAN
  - Check the box for **Local EAP Authentication** and then choose: **WLC\_Local\_EAP** as the EAP Profile name to use.

**Step 7** Click **Apply** and **OK** to any pop-up warnings.

**Step 8** Click **Back** and verify that the WLAN shows **[WPA2][Auth(802.1X)]**

### Verify EAP Operation with the Client

**Step 9** Connect to the Client PC.

**Step 10** You cannot connect to this WLAN without creating a profile that takes into account our specific parameters. EAP parameters will vary based on type and security needs.

**Step 11** On the desktop, right-click on **Network** and choose **Properties** to go to the **Network and Sharing Center**.

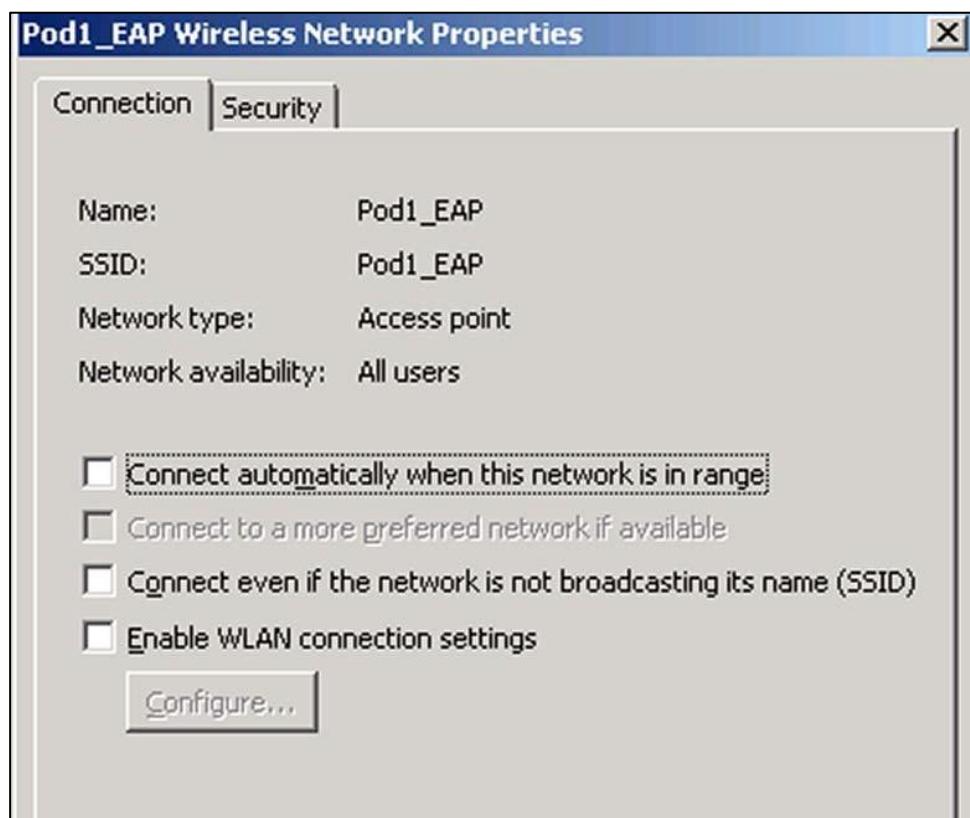
**Step 12** Click **Manage Wireless Networks**.

**Step 13** Click **Add**. Then, select **Manually create a network profile** and enter the following:

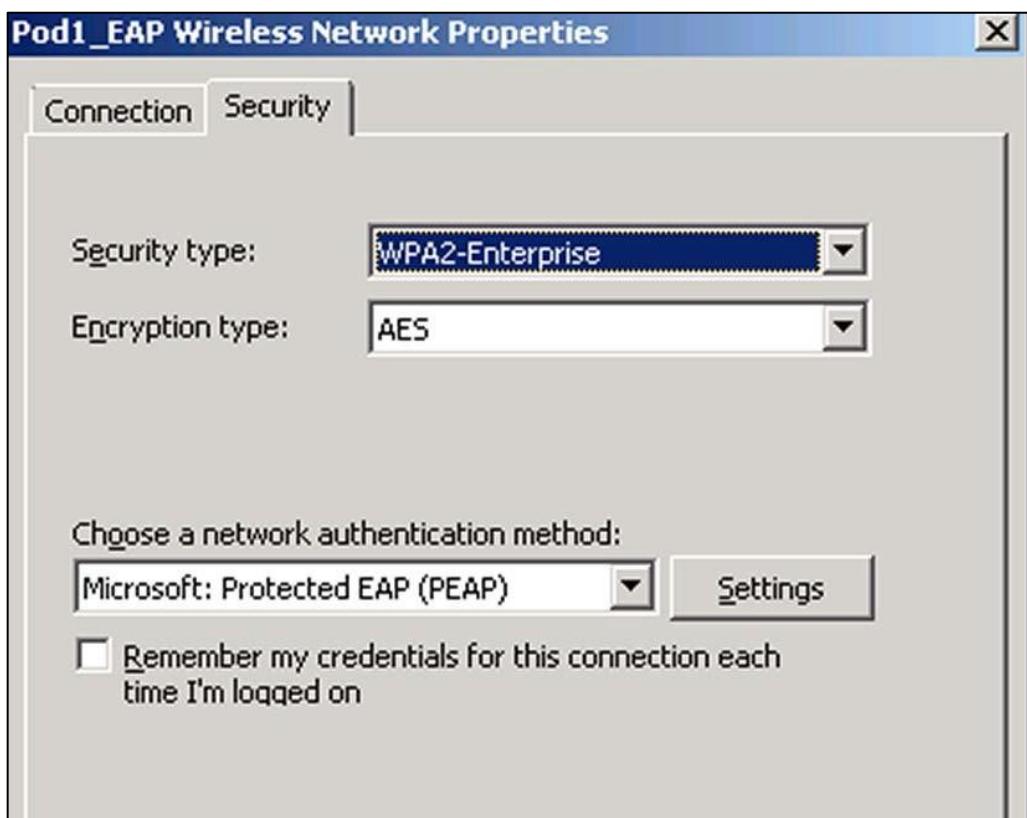
- Network Name: **Podx\_EAP**
- Security type dropdown: **WPA2-Enterprise**
- Encryption type dropdown: **AES**
- Start this connection automatically: **Uncheck** (you want to manually connect):
- Click **Next**

**Step 14** Click on **Change connection settings**.

**Step 15** On the Podx\_EAP Wireless Network Properties, verify the option to Connect automatically when this network is in range is **unchecked**.

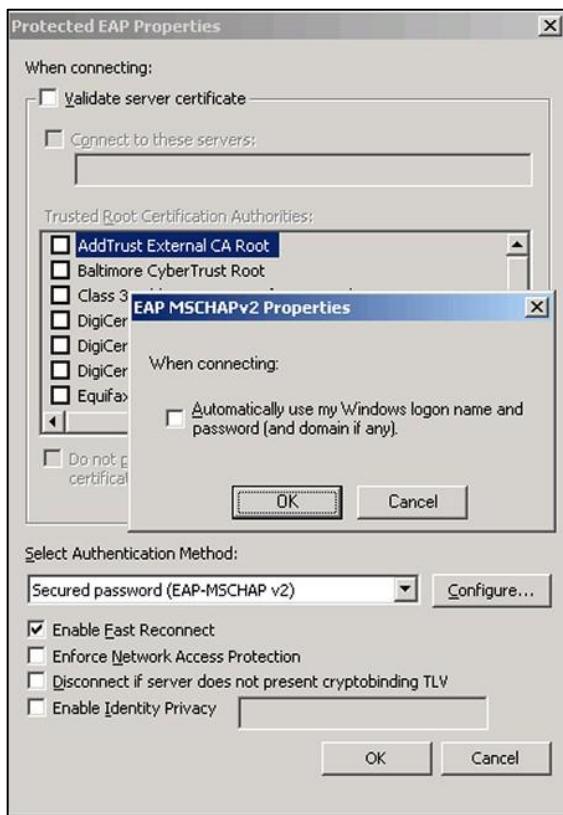


**Step 16** Click on the **Security** tab, verify that the Network Authentication Method is **Microsoft: Protected EAP (PEAP)**. Uncheck **Remember my credentials...** (You want to enter our credentials each time that you connect).



**Step 17** Click **Settings** beside Microsoft: Protected EAP (PEAP) and enter the following:

- Under “When connecting”: uncheck the Validate server certificate (because we can’t validate certificates in our lab)
- Verify under the “Select Authentication Method” that the dropdown is set to: **Secured password (EAP-MSCHAP v2)**
- Next to this dropdown, click **Configure**
- Uncheck the box for “Automatically use my Windows logon name...”
- Click **OK** and then **OK** to return to the **Security** tab

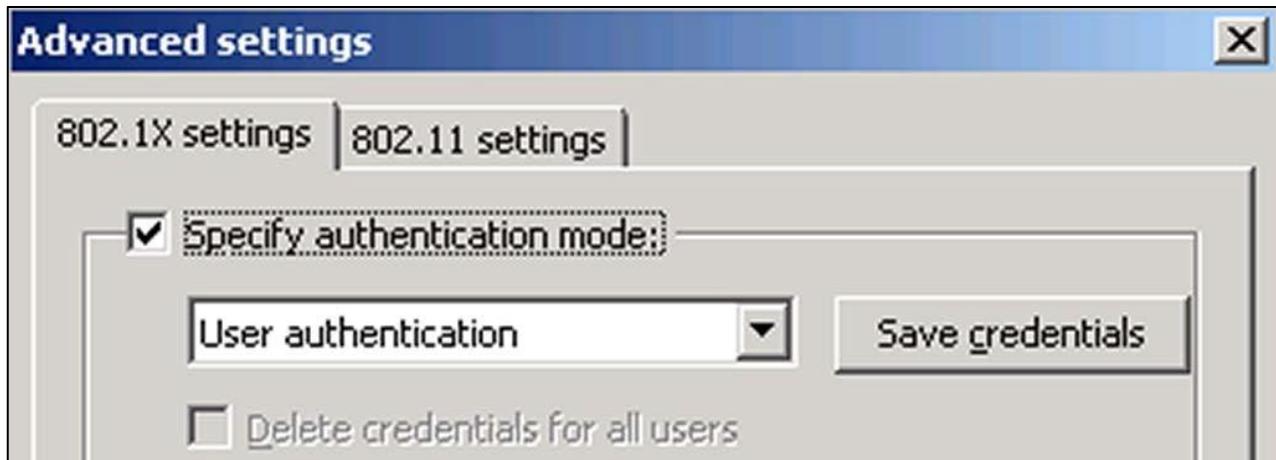


**Step 18** On the **Security** tab, click the **Advanced Settings** button and enter the following:

- 802.1X settings: Check the box for **Specify authentication mode**

**Step 19** Change the dropdown to **User authentication** (username/password)

**Step 20** Look at the **802.11 settings** tab, but do not make any changes. Click **OK** and **OK**.



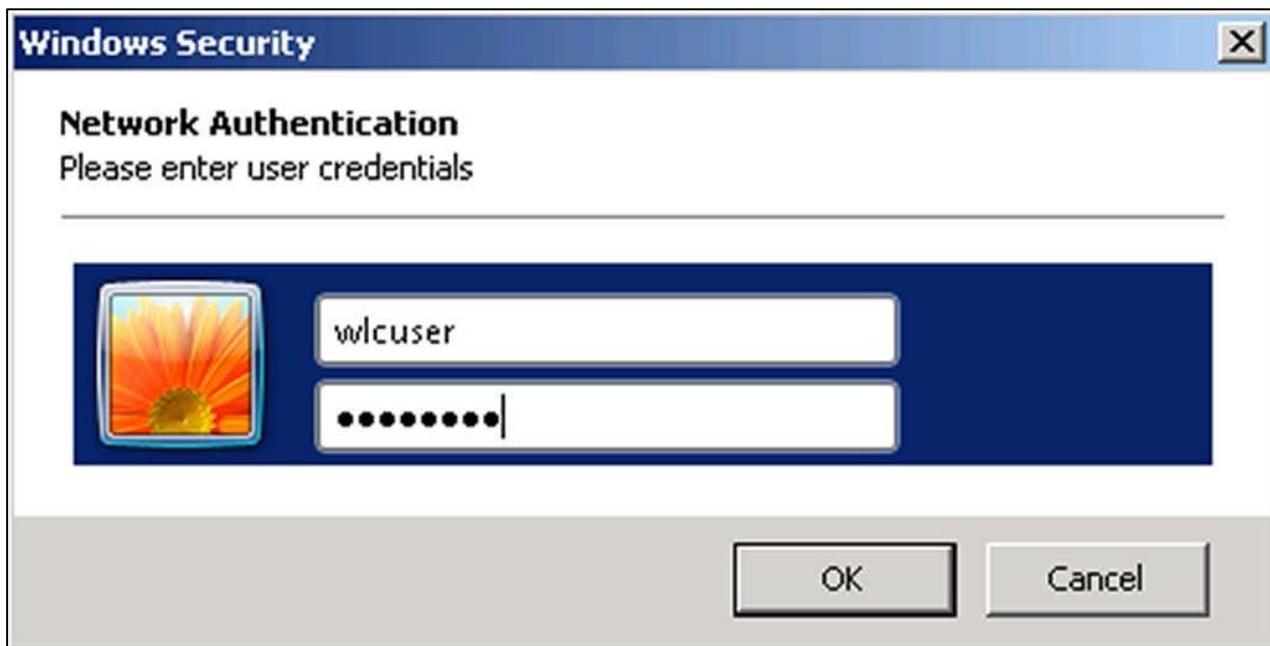
**Step 21** Click **Close** on Profile Wizard.

**Step 22** Observe the new profile (**Podx\_EAP**)

**Step 23** Click the WLAN tray.

**Step 24** Click on the **Podx\_EAP** network, and then click **Connect**.

**Step 25** A Network Authentication screen will pop-up, enter your username of **wlcuser** and password of **Cisco123** and click **OK**.



**Note** If authentication fails, verify that you entered the correct username/password and verify the same username/password on the WLC. Also recheck EAP profile and WLAN settings.

**Step 26** Click the WLAN tray.

**Step 27** Right click the **Podx\_EAP** network and select **Status**.

**Step 28** On the **General** tab of the Status window, click the **Details** button.

**Step 29** You will now see your IP address (network 192.168.14.0).

**Step 30** Open a Command Prompt and ping your gateway (192.168.14.254).

**Step 31** Verify your client connection on the WLC Monitor menu.

**Step 32** Close all dialogue windows.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Created a WLAN with Local EAP authentication.
- Connected your wireless client to the EAP WLAN
- Client got an IP address in the proper range and could ping the gateway.

# Task 3: Implement EAP with RADIUS Authentication

## Activity Procedure

In this task, you will implement EAP with RADIUS authentication on the WLC with ISE and test with a wireless client.

---

<b>Note</b>	The lower case “x” in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

### Connect to the RADIUS Server (ISE)

Complete these steps:

**Step 1** Open a browser and connect to the WLC from the Admin PC. **Step 2**

Still on the Admin PC, open the Firefox browser to connect to the Cisco ISE.

**Step 3** Enter **192.168.11.21** for the address of the ISE.

**Step 4** On the Untrusted Connection warning, click on **I Understand the Risks**, and click on **Add Exception**.

**Step 5** On the pop-up, click **Confirm Security Exception**.

---

<b>Note</b>	This warning is issued because the ISE uses a self-signed certificate.
-------------	--

---

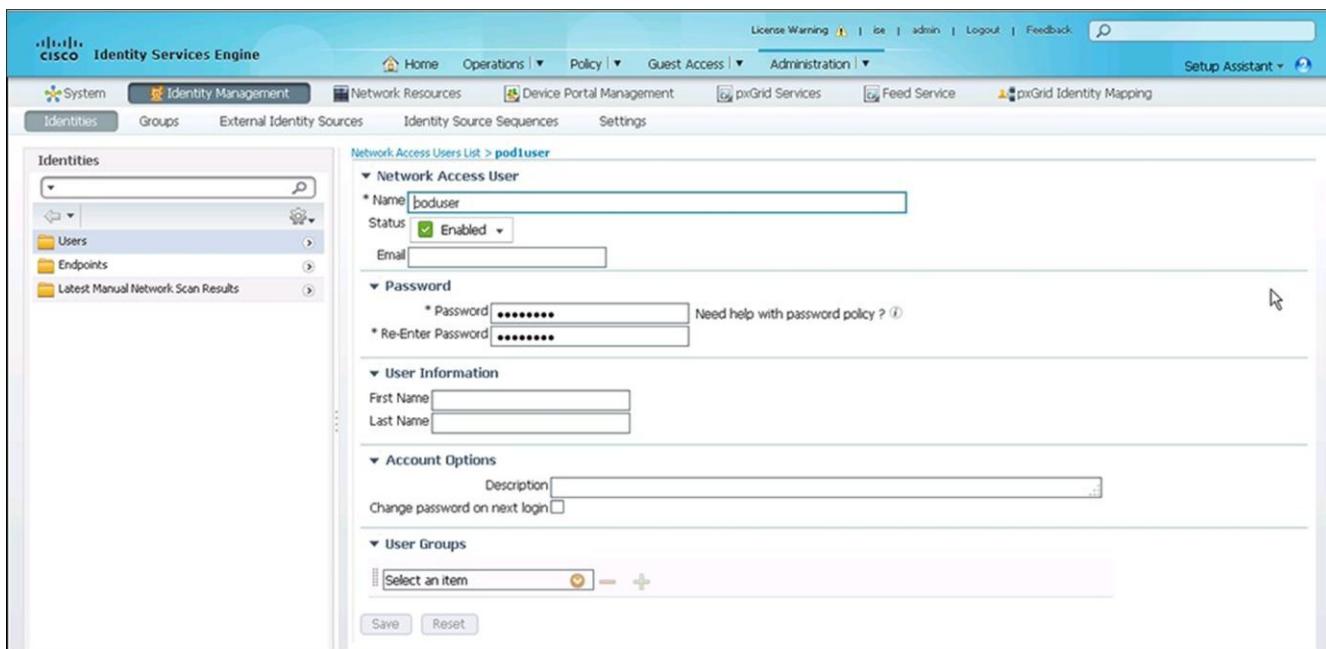
**Step 6** At the ISE login screen, enter the username of **admin** and password of **1234QWer** and click **Login**.

**Step 7** Click **OK** on any warnings about the license expiration.

### Create a User Account on ISE for EAP with RADIUS Usage

**Step 8** Go to **Administration > Identity Management > Identities > Users**. Click **+Add** and enter the following:

- Name: **poduser** (naming convention for remote users)
- Email: leave empty
- Enter/Renter the password: **Cisco123**
- Click **Submit**



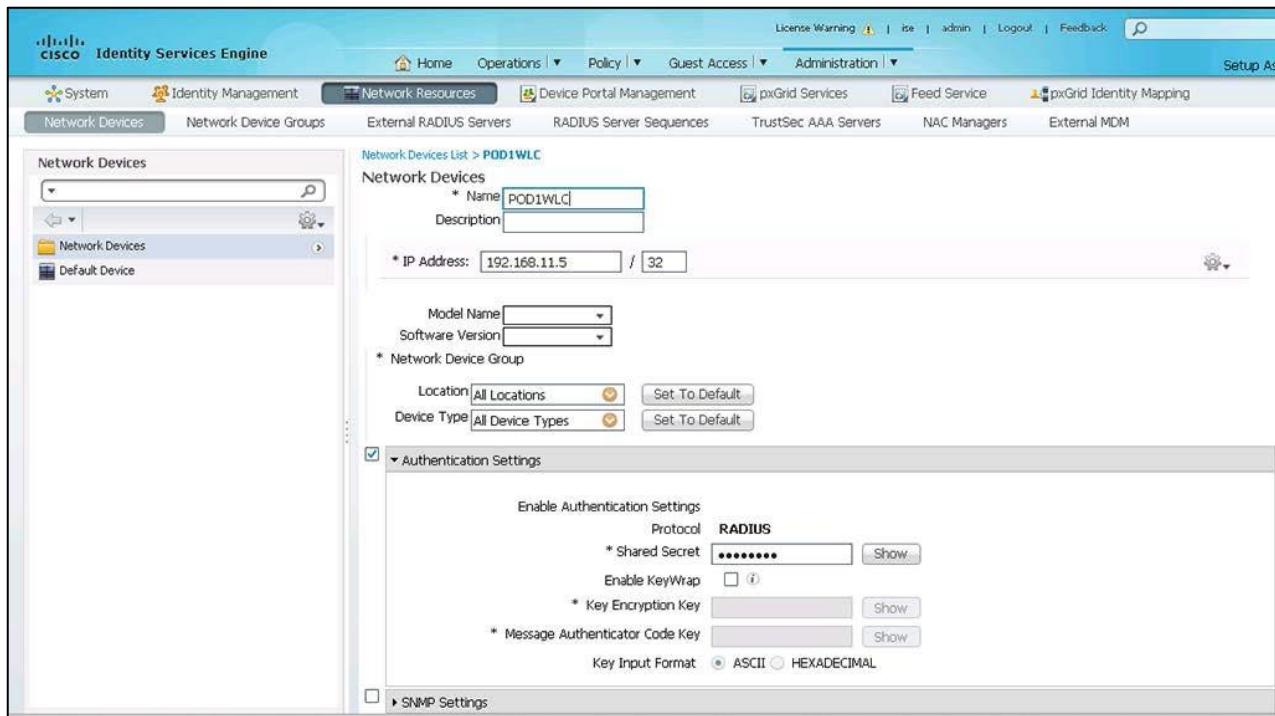
**Step 9** To see the Password Policy settings, go to **Administration > Identity Management > Settings > User Password Policy**. Don't change anything, but observe the policy. Is Lockout/Suspend enabled? (On systems where this is true, your account may get locked out over too many failed attempts). Also notice Password History is 3 versions.

#### Create an Entry in ISE for the WLC 2504 (NAD)

Here you will create an entry in ISE to recognize the WLC 2504 as a Network Access Device (NAD) for authentication purposes.

**Step 10** Go to **Administration > Network Resources > Network Devices**. Click **+Add** and enter the following:

- Name for the WLC: **WLC**
- IP address of the WLC and network mask: **192.168.11.5 / 32** (management address)
- Check the box for **Authentication Settings** and window opens for the settings.
- Enter a password for the Shared Secret entry: **Cisco123** (you will use this same Shared Secret password on the WLC 2504)
- Click **Submit**



### Create an Entry in the WLC 2504 for ISE (RADIUS)

Next, create a connection between the Pod WLC 2504 and the RADIUS server using a Shared Secret password.

**Step 11** On the WLC, go to the **Security** menu and choose **AAA > RADIUS > Authentication**. Click **New** and enter the following:

- IP address of the RADIUS server (ISE): **192.168.11.21**
- Enter the same Shared Secret password you entered on the RADIUS server: **Cisco123**
- Click **Apply**

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface under the 'SECURITY' tab. On the left, a navigation tree includes 'AAA' (General, RADIUS, TACACS+), 'Local EAP' (General, Profiles, EAP-FAST Parameters, Authentication Priority), and 'RADIUS Authentication Servers'. The main panel displays the 'RADIUS Authentication Servers > New' configuration page. It has fields for 'Server Index (Priority)' (set to 1), 'Server IP Address(Ipv4/Ipv6)' (192.168.11.21), 'Shared Secret Format' (ASCII), 'Shared Secret' (a masked password), 'Confirm Shared Secret' (another masked password), 'Key Wrap' (unchecked), 'Port Number' (1812), 'Server Status' (Enabled), 'Support for RFC 3576' (Disabled), 'Server Timeout' (2 seconds), and checkboxes for 'Network User' (checked), 'Management' (checked), and 'IPSec' (unchecked). A note indicates that 'Key Wrap' is designed for FIPS customers.

**Step 12** Hover over the blue arrow on the far right side of the row with the new server and choose **Ping**. You will get a ping response that verifies the connection is good.

The screenshot shows the 'RADIUS Authentication Servers' list. At the top, there are dropdown menus for 'Auth Called Station ID Type' (set to 'AP MAC Address:SSID') and 'Use AES Key Wrap' (unchecked). Below these are fields for 'MAC Delimiter' (set to 'Hyphen'). The main area is a table with columns: Network User, Management, Server Index, Server Address(Ipv4/Ipv6), Port, IPSec, and Admin Status. One row is visible, showing a checked 'Network User' box, a checked 'Management' box, '1' as the 'Server Index', '192.168.11.21' as the 'Server Address', '1812' as the 'Port', 'Disabled' as the 'IPSec' status, and 'Enabled' as the 'Admin Status'.

### Modify the WLAN for EAP with RADIUS

**Step 13** Go to the **WLANS** menu.

**Step 14** Click on the ID for the **Podx\_EAP** WLAN.

**Step 15** On the **Security** tab, select the following:

- Layer 2: (no changes from Local\_EAP)
  - Choose WPA+WPA2 as the Layer 2 Security
  - Under WPA + WPA2 Parameters, select only WPA2 Policy-AES
  - Under Authentication Key Management, choose 802.1X
- AAA Servers:
  - Verify that the **Enabled** box is checked for under **Authentication Servers**
  - Uncheck the box for **Local EAP Authentication** (now using remote authentication)

---

<b>Note</b>	In Remote EAP, you are not changing the authentication type, but where the authentication server is at (now remote vs. local).
-------------	--

---

**Step 16** Click **Apply** and **OK** to any pop-up warnings. (**Save Configuration**)

**Step 17** Click **Back** and verify that the WLAN shows **[WPA2][Auth(802.1X)]**

#### Verify EAP Operation with the Client

**Step 18** Connect to the Client PC.

**Step 19** You will use the existing EAP profile.

---

<b>Note</b>	Again, the authentication type does not change, but the server that does the authentication is now ISE.
-------------	---

---

**Step 20** Click the WLAN tray.

**Step 21** Click on the **Podx\_EAP** network, and then click **Disconnect** (if connected).

**Step 22** Click on the **Podx\_EAP** network, and then click **Connect**.

**Step 23** A Network Authentication screen will pop-up, enter your username of **poduser** and password of **Cisco123** and click **OK**.

---

<b>Note</b>	If authentication fails, verify that you entered the correct username/password and verify the same username/password on the ISE. Also recheck EAP profile and WLAN settings.
-------------	--

---

**Step 24** Click the WLAN tray.

**Step 25** Right click the **Podx\_EAP** network and select **Status**.

**Step 26** On the **General** tab of the Status window, click the **Details** button.

**Step 27** You will now see your IP address (network 192.168.14.0).

**Step 28** Open a Command Prompt and ping your gateway (192.168.14.254).

**Step 29** Verify your client connection on the WLC **Monitor > Clients** menu.

#### Verify EAP Operation with ISE

**Step 30** Open a Web Browser and connect to the ISE host again (192.168.11.21).

**Step 31** Login and navigate to **Operations > Authentications**.

**Step 32** Here you will see the Authentications in the last 24 hours.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device
2015-06-10 16:54:45.634	<span style="color:blue;">i</span>	0	pod1user	6C:B0:CE:F6:32:05	Netgear-Device					Default >> Dot1X >> ... Default >> Basic_Aut...	PermitAccess
2015-06-10 16:54:45.634	<span style="color:green;">✓</span>	0	pod1user	6C:B0:CE:F6:32:05	Netgear-Device					Default >> Dot1X >> ... Default >> Basic_Aut...	POD1WLC
2015-06-10 16:54:45.548	<span style="color:green;">✓</span>	0		6C:B0:CE:F6:32:05							

**Step 33** Look closely at what is displayed. Click the icon under "Details" to see even more information.

**Step 34** On the Client PC desktop, right-click on **Network** and choose **Properties** to go to the **Network and Sharing Center**.

**Step 35** Click **Manage Wireless Networks** and right-click and **remove all profiles** that may exist.

## Activity Verification

You have successfully completed this task when you attain this result:

- Created a WLAN with Local EAP authentication.
- Connected your wireless client to the EAP WLAN.
- Client got an IP address in the proper range and could ping the gateway.
- Verified your user authentication on ISE.

## Task 4: Implement WebAuth Authentication

### Activity Procedure

In this task, you will implement WebAuth authentication on the WLC and test with a wireless client.

---

**Note** The lower case "x" in a command will be your pod number, ex: pod 1, x=1

---

### Modify the WLAN for WebAuth

Complete these steps:

- Step 1** Connect to the Admin PC.
- Step 2** Open a browser and connect to the WLC from the Admin PC
- Step 3** Open the **WLANS** menu.
- Step 4** Click on the ID for the **Podx\_EAP** WLAN and on the **General** tab. Enter the following:

- Profile Name to: **Podx\_Guest** (x=pod)
- SSID to: **Podx\_Guest** (x=pod)

**Step 5** On the **Security** tab, enter the following:

- Layer 2:
  - Layer 2 Security: **None**
- Layer 3:
  - Layer 3 Security: **Web Policy**
  - Note the warning and click **OK**
  - Check the radio button for **Passthrough**

Guest will just need to click an accept button.

---

<b>Note</b>	There are several Web Policy methods (ex: Pass-through and Authentication) For pass-through, the guest client would just need to click an accept button (agreeing to a EULA). For authentication, the guest client would have to enter a user name and password. The user name and password can be local (like Local-EAP) or remote (like on a RADIUS server. The AAA Server tab is where you choose the order of authentication.
-------------	---

---

**Step 6** Click **Apply** and **OK** to any pop-up warnings.

**Step 7** Click **Back** and verify that the WLAN shows [**Web-Passthrough**]

#### Verify WebAuth Authentication with the Client

**Step 8** Connect to the Client PC.

**Step 9** Click the WLAN tray.

**Step 10** Click on the **Podx\_Guest** network, and then click **Connect**. (Uncheck the box for “Connect automatically”, you don’t want to create a profile).

**Step 11** Click the WLAN tray.

**Step 12** Right click the **Podx\_Guest** network and select **Status**.

**Step 13** On the **General** tab of the Status window, click the **Details** button.

**Step 14** You will now see your IP address (network 192.168.14.0).

**Step 15** Open a Command Prompt and ping your gateway (192.168.14.254). This attempt should fail.

---

<b>Note</b>	Even though you have an IP address, you have not yet authenticated, so the gateway is not accessible.
-------------	---

---

**Step 16** Verify your client connection on the WLCs **Monitor > Clients** menu and notice that the client is Associated, but not Authorized (Auth).

**Step 17** Open Firefox on the Client PC.

**Step 18** For the URL address, type: **192.168.11.5** and **Enter**.

**Step 19** On the Untrusted Connection” warning, click on **I Understand the Risks** and click on **Add Exception**.

**Step 20** On the pop-up, click **Confirm Security Exception**.

---

**Note** This warning is issued because the WLC uses a self-signed certificate.

---

**Step 21** You will now see the Welcome Screen where you will click **Accept**.

**Step 22** You will now see the original destination (POD 2504 WLC Login) displayed.

**Step 23** Open a Command Prompt and ping your gateway (192.168.14.254), it should be successful now.

**Step 24** Verify your client connection on the WLCs **Monitor > Clients** menu and notice that the client is Associated and Authorized (Auth).

**Step 25** When done, disconnect from the Podx\_Guest WLAN.

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- Created a WLAN with WebAuth authentication.
- Connected your wireless client to the Guest WLAN.
- Client got an IP address in the proper range and could ping the gateway.

# **Hardware Lab 6: Configuring Guest Access Using the Anchor WLC**

---

## **Overview**

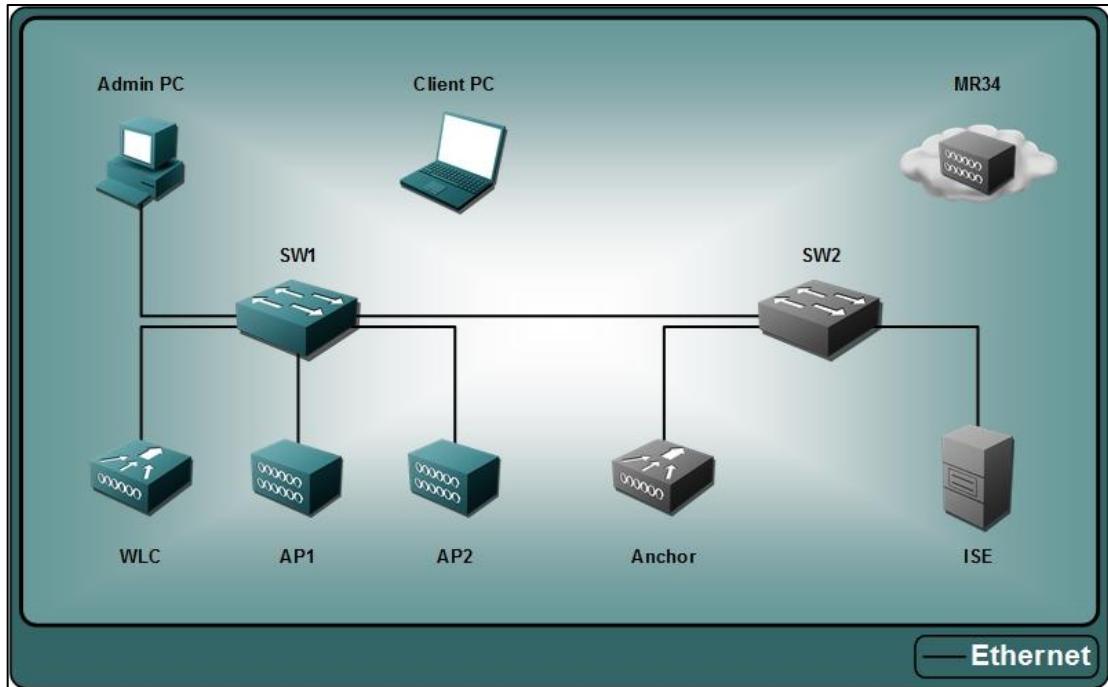
In this activity, you configure the WLC provide security on the WLAN centralized WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Add a Foreign WLC Mobility Member to an Anchor WLC
- Add an Anchor WLC Mobility Member to a Foreign WLC
- Configure guest WLANs on both the Anchor and Foreign WLCs
- Implement and test Remote EAP security
- Create a local user on the Anchor and test guest access with a wireless client
- Create connection to the Anchor WLC from the ISE and add a guest ISE user on the ISE
- Create connection to the ISE from the Anchor WLC and test the guest access

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Anchor 2504 WLC (Back Bone)
- Foreign WLC 2504 (Pod)
- AP 3700i (Centralized AP)
- Cisco ISE

## VLANs and IP Ranges

### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
WLC 2504	192.168.11.5	admin	Cisco123	
Pod 3650 Switch	192.168.11.254	admin	Cisco123	cisco
AnchorWLC 2504	172.16.0.20	admin	Cisco123	
ISE (RADIUS)	192.168.11.21	admin	1234QWer	

## Task 1: Add Foreign WLC on Anchor WLC

### **Activity Procedure**

In this task, you will add the foreign WLC (POD 2504 WLC) as a Mobility Group Member to the Anchor WLC (AnchorWLC).

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

### **Document the Pod WLC 2504 Mobility Information**

Complete these steps:

**Step 1** Connect to the Admin PC.

**Step 2** Open a browser and connect to the WLC from the Admin PC.

---

**Note** The Backbone WLC is going to be the Anchor Controller and the WLC is going to be the Foreign Controller.

---

**Step 3** Select **Controller > Mobility Management > Mobility Groups**.

**Step 4** Document the following:

- POD 2504 WLC MAC address: XX:XX:XX:XX:XX:XX (Pod MAC)
- POD 2504 WLC IPv4 address: 192.168.11.5
- POD 2504 WLC Group Name: Podx (x=pod#)

MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Static Mobility Group Members							
<b>Local Mobility Group</b> Pod1							
MAC Address	IP Address(Ipv4/Ipv6)		Group Name	Multicast IP			
80:e8:6f:03:a5:a0	192.168.11.5		Pod1	0.0.0.0			

#### Configure the Anchor WLC to make Your Pod WLC a Mobility Member

**Step 5** Open another browser or browser tab and type in the url of the AnchorWLC **172.16.0.20** and press Enter and select the following:

- Username: **admin**
- Password: **Cisco123**
- Press **Ok**

---

**Note** The AnchorWLC background is red (due to Controller > General > Web Color theme).

---

**Step 6** On the AnchorWLC, select **Controller > Mobility Management > Mobility Groups**, click **New** and enter the following:

Using the information from your POD 2504 WLC, enter:

- POD 2504 WLC IPv4 address: 192.168.11.5
- POD 2504 WLC MAC address: XX:XX:XX:XX:XX:XX (Pod MAC)
- POD 2504 WLC Group Name: Podx (x=pod#)
- Click **Apply** and **Save Configuration**.

**MONITOR   WLANs   CONTROLLER   WIRELESS   SECURITY   MANAGEMENT**

### Mobility Group Member > New

Member IP Address(Ipv4/Ipv6)	192.168.11.5
Member MAC Address	1c:de:a7:06:3c:20
Group Name	Pod5 <input type="button" value="X"/>
Hash	none

*1. Hash is not supported for IPv6 members*

#### Verify Mobility Communications between the Anchor WLC and the Pod WLC

**Step 7** Go back to **Mobility Groups** to view the new member of Podx.

**Step 8** Hover the mouse over the blue dropdown arrow to the far right of the Podx member and choose **Ping**. You should get a successful ping response.

Members					<input type="button" value="New..."/>	<input type="button" value="EditAll"/>
Anchor						
Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key		
6.0.20	Anchor	0.0.0.0	Up	none		
192.168.11.5	Pod5	0.0.0.0	Up	none	<input type="button" value="Remove"/> <input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; border-radius: 5px; padding: 2px 10px; font-weight: bold; font-size: inherit;" type="button" value="Ping"/>	

**Note** The status will be “Control and Data Path Down” until you complete the entire configuration.

### Activity Verification

You have successfully completed this task when you attain this result:

- Added the Podx as a Mobility Group member on the AnchorWLC.
- Verified that the AnchorWLC can ping the WLC

# Task 2: Add Anchor WLC on Foreign WLC

## Activity Procedure

In this task, you will add the Anchor (AnchorWLC) as a Mobility Group Member to the foreign WLC (POD 2504 WLC).

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

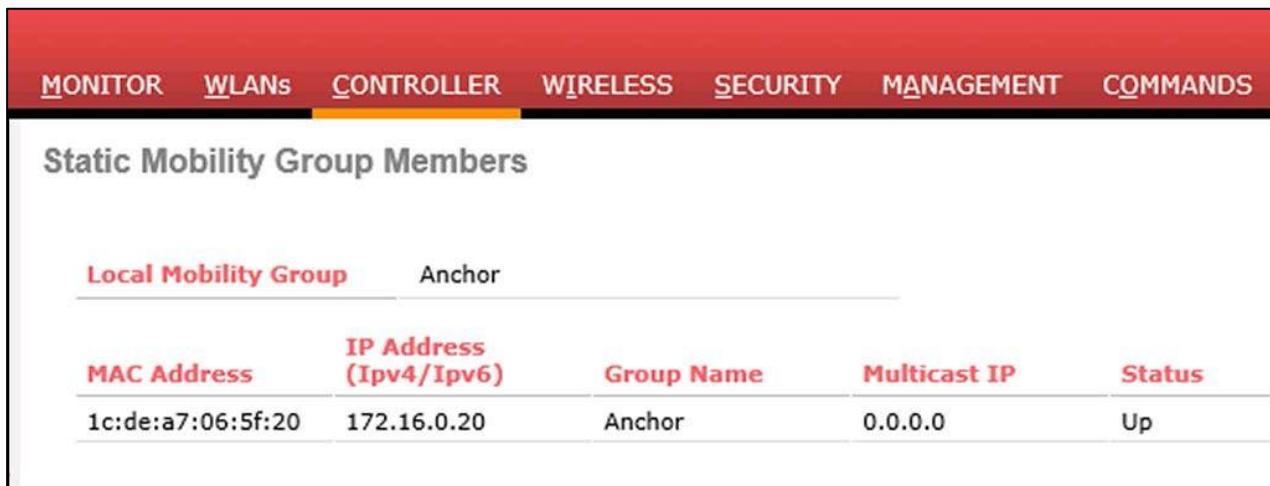
### Document the Anchor WLC 2504 Mobility Information

Complete these steps:

**Step 1** Open a browser and connect to the AnchorWLC from the Admin PC

**Step 2** Select **Controller > Mobility Management > Mobility Groups** and document the following:

- AnchorWLC MAC address: **XX:XX:XX:XX:XX:XX** (Anchor MAC)
- AnchorWLC IPV4 address: **172.16.0.20**
- AnchorWLC Group Name: **Anchor**



Static Mobility Group Members				
Local Mobility Group	Anchor			
MAC Address	IP Address (Ipv4/Ipv6)	Group Name	Multicast IP	Status
1c:de:a7:06:5f:20	172.16.0.20	Anchor	0.0.0.0	Up

### Configure the Pod WLC to Make the Anchor WLC a Mobility Member

**Step 3** On the WLC, select **Controller > Mobility Management > Mobility Groups**, and click **New**.

Using the information from your AnchorWLC, enter:

- AnchorWLC IPV4 address: **172.16.0.20**
- AnchorWLC MAC address: **XX:XX:XX:XX:XX:XX** (Anchor MAC)
- AnchorWLC Group Name: **Anchor** (not Podx, the Anchor has its own Group Name)
- Click **Apply** and **Save Configuration**.

**MONITOR   WLANS   CONTROLLER   WIRELESS   SECURITY   MANAGEMENT**

### Mobility Group Member > New

Member IP Address(Ipv4/Ipv6)	172.16.0.20
Member MAC Address	1c:de:a7:06:5f:20
Group Name	Anchor <input type="button" value="X"/>
Hash	none

*1. Hash is not supported for IPv6 members*

#### Verify Mobility Communications between the Pod WLC and the Anchor WLC

- Step 4** Go back **Mobility Groups** to view the new member of Anchor.
- Step 5** Hover the mouse over the blue dropdown arrow to the far right of the Anchor member and choose **Ping**. You should get a successful ping response.

Members					New...	EditAll
Pod5						
Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key		
68.51.5	Pod5	0.0.0.0	Up	none		
6.0.20 db8:1:a::2	Anchor	0.0.0.0	Up	none	<input type="button" value="Remove"/>	<input checked="" type="button" value="Ping"/>
	Pod5	::	Up	none		

**Note** The status will be “Control and Data Path Down” until you complete the entire configuration.

#### Verify Status between the Pod WLC and the Anchor WLC

- Step 6** On the WLC click Refresh at the top right.
- Step 7** On the AnchorWLC click Refresh at the top right.
- Step 8** The **Status** on POD 2504 WLC and AnchorWLC should be **Up** (it may take a minute or two).

Static Mobility Group Members						
Local Mobility Group		Pod5				
MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key	
e0:89:9d:42:b4:60	192.168.51.5	Pod5	0.0.0.0	Up	none	
1c:de:a7:06:5f:20	172.16.0.20	Anchor	0.0.0.0	Up	none	
e0:89:9d:42:b4:60	2001:db8:1:a::2	Pod5	::	Up	none	

Static Mobility Group Members						
Local Mobility Group		Anchor				
MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key	
1c:de:a7:06:5f:20	172.16.0.20	Anchor	0.0.0.0	Up	none	
e0:89:9d:42:b4:60	192.168.51.5	Pod5	0.0.0.0	Up	none	

## Activity Verification

You have successfully completed this task when you attain this result:

- Added the AnchorWLC as a Mobility Group member of the WLC.
- Verified that the WLC can ping the AnchorWLC.
- Verified that the Mobility Status was Up.

## Task 3: Configure the Guest WLAN on the Foreign WLC

### Activity Procedure

In this task, you will add a guest WLAN to the foreign WLC.

- Step 1** Open a browser and connect to the WLC from the Admin PC.
- Step 2** Click on the ID for the **Podx\_Guest**, and on the **General** tab, select the following:
- Status: **Enabled** (checked)
  - Change the Interface/Interface Group to: **management** (you need the management interface to source your EoIP/CAPWAP packets to the anchor and since our destination is NOT the local Ethernet ports or VLANs).

**Step 3** On the **Security** tab, select the following:

- Layer 2 tab:
  - Verify that the Layer 2 Security is: **None**
- Layer 3 tab:
  - Verify that the Layer 3 Security is: **Web Policy**
  - Click **OK** on the pop-up warning (if prompted)
  - Verify that the **Authentication** radio button is selected (authentication will be prompting for a username/password)

WLANS > Edit 'Pod5\_Guest'

General		Security	QoS	Policy-Mapping	Advanced
Profile Name	Pod5_Guest				
Type	WLAN				
SSID	Pod5_Guest				
Status	<input checked="" type="checkbox"/> Enabled				
Security Policies	WEB POLICY, Web-Auth (Modifications done under security tab will appear after applying the changes.)				
Radio Policy	All				
Interface/Interface Group(G)	management				
Multicast Vlan Feature	<input type="checkbox"/> Enabled				
Broadcast SSID	<input checked="" type="checkbox"/> Enabled				
NAS-ID	POD5WLC				

WLANS > Edit 'Pod5\_Guest'

<b>General</b>	<b>Security</b>	<b>QoS</b>	<b>Policy-Mapping</b>	<b>Advanced</b>
<b>Layer 2</b>	<b>Layer 3</b>	<b>AAA Servers</b>		
Layer 3 Security <a href="#">1</a> Web Policy <input type="button" value="▼"/> <ul style="list-style-type: none"> <li><input checked="" type="radio"/> Authentication</li> <li><input type="radio"/> Passthrough</li> <li><input type="radio"/> Conditional Web Redirect</li> <li><input type="radio"/> Splash Page Web Redirect</li> <li><input type="radio"/> On MAC Filter failure <a href="#">10</a></li> </ul> Preauthentication ACL      IPv4 <input type="button" value="None"/> IPv6 <input type="button" value="None"/> WebAuth FlexAcl <input type="button" value="None"/> Sleeping Client <input type="checkbox"/> Enable				
Over-ride Global Config <input type="checkbox"/> Enable				

**Step 4** On the **Advanced** tab:

- Set the **Enable Session Timeout** is **Enabled** and set to **600**
- Check the **Required** box for **DHCP Addr. Assignment**

<b>General</b>	<b>Security</b>	<b>QoS</b>	<b>Policy-Mapping</b>	<b>Advanced</b>
Allow AAA Override <input type="checkbox"/> Enabled Coverage Hole Detection <input checked="" type="checkbox"/> Enabled <div style="border: 1px solid red; padding: 5px;">           Enable Session Timeout <input checked="" type="checkbox"/> <input type="text" value="600"/> Session Timeout (secs)         </div> Aironet IE <input checked="" type="checkbox"/> Enabled Diagnostic Channel <a href="#">18</a> <input type="checkbox"/> Enabled				
<b>DHCP</b> DHCP Server <input type="checkbox"/> Override <div style="border: 1px solid red; padding: 5px;">           DHCP Addr. Assignment <input checked="" type="checkbox"/> Required         </div> <b>OEAP</b> Split Tunnel <input type="checkbox"/> Enabled				

**Note** Session Timeout was lowered to require a client re-authorization sooner. DHCP Addr. Required was set to for security purposes and blocks clients with a static IP address.

**Step 5** Click **Apply** and **OK**.

**Make the New WLAN Point to the Mobility Anchor WLC**

**Step 6** Hover the mouse over the blue dropdown arrow on the far right of the new WLAN and choose **Mobility Anchors**.

WLANS						
Current Filter:		None	[Change Filter] [Clear Filter]	Create New	Go	
WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
1	WLAN	Pod5_Guest	Pod5_Guest	Enabled	Web-Auth	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <span>Remove</span>  <span>Mobility Anchors</span> <span style="background-color: #0070C0; color: white; padding: 2px 5px;"> </span> <span>→</span>  <span>802.11u</span>  <span>Foreign Maps</span>  <span>Service Advertisements</span>  <span>Hotspot 2.0</span> </div>

**Step 7** On the **Switch IP Address (Anchor)** dropdown, choose: **172.16.0.20** (Anchor IP). Click on **Mobility Anchor Create**.

### Mobility Anchors

<b>WLAN SSID</b>	Pod5_Guest
<b>Switch IP Address (Anchor)</b>	172.16.0.20
<b>Mobility Anchor Create</b>	
<b>Switch IP Address (Anchor)</b>	172.16.0.20 <input type="button" value="▼"/>

**Step 8** Click **Ok** on the warning pop-up. The Data and Control Paths should be up (you can also do an ICMP ping from the dropdown to test connectivity).

### Mobility Anchors

<b>WLAN SSID</b>	pod1guest	<b>&lt; Back</b>	
<b>Switch IP Address (Anchor)</b>	172.16.0.20	<b>Data Path</b>	<b>Control Path</b>
<b>Mobility Anchor Create</b>		up	up <input checked="" type="checkbox"/>
<b>Switch IP Address (Anchor)</b>	local <input type="button" value="▼"/>		

**Note** Now the WLAN points to the Anchor (AnchorWLC).

## **Activity Verification**

You have successfully completed this task when you attain this result:

- Created a guest WLAN on the foreign controller (POD 2504 WLC)
- Added the Mobility Anchor to the guest WLAN.
- Verified that the Data path and Control Path are both up.

## **Task 4: Configure the Guest WLAN on the Anchor WLC.**

### **Activity Procedure**

In this task, you will add a guest WLAN to the Anchor WLC.

---

<b>Note</b>	The lower case "x" in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

#### **Create a New WLAN on the Mobility Anchor WLC**

Complete these steps:

**Step 1** Open a browser and connect to the AnchorWLC from the Admin PC

**Step 2** Navigate to **WLANS** and click on **Go** next to the **Create New** dropdown and enter the following:

- Profile Name: **Podx\_Guest** (x=pod#)
- SSID: **Podx\_Guest**
- Click **Apply**

**Step 3** On the **General** tab, enter the following:

- Status: **Enabled** (checked)
- Interface/Interface Group: **dmz** (the final destination of the guest tunnel will be exchanged with a local interface of which is common for a DMZ interface)

WLANS > Edit 'Pod5\_Guest'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	Pod5_Guest			
Type	WLAN			
SSID	Pod5_Guest			
Status	<input checked="" type="checkbox"/> Enabled			
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)			
Radio Policy	All			
Interface/Interface Group(G)	dmz			
Multicast Vlan Feature	<input type="checkbox"/> Enabled			
Broadcast SSID	<input checked="" type="checkbox"/> Enabled			
NAS-ID	AnchorWLC			

**Step 4** On the **Security** tab, enter the following:

- Layer 2 tab:
  - Layer 2 Security: **None**
- Layer 3 tab:
  - Layer 3 Security: **Web Policy**
  - Click **OK** on the pop-up warning
  - Verify that the **Authentication** radio button is selected

**Step 5** On the **Advanced** tab, enter the following:

- Enable Session Timeout: **Enabled** and set to **600**
- DHCP Addr. Assignment: **Required** (checked)

WLANS > Edit 'Pod5\_Guest'

General	Security	QoS	Policy-Mapping	Advanced
Allow AAA Override	<input type="checkbox"/> Enabled			
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled			
Enable Session Timeout	<input checked="" type="checkbox"/>	600	Session Timeout (secs)	
Aironet IE	<input checked="" type="checkbox"/> Enabled			
<b>DHCP</b> DHCP Server <input type="checkbox"/> Override DHCP Addr. Assignment <input checked="" type="checkbox"/> Required				
<b>OEAP</b>				

---

<b>Note</b>	Again, Session Timeout was lowered to require a client re-authorization sooner. And DHCP Addr. Required was set to for security purposes and blocks clients with a static IP address.
-------------	---

---

**Step 6** Click **Apply** and **Back**.

**Make the New WLAN Point to the Mobility Anchor WLC (itself)**

**Step 7** Hover the mouse over the blue dropdown arrow on the far right of the new WLAN and choose **Mobility Anchors**.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	anchor	anchor	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Pod5_Guest	Pod5_Guest	Enabled	Web-Auth

**Step 8** On the Switch IP Address (Anchor) dropdown, choose: **local** (Anchor). Then click on **Mobility Anchor Create**.

WLAN SSID	Pod5_Guest	
Switch IP Address (Anchor)	Data Path	Control Path
<b>Mobility Anchor Create</b>		
Switch IP Address (Anchor)	local	

**Step 9** Click **Ok** on the warning pop-up. The Data and Control Paths should be up (you can also do an ICMP ping from the dropdown to test connectivity).

WLAN SSID	Pod5_Guest	
Switch IP Address (Anchor)	Data Path	Control Path
local	up	up
<b>Mobility Anchor Create</b>		
Switch IP Address (Anchor)	192.168.51.5	

---

<b>Note</b>	Now the WLAN points to the Anchor itself (AnchorWLC) and is identified as the Anchor for your Podx WLC.
-------------	---

---

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- Created a guest WLAN on the Anchor controller (AnchorWLC).
- Added the Mobility Anchor to the guest WLAN.
- Verified that the Data path and Control Path are both up.

## **Task 5: Create Local User on the Anchor WLC.**

### ***Activity Procedure***

In this task, you will create a local user account on the Anchor WLC.

---

<b>Note</b>	The lower case “x” in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

#### **Create a Local User for your Podx on the Anchor WLC for Guest Access**

Complete these steps:

**Step 1** Open a browser and connect to the AnchorWLC from the Admin PC.

---

<b>Note</b>	Guest accounts can be created by admins, but you may also create a user with the Lobby role (Management > Local Mgt Users) and they can create guest accounts.
-------------	--

---

**Step 2** Go to the **Security** menu and on the left side, choose **AAA > Local Net Users** and select **New**. Then enter the following:

- User Name: **WLC**
- Password: **Cisco123**
- Confirm Password: **Cisco123**
- Guest User: **Checked**
- Lifetime: **86400** (24 hours)
- WLAN Profile: **Podx\_Guest** (only on your WLAN)
- Click **Ok** to information pop-up and **Apply**.

MONITOR   WLANS   CONTROLLER   WIRELESS   SECURITY   MANAGEMENT

Local Net Users > New

User Name	<input type="text" value="WLC"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>
Guest User	<input checked="" type="checkbox"/>
Lifetime (seconds)	<input type="text" value="86400"/>
Guest User Role	<input type="checkbox"/>
WLAN Profile	<input type="button" value="Pod5_Guest ▾"/>
Description	<input type="text"/>

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- Created a local Net User account on the Anchor WLC

## **Task 6: Associate the Client using WLC Credentials.**

### ***Activity Procedure***

In this task, you will test the Guest Web authentication using the WLC credentials.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

- Step 1** Connect to the Client PC.
- Step 2** Click the WLAN tray.
- Step 3** Click on the **Podx\_Guest** network, and then click **Connect**. (Uncheck the box for “Connect automatically”, you don’t want to create a profile).
- Step 4** Click the WLAN tray.
- Step 5** Right click the **Podx\_Guest** network and select **Status**.
- Step 6** On the **General** tab of the Status window, click the **Details** button.

**Step 7** You will now see your IP address (**dmz** network 172.16.2.0).

**Step 8** Open a Command Prompt and ping your gateway (172.16.2.254). This attempt should fail.

---

<b>Note</b>	Even though you have an IP address, you have not yet authenticated, so the gateway is not accessible.
-------------	---

---

**Step 9** Verify your client connection on the WLC and on the AnchorWLC Monitor menus.

**Step 10** Open a Firefox browser on the Client PC.

**Step 11** For the URL address, type: **192.168.11.5** and **Enter**.

**Step 12** On the Untrusted Connection warning, click on **I Understand the Risks**, and then **Add Exception**.

**Step 13** On the pop-up, click **Confirm Security Exception**. You will now see the Login screen.



The screenshot shows a web browser window with a blue header bar containing the word "Login". Below the header, the main content area has a title "Welcome to the Cisco wireless network" followed by a message: "Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work." There are two input fields: "User Name" with the value "WLC" and "Password" with the value "Cisco123". A "Submit" button is located at the bottom of the form.

**Step 14** Enter your username of **WLC** and password of **Cisco123** and click **Submit**.



**Step 15** The system will try to direct you to your original destination (POD 2504 WLC Login), but will fail, as that address is not reachable from the Anchor's **dmz** VLAN.

---

<b>Note</b>	Depending on the Lab setup, you may not be able to reach the internet. In a normal situation, the dmz VLAN would be routed directly to the internet.
-------------	--

---

**Step 16** Open a Command Prompt and ping your gateway (172.16.2.254), it should be successful now.

**Step 17** Verify your client connection on the WLC and AnchorWLC Monitor menus.

**Step 18** When done, disconnect from the **Podx\_Guest** WLAN.

## **Activity Verification**

You have successfully completed this task when you attain this result:

- Connected your wireless client to the Guest WLAN using your local user credentials.
- Client got an IP address in the proper range and could ping the gateway.

# Task 7: Associate the Client using ISE Credentials.

## Activity Procedure

In this task, you will test the Guest Web authentication using the ISE credentials.

<b>Note</b>	Although we will point to each Pod's ISE host, in a production environment, our ISE host would be centralized.
-------------	--

### Create a User in ISE for Guest Authentication

First, you will need to connect to our RADIUS server (Cisco ISE) to create a remote user account.

Complete these steps:

- Step 1** Connect to the Admin PC.
- Step 2** Open a browser and connect to the AnchorWLC from the Admin PC.
- Step 3** Still on the Admin PC, open the Firefox browser to connect to the Cisco ISE.
- Step 4** Enter **192.168.11.21** for the address of the ISE.
- Step 5** On the Untrusted Connection warning, click on **I Understand the Risks**, and then **Add Exception**.
- Step 6** On the pop-up, click **Confirm Security Exception**.
- Step 7** At the ISE login screen, enter the username of **admin** and password of **1234QWer** and click **Login**.
- Step 8** Click **OK** on any warnings about the license expiration.
- Step 9** You should already have a user from a previous lab. Verify this by going to **Administration > Identity Management > Identities > Users** and confirming that the user, **poduser** is available.
- Step 10** If there is not a user, create a user with the name of **poduser** with a password of **Cisco123** and click **Submit**.

### Add the Anchor WLC (NAD) in ISE

You will need to connect to our RADIUS server (Cisco ISE) to create a connection to the AnchorWLC.

- Step 11** Select **Administration > Network Resources > Network Devices** and click **+Add** and enter the following:
  - Name for the WLC: **AnchorWLC**
  - IP address and network mask of the AnchorWLC: **172.16.0.20 / 32**
  - Authentication Settings: **Checked** (the window opens for the settings)
  - Password for the Shared Secret entry: **Cisco123**
  - Click **Submit**.

The screenshot shows the 'Network Devices List > New Network Device' configuration page. The 'Name' field is set to 'AnchorWLC'. The 'IP Address' field shows '172.16.0.20 / 32'. Under 'Authentication Settings', the 'Protocol' is set to 'RADIUS' and the 'Shared Secret' is listed as 'Cisco123'.

### Add the ISE (RADIUS) in the Anchor WLC

Next, create a connection between the AnchorWLC and the RADIUS server using a Shared Secret password.

**Step 12** On the AnchorWLC, go to the **Security** menu and choose **AAA > RADIUS > Authentication**, select **New** and enter the following:

- IP address of the RADIUS server (ISE): **192.168.11.21**
- Enter the same Shared Secret password the you entered on the RADIUS server: **Cisco123**
- Click **Apply**

The screenshot shows the 'RADIUS Authentication Servers > New' configuration page. The fields filled in are:

- Server Index (Priority): 1
- Server IP Address(Ipv4/Ipv6): 192.168.51.21
- Shared Secret Format: ASCII
- Shared Secret: (redacted)
- Confirm Shared Secret: (redacted)
- Key Wrap: (unchecked) (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Disabled
- Server Timeout: 2 seconds
- Network User:  Enable
- Management:  Enable
- IPSec:  Enable

**Step 13** Hover over the blue arrow on the far right side of the row with the new server and choose **Ping**. You will get a ping response that verifies the connection is good.

#### Modify the WLAN for your ISE (AAA) Server

**Step 14** On the Anchor WLC GUI, navigated to **WLANS > WLANS**.

**Step 15** Click on the WLAN ID for your **Podx\_Guest** WLAN.

**Step 16** Navigate to **Security tab > AAA servers** and enter the following:

- Verify that under **Authentication Servers**, the **Enabled** option is checked.
- Under **Accounting Servers**, the **Enabled** option should be unchecked.
- For the drop down for **Server 1**, choose your ISE (AAA) server: **192.168.11.21**
- Click **Apply**

WLANS > Edit 'Pod5\_Guest'

<b>General</b>	<b>Security</b>	<b>QoS</b>	<b>Policy-Mapping</b>	<b>Advanced</b>																																
<b>Layer 2</b>	<b>Layer 3</b>	<b>AAA Servers</b>																																		
<p>Select AAA servers below to override use of default servers on this WLAN</p> <p><b>Radius Servers</b></p> <p>Radius Server Overwrite interface <input type="checkbox"/> Enabled</p> <table border="1"> <thead> <tr> <th colspan="2">Authentication Servers</th> <th colspan="2">Accounting Servers</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Enabled</td> <td></td> <td><input type="checkbox"/> Enabled</td> <td></td> </tr> <tr> <td>Server 1</td> <td>IP:192.168.51.21, Port:1812</td> <td>None</td> <td>None</td> </tr> <tr> <td>Server 2</td> <td>None</td> <td>None</td> <td>None</td> </tr> <tr> <td>Server 3</td> <td>None</td> <td>None</td> <td>None</td> </tr> <tr> <td>Server 4</td> <td>None</td> <td>None</td> <td>None</td> </tr> <tr> <td>Server 5</td> <td>None</td> <td>None</td> <td>None</td> </tr> <tr> <td>Server 6</td> <td>None</td> <td>None</td> <td>None</td> </tr> </tbody> </table> <p><b>Radius Server Accounting</b></p>					Authentication Servers		Accounting Servers		<input checked="" type="checkbox"/> Enabled		<input type="checkbox"/> Enabled		Server 1	IP:192.168.51.21, 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
Authentication Servers		Accounting Servers																																		
<input checked="" type="checkbox"/> Enabled		<input type="checkbox"/> Enabled																																		
Server 1	IP:192.168.51.21, 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																																	

### Verify WebAuth with ISE on Client

- Step 17** Connect to the Client PC.
- Step 18** Click the WLAN tray.
- Step 19** Click on the **Podx\_Guest** network, and then click **Connect**. (Uncheck the box for “Connect automatically”, you don’t want to create a profile).
- Step 20** Click the WLAN tray.
- Step 21** Right click the **Podx\_Guest** network and select **Status**.
- Step 22** On the **General** tab of the Status window, click the **Details** button.
- Step 23** You will now see your IP address (**dmz** network 172.16.2.0).
- Step 24** Open a Command Prompt and ping your gateway (172.16.2.254). This attempt should fail.

---

<b>Note</b>	Even though you have an IP address, you have not yet authenticated, so the gateway is not accessible.
-------------	---

---

- Step 25** Verify your client connection on the WLC and on the AnchorWLC Monitor menus.
- Step 26** Open a Firefox browser on the Client PC.
- Step 27** For the URL address, type: **192.168.11.5** and **Enter**.
- Step 28** On the Untrusted Connection warning, click on **I Understand the Risks**, and then **Add Exception**.
- Step 29** On the pop-up, click **Confirm Security Exception**.

---

<b>Note</b>	This warning is issued because the WLC uses a self-signed certificate.
-------------	--

---

**Step 30** At the Login Screen, enter your username of **poduser** and password of **Cisco123** and click **Submit**.

**Step 31** The system will try to direct you to your original destination (POD 2504 WLC Login), but will fail, as that address is not reachable from the Anchor's **dmz** VLAN.

---

<b>Note</b>	Depending on the Lab setup, you may not be able to reach the internet. In a normal situation, the <b>dmz</b> VLAN would be routed directly to the internet.
-------------	---

---

**Step 32** Open a Command Prompt and ping your gateway (172.16.2.254), it should be successful now.

**Step 33** Verify your client connection on the WLC and AnchorWLC Monitor menus.

#### Verify WebAuth Operation with ISE

**Step 34** Open a Web Browser and connect to the ISE host (192.168.11.21).

**Step 35** Login and navigate to **Operations > Authentications**. Here you will see the Authentications in the last 24 hours. Look closely at what is displayed.

**Step 36** Click the icon under Details to see even more information.

**Step 37** When done, disconnect from the **Podx\_Guest** WLAN.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Connected your wireless client to the Guest WLAN using your ISE user credentials.
- Client got an IP address in the proper range and could ping the gateway.
- Verified your use authentication on ISE

# Task 8: Lab Cleanup

## ***Activity Procedure***

### **Temporality Turn off Centralized AP on AireOS WLC**

---

**Note** You are going to disable the Centralized AP to create channel space and remove any distractions of another AP for now.

**Note** Complete these steps:

---

**Step 1** On the Admin PC, open another tab on the browser and connect to the **WLC** (IP = 192.168.11.5 and username/password = **admin/Cisco123**).

**Step 2** Navigate to the **Wireless** menu.

**Step 3** Click on the AP1 and select the following:

- On the **General** Tab, choose **Disable** from the **Admin Status** dropdown.
- Click **Apply** and **Back**.

AP **Admin Status** should now be **Disabled**.

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- Temporality turned off Centralized AP on AireOS WLC.



# **Hardware Lab 7: Deploying a Converged Access WLAN**

## **Overview**

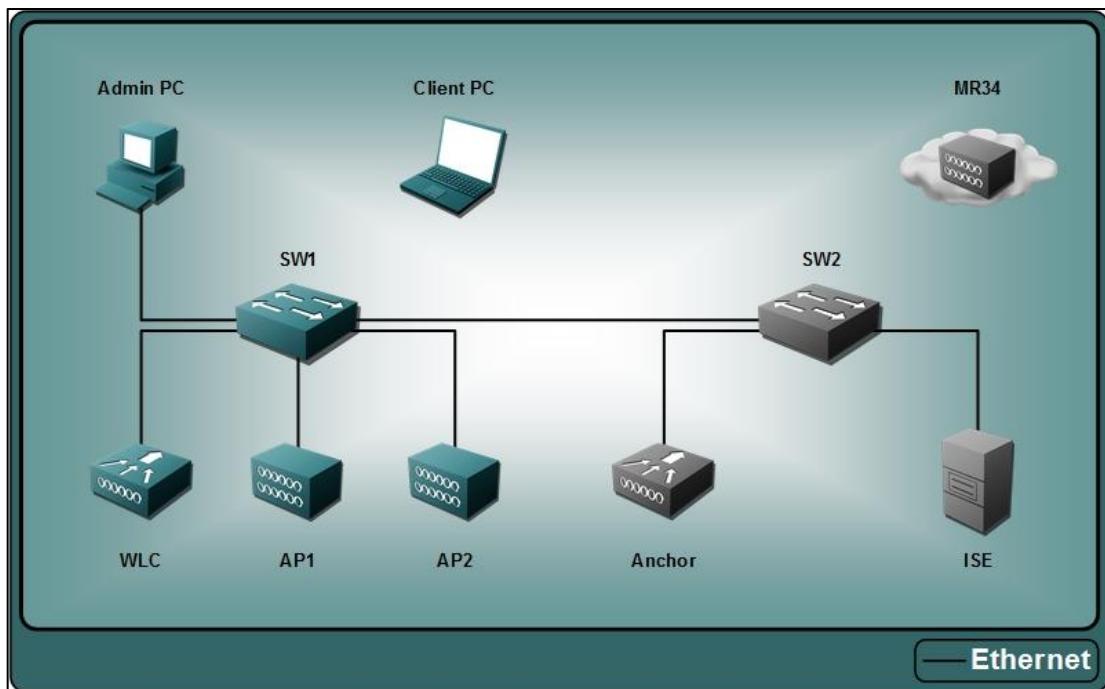
In this activity, you configure the switch to enable converged WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Verify the 3650 status
- Initialize 3650 WCM and AP
- Adjust RF power and channel settings
- Create a WLAN
- Enable additional features for the WLAN
- Associate a wireless client
- Review CleanAir
- Disassociate the wireless client

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

Here are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 3650 IOS-XE Switch (WCM)
- AP 3700i (Converged AP)

## VLANs and IP Ranges

### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
Pod 3650 Switch	192.168.11.254	admin	Cisco123	cisco
ISE (RADIUS)	192.168.11.21	admin	1234QWer	

## RF Channels

Pod	RF Channel 802.11b/g/n	RF Channel 802.11a/n/ac
1, 9, 17	1	36
2, 10, 18	6	40
3, 11, 19	11	44
4, 12, 20	1	48
5, 13, 21	6	52
6, 14, 22	11	56
7, 15, 23	1	60
8, 16, 24	6	64

## Task 1: Verify the Catalyst 3650 Status

### Activity Procedure

In this task, you will verify the initial settings of the Catalyst 3650 for wireless. Although the switch was previously set up (wired portion), the wireless portion has not been configured (WCM). It is a converged switch, but you will have to manage it separately in the Web GUI. Be aware the IOS-XE WEB GUI is a little slow in responding.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

- Step 1** Connect to the Admin PC.
- Step 2** Open a web browser (IE) and type the URL address of **http://192.168.11.254** and press **Enter**.
- Step 3** You will be prompted for a username/password, type in the following and press **OK**:
  - Username : **admin**
  - Password: **Cisco123**

---

**Note** If you typed “https” then you will get a Certificate Warning” page. You must go back and use HTTP for our lab.

---

**Note** If the login does not work, the initial configuration script might have misconfigured the user due to a bug.

Use the following command on the SW1 CLI to see what the script configured:

```
show running-config | include username
```

Use the following command to correct this error:

```
username admin privilege 15 password 0 Cisco123
```

---

## Cisco Systems

### Accessing Cisco WS-C3650-24PS "SW1"

Telnet - to the router.

Show interfaces - display the status of the interfaces.

Show diagnostic log - display the diagnostic log.

Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Show tech-support - display information commonly needed by tech support.

Extended Ping - Send extended ping commands.

Wired Web GUI - Configure basic connectivity on the Switch.

Wireless Web GUI - Configure wireless on the Switch through the Web GUI interface.

---

### Help resources

1. [CCO at www.cisco.com](http://www.cisco.com) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. [tac@cisco.com](mailto:tac@cisco.com) - e-mail the TAC.
3. [1-800-553-2447](tel:1-800-553-2447) or [+1-408-526-7209](tel:+1-408-526-7209) - phone the TAC.
4. [cs-html@cisco.com](mailto:cs-html@cisco.com) - e-mail the HTML interface development group.

**Step 4** You will now see the main Web GUI screen. From here you can:

- Access a few basic commands (ex: show interfaces and diagnostic logs)
- Access the Wired Web GUI
- Access the Wireless Web GUI

**Step 5** Click the **Wireless Web GUI**

**System Summary**

System Time	18:01:44.875 UTC Tue May 5 2015
Software Version	03.06.01E RELEASE SOFTWARE (fc3)
System Name	SwitchPod1
System Model	WS-C3650-24PS
Up Time	1 hour, 31 minutes
Wireless Management IP	169.254.1.1
802.11 a/n/ac Network State	Enabled
802.11 b/g/n Network State	Enabled
Mobility Role	MA
Software Activation	<a href="#">Detail</a>

**Access Point Summary**

	Total	Up	Down
802.11a/n/ac Radios	0	0	0
802.11b/g/n Radios	0	0	0
All APs	0	0	0

**Client Summary**

**Protocol Statistics**

**Top WLANs**

Profile Name	Number of Clients
--------------	-------------------

**Rogue APs**

Active Rogue APs	0	<a href="#">Detail</a>
------------------	---	------------------------

Active Rogue Clients	0	<a href="#">Detail</a>
----------------------	---	------------------------

Adhoc Rogues	0	<a href="#">Detail</a>
--------------	---	------------------------

**Step 6** You will now be at the **Home** screen of the Wireless Controller.

You will notice that the wireless portion is not yet configured, so there is not an IP address for the Wireless Management Interface. The default role is Mobility Agent as the WCM is not yet activated. There are no APs connected, because the Wireless Interface has not been defined.

- System Name is SW1 (done in previous lab)
- Wireless Management IP is a link local address (ex:169.254.1.1)
- Mobility Role is MA (Mobility Agent)
- No APS (3650 WCM/Switch needs additional configuration)

**Step 7** At the top the screen is menus (Home, Monitor, Configuration, Administration, and Help), click the arrow beside **Configuration** and choose **Controller**.

**Step 8** On the left side, click **Internal DHCP Server** folder and then **DHCP Scope**. Review the following options:

- The **mgt** scope was created for management addresses, which will include your eventual AP IP address.
- The **ap** scope was created for the Centralized AP IP addresses.
- The **client** scope was created for the wireless client subnet.
- Click the **ap** pool name and see that Option 43 is not here (even though it's configured)

The screenshot shows the Cisco Wireless Controller Web GUI. The left sidebar has a tree view with nodes like System, Interfaces, VLAN, Internal DHCP Server (with DHCP Scope selected), and Management. The main panel is titled 'DHCP Scope' and contains a table with three rows. The columns are 'Pool name' and 'IP Type'. The rows are: mgt (ipv4), ap (ipv4), and client (ipv4). There are 'New' and 'Remove' buttons at the top of the table.

	Pool name	IP Type
<input type="checkbox"/>	mgt	ipv4
<input type="checkbox"/>	ap	ipv4
<input type="checkbox"/>	client	ipv4

**Note** The above is an example of what is sometimes “not displayed” from the Wireless Web GUI. To see the total settings for this DHCP Scope, you would need to go to the CLI.

**Step 9** On the left side, click **NTP** folder and then **Server**.

**Step 10** Notice that the following the NTP server IP address is there from the switch setup that was done previously.

**Step 11** Close the web browser.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- You have logged on to the Wireless Web GUI interface and observed the default configuration for the Wireless Controller.
- You have verified that the Wired configuration overlaps in some places with the Wireless configuration.

## **Task 2: Initialize the Cat3650 Wireless Controller and AP**

### **Activity Procedure**

In this task, you will initialize the Cat3650 WCM /switch to connect the AP.

Complete these steps:

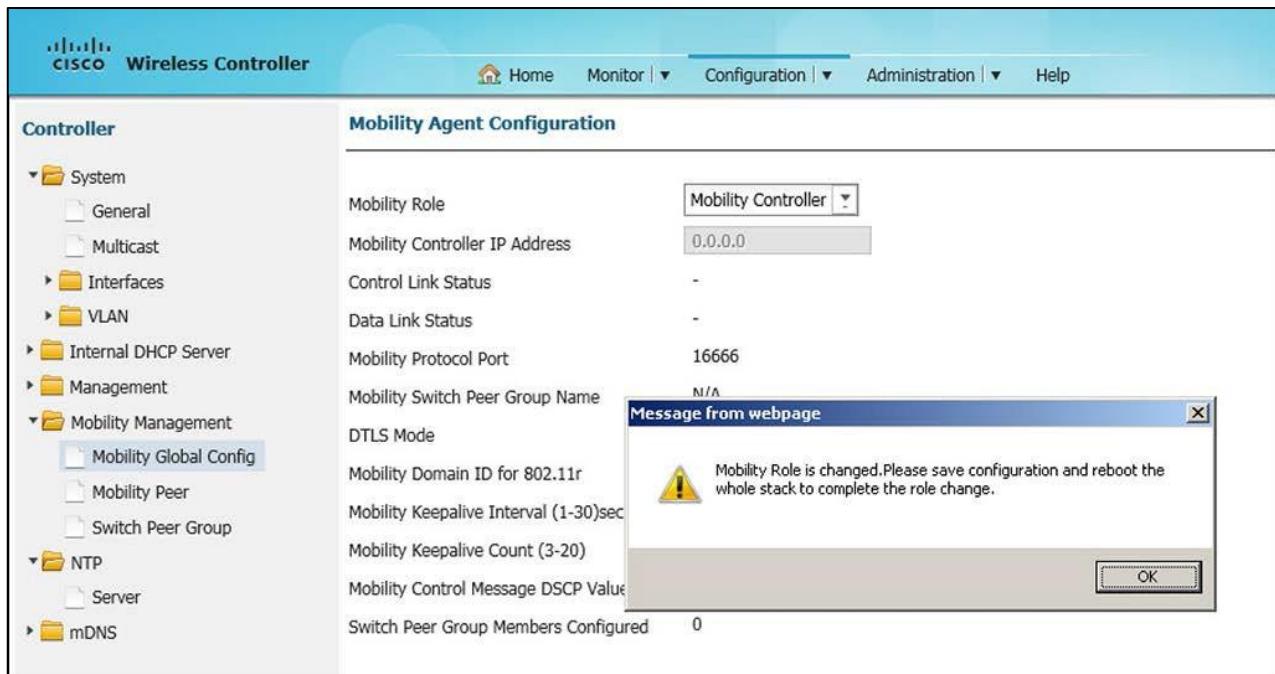
**Step 1** Connect to the Admin PC.

- Step 2** Open a web browser (**IE**), and type the URL address of **http://192.168.11.254/wireless** (x=pod#) and press **Enter**. This time, you will bypass the Wired/Wireless GUI and go right to Wireless.
- Step 3** You will be prompted for a username/password, enter the following, and press **OK**.
- Username : **admin**
  - Password: **Cisco123**

### Make the Catalyst 3650 a Mobility Controller

You saw earlier that the Catalyst 3650 was a Mobility Agent. Since you don't have a WLC acting as a Mobility Controller, you will make the switch a Mobility Controller.

- Step 4** At the top the screen, go to **Configuration > Controller**.
- Step 5** On the left side, click **Mobility Management** folder and then **Mobility Global Config**.
- Step 6** From the Mobility Role dropdown, select **Mobility Controller**.



- Step 7** Near the top right, click **Apply**. Click **OK** and **OK** on the pop-up that your configuration was submitted (running configuration).

<b>Note</b>	Notice the pop-up indicating that you must save the configuration and reboot (changing the Role requires a reboot).
-------------	---

- Step 8** On the top right of the screen, click **Save Configuration** (startup configuration).
- Step 9** Click **OK** on pop-up stating: Are you sure you want to save the configuration to flash...
- Step 10** Click **OK** on the save confirmation pop-up.

### Reboot the Catalyst 3650 a Mobility Controller

For an MA to become an MC requires a reboot for it to take effect.

- Step 11** Navigate to **Configuration > Commands** from the top menu.

- Step 12** On the left side, click **Reboot**.
- Step 13** Click **Save and Reboot**—(yes, you did already perform a save, but it's good to verify that).
- Step 14** Click **OK** on the save confirmation/reboot pop-up.
- Step 15** The switch will now reload, and it will take approx. 5 minutes.
- Step 16** Connect to the Console port of the switch to verify when it is back up and watch the reboot.
- Verify the Catalyst 3650 is a Mobility Controller**
- Step 17** If logged out of the 3650 WCM, then log back using earlier steps.

System Summary	
System Time	19:20:40.558 UTC Tue May 5 2015
Software Version	03.06.01E RELEASE SOFTWARE (fc3)
System Name	SwitchPod1
System Model	WS-C3650-24PS
Up Time	10 minutes
Wireless Management IP	169.254.1.1
802.11 a/n/ac Network State	Enabled
802.11 b/g/n Network State	Enabled
Mobility Role	MC
Software Activation	<a href="#">Detail</a>

- Step 18** Notice at the Home screen, the **Mobility Role** is now **MC** (Mobility Controller) and not **MA** (as it was in the beginning).

### Configure Mobility Options

Next you want to change your Mobility Group to match the one for the WLC 2504. Being in the same Mobility Group, the Controllers can share the context and state of client device and their list of access points so that they do not consider each other's access points as rogue devices.

- Step 19** At the top the screen, click the arrow beside **Configuration** and choose **Controller**.
- Step 20** On the left side, click **Mobility Management** folder and then **Mobility Global Config**.
- Step 21** Change the Mobility Group Name to **Podx** (x=pod#) to match the AireOS WLC.
- Step 22** Click **Apply** and **OK** on the pop-up that your configuration was submitted.

The screenshot shows the Cisco Wireless Controller web interface. The left sidebar has a tree view under 'Controller' with 'System' and 'Interfaces' expanded. Under 'System', 'General' and 'Multicast' are listed. Under 'Interfaces', 'Port Summary' and 'Wireless Interface' are listed. The main panel is titled 'Mobility Controller Configuration' and contains the following fields:

Mobility Role	<input type="text" value="Mobility Controller"/>
Mobility Controller IP Address	<input type="text" value="0.0.0.0"/>
Mobility Protocol Port	16666
Mobility Group Name	<input type="text" value="Pod1"/>
Mobility Oracle IP Address	<input type="text" value="0.0.0.0"/>

**Note** Take note that the Mobility Group Name is now the same for both the AireOS and IOS-XE WCMs.

### Configure for AP Connectivity

**Step 23** Select **Configuration > Controller > System > Interfaces > Wireless Interface**. The Management Interface is currently **Unconfigured**. Click **Unconfigured** and enter the following:

- VLAN dropdown: **VLAN11**
- It changes the wireless management VLAN to 11
- Click **Apply**

**Step 24** Click **OK** on the pop-up that your management interface was created.

**Note** Now the Wireless Interface for AP connectivity is associated with Management VLAN of 11

**Step 25** Verify the following:

- Wireless Interface name: **VLAN11**
- IP Address: **192.168.11.254**

**cisco Wireless Controller**

Home Monitor | Configuration | Administration | Help

**Controller**

Wireless Interface

New Remove Show

Interface Type	Interface Name	IP Address	IP Netmask	MAC Address	VlanID
<input type="checkbox"/> Management	Vlan11	192.168.11.254	255.255.255.0	24E9:B308:6A54	11

System  
General  
Multicast  
Interfaces  
Port Summary  
Wireless Interface



**Step 26** Click the **Home** menu and verify that the Wireless Management IP Address is now **192.168.11.254**.

**Step 27** Navigate to **Configuration > Wireless > Access Points > All APs** and notice that there are no APs connected.

---

**Note** At this point, the AP is still not connected. You now need to make some switch port changes for the AP to connect.

---

**Step 28** Connect to the console port of the Pod 3650 switch.

**Step 29** Press enter until the **SW1** prompt appears.

**Step 30** Type: **enable** and press **Enter**.

**Step 31** Type: password of **cisco** and press **Enter**.

**Step 32** Type: **config term** and press **Enter** to enter global configuration mode.

**Step 33** Enter the following to change the AP1 switch port:

```
SW1 (config)# interface g1/0/1
SW1 (config-if)# switchport access vlan 11
SW1 (config-if)# shut
SW1 (config-if)# no shut
```

---

**Note** The connection port for the AP has to have the same VLAN as the Wireless Interface (Vlan 11), so the AP could get an IP address (from our DHCP Pool of 192.168.11.0) and connect.

---

**Step 34** Connect to the console port of the **AP1**.

**Step 35** Observe the AP boot up process. You will see the AP get an IP address (192.168.11.0 network) and join the WCM 3650 .

- As the AP is most likely not on the correct software level, it may have to update the software and reboot (few minutes).
- You will eventually see on the AP a message that it has **joined to SW1**.

```
*Jun 23 22:36:44.831: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to r
eset
*Jun 23 22:36:44.855: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller Switc
hPod1
*Jun 23 22:36:44.995: %LINK-6-UPDOWN: Interface Dot11Radio0, changed state to up
*Jun 23 22:36:45.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio
0, changed state to down
*Jun 23 22:36:45.859: %LINK-6-UPDOWN: Interface Dot11Radiol, changed state to do
wn
```

**Step 36** Verify DHCP IP address from **SW1**:

- Connect to the **SW1** Console port and login

- At the Enable prompt, type: **show ip dhcp bind**
- Look for an address in the **192.168.11.0** network
- It should be the AP and you will verify that next

### Verify that AP is connected to WCM 3650

**Step 37** From the Web GUI of the WCM 3650, navigate to **Configuration > Wireless** and then the **Access Points** folder and then **All APs**.

**Step 38** You will see the AP and note what you saw earlier, that the **Operation State** is **Registered**.

AP Name	AP Model	AP Mac	Operation State	Location	Slot	Priority	Group Name	Country
AP07f.06da.6be4	3702I	F07F.06DA.6BE4	Download or Registered	default location	2	Critical	default-group	US

**Note** The AP Operational State may show “Download” (updating software), but will eventually show as “Registered” (just refresh the screen).

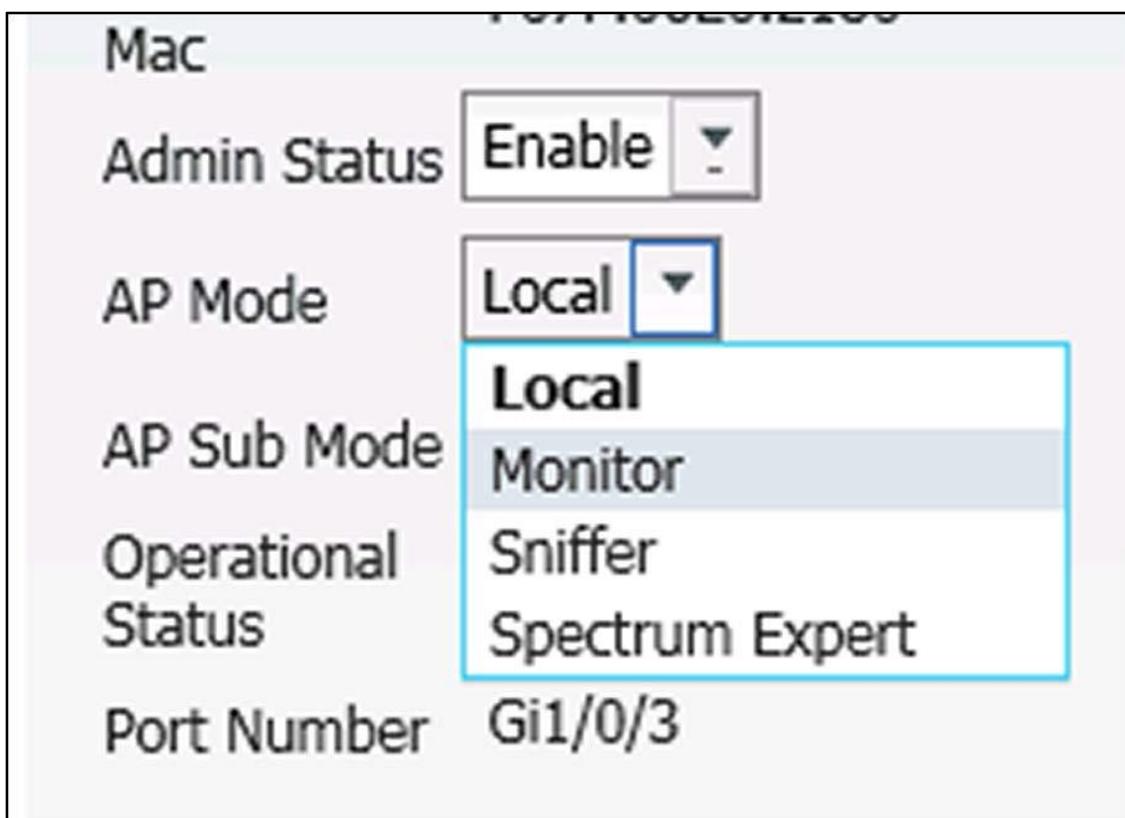
### Configure the Converged AP on WCM 3650

The AP is connected, but you want to configure it with a host name and enable it for operation.

AP Name	AP Model	AP Mac	Operation State	Location	Slot	Priority	Group Name	Country
APa89d.21ed...	3702I	A89D.21ED.90...	Registered	default location	2	Low	default-group	US

**Step 39** You will also see on that same row, the MAC, Model, Country, and more.

**Step 40** Click the AP name and configure the following:



- AP name: **AP1**
- Verify that Admin Status drop-down is **Enable**.
- Notice that the AP Mode is **Local** (check the drop-down for limited AP modes)
- Click **Apply**. Read the Pop-up message and click **OK**.

The screenshot shows the Cisco Wireless Controller interface. In the left sidebar under 'Wireless', 'Access Points' is expanded, and 'All APs' is selected. The main content area is titled 'AP' and 'AP > Edit'. The 'General' tab is active. The 'General' section contains fields for AP Name (set to 'AP1'), Location ('default location'), AP MAC Address ('F07F.06DA.6BE4'), Base Radio Mac ('F07F.06E0.2180'), Admin Status ('Enable'), AP Mode ('Local'), AP Sub Mode ('None'), Operational Status ('REG'), and Port Number ('Gi1/0/3'). To the right of these fields is a 'Version' section with various status parameters. Below the general section is an 'IP Config' section with fields for IP Address (192.168.11.27) and Static IP (unchecked). At the bottom is a 'Time Statistics' section.

**Step 41** The AP Operation State should be **Registered** and display its new name.

The screenshot shows the Cisco Wireless Controller home screen. The left sidebar shows 'Wireless' with 'Access Points' expanded and 'All APs' selected. The main area is titled 'All APs' and displays a table with one row. The table columns are AP Name, AP Model, AP Mac, Operation State, Location, Slot, Priority, Group Name, and Country. The single entry is 'Converged\_AP' (Model 3702I, Mac F07F.06DA.6B..., State Registered, Location default location, Slot 2, Priority Low, Group Name default-group, Country US).

**Step 42** The AP will also show as **Up** in the **Home** screen **Access Point Summary**.

**Step 43** On the top right of the screen, click **Save Configuration**.

**Step 44** Click **OK** on pop-up stating: Are you sure you want to save the configuration to flash...

**Step 45** Click **OK** on the save confirmation pop-up.

## Activity Verification

You have successfully completed this task when you attain this result:

- You have made the WCM 3650 a Mobility Controller and added it to the Podx Mobility Group.
- You have changed the Management VLAN to x1.
- You have modified the AP switch port to use Vlan 11 and turned on the port.
- The Converged AP has joined the controller.
- The Centralized AP on WLC has been administratively disabled.

- The Converged AP name has been changed and has been administratively enabled.
- You have verified that the AP is in Local Mode.
- The configuration on the 3650 has been saved.

### CLI Changes

```
SW1 (config) # interface GigabitEthernet1/0/1
SW1 (config-if) # description Converged
SW1 (config-if) # switchport access vlan 11
SW1 (config-if) # switchport mode access
```

## Task 3: Adjust RF Power and Channel

### **Activity Procedure**

In this task, you will adjust the RF power and channel information for the AP Radios.

Since the pods are close, you want to allocate channels as best as you can and dial the power down.

**Step 1** Connect to the **SW1** from the Admin PC.

**Step 2** Log in to the WCM 3650 (SW1)

#### **RF Channel settings and Power levels (per radio type by AP)**

**Step 3** At the top, navigate to **Configuration > Wireless**. Select the **Access Points** folder and then **Radios** folder.

**Step 4** Click the **802.11b/g/n** Radios.

**Step 5** Check the box next to the **Converged AP** and then Click on **Configure** (above the menu).

<b>Note</b>	The following settings might already be in place. In this case you just need to verify them.
-------------	--

**Step 6** Change the **RF Channel Assignment** to **Custom** and then choose a channel as stated in the **Job Aids** section from the dropdown.

It allows for three non-overlapping channels. There will be co-channel interference (two or more on same channel), but they can “see each other” from an RF standpoint. You don’t want overlapping channels (ex: 1 and 2), as they just can’t “see each other” and it looks like interference.

**Step 7** Change the **Tx Power level Assignment** to **Custom** and choose **5** (lowest to mitigate the co-channel transmissions) and click **Apply** and **OK** to pop up.

**Wireless**

**802.11 b/g/n Radios**

802.11 b/g/n Radios > Edit

**General**

AP Name: AP1  
Admin Status: Enabled  
Operation Status: DOWN  
Slot #: 0

**11n Parameters**

11n Supported: Yes

**CleanAir**

**RF Channel Assignment**

Current Channel: 1  
Assignment Method:  Global  Custom  
1

**Tx Power Level Assignment**

Current Tx Power Level: 8  
Assignment Method:  Global  Custom  
5

**Performance Profile**

**Step 8** Under Access Points folder and then Radios folder, click the **802.11a/n/ac Radios**.

**Step 9** Check the box next to the **Converged AP** and then Click on **Configure** (above the menu).

**Step 10** Change the **RF Channel Assignment** to **Custom** and then choose the channels from the dropdown as stated in the **Job Aids** section.

You are again picking non-overlapping channels, but now you have more channels. The co-channel issue is now lessened with this many channels.

**Step 11** Change the **Tx Power level Assignment** to **Custom** and choose **6**(lowest—you don't need much coverage) then click **Apply** and **OK** to pop up

**Wireless**

**802.11 a/n/ac Radios**

802.11 a/n/ac Radios > Edit

**General**

AP Name: AP1  
Admin Status: Enabled  
Operation Status: DOWN  
Slot #: 1

**11n and 11ac Parameters**

11n Supported: Yes  
11ac Supported: Yes

**CleanAir**

**RF Channel Assignment**

Current Channel: 165  
Channel width: 20 MHz  
Assignment Method:  Global  Custom  
165

**Tx Power Level Assignment**

Current Tx Power Level: 5  
Assignment Method:  Global  Custom  
6

**Performance Profile**

---

<b>Note</b>	Notice that channels 120-128 Dynamic frequency Selection (DFS) channels and are unusable.
-------------	---

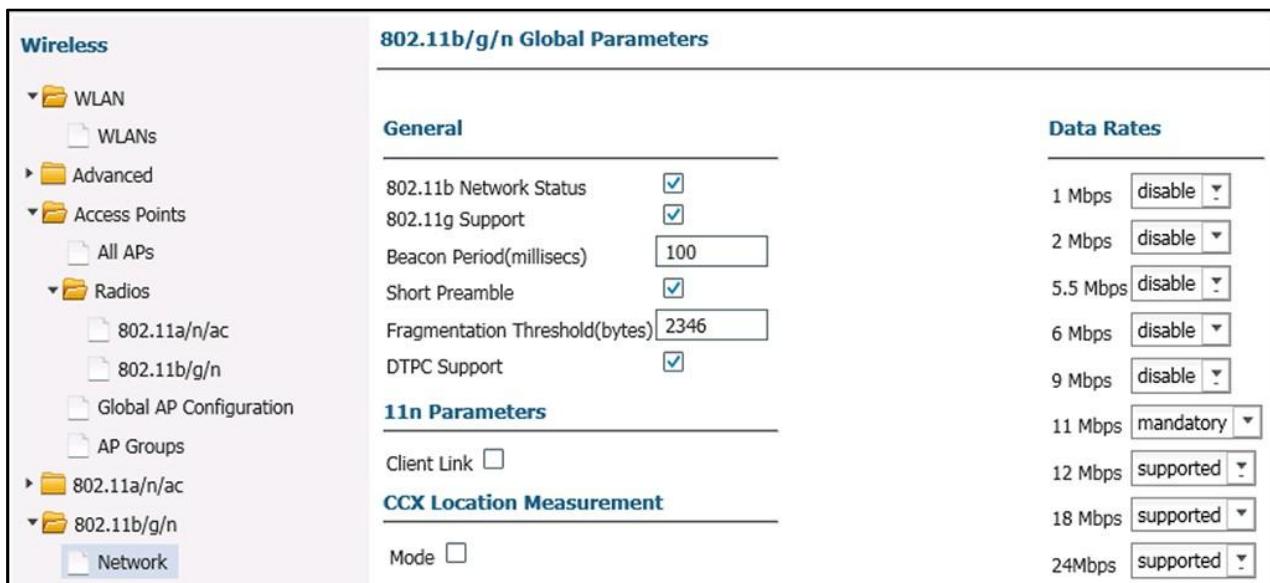
---

## Global Radio Settings

To improve performance, you are going to disable the low data rates.

**Step 12** On the left side, click the **802.11b/g/n** folder and then click **Network** and select the following:

- Disable the **1, 2, 5.5, 6, 9, Data Rates** and make **11 mandatory** (it improves roaming at the cell edge. You could also eliminate 11 Mbps and make a higher rate mandatory. It would stop your 802.11b clients from connecting).
- Click **Apply** and **OK** to pop up warning and then OK on change confirmation.



**Step 13** On the top right of the screen, click **Save Configuration** and click **OK** on the pop-ups.

## Activity Verification

You have successfully completed this task when you attain this result:

- You have configured the 2.4/5 GHz radios channel and power setting according to the instructions.
- Verified settings, by going to Monitor>Wireless and look at each radio for the AP (channel and power).

## Task 4: Configure a WLAN

### Activity Procedure

In this task, you will configure a WLAN with Open Authentication. You will later use it to verify the operation of your deployment.

Complete these steps:

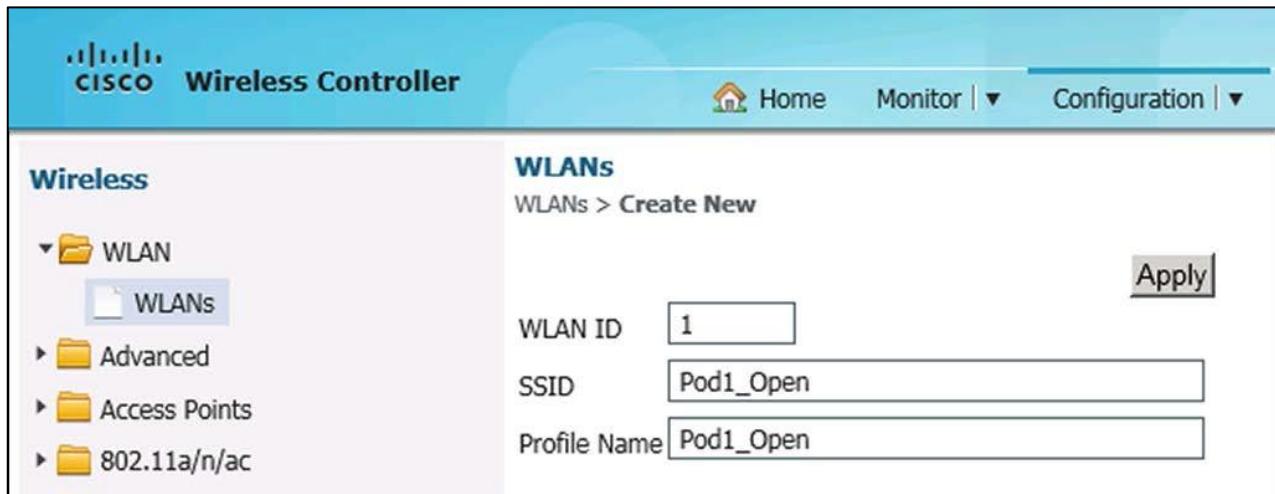
**Step 1** Connect to the **SW1** from the Admin PC.

**Step 2** Log in to the **WCM 3650 (SW1)**.

**Step 3** At the top, navigate to **Configuration > Wireless** and select the **WLAN** folder on the left, and then **WLANS**.

**Step 4** Click **New** at the top and enter the following information (x=pod#):

- WLAN ID: **1**
- SSID: **Podx\_Open** (name indicates location and purpose)
- Profile: **Podx\_Open**
- Click **Apply** and **OK** to pop up



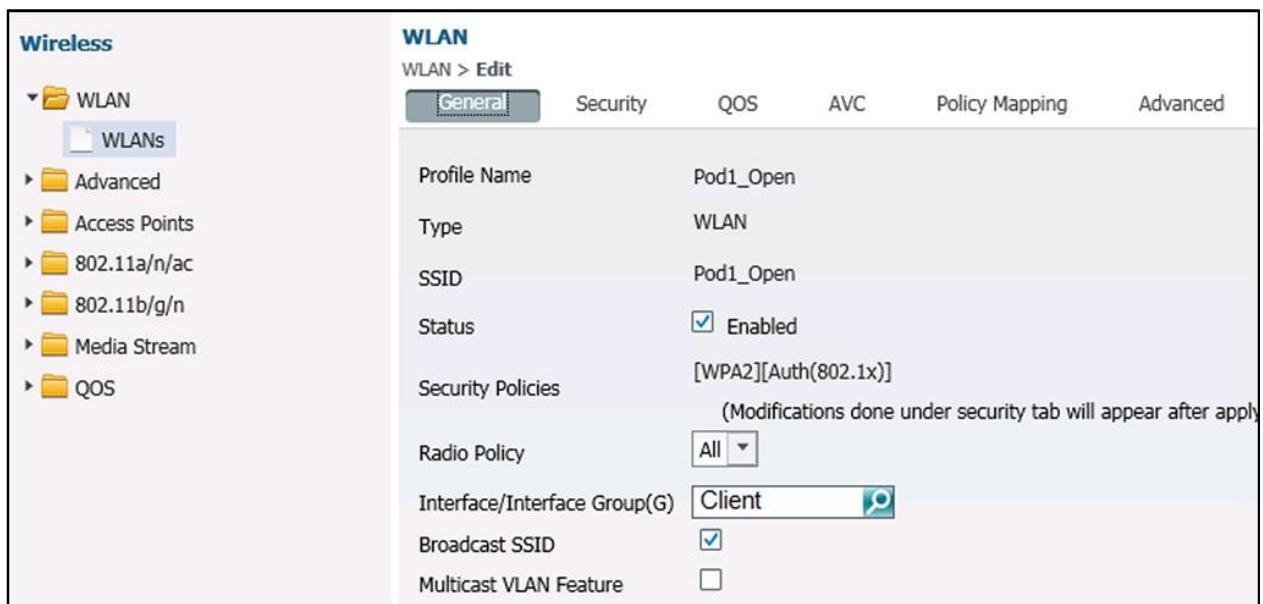
The screenshot shows the Cisco Wireless Controller interface. On the left, there's a navigation tree under 'Wireless' with 'WLAN' expanded, showing 'WLANS' selected. The main panel is titled 'WLANS' and has a sub-titile 'WLANS > Create New'. It contains three input fields: 'WLAN ID' with value '1', 'SSID' with value 'Pod1\_Open', and 'Profile Name' with value 'Pod1\_Open'. A large 'Apply' button is located on the right side of the form.

**Step 5** At the **WLAN > WLANS** screen, notice that the Status is **Disabled** (default behavior)

**Step 6** Click the Profile Open and make the following changes:

On the General tab:

- Check the Status box for **Enabled**
- On the **Interface/Interface Group(G)**, click the **search icon**. When the pop-up appears, choose the **Client** interface from the drop and click **OK**
- Broadcast SSID = **checked** (by default as that would be normal operation)



The screenshot shows the 'WLAN > Edit' screen. The left sidebar shows the 'General' tab is selected. The main area displays the following configuration:

Profile Name	Pod1_Open
Type	WLAN
SSID	Pod1_Open
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1x)] <small>(Modifications done under security tab will appear after apply)</small>
Radio Policy	All
Interface/Interface Group(G)	Client <input type="button" value="🔍"/>
Broadcast SSID	<input checked="" type="checkbox"/>
Multicast VLAN Feature	<input type="checkbox"/>

- Step 7** On the Security tab, change the **Layer 2 Security** dropdown to **None** (no security is required now).
- Step 8** Click **Apply** and **OK** to both pop-ups.
- Step 9** On the top right of the screen, click **Save Configuration** and click **OK** on the pop-ups.

## **Activity Verification**

You have successfully completed this task when you attain this result:

- Created a new profile with an SSID of Podx\_Open WLAN with Open authentication.

# **Task 5: Enable Additional Features**

## **Activity Procedure**

In this task, you will configure the WCM 3650 for additional features like Band Select, CleanAir, and Local Profiling.

Complete these steps:

- Step 1** Connect to the **SW1** from the Admin PC.
- Step 2** Log in to the WCM 3650 (SW1) via browser.
- Step 3** At the top, navigate to **Configuration > Wireless**, then select the **WLAN** folder on the left and then **WLAN**.

### **Band Select and Local Profiling (set per WLAN)**

- Step 4** Click the new WLAN profile (**Podx\_Open**) and enter the following:
- On the **Policy Mapping** Tab (on AireOS, it was on Advanced tab):
- Check the box for **Device Classification** (classification that is based on device type)
  - Check the box for **Local HTTP Profiling** (based on HTTP)

The screenshot shows the 'WLAN' configuration interface. The 'Policy Mapping' tab is selected. Under the 'Policy Mapping' tab, there are four configuration options:

Setting	Value
Device Classification	<input checked="" type="checkbox"/>
Local Subscriber Policy	Disabled <input type="button" value=""/>
Local HTTP Profiling	<input checked="" type="checkbox"/>
Radius HTTP Profiling	<input type="checkbox"/>

- Step 5** On the Advanced tab, check the box for **Band Select** (Under Load balancing and Band Select).

**WLAN**

WLAN > Edit

General	Security	QoS	AVC	Policy Mapping	Advanced
Allow AAA Override	<input type="checkbox"/>				
Coverage Hole Detection	<input checked="" type="checkbox"/>				
Session Timeout (secs)	1800				
Aironet IE	<input type="checkbox"/>				
Diagnostic Channel	<input type="checkbox"/>				
P2P Blocking Action	Disabled				
Media Stream Multicast-direct	<input type="checkbox"/>				
Client Exclusion	<input checked="" type="checkbox"/>				
Timeout Value(secs)	60				
Max Allowed Client	0				
<b>DHCP</b>					
DHCP Server IP Address		0.0.0.0			
DHCP Address Assignment required		<input type="checkbox"/>			
DHCP Option 82		<input type="checkbox"/>			
DHCP Option 82 Format		None			
DHCP Option 82 Ascii Mode		<input type="checkbox"/>			
DHCP Option 82 Rid Mode		<input type="checkbox"/>			
<b>NAC</b>					
NAC State <input type="checkbox"/>					
<b>Load Balancing and Band Select</b>					
Load Balance <input type="checkbox"/>					
Band Select <input checked="" type="checkbox"/>					
<b>Off Channel Scanning Defer</b>					

**Step 6** Click **Apply** and **OK** to both pop-ups.

#### CleanAir (Enabled Globally for Radios)

CleanAir is enabled globally here and then set for each radio by AP.

---

**Note** Use Internet Explorer only for CleanAir Changes.

---

**Step 7** At the top, navigate to **Configuration > Wireless**. Select the **802.11a/n/ac** folder on the left, and then **CleanAir**.

**Step 8** Check the box for **CleanAir** (Under the CleanAir section). Click **Apply** and **OK** to the pop-up.

Adjustments can be made for detecting and alarming on interference devices. Example: You may want to know if “DECT-like Phones” are being used and want an alarm. Add it to the right column for Trap Configuration.

**Step 9** Navigate to **802.11b/g/n** folder on the left, and then **CleanAir**.

**Step 10** Check the box for **CleanAir** (Under the CleanAir section). Click **Apply** and **OK** to the pop-up.

**Step 11** On the top right of the screen, click **Save Configuration** and click **OK** on the pop-ups.

## CleanAir (set per Radio type by AP)

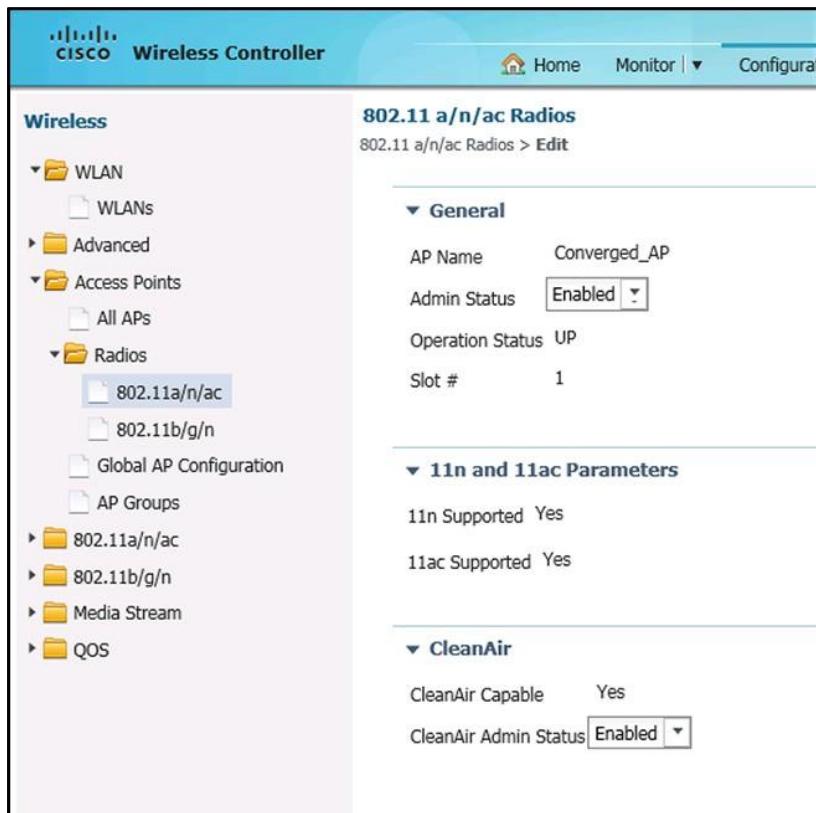
CleanAir can be enabled/disabled per radio type for each AP.

<b>Note</b>	As with AireOS WLCs and APs, CleanAir is automatically enabled for APs that support it.
-------------	---

**Step 12** At the top, navigate to **Configuration > Wireless**. Then select the **Access Points** folder on the left, and then **Radios** folder followed by **802.11a/n/ac**.

**Step 13** Check the box next to the **AP1** and then Click on **Configure** (above the menu).

**Step 14** Under the CleanAir section, verify that the CleanAir dropdown is set for **Enabled**.



**Step 15** Navigate to **Access Points** folder on the left, and then **Radios** folder and then **802.11b/g/n**.

**Step 16** Check the box next to the **AP1** and then Click on **Configure**.

**Step 17** Under the CleanAir section, verify that the CleanAir dropdown is set for **Enabled**.

## Activity Verification

You have successfully completed this task when you attain this result:

- Enabled Band Select on the WLAN (Podx\_Open).
- Enabled Local Profiling on the WLAN (Podx\_Open).
- Enabled CleanAir for each radio per AP.
- Enabled CleanAir globally by radio type.

- Verified settings, by going to **Monitor > Wireless** and look at each radio for the AP (**Clean-Air Admin Status – Enabled** and **Clean-Air Oper Status - Up**).

## Task 6: Associate the Client

### **Activity Procedure**

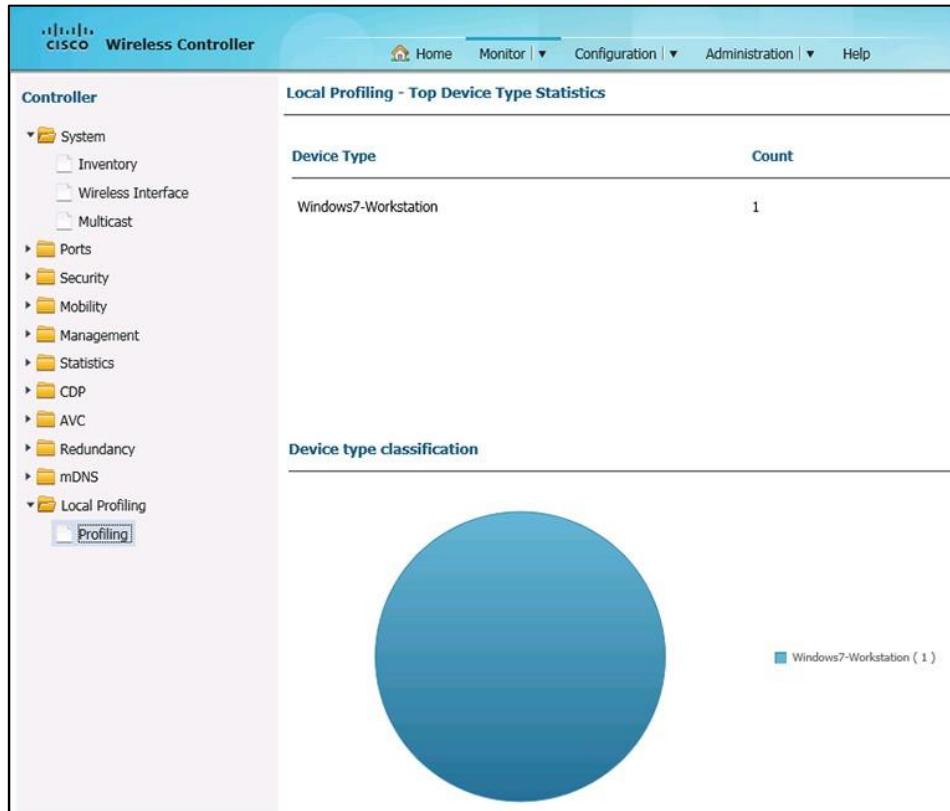
In this task, you will configure the Client PC to connect to the Open WLAN that you created and test operation of the deployment.

Complete these steps:

- Step 1** Connect to the Client PC.
- Step 2** Click the **Wireless** icon in the bottom right tray.
- Step 3** Click **Podx\_Open** and then click **Connect**.
- Step 4** After connection (there may not be internet connectivity now), Click the **Wireless** icon in the tray again.
- Step 5** Right click on the **Podx\_Open** WLAN and choose **Status**.
- Step 6** Observe your **Speed** and **Signal Quality**.
- Step 7** Click the **Details** button icon the **Status** screen.
- Step 8** You should have an IP address in the **192.168.14.0** network.
- Step 9** Connect to the **SW1** from the Admin PC.
- Step 10** Click top menu for **Monitor > Clients**. The information that can be seen here include the Client MAC, IP Address, WLAN ID, State, Protocol, and Device Type.

Client MAC Address	AP Name	WLAN	State	Protocol	Username	Device Type
6cb0.cef6.3256	Converged_AP	1	UP	802.11ac-5ghz	Unknown	Netgear-Device

- Step 11** Click the Client's **MAC address** to see the information for the **General** tab to see additional information like IP address, VLAN ID, WLAN Profile, and AP that the client is connected to.
- Step 12** Click **Clients** on the left side to return to the **Clients** screen.
- Step 13** You should have noticed on the far right under Device Type, that your client type was detected (Microsoft-Workstation). It is available because Local Profiling was turned on for this WLAN.
- Step 14** Navigate to **Monitor > Controller** and select the **Local Profiling** folder on the left, and then **Profiling**.



**Step 15** View the statistics.

---

**Note** As the client used HTTP, the profiling detected the operating system( Windows 7 - Workstation)

---

## Activity Verification

You have successfully completed this task when you attain this result:

- Associated the wireless client with the new WLAN.
- Verified on the client on PC side (IP address, signal, and speed).
- Verified on the SW1 side, the detailed information about the client, including their device type.

# Task 7: Review CleanAir

## Activity Procedure

In this task, you will review the CleanAir reports.

Now that you have enabled CleanAir, you should see what is in your RF space.

Complete these steps:

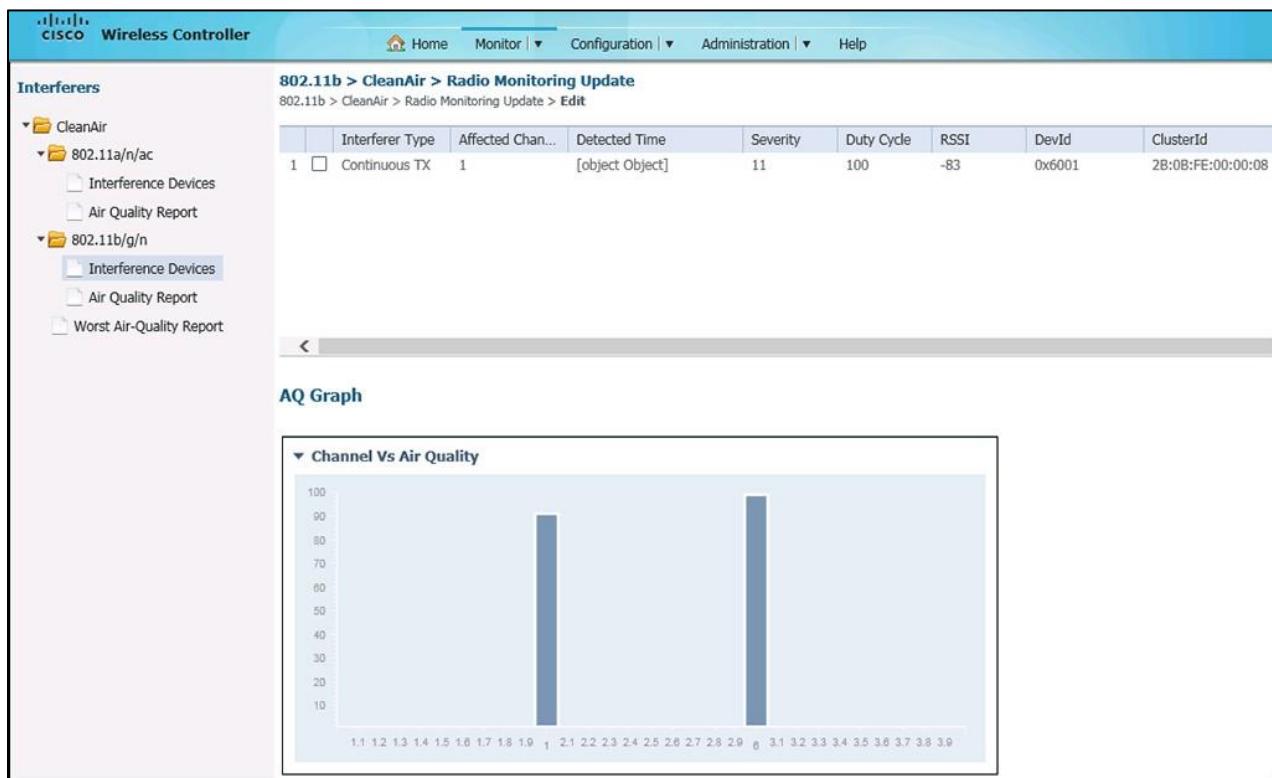
**Step 1** Connect to the SW1 from the Admin PC.

**Step 2** Navigate to **Monitor > Interferers** and select the **802.11b/g/n** folder on the left, then click **Interference Devices**.

---

**Note** Optionally, the instructor may turn on an interfering device to display information in the report.

---



**Step 3** If there are devices that are listed, check the box beside it the **AP Name** and then click **Interference Graph** at the top.

---

**Note** If there is interference, you can see the channel affected and interference power.

---

**Step 4** Under the **802.11b/g/n** folder on the left, click **Air Quality Report**.

The screenshot shows the Cisco Wireless Controller interface. The left sidebar lists 'Interferers' with sections for 'CleanAir', '802.11a/n/ac', and '802.11b/g/n'. Under '802.11b/g/n', there are 'Interference Devices' and 'Air Quality Report'. The right panel is titled 'Air Quality' and contains a table:

AP Name	Channel	Average AQ	Minimum AQ	Interferers	DFS
Converged_AP	1	91	91	1	No
Converged_AP	6	99	99	0	No

**Step 5** View the information for the report. On the left side, click **Worst Air-Quality Report**.

The screenshot shows the Cisco Wireless Controller interface. The left sidebar lists 'Interferers' with sections for 'CleanAir', '802.11a/n/ac', and '802.11b/g/n'. Under '802.11b/g/n', there are 'Interference Devices' and 'Air Quality Report'. The right panel displays two reports:

**802.11a/n Air Quality Report**

AP Name	Converged_AP
Channel Number	36
Minimum Air Quality Index(1 to 100)	100
Average Air Quality Index(1 to 100)	100
Interference Device Count	0

**802.11b/g/n Air Quality Report**

AP Name	Converged_AP
Channel Number	1
Minimum Air Quality Index(1 to 100)	91
Average Air Quality Index(1 to 100)	91
Interference Device Count	1

**Step 6** Here you will see the AP and radio for the Air-Quality.

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- Review the CleanAir interfering devices and CleanAir AQ reports.

# Task 8: Disassociate the Client

## ***Activity Procedure***

In this task, you will configure the Client PC to disconnect from the WLAN.

Complete these steps:

- Step 1** Connect to the Client PC.
- Step 2** Click the **Wireless** icon in the bottom right tray.
- Step 3** Right click on **Podx\_Open** and choose **Disconnect**.
- Step 4** Click the **Wireless** icon in the bottom right tray.
- Step 5** At the bottom, click **Open Network and Sharing Center**.
- Step 6** On the left side, click **Manage Wireless Networks**.
- Step 7** Delete any network profiles and close all open dialog windows.

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- Disconnected the wireless client from the WLAN.
- Removed the wireless client connection from the SW1.

# **Hardware Lab 8: Configuring Security on a Converged WLAN Deployment**

---

## **Overview**

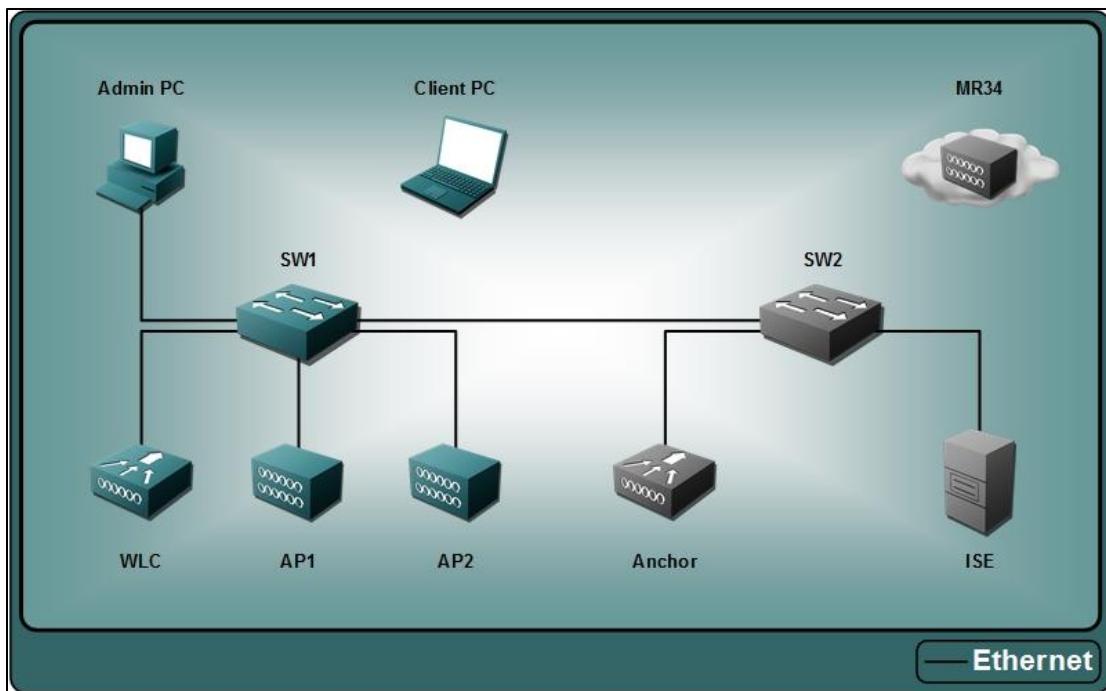
In this activity, you configure the converged access Switch provide security on the WLAN converged WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Implement and test WPA2-PSK security.
- Implement test Local-EAP security.
- Implement and test RADIUS security.
- Implement and test WebAuth security.

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 3650 IOS-XE Switch (WCM)
- AP 3700i (Converged AP)
- Cisco ISE

### VLANs and IP Ranges

### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
Pod 3650 Switch	192.168.11.254	admin	Cisco123	cisco
ISE (RADIUS)	192.168.11.21	admin	1234QWer	

## Task 1: Implement WPA2 PSK Authentication

### Activity Procedure

In this task, you will implement WPA2 PSK authentication on the SW1 and test with a wireless client. You have tested with Open Authentication, now you add some security.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

- Step 1** Connect to the Admin PC.
- Step 2** Open a browser and connect to SW1.

#### Create a new WLAN for WPA2-PSK

- Step 3** Navigate to **Configuration>Wireless > WLAN > WLANs**.

---

**Note** To help keep the number of broadcasting SSID to a minimum, you will disable the WLANs that you are not using.

---

- Step 4** Click on the Profile name of **Podx\_Open**:

- The Status should be changed to disabled (Enable is unchecked).

- Click **Apply** and **OK** to any pop-ups.

---

<b>Note</b>	In IOS-XE you cannot change the Profile Name and SSID for existing WLANs. Because of this, you will be creating multiple WLANs for testing.
-------------	---

---

**Step 5** Go back to **WLANs** and click **New** at the top and enter the following information (x=pod#):

- WLAN ID: **2**
- SSID: **Podx\_PSK**
- Profile: **Podx\_PSK**
- Click **Apply** and **OK** to pop-up.

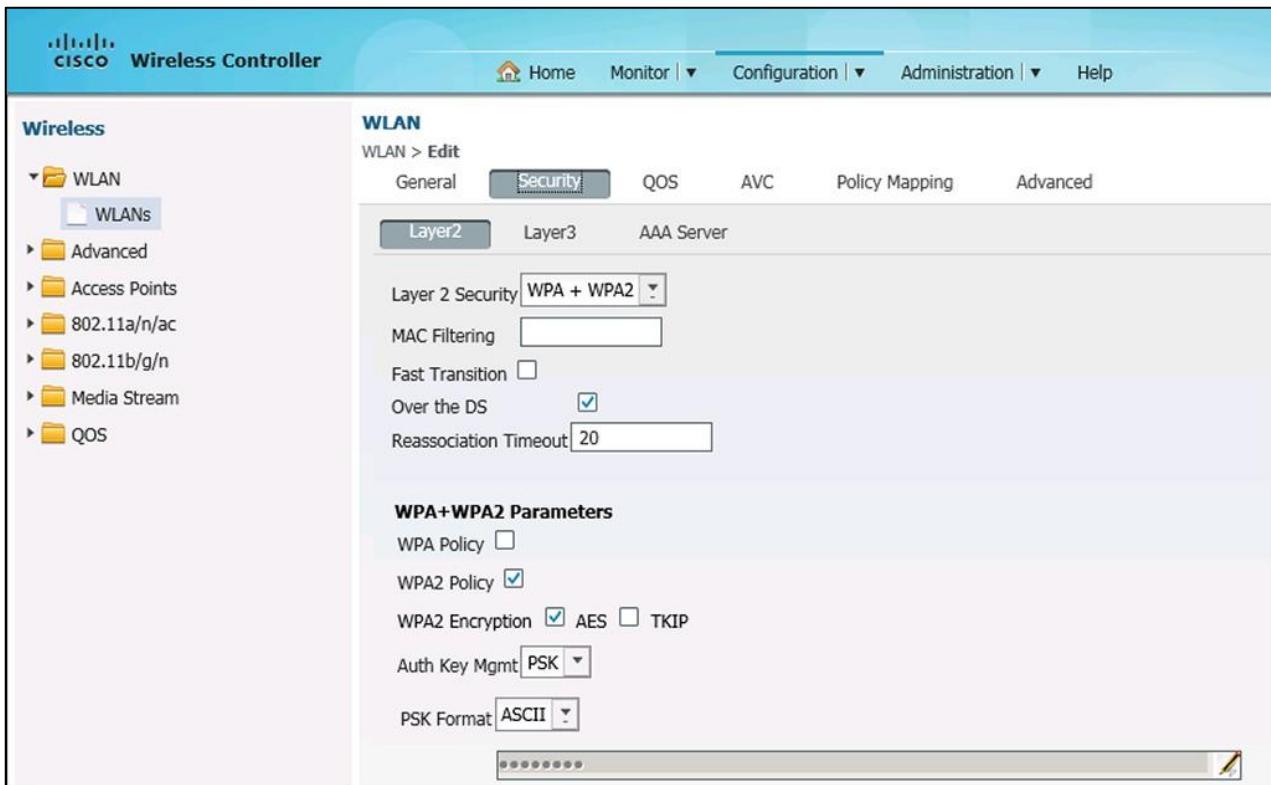
**Step 6** Click on the **Podx\_PSK** profile and make the following changes:

On the General tab:

- Check the Status box for **Enabled** (was disabled after creation))
- On the **Interface/Interface Group(G)** click on the **search icon**. When the pop-up appears, choose the **Client** interface from the drop and click **OK**.
- Broadcast SSID: **checked** (by default)

**Step 7** Go to the Security tab. You will use WPA2 with AES, as you want the best level of security available for PSK. Under Layer 2, select the following:

- Under Layer 2 Security: **WPA + WPA2**
- Under WPA + WPA2 Parameters, select only: **WPA2 Policy-AES** (checked – all others unchecked)
- Under Auth Key Mgmt dropdown: **PSK**
- For the PSK Format, use ASCII and click on the pencil icon and on the pop-up, enter a key in of: **Cisco123** and click **OK**.



**Step 8** Click **Apply** and **OK** to any pop-ups.

**Step 9** Click **WLANS** and verify that the WLAN shows **[WPA2][Auth(PSK)]**.

WLANS						
Mobility Anchor	New	Remove	Show All			
			Profile	ID	SSID	VLAN
<input type="checkbox"/> Open	1	Pod1_Open	14	Disabled	None	
<input type="checkbox"/> Pod1_PSK	2	Pod1_PSK	1	Disabled	[WPA2][Auth(802.1x)]	

**Step 10** On the top right of the screen, click **Save Configuration** and click **OK** on the pop-ups.

#### Verify Client Access

**Step 11** Connect to the Client PC.

**Step 12** On the desktop, right-click on **Network** and choose **Properties** to go to the **Network and Sharing Center**.

**Step 13** Click **Manage Wireless Networks** and right-click and delete all profiles that may exist.

**Step 14** Click the WLAN tray.

**Step 15** Click on the **Podx\_PSK** network, and then click **Connect**. (Uncheck the box for “Connect automatically”, you don’t want to create a profile that the client will automatically reconnect to).

**Step 16** You will be prompted for the Network Security Key, type **Cisco123** and click **OK**.

---

<b>Note</b>	If you are prompted for the key again, try again. If this still fails, check the key.
-------------	---

---

**Step 17** Click the WLAN tray.

**Step 18** Right click the **Podx\_PSK** network and select **Status**.

**Step 19** On the **General** tab of the Status window, click the **Details** button.

**Step 20** You will now see your IP address (network 192.168.14.0).

**Step 21** Open a Command Prompt and ping your gateway (192.168.14.254).

**Step 22** Verify your client connection on the SW1 **Monitor > Clients** menu.

**Step 23** Close all dialogue windows.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Created a WLAN with PSK authentication.
- Connected your wireless client to the PSK WLAN.
- Client has an IP address in the proper range and could ping the gateway.

## **Task 2: Implement Local EAP Authentication**

### **Activity Procedure**

In this task, you will implement Local EAP authentication on the SW1 and test with a wireless client. Now you will move to using a higher level of security.

---

<b>Note</b>	The lower case “x” in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

Complete these steps:

**Step 1** Open a browser and connect to the SW1 from the Admin PC.

#### **Create a Local EAP User Account on the WCM 3650**

Similar to the AireOS, we need to create a local account for the EAP user as you will be using PEAP.

**Step 2** Navigate to **Configuration > Security > AAA > RADIUS > Users** and click **New** and make the following selections:

- User Name: **switchuser**
- Privilege: **15**
- Password: **Cisco123**
- Confirm Password: **Cisco123**

- Type: **network-user** (as opposed to a Lobby-Admin or Management user)
- Description: **Local\_EAP\_User**
- Click **Apply** and **OK** to the pop-up

The screenshot shows the Cisco Wireless Controller's web-based management interface. The top navigation bar includes links for Home, Monitor, Configuration, and Admin. The main content area is titled "AAA Users" and shows the path "AAA Users > New". On the left, a sidebar under "Security" has "AAA" expanded, with "Users" selected. The main form fields are as follows:

User Name	switchuser
Privilege	15
Password	*****
Confirm Password	*****
Type	network-user
Description	[Empty]
Guest User	<input type="checkbox"/>

#### Create a Local EAP Profile to specify EAP type(s)

Here you will create an EAP profile and specify PEAP as the EAP type.

**Step 3** Navigate to **Configuration > Security > Local EAP > Local EAP Profiles** and click **New**. Then make the following selections:

- Profile Name: **Switch\_Local\_EAP**
- Check the EAP type(s) to be used: **PEAP**
- Click **Apply** and **OK** to the pop-up.

The screenshot shows the Cisco Wireless Controller web interface. The top navigation bar includes links for Home, Monitor, and Configuration. On the left, a sidebar titled 'Security' lists several categories: AAA, Local EAP (which is expanded to show Local EAP Profiles, EAP-FAST Parameters, and Trustpoint), Wireless Protection Policies, CIDS, FQDN, and others. The main content area is titled 'Local EAP Profiles' and shows a sub-page for 'New'. It has a form with a 'Profile Name' field containing 'Switch\_Local\_EAP'. Below this are checkboxes for various EAP methods: LEAP, EAP-FAST, EAP-TLS, PEAP (which is checked), and Trustpoint.

### Configure Method Lists – Authentication

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user.

---

**Note** You will first create the “default” list that will automatically be applied to all interfaces and then a regular list for specific authentication.

---

**Step 4** Navigate to **Configuration > Security > AAA > Method Lists > Authentication** and click **New**. Then make the following selections:

- Method List Name: **default**
- Type: **dot1x** (using 802.1x)
- Group Type: **local** (local not remote)
- Click **Apply** and **OK** to the pop-up.

The screenshot shows the Cisco Wireless Controller's web-based management interface. In the top navigation bar, the 'Home', 'Monitor', 'Configuration', 'Administration', and 'Help' links are visible. On the left, a sidebar under the 'Security' heading shows the 'AAA' configuration with 'Method Lists' expanded. Under 'Method Lists', there are options for 'General', 'Authentication' (which is highlighted in blue), 'Accounting', 'Authorization', 'Server Groups', 'RADIUS', 'TACACS+ Servers', and 'LDAP Servers'. The main content area is titled 'Authentication' and shows the 'Authentication > New' configuration page. It includes fields for 'Method List Name' (set to 'default'), 'Type' (set to 'dot1x'), 'Group Type' (set to 'local'), and a note stating '\* Method List Name can be 'default' or any User defined Name.' Below these are two lists: 'Available Server Groups' and 'Assigned Server Groups', each with a double-headed arrow button between them.

**Note** Now the default Method List will automatically be applied to all interfaces.

**Step 5** Click **Authentication** and then **New** again. Make the following selections:

- Method List Name: **authen\_list**
- Type: **dot1x**
- Group Type: **local**
- Click **Apply** and **OK** to the pop-up.

**Note** Now you have added a specific (authen\_list) authentication method that determines that you are using 802.1x and the authentication is local. It will be added as the authentication list for the General Method List.

### Configure Method Lists – Authorization

You must also create an Authorization Method List to specify the Type and Group Type.

**Step 6** Under the **Method Lists** subfolder choose **Authorization** and click **New**. Then make the following selections:

- Method List Name: **author\_list**
- Type: **credential-download** (downloads credentials from local server)
- Group Type: **local** (local not remote)
- Click **Apply** and **OK** to the pop-up.

**Note** If this step fails, please try to use IE.

**CISCO Wireless Controller**

Home Monitor | ▾ Configuration | ▾ Administration | ▾ Help

**Security**

AAA  
Method Lists  
General  
Authentication  
Accounting  
Authorization  
Server Groups  
RADIUS  
TACACS+ Servers  
LDAP Servers

**Authorization**  
Authorization > New

Method List Name: author\_list  
Type: credential-download  
Group Type: local

Available Server Groups  
Assigned Server Groups

Groups In This Method

\* Method List Name can be 'default' or any User defined Name.

The screenshot shows the Cisco Wireless Controller's web interface. On the left, there's a navigation tree under 'Security' for AAA, Method Lists, RADIUS, and TACACS+. The 'Authorization' section is selected. The main pane shows a form for creating a new method list named 'author\_list'. It includes fields for 'Type' (set to 'credential-download') and 'Group Type' (set to 'local'). Below these are two lists: 'Available Server Groups' and 'Assigned Server Groups', separated by a double-headed arrow indicating they can be moved between them. A note at the bottom states that the method list name can be 'default' or any user-defined name.

**Note** You have now configured a specific (author\_list) authorization method that determines that your EAP credentials will be downloaded locally.

### Configure Method Lists – General

Here you will use the method lists that you just created for authentication and authorization.

**Step 7** Under the **Method Lists** subfolder choose **General** and make the following selections:

- Dot1x System Auth Control: **Checked** (to enable)
- Local Authentication: **Method List**
- Authentication Method List: **authen\_list** (authentication method list)
- Local Authorization: **Method List**
- Authorization Method List: **author\_list** (authorization method list)
- Click **Apply** and **OK** to the pop-up.

The screenshot shows the Cisco Wireless Controller configuration interface. The left sidebar is titled "Security" and contains the following navigation tree:

- AAA
  - Method Lists
    - General
    - Authentication
    - Accounting
    - Authorization
  - Server Groups
  - RADIUS
    - TACACS+ Servers
    - LDAP Servers
  - Users

The main panel is titled "General" and contains the following configuration options:

Dot1x System Auth Control	<input checked="" type="checkbox"/>
Local Authentication	Method List <input type="button" value="▼"/>
Authentication Method List	authen_list <input type="button" value="▼"/>
Local Authorization	Method List <input type="button" value="▼"/>
Authorization Method List	author_list <input type="button" value="▼"/>
<b>Radius-server load-balance method</b>	
Least Outstanding	<input type="checkbox"/>

**Note** Now you have a General Method List that determines the Authentication and Authorization to be used.

### Disable Podx\_PSK WLAN

To focus on our new WLAN, you will disable the Podx\_PSK WLAN.

**Step 8** Navigate to **Configuration > Wireless > WLAN > WLANS** and select the **Podx\_PSK** profile.

**Step 9** Change the Status to **disabled** (Enable is unchecked).

**Step 10** Click **Apply** and **OK** to any pop-ups.

### Create a new WLAN for EAP

Create a WLAN using WPA2 with 802.1X and use Local EAP.

**Step 11** Go back to **WLANS** and click **New** at the top and enter the following information (x=pod#):

- WLAN ID: 3
- SSID: **Podx\_EAP**
- Profile: **Podx\_EAP**
- Click **Apply** and **OK** to the pop-up.

**Step 12** Click on the **Podx\_EAP** profile and make the following changes on the General tab:

- Check the Status box for **Enabled**
- On the **Interface/Interface Group(G)** click on the **search icon**. When the pop-up appears, choose the **Client** interface from the drop and click **OK**.

- Broadcast SSID: **checked** (by default)

**Step 13** On the **Security** tab, make the following selections:

Layer 2 tab:

- Under Layer 2 Security, select: **WPA + WPA2**
- Under WPA + WPA2 Parameters, select only: **WPA2 Policy-AES** (checked – all others unchecked))
- Under Auth Key Mgmt, select **802.1x**

AAA Server tab:

- Leave the Authentication/Authorization Methods to **Disabled**, to disable RADIUS accounting and authentication for this WLAN
- Local EAP Authentication: **Checked**
- Type in the EAP Profile Name exactly as it was entered earlier: **Switch\_Local\_EAP**

**Step 14** Click **Apply** and **OK** to any pop-up.

**Step 15** Click **WLANS** and verify that the WLAN shows **[WPA2][Auth(802.1X)]**.

The screenshot shows the Cisco Wireless Controller interface with the 'WLANS' configuration page selected. The table lists three WLAN profiles: 'Open', 'Pod1\_PSK', and 'Pod1\_EAP'. The 'Pod1\_EAP' profile is highlighted. The table columns include Profile, ID, SSID, VLAN, Status, and Security Policies. The 'Pod1\_EAP' row shows 'Enabled' status and '[WPA2][Auth(802.1X)]' in the Security Policies column.

Profile	ID	SSID	VLAN	Status	Security Policies
Open	1	Pod1_Open	14	Disabled	None
Pod1_PSK	2	Pod1_PSK	14	Enabled	[WPA2][Auth(PSK)]
Pod1_EAP	3	Pod1_EAP	14	Enabled	[WPA2][Auth(802.1X)]

---

**Note** Note the Method List was not entered in the WLAN profile, as our General Method list will be used by default (for authentication and authorization).

---

**Step 16** On the top right of the screen, click **Save Configuration** and click **OK** on the pop-ups.

#### Verify Client Access

We need to create a specific 802.1x profile that uses Local EAP (PEAP) and will prompt for the username/password to be authenticated.

**Step 17** Connect to the Client PC.

---

**Note** You cannot connect to this WLAN without creating a profile that takes into account our specific parameters. EAP parameters will vary based on type and security needs. Our need is to use PEAP without requiring certificates and prompt for a user name and password.

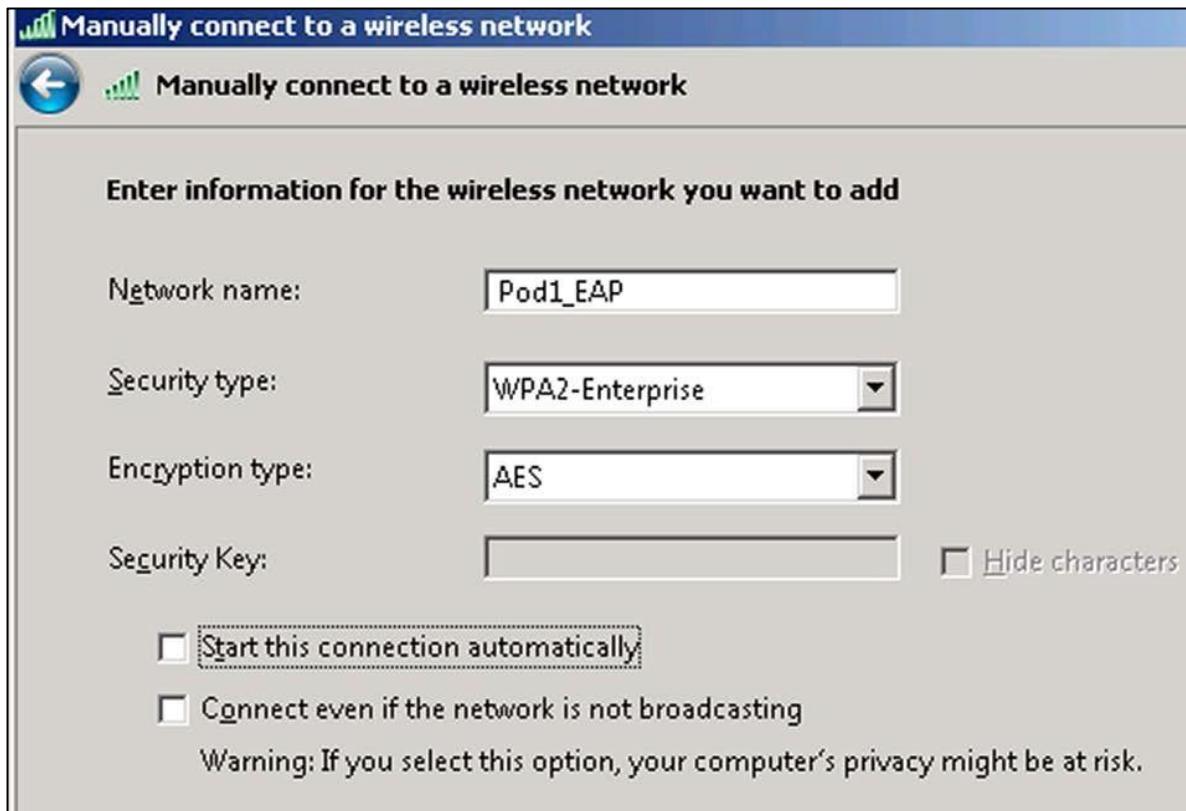
---

**Step 18** On the desktop, right-click on **Network** and choose **Properties** to go to the **Network and Sharing Center**.

**Step 19** Select **Manage Wireless Networks** and click **Add**. Then make the following selections:

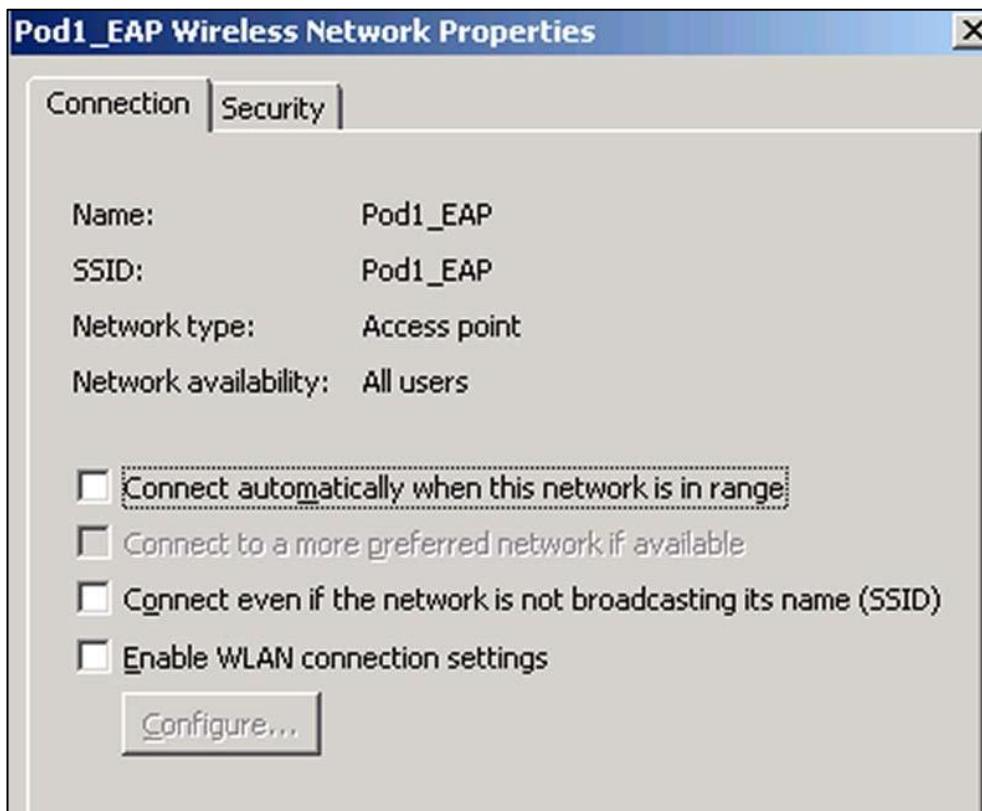
- Select: **Manually create a network profile**

- Network Name: **Podx\_EAP**
- Security type dropdown: **WPA2-Enterprise**
- Encryption type dropdown: **AES**
- Start this connection automatically: **Uncheck** (manual connection to WLAN)



**Step 20** Click **Next**, then **Change connection settings**.

**Step 21** On the Podx\_EAP Wireless Network Properties, verify that **Connect automatically when this network is in range** is unchecked.

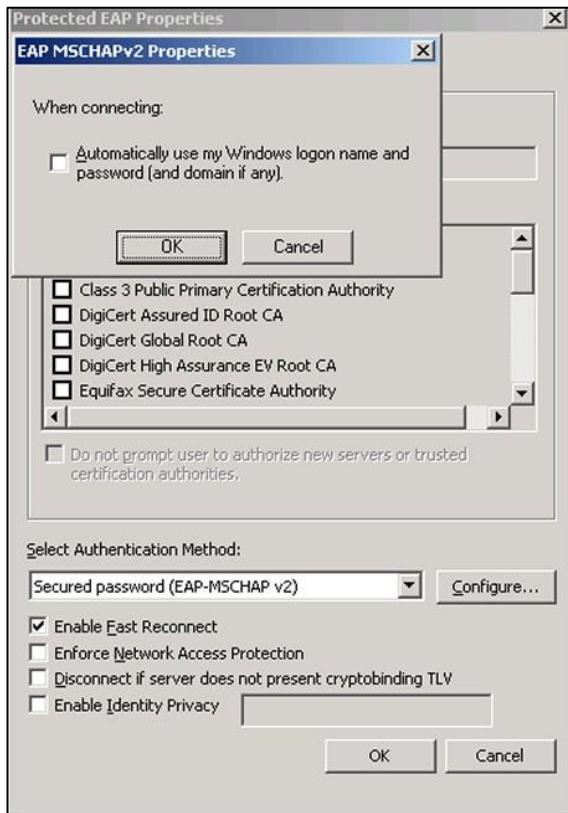


- Step 22** Click on the Security tab and verify that the Network Authentication Method is **Microsoft Protected EAP (PEAP)**. Uncheck **Remember my credentials...** (You want to enter our credentials each time that you connect).



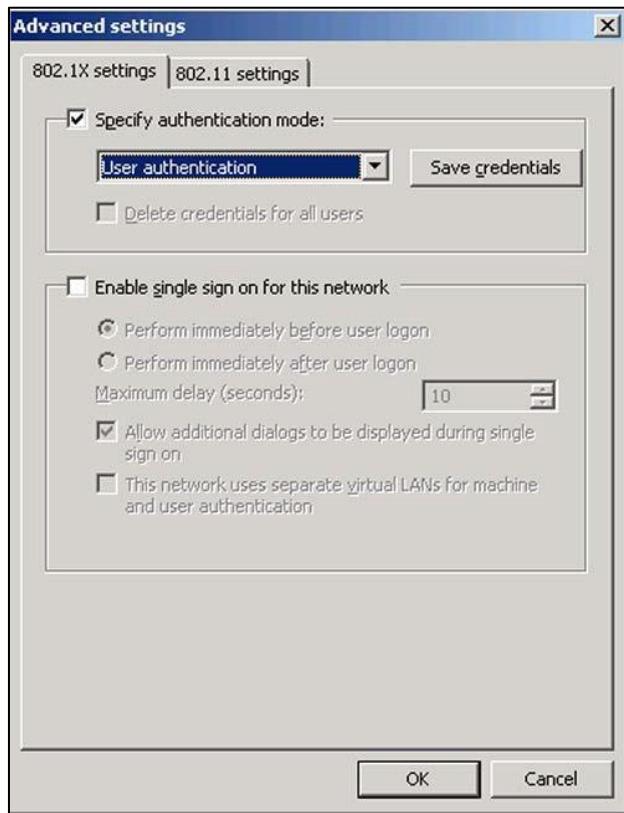
**Step 23** Click **Settings** to the right of Microsoft: Protected EAP (PEAP) and make the following selections:

- Under **When connecting**: uncheck the Validate server certificate (we only have a self-signed certificate on our WCM).
- Verify under the **Select Authentication Method** that the dropdown is set to: **Secured password (EAP-MSCHAP v2)**
- Select Configure on the right and uncheck **Automatically use my Windows logon name...** checkbox (you want to use the user that you created on the WCM).
- Click **OK** and then **OK** to return to the **Security** tab.



**Step 24** On the **Security** tab, click the **Advanced Settings** button and make the following selections:

- On the 802.1X settings, Check the **Specify authentication mode** checkbox (you don't want default authentication – you want to use the User Authentication).
- Change the dropdown to **User authentication** (username/password).
- Observe the **802.11 settings** tab, but do not make any changes.
- Click **OK** and **OK**.



**Step 25** Click **Close** on Profile Wizard.

**Step 26** Observe the new profile (**Podx\_EAP**)

**Step 27** Click the WLAN tray.

**Step 28** Click on the **Podx\_EAP** network, and then click **Connect**.

**Step 29** A Network Authentication screen will pop-up, enter your username of **switchuser** and password of **Cisco123** and click **OK**

---

**Note** If authentication fails, verify that you entered the correct username/password and verify the same username/password on the Switch. Also recheck EAP profile and WLAN settings.

---

**Step 30** Click the WLAN tray.

**Step 31** Right click the **Podx\_EAP** network and select **Status**.

**Step 32** On the **General** tab of the Status window, click the **Details** button

**Step 33** You will now see your IP address (network 192.168.14.0).

**Step 34** Open a Command Prompt and ping your gateway (192.168.14.254).

**Step 35** Verify your client connection on the SW1 Monitor menu.

Client MAC Address	AP Name	WLAN	State	Protocol	Username	Device Type
6cb0.ce47.866b	Converged_AP	3	UP	802.11ac-5ghz	switchuser	Unknown

**Step 36** On the Client PC, disconnect from the Podx\_EAP WLAN.

**Step 37** On the SW1, remove the client (from Monitor>Clients).

**Step 38** Close all dialogue windows.

## Activity Verification

You have successfully completed this task when you attain this result:

- Created a WLAN with Local EAP authentication.
- Connected your wireless client to the EAP WLAN
- Client got an IP address in the proper range and could ping the gateway.

## Task 3: Implement RADIUS Authentication

### Activity Procedure

In this task, you will implement RADIUS authentication on the SW1 with ISE and test with a wireless client. Now you can centralize the user credentials and not have to create them on individual WCMs or WLCs.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

**Step 1** Open a browser and connect to the SW1 from the Admin PC.

#### Add Remote User Account to ISE

You could use the existing user from earlier, but to avoid confusion, create a new user for RADIUS authentication.

**Step 2** Still on the Admin PC, open the Firefox browser to connect to the Cisco ISE.

**Step 3** Enter **192.168.11.21** for the address of the ISE.

**Step 4** On the Untrusted Connection warning, click on **I Understand the Risks**, then select **Confirm Security Exception**.

---

<b>Note</b>	This warning is issued because the ISE uses a self-signed certificate.
-------------	--

---

**Step 5** AT the ISE login screen, enter the username of **admin** and password of **1234QWer** and click **Login**.

**Step 6** Click **OK** on any warnings about the license expiration.

**Step 7** The next step is to create a remote user account. Select to **Administration > Identity Management > Identities > Users**. Then click **+Add** and enter the following:

- Name: **iseuser**
- Email: *leave empty*
- Password: **Cisco123**
- Click **Submit**.

The screenshot shows the ISE interface with the following details:

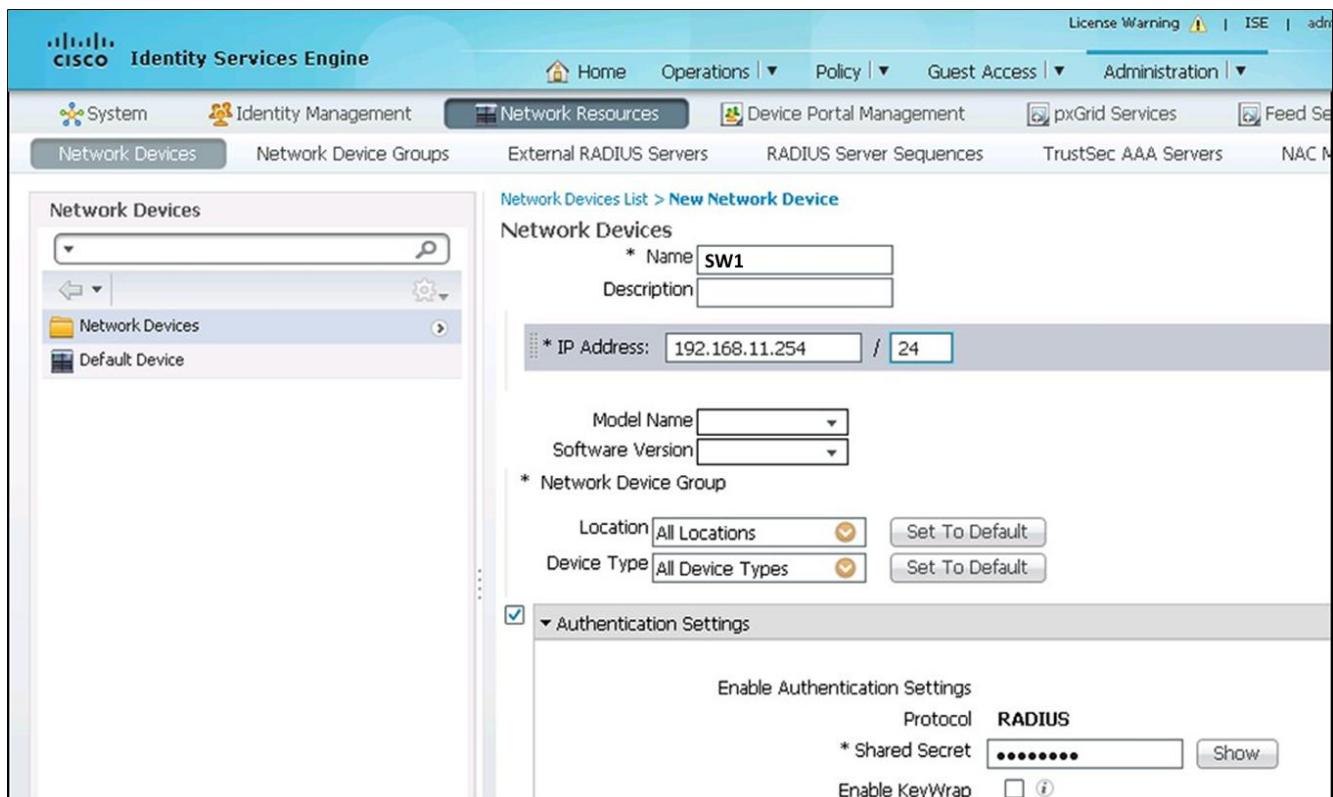
- Identity Management** tab selected.
- Identities** sub-tab selected in the navigation bar.
- Network Access Users List > New Network Access User** page.
- Name:** iseuser
- Status:** Enabled
- Email:** (empty)
- Password:** Cisco123 (entered twice)
- User Information:** First Name: ise, Last Name: user

### Add Connection in ISE for Converged Switch

The ISE needs to be aware that the WCM 3650 will be a NAD and will be sending authentication requests.

**Step 8** Select to **Administration > Network Resources > Network Devices**. Then click **+Add** and enter the following:

- Name for the WCM: **SW1**
- IP address of the SW1 and mask: **192.168.11.254 / 32**
- Check the box for **Authentication Settings** and window opens for the settings.
- Enter a password for the Shared Secret entry: **Cisco123** (you will use this on the WCM too)
- Click **Submit**.



### Add Connection in Converged Switch for ISE

The WCM 3650 needs to know where the ISE server's information (IP and Shared Secret).

**Step 9** Open a browser and connect to the SW1 from the Admin PC.

**Step 10** Navigate to Configuration > Security > AAA > RADIUS > Servers and click New. Then enter the following information:

- Server name: **ISE**
- Server IP Address: **192.168.11.21** (ISE PSN address)
- Shared Secret: **Cisco123**
- Confirm Shared Secret: **Cisco123** (same as was done on ISE)
- Change auth/acct ports from default to: **1812/1813**
- Server Timeout: **10**
- Retry Count: **2**
- Click **Apply** and **OK** to pop-up.

The screenshot shows the Cisco Wireless Controller interface under the Configuration > Security > AAA > RADIUS > Servers section. The left sidebar lists AAA, Method Lists (General, Authentication, Accounting, Authorization), Server Groups, RADIUS (Servers, Fallback), and TACACS+ Servers. The main panel is titled 'Radius Servers' and shows the configuration for a server named 'ISE'. The fields are as follows:

Server Name	ISE
Server IP Address	192.168.11.21
Shared Secret	*****
Confirm Shared Secret	*****
Auth Port (0-65535)	1812
Acct Port (0-65535)	1813
Server Timeout (0-1000) secs	10
Retry Count (0-100)	2
Support for RFC 3576	Enable

### Create RADIUS Server Group and add ISE

The RADIUS server (ISE) needs to be put into a group. This group will be used by the Method List. The WLAN will then use the Method List (which has our Server Group).

**Step 11** Navigate to Configuration > Security > AAA > Server Groups > Radius and click New.

There enter the following information:

- Name: **ISE\_GROUP**
- Move **ISE** to **Assigned Servers**
- Click **Apply** and **OK** to pop-up.

The screenshot shows the Cisco Wireless Controller interface under the Configuration > Security > AAA > Server Groups > Radius section. The left sidebar lists AAA, Method Lists, Server Groups (Radius, Tacacs+, Ldap), and RADIUS (Servers, Fallback, TACACS+ Servers, LDAP Servers, Users, Attribute List). The main panel is titled 'Radius Server Groups' and shows the configuration for a group named 'ISE\_GROUP'. The fields are as follows:

Group Name	ISE_GROUP
MAC-delimiter	none
MAC-filtering	none
Dead-time (0-1440) in minutes	
Group Type	Radius

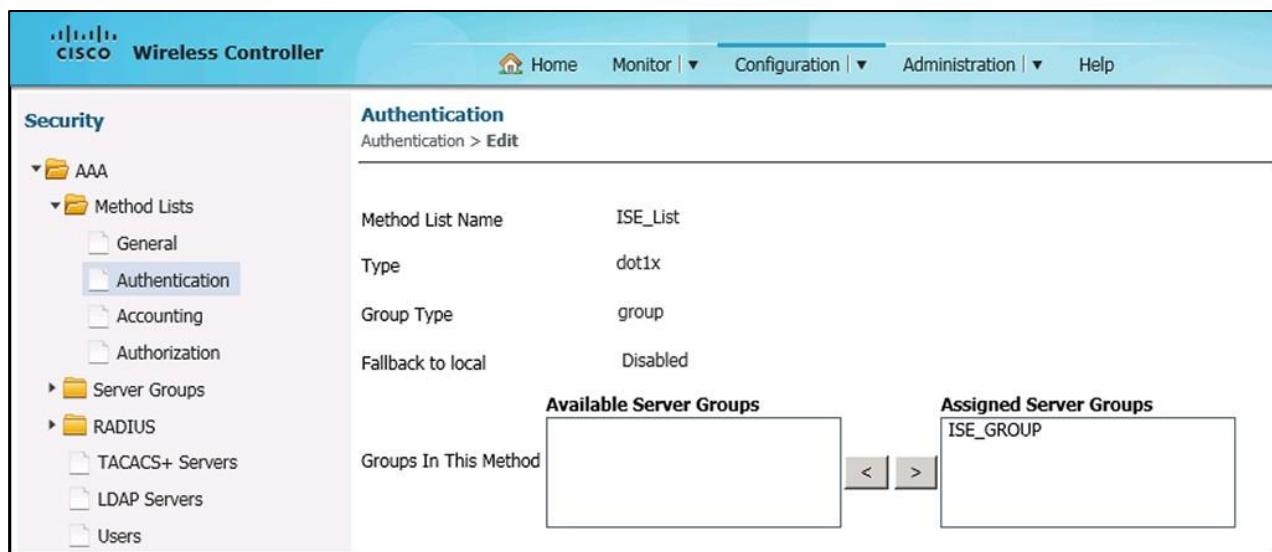
Below these settings, there are two panels: 'Available Servers' and 'Assigned Servers'. The 'Available Servers' panel contains a list of servers, and the 'Assigned Servers' panel contains a list with 'ISE'. Between the two panels are '<' and '>' buttons for moving servers between them.

## Configure Method Lists – Authentication

The Method List will be different, as it needs to use the ISE\_Group.

**Step 12** Navigate to **Configuration > Security > AAA > Method Lists > Authentication** and click **New**. There enter the following information:

- Name: **ISE\_List**
- Type: **dot1x**
- Group Type: **group**
- Move **ISE\_GROUP** to **Assigned Server Groups**
- Click **Apply** and **OK** to pop-up.



## Configure Method Lists – General

Change the General method List for Local Authentication/Authorization to be “None”. It will no longer be local.

**Step 13** Under the **Method Lists** subfolder choose **General** and select the following:

- Dot1x System Auth Control: **Checked** (to enable)
- Local Authentication: **None**
- Local Authorization: **None**
- Click **Apply** and **OK** to the pop-up.

The screenshot shows the Cisco Wireless Controller configuration interface. On the left, under the 'Security' section, there is a tree view: 'AAA' is expanded, showing 'Method Lists'. 'Method Lists' is also expanded, showing 'General', 'Authentication', 'Accounting', and 'Authorization'. Under 'General', there are several configuration options:

Setting	Value
Dot1x System Auth Control	<input checked="" type="checkbox"/>
Local Authentication	<input type="button" value="None"/>
Local Authorization	<input type="button" value="None"/>
<b>Radius-server load-balance method</b>	
Least Outstanding	<input type="checkbox"/>

#### Configure RADIUS Source Interface VLAN

Here you are specifying that the RADIUS communication will use VLAN11 as the source for communication. The default IP is the switch's outbound interface and that might not match ISE configuration (of the NAD) and reject authentication. Therefore you need to statically define the source IP address from 3650.

**Step 14** Connect to the **SW1** console port.

**Step 15** Type: **enable** and press **Enter**.

**Step 16** Type: **in password of cisco** and press **Enter**.

**Step 17** Type: **config term** and press **Enter** to enter global configuration mode.

**Step 18** Enter the following to change the RADIUS Source Interface VLAN:

```
SW1(config)# ip radius source-interface vlan 11  
SW1(config)# exit
```

**Step 19** Type **copy run start** and **Enter** twice.

**Step 20** Disconnect from switch.

#### Modify the EAP WLAN

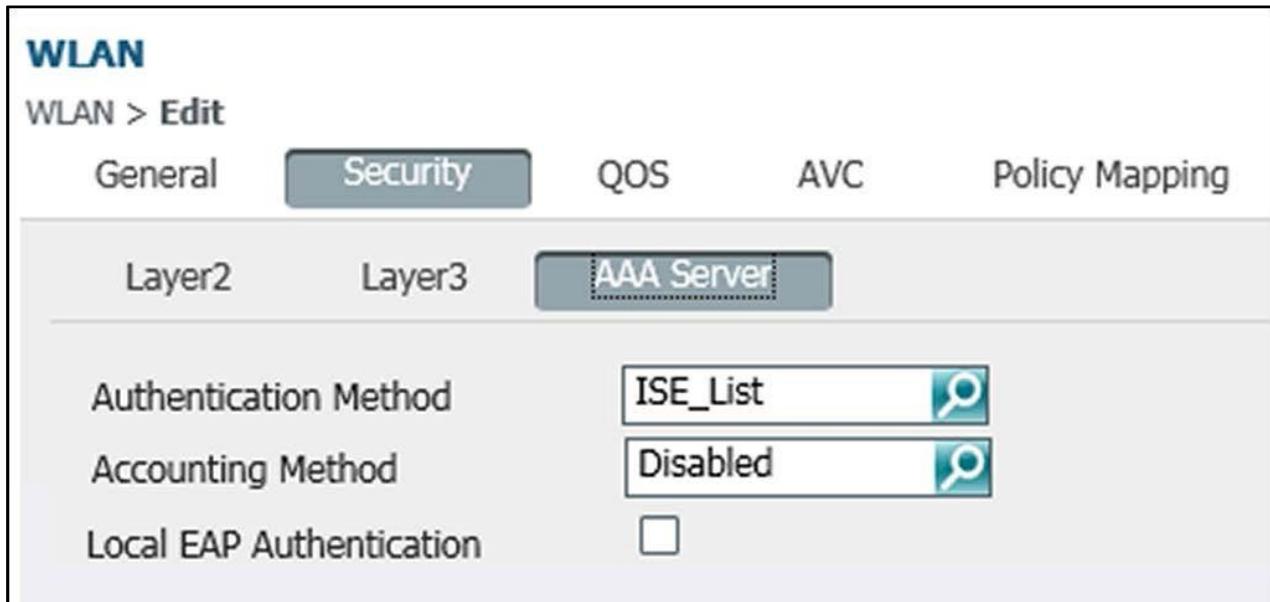
You can use the existing WLAN, as you are just changing the EAP from local to remote to use our ISE\_list. The ISE\_List will use the ISE\_GROUP, which will use our ISE server (192.168.11.21).

**Step 21** Navigate to **Configuration > Wireless** and then choose **WLAN > WLANs**.

**Step 22** Click on **Poxid\_EAP** and select the Security tab. Then enter the following:

- Leave **Layer 2** as set
- On the **AAA Server** tab:

- Local EAP Authentication: **Unchecked**
- Authentication Method: **ISE\_List**
- Leave the **General** tab settings as set
- Click **Apply** and **OK** to pop-ups.




---

**Note** When using RADIUS you are not changing the authentication type, but where the authentication server is at (now remote vs. local).

---

**Step 23** Click **WLANS** and verify that the WLAN shows **[WPA2][Auth(802.1X)]**

**Step 24** On the top right of the screen, click **Save Configuration** and click **OK** on the pop-ups.

#### Verify Client Access

**Step 25** Connect to the Client PC.

**Step 26** You will use the existing EAP profile (the client doesn't care where the credentials are being authenticated at, just how).

---

**Note** Again, the authentication type does not change, but the server that does the authentication is now ISE.

---

**Step 27** Click the WLAN tray.

**Step 28** Click on the **Podx\_EAP** network, and then click **Disconnect** (if connected).

**Step 29** Click on the **Podx\_EAP** network, and then click **Connect**.

**Step 30** A Network Authentication screen will pop-up, enter your username of **iseuser** and password of **Cisco123** and click **OK**.

---

<b>Note</b>	If authentication fails, verify that you entered the correct username/password and verify the same username/password on the ISE. Also recheck EAP profile and WLAN settings.
-------------	--

---

- Step 31** Click the WLAN tray.
- Step 32** Right click the **Podx\_EAP** network and select **Status**.
- Step 33** On the **General** tab of the Status window, click the **Details** button.
- Step 34** You will now see your IP address (network 192.168.14.0).
- Step 35** Open a Command Prompt and ping your gateway (192.168.14.254).
- Step 36** Verify your client connection on the SW1 Monitor menu.
- Step 37** On the Client PC desktop, right-click on **Network** and choose **Properties** to go to the **Network and Sharing Center**.
- Step 38** Click **Manage Wireless Networks** and right-click and delete all profiles that may exist.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Created a WLAN with Local EAP authentication.
- Connected your wireless client to the EAP WLAN.
- Client got an IP address in the proper range and could ping the gateway.

## **Task 4: Implement WebAuth Passthrough**

### **Activity Procedure**

In this task, you will implement WebAuth Passthrough on the converged access Switch and test with a wireless client. Here you will setup guest access that only requires consent to an AUP to access the network.

---

<b>Note</b>	The lower case "x" in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

#### **Modify Webauth Parameters**

Here you will specify that the authentication is consent (pass-through, not credentials) and the virtual IP address for redirect.

Complete these steps:

- Step 1** Open a browser and connect to the **SW1** from the Admin PC.
- Step 2** Navigate to **Configuration > Security > Web Auth > Webauth Parameter Map**. Click on **global** and enter the following information:
- Type dropdown: **consent** (agreement to AUP)

- Virtual IPv4 Address: **192.0.2.1** (Redirect address for web access)
- Click **Apply** and **OK** to pop-up.

**Security**

**Webauth Parameter Map**

Webauth Parameter Map > Edit

Parameter-map name	global
Banner	[Empty]
Maximum HTTP connections(1-200)	30
Init-State Timeout (60-3932100 in seconds)	120
Fin-Wait Timeout (1-2147483647 in millisecond)	3000
Type	consent
Turn-on Consent with Email	<input type="checkbox"/>
Virtual IPv4 Address	192.0.2.1
Virtual IPv4 hostname	[Empty]
Virtual IPv6 Address	[Empty]
Virtual IPv6 hostname	[Empty]
<b>Customized page</b>	
Failed authentication proxy	--Select--
Auth-proxy login parameters	--Select--
Customized page	--Select--

---

**Note** Global settings define the virtual address and webauth defaults. These can be refined using custom settings which you will also define next.

---

### Step 3 Continuing on Webauth Parameter Map, click New and enter the following:

- Parameter map name: **Web**
- Banner: **Hello There** (or whatever you want)
- Type dropdown: **consent** (not webconsent)
- Click **Apply** and **OK** to pop-up.

**Note** There are other Web Policy methods, like Authentication. This would require a user name and password. The user name and password can be local (like Local-EAP) or remote (like on a RADIUS server). The AAA Server tab is where you choose the order of authentication.

### Create a new WLAN

- Step 4** Navigate to **Configuration > Wireless** and then choose **WLAN > WLANs**.
- Step 5** Click on the Profile name of **Podx\_EAP**. The Status should be changed to **disabled** (Enable is unchecked).
- Step 6** Click **Apply** and **OK** to any pop-ups.
- Step 7** Go back to **WLANs** and click **New** at the top and enter the following information (x=pod#):
  - WLAN ID: **4**
  - SSID: **Podx\_Web**
  - Profile: **Podx\_Web**
  - Click **Apply** and **OK** to pop-up.
- Step 8** Select the **Podx\_Web** profile and make the following changes:
  - On the **General** tab:
    - Check the Status box for **Enabled**
    - On the **Interface/Interface Group(G)** click on the **search icon**. When the pop-up appears, choose the **Client** interface from the dropdown and click **OK**.

- Broadcast SSID = **checked** (by default)

**Step 9** Go to the **Security** tab and select the following:

- Layer 2 tab:
  - Under Layer 2 Security, select: **None**
- Layer 3 tab:
  - Web Policy: **Check to enable**
  - Weauth Parameter Map: **Web** (from the dropdown)
- Click **Apply** and **OK** to pop-ups.

The screenshot shows the 'WLAN' configuration page with the 'Edit' tab selected. The 'Security' tab is active, and the 'Layer3' sub-tab is selected. The configuration options shown are:

Web Policy	<input checked="" type="checkbox"/>
Conditional Web Redirect	<input type="checkbox"/>
Weauth Authentication List	Disabled <input type="button" value="🔍"/>
Weauth Parameter Map	Web <input type="button" value="🔍"/>
Weauth On-mac-filter Failure	<input type="checkbox"/>
Preattentiation IPv4 ACL	Unconfigured <input type="button" value="🔍"/>
Preattentiation IPv6 ACL	none <input type="button" value="🔍"/>

---

**Note** Here you defined that you are using Web Policy and WebAuth Parameter Map is Web (which will use our custom banner).

---

**Step 10** Click **WLANS** and verify that the WLAN shows **Web-Auth**.

**Step 11** On the top right of the screen, click **Save Configuration** and click **OK** on the pop-ups.

#### Verify Client Access

**Step 12** On the lab diagram, hover the cursor over the **Client PC** and left click.

**Step 13** You are now connected to the Client PC.

**Step 14** Verify operation with a wireless client.

**Step 15** Click the WLAN tray.

**Step 16** Click on the **Podx\_Web** network, and then click **Connect**. (Uncheck the box for “Connect automatically”, you don’t want to create a profile).

- Step 17** Click the WLAN tray.
- Step 18** Right click the **Podx\_Web** network and select **Status**.
- Step 19** On the **General** tab of the Status window, click the **Details** button
- Step 20** You will now see your IP address (network 192.168.14.0).
- Step 21** Open a Command Prompt and ping your gateway (192.168.14.254). This attempt should fail.

---

**Note** Even though you have an IP address, you have not yet authenticated, so the gateway is not accessible.

---

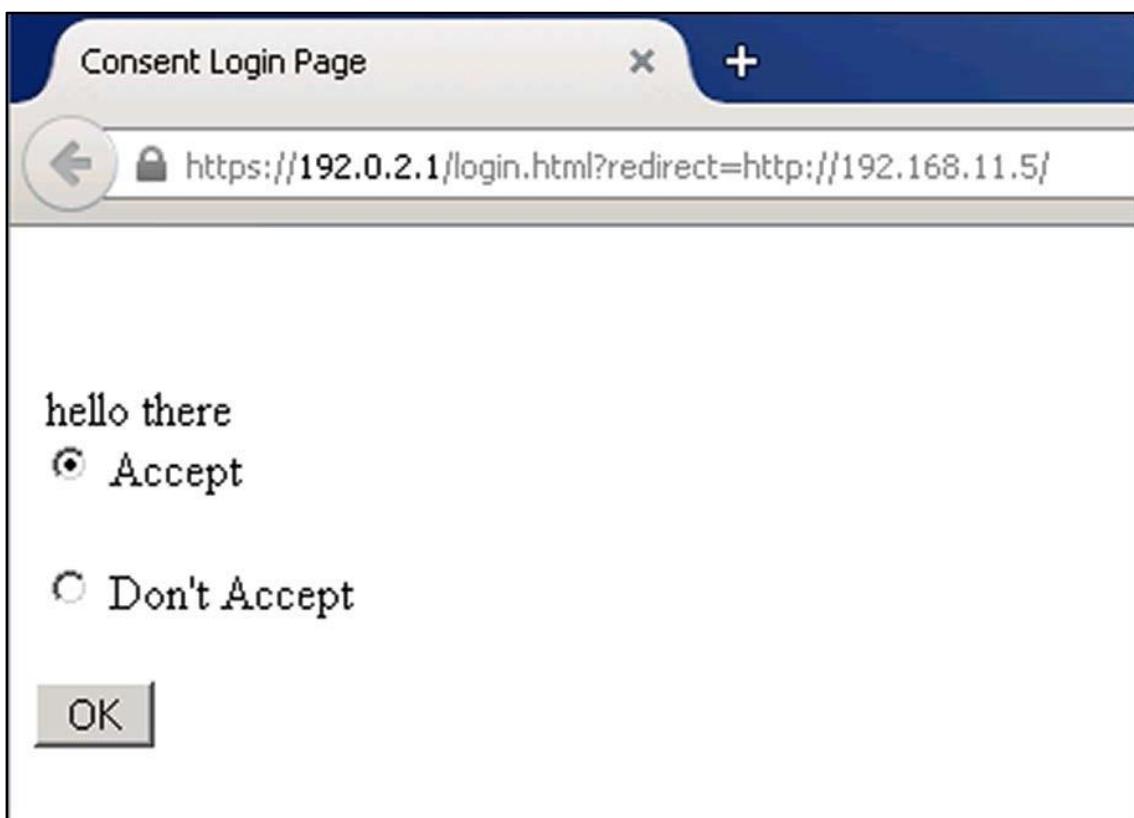
- Step 22** Verify your client connection on the **SW1 Monitor** menu and notice that the client's State is **WEBAUTH\_PEND**.
- Step 23** Open a Firefox browser on the Client PC.
- Step 24** For the URL address, type: **192.168.11.5** (Pod 2504) and **Enter**.
- Step 25** On the Untrusted Connection warning, click on **I Understand the Risks** and select **Add Exception**.
- Step 26** On the pop-up, click **Confirm Security Exception**.

---

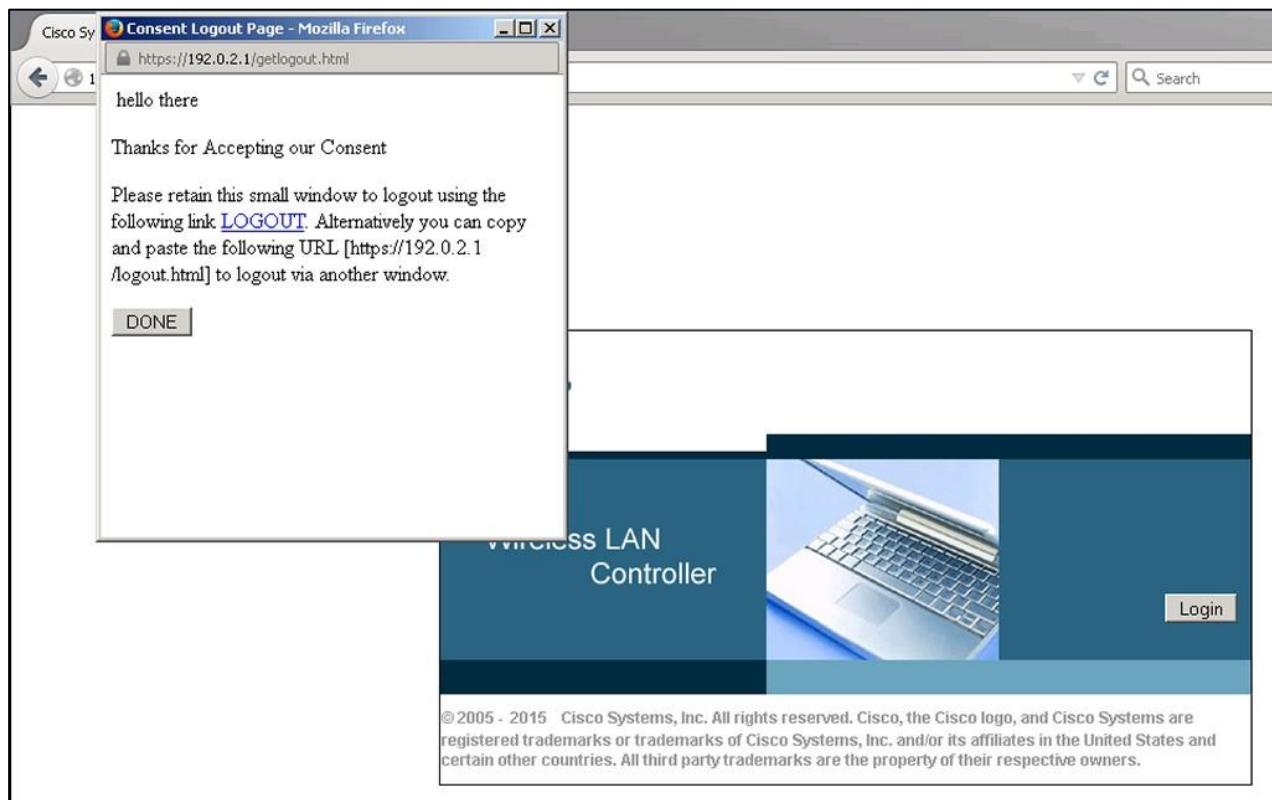
**Note** This warning is issued because the SW1 uses a self-signed certificate.

---

- Step 27** You will now see the custom banner that you created. Click **Accept** and **OK**.



**Step 28** You will see the Confirmation pop-up.



**Step 29** You will now see the original destination (WLC Login) displayed.

- Step 30** Open a Command Prompt and ping your gateway (192.168.14.254), it should be successful now.
- Step 31** Verify your client connection on the SW1 Monitor menu and notice that the client's State is **UP**.
- Step 32** When done, disconnect from the Podx\_Web WLAN on Client PC and on **SW1 Monitor > Clients**, remove the client.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Created a WLAN with WebAuth authentication.
- Connected your wireless client to the Guest WLAN.
- Client got an IP address in the proper range and could ping the gateway.

## **Task 5: Implement Local WebAuth**

### **Activity Procedure**

In this task, you will implement Local WebAuth on the converged access Switch and test with a wireless client. Here you will provide guest access gain, but now require a username and password to access the network.

---

<b>Note</b>	The lower case "x" in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

### **Modify Webauth Parameters**

This is the same as you did for pass-through, except now instead of "consent", you will require the user to authenticate (webauth) for "global" Method List and your custom (Web) Method List.

Complete these steps:

- Step 1** Open a browser and connect to the SW1 from the Admin PC.
- Step 2** Navigate to **Configuration > Security** and then to **Web Auth** Folder and then **Webauth Parameter Map**. Click on **global** and enter the following:
- Type: **webauth** (require username/password)
  - Virtual IPv4 Address: **192.0.2.1** (Redirect address for web access)
  - Click **Apply** and **OK** to pop-up.

## Webauth Parameter Map

Webauth Parameter Map > Edit

Parameter-map name	global
Banner	
Maximum HTTP connections(1-200)	30
Init-State Timeout (60-3932100 in seconds)	120
Fin-Wait Timeout (1-2147483647 in millisecond)	3000
Type	webauth ▾
Turn-on Consent with Email	<input type="checkbox"/>
Virtual IPv4 Address	192.0.2.1

**Step 3** Continue on **Webauth Parameter Map** and click **Web**. Then enter the following:

- Type dropdown: **webauth**
- Click **Apply** and **OK** to pop-up.

## Webauth Parameter Map

Webauth Parameter Map > Edit

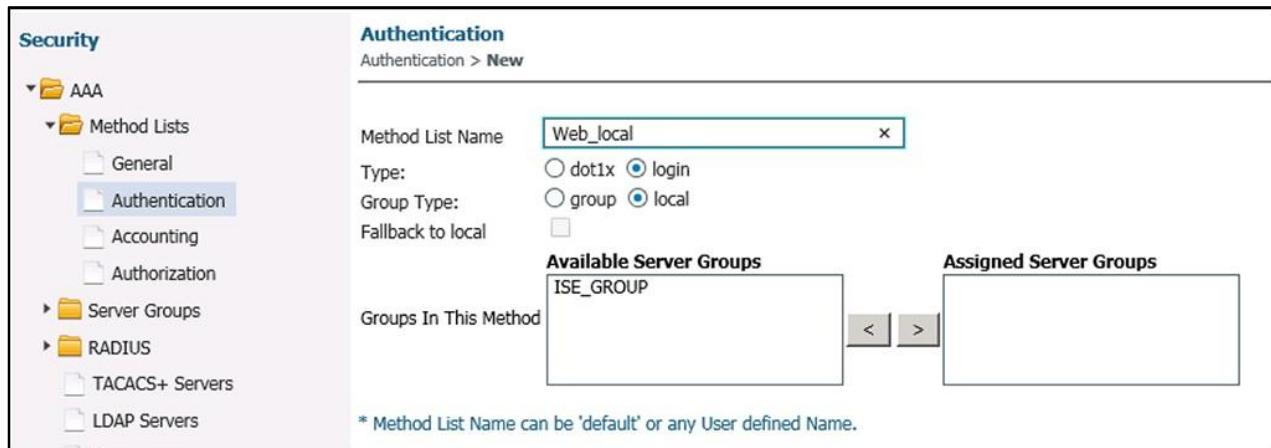
Parameter-map name	Web
Banner	hello there
Maximum HTTP connections(1-200)	30
Init-State Timeout (60-3932100 in seconds)	120
Fin-Wait Timeout (1-2147483647 in millisecond)	3000
Type	webauth ▾
Turn-on Consent with Email	<input type="checkbox"/>

## Modify Security Configurations for Authentication

This is the same as with previous authentications, you are defining method (login) and that it is local.

**Step 4** Navigate to **AAA** Folder and then **Method Lists** folder and then **Authentication**. Click **New** and enter the following:

- Method List name: **Web\_local**
- Type: **login**
- Group Type: **local**
- Click **Apply** and **OK** to pop-up.

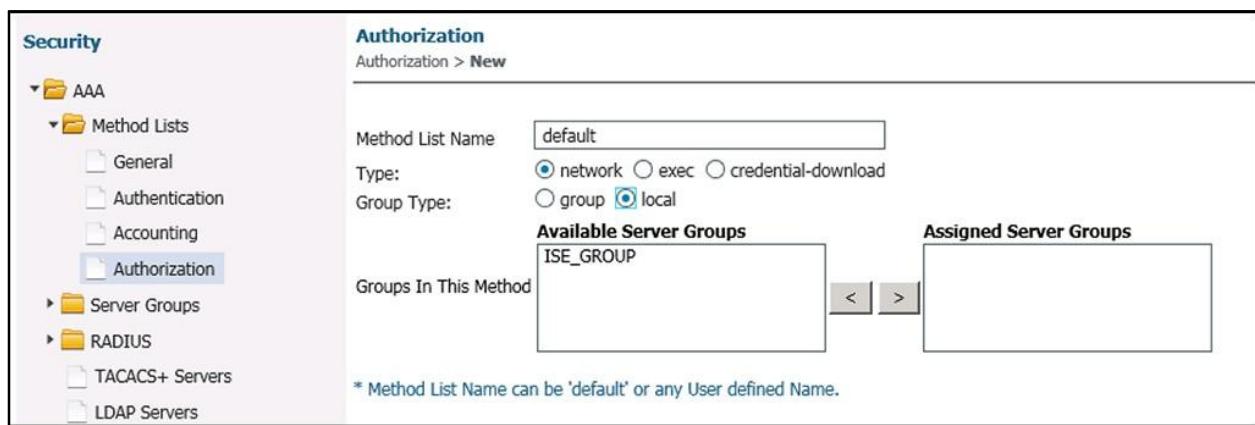


## Modify Security Configurations for Authorization

This is the same as with previous authorizations, you are defining method (network) and where the authorization will be local.

**Step 5** Navigate to **AAA** Folder and then **Method Lists** folder and then **Authorization**. Click **New** and enter the following:

- Method List name: **default**
- Type: **network**
- Group Type: **local**
- Click **Apply** and **OK** to pop-up.



## Modify WLAN

**Step 6** Navigate to **Configuration > Wireless**, select the **Podx\_Web** profile and make the following changes:

- On the **General** tab: no changes
- On the **Security** tab:
  - **Layer 2** tab: no changes
  - **Layer 3** tab:
    - Web Authentication List: **Web\_local** (from drop down)
    - Leave other settings as they were (ex: Webauth parameter Map = Web)
- Click **Apply** and **OK** to pop-ups.

The screenshot shows the 'WLAN' configuration page. At the top, there are tabs for General, Security (which is selected), QoS, AVC, Policy Mapping, and Advanced. Below these, there are sub-tabs for Layer2 and Layer3, with Layer3 being the active tab. Under the Layer3 tab, there are several configuration options: 'Web Policy' (checkbox checked), 'Conditional Web Redirect' (checkbox unselected), 'Webauth Authentication List' (dropdown set to 'Web\_local'), 'Webauth Parameter Map' (dropdown set to 'Web'), 'Webauth On-mac-filter Failure' (checkbox unselected), 'Preauthentication IPv4 ACL' (dropdown set to 'Unconfigured'), and 'Preauthentication IPv6 ACL' (dropdown set to 'none').

**Step 7** Click WLANs and verify that the WLAN shows Web-Auth

<b>Note</b>	Here you defined that you are still using Web Policy and the WebAuth Parameter Map is still Web (which will use our custom banner), but added Authentication (Web_local).
-------------	---

**Step 8** On the top right of the screen, click **Save Configuration** and click **OK** on the pop-ups.

### Verify Client Access

**Step 9** On the lab diagram, hover the cursor over the **Client PC** and left click.

**Step 10** You are now connected to the Client PC.

**Step 11** Verify operation with a wireless client.

**Step 12** Click the WLAN tray.

- Step 13** Click on the **Podx\_Web** network, and then click **Connect**. (Uncheck the box for “Connect automatically”, you don’t want to create a profile).
- Step 14** Click the WLAN tray.
- Step 15** Right click the **Podx\_Web** network and select **Status**.
- Step 16** On the **General** tab of the Status window, click the **Details** button
- Step 17** You will now see your IP address (network 192.168.14.0).
- Step 18** Open a Command Prompt and ping your gateway (192.168.14.254). This attempt should fail.

---

**Note** Even though you have an IP address, you have not yet authenticated, so the gateway is not accessible.

---

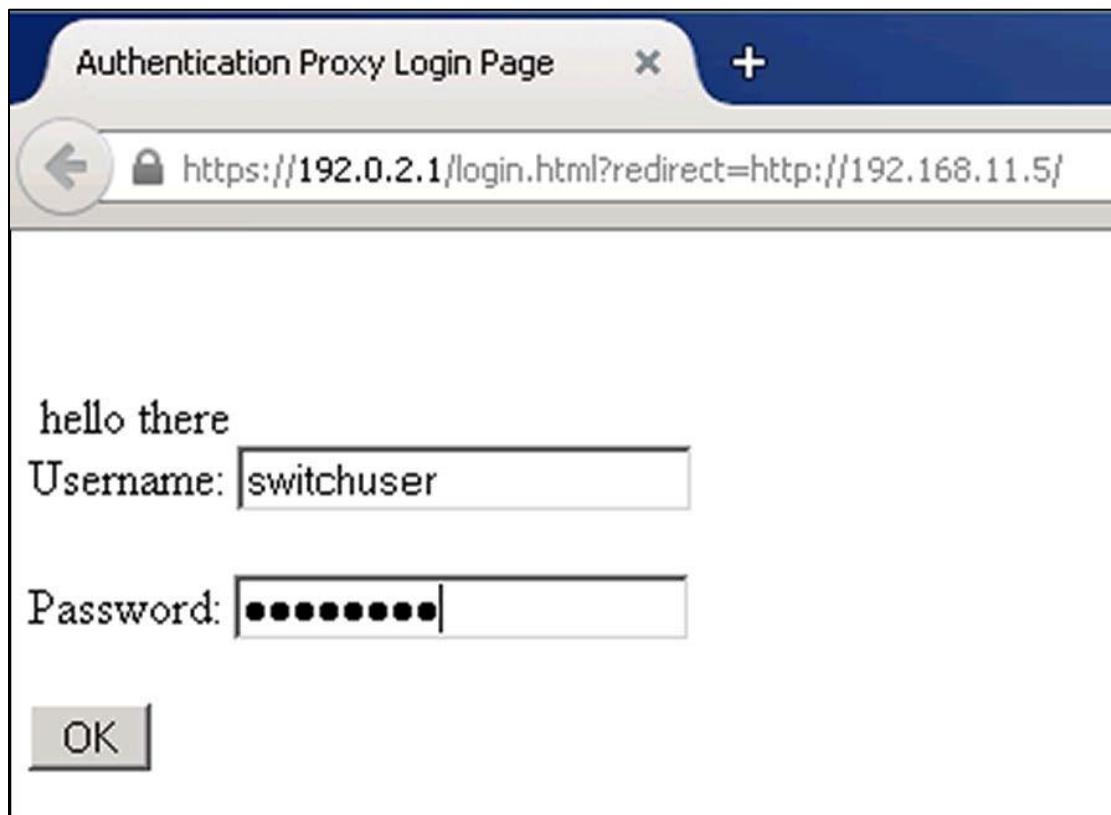
- Step 19** Verify your client connection on the SW1 Monitor menu and notice that the client’s State is **WEBAUTH\_PEND**.
- Step 20** Open a Firefox browser on the Client PC.
- Step 21** For the URL address, type: **192.168.11.5** and **Enter**.
- Step 22** On the Untrusted Connection warning, click on **I Understand the Risks**, and select **Add Exception**.
- Step 23** On the pop-up, click **Confirm Security Exception**.

---

**Note** This warning is issued because the **WLC** uses a self-signed certificate.

---

- Step 24** You will now see the custom banner that you created and be prompted for a username and password. Select the following:
- Username: **switchuser**
  - Password: **Cisco123**



**Note** Since you are using local authentication for the Web, you can reuse our predefined user of **switchuser**.

**Step 25** You will see the Confirmation pop-up.

**Step 26** You will now see the original destination (WLC Login) displayed.

**Step 27** Open a Command Prompt and ping your gateway (192.168.14.254), it should be successful now.

**Step 28** Verify your client connection on the SW1 Monitor>Client menu and notice that the client's State is **UP** and the Username is **switchuser**.

**Step 29** When done, disconnect from the Podx\_Web WLAN on Client PC and on **SW1 Monitor>Clients**, remove the client.

#### Disable WLANs

**Step 30** Navigate to **Configuration > Wireless** and then choose **WLAN > WLANs**.

**Step 31** Click on the Profile name of **Podx\_Web** and enter the following:

- Status: **disabled** (Enable is unchecked)
- Click **Apply** and **OK** to any pop-ups.

**Step 32** Verify that all WLANs are disabled (allows clean RF space for next lab).

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- Created a WLAN with WebAuth authentication.
- Connected your wireless client to the Guest WLAN.
- Client got an IP address in the proper range and could ping the gateway.



# **Hardware Lab 9: Implement a FlexConnect WLAN Deployment**

---

## **Overview**

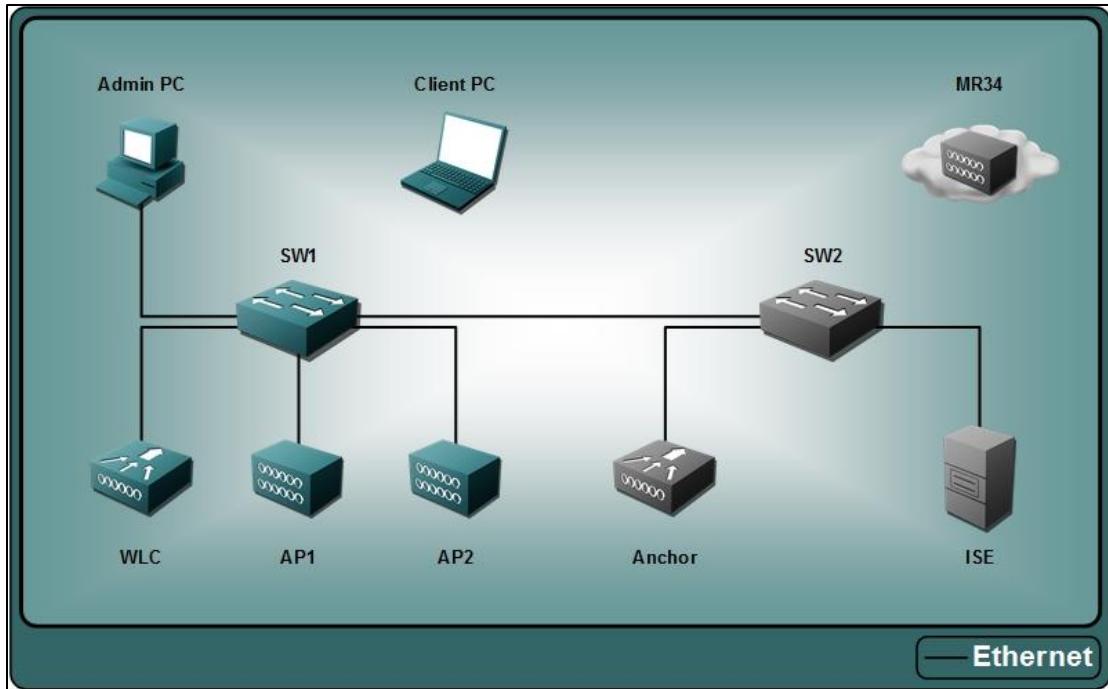
In this activity, you configure the WLC 2504 to enable FlexConnect WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Configure the Switch for FlexConnect connectivity
- Add a new WLAN for FlexConnect testing
- Adjust AP mode of operation
- Test client access for FlexConnect
- Implement a FlexConnect Group
- Test client access for FlexConnect Group
- Reset AP back to Local Mode

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 3650 IOS-XE Switch
- Pod 2504 WLC
- AP 3700i (Converged-Flex)

### VLANs and IP Ranges

#### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
WLC 2504	192.168.11.5	admin	Cisco123	
Pod 3650 Switch	192.168.11.254	admin	Cisco123	cisco

## Task 1: Configure the Switch for FlexConnect Connectivity

### **Activity Procedure**

In this task, you will make the necessary changes for the FlexConnect AP. This includes a new VLAN, VLAN interface and DHCP Scope. You will also change the port settings for the switch port that the AP is connected to.

---

**Note**      Add a DHCP Scope for the FlexConnect AP

**Note**      You will be adding a new DHCP pool for client access to test our FlexConnect deployment with local switching.

**Note**      Complete these steps:

---

**Step 1**    Connect to **SW1** on the console port.

**Step 2**    At the SW1> prompt go to the **enable** mode (password: cisco)

**Step 3**    Enter Global Config mode: **config term** and press **Enter** and type the following (enter after each line):

```
SW1(config)# ip dhcp excluded-address 192.168.16.1 192.168.16.10
SW1(config)# ip dhcp pool flex
SW1(dhcp-config)# network 192.168.16.0 255.255.255.0
SW1(dhcp-config)# default-router 192.168.16.254
```

### Add a VLAN and VLAN Interface for the FlexConnect AP

This is the VLAN that will be used for clients and for local switching.

**Step 4** Still in Global Config mode, type the following:

```
SW1(config)# vlan 16
SW1(config)# name flex
SW1(config)# interface vlan 16
SW1(config)# ip address 192.168.16.254 255.255.255.0
```

### Change the switch port type for FlexConnect AP

The port for the AP must be a trunk type port, because a FlexConnect AP will have a VLAN for the WCM Management Interface and at least one for local switching. The WLC management VLAN needs to be native for the trunk port. Any other VLANS (like Vlan 16 for local clients) must be on the “allowed” list.

**Step 5** Still in Global Config mode, type the following:

```
SW1(config)# default interface g1/0/1
SW1(config)# interface g1/0/1
SW1(config-if)# shutdown
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk native vlan 12
SW1(config-if)# switchport trunk allowed vlan 12,16
SW1(config-if)# no shutdown
```

**Step 6** Type: **copy running-config startup-config** and **Enter** to save the configuration.

**Step 7** Close the console connection to the switch.

## **Activity Verification**

You have successfully completed this task when you attain this result:

- You have configured the DHCP Scope for the FlexConnect.
- You have added a new VLAN and VLAN Interface for FlexConnect (Vlan 16).
- You modified the AP's switch port for “trunk” mode and added a VLAN (Vlan 16).

## **Task 2: Add a New WLAN for FlexConnect Testing**

### **Activity Procedure**

In this task, you will add a new WLAN for local switching, so that the AP can be tested once configured. You will set this WLAN up for Local EAP and reuse the profile and user that you created in an earlier lab.

Complete these steps:

**Step 1** Connect to the Admin PC.

**Step 2** Open a browser and connect to the GUI of the WLC (192.168.11.5).

#### **Create a new WLAN**

Here you will create a WLAN with Local-EAP and local switching.

**Step 3** Navigate to **WLANS > WLANS** and create a new WLAN with these parameters: (where x= pod#).

- Profile name: **Podx\_Flex**
- SSID: **Podx\_Flex**
- **General:**
  - Status: **Enabled**
  - Interface/Interface Group(s): **client**
  - Broadcast SSID: **Enabled**
- **Security Layer 2:**
  - Layer 2 Security: **WPA+WPA2**
  - WPA2 Policy-AES: **checked**
  - 802.1X: **Enabled**
- **Security AAA Servers:**
  - Authentication and Accounting Servers: **Uncheck Enabled boxes**
  - Local EAP Authentication: **Enabled**
  - EAP Profile Name: **WLC\_Local\_EAP**
  - Note: You created this profile and a local user on the WLC in an earlier Lab and the settings will not need to be changed.
- **Advanced:**
  - FlexConnect section: FlexConnect Local Switching: **check Enabled**

- Learn Client IP Address: **Enabled** (by default)

**WLANS > Edit 'Pod1\_Flex'**

**General Security QoS Policy-Mapping Advanced**

**Off Channel Scanning Defer**

Scan Defer Priority: 0 1 2 3 4 5 6 7

Scan Defer Time(msecs):

**FlexConnect**

FlexConnect Local Switching <sup>2</sup>	<input checked="" type="checkbox"/> Enabled
FlexConnect Local Auth <sup>12</sup>	<input type="checkbox"/> Enabled
Learn Client IP Address <sup>3</sup>	<input checked="" type="checkbox"/> Enabled
Vlan based Central Switching <sup>13</sup>	<input type="checkbox"/> Enabled
Central DHCP Processing	<input type="checkbox"/> Enabled
Override DNS	<input type="checkbox"/> Enabled
NAT-PAT	<input type="checkbox"/> Enabled
Central Assoc	<input type="checkbox"/> Enabled

---

**Note** Local switching must be enabled to allow Vlan 16 to be switched locally. “Learn Client IP Address” reports the client IP address to the WLC (remember, when using an AP in FlexConnect mode and Local Switching, it won’t know the IP address that the client received. Because the IP address is assigned locally to the client.).

---

#### Step 4 Apply (note message) and Save Configuration.

#### Activity Verification

You have successfully completed this task when you attain this result:

- Created a new WLAN with Local\_EAP authentication.
- Changed WLAN to enable FlexConnect Local Switching.

## Task 3: Adjust the AP Mode of Operation

#### Activity Procedure

In this task, you will change the AP mode from Local to FlexConnect.

#### Change the AP to FlexConnect Mode

Complete these steps:

- Step 1** Connect to the Admin PC.
- Step 2** Open a browser and connect to the GUI of the WLC (192.168.11.5).
- Step 3** Navigate to **Wireless > Access Points > All APs** and click on the AP1.
- Step 4** On the **General** tab, change the **AP Mode** to **FlexConnect** and click **Apply**.

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. On the left, a sidebar lists various wireless management categories like Access Points, Advanced, Mesh, RF Profiles, etc. The main panel title is "All APs > Details for Centralized\_AP". It features four tabs: General (selected), Credentials, Interfaces, and High Availability. Under the General tab, there are several configuration fields: AP Name (Centralized\_AP), Location (default location), AP MAC Address (f0:7f:06:da:6c:34), Base Radio MAC (f0:7f:06:e0:22:a0), Admin Status (Disable), AP Mode (FlexConnect, highlighted with a red box), AP Sub Mode (None), Operational Status (REG), Port Number (1), Venue Group (Unspecified), Venue Type (Unspecified), Venue Name (empty), and Language (empty).

### Step 5

<b>Note</b>	In the current code, the AP does not need to reboot to change from Local to FlexConnect mode (or any other mode).
-------------	---

### Add the VLAN Information on the FlexConnect Tab

When using “VLAN Support” for FlexConnect APs, the VLANs must be specified. Here you VLAN will specify the management VLAN (x2).

- Step 6** Notice the new **FlexConnect** tab and select the following:

- VLAN Support: **Checked**
- Native VLAN: **12** (matching the switch configuration for the port)

All APs > Details for Centralized\_AP

<b>General</b>	<b>Credentials</b>	<b>Interfaces</b>	<b>High Availability</b>	<b>Inventory</b>	<b>FlexConnect</b>	<b>Advanced</b>
VLAN Support <input checked="" type="checkbox"/> Native VLAN ID <input type="text" value="12"/> <b>VLAN Mappings</b> FlexConnect Group Name Not Configured						

**Step 7** Click **Apply**.

**Note** You need to have support for the native AP management VLAN.

We can override the WLAN to VLAN mapping on the APs. We can make this AP specific, and configure a different VLAN for a specific WLAN ID per AP basis (each AP can have its own configuration) or we can remove this AP specific configuration.

**Step 8** Change the following in the **FlexConnect** tab:

Click **VLAN Mappings** and make the following selections:

- Check the box next to **WLAN ID** and verify the box next to **Podx\_Flex** will be automatically checked
- Change the VLAN ID to **16**

All APs > Centralized\_AP > VLAN Mappings

AP Name	Centralized_AP																		
Base Radio MAC	f0:7f:06:e0:22:a0																		
<b>WLAN VLAN Mapping</b> <input type="button" value="Make AP Specific"/> <input type="button" value="Go"/> <table border="1"> <thead> <tr> <th>WLAN Id</th> <th>SSID</th> <th>VLAN ID</th> <th>NAT-PAT</th> <th>Inheritance</th> </tr> </thead> <tbody> <tr> <td>5</td> <td>Pod1_Flex</td> <td>16</td> <td>no</td> <td>AP-specific</td> </tr> </tbody> </table>		WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance	5	Pod1_Flex	16	no	AP-specific								
WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance															
5	Pod1_Flex	16	no	AP-specific															
<b>Centrally switched Wlans</b> <table border="1"> <thead> <tr> <th>WLAN Id</th> <th>SSID</th> <th>VLAN ID</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Pod1_Open</td> <td>N/A</td> </tr> <tr> <td>2</td> <td>pod1guest</td> <td>N/A</td> </tr> <tr> <td>3</td> <td>Pod1_EAP</td> <td>N/A</td> </tr> <tr> <td>4</td> <td>Pod1_Roam</td> <td>N/A</td> </tr> <tr> <td>6</td> <td>dssdsd</td> <td>N/A</td> </tr> </tbody> </table>		WLAN Id	SSID	VLAN ID	1	Pod1_Open	N/A	2	pod1guest	N/A	3	Pod1_EAP	N/A	4	Pod1_Roam	N/A	6	dssdsd	N/A
WLAN Id	SSID	VLAN ID																	
1	Pod1_Open	N/A																	
2	pod1guest	N/A																	
3	Pod1_EAP	N/A																	
4	Pod1_Roam	N/A																	
6	dssdsd	N/A																	
<b>AP level VLAN ACL Mapping</b> <table border="1"> <thead> <tr> <th>Vlan Id</th> <th>Ingress ACL</th> <th>Egress ACL</th> </tr> </thead> <tbody> <tr> <td>16</td> <td>none</td> <td>none</td> </tr> </tbody> </table>		Vlan Id	Ingress ACL	Egress ACL	16	none	none												
Vlan Id	Ingress ACL	Egress ACL																	
16	none	none																	
<b>Group level VLAN ACL Mapping</b> <table border="1"> <thead> <tr> <th>Vlan Id</th> <th>Ingress ACL</th> <th>Egress ACL</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>		Vlan Id	Ingress ACL	Egress ACL															
Vlan Id	Ingress ACL	Egress ACL																	
<b>Foot Notes</b> 1. Vlan does not take effect for NAT-PAT enabled WLANs.																			

**Step 9** Click **Apply** and notice the message pop-up.

---

**Note** You need to map the Vlan 16 for client access to the WLAN and this will be switched locally.

---

**Step 10** Save Configuration.

### **Alternative (not to be done for this lab):**

If you remove the AP specific we can have two options:

- The VLAN mapping or the subnet assigned to this SSID will be the same as the configuration on the interface on the WLAN (WLAN specific). This is how it was before you made it AP Specific.
- If the AP belongs to a FlexConnect group, the VLAN mapping will be determined by the FlexConnect group WLAN-VLAN mapping (Group-specific). You will do this later in the lab.

### **WLAN-VLAN Mapping Examples :**

WLAN VLAN Mapping				
Make AP Specific		Go		
WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance
3	Podx_Flex	16	no	Group-specific
4	Pod2_Flex	1	no	Wlan-specific
5	Pod3_Flex	50	no	AP-specific

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Changed the AP mode from Local to FlexConnect.
- Changed the Native VLAN for the AP to Vlan 12.
- Changed the VLAN Mapping in the AP for the WLAN Podx\_Flex to Vlan 16.

# Task 4: Test Client Access for FlexConnect

## Activity Procedure

In this task, you will test the client access to verify FlexConnect operation. You will need to create a new EAP profile as it was most likely deleted from your earlier lab for cleanup.

### Create an EAP Profile on the Client

---

<b>Note</b>	If you need additional help in setting up the EAP client, refer back to Lab 4-3 (Task #2).
-------------	--

---

Complete these steps:

- Step 1** Connect to the Client PC.
- Step 2** On the desktop, right click on **Network** and choose **Properties** to go to the **Network and Sharing Center**.
- Step 3** Click **Manage Wireless Networks**. Click **Add** and enter the following information:
  - Click on **Manually create a network profile**
  - Enter a Network Name: **Podx\_Flex**
  - Security type dropdown: **WPA2-Enterprise**
  - Encryption type dropdown: **AES**
  - Start this connection automatically: **Uncheck**
- Step 4** Click on **Change connection settings**. On the Podx\_Flex Wireless Network Properties, verify that **Connect automatically when this network is in range** is unchecked.
- Step 5** Click on the **Security** tab and select the following:
  - Network Authentication Method is **Microsoft: Protected EAP (PEAP)**
- Step 6** Remember my credentials....: **Uncheck** (You want to enter our credentials each time that you connect).
- Step 7** Click **Settings** beside Microsoft: Protected EAP (PEAP) and under **When connecting**, uncheck the **Validate server certificate**.
- Step 8** Verify under the **Select Authentication Method** that the dropdown is set to: **Secured password (EAP-MSCHAP v2)**
- Step 9** Next to this dropdown, click **Configure**.
- Step 10** Uncheck the box for **Automatically use my Windows logon name...**
- Step 11** Click **OK** and then **OK** to return to the **Security** tab.
- Step 12** On the **Security** tab, click the **Advanced Settings** button and make the following selections on the 802.1X setting:
  - Specify authentication mode: **Checked**
  - Change the dropdown to **User authentication** (username/password)
- Step 13** Click **OK** and **OK** and **Close** on Profile Wizard.
- Step 14** Observe the new profile (**Podx\_Flex**).

## Test the EAP Authentication Client

**Step 15** Connect to the **Podx\_Flex** network.

**Step 16** Enter your username of **wlcuser** and password of **Cisco123** and click **OK**.

---

**Note** Although you are locally switched, you are centrally authenticated (WLC).

---

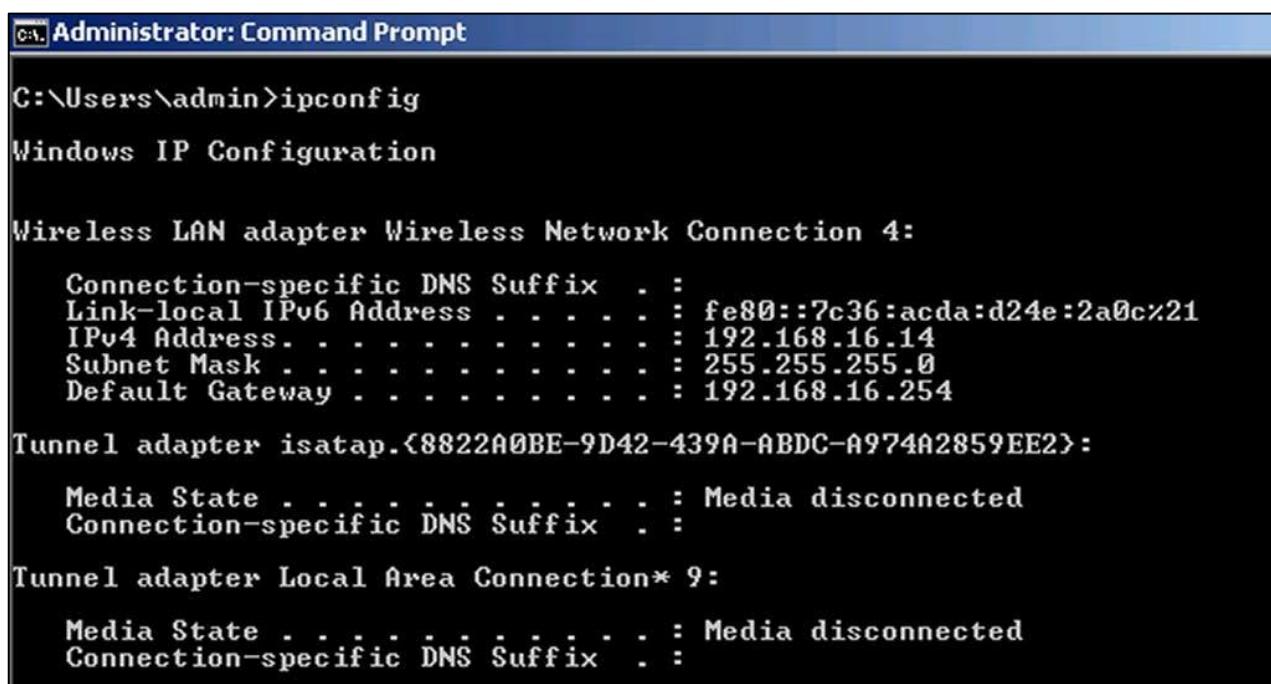
**Step 17** If authentication fails, verify that you entered the correct username/password and verify the same username/password on the WLC. Also recheck EAP profile and WLAN settings.

**Step 18** Click the WLAN tray.

**Step 19** Right click the **Podx\_Flex** network and select **Status**.

**Step 20** On the **General** tab of the Status window, click the **Details** button.

**Step 21** You will now see your IP address (network 192.168.16.0/24).



```
Administrator: Command Prompt
C:\Users\admin>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 4:
  Connection-specific DNS Suffix . . . .
  Link-local IPv6 Address . . . . . : fe80::7c36:acda:d24e:2a0c%21
  IPv4 Address . . . . . : 192.168.16.14
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.16.254

Tunnel adapter isatap.{8822A0BE-9D42-439A-ABDC-A974A2859EE2}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . .

Tunnel adapter Local Area Connection* 9:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .
```

---

**Note** Remember this IP address came from the dhcp pool/vlan that you created. The SSID was configured to user the Client VLAN (14), but the WLAN to VLAN mapping was AP Specific to the Flex Vlan (16).

---

**Step 22** Open a Command Prompt and ping your gateway (192.168.16.254).

---

**Note** Your VLAN/IP is locally switched.

---

**Step 23** Verify your client connection on the WLC Monitor menu.

Clients						Entries 1 - 1 of 1
Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	
6c:b0:ce:f6:32:05	192.168.16.14	Centralized_AP	Pod1_Flex	Pod1_Flex	wlcuser	

**Step 24** Disconnect Client from WLAN on Client PC and from WLC menu.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Connected the wireless client to the new WLAN.
- Client got an IP from the 192.168.16.0/24 network and could ping the gateway.

## **Task 5: Implement a FlexConnect Group**

### **Activity Procedure**

In this task, you will implement a FlexConnect Group on the WLC and you will switch from centralized to local authentication. FlexConnect Groups allow you to better manage the branch APs as a group, instead of individually. It also allows for local authentication as primary or backup.

#### **Modify the WLAN Profile for Local Authentication**

Complete these steps:

- Step 1** Connect to the Admin PC.
- Step 2** Open a browser and connect to the GUI of the WLC (192.168.11.5).
- Step 3** Navigate to **WLANS > WLANS** and click on the WLAN ID for the **Podx\_Flex** WLAN.
- Step 4** On the **Advanced** tab, in the FlexConnect section, set **FlexConnect Local Auth:** check **Enabled**.

Scan Defer Time(msecs)	<input type="text" value="100"/>
<b>FlexConnect</b>	
FlexConnect Local Switching <a href="#">2</a>	<input checked="" type="checkbox"/> Enabled
FlexConnect Local Auth <a href="#">12</a>	<input checked="" type="checkbox"/> Enabled
Learn Client IP Address <a href="#">5</a>	<input checked="" type="checkbox"/> Enabled
Vlan based Central Switching <a href="#">13</a>	<input type="checkbox"/> Enabled
Central DHCP Processing	<input type="checkbox"/> Enabled
Override DNS	<input type="checkbox"/> Enabled
NAT-PAT	<input type="checkbox"/> Enabled
Central Assoc	<input type="checkbox"/> Enabled

---

**Note** Now the authentication will be local (switching was already local).

---

**Step 5** Click **Apply**.

**Create a FlexConnect Group and Add the AP**

You will create a new FlexConnect Group, Add your AP (as it isn't there automatically) and enable AP Authentication.

**Step 6** Navigate to **Wireless > FlexConnect Groups**, click **New** and enter a Group Name: **FlexGroup**.

**Step 7** Click **Apply**.

**Step 8** Click on the new **FlexGroup** and edit the following on the **General** tab:

- Add AP: **Click**
  - Select APs from current controller: **check**
  - AP Name: **AP1** (Only FlexConnect APs will be displayed)
  - You will now see the AP1 listed and associated.

**FlexConnect Groups > Edit 'FlexGroup'**

<b>General</b>	<b>Local Authentication</b>	<b>Image Upgrade</b>
<b>Group Name</b> FlexGroup Enable AP Local Authentication <input checked="" type="checkbox"/>		
<b>FlexConnect APs</b>		
<b>Add AP</b>		
Select APs from current controller <input checked="" type="checkbox"/> AP Name AP1 ▼ Ethernet MAC 54:a2:74:73:78:88 <input type="button" value="Add"/> <input type="button" value="Cancel"/>		

**Step 9** Continuing on the **General** tab, select the checkbox for Enable AP Local Authentication (AP will now authenticate clients locally, not the WLC).

<b>General</b>	<b>Local Authentication</b>	<b>Image Upgrade</b>	<b>ACL Mapping</b>	<b>Central DHCP</b>						
<b>Group Name</b> FlexGroup Enable AP Local Authentication <input checked="" type="checkbox"/>										
<b>FlexConnect APs</b>										
<b>Add AP</b>										
Select APs from current controller <input type="checkbox"/> Ethernet MAC <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Cancel"/>										
<table border="1"> <thead> <tr> <th>AP MAC Address</th> <th>AP Name</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>54:a2:74:73:78:88</td> <td>AP1</td> <td>Associated</td> </tr> </tbody> </table>					AP MAC Address	AP Name	Status	54:a2:74:73:78:88	AP1	Associated
AP MAC Address	AP Name	Status								
54:a2:74:73:78:88	AP1	Associated								

**Step 10** Click **Apply**.

**Verify that the AP is in the FlexConnect Group AP**

**Step 11** Navigate to **Wireless > Access Points > All APs** and select the **AP1** and go to the **FlexConnect** tab.

**Step 12** Verify that the FlexConnect Group name is now **FlexGroup**.

All APs > Details for Centralized\_AP

**General    Credentials    Interfaces    High Availability**

VLAN Support

Native VLAN ID  **VLAN Mappings**

**FlexConnect Group Name** **FlexGroup**

The screenshot shows the 'Centralized\_AP' configuration page. The 'General' tab is active. Under 'VLAN Support', there is a checked checkbox. The 'Native VLAN ID' is set to 12. A red box highlights the 'FlexConnect Group Name' field, which contains 'FlexGroup'. The 'VLAN Mappings' button is also visible.

#### Modify the FlexConnect Group to Use PEAP

Local Authentication has several protocols that can be used for authentication; you will choose PEAP (PEAP and EAP-TLS added in AireOS 7.5). You will use PEAP, as you can disable the use of certificates authentication side (from the client profile).

**Step 13** Navigate to **Wireless > FlexConnect Groups** and click the Group Name: **FlexGroup**.

**Step 14** On the **Local Authentication** tab and then **Protocols** tab, change the following:

- Enable PEAP Authentication: **Checked**
- All others: **Unchecked**
- Click **Apply**

Wireless

- Access Points**
  - All APs
  - Radios
    - 802.11a/n/ac
    - 802.11b/g/n
    - Dual-Band Radios
    - Global Configuration
- Advanced**
  - Mesh
  - RF Profiles
  - FlexConnect Groups**
    - FlexConnect ACLs
  - OEAP ACLs**
  - Network Lists**
  - 802.11a/n/ac
  - 802.11b/g/n
  - Media Stream
  - Application Visibility And Control
  - Country
  - Timers
  - Netflow
  - QoS

FlexConnect Groups > Edit 'FlexGroup'

General	Local Authentication	Image Upgrade	ACL Mapping	Central DHCP	WLAN
	<b>Local Users</b>	Protocols			
<b>LEAP</b> <input type="checkbox"/> Enable LEAP Authentication <sup>2</sup> <b>EAP Fast</b> <input type="checkbox"/> Enable EAP Fast Authentication <sup>2</sup> Server Key (in hex) <input type="checkbox"/> Enable Auto key generation <small>*****</small> <small>*****</small> (Confirm server key) Authority ID (in hex) 436973636f0000000000000000000000 Authority Info Cisco A_ID PAC Timeout (2 to 4095 days) <input type="checkbox"/> <b>PEAP</b> <input checked="" type="checkbox"/> Enable PEAP Authentication <sup>2</sup> <b>EAP TLS</b> <input type="checkbox"/> Enable EAP TLS Authentication <sup>2</sup> <input type="checkbox"/> EAP TLS Certificate download <sup>2</sup>					

### Add a User for Local AP Authentication

For the AP to do Local PEAP authentication, you will need a user list that will be downloaded to the APs in the FlexConnect group.

**Step 15** On the **Local Authentication** tab and then **Local Users** tab, add the following:

- Username: **flexuser**
- Password/Confirm: **Cisco123**
- Click **Add**

FlexConnect Groups > Edit 'FlexGroup'

General	Local Authentication	Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping
	<b>Local Users</b>	Protocols			
No of Users 0 User Name <input type="text"/> Add User Upload CSV file <input type="checkbox"/> File Name <input type="text"/> Browse... UserName <input type="text"/> flexuser Password <input type="text"/> <small>*****</small> Confirm Password <input type="text"/> <small>*****</small> <input type="button" value="Add"/>					

**Step 16** Go back to the **Local Authentication** tab and then **Local Users** tab, verify that the User Name of **flexuser** is listed.

## Map the WLAN to the Correct VLAN

Earlier, you mapped VLANs to be AP Specific, now you will map them to me Group Specific, because the FlexConnect Group will determine the VLAN mapping.

**Step 17** Still on the Flex Group, go to the **WLAN VLAN mapping** tab and enter the following:

- WLAN Id: (**WLAN ID** for the Podx\_Flex WLAN – check **WLANS > WLANS**)
- VLAN Id: **16**
- Click **Add** and **Apply**.

FlexConnect Groups > Edit 'FlexGroup'

**General Local Authentication Image Upgrade ACL Mapping**

**WLAN VLAN Mapping**

WLAN Id	<input type="text" value="2"/>
Vlan Id	<input type="text" value="16"/>
<b>Add</b>	

WLAN Id	WLAN Profile Name	Vlan
5	Pod1_Flex	<input type="text" value="16"/>

**Step 18** Go back to the **WLAN VLAN mapping tab** and verify that the WLAN Id/WLAN Profile Name are correct (**Podx\_Flex**) and the VLAN is correct (**16**).

FlexConnect Groups > Edit 'FlexGroup'

**General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping**

**WLAN VLAN Mapping**

WLAN Id	<input type="text" value="1"/>
Vlan Id	<input type="text" value="1"/>
<b>Add</b>	

WLAN Id	WLAN Profile Name	Vlan
5	Pod1_Flex	<input type="text" value="16"/>

## **Step 19 Save Configuration.**

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- Modified the Podx\_Flex WLAN for FlexConnect Local Authentication.
- Added a FlexConnect Group.
- Added the AP to the FlexConnect Group and changed the following:
  - Changed the Local Authentication Protocol to PEAP only
  - Added a local user (flexuser)
  - Mapped the WLAN/VLAN to the WLAN of Podx\_Flex and Vlan 16

## **Task 6: Test Client Access for FlexConnect Group**

### ***Activity Procedure***

In this task, you will test the client access to verify FlexConnect Group operation. Here you will use the Local username/password that you created for the FlexConnect Group.

Complete these steps:

**Step 1** Connect to the Client PC.

**Step 2** Connect to the **Podx\_Flex** network and enter your username of **wlcuser** and password of **Cisco123** and click **OK**.

---

<b>Note</b>	Authentication should fail because you are no longer Centrally authenticating and that username/password is stored on the WLC.
-------------	--

---

**Step 3** Click **Cancel**.

**Step 4** Connect to the **Podx\_Flex** network again and enter your username of **flexuser** and password of **Cisco123** and click **OK**.

---

<b>Note</b>	This should work because this is the user that was downloaded to the AP for Local authentication. If it does not work, check your username/password on the FlexConnect Group.
-------------	---

---

**Step 5** Click the WLAN tray.

**Step 6** Right click the **Podx\_Flex** network and select **Status**.

**Step 7** On the **General** tab of the Status window, click the **Details** button

**Step 8** You will now see your IP address (network 192.168.16.0/24).

---

<b>Note</b>	This is IP is from the locally switched VLAN that you mapped it at the FlexConnect Group.
-------------	---

---

**Step 9** Open a Command Prompt and ping your gateway (192.168.16.254).

**Step 10** Verify your client connection on the WLC Monitor menu.

---

<b>Note</b>	Notice that the client's User name is listed. That is because the AP is in Connected mode and the security information is passed up to the WLC.
-------------	---

---

### **Optional LAB - FlexConnect in Standalone Mode Check**

In this optional assignment, you will force the FlexConnect AP into standalone mode by disconnecting the WLC (turning off its switch port).

**Step 11** Disconnect Client from WLAN on Client PC and from WLC menu.

**Step 12** Connect to the **SW1** console port.

**Step 13** Login and go to Enable mode (cisco).

**Step 14** Type: **show cdp neighbors**

**Step 15** Verify that the WLC (2504) is on interface g1/0/12.

**Step 16** You will now disconnect the WLC 2504 by shutting off its port.

**Step 17** Go into Global Configuration (config term) and enter the following:

```
PodSwitchx (config)# interface g1/0/12  
PodSwitchx (config-if)# shutdown
```

**Step 18** Leave Console connection open.

**Step 19** Connect to the **Podx\_Flex** network again and enter your username of **flexuser** and password of **Cisco123** and click **OK**.

**Step 20** Verify your IP address is on the 192.168.16.0/24 network and you can ping the gateway (192.168.16.254).

**Step 21** You will not be able to verify the connection on the WLC, as network connectivity to the WLC was cutoff. The AP is operating on its own.

**Step 22** Connect to the **SW1** console port and enter the following:

```
PodSwitchx (config)# interface g1/0/12  
PodSwitchx (config-if)# no shutdown  
PodSwitchx (config-if)# exit
```

**Step 23** Disconnect from the **SW1**.

---

**Note** You should have connectivity to WLC in about a minute.

---

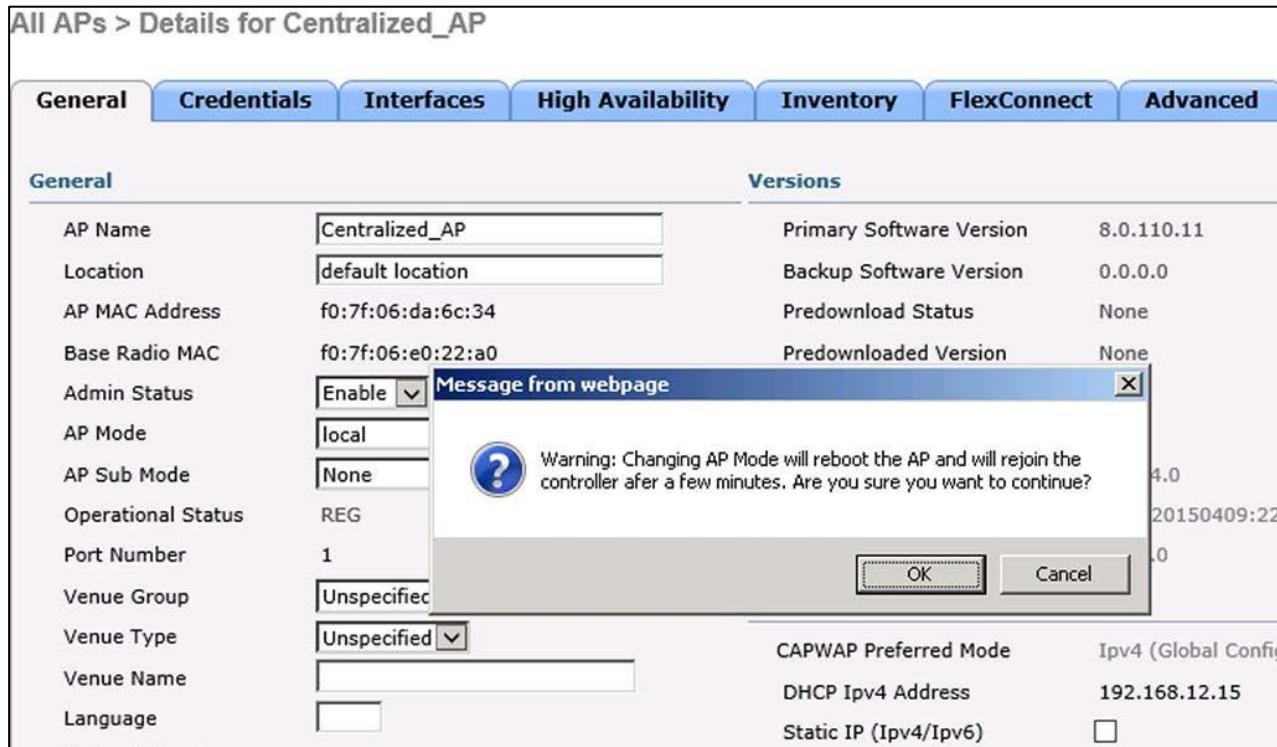
**Step 24** Once the WLC is back up, you should be able to verify the AP is connected and the client is connected.

#### Clean-up for Flex Lab

**Step 25** Disconnect Client from WLAN on Client PC and from WLC menu

**Step 26** Navigate to **Wireless > Access Points > All APs** and click on the **AP1** and change the following:

- AP Mode: **local**
- Click **Apply**



**Step 27** You will get a popup message indicating that it must reboot, click **OK**.

---

**Note** Going from FlexConnect to local mode will reboot the AP.

---

**Step 28** When the AP reconnects (click refresh periodically), click on it to edit the following:

- On the General tab, set the Admin Status to **Disable**
- Click **Apply**

**Step 29** From the **All APs** menu, verify that the Admin Status is **Disabled**.

---

<b>Note</b>	This AP was disabled to clear the RF space for the next lab.
-------------	--

---

**Step 30** Navigate to **WLANs > WLANs** and edit the **Podx\_Flex** WLAN and on the General tab, **uncheck** the box beside Status to disable this WLAN.

**Step 31** Click **Apply**.

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- Connected the wireless client to the Podx\_Flex WLAN using the local FlexConnect credentials (flexuser).
- Verified IP connectivity to the correct network (192.168.16.0/24).
- Optionally, cut communication to the WLC to test FlexConnect operation.
- Disconnected client and restored Switch connectivity to the WLC, if required.
- Changed Flex AP back to Local mode.
- Administratively disabled the AP.

## **Task 7: Switch Configuration Example**

**This section presents the switch configuration for Podx as an example.**

**Podx – Running Configuration Changes**

**CLI Changes for Task #1**

```
ip excluded-address 192.168.16.1 192.168.16.10
!
ip dhcp pool flex
network 192.168.16.0 255.255.255.0
default-router 192.168.16.254
!
vlan 16
name flex
!
interface GigabitEthernet1/0/1
description Centralized
switchport access vlan 12
switchport trunk native vlan 12
switchport trunk allowed vlan 12,16
switchport mode trunk
spanning-tree portfast
```



# **Hardware Lab 10: Initialize an Autonomous WLAN Deployment**

---

## **Overview**

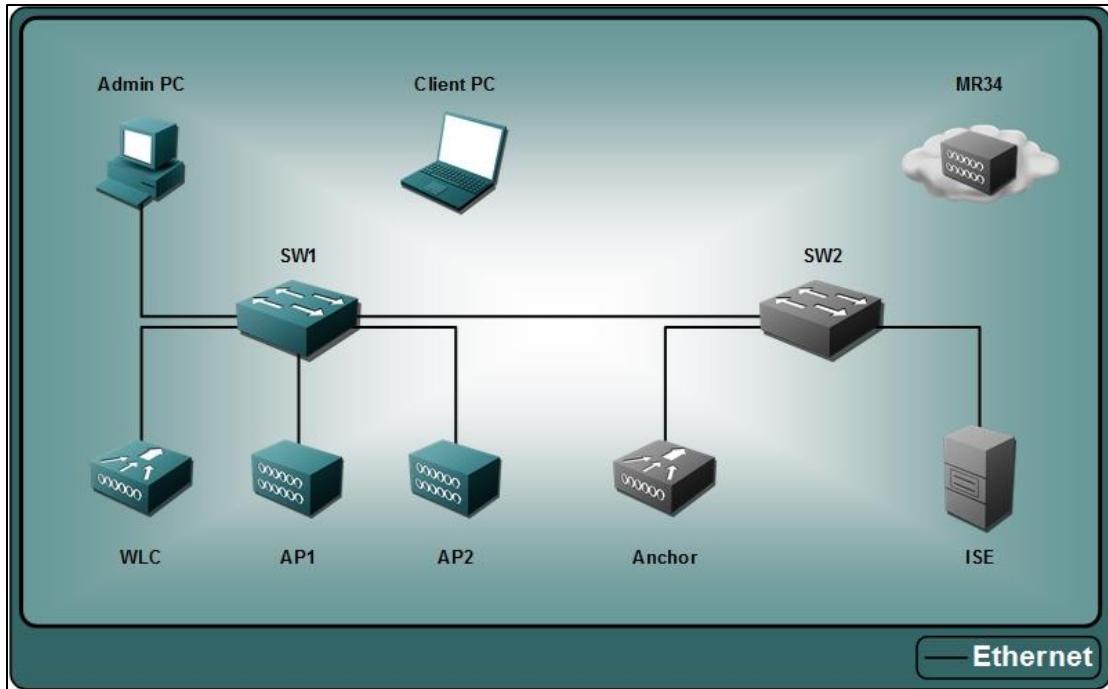
In this activity, you configure an autonomous AP WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Initialize and configure an autonomous AP.
- Test client access to the autonomous AP.

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 3650 IOS-XE Switch
- Pod 2504 WLC
- AP 3700i (Autonomous)

### VLANs and IP Ranges

#### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
WLC 2504	192.168.11.5	admin	Cisco123	
Autonomous AP	192.168.12.5	cisco	Cisco	

## Task 1: Initialize and Configure the Autonomous AP

### **Activity Procedure**

In this task, you will make the necessary changes initialize and configure the autonomous AP.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

#### **Modify the Autonomous AP’s Switch Port**

Here you will add the VLANs for the AP: DHCP for AP IP address (12) and the client DHCP (14).

Complete these steps:

**Step 1** Connect to the SW1 console port.

**Step 2** Login and go to Enable mode (**cisco**).

**Step 3** Go into Global Configuration (config term), then enter the following:

```
SW1 (config)# interface g1/0/2
SW1 (config-if)# switchport trunk allowed vlan 12,14
SW1 (config-if)# no shutdown
```

**Step 4** Exit Global Configuration and save the configuration (**copy running-config startup-config**).

**Step 5** Close the Console connection.

### Explore and Configure the Autonomous AP

You need to know the IP Address of the Autonomous AP to be able to manage it and make any changes that can only be done from the CLI.

**Step 6** Connect to the Console Port of the AP2 and go to the enable mode (password = **Cisco**).

**Step 7** Type **show ip interface brief** and look for the BVI1 interface. You will see the IP address (DHCP) and it is the same one shown for the AP on the WLC (network 192.168.12.0/24). Record your IP address.

---

**Note** IP is from DHCP scope with VLAN of 12.

---

**Step 8** Go to Global Configuration (**config term**) and type:

```
ip http timeout-policy idle 300 life 300 requests 100
dot11 wpa handshake timeout 500
dot11 wpa handshake init-delay 10
```

**Step 9** Exit Global Configuration.

**Step 10** At the Enable prompt, save the configuration (**copy running-config startup-config**).

**Step 11** Close Console connection.

### Configure the Autonomous AP via the Web GUI for Basic Operation

Here you will assign a hostname and a static IP (since this is autonomous, is usually a good idea to use static IPs for management purposes).

Here you will access the AP via the GUI and run the EASY Setup option to quickly configure the AP.

**Step 12** Connect to the Admin PC.

**Step 13** Open a web browser (IE) and enter the IP address of the AP (from previous section) as the URL.

**Step 14** You will be prompted for username/password (enter **cisco/Cisco**) - default for AP.

**Step 15** On the left navigation panel, click on **Easy Setup** and then **Network Configuration**.

The screenshot shows the Cisco Aironet 3700 Series Access Point configuration interface. The top navigation bar includes links for Save Configuration, Ping, Logout, and Refresh. The main menu bar has options: HOME, NETWORK, ASSOCIATION, WIRELESS, SECURITY, SERVICES, MANAGEMENT, SOFTWARE, and EVENT LOG. On the left sidebar, there are links for Home, Summary, Easy Setup, and Network Assistant. The central content area displays the 'Cisco Aironet 3700 Series Access Point' summary page. It shows the Hostname as Autonomous\_AP and the uptime as 19 hours, 52 minutes. The 'Association' section indicates 0 clients and 0 infrastructure clients. The 'Network Identity' section provides IP Address (192.168.12.5), IPv6 Address (FE80::F27F:6FF:FECD:22C4), and MAC Address (f07f.06cd.22c4). The 'Network Interfaces' section lists three interfaces: GigabitEthernet (f07f.06cd.22c4, 1Gbps), Radio0-802.11N<sup>40MHz</sup> (f07f.06da.a9f0, MCS Index 23), and Radio1-802.11AC<sup>5GHz</sup> (f07f.06da.db70, 9.3Mb/s). The 'Event Log' section shows three entries from March 19, 2016, at 19:51:06.003:

Time	Severity	Description
Mar 1 19:51:06.003	◆Notification	Line protocol on Interface Dot11Radio1, changed state to down
Mar 1 19:51:06.003	◆Warning	No SSID configured. Dot11Radio1 not started.
Mar 1 19:51:05.015	◆Notification	Interface Dot11Radio1, changed state to reset

**Step 16** Enter the following on the **Network Configuration** page:

- Host name: **Autonomous\_AP**
- Click **Static IP** radio button and enter:
  - IP Address: **192.168.12.5** (in DHCP excluded range)
  - IP Subnet Mask: **255.255.255.0**
  - Default Gateway: **192.168.12.254**
  - IPv6 Address: **Uncheck DHCP and Autoconfig**

The screenshot shows the Cisco Network Configuration interface. The top navigation bar includes links for HOME, NETWORK, ASSOCIATION, WIRELESS, SECURITY, SERVICES, MANAGEMENT, and SOFTWARE. On the left sidebar, under the 'Easy Setup' section, 'Network Configuration' is selected. The main content area is titled 'Network Configuration' and contains the following fields:

Host Name:	Autonomous_AP
Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address:	192.168.12.5
IP Subnet Mask:	255.255.255.0
Default Gateway:	192.168.12.254
IPv6 Protocol:	<input type="checkbox"/> DHCP <input type="checkbox"/> Autoconfig <input type="checkbox"/> Static IP
IPv6 Address:	(X:X:X::X/<0-128>)
Username:	[empty]
Password:	[empty]
SNMP Community:	defaultCommunity
<input type="radio"/> Read-Only <input checked="" type="radio"/> Read-Write	

At the bottom of the configuration box are two buttons: 'Apply' and 'Cancel'.

---

**Note** We are not using IPv6, but it is IPv6 capable.

---

**Step 17** Now click **Apply** in the Network Configuration box (top area).

**Step 18** Click **OK** on the message popup.

**Step 19** Type the new **IP address as the URL** (192.168.12.5).

**Step 20** Log back in (cisco/Cisco).

#### Configure the Autonomous AP Radio Settings

Just like any WLAN, you need to setup radio channels and power.

**Step 21** Notice both radios (2.4/5 GHz) are disabled (not enabled).

The screenshot shows the Cisco Aironet 3700 Series Access Point configuration interface. The top navigation bar includes links for Save Configuration, Ping, Logout, and Refresh. The main menu on the left has options for Home, Summary, Easy Setup, and Network Assistant. The central pane displays the 'Cisco Aironet 3700 Series Access Point' interface for 'Hostname Autonomous\_AP'. It shows summary status, association details (Clients: 0, Infrastructure clients: 0), network identity (IP Address: 192.168.12.5, IPv6 Address: FE80:F27F:6FF:FECD:22C4, MAC Address: f07f.06cd.22c4), and network interfaces (Interface: GigabitEthernet, MAC Address: f07f.06cd.22c4, Transmission Rate: 1Gbps; Interface: Radio0-802.11N2.4GHz, MAC Address: f07f.06da.a9f0, MCS Index: 23; Interface: Radio1-802.11AC5GHz, MAC Address: f07f.06da.db70, 9.3Mbps). An event log section is also present.

**Note** You are only going to enable the 802.11ac radio for this lab.

**Step 22** Click on the **Radio1-802.11AC**.

**Step 23** Click on the **Settings** tab.

The screenshot shows the 'RADIO1-802.11AC STATUS' tab selected in the navigation bar. The central pane displays the 'Network Interfaces: Radio1-802.11AC Status' configuration. It includes sections for Configuration (Software Status: Disabled, Hardware Status: Down), Operational Rates (a list of supported rates including 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0, m0-2, m1-2, m2-2, m3-2, m4-2, m5-2, m6-2, m7-2, m8-2, m9-2, m10-2, m11-2, m12-2, m13-2, m14-2, m15-2, m16-2, m17-2, m18-2, m19-2, m20-2, m21-2, m22-2, m23-2, a0-1-2, a1-1-2, a2-1-2, a3-1-2, a4-1-2, a5-1-2, a6-1-2, a7-1-2, a8-1-2, a9-1-4, a0-2-2, a1-2-2, a2-2-2, a3-2-2, a4-2-2, a5-2-2, a6-2-2, a7-2-2, a8-2-2, a9-2-4, a0-3-2, a1-3-2, a2-3-2, a3-3-2, a4-3-2, a5-3-2, a6-3-2, a7-3-2, a8-3-2, a9-3-2 Mb/sec), Aironet Extensions (Enabled, Carrier Set, Americas), Configured Radio Channel (0 MHz Channel 0, Transmitter Power, 15 dBm), Role in Network (Access Point), Antenna Gain (0 dB), and Interface Statistics (Interface Resets, 0).

**Step 24** On Settings tab, select the **Enable** radio button to the right of the **Enable Radio**.

The screenshot shows the 'RADIO1-802.11AC STATUS' tab selected. The 'HOSTNAME' is set to 'Autonomous\_AP'. Under 'Network Interfaces: Radio1-802.11AC Settings', the 'Enable Radio' option is set to 'Enable' (radio button selected). The 'Current Status (Software/Hardware)' is 'Disabled' (red arrow icon) and 'Role in Radio Network' is 'Access Point' (radio button selected). Other options include 'Access Point (Fallback to Radio Shutdown)', 'Access Point (Fallback to Repeater)', and 'Repeater'.

**Step 25** At the bottom of the page, click **Apply**.

**Step 26** The 5GHZ radio is still down (no SSID). Scroll down to the channel settings (**DefaultRadio Channel**).

The screenshot shows the 'DefaultRadio Channel' setting set to 'Dynamic Frequency Selection (DFS) Channel 0 0 MHz'. Below it, the 'Dynamic Frequency Selection Bands' dropdown menu is open, showing three options: 'Band 1 - 5.150 to 5.250 GHz', 'Band 2 - 5.250 to 5.350 GHz' (selected), and 'Band 3 - 5.470 to 5.725 GHz'.

**Step 27** The Radio is set for DFS and in this example is currently on channel 36. Also notice that that Band 3 will not be used for DFS Selection (channel assignment will be modified later).

---

**Note** Channel Width is 20MHz by default for 5GHz and must be changed at the command line for channel bonding.

---

**Step 28** Click on the **Home** Menu to return to Home Screen.

**Step 29** To change the 2.4GHz , click the **Radio0-802.11N – 2.4 GHz radio** option.



**Step 30** Go to the **Settings** tab and scroll down to the channel settings (**DefaultRadio Channel**).

<b>DefaultRadio Channel:</b>	Least Congested Frequency <input type="button" value="▼"/> Channel 0 0 MHz
<b>Least Congested Channel Search:</b> (Use Only Selected Channels)	<input type="button" value="Channel 1 - 2412 MHz"/> <input type="button" value="Channel 2 - 2417 MHz"/> <input type="button" value="Channel 3 - 2422 MHz"/> <input type="button" value="Channel 4 - 2427 MHz"/> <input type="button" value="Channel 5 - 2432 MHz"/> <input type="button" value="Channel 6 - 2437 MHz"/> <input type="button" value="Channel 7 - 2442 MHz"/> <input type="button" value="Channel 8 - 2447 MHz"/> <input type="button" value="Channel 9 - 2452 MHz"/> <input type="button" value="Channel 10 - 2457 MHz"/> <input type="button" value="Channel 11 - 2462 MHz"/> <input type="button" value="Channel 12 - 2467 MHz"/> <input type="button" value="Channel 13 - 2472 MHz"/>
<b>Channel Width:</b>	20 MHz <input type="button" value="▼"/> 20 MHz

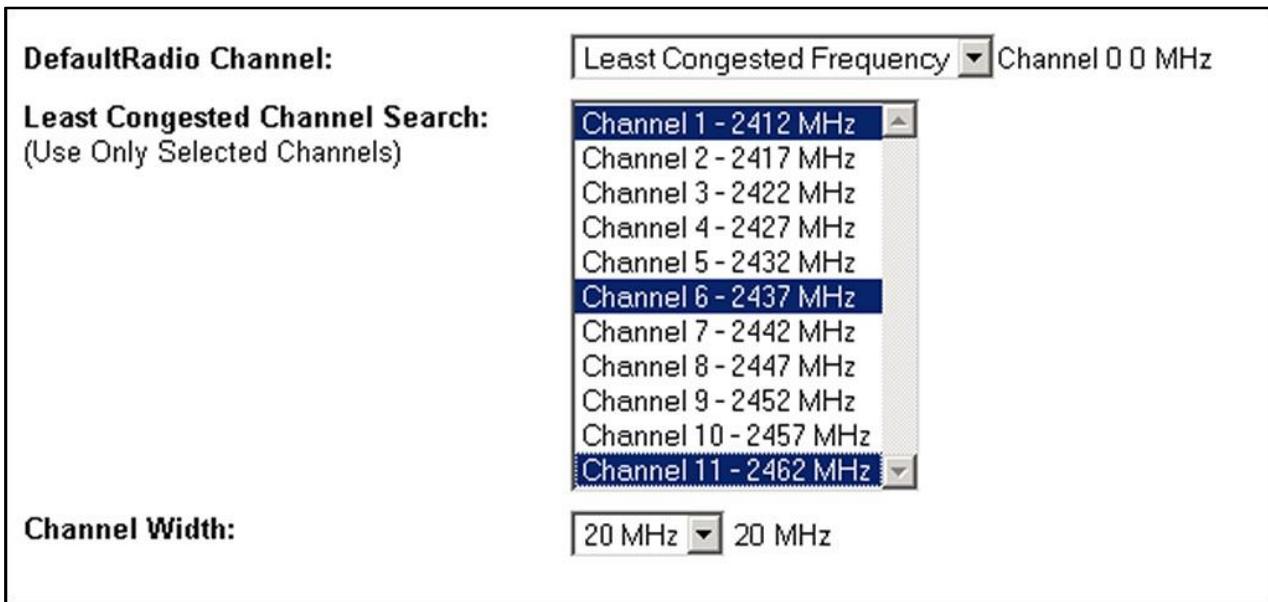
**Step 31** The 2.4 GHz radio is automatically set to use **Least Congested Channel**.

---

<b>Note</b>	Remember from the lesson , that the AP does not know about adjacent channels and it will move to any channel (1-11).
-------------	--

---

**Step 32** If you were using the 2.4 GHz radio, you would set the channel and also use only channels 1, 6, 11 to avoid adjacent channel issues.



### Configure the Autonomous AP WLAN

Here you will only use the 5GHz radio for the WLAN. If you needed to add the other radio later, you could do that through SSID Manager.

**Step 33** Navigate to **Home > Easy Setup** and then **Network Configuration** and enter the following in **Radio Configuration** under the **Radio 5 GHz**:

- **SSID:** **Padx\_Auto**
- Broadcasts SSID in Beacon: **Checked**
- Enable VLAN ID: **Enable** and set VLAN ID to: 14 (client VLAN)
- Universal Admin Mode: **Disable**
- Security: **No Security**
- Role in Radio Network: **Access Point** (other option of bridge, scanner and etc.)
- Optimize Radio Network: **Default** (could choose range or throughput for data rates)
- Aironet Extensions: **Enable**
- Channel: **Dynamic Frequency Selection**
- Transmitter Power: **3** (or lowest number)

**Radio 5GHz**

SSID :	Pod14_Auto
<input checked="" type="checkbox"/> <a href="#">Broadcast SSID in Beacon</a>	
VLAN :	<input type="radio"/> No VLAN <input checked="" type="radio"/> Enable VLAN ID: 14 (1-4094) <input type="checkbox"/> Native VLAN
Universal Admin Mode:	Disabled
Security :	No Security
Role in Radio Network :	Access Point
Optimize Radio Network :	Default
Aironet Extensions:	Enable
Channel:	Dynamic Frequency Selection
Power:	3
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Step 34** At the bottom of the page, click **Apply** and **OK** to popup.

**Step 35** Navigate back to the Home Menu and notice that the 5GHz radio is up (SSID enabled).

**Step 36** Click the **Save Configuration** at the top of the screen (again, saves to flash).

#### Verify the Configuration Changes

Here you will view the configuration from within the GUI and note the bridged interfaces.

**Step 37** Navigate to **Software > System configuration** and click on the hyperlink: **config.txt**. This is the same as the **show run** command.

<b>System Software</b>  <b>Software upgrade</b>  <b>System configuration</b>	<pre> channel 5100 station-role root no dot11 extension aironet bridge-group 1 bridge-group 1 subscriber-loop-control bridge-group 1 spanning-disabled bridge-group 1 block-unknown-source no bridge-group 1 source-learning no bridge-group 1 unicast-flooding ! interface Dot11Radio1.14 encapsulation dot1Q 14 bridge-group 14 bridge-group 14 subscriber-loop-control bridge-group 14 spanning-disabled bridge-group 14 block-unknown-source no bridge-group 14 source-learning no bridge-group 14 unicast-flooding ! interface GigabitEthernet0 no ip address duplex auto speed auto bridge-group 1 bridge-group 1 spanning-disabled no bridge-group 1 source-learning ! interface GigabitEthernet0.14 encapsulation dot1Q 14 bridge-group 14 bridge-group 14 spanning-disabled no bridge-group 14 source-learning ! interface EVII mac-address f07f.06cd.22c4 ip address 192.168.12.5 255.255.255.0 ipv6 enable </pre>
--	--

**Step 38** Scroll through the Configuration to see you SSID and Interface settings from the CLI perspective.

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- Changed the switch port for the AP to reflect the native Vlan 12 and the Client Vlan 14.
- Performed the Easy Setup to change the hostname and set static IP address (192.168.12.5).
- Enabled the 5GHz radio.
- Set the SSID, VLAN (x4 for client), broadcast, power and channel settings.
- Verified the Local-MAC configuration.

## **Task 2: Test Client Access to the Autonomous AP**

### ***Activity Procedure***

This this task, you will test the client access to the autonomous AP.

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

Complete these steps:

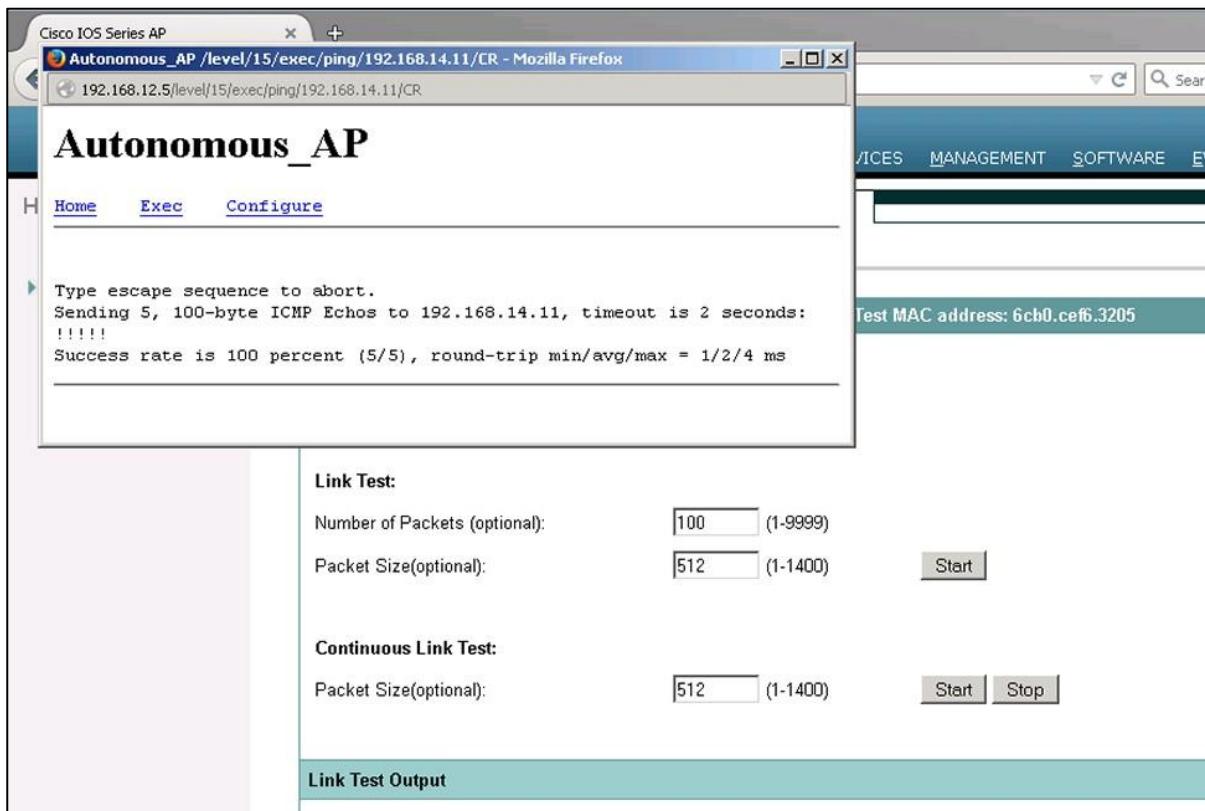
- Step 1** Connect to the Client PC and then to the **Podx\_Auto WLAN**.
- Step 2** Verify your IP address (192.168.14.0/24 network) and ping the default gateway.
- Step 3** Connect to the **Admin PC** and open a browser (FF) to the Autonomous\_AP (192.168.12.5) and login.
- Step 4** Click on the **Association** menu. Review the connected clients and their IP addresses.

Association					
Clients: 1		Infrastructure clients: 0			
View: <input checked="" type="checkbox"/> Client <input type="checkbox"/> Infrastructure client		<input type="button" value="Apply"/>			
Radio0-802.11N <sup>2.4GHz</sup>					
Radio1-802.11AC <sup>5GHz</sup>					
SSID Pod1_Auto :					
Device Type	Name	IPv4 Address	IPv6 Address		
unknown	NONE	192.168.14.11	2001:DB8:1:E:7992:6662:2185:6F1E		
			<a href="#">6cb0.ceff.3205</a>		
			Associated		
			self		
			14		

- Step 5** Click on the MAC address of the client and view client statistics from the **STATISTICS** tab.

STATISTICS	PING/LINK TEST			
Hostname Autonomous_AP	Autonomous_AP uptime is 21 hours, 3 minutes			
Association: Station View- Client				
Station Information and Status				
MAC Address	6cb0.ceff.3205	Name		
IP Address	192.168.14.11	Class		
Device	unknown	Software Version		
CCX Version	NONE	Client MFP		
State	Associated	Parent		
SSID	Pod1_Auto	VLAN		
Hops To Infrastructure	1	Communication Over Interface		
		Radio1-802.11AC <sup>5GHz</sup>		

- Step 6** Select the **PING/LINK TEST** tab. It is here that you can run a Ping test to the client or a Link Test (radio link performance).
- Step 7** Click on **Start** beside the **Begin Ping Test**.
- Step 8** A popup window will display, click on **CR** button where you should get a successful ping.



**Step 9** Close the popup window.

**Step 10** On the Client PC, disconnect from the **Podx\_Auto** WLAN.

**Step 11** Go back to the browser for the Auto\_AP and notice that the Client is no longer associated (menu - Association).

## Activity Verification

You have successfully completed this task when you attain this result:

- Connect the client to the Podx\_Auto WLAN.
- Got an IP from the correct network and could ping the default gateway.
- Pinged the client from the Auto\_AP.
- Verified that when the client disconnected from the WLAN, they were also disassociated from the Auto\_AP.

# **Hardware Lab 11: Configure Security on an Autonomous AP WLAN Deployment**

---

## **Overview**

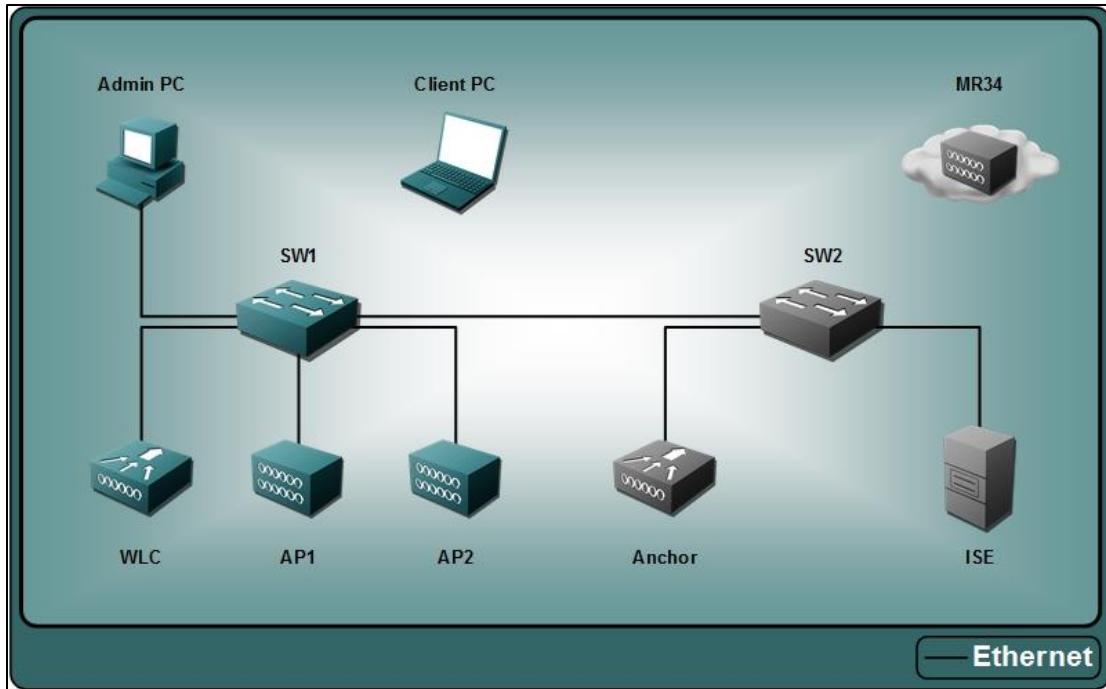
In this activity, you configure security for an autonomous AP WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Implement PSK authentication.
- Implement RADIUS authentication.

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 3650 IOS-XE Switch
- Pod 2504 WLC
- AP 3700i (Autonomous)

### VLANs and IP Ranges

#### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
WLC 2504	192.168.11.5	admin	Cisco123	
Pod 3650 Switch	192.168.11.254	admin	cisco	cisco
ISE (RADIUS)	192.168.11.21	admin	1234QWer	
Autonomous AP	192.168.12.5	cisco	Cisco	

## Task 1: Implement PSK Authentication on an Autonomous AP

### ***Activity Procedure***

In this task, you will implement PSK authentication on the autonomous AP and test client access.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

#### **Set the Encryption for the VLAN**

Before setting the authentication type, the encryption must first be configured for the VLAN.

Complete these steps:

- Step 1** Connect to Admin PC and open a browser (IE) and connect to the Auto\_AP (192.168.12.5) and login (**cisco/Cisco**).
- Step 2** Navigate to **Security > Encryption Manager** and take notice at the top of the page that that **Vlan 14** is selected (created from Easy Setup).  
(It may be already configured from the previous lab steps.)
- Step 3** Under the Encryption Modes, select the **Cipher** radio button and choose **AES CCMP** from the dropdown.

**Step 4** At the bottom of the page, click **Apply** and **OK** to popup.

---

**Note** Encryption is set by VLAN and Authentication is set by SSID.

---

#### Modify Authentication for the WLAN (SSID) to use PSK

You could create a new SSID here, but instead; you will modify the SSID that you initially setup earlier.

**Step 5** Navigate to **Security > SSID Manager** and click on the **Podx\_Auto** under the Current SSID List.

**Step 6** Review the following (configured in Easy Setup and can be modified here) in the SSID Current List section (top):

- SSID Podx\_Auto links to Vlan 14
- Band Select can be enabled here (and feature must be turned on under Services)
- Radio selection for the SSID is 5 GHz, but 2.4 GHz could be added

**Step 7** Review the following (again, done in Easy Setup, ) in the Client Authentication Settings section, verify that the Current Authentication is **Open Authentication**.

The screenshot shows the Cisco Wireless LAN Controller (WLC) Global SSID Manager interface. The left sidebar under 'Security' includes links for Admin Access, Encryption Manager, **SSID Manager**, Server Manager, AP Authentication, Intrusion Detection, Local RADIUS Server, and Advance Security. The main panel has a 'Hostname Autonomous\_AP' header and a 'Autonomous\_AP' save button. It displays the 'SSID Properties' section for the 'Current SSID List'. A dropdown menu shows '< NEW >' and 'Pod1\_Auto'. To the right, the 'SSID' field is set to 'Pod1\_Auto', 'VLAN' to '14', and 'Band-Select' is checked. Under 'Client Authentication Settings', 'Methods Accepted' includes 'Open Authentication' (checked), 'Web Authentication' (unchecked), and 'Shared Authentication' (unchecked). The 'Interface' section shows 'Radio1-802.11AC5GHz' is selected.

**Step 8** Scroll down to the section for Client Authenticated Key Management and make the following changes:

- Key Management: **Mandatory**
- Enable WPA: **Checked** and choose **WPAv2** from drop down
- WPA Pre-shared Key: **Cisco123**
- Under the section for IDS Client MFP, make the following change:
  - Enable Client MFP on this SSID: **Unchecked**

---

**Note** This disables the use of Management Frame Protection for this WLAN.

---

**Step 9** Scroll down and click on the first **Apply** that you see (right above Guest Mode Infrastructure SSID Settings section).

## Client Authenticated Key Management

Key Management:	<input type="button" value="Mandatory"/>	<input type="checkbox"/> CCKM	<input checked="" type="checkbox"/> Enable WPA	<input type="button" value="WPAv2"/>
WPA Pre-shared Key:	XXXXXXXXXXXXXX			<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal
11w Configuration:	<input type="button" value="Optional"/>			
11w Association-comeback:	<input type="text" value="1000"/> (1000-20000)			
11w Saquery-retry:	<input type="text" value="100"/> (100-500)			

## IDS Client MFP

<input type="checkbox"/> Enable Client MFP on this SSID:	<input type="button" value="&lt;NONE &gt;"/>
--	--

- Note** In the Autonomous GUI, you must click apply on the section that you are modifying or risk losing your work if navigate to another section without applying.

**Step 10** Click **Save Configuration**.

**Step 11** Review the Security settings by navigating to the Security menu. The summary screen will display the current encryption and authentication settings.

## Test PSK Authentication with the Client

**Step 12** Connect to the Client PC and connect to the **Podx\_Auto** WLAN.

**Step 13** Enter your Pre-shared Key when prompted (**Cisco123**).

**Step 14** Verify your IP address (192.168.14.0/24 network) and ping the default gateway.

**Step 15** Connect to the Admin PC and open a browser (FF) to the Autonomous\_AP (192.168.12.5) and login.

**Step 16** Click on the **Association** menu and select the MAC address of the client. Notice that you see that the client is using WPAv2 PSK with AES-CMP Encryption.

Association: Station View- Client				
Station Information and Status				
MAC Address	6cb0.cefb.3205	Name		NONE
IP Address	192.168.14.11	Class		unknown
Device	unknown	Software Version		NONE
CCX Version	NONE	Client MFP		Off
State	Associated	Parent		self
SSID	Pod1_Auto	VLAN		14
Hops To Infrastructure	1	Communication Over Interface		Radio1-802.11AC <sup>5GHz</sup>
Clients Associated	0	Repeaters Associated		0
Key Mgmt type	WPAv2 PSK	Encryption		AES-CCMP
Current Rate (Mb/sec)	a8.2	Capability		WMM 11h

**Step 17** Click on the **PING/LINK TEST** tab and ping the client.

**Step 18** On the Client PC, disconnect from the **Podx\_Auto WLAN**.

**Step 19** Go back to the browser for the Auto\_AP and notice that the Client is no longer associated (menu - Association).

## **Activity Verification**

You have successfully completed this task when you attain this result:

- Modified the Podx\_Auto WLAN to use WPAv2 PSK with AES-CCMP.
- Connected the client to the Podx\_Auto WLAN with the Pre-Shared Key.
- Got an IP from the correct network and could ping the default gateway.
- Verified the client authentication and encryption from the AP GUI.
- Pinged the client from the Auto\_AP.
- Verified that when the client disconnected from the WLAN, they were also disassociated from the Auto\_AP.

## **Task 2: Implement RADIUS Authentication on an Autonomous AP**

### **Activity Procedure**

In this task, you will implement RADIUS authentication using PEAP on the autonomous AP and test client access.

---

**Note**

The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

### **Configure ISE for the Autonomous AP**

Just like you would do for a WLC with a centralized AP, the autonomous AP will need to use ISE for client authentication. Therefore, ISE must know about the AP and have client credentials.

Complete these steps:

**Step 1** On the Admin PC, open browser or tab (using Firefox) to access ISE (192.168.11.21) and confirm the Security Exceptions and login (**admin/1234QWer**).

**Step 2** Navigate to **Administration > Network Resources > Network Devices** and click **Add**. You need to make a connection from ISE to the Auto\_AP. Enter the following:

- Name: **Auto\_AP**
- IP Address: **192.168.12.5 / 32**
- Check Authentication Settings: Shared Secret: **Cisco123**
- Click **Submit**

**Step 3** Verify new entry is correct. There should already be a **poduser** created from a previous lab, so if it's gone, create a new user (**Administration Identity Management > Identities > Users**).

## Configure the Autonomous AP for ISE

**Step 4** Navigate to **Security > Server Manager** and make the following changes under **Corporate Servers** (mid panel):

- IP Version: **IPV4**
- Server Name: **ISE**
- Server: **192.168.11.21**
- Shared Secret: **Cisco123**
- Authentication Port: **1812**
- Accounting Port: **1813**
- Click the **Apply** in this section and **OK** to popup.

The screenshot shows the 'Corporate Servers' configuration interface. In the 'Current Server List' panel, there is a dropdown menu set to 'RADIUS'. Below it, a table lists a single server entry:

<NEW>	IP Version:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
	Server Name:	ISE
	Server:	192.168.11.21 (Hostname or IP Address)
	Shared Secret:	*****

Below the table, there are optional port settings: 'Authentication Port (optional)' set to 1812 (0-65535) and 'Accounting Port (optional)' set to 1813 (0-65535). At the bottom right are 'Apply' and 'Cancel' buttons.

**Step 5** Make the following changes under **Default Server Priorities** (bottom panel):

- EAP Authentication: **ISE** (from drop down)
- Accounting: **ISE** (from drop down)
- Click the **Apply** in this section and **OK** to popup.

The screenshot shows the 'Default Server Priorities' configuration interface. It contains several sections for different authentication methods:

- EAP Authentication:** Priority 1: ISE, Priority 2: <NONE>, Priority 3: <NONE>.
- MAC Authentication:** Priority 1: <NONE>, Priority 2: <NONE>, Priority 3: <NONE>.
- Accounting:** Priority 1: ISE, Priority 2: <NONE>, Priority 3: <NONE>.
- Admin Authentication (RADIUS):** Priority 1: <NONE>, Priority 2: <NONE>, Priority 3: <NONE>.
- Admin Authentication (TACACS+):** Priority 1: <NONE>, Priority 2: <NONE>, Priority 3: <NONE>.

At the bottom right are 'Apply' and 'Cancel' buttons.

---

<b>Note</b>	If no other servers are defined for Priority in the SSID Manager, then the AP will use the Default Servers.
-------------	---

---

## Modify the SSID for RADIUS

Previously, you used this SSID for PSK. Now you will remove the PSK and make it RADIUS.

- Step 6** Navigate to **Security > SSID Manager** and select the **Podx\_Auto** under the Current SSID List.
- Step 7** Scroll down to the section for **Client Authentication Settings** and set the **Open Authentication** option as **checked** and set to: **with EAP**.

Client Authentication Settings	
<b>Methods Accepted:</b>	
<input checked="" type="checkbox"/> Open Authentication:	with EAP
<input type="checkbox"/> Web Authentication	Web Pass
<input type="checkbox"/> Shared Authentication:	< NO ADDITION >
<input type="checkbox"/> Network EAP:	< NO ADDITION >

---

<b>Note</b>	Notice that under the Default Server Priorities that an EAP Authentication server was not chosen. The system will use the default server configuration that you did earlier (configuring Autonomous AP for ISE). If you want to be sure, you could choose the “ISE” server as Priority 1.
-------------	---

---

- Step 8** Scroll down to the section for Client Authenticated Key Management and make the following changes:

- WPA Pre-shared Key: delete key (**empty**)
- Scroll down and click on the first **Apply** that you see (right above Guest Mode Infrastructure SSID Settings section). You can go to the **Security Summary** screen to verify your settings.

Client Authenticated Key Management	
<b>Key Management:</b>	Mandatory
	<input type="checkbox"/> CCKM
	<input checked="" type="checkbox"/> Enable WPA
	WPAv2
<b>WPA Pre-shared Key:</b>	
<b>11w Configuration:</b>	<input type="radio"/> Optional <input type="radio"/> Required
<b>11w Association-callback:</b>	1000 (1000-20000)
<b>11w Saquery-retry:</b>	100 (100-500)

## Test RADIUS with the Client

Here you will test Remote EAP-PEAP at the client as you have done in previous labs. That means that a PEAP profile must be created.

- Step 9** Connect to Client PC and create a Remote EAP profile like you did in previous labs.
- Step 10** Connect and enter your ISE credentials (**poduser/Cisco123**), verify IP connectivity, view the Client in AP Web GUI and see authentication.
- Step 11** Disconnect client connection when finished.

## Activity Verification

You have successfully completed this task when you attain this result:

- Modified the Podx\_Auto WLAN to use Remote EAP-PEAP.
- Connected the client to the Podx\_Auto WLAN with remote user account (from ISE).
- Got an IP from the correct network and could ping the default gateway.
- Verified the client authentication and encryption from the AP GUI.
- Pinged the client from the Auto\_AP.
- Verified that when the client disconnected from the WLAN, they were also disassociated from the Auto\_AP.

## Task 3: Autonomous Lab Cleanup

### Activity Procedure

This task, you will disable the Autonomous AP radios to reduce RF traffic for subsequent labs.

---

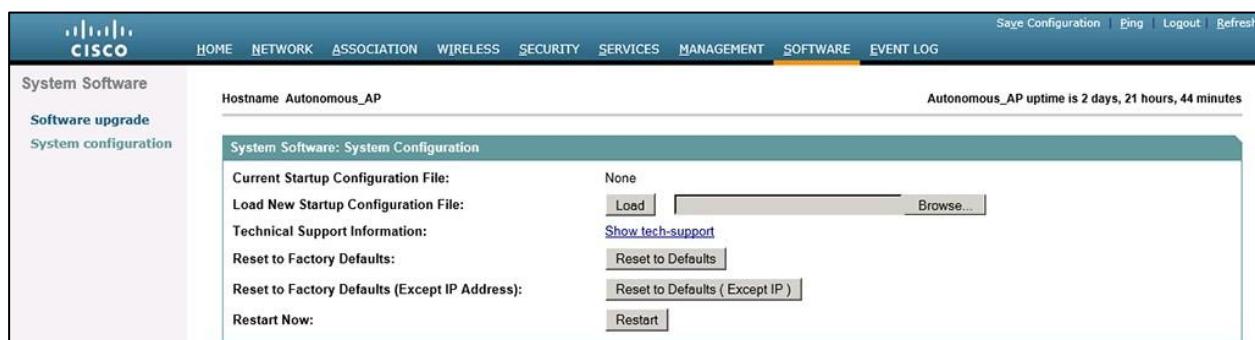
<b>Note</b>	The lower case "x" in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

### Connect to the Autonomous AP

Complete these steps:

- Step 1** Connect to Admin PC and open a browser (FF) and connect to the Auto\_AP (192.168.12.5) and login (**cisco/Cisco**).
- Step 2** Navigate to **Software > System configuration** and click on **Reset to Defaults** (and **OK** to popup).



The screenshot shows the Cisco Web UI interface. At the top, there's a navigation bar with links for HOME, NETWORK, ASSOCIATION, WIRELESS, SECURITY, SERVICES, MANAGEMENT, SOFTWARE (which is highlighted in orange), and EVENT LOG. On the left, a sidebar has links for System Software, Software upgrade, and System configuration. The main content area shows the following details:

- Hostname:** Autonomous\_AP
- Uptime:** Autonomous\_AP uptime is 2 days, 21 hours, 44 minutes
- System Software:** System Configuration
- Current Startup Configuration File:** None
- Load New Startup Configuration File:** Input field and Browse... button
- Technical Support Information:** Show tech-support link
- Reset to Factory Defaults:** Reset to Defaults button
- Reset to Factory Defaults (Except IP Address):** Reset to Defaults ( Except IP ) button
- Restart Now:** Restart button

**Step 3** AP will erase configuration and restart.

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- Defaulted the AP to factory settings



# **Hardware Lab 12: Configure Security on a Cloud WLAN Deployment**

---

## **Overview**

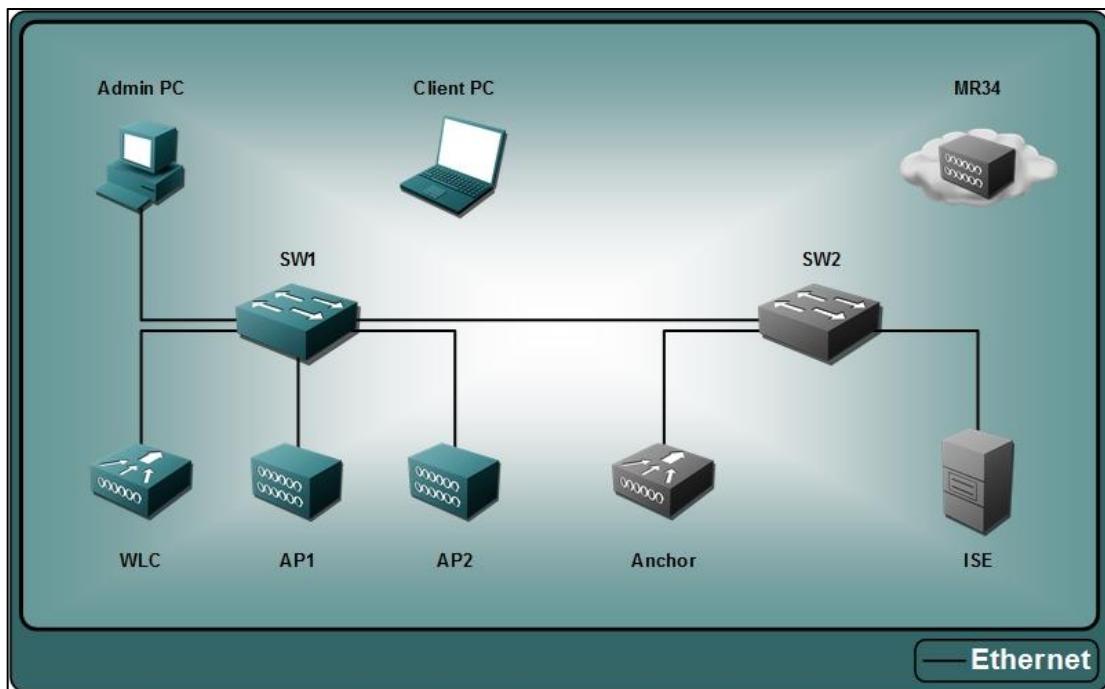
In this activity, you configure security for a Cloud WLAN deployment.

After completing this activity, you will be able to meet these objectives:

- Implement PSK authentication.
- Implement Local EAP-PEAP authentication.
- Implement Webauth authentication.
- Disable the Cloud SSIDs.

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Meraki MR-34

### VLANs and IP Ranges

#### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password
Meraki AP	172.16.0.30	see below	see below

## Meraki SSIDs and Admins

### Device Information

Pod	Starting SSID	Local Admin User	Password	Created User	Password
Pod1	Pod1	meraki@example.com	Cisco123	pod1.meraki@flane.de	Cisco123
Pod2	Pod2	meraki@example.com	Cisco123	pod2.meraki@flane.de	Cisco123
Pod3	Pod3	meraki@example.com	Cisco123	pod3.meraki@flane.de	Cisco123
...					
Pod24	Pod24	meraki@example.com	Cisco123	pod24.meraki@flane.de	Cisco123

# Task 1: Implement PSK Authentication on a Cloud WLAN Deployment

## Activity Procedure

In this task, you will implement PSK authentication on a Cloud WLAN deployment and test client access.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

### Access the Cisco Meraki Dashboard

Multiple users can concurrently use the Dashboard.

Complete these steps:

- Step 1** Use your local PC for Meraki Dashboard access and open a browser and type in the URL:  
<http://dashboard.meraki.com>.
- Step 2** Enter your email/password (podox.meraki@flane.de / **Cisco123**).
- Step 3** On the left side, you will have three menus: **Network-wide**, **Wireless** and **Help**.

---

**Note** Cloud based “Organizations” can have many networks and therefore assign admin access at that level. That is the level that you have in class. If you were a higher level, you would see “Organization” as a menu choice. Please, out of respect for your classmates, do not make any changes other than those specified for your WLAN.

---

### Familiarize Yourself with the Dashboard Interface

- Step 4** Hover your cursor over the **Network-wide** and choose **Monitor > Summary Reports**. From here you will see an overview of the WLAN usage in different categories.
- Step 5** Hover your cursor over the **Wireless** and choose **Monitor > Access Points** and click on the name of the access point, **MR34-L-X** (where L is your lab number as stated in the Student Notes). This will show the information for one access point in the network (traffic, SSIDs, VLANs and etc.).

## Configure the SSID for PSK

- Step 6** Hover your cursor over the Wireless and choose **Configure > SSIDs** and select **Show all my SSIDs** at the top.

Pod1	Pod2	Pod3	Pod4	Pod5	Pod6	Pod7	Pod8
enabled ▾	disabled ▾	disabled ▾	disabled ▾	disabled ▾	disabled ▾	disabled ▾	disabled ▾
<a href="#">rename</a>							
<a href="#">edit settings</a>							
WPA2-PSK	Open						
None							
unlimited Local LAN	unlimited Meraki DHCP						
n/a	no						
no							
n/a							
Disabled							
no							
Modern	n/a						

**Step 7** Underneath the SSID for your pod (Podx), click on **rename** (to change SSID) and set the name to: **Podxmr\_PSK** (x=Pod#).

**Step 8** At the bottom of the screen, click **Save Changes** and verify that the SSID name changed.

**Step 9** Underneath the SSID for your pod click on **edit settings** and change the following on this screen:

### Access control

SSID: Pod1mr\_PSK (disabled)

#### Network access

Association requirements	<input type="radio"/> Open (no encryption) Any user can associate
	<input checked="" type="radio"/> Pre-shared key with <input type="button" value="WPA2 ▼"/> Users must enter this key to associate: <input type="text" value="*****"/> <a href="#">Show key</a>
	<input type="radio"/> MAC-based access control (no encryption) RADIUS server is queried at association time
	<input type="radio"/> WPA2-Enterprise with <input type="button" value="Meraki authentication ▼"/> User credentials are validated with 802.1X at association time
WPA encryption mode	<input type="button" value="WPA2 only ▼"/>
Splash page	<input checked="" type="radio"/> None (direct access) Users can access the network as soon as they associate
	<input type="radio"/> Click-through Users must view and acknowledge your splash page before being allowed on the network
	<input type="radio"/> Sign-on with <input type="button" value="Meraki authentication ▼"/> Users must enter a username and password before being allowed on the network

- Network Access - Association requirements: **Pre-shared key with WPA2 - Key: Cisco123**
  - Network Access – WPA encryption mode: **WPA2 only**
  - Network Access – Splash Page: **None**
  - Addressing and traffic – Client IP assignment: **NAT mode**
- Note:** Notice the other options for VLAN tagging and filtering.
- Wireless options – Band selection: **5 GHz band only**
  - Wireless options – Minimum bitrate: 12Mbps
  - **Click Save Changes**

#### Addressing and traffic

Client IP assignment	<input checked="" type="radio"/> NAT mode: Use Meraki DHCP Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the <a href="#">SSID firewall settings</a> permit.
	<input type="radio"/> Bridge mode: Make clients part of the LAN Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras.
	<input type="radio"/> Layer 3 roaming Clients receive DHCP leases from the LAN or use static IPs as in bridge mode. If they roam between APs their traffic will be forwarded to an AP on the same subnet they originally joined, so they will keep the same IP address.
	<input type="radio"/> Layer 3 roaming with a concentrator Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.
	<input type="radio"/> VPN: tunnel data to a concentrator Meraki devices send traffic over a secure tunnel to an MX or VM concentrator. Note: VPN and Layer 3 roaming with concentrator require an MX or VM concentrator. To use them, <a href="#">add an MX</a> , or <a href="#">create a concentrator</a> .
VLAN tagging	<input type="button" value="Bridge mode and layer 3 roaming only"/>
	<input type="button" value="Don't use VLAN tagging ▼"/>
Content filtering	<input type="button" value="NAT mode only"/>
	<input type="button" value="Don't filter content ▼"/>
Bonjour forwarding	<input type="button" value="Bridge mode and layer 3 roaming only"/>
	<input type="button" value="Disable Bonjour Forwarding ▼"/>
Wireless options	
Band selection	<input type="radio"/> Dual band operation (2.4 GHz and 5 GHz)
	<input checked="" type="radio"/> 5 GHz band only 5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it.
	<input type="radio"/> Dual band operation with Band Steering Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.
Minimum bitrate (Mbps)	<input type="button" value="Lower Density"/>  <input type="button" value="Higher Density"/>

**Step 10** Verify that the changes were made.

- Step 11** Hover your cursor over the **Wireless** and choose **Configure > SSIDs** and on **Show all my SSIDs** at the top.
- Step 12** Underneath the SSID for your pod (**Podxmr\_PSK**) , change the first drop down to: **enabled**.
- Step 13** At the bottom of the screen, click **Save Changes** and verify that the SSID is now enabled.
- Step 14** Hover your cursor over the **Wireless** and choose **Configure > SSID availability** and select your SSID from the drop down (**Podxmr\_PSK**) and verify that your SSID is **Visible** and **Enabled on all APs**.
- Step 15** **Save Changes** if needed.

### Test PSK Authentication with the Client

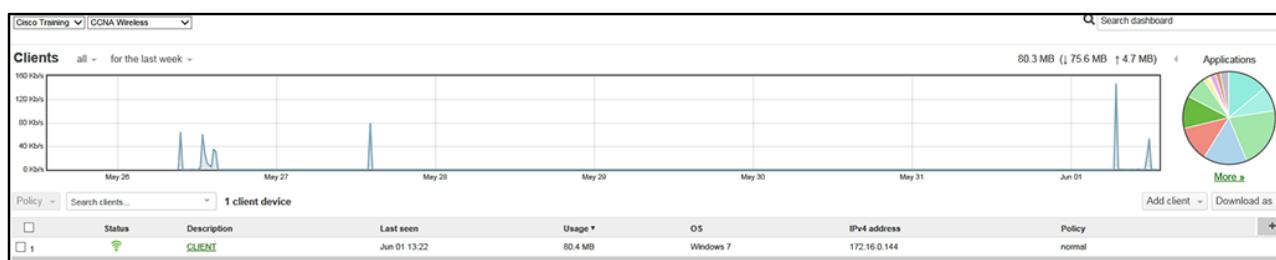
- Step 16** Connect to the Client PC and then to the **Podxmr\_PSK WLAN**.

---

<b>Note</b>	It may take 2-3 minutes for SSID changes to propagate to the AP, so your SSID may not be there right away.
-------------	--

---

- Step 17** Enter your Pre-shared Key when prompted (**Cisco123**).
- Step 18** Verify your IP address (10.0.0.0/24 backbone network per setting on Meraki for Bridge Mode) and ping the default gateway.
- Step 19** On your local PC, open a browser to the Meraki Dashboard (<http://dashboard.meraki.com>).
- Step 20** Hover your cursor over the **Network-wide** and choose **Monitor > Clients** and look for your client IP address (all clients will be **CLIENT**). Notice that the client's OS has been identified (Windows 7).



### Modify Client Name

One of the Meraki features is the ability to rename a client for easy identification.

- Step 21** Click on your client name (for the correct IP address). At the **Clients > Client** screen, click on the “pencil icon” beside your client name to edit the name to **Podx\_Client**.
- Step 22** Click **Save**.

## Clients > Pod1\_Client

Status:	 associated since Jun 01 13:22
SSID:	Pod1_PSK
Access point:	<u>MR34</u>
Splash:	N/A
Signal:	 58dB (channel 44)
Device type:	Netgear Windows 7 
Capabilities:	802.11ac - 2.4 and 5 GHz <a href="#">details »</a> <a href="#">event log</a>   <a href="#">packet capture</a>   <a href="#">add note</a>

**Step 23** Go back to **Network-wide** and choose **Monitor>Clients**. Notice that your client has a name (Description for your client) and that the Meraki has identified your device type and OS.

### View the Event Log for the Client

**Step 24** Click on your client name (**Podx\_Client**) and look at the **event log** (under Capabilities) at the top left of the screen for this client to see clients connectivity information.

**Step 25** On the Client PC, disconnect from the **Podxmr\_PSK** WLAN and verify from the Network Sharing Center that there are no profiles saved.

**Step 26** Go back to the browser for the Meraki Dashboard and go to **Network-wide** and choose **Monitor > Clients**. Your client will still be there, but if you click on the client (Podx\_Client), you will go to the next screen and see that they are no longer associated. You will also see when they were last seen (may take a minute).

If you still have time, go back to the Dashboard and see the different aspects of objects that you can monitor (don't make any configuration changes outside of the lab guide steps).

## **Activity Verification**

In the next few steps, you will ...

You have successfully completed this task when you attain this result:

- Modified the Podx WLAN to be Podxmr\_PSK and use WPA2 PSK.
- Modified the WLAN to use only 5 GHz radio and Local LAN (Bridge).
- Disabled the 802.11b legacy data rates.
- Connected the client to the Podxmr\_PSK WLAN with the Pre-Shared Key.
- Got an IP from the correct network and could ping the default gateway.
- Verified the client connection from the Meraki Dashboard.
- Verified that when the client disconnected from the WLAN, that their connection history was still on Meraki Dashboard.

# Task 2: Implement Local EAP-PEAP on a Cloud WLAN Deployment

## Activity Procedure

In this task, you will implement Local EAP-PEAP authentication on a Cloud WLAN deployment and test client access. The Meraki can provide RADIUS by itself. The Meraki can also use external RADIUS servers.

---

<b>Note</b>	The lower case “x” in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

### Modify the SSID for Local EAP-PEAP

Due to the limited number of SSIDs, you will just rename the old SSID.

Complete these steps:

- Step 1** Use your local PC for Meraki Dashboard access and open a browser and type in the URL: <http://dashboard.meraki.com>.
- Step 2** Enter your email/password (podx.meraki@flane.de / **Cisco123**) and navigate to **Wireless > SSIDs**.
- Step 3** Click on **Show all my SSIDs** and rename the Podxmr\_PSK to **Podxmr\_EAP**.
- Step 4** **Save Changes**.
- Step 5** On the left side, go to **Wireless > SSIDs** and select **Show All SSIDs**.
- Step 6** Underneath your SSID (Podxmr\_EAP) click on **edit settings** and change the following on the Access Control screen:
  - Network Access - Association requirements: **WPA2-Enterprise - with: Meraki authentication**
  - Click **Save Changes**

### Access control

SSID: Pod1mr\_EAP

#### Network access

Association requirements	<input type="radio"/> Open (no encryption) Any user can associate
	<input type="radio"/> Pre-shared key with WPA2 Users must enter a passphrase to associate
	<input type="radio"/> MAC-based access control (no encryption) RADIUS server is queried at association time
	<input checked="" type="radio"/> WPA2-Enterprise with Meraki authentication User credentials are validated with 802.1X at association time
WPA encryption mode	WPA2 only
802.11r	Disabled

### Create a Local User

You will create a local user for the Meraki Authentication (802.1x, Local EAP-PEAP).

**Step 7** Navigate to Network-wide > Users and verify that the SSID is **Podxmr\_EAP** from the drop down.

**Step 8** Click on **Add new user** (right side) and enter the following, (where x=pod#):

- Name: **podx**
- Email: **podx@domain.com**
- Password: **Cisco123**
- Email new password to user: **Unchecked**
- Authorized: **Yes**
- Expires: **Never**
- **Create User**
- **Save Changes**

**Create user**

Account type: Guest

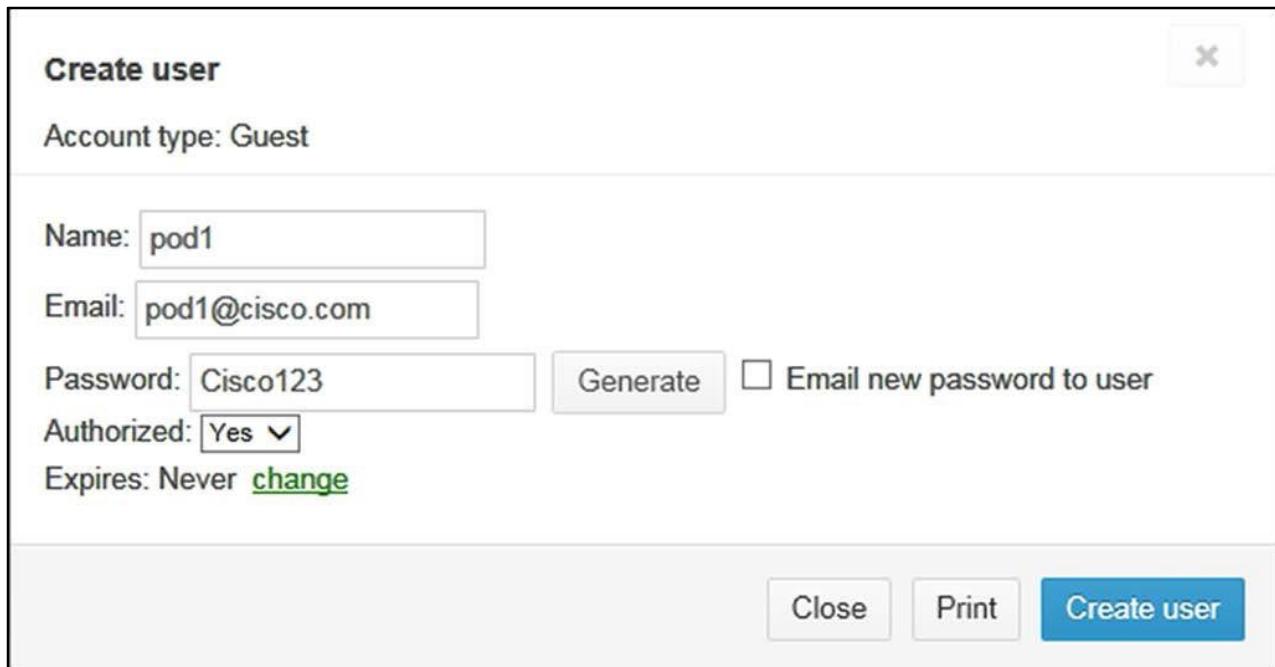
Name:

Email:

Password:    Email new password to user

Authorized:

Expires: Never [change](#)



**Step 9** Verify that the user is authorized (“Authorized for SSID”) and Admin that authorized them.

#### Test Local EAP-PEAP Authentication with the Client

**Step 10** Connect to the Client PC and then to the **Podxmr\_EAP** network (Uncheck the box for “Connect automatically”, you don’t want to create a profile).

**Step 11** At the Windows Security pop-up screen, enter **podx@domain.com** on the first line and **Cisco123** on the second line and click **OK**.

**Step 12** At the next Windows Security Alert pop-up, click the **Connect** button to continue. Normally you would not accept untrusted certificates or certificate authorities, but in this lab example the risk is controlled.

---

**Note**

You could have created a manual profile, but the test does not require it.

---

**Step 13** Verify your IP address (10.0.0.0/8 network) and ping the default gateway.

**Step 14** On your local PC, open a browser to the Meraki Dashboard (<http://dashboard.meraki.com>).

**Step 15** Navigate to **Network-wide** and choose **Monitor > Clients** and take note that your client has a name (from the last task). Click on your client name (**Podx\_Client**). Notice that the User is: **podx@domain.com (802.1x login)**.

## [Clients](#) > **Pod1\_Client**

Status:	 associated since Jun 01 13:56
SSID:	Pod1_EAP
Access point:	<a href="#">MR34</a>
Splash:	N/A
Signal:	 58dB (channel 44)
User:	pod1@domain.com (802.1X login)
Device type:	Netgear Windows 7 
Capabilities:	802.11ac - 2.4 and 5 GHz <a href="#">details »</a> <a href="#">event log</a>   <a href="#">packet capture</a>   <a href="#">add note</a>

**Step 16** You may also look at the **event log** (under Capabilities) at the top left of the screen for this client to see clients connectivity information.

**Step 17** On the Client PC, disconnect from the **Podxmr\_EAP** WLAN and verify from the Network Sharing Center that there are no profiles saved.

**Step 18** Go back to the browser for the Cloud Management and go to **Network-wide** and choose **Monitor > Clients**. Your client will still be there, but if you click on the client (Podx\_Client), you will go to the next screen and see that they are no longer associated. You will also see when they were last seen (may take a minute).

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Modified the Podxmr\_PSK WLAN to be Podxmr\_EAP and use WPA2 Enterprise.
- Connected the client to the Podxmr\_EAP WLAN with the local user credentials.
- Got an IP from the correct network and could ping the default gateway.
- Verified the client connection from the Meraki Dashboard.
- Verified that when the client disconnected from the WLAN, that their connection history was still on the Meraki Dashboard.

# Task 3: Implement WebAuth on a Cloud WLAN Deployment

## Activity Procedure

In this task, you will implement WebAuth authentication on a Cloud WLAN deployment and test client access.

---

<b>Note</b>	The lower case “x” in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

### Modify the SSID for Local EAP-PEAP

Complete these steps:

- Step 1** Use your local PC for Meraki Dashboard access and open a browser and type in the URL: <http://dashboard.meraki.com>. Enter your email/password (podx.meraki@flane.de / Cisco123).
- Step 2** Navigate to **Wireless > SSIDs** and select **Show All SSIDs**.
- Step 3** Rename the Podxmrx\_EAP to **Podxmrx\_WEB** and **Save Changes**.
- Step 4** On the left side, go to **Wireless > SSIDs** and select **Show all my SSIDs**.
- Step 5** Underneath your SSID (Podxmrx\_WEB), click on **edit settings** and change the following on the Access Control screen:
  - Network Access - Association requirements: **Open**
  - Network Access – Splash page: **Click-through**
  - Network Access – Captive port strength: **Block all access until sign-on is complete**
  - Click **Save Changes**

Splash page	<input type="radio"/> None (direct access) Users can access the network as soon as they associate <input checked="" type="radio"/> Click-through Users must view and acknowledge your splash page before being allowed on the network <input type="radio"/> Sign-on with <a href="#">Meraki authentication</a> Users must enter a username and password before being allowed on the network <input type="radio"/> Sign-on with SMS Authentication <small>BETA</small> Users enter a mobile phone number and receive an authorization code via SMS. After a trial period of 25 texts, you will need to connect with your Twilio account on the <a href="#">Network-wide settings</a> page. <input type="radio"/> Billing (paid access) Users choose from various pay-for-access options, or an optional free tier <input type="radio"/> Systems Manager Sentry enrollment <small>?</small> Only devices with Systems Manager can access this network
Network access control <small>?</small>	<a href="#">Disabled: do not check clients for antivirus software</a>
Assign group policies by device type <small>?</small>	<a href="#">Disabled: do not assign group policies automatically</a>
Captive portal strength <small>?</small>	<a href="#">Block all access until sign-on is complete</a>
Walled garden <small>?</small>	<a href="#">Walled garden is disabled</a>

**Step 6** Connect to the Client PC and then to the **Podxmr\_WEB** network.

**Step 7** Verify your IP address (10.0.0.0/8 network) and ping the default gateway (should fail – not authenticated yet).

**Step 8** Open a browser (FF) and type the url of <http://www.cisco.com> and **Enter**. On the welcome screen, click on: **Continue to the internet**.

# Welcome to PodXmr\_WEB

Continue to the Internet

POWERED BY



- Step 9** Now browse to <http://www.cisco.com> and ping the default gateway. This should work now, because the client is authenticated.
- Step 10** On your local PC, and open a browser to the Meraki Dashboard (<http://dashboard.meraki.com>).
- Step 11** Navigate to **Network-wide** and choose **Monitor > Clients** and click on your client name (Podx\_Client). Notice under the client info that Splash is: **Click-through splash**.

## [Clients](#) > **Pod1\_Client**

Status:	 associated since May 26 13:17
SSID:	<b>PodXmr_WEB</b>
Access point:	<u>MR34</u>
Splash:	Click-through splash ( <a href="#">revoke</a> ) Authorized 1 minute ago. Expires in 29 minutes.
Signal:	 60dB (channel 44)
Device type:	Netgear Windows 7 
Capabilities:	802.11ac - 2.4 and 5 GHz <a href="#">details »</a> <a href="#">event log</a>   <a href="#">packet capture</a>   <a href="#">add note</a>

**Note** Notice the word “revoke” beside the Splash info. Here you can click this and revoke the user’s credentials and force them to re-authenticate.

- Step 12** On the Client PC, disconnect from the **Podxmr\_WEB** WLAN and from the Network Sharing Center, delete any saved profiles.
- Step 13** Go back to the browser for the Meraki Dashboard and go to **Network-wide** and choose **Monitor > Clients** and click on your client to go to the **Clients** page.
- Step 14** Beside the word Splash (under your client info, on top left side), click on **Revoke**. The client must now re-authenticate (you must do this if you wish to re-test).

### **OPTIONAL - Modify Webauth for Sign-on Authentication (part 1 of 2)**

Here you configure for Guest Access, but require a username/password.

- Step 15** From your local PC, open a browser and type in the URL: <http://dashboard.meraki.com>.
- Step 16** Enter your email/password (podox.meraki@flane.de / Cisco123 , x=pod) and on the left, select **Wireless>SSIDs** and click on **Show all my SSIDs**.
- Step 17** Underneath your SSID (Podxmr\_WEB). click on **edit settings** and change the following on the Access Control screen:
- Network Access - Association requirements: **Open**
  - Network Access – Splash page: **Sign-on with Meraki Authentication**
  - Click **Save Changes**

Splash page	<input type="radio"/> None (direct access) Users can access the network as soon as they associate
	<input type="radio"/> Click-through Users must view and acknowledge your splash page before being allowed on the network
	<input checked="" type="radio"/> Sign-on with <input type="text" value="Meraki authentication"/> <input type="button" value="▼"/> Users must enter a username and password before being allowed on the network
	<input type="radio"/> Sign-on with SMS Authentication <small>BETA</small> Users enter a mobile phone number and receive an authorization code via SMS. After a trial period of 25 texts, you will need to connect with your Twilio account on the <a href="#">Network-wide settings</a> page.
	<input type="radio"/> Billing (paid access) Users choose from various pay-for-access options, or an optional free tier
	<input type="radio"/> Systems Manager Sentry <small>?</small> Only devices with Systems Manager can access this network

### OPTIONAL – Verify the Client Access (part 2 of 2)

We will use the existing user for this part. We will not have re-authorize them, as we are using the same SSID (just renamed). It might be a good idea to verify this.

**Step 18** Connect to the Client PC and remove any saved profiles.

**Step 19** Connect to the **Podxmr\_WEB** network and open a browser (FF) and type the url of <http://www.cisco.com> and Enter.

Welcome to PodXmr\_WEB

EMAIL  
podox.meraki@flane.de

PASSWORD  
••••••••|

Sign In

Create an Account

**Step 20** On the welcome screen, enter your **podox@domain.com/Cisco123** and click **Sign in**. You will be directed to <http://www.cisco.com>.

**Step 21** Connect back to the Admin PC and open a browser to the Meraki Dashboard (<http://dashboard.meraki.com>).

**Step 22** Navigate to **Network-wide** and choose **Monitor > Clients** and click on your client name (**Podx\_Client**).

**Step 23** Under the client info, select the following:

- Splash is:
- User: [podox.meraki@flane.de](mailto:podox.meraki@flane.de) (**sign-on splash**)

## Clients > **PC**

Status:	associated since Jan 05 15:28
SSID:	PodXmr_WEB
Access point:	<a href="#">88:15:44:f3:23:60</a>
Splash:	User splash ( <a href="#">revoke</a> ) Authorized 2 minutes ago. Expires in about 24 hours.
Signal:	25dB (channel 56)
User:	podox.meraki@flane.de (sign-on splash)
Device type:	Netgear Windows 7/Vista
Capabilities:	802.11ac - 2.4 and 5 GHz <a href="#">details »</a> <a href="#">event log</a>   <a href="#">packet capture</a>   <a href="#">add note</a>

**Step 24** Revoke user credentials and delete any profiles on the Client PC.

### ***Activity Verification***

You have successfully completed this task when you attain this result:

- Modified the Podxmr\_EAP WLAN to be Podxmr\_WEB and used WebAuth Click-Through.
- Connected the client to the Podxmr\_WEB WLAN and authenticated through the Welcome Screen.
- Acquired an IP from the correct network and could ping the default gateway.
- Verified the client connection from the Meraki Dashboard.
- Revoked the clients credentials.
- Optionally modified the WLAN for WebAuth with local user authentication

## **Task 4: Disable SSIDs on the Cloud WLAN Deployment**

### ***Activity Procedure***

This this task, you will disable your SSID on the Cloud WLAN deployment and test client access.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

- Step 1** Use your local PC for Meraki Dashboard access and open a browser and type in the URL:  
<http://dashboard.meraki.com>.
- Step 2** Navigate to **Wireless > SSIDs** and click on **Show all my SSIDs**.
- Step 3** Under your SSID (Podxmr\_WEB) choose **Disable**.

The screenshot shows the Meraki Dashboard interface for managing wireless networks. A specific network named "Pod1\_WEB" is selected. The configuration page displays various parameters for this network. At the top, there is a dropdown menu set to "disabled". Below it, there are several configuration fields and status indicators:

- rename
- edit settings
- Open
- Password-protected with Meraki RADIUS
- unlimited
- Local LAN
- n/a
- no
- n/a
- Disabled
- yes
- Modern

- Step 4** Save Changes.
- Step 5** Rename the Podxmr\_WEB to **Podx** (x=pod#) and Save Changes.
- Step 6** Sign Out of the Meraki Dashboard.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Disabled your SSID and saved changes.
- Renamed SSID and saved changes.
- Sign out of the Meraki Dashboard.



# **Hardware Lab 13: Perform Centralized Controller Maintenance**

---

## **Overview**

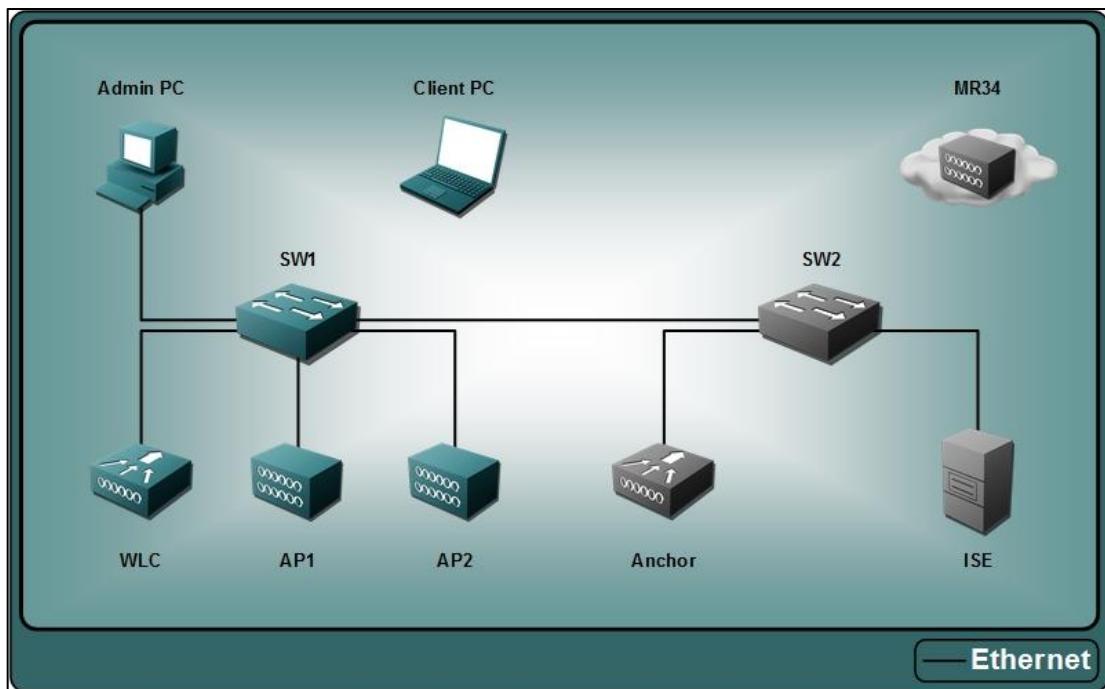
In this activity, you will perform centralized controller maintenance.

After completing this activity, you will be able to meet these objectives:

- Back up the WLC configuration
- Perform an AireOS upgrade to the WLC

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

Here are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 2504 WLC

### VLANs and IP Ranges

#### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
Pod 3650 Switch	192.168.11.254	admin	Cisco123	cisco

## Task 1: Backup the WLC Configuration

### ***Activity Procedure***

In this task, you will back up the WLC's configuration.

---

**Note** The lower case "x" in a command will be your pod number, ex: pod 1, x=1

---

### **Prepare the SFTP server**

You can use a FTP/TFTP or SFTP server to back up your configuration. For your purposes, you will set up a SFTP server.

Complete these steps:

**Step 1** Connect to the Admin PC and select **Start > All Programs** and select the **SolarWinds SFTP/SCP Server**.

---

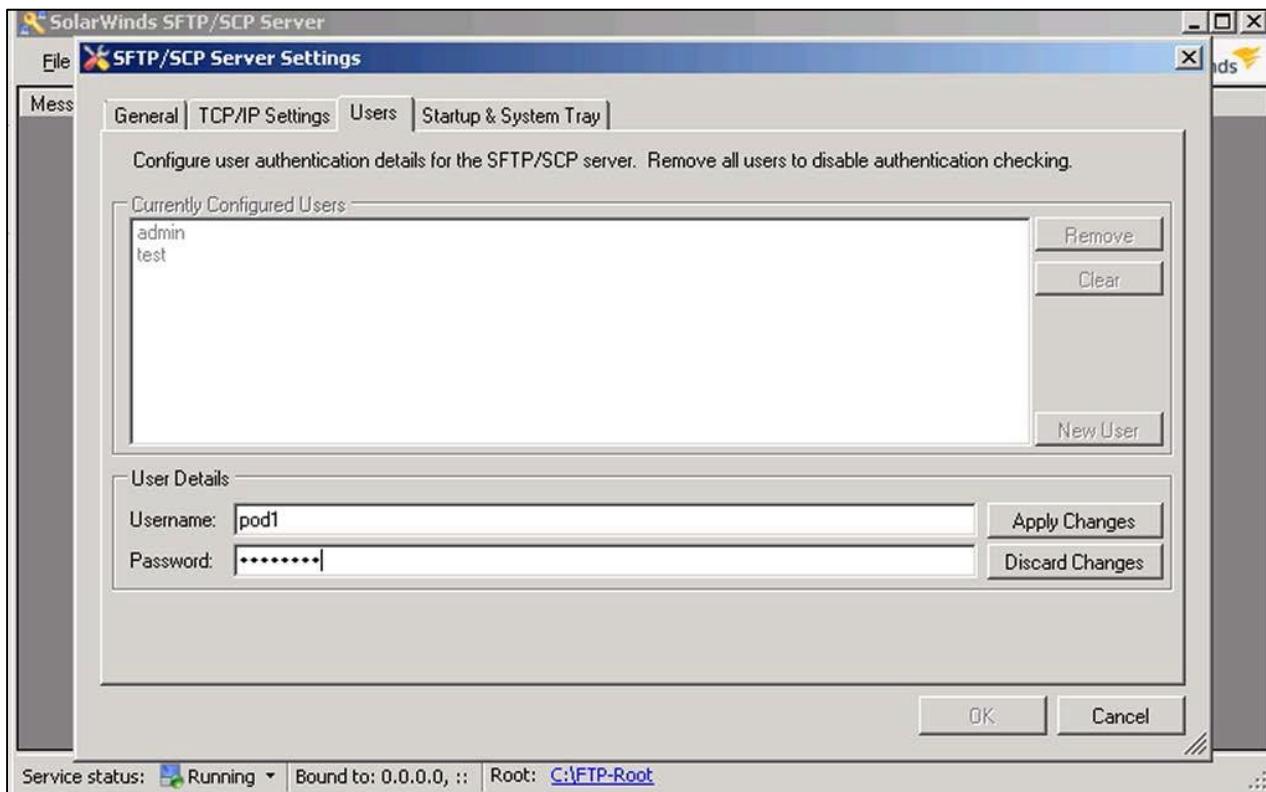
**Note** If it indicates that it is running, click OK. Then go to the task tray and right click the icon and select :Open SolarWinds SFTP/SCP Server.

---

**Step 2** When the SFTP server opens, go to File > Configure and select Users tab (SFTP requires a username/password authentication).

**Step 3** Click **New User** and enter the following:

- Username: **podx**
- Password: **Cisco123**
- **Apply Changes**



**Step 4** You will now have a new user listed. Click **OK**.

**Step 5** Stop the SFTP service by left clicking on the arrow beside the word **Running** (bottom left of SFTP Server screen) and click **Stop** and then wait and click **Start**.

---

**Note** This is done to verify new user info is loaded.

---



### Prepare the WLC for the Backup

Verify that the configuration is saved to flash memory.

**Step 6** Connect to the Admin PC and open a browser to the WLC administration (192.168.11.5).

**Step 7** Click **Save Configuration** and acknowledge popups.

**Step 8** Navigate to **Commands > Upload File** (uploading a file from the WLC to a server) and enter the following:

- File Type: **Configuration**
- Configuration File Encryption (DO NOT CHECK)
- Transfer Mode: **SFTP**
- IP Address: **192.168.11.11** (SFTP server IP)
- File Path: **/** (root path of SFTP server)
- File Name: **PodxBackupLab**
- Server Login Username: **podx**
- Server Login Password: **Cisco123**
- Server Port number: **22**

**Upload file from Controller**

File Type	<input type="text" value="Configuration"/>
Configuration File Encryption	<input type="checkbox"/>
Transfer Mode	<input type="text" value="SFTP"/>
<b>Server Details</b>	
IP Address(Ipv4/Ipv6)	<input type="text" value="192.168.11.11"/>
File Path	<input type="text" value="/"/>
File Name	<input type="text" value="Pod1BackupLab"/>
Server Login Username	<input type="text" value="pod1"/>
Server Login Password	<input type="text" value="*****"/>
Server Port Number	<input type="text" value="22"/>

### Start the Backup

**Step 9** Click the **Upload** button and **OK** to the warning.

---

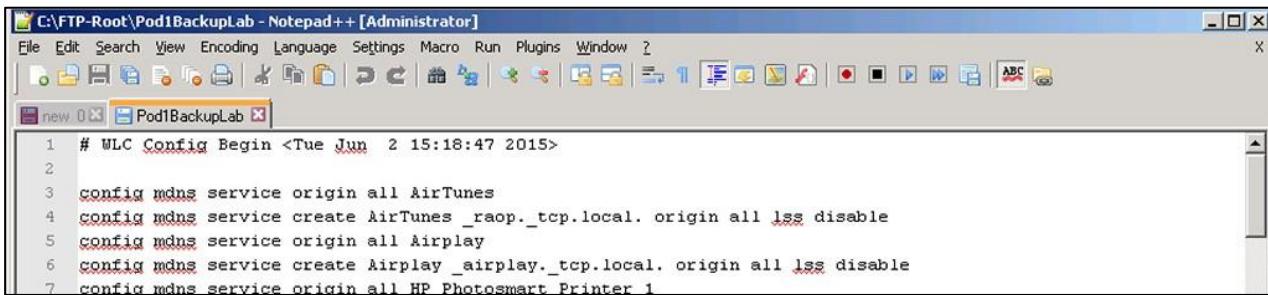
**Note** Most common error is a login error (check username/password on SFTP and WLC).

---

**Step 10** When completed, you should see **File transfer operation completed** on the WLC Upload file screen.

### Verify that the Backup File is on the SFTP Server

**Step 11** On the Admin PC, open File Explorer and then to **C:\SFTP\_Root** and look for your file: **PodxBackupLab**. Right-click and choose open with Notepad++.



A screenshot of the Notepad++ application window. The title bar reads "C:\FTP-Root\Pod1BackupLab - Notepad++ [Administrator]". The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Macro, Run, Plugins, Window, and Help. Below the menu is a toolbar with various icons. The main text area contains the following WLC configuration code:

```
1 # WLC Config Begin <Tue Jun 2 15:18:47 2015>
2
3 config mdns service origin all AirTunes
4 config mdns service create AirTunes _raop._tcp.local. origin all lss disable
5 config mdns service origin all Airplay
6 config mdns service create Airplay _airplay._tcp.local. origin all lss disable
7 config mdns service origin all HP Photosmart Printer 1
```

**Step 12** Review the configuration, but don't change anything. When done in Notepad++, go to **File > Exit** (If prompted to save, click NO).

**Step 13** Close the File Explorer window.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Saved the WLC Configuration to Flash.
- Back up the WLC Configuration to the SFTP server.
- Verified that the backup file on the SFTP server was good.

## **Task 2: Optional—Perform an AireOS Upgrade to the WLC**

### **Activity Procedure**

For this task, you will perform a software upgrade to the WLC. Before doing any upgrade, the configuration should be backed up (you did it in the last task). Backing up a device before a software update is standard practice.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

#### **Prepare the SFTP server**

Here you will verify that the SFTP server is up and the correct image file is available. Your WLC is already on the correct software, but you are going to “update” it.

Complete these steps:

- Step 1** Connect to the Admin PC and verify that the SFTP server is still running.
- Step 2** Open a File Explorer window and navigate to **C:\SFTP\_Root**. Here you will see the files, look for a file named: **AIR-CT2500-K9-8-0-121-0.aes**.

Name	Date modified	Type	Size
AIR-CT2500-K9-8-0-120-0.aes	7/10/2015 7:00 PM	AES File	169,123 KB

**Step 3** Here is the WLC image software for your upgrade. Close the File Explorer Window.

#### Download the new Software Image to the WLC

**Step 4** On the Admin PC, Open a browser to the **WLC** administration (192.168.11.5).

**Step 5** Navigate to **Commands > Download File** and enter the following changes:

- File Type: **Code**
- Transfer Mode: **SFTP**
- IP Address: **192.168.11.11**
- File Path: **/**
- File Name: **AIR-CT2500-K9-8-0-121-0.aes**
- Server Login Username: **podx**
- Server Login Password: **Cisco123**
- Server Port number: **22**

**Download file to Controller**

File Type	<input type="text" value="Code"/>
Transfer Mode	<input type="text" value="SFTP"/>
<b>Server Details</b>	
IP Address(Ipv4/Ipv6)	<input type="text" value="192.168.51.11"/>
File Path	<input type="text" value="/"/>
File Name	<input type="text" value="AIR-CT2500-K9-8-0-120-0.aes"/>
Server Login Username	<input type="text" value="pod5"/>
Server Login Password	<input type="text" value="****"/>
Server Port Number	<input type="text" value="22"/>

#### Upgrade and Reboot the WLC

**Step 6** Click the **Download** button and **OK** to warning popup.

**Step 7** Message on Download screen: **SFTP Code transfer starting.**

**Step 8** You will then receive several other messages on the progress. Last Message will be: **File transfer is successful. Reboot the controller for update to complete. Optionally, pre-download the image to the APs before rebooting to reduce network downtime. For the new Code to take effect, you need to reboot the system. Click Here to get redirected to the reboot page.**

---

<b>Note</b>	The message is advising you of two major things: One, the WLC must be rebooted for the change to take effect. Two, you may want to pre-download any new AP images to reduce their downtime (they would have to download their code, install and reboot).
-------------	--

---

**Step 9** Click the **Click Here** link.

**Step 10** On the System Reboot screen, click the **Save and Reboot** button. Then click **OK** to popup confirmation. The WLC will reboot. You can connect to the **WLC** Console Port to monitor the reboot.

**Step 11** When the Console Port prompts for the login, then the upgrade is complete. Disconnect the Console Port connection.

#### Verify the WLC Upgrade

**Step 12** On the Admin PC, log in to the **WLC** administration. The Monitor screen should display the new software version (8.0.120.0).

**Step 13** Navigate to **Commands > Config Boot**. From here, you could change your boot image and go back to the previous version if the upgrade presented a problem. All the APs would have to update, so check to make sure that they reconnect and that they are all there.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Upgraded the WLC to a new software version.
- Rebooted the WLC.
- Verified that the new software was loaded.
- Verified that all the APs were reconnected to the WLC.

# **Hardware Lab 14: Perform WiFi Scanning**

---

## **Overview**

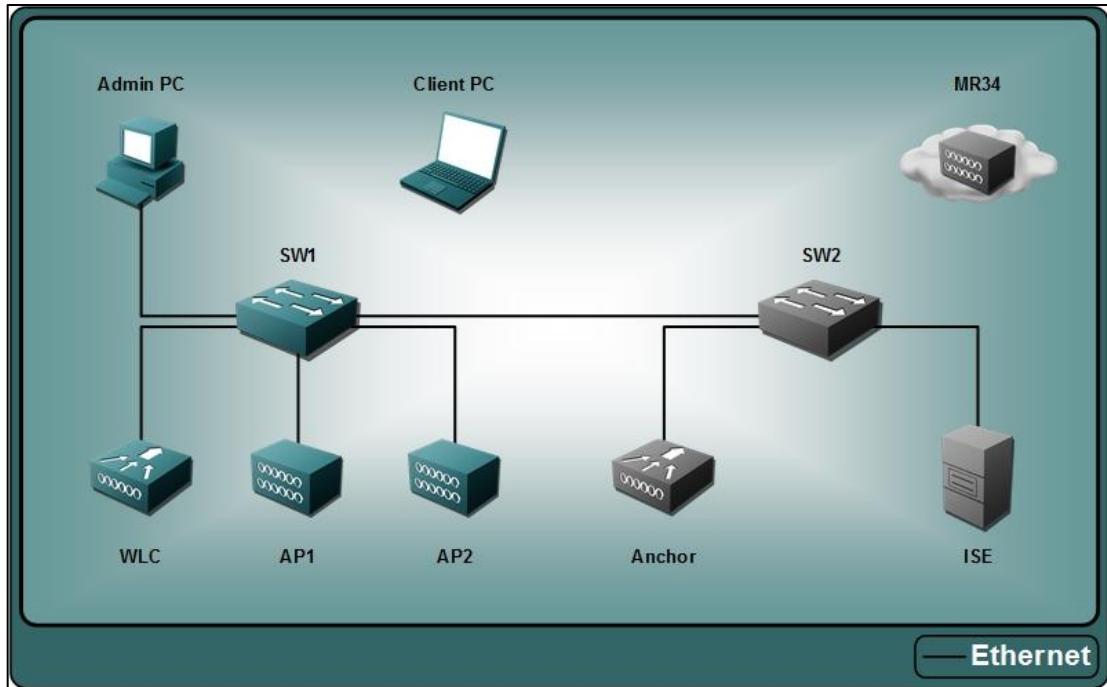
In this activity, you will perform a Layer 2 analysis of the SSIDs.

After completing this activity, you will be able to meet these objectives:

- Enable MetaGeek InSSIDer.
- Review 2.4 GHz activity.
- Review 5 GHz activity.

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

Here are the resources and equipment that are required to complete this activity:

- A Windows 7 PC with Metageek inSSIDer
- Pod 2504 WLC
- AP 3700i

## VLANs and IP Ranges

### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

# Task 1: Enable Metageek inSSIDer

## ***Activity Procedure***

In this task, you enable the Metageek InSSIDer tool.

---

**Note**

The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

- Step 1** Connect to the Client PC and right-click on the **Network** icon on the desktop. Choose properties. You are now at the Network and Sharing Center.
- Step 2** Delete any WLAN profiles and disconnect from any WLANs.
- Step 3** Click the **inSSIDer 4** icon on the desktop. Select the **View** menu and make sure that both radio bands are enabled. Then select **Physical View**.

---

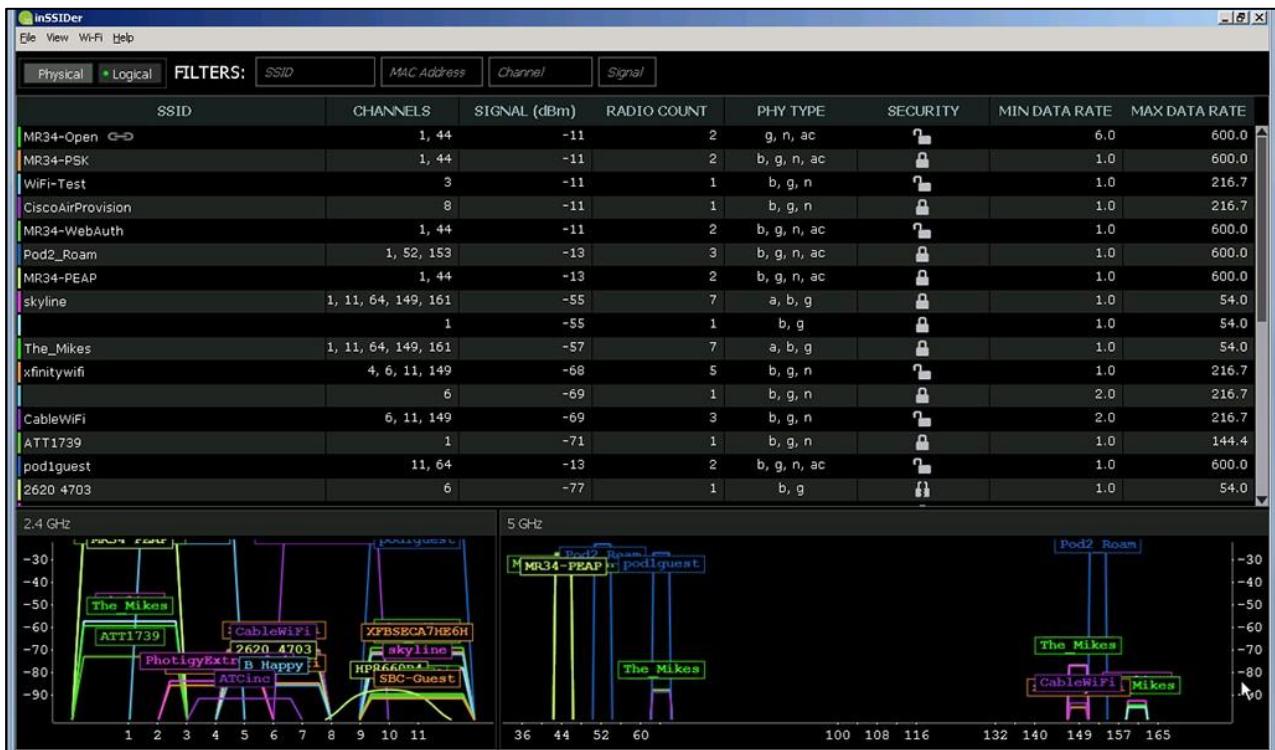
**Note**

If inSSIDer cannot verify the license, connect to the MR34-L-Open-SSID.  
Disconnect from the SSID once the license is verified.

---



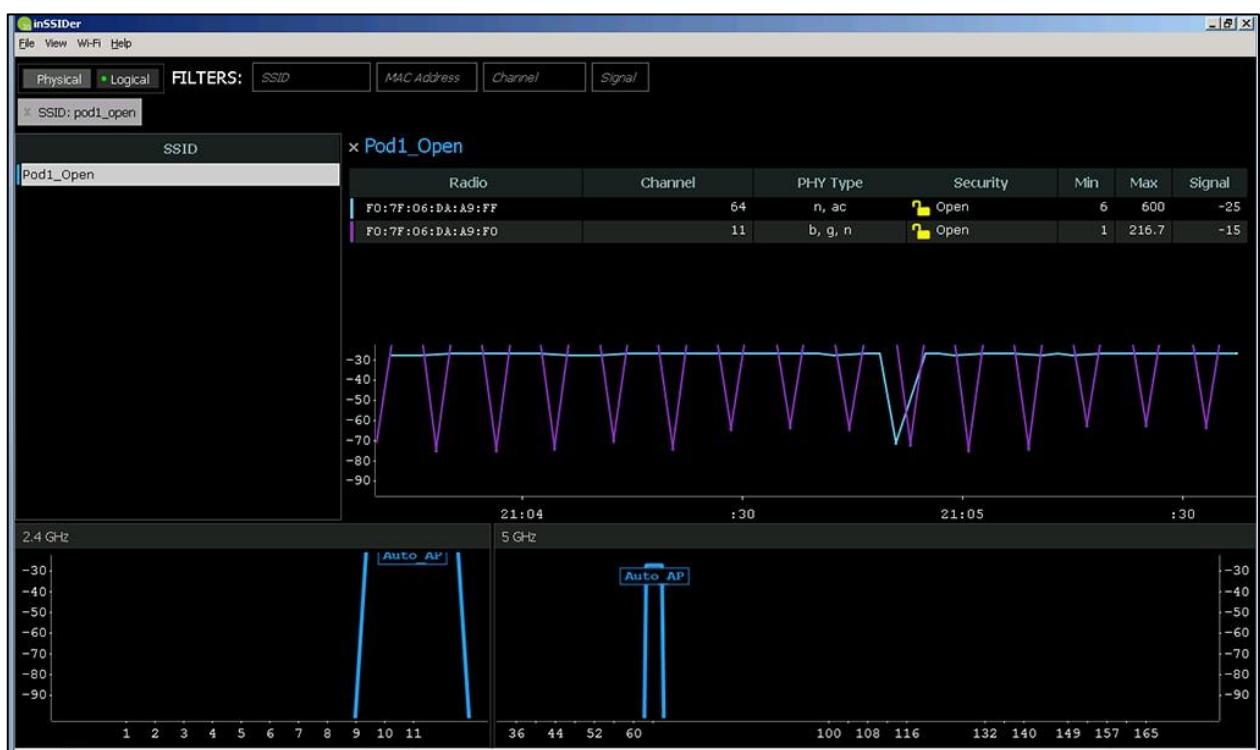
**Step 4** Notice that the MAC addresses appear for the radios (a MAC ending in "x" indicated that the SSID is transmitting on both bands). Go to the View menu and choose Logical View.



- Step 5** Now the MAC addresses are gone and only the SSIDs are displayed. In the **Filter** box at the top, type in one of your SSIDs (ex: MR34-L-PSK) and press **Enter**. Now you can see your SSID in both radio bands (and easily identify the channels and signal strength).



- Step 6** Click **MR34-L-PSK** (where L is your lab number) and another window will open showing you both radios with additional information (individual radio MAC addresses and data rates).



**Step 7** To get help, verify that you are connected to the internet (use WLAN MR34-L-Open) and then select the Help menu and User Guide. The User guide and all support are online.

**Step 8** Close the MetaGeek inSSIDer program.

## ***Activity Verification***

You have successfully completed this task when you attain this result:

- Verified the Metageek inSSIDer tool functions.
- Verified physical and logical information for both radio bands.
- Filtered out all SSIDs except your own.
- Accessed online help and support.

## **Task 2: Review 2.4 GHz Activity**

### ***Activity Procedure***

In this task, you use the Metageek InSSIDer tool to review 2.4 GHz activity.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

**Step 1** Connect to the Client PC and click the **inSSIDer 4** icon.

**Step 2** Go to the **View** menu and make sure only the 2.4 GHz radio is selected. Then select the **Logical View**.

---

**Note** Logical and Physical can be toggled from the buttons beside the FILTERS.

---

**Step 3** Now the MAC addresses are gone and only the SSIDs are displayed. In the Filter box at the top, type in the word **MR34** and press **Enter**.

---

**Note** To remove a Filter, just click the x beside the filter type: name.

---

**Step 4** Now you will see all SSIDs with the word “open” in their name. For any SSID that you are connected to, there will be a “link” icon beside it.

**Step 5** Click **Podx\_Open** and note the following:

- Channel: \_\_\_\_\_ (for 2.4 GHz)
- Signal : \_\_\_\_\_ (it may vary)

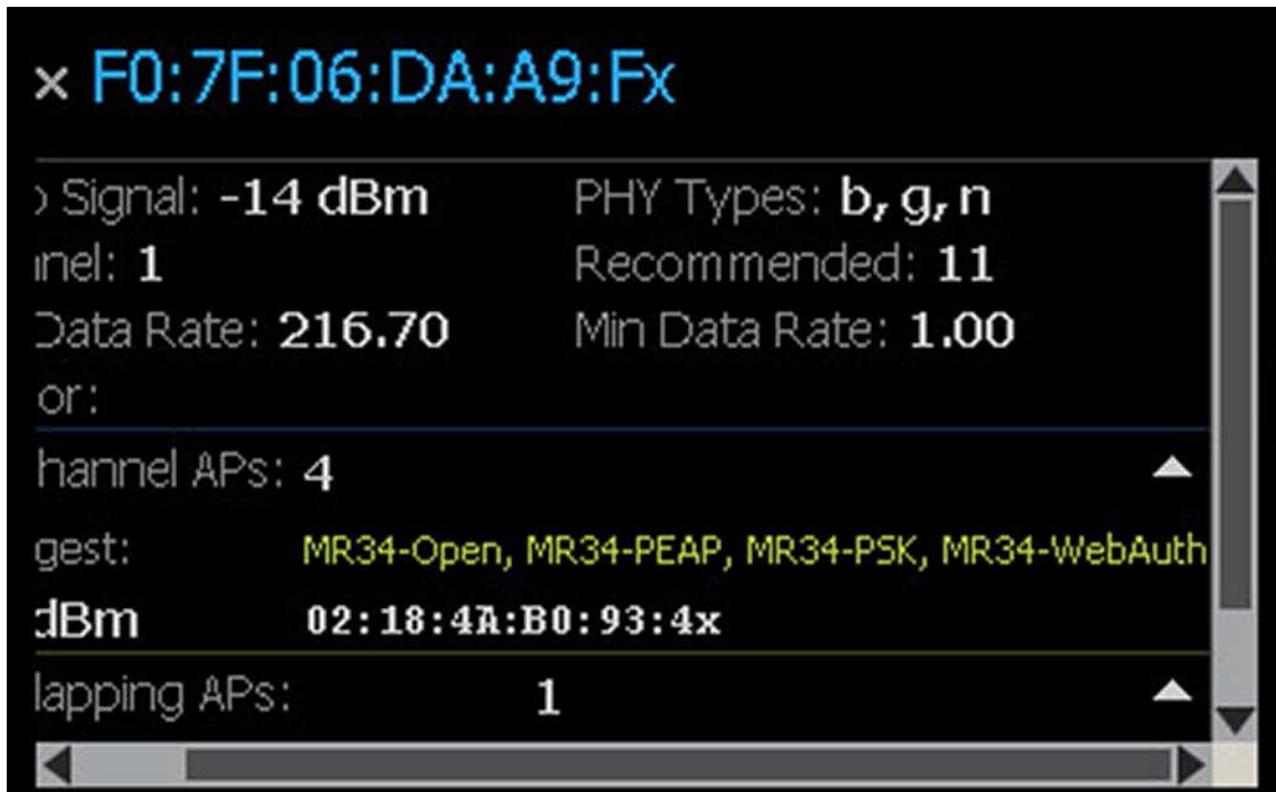
- Radio Count: \_\_\_\_\_ (radios for this SSID)
- Physical Types: \_\_\_\_\_ (b/g/n/ac)
- Security: \_\_\_\_\_

---

**Note** Note the two Radio MACs, one for each band. If you go to another of your SSIDs (MR34-L-PSK) you will see two more MACs.

---

**Step 6** Remove any Filters and click the **Physical** button. Click the MAC for MR34-L-PSK, where L is your lab number (there are several that begin with MR34).



**Step 7** A small window will open with details about your WLAN. It will display the channel that you are on and the recommended channel. It will also display co-channel APs (based on SSID) and overlapping APs.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Verified your 2.4 GHz information.
- Displayed information on how your channel is affected by other channels.

# Task 3: Review 5 GHz Activity

## Activity Procedure

In this task, you use the Metageek InSSIDer tool to review 5 GHz activity.

---

<b>Note</b>	The lower case “x” in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

Complete these steps:

- Step 1** Connect to the Client PC and click the **inSSIDer 4** icon.
- Step 2** Go to the **View** menu and make sure only the 5 GHz radio is selected. Then choose **Logical View** and notice that the 5 GHz space is not so cluttered, but you will see SSIDs on the same channels.
- Step 3** Click the **MR34-L-PSK** SSID, where **L** is your lab number. What type of security is it using?
- Step 4** Compare the Max (speed) between 2.4 GHz and 5 GHz radios.
- Step 5** Look at the bottom of screen and see the channel and AP graph. Sometimes the AP hostname is known (click your SSID). Remove any Filters and click the **Physical** button.
- Step 6** Click the MAC for **MR34-L- PSK**, where **L** is your lab number (there are several that begin with MR34). A small window will open with details about your WLAN. It will display the channel that you are on and the recommended channel. It will also display co-channel APs (based on SSID) and overlapping APs.
- Step 7** Close the inSSIDer tool.

## Activity Verification

You have successfully completed this task when you attain this result:

- Verified your 5 GHz information.
- Verified the 5 GHz RF space.
- Discovered security settings.
- Compared speeds between radio bands.
- Discovered AP host names.
- Displayed information on how your channel is affected by other channels.

# **Hardware Lab 15: Challenge—Various Trouble Tickets**

---

## **Overview**

In this activity, various problems will be introduced and you will have to troubleshoot them and resolve them.

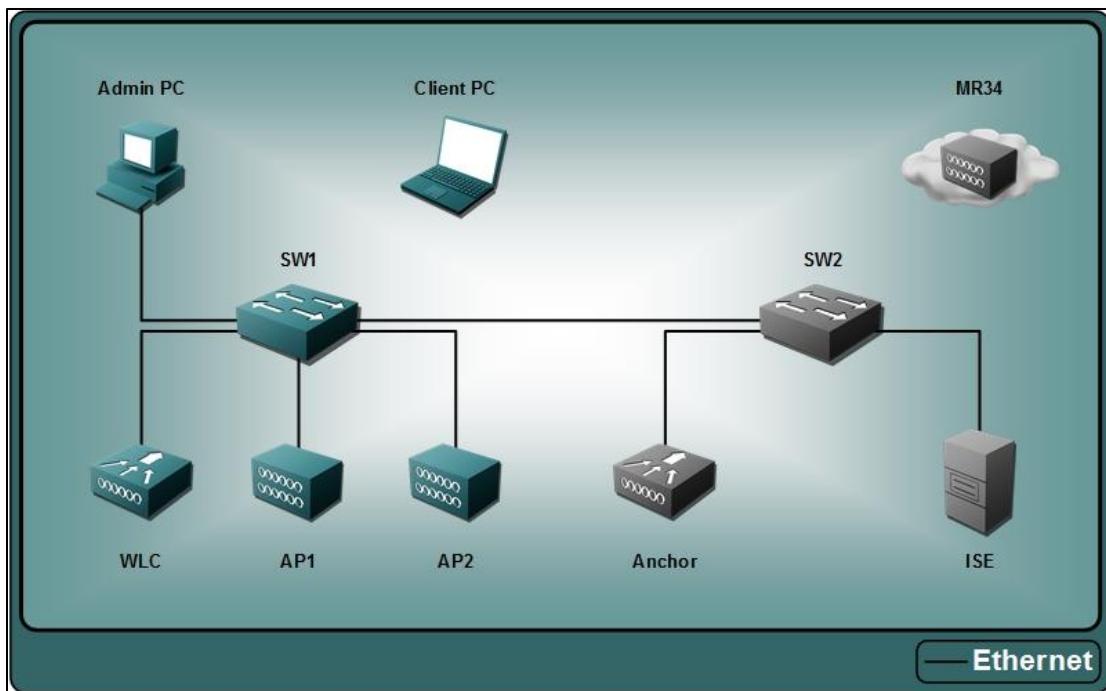
After completing this activity, you will be able to meet these objectives:

- Resolve open trouble tickets



# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

Here are the resources and equipment that are required to complete this activity:

- A Windows 7 PC
- Pod 2504 WLC
- Pod 3650 Switch
- AP 3700 (Converged and Centralized)

## VLANs and IP Ranges

### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password	Enable/CLI
WLC 2504	192.168.11.5	admin	Cisco123	
Pod 3650 Switch	192.168.11.254	admin	Cisco123	cisco
ISE (RADIUS)	192.168.11.21	admin	Cisco123	

## Task 1: Challenge Ticket #1

### ***Activity Procedure***

The company that you work for has employees that are getting the wrong IP address when connecting to Podx\_PSK using the Centralized deployment wireless network. You decide to use “follow the path” troubleshooting technique starting at the wireless Client RF working upstream to the VLAN and IP addressing. Find and correct the problem. Then verify correct wireless client access. Clients are supposed to get IP addresses from the 192.168.14.0/24 network.

#### **Task 1—Check the Wireless Client access**

Complete these steps:

**Step 1** Verify if the wireless client is connecting to the correct SSID.

**Step 2** Verify the IP network that the client is on.

#### **Task 2—Check the WCM (DHCP, VLANs, WLANs)**

Complete these steps:

**Step 3** Verify the client VLAN and IP network.

**Step 4** Verify the WLAN settings.

## Activity Verification

### Task 1—Check the Wireless Client Access

**Step 1** Verify that Client is connection is similar to the following:



**Step 2** Verify that the client IP network is similar to the following:

Hint: The client network is supposed to be 192.168.14.0/24

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 4:

  Connection-specific DNS Suffix . . . . .
  Link-local IPv6 Address . . . . . : fe80::3017:d9c0:9c76:abe4%21
  IPv4 Address . . . . . : 192.168.56.11
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.56.254

E:\>
```

A screenshot of an Administrator Command Prompt window. The command "ipconfig" is run, and the output shows the configuration for the "Wireless Network Connection 4". The output includes the connection-specific DNS suffix, link-local and IPv4 addresses, subnet mask, and default gateway.

## Task 2—Check the WCM (DHCP, VLANs, WLANs)

**Step 3** Does your client vlan look similar to this?

Vlan Configuration			
New Remove		Show	
Interface Name	Status	Protocol	IP-Address
<input type="checkbox"/> Vlan1	up	up	unassigned
<input type="checkbox"/> Vlan51	up	up	192.168.51.254
<input type="checkbox"/> Vlan52	up	up	192.168.52.254
<input type="checkbox"/> Vlan54	up	up	192.168.54.254
<input type="checkbox"/> Vlan56	up	up	192.168.56.254

**Step 4** Verify that the WLAN settings look similar to this.

Hint: The Interface/Interface Group determines the client IP addresses.

**WLAN**  
WLAN > Edit

General	Security	QOS	AVC	Policy Mapping	Advanced
Profile Name	Pod5_PSK				
Type	WLAN				
SSID	Pod5_PSK				
Status	<input checked="" type="checkbox"/> Enabled				
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)				
Radio Policy	All	▼			
Interface/Interface Group(G)	flex <input type="button" value="🔍"/>				
Broadcast SSID	<input checked="" type="checkbox"/>				
Multicast VLAN Feature	<input type="checkbox"/>				

# Task 2: Challenge Ticket #2

## ***Activity Procedure***

Your new hire has just setup RADIUS authentication, but the wireless client cannot connect to the Centralized WLAN Podx\_EAP. Find the problem and resolve it. Afterwards you are required to verify client access. You decide to use the “Prior Knowledge” troubleshooting technique.

### **Task 1—Check the WLC (WLAN, RADIUS)**

Complete these steps.

**Step 1** Verify that WLAN is correct for RADIUS authentication.

**Step 2** Verify that the RADIUS server (ISE) is correctly configured.

### **Task 2—Check the ISE (NAD entry)**

Complete these steps:

**Step 3** Verify that the ISE has the correct entry for the WLC (NAD).

---

**Note** Test client account: user = **podoxuser** and password = **Cisco123**

---

## ***Activity Verification***

### **Task 1—Check the WLC (WLAN, RADIUS)**

**Step 1** Verify that the Podx\_EAP WLAN looks similar to this:

WLANS > Edit 'Pod5\_EAP'

<b>General</b>	<b>Security</b>	<b>QoS</b>	<b>Policy-Mapping</b>	<b>Advanced</b>
<b>Layer 2</b>	<b>Layer 3</b>	<b>AAA Servers</b>		
Select AAA servers below to override use of default servers on this WLAN				
<b>Radius Servers</b>				
Radius Server Overwrite interface <input type="checkbox"/> Enabled				
<b>Authentication Servers</b>		<b>Accounting Servers</b>		
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled		
Server 1	None	None	None	None
Server 2	None	None	None	None
Server 3	None	None	None	None
Server 4	None	None	None	None
Server 5	None	None	None	None
Server 6	None	None	None	None

**Step 2** Verify that the RADIUS settings look similar to this:

Hint: What is the IP address for ISE and what is the “Shared Secret” password?

RADIUS Authentication Servers > Edit

Server Index	2
Server Address(Ipv4/Ipv6)	192.168.59.21
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Disabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
<a href="#">Realm List</a>	
IPSec	<input type="checkbox"/> Enable

## Task 2—Check the ISE (NAD entry)

**Step 3** Verify that the ISE entry for the WLC (NAD) is similar to this:

If you think it is working, test with the Client PC

Network Devices List > POD5WLC

Network Devices

\* Name

Description

\* IP Address:  /

Model Name

Software Version

\* Network Device Group

Device Type

Location

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

**Step 4** Verify that the WLAN settings look similar to this.

Hint: The Interface/Interface Group determines the client IP addresses.

**WLAN**

WLAN > Edit

General	Security	QOS	AVC	Policy Mapping	Advanced
Profile Name	Pod5_PSK				
Type	WLAN				
SSID	Pod5_PSK				
Status	<input checked="" type="checkbox"/> Enabled				
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)				
Radio Policy	<input type="button" value="All"/>				
Interface/Interface Group(G)	<input type="text" value="flex"/> <input type="button" value=""/>				
Broadcast SSID	<input checked="" type="checkbox"/>				
Multicast VLAN Feature	<input type="checkbox"/>				

## Task 3: Answer Key

### ***Activity Procedure***

ONLY AFTER COMPLETING ALL TASKS:

#### **Challenge Ticket #1**

WLAN had incorrect Interface/Interface Group

It should look similar to the following, when corrected:

**WLAN**

WLAN > Edit

General	Security	QOS	AVC	Policy Mapping	Advanced
Profile Name	Pod1_PSK				
Type	WLAN				
SSID	Pod1_PSK				
Status	<input checked="" type="checkbox"/> Enabled				
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)				
Radio Policy	All <input type="button" value="▼"/>				
Interface/Interface Group(G)	Client <input type="button" value="🔍"/>				
Broadcast SSID	<input checked="" type="checkbox"/>				
Multicast VLAN Feature	<input type="checkbox"/>				

## Activity Procedure

### Challenge Ticket #2

WLAN had incorrect Interface/Interface Group.

The IP address cannot be modified. You must create a new RADIUS server entry with the correct ISE IP (192.168.11.21) with a “Shared Secret” of “Cisco123”. Don’t forget to delete the incorrect RADIUS server entry.

It should look similar to the following, when corrected:

## RADIUS Authentication Servers > Edit

Server Index	1
Server Address(Ipv4/Ipv6)	192.168.51.21
Shared Secret Format	<input type="button" value="ASCII"/>
Shared Secret	<input type="text" value="***"/>
Confirm Shared Secret	<input type="text" value="***"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	<input type="button" value="Enabled"/>
Support for RFC 3576	<input type="button" value="Disabled"/>
Server Timeout	<input type="text" value="2"/> seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
<u>Realm List</u>	
IPSec	<input type="checkbox"/> Enable

---

**Note** The problem could also have been incorrect client settings (EAP Profile), bad credentials from client or incorrect credentials entered for the client in ISE.

---



# **Hardware Lab 16: Perform a Predictive WLAN Design**

---

## **Overview**

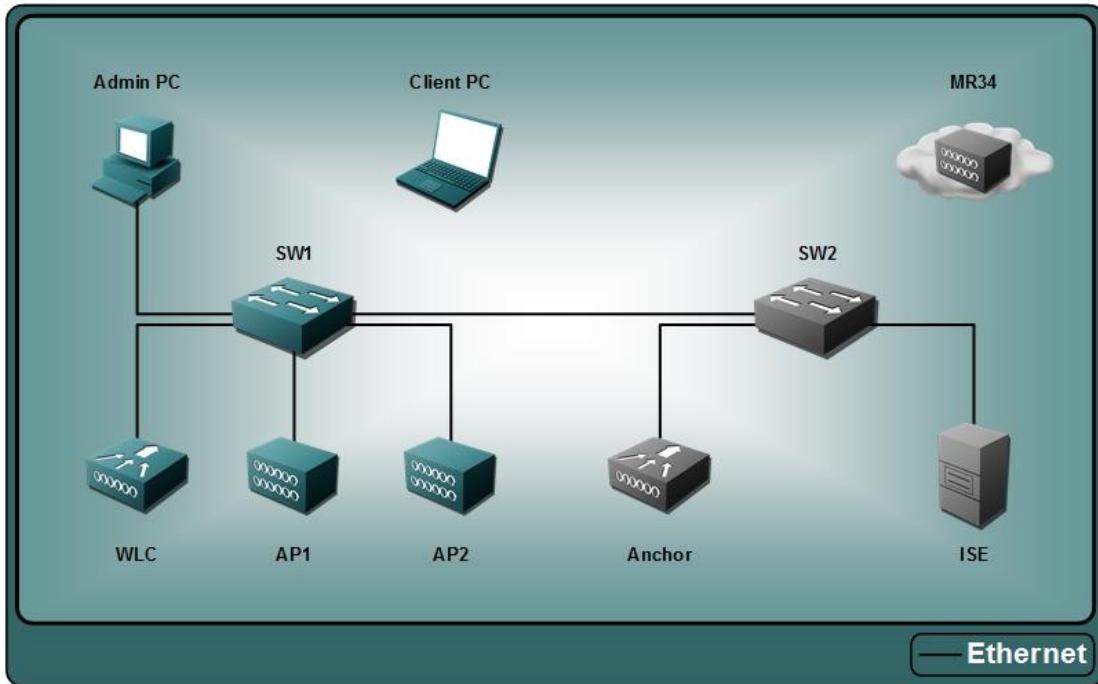
In this scenario, a customer has decided to implement a WLAN. They have contacted ABC consulting, LLC. and have requested a WLAN be designed and implemented. You have been asked to take care of this customer's request. You will assume the role as the WLAN design engineer. After performing the information gathering process with the customer, it is time to perform the predictive WLAN design using the Ekahau Site Survey Pro + Planner application. Since you are new to using Ekahau Site Survey Pro + Planner it will be necessary to familiarize yourself with the graphical interface prior to performing the predictive WLAN design.

In this activity, you will access and navigate through the Ekahau Site Survey Pro + Planner graphical interface. You will also perform a basic predictive WLAN design. After completing this activity, you will be able to meet these objectives:

- Understand the basic steps involved in navigating the Ekahau Site Survey Pro + Planner graphical interface.
- Perform a basic predictive WLAN design using a single floor layout.

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- Client PC
- Ekahau Site Survey Pro + Planner

## VLANs and IP Ranges

### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

# Task 1: Familiarization with Ekahau Site Survey Pro + Planner

## **Activity Procedure**

Ekahau Site Survey Pro + Planner can be used to perform predictive planning and/or active/passive site surveys. In this task, using Ekahau Site Survey Pro + Planner, you will load an example project and perform a series of steps to familiarize yourself with the graphical interface. Later in the lab activity you will perform a basic predictive WLAN design.

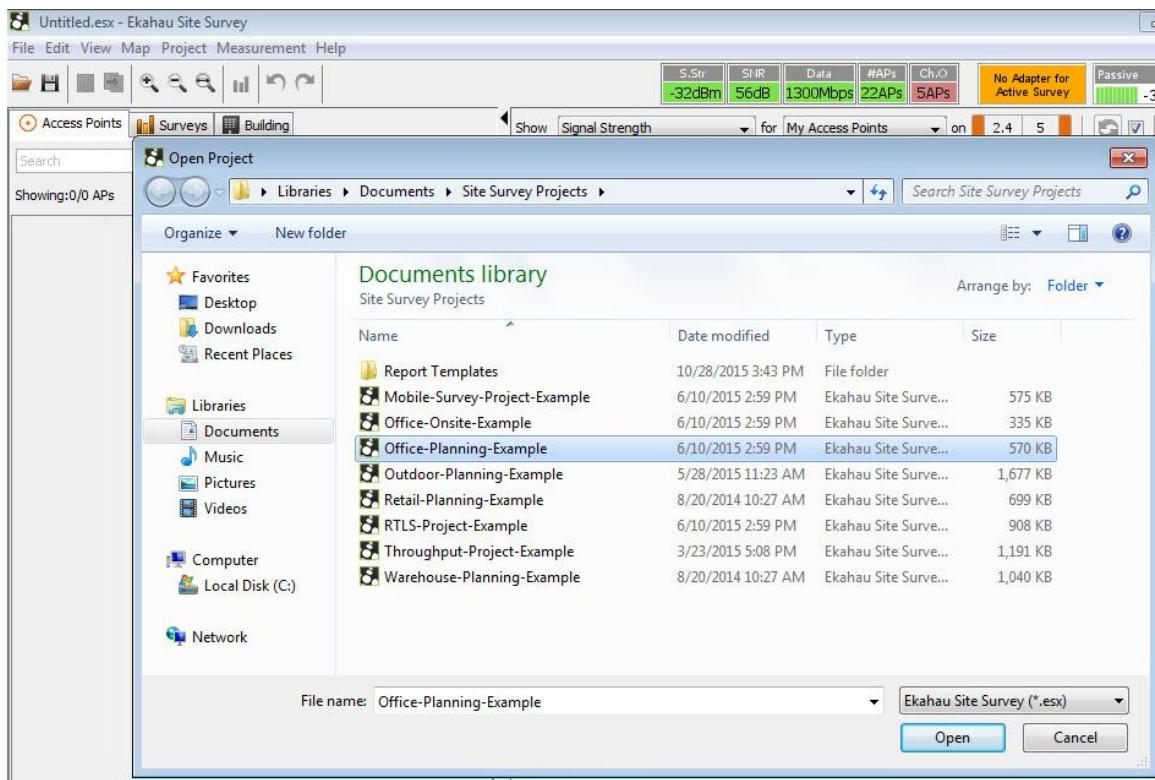
---

<b>Note</b>	The lower case “x” in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

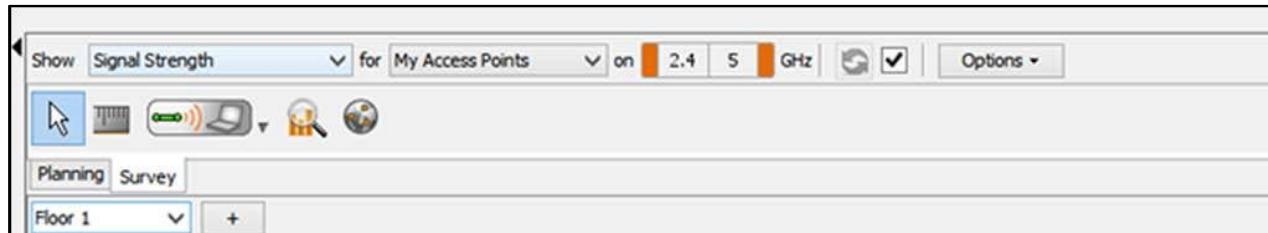
Complete these steps:

- Step 1** Connect to the Client PC and right-click on the **Network** icon on the desktop and choose properties. You are now at the **Network and Sharing Center**.
  - Step 2** Click on **Change adapter settings** and right-click on the **Ekahau\_only** and choose **Enable**. Local Area Connection should now be enabled.
  - Step 3** Delete any WLAN profiles and disconnect from any WLANs. From the Client desktop, double-click the **Ekahau Site Survey** icon (takes a minute to open).
- In order to create a predictive WLAN design using Ekahau Site Survey Pro + Planner it is necessary to create a project. In the following steps you will open an example project that has already been created.
- Step 4** Open an example project from the menu **File > Open**. From the Open Project screen, locate and double-click the **Site Survey Projects** folder, select the **Office-Planning-Example** project.

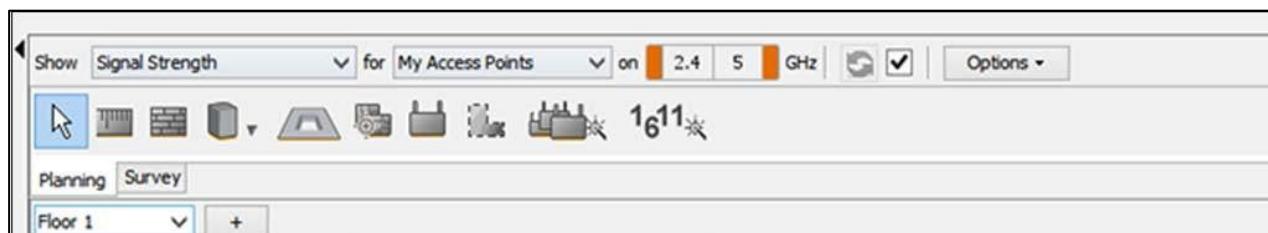


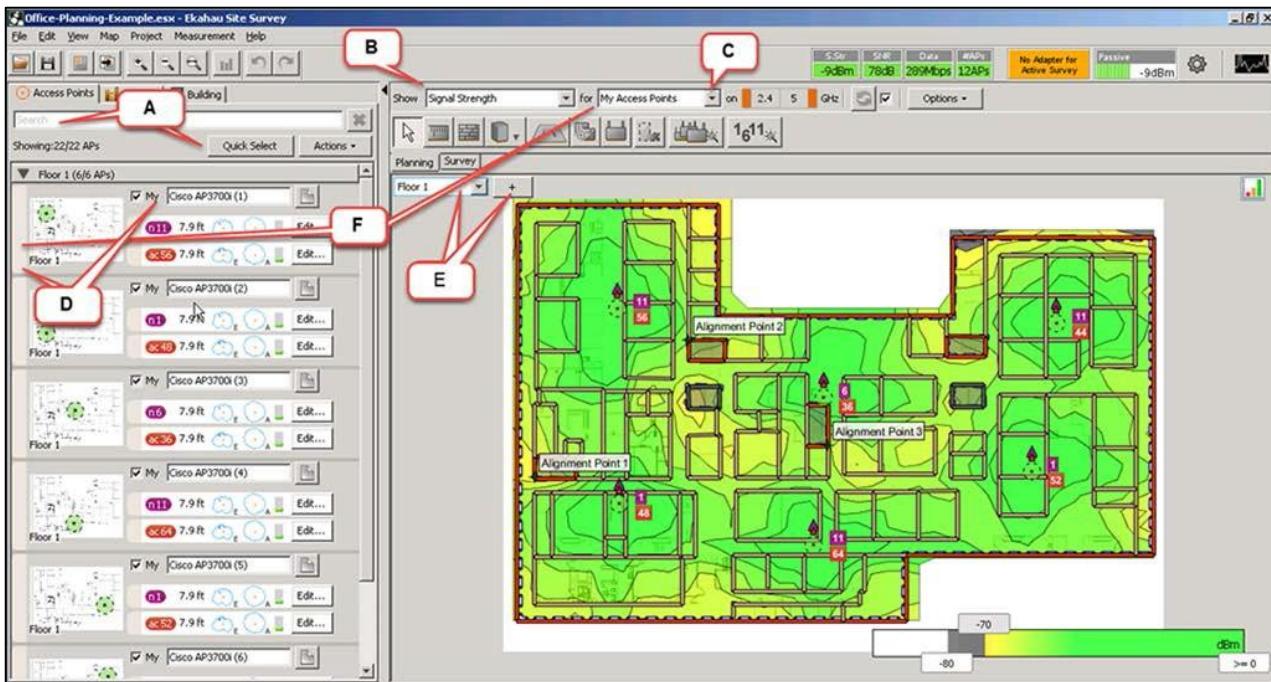
**Step 5** The next steps will introduce you to the Survey and Planning tabs used in the tool. From the right side of the screen you will notice two tabs.

**Survey:** This tab will provide the tools necessary to perform active/passive site surveys.



**Planning:** This tab is used when performing predictive WLAN designs. It allows a WLAN design engineer to input information gathered from the Customer. Ekahau Site Survey Pro + Planner will use this to perform the predictive design.





### Step 6 Using the information below, familiarize yourself with Ekahau Site Survey Pro + Planner:

1. The **Access Points** tab, on the left side of the screen, is used to quickly search or select actual or simulated APs that are located on the floor layout(s). This is helpful when locating specific AP types, SSIDs, Band(s), or Channel on single or multi floor layout(s).
  - Under the Access Points tab, in the Search text box, type **802.11ac**. This will display: **Showing:22/22 APs**. Click the red X to remove the search results.
  - Under the Access Points tabs (A), click **Quick Select > AP** and type : **Simulated > Close**. This will display: **Showing:22/22 APs**.
2. Located on the right side of the screen, the Show dropdown list box is used to choose the type of visualization that will be displayed. Several examples of the visualization types are: signal strength, channel bandwidth, packet loss, & throughput.
  - From the Show dropdown list box (B), select **Channel Coverage**. Notice the screen colors and coverage will change. Depending on the visualization type you select the colors and coverage will change.
3. Located on the right side of the screen, the for dropdown list box (C) is used to select the AP(s) that will be used to display the visualization results on the floor layout. The options are: All Access Points, My Access Points, Other Access Points, Selected Access Points
  - From the for dropdown list box (C), select **All Access Points**. Notice several options appear in the for dropdown list box.
4. Listed on the left side of the screen in the Floor section that allows you to select the floor diagrams and the simulated AP placements that were calculated by the predict WLAN design. Unchecking a selected AP will cause the signal coverage to be removed.
  - On the left side, click on the arrow to expand the **Floor 1 section (D)**.
  - On the right side, beside **Show (B)**, choose **Signal Strength** from the dropdown.
  - On the right side, beside **for (C)**, choose **My Access Points** from the dropdown

- From the **floor** list, uncheck the first (1) **My-Cisco AP3700i** checkbox. Notice the previous AP coverage is no longer displayed. In a multi-floor design you may only want display to the signal coverage one floor at time.
  - On the left side of the screen in the **Floor** section, select the arrow next **Floor 1** and collapse the floor from view. Notice the previously displayed floor will collapse from sight.
5. Located on the right side of the screen, you are given the option to view or add additional floor layout to be used during the planning phase.
    - From the right side of the screen, under the **Planning** tab, locate the dropdown list box that currently lists **Floor 1 (E)**. Open the dropdown list box (E) and switch between **Floor 1**, **Floor 2**, or **Floor 3**. Notice the select floor is displayed on the screen.
    - From the right side of the screen, under the **Planning** tab, click the plus sign + to place additional floor layouts in this project.
  6. The **Floor (D)** section on left side of the screen and the **for** dropdown list box (C) on the right side of the screen are used in conjunction (F) to filter and display the appropriate APs, maps, or visualizations.

## **Activity Verification**

You have successfully completed this task when you attain this result:

- Using Ekahau Site Survey Pro + Planner, you open an example project and perform specific tasks and change specific screen options to become familiar with the application.

## **Task 2: Perform a basic predictive WLAN design using a single floor layout.**

### **Activity Procedure**

In this task, using Ekahau Site Survey Pro + Planner, you will perform the following: load a basic office layout, scale the map, draw walls, and run auto-planner.

---

<b>Note</b>	The lower case “x” in a command will be your pod number, ex: pod 1, x=1
-------------	---

---

Complete these steps:

- Step 1** Select **File > New** from the Ekahau Site Survey dashboard and answer **NO** in the dialog box.
- Step 2** From the right side of the screen, select the **Planning** tab, click the + to add a new map.

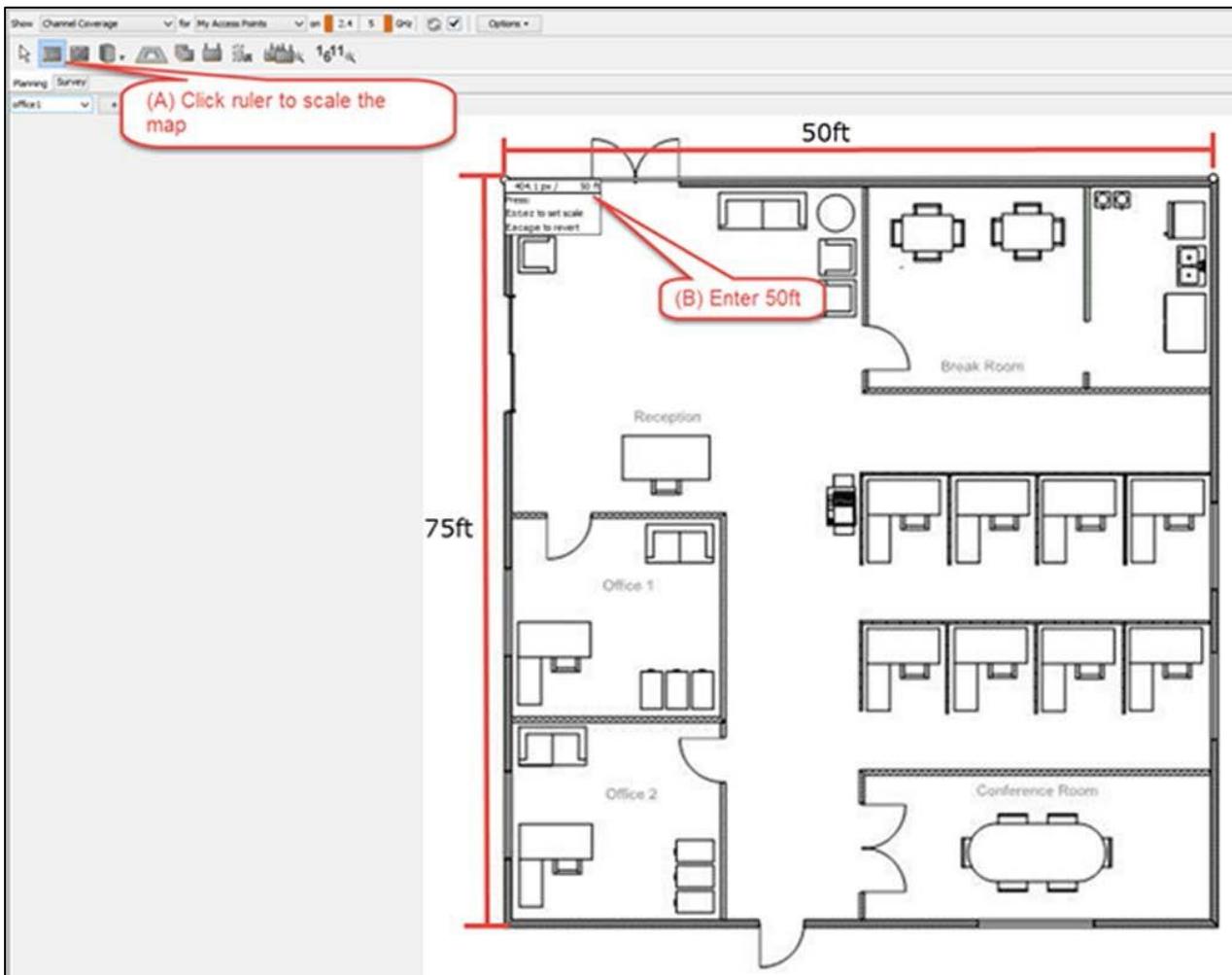


**Step 3** Locate **office1.jpg** map from the My Tools folder on the desktop and click **Open**.

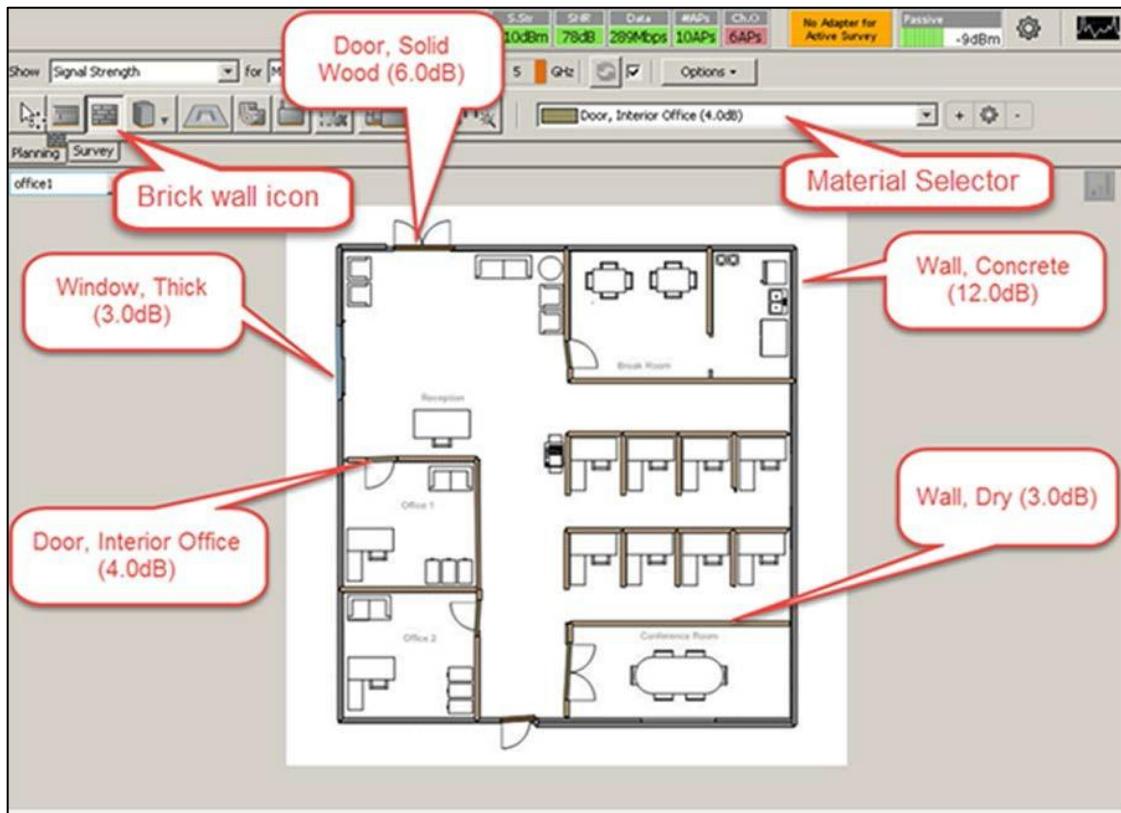
**Note** For this lab activity the example dimensions of the floor layout will be 50ft x 75ft. Typically this information would be provided by the customer during the information gathering phase.

**Step 4** After loading the new floor layout, it is necessary to scale the map (map scale). The map scale refers to the relationship (or ratio) between the floor layout/map(s) dimensions and the corresponding physical dimensions of the actual floor(s).

1. On the right side of the screen, above the **Planning** tab, select the ruler icon to begin scaling the map.
2. From the top left edge of the office diagram, draw a line from the left corner of the office suite to the right corner of the office suite. Type **50 ft (15.2m)** in the dialog box to set the scale of the map and press **Enter**.



**Step 5** Now that the floor layout has been scaled, it is now time to draw the walls, windows, door, etc.... This will allow the predictive software to best determine the number and placement of the APs.



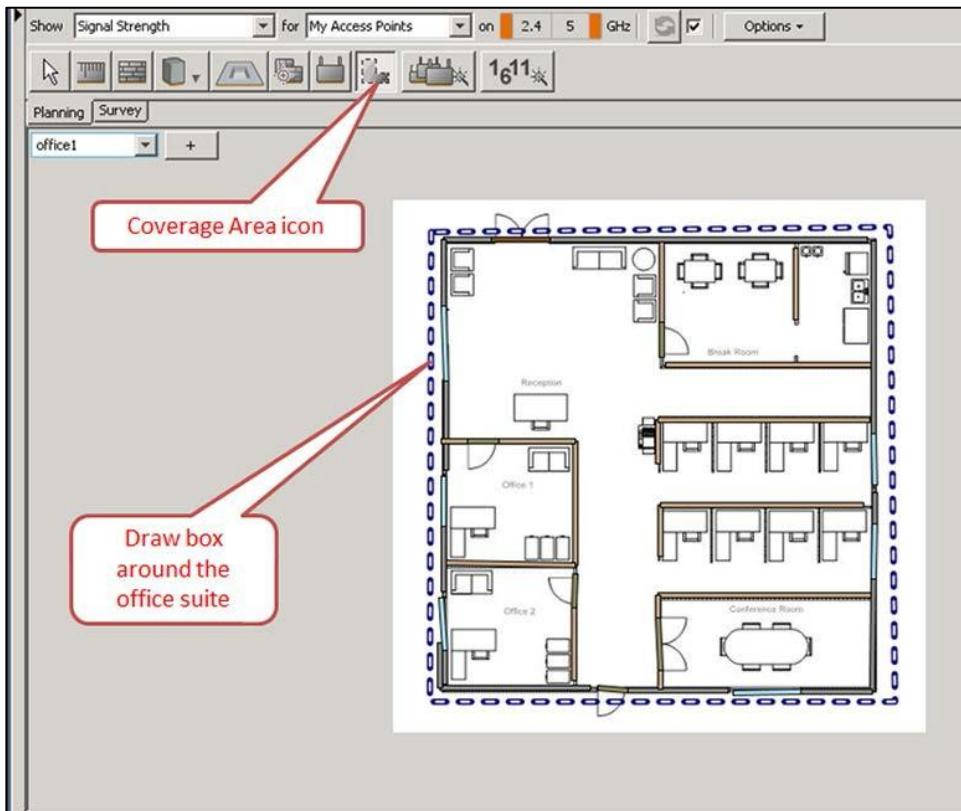
- Step 6** On the right side of the screen, above the **Planning** tab, select the **brick wall** icon to begin drawing the walls.
- Step 7** Using the material selector dropdown list box, select and draw **Wall, Concrete (12.0dB)** or easier viewings choose: **Wall, Brick (9.9dB)** walls along the outside walls of the office suite. Be sure to stop and start again for doors or windows.

---

**Note** Use your mouse right-click to stop the drawing tool. Use your mouse left-click to start the drawing tool.

---

- Step 8** Using the material selector dropdown list box, select and draw **Door, Solid Wood (6.0dB)** along the outside of the office suite.
- Step 9** Using the material selector dropdown list box, select and draw **Window, Thick (3.0dB)** along the outside of the office suite.
- Step 10** Using the material selector dropdown list box, select and draw **Wall, Dry (3.0dB)** walls for the offices, cubicles, break room, & conference along the inside of the office suite. Be sure to stop and start again for the doors.
- Step 11** Using the material selector dropdown list box, select and draw **Door, Interior Office (4.0dB)** along the inside of the office suite.
- Step 12** Now that you are finished scaling the map, drawing the walls, windows, and doors, it is time to setup the coverage area. On the right side of the screen, above the **Planning** tab, select the **coverage area** icon.



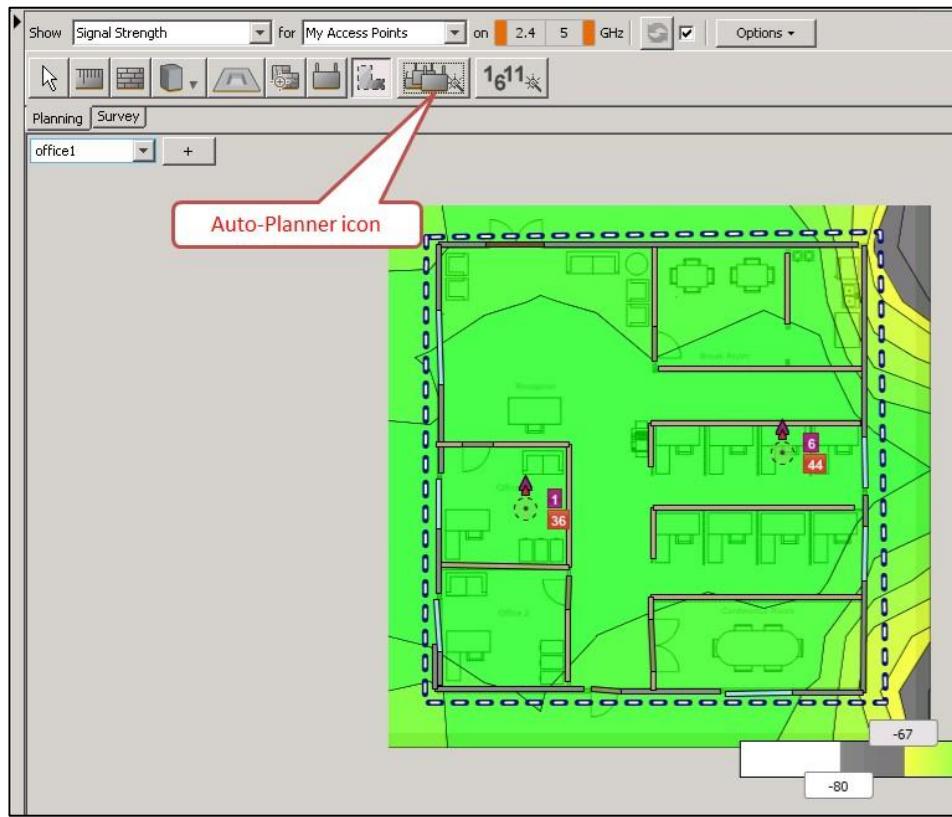
**Step 13** Using the coverage area tool draw a box around the office suite to designate the WLAN coverage area.

---

**Note** Use your mouse right-click to stop the Coverage tool. Use your mouse left-click to start the Coverage tool.

---

**Step 14** On the right side of the screen, above the **Planning** tab, select the **Auto-Planner** icon.



**Step 15** Choose **Generic .11n/ac Dual Radio** from the **Access Point** dropdown and then click **Create Plan**.

**Step 16** Process complete. At this point in time you could start analyzing the results of the auto-planner.

**Optional:**

Try different materials in the Planner for inside and outside walls to see where your RF goes. Move the APs around to see how it affects coverage. Add an additional access point (Simulated Access Point icon) to the conference room in the bottom right of the office, (to see how it affects your coverage. Change your channel bandwidth for 5GHz to 40MHz (Channel Planner icon). Then change the Show dropdown to verify new throughput.

### **Activity Verification**

You have successfully completed this task when you attain this result:

- Using Ekahau Site Survey Pro + Planner, you performed the following: load a basic office layout, scale the map, draw walls, and run Auto-planner.



# **Hardware Lab 17: Perform Passive Site Survey**

---

## **Analysis**

### **Overview**

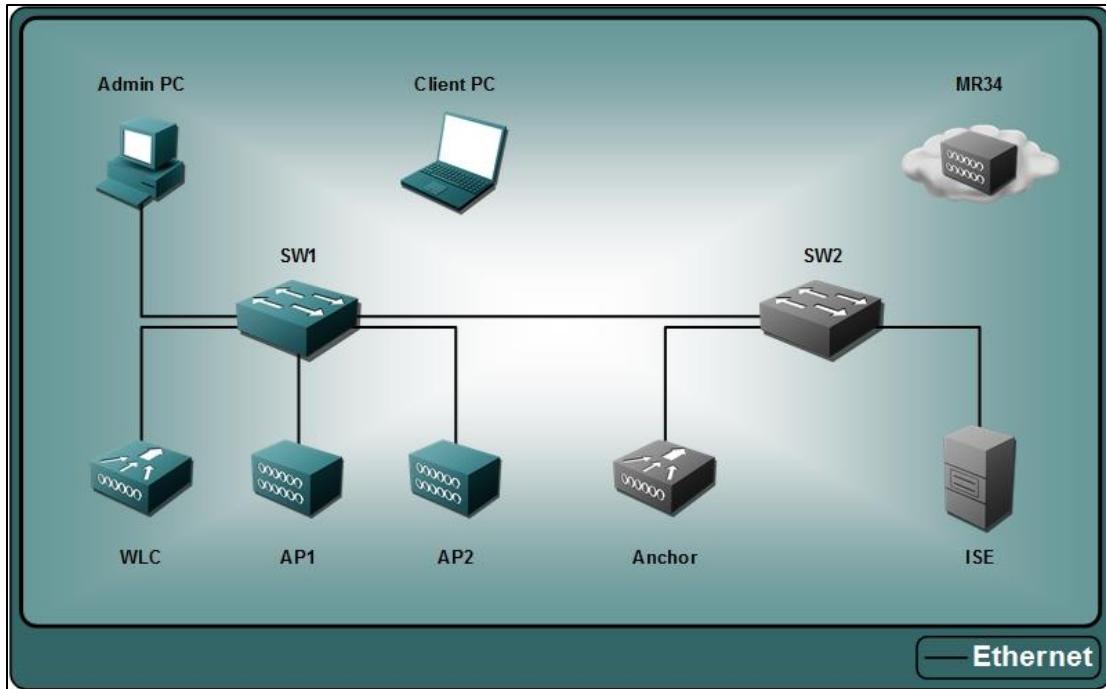
In this scenario, as the WLAN design engineer you have performed the information gathering process with the customer and used that information to perform the predictive WLAN design using the Ekahau Site Survey Pro + Planner application. The active site survey has been performed, the customer has signed off on BOM, and the WLAN has been deployed. It has been several weeks since the deployment and the customers is experiencing what they believe to be possible RF interference. They have ask you to return to perform a passive site survey using the Cisco CleanAir AP(s) and locate the RF interference devices and recommend a solutions.

In this activity, you perform passive site survey using an AP and Metageek Chanalyzer spectrum analyzer software. After completing this activity, you will be able to meet these objectives:

- Configure an AP for Spectrum Expert AP (SE) mode of operation.
- Configure Metageek Chanalyzer - spectrum analyzer software.
- Analyze RF information locating a RF interference device using metageek Chanalyzer - spectrum analyzer software.

# Visual Objective

The figure illustrates what you will accomplish in this activity.



## Job Aids

These are the resources and equipment that are required to complete this activity:

- Client PC
- Pod 2504 WLC
- Centralized AP w/ Cisco Clean Air
- metageek Chanalyzer - spectrum analyzer software

## VLANs and IP Ranges

### Device Information

Management IP Addresses (Vlan 11 – mgt)	Access Point IP Addresses (Vlan 12 – AP)	Wireless Client IP Addresses (Vlan 14 – Client)	Backbone IP Addresses
192.168.11.0/24	192.168.12.0/24	192.168.14.0/24	172.16.0.0/24

## Usernames and Passwords

Device	IP Address	Username	Password
WLC 2504	192.168.11.5	admin	Cisco123

## Task 1: Configure AP for Spectrum Expert AP mode of operation

### ***Activity Procedure***

In preparation for the passive site survey it is necessary to access the pod WLC and configure the centralized AP for Spectrum Expert AP (SE) mode of operation. It is only necessary to copy the network spectrum interface key and IP address the AP. The key and IP address will be used to configure metageek Chanalyzer to communicate with the AP.

---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

- Step 1** Connect to the Admin PC and verify that the **Local Area Connection** is still enabled.
- Step 2** From the Admin PC, connect to your pod WLC web interface (192.168.11.5).
- Step 3** From the WLC dashboard, select **Wireless > Access Points > All APs**. Then select **AP1** from the list of APs by clicking the hyperlink.

The screenshot shows the Cisco Wireless Controller (WLC) interface. In the top navigation bar, the 'WIRELESS' tab is selected. On the left, the 'Access Points' section is expanded, showing 'All APs' and various configuration options like 'Radios' and 'Advanced'. The main content area is titled 'All APs > Details for Centralized\_AP'. Below this, there are tabs for 'General', 'Credentials', 'Interfaces', 'High Availability', 'Inventory', and 'Advanced'. The 'General' tab is active. On the right, there are two columns: 'General' and 'Versions'. Under 'General', the 'AP Name' is 'Centralized\_AP', 'Location' is 'default location', and 'Base Radio MAC' is '84:b8:02:00:58:d0'. The 'AP Mode' dropdown is highlighted with a red box and labeled 'AP Mode'. The 'AP Sub Mode' dropdown is also highlighted with a red box and labeled 'SE-Connect'. Other fields include 'Admin Status' (Enable), 'Operational Status' (monitor), 'Port Number', 'Venue Group', 'Venue Type' (Unspecified), 'Venue Name', 'Language', and 'GPS Location' (Network Spectrum Interface Key: 6DBED0EB2B94A4D0F389F7913E6F07F9). The 'Versions' column lists software versions and download status. Below these are sections for 'IP Config' (CAPWAP Preferred Mode: IPv4 (Global Config), DHCP Ipv4 Address: 192.168.22.15, Static IP (Ipv4/Ipv6)), 'Time Statistics' (UP Time: 8 d, 00 h 17 m 46 s, Controller Associated Time: 7 d, 20 h 00 m 04 s, Controller Association Latency: 0 d, 00 h 04 m 24 s), and a clipboard icon.

**Step 4** Under the **General** tab, locate the **AP Mode** dropdown list box and select **SE-Connect** from the list.

When using a Cisco centralized AP w/Clean Air, depending on the type of analysis that you are doing you must configure the AP in one of three modes: SE-connect, local, or monitor. In this lab activity we are using SE-connect. Listed below are the three modes explained.

- **SE-Connect:** This mode enables a user to connect Chanalyzer running on an external PC to a Cisco Clean Air-enabled AP in order to display and analyze detailed spectrum data for all WLAN channels on the radio. In this mode, an AP is used strictly as a spectrum analysis capture interface and sends the data directly to the spectrum analyzer. In this mode the AP does not send any Wi-Fi, RF, or spectrum data to the WLC.
- **Local:** Each Cisco Clean Air-enabled AP radio provides air quality and interference detection reports for the current operating channel only. Local mode does not disrupt client connections.
- **Monitor:** When Cisco Clean Air is enabled in monitor mode, the AP provides air quality and interference detection reports for all monitored channels. Monitor mode allows the AP to share spectrum analysis dwells for collection for WLAN data.

**Step 5** Click **Apply** to save the changes. This will cause the AP to reboot into SE-Connect mode.

**Step 6** Click **OK** to reboot the AP.

**Step 7** After the AP reboots, select **AP1** from the list of APs by clicking the hyperlink.

**Step 8** Under the **General** tab, locate the **Network Spectrum Interface** key field and document or copy the key to the clipboard. This be used by Metageek Chanalyzer software to connect to the AP. Document the IP address of the centralized AP. This information will be used when configuring the metageek Chanalyzer software.

The screenshot shows the Cisco Wireless Controller (WLC) web interface under the 'Wireless' tab. On the left, a sidebar lists various configuration categories like Access Points, Advanced, Mesh, RF Profiles, and Network Lists. The main panel displays 'All APs > Details for Centralized\_AP'. The 'General' tab is selected. In the 'General' section, the AP Name is 'Centralized\_AP', Location is 'default location', AP MAC Address is '84:b8:02:05:97:f0', Base Radio MAC is '84:b8:02:00:58:d0', Admin Status is 'Enable', and AP Mode is 'SE-Connect'. The 'Network Spectrum Interface Key' field contains the value '79C3AD30B02572149A661D74B9F43A65'. A red callout box highlights this key with the text 'Copy Network Spectrum Interface Key to the clipboard'. To the right, the 'Versions' section shows Primary Software Version 8.0.110.11 and Backup Software Version 3.0.51.0. Below that is the 'IP Config' section with CAPWAP Preferred Mode set to 'Ipv4 (Global Config)', DHCP Ipv4 Address 192.168.22.16, and Static IP (Ipv4/Ipv6) set to 'None'. The 'Time Statistics' section shows UP Time, Controller Associated Time, and Controller Association Latency.

## Activity Verification

You have successfully completed this task when you attain this result:

- You have configured Spectrum Expert AP mode of operation on an AP.
- You have copied the Network Spectrum Interface key and AP IP address. This information will be used by the metageek Chanalyzer software to connect to the AP.

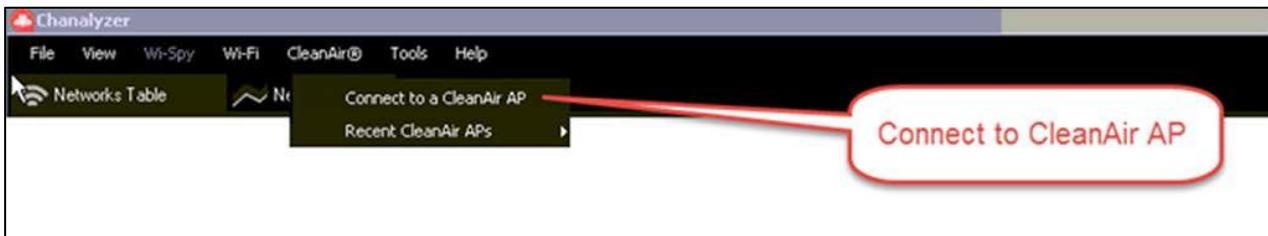
## Task 2: Configure Metageek Chanalyzer - spectrum analyzer software

### Activity Procedure

In this task, you will continue to prepare for your passive site survey by configuring Metageek Chanalyzer w/ Cisco CleanAir option to communicate with the previously configured centralized AP. The communication between the metageek Chanalyzer and the AP is necessary to be able to analyze the information captured by the AP in SE-Connect mode.

Complete these steps:

- Step 1** From the Admin PC, install the metageek Chanalyzer software as described in the Student Notes and start it using the shortcut located on the desktop.

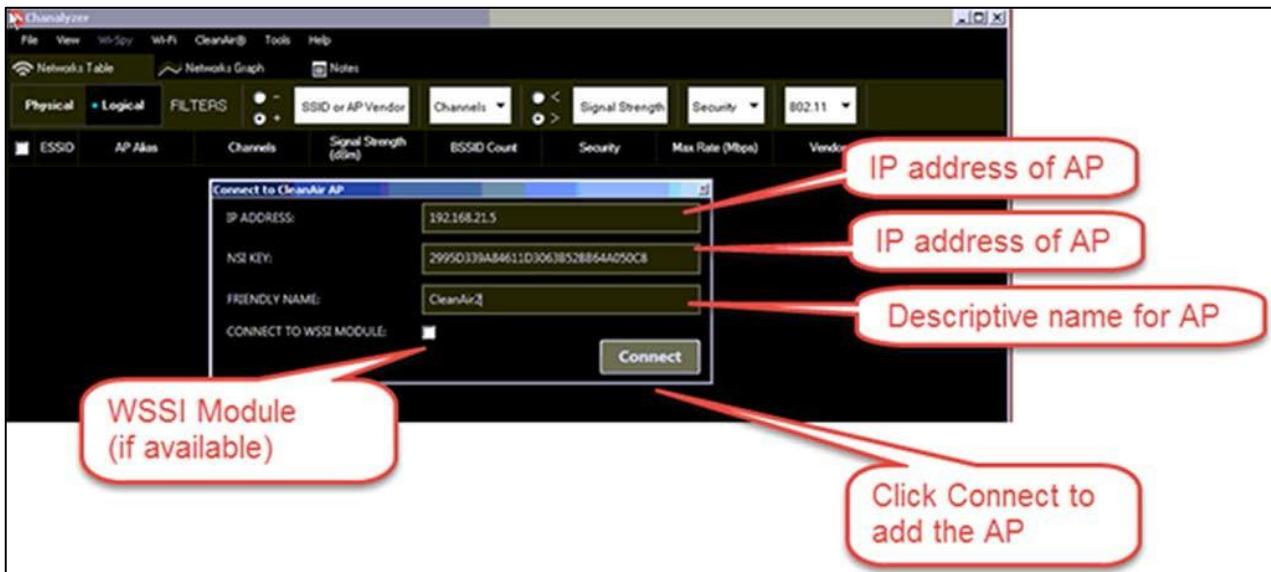


**Step 2** From the Metageek Chanalyzer dashboard, select **Clean Air > Connect to CleanAir AP** located in the menu.

**Step 3** Add the centralized AP to metageek Chanalyzer. The information entered will allow Chanalyzer to communicate and extract information from the centralized AP. The information captured will be used to analyze the RF environment for possible sources of interference.

Enter the following information:

- **IP ADDRESS: #####.#####.#####.#####**
  - This is the IP address of the centralized AP. Chanalyzer uses this information to communicate with the AP.
  - Use information from the preview task.
- **NSI KEY: XXXXXXXXXXXX**
  - Network Spectrum Interface key is used to allow external analysis tools to access the AP remotely.
  - Use information from the preview task.
- **FRIENDLY NAME: CleanAir\_x**
  - The friendly name is used as a descriptive name of the AP - it is not required to be the hostname of the AP.
- **CONNECT TO WSSI MODULE: unchecked**
  - The Cisco Wireless Security and Spectrum Intelligence (WSSI) field-upgradeable module is a dedicated radio that off-loads all monitoring and security services from the client/data serving radios to the security monitor module. This not only allows for better client performance but also reduces costs by eliminating the need for dedicated monitor mode access points and the Ethernet infrastructure required to connect those devices into their network. Not all Cisco APs have this module installed. If you have a Cisco APs with the WSSI module you would check the CONNECT TO WSSI MODULE when adding an AP to metageek Chanalyzer.

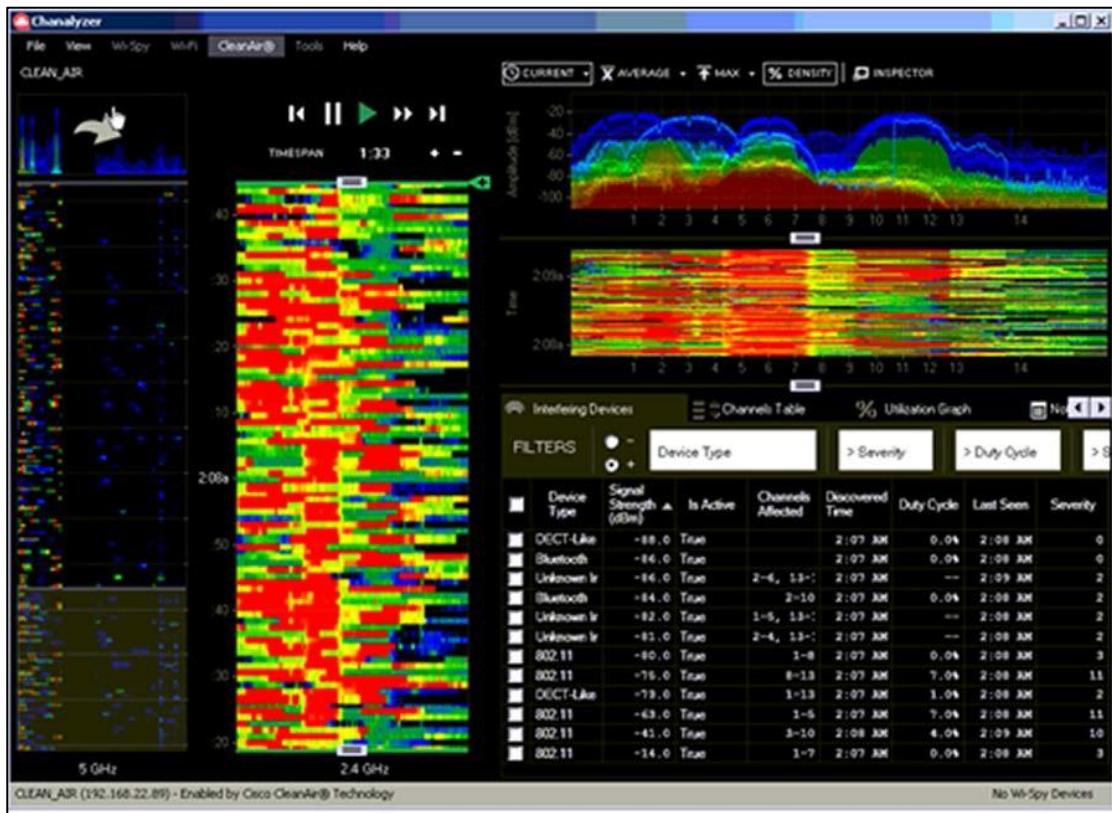


**Step 4** Click the **Connect** button. You will see metageek Chanalyzer connecting the centralized AP.



**Note** Chanalyzer may minimize after connecting.

**Step 5** Once connected you can verify metaGeek Chanalyzer connected to the AP by reviewing the RF information displayed on the screen. In the next lab activity we will perform a passive site survey and locate the RF interference device(s).



**Step 6** Close Chanalyzer when done.

### Activity Verification

You have successfully completed this task when you attain this result:

- You have configured metageek Chanalyzer – spectrum analyzer software to communicate with your centralized AP.
- You have connected metageek Chanalyzer to the Cisco Clean Air AP and viewed the screen.

## Task 3: Load RF capture information into metageek Chanalyzer - spectrum analyzer software.

### Activity Procedure

In this task, the passive site survey has been completed and the data collected has been saved. Based on your busy schedule, you decide to return to your office to analyze the captured RF information offline. This will require loading the saved data capture file into the spectrum analyzer software.

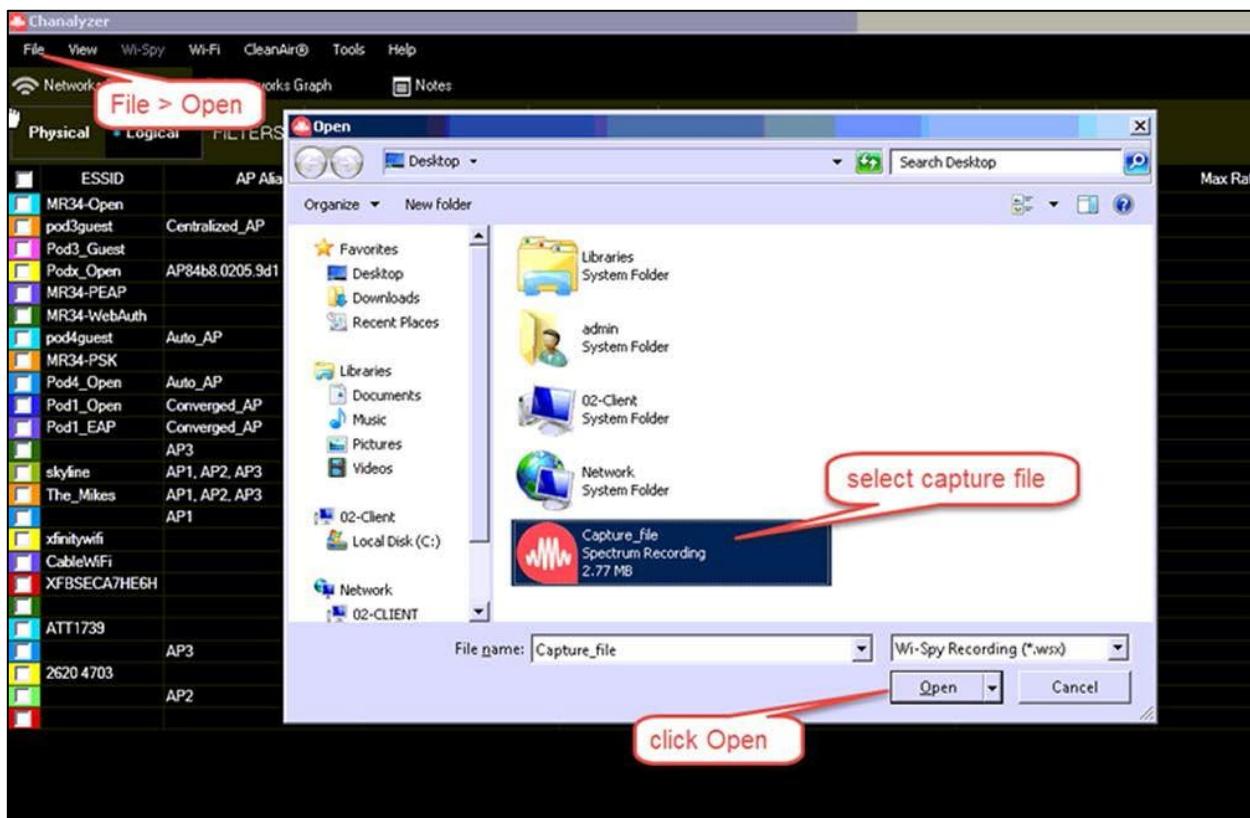
---

**Note** The lower case “x” in a command will be your pod number, ex: pod 1, x=1

---

Complete these steps:

- Step 1** From the Admin PC, connect to the Metageek Chanalyzer software shortcut located on the desktop.
- Step 2** From the Metageek Chanalyzer dashboard, select **File > Open**. Select the **Capture\_file.wsx** file from the Client PC desktop and click **Open**.



### Activity Verification

You have successfully completed this task when you attain this result:

- You have loaded the RF capture file into Metageek Chanalyzer – spectrum analyzer software.

## Task 4: Analyze RF capture information into Metageek Chanalyzer - spectrum analyzer software.

### Activity Procedure

In this task, you have loaded the saved data capture file into the spectrum analyzer software. It is now time to begin analyzing the information to locate the RF interference device(s).

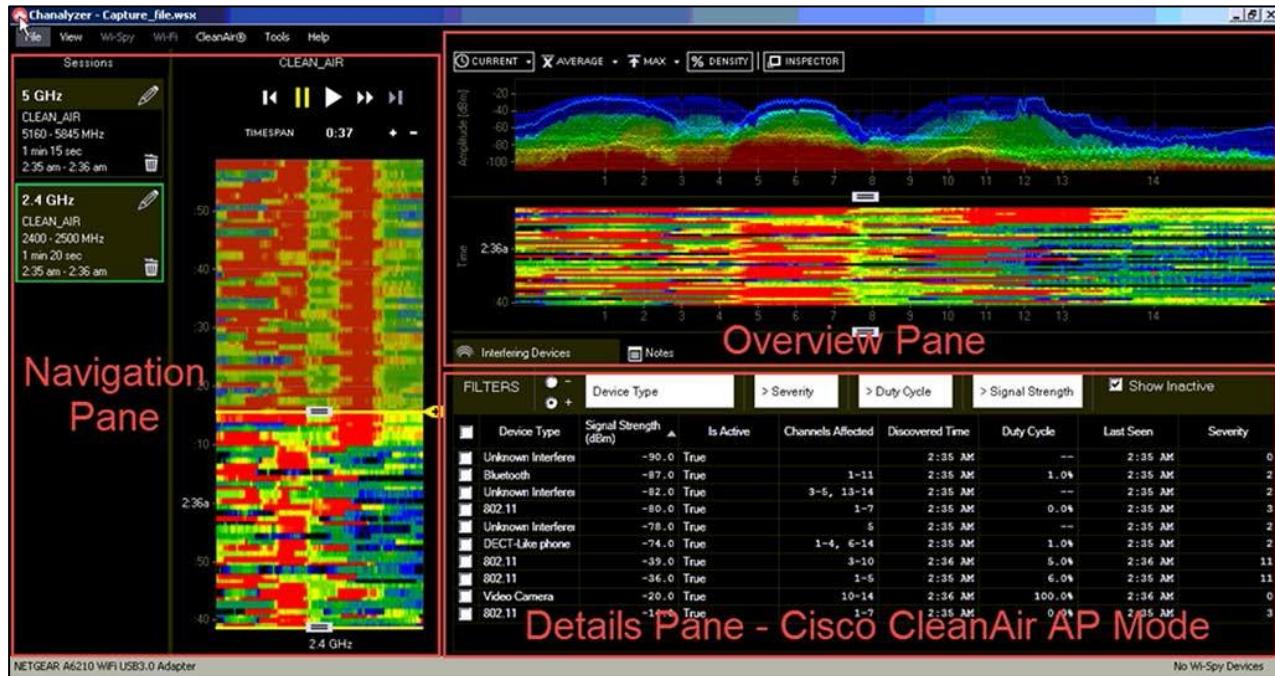
---

**Note** The lower case "x" in a command will be your pod number, ex: pod 1, x=1

---

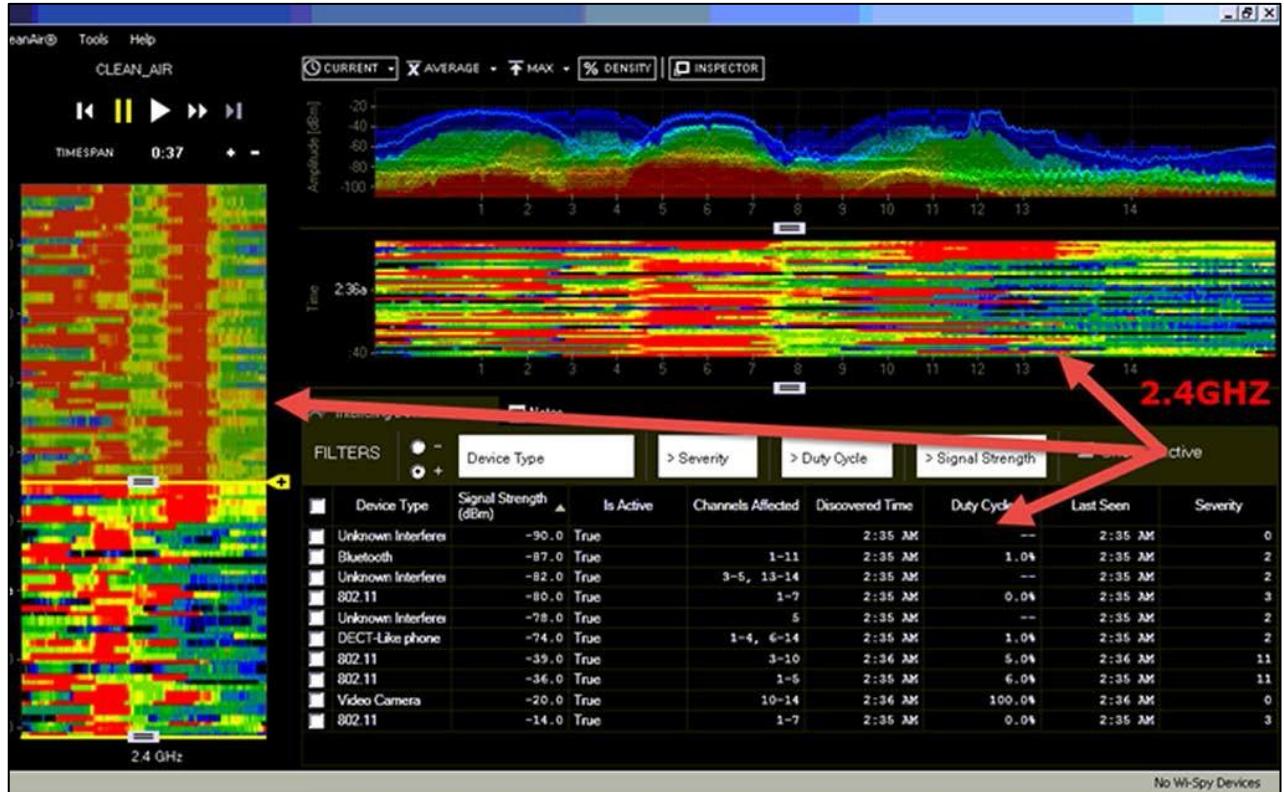
Complete these steps:

- Step 1** After loading the capture file, let's take some time to view and understand the metageek Chanalyzer graphical interface.
- **Navigation Pane:** This provides controls for browsing Wi-Fi capture sessions or recordings.
  - **Overview Pane:** This pane, located at the top right of the Navigation pane, contains the Waterfall and Density views.
  - **Details Pane:** When connected to a CleanAir AP, Chanalyzer will begin populating the Interfering Devices table with any non-Wi-Fi transmitters that are detected. The table is fully filterable by Device Type, Severity, Duty Cycle, and Signal Strength.



## Navigation Pane

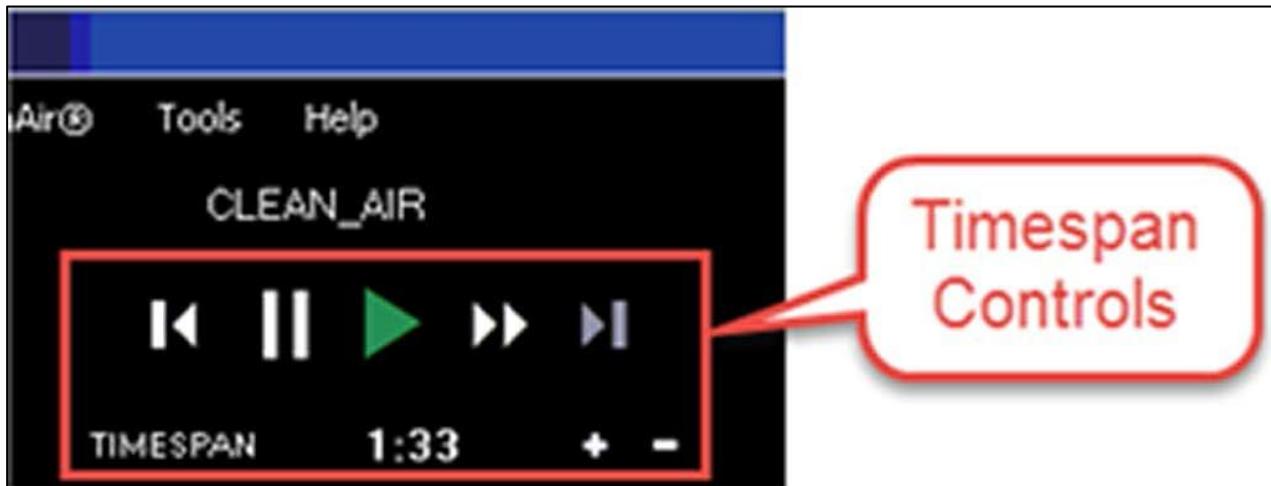
- Step 2** From the **Navigation** pane, locate the **Session Navigator**, click **2.4GHz** to display the 2.4GHz band information on the screen.
- Step 3** From the **Navigation** pane, locate the **Session Navigator**, click the **pencil** icon to edit the session name. Change the name of the session to **ABC-2.4GHz**.



- The **Session Navigator** is used to select the session to be displayed in Chanalyzer. The selected session will have a green box around it.

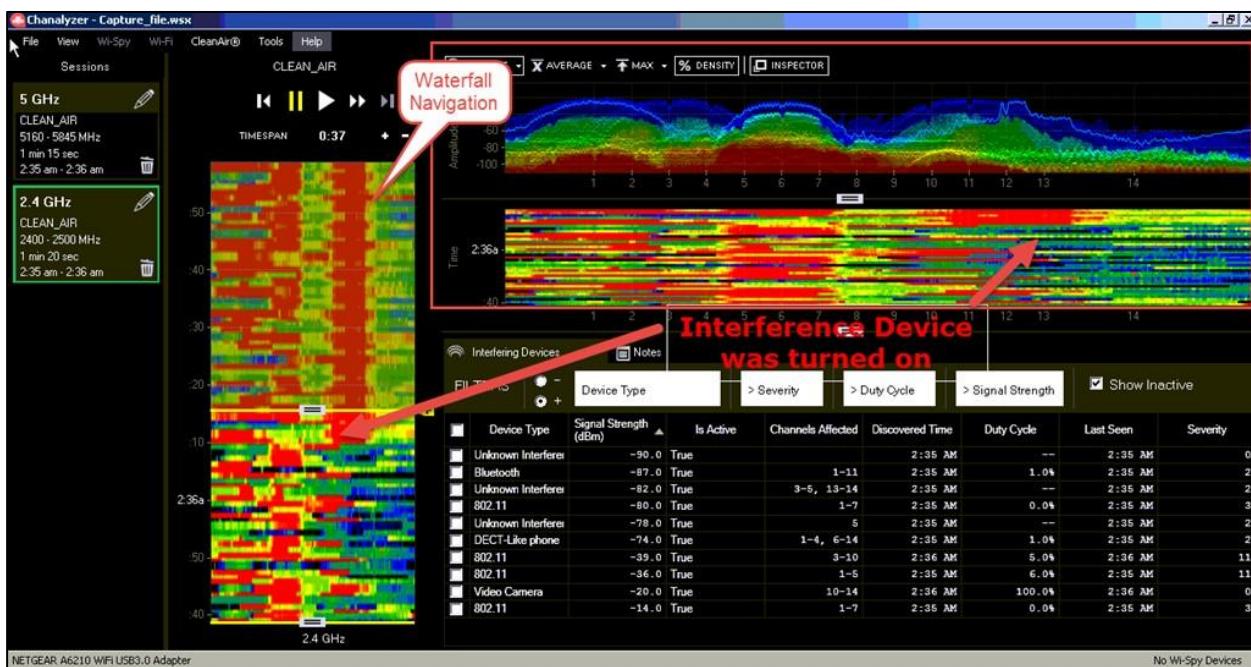
- **Sessions** can be renamed to represent various points in a recording. This feature is primarily used to identify locations however it can also be used to identify smaller frequency ranges. It can be helpful to rename sessions to help you navigate through several surveys.

**Step 4** From the **Navigation** pane, locate the **Timespan Controls**, and click the **Play** button to begin the playback of the capture file from the passive site survey.



The **Timespan controls** adjust the length of time users see in the **Overview** and **Details** panes. Timespan adjustments allow users to narrow in on anomalies and moments in time when WLAN performance suffered. The playback buttons are used to **Play**, **Pause**, **Rewind**, and **Fast Forward** while viewing a capture. The playback controls can also aid in selecting smaller time spans in the waterfall navigation.

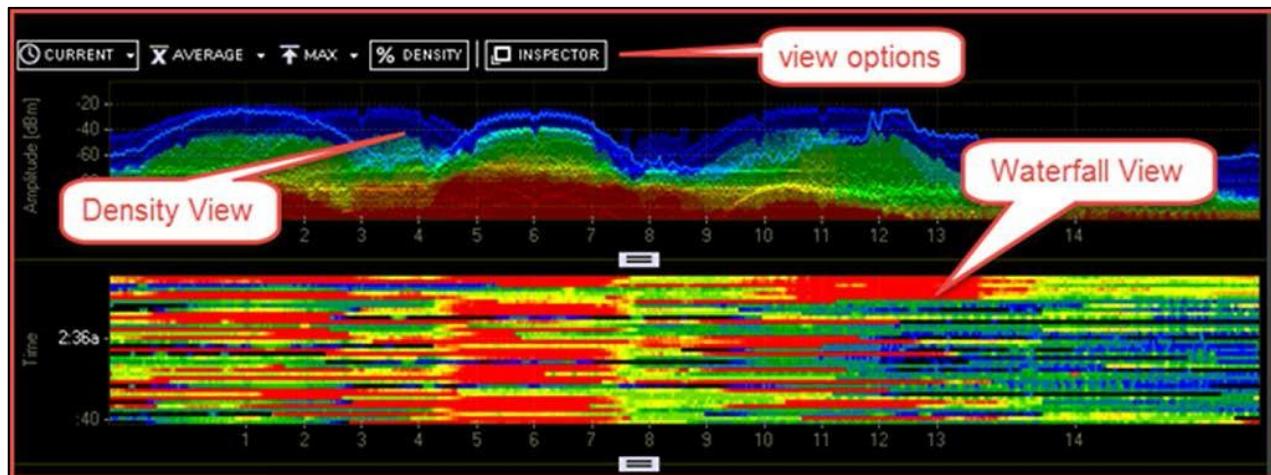
**Step 5** From the **Navigation** pane, locate the **Waterfall Navigation** section, double-click a point on graph where the **bright red begins** (2:36a) is around the point in the capture an interference device was turned on. This double-click will move you to a specific time of the capture.



The **Waterfall Navigation** section displays a smaller vertical view of the **Overview Pane's Waterfall View**. The waterfall graphs amplitude over time for each frequency in the selected ISM band.

### Overview Pane

- Step 6** It may be necessary to replay the capture file. Return to the **Timespan Controls**, rewind and begin playing the capture again.
- Step 7** From the **Overview Pane** on the right side of the screen, let's take some time to review the **Density View** of captured information. The interference device was turned on around **2:36** of the capture. There are several view options available. All of the display options can be toggled on and off as needed, and the trace colors customized. Users can employ combinations of these options to troubleshoot more efficiently.



- The **Density View** displays how often a signal is detected at a specific amplitude. After a short time of gathering data, patterns begin to emerge in the Density View. A density map view enables the user to quickly identify packet-based and analog patterns that may be interfering with your network.
- This view emphasizes how constant noise is across the spectrum. At any given point, Chanalyzer assigns a color based on how much of the energy in a range of time is above that point. If 50% of all the activity is above an amplitude point, Chanalyzer colors it red. This display option is especially useful in understanding just how constant interference is within a given range of time.
- The **Density View** has several view options. All of the display options can be toggled on and off as needed, and the trace colors customized. Users can employ combinations of these options to troubleshoot more efficiently.

- Step 8** It may be necessary to replay the capture file. Return to the **Timespan Controls**, rewind and begin playing the capture again.

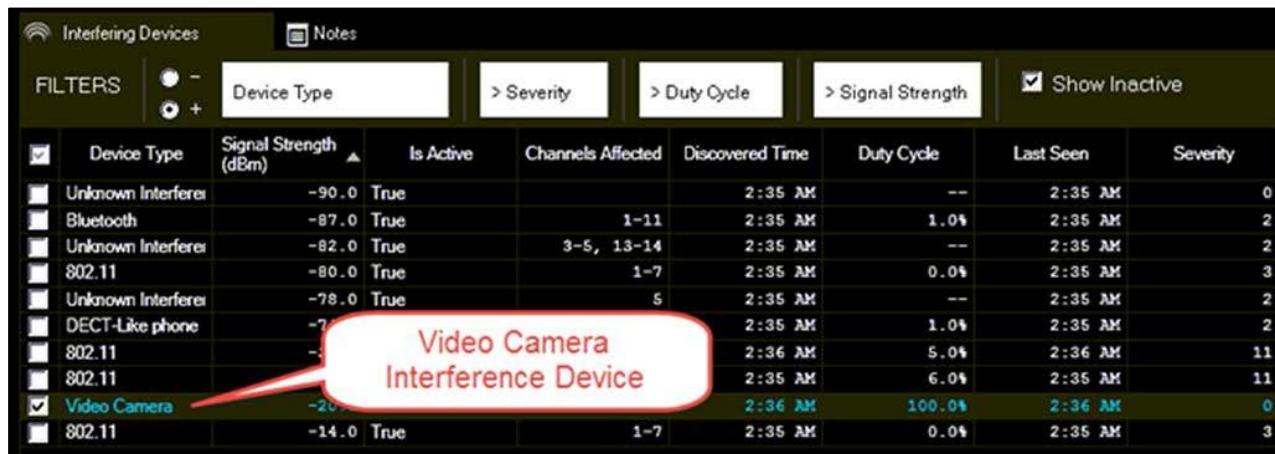
- Step 9** From the **Overview Pane** on the right side of the screen, let's take some time to review the **Waterfall View**. At roughly 2:36 the interference device was turned on. Notice the bright red consolidation on the right side of the **Waterfall View**.

The **Waterfall View** uses a color scale to represent amplitude levels – low levels are dark blue, while high amplitudes are bright red. This emphasizes instances where wireless devices like cordless phones or microwaves may have changed the spectrum. For example, when a microwave is turned on or a cordless phone changes channels, it is very noticeable in the Waterfall View.

## Details Pane (CleanAir AP Mode)

**Step 10** It may be necessary to replay the capture file. Return to the **Timespan Controls**, rewind and begin playing the capture again.

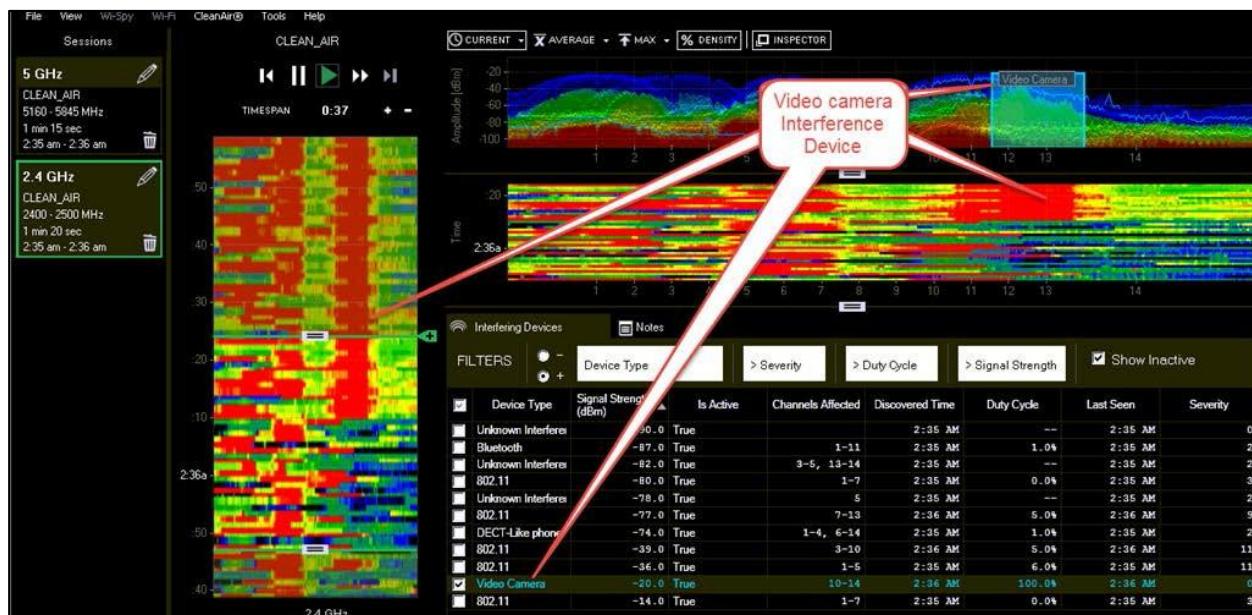
**Step 11** From the **Details Pane** on the lower right side of the screen, let takes some time to review the **Details Pane** of captured information for RF interference devices. The interference device was turned on around **2:36** of the capture. Click on **Interfering Devices** and then select the **Video Camera** checkbox from the list.



<input checked="" type="checkbox"/> Device Type	Signal Strength (dBm)	Is Active	Channels Affected	Discovered Time	Duty Cycle	Last Seen	Severity
Unknown Interferer	-90.0	True		2:35 AM	--	2:35 AM	0
Bluetooth	-87.0	True	1-11	2:35 AM	1.0%	2:35 AM	2
Unknown Interferer	-82.0	True	3-5, 13-14	2:35 AM	--	2:35 AM	2
802.11	-80.0	True	1-7	2:35 AM	0.0%	2:35 AM	3
Unknown Interferer	-78.0	True	5	2:35 AM	--	2:35 AM	2
DECT-Like phone	-77.0	True		2:35 AM	1.0%	2:35 AM	2
802.11	-76.0	True		2:36 AM	5.0%	2:36 AM	11
802.11	-75.0	True		2:35 AM	6.0%	2:35 AM	11
<b>Video Camera</b>	<b>-20.0</b>	<b>True</b>	<b>1-7</b>	<b>2:36 AM</b>	<b>100.0%</b>	<b>2:36 AM</b>	<b>0</b>
802.11	-14.0	True		2:35 AM	0.0%	2:35 AM	3

When connected to a CleanAir AP, Chanalyzer will begin populating the Interfering Devices table with any non-Wi-Fi transmitters that are detected. The table is fully filterable by Device Type, Severity, Duty Cycle, and Signal Strength.

**Step 12** Clicking the checkbox next to an interferer will display a visual indicator in the density view that spans the channels where the device is active. The spanning area will be filled in depending on the severity of the interference-- The higher the severity, the more opaque the overlay will be (and the more impact your users are likely to experience).



## ***Activity Verification***

You have successfully completed this task when you attain this result:

- You have performed an RF interference analysis of the loaded capture file.
- Using the information from the capture file, you have located the cause of the RF interference - video camera

# Glossary

## AES

Advanced Encryption Standard.

## EAP

Extensible Authentication Protocol. Framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences.

## IP

Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

## PEAP

Protected Extensible Authentication Protocol.

## PSK

preshared key. Shared secret key that is used during IKE authentication.

## SSID

Service Set Identifier.

## WLAN

wireless LAN. A LAN is a high-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

## WPA2

WiFi Protected Access 2.