cisco

Lab 6-2 Configuring a WLAN Controller via the Web Interface

Topology Diagram



Scenario

Continuing from the previous lab, you will now set up the WLAN controller through its web interface. Previously you configured it through the CLI.

Step 1

Set up all the switches as they were in the previous lab. Make sure that the WLAN controller and host also have the same configuration as before.

Step 2

1 - 15

On the host, open up Internet Explorer and go to the URL "https://172.16.1.100". This is the secure method of connecting to the management interface of the WLAN controller. You can also use

"http://172.16.1.100" since we previously enabled regular insecure HTTP access in the CLI for Lab 6.1. If you connect to the secure address, you may be prompted with a security warning. Click **Yes** to accept it and you will be presented with the login screen for the WLAN controller. Click **Login** and an authentication dialog box will appear.



Figure 2-1: Authentication Dialog Box for WLAN Controller Web Access

Use "cisco" as both the username and password. You configured these in the previous lab. Click **OK** to get to the main page of the graphical user interface (GUI). You are then presented with the monitor page for the WLAN controller.

Cisco - Microsoft Internet	t Explorer								-	a ×	
File Edit View Favorites	Tools Help									1	
🔇 Back 🝷 🕤 👻 😰 🦿	🏠 🔎 Search 🛭 👷 Favorites 🛛 🦑) 🔝 - 🗞 🗔									
Address 🙆 https://172.16.1.1	100/screens/frameset.html								💌 🛃 Go 🛛 Li	inks »	
CISCO SYSTEMS								Save Config	uration Ping Logout Ref	fresh	
adhu adhu	MONITOR WLANS		VIRELESS SEG	CURITY	MANAGEMENT	COMMANDS	HELP				
										_	
Monitor	summary										
Summary											
Statistics	Controller Summary						Rogue Summary				
Ports	Management IP Address		172.16.1	.100			Active Rogue APs	2	Detail		
Wireless Rogue APs Known Rogue APs Rogue Clients Adhoc Rogues 802.116 Kadios 802.111b/g Radios Clients RADIUS Servers	Software Version		4.0.179.3	11			Active Rogue Clients	1	Detail		
	System Name		Cisco_49	0. h a una	10		Adhoc Rogues	0	Detail		
	System Time		U days, J	10 nours,	12 minutes		Rogues on Wired Network	0			
	System Time		Enabled	10 04.30.	.30 2000						
	802.11b/g Network State	3	Enabled				Top WLANs				
	Access Boint Summa	Annual Delat Organization					WLAN	# of Clien	ts by SSID		
	Access Forne outrinit	ur y					conppod	U	Detail		
		Total	Up		Down						
	802.11a Radios	2	0 2	•	0	Detail	Most Recent Traps				
	802.11b/g Radios	2	0 2	•	0	Detail	RF Manager updated Channel f	for Base Radio MAC: 00:1			
	All APs	2	• 2	•	0	Detail	Rogue AP : 00:13:60:00:34:90 detected on Base Radio				
							Rogue AP : 00:60:1d:f0:a6:26 detected on Base Radio				
	Client Summary						AP's Interface:1(802.11a) Ope	ration State Up: Base Rac			
	Current Clients		1		Detail		AP's Interface:0(802.11b) Operation State Up: Base Rac				
	Excluded Clients		0	0 Detail		L		View All			
	Disabled Clients		0	0 Detail							
							This page refreshes every 30 seconds.				
(i) Done									🔒 🍘 Internet	_	

Figure 2-2: WLAN Controller Monitor Page

Make sure you see 2 access points under the "Access Point Summary" part of the page. You may also see it detecting rogue access points if your lab has other wireless networks around it; this behavior is normal. You can also see various port controller and port statistics by clicking their respective links on the left-hand menu on the screen.

Step 3

The next task in configuring WLANs is to add in the logical interfaces on the WLAN controller corresponding to VLANs 2 and 3. To do this, click the **Controller** link on the top of the web interface. Then, click **Interfaces** link on the left side bar.

🖉 Cisco - Microsoft Internet Exp	olorer						
File Edit View Favorites Iools Help							
🔇 Back 🔻 🕥 👻 😰 🏠 🔎 Search 👷 Favorites 🛛 😥 🔹 😓							
Address 🕘 https://172.16.1.100/s	creens/frameset.html				Go Links »		
CISCO SYSTEMS			Save Configuratio	on Ping Log	out Refresh		
authorithus	MONITOR WLANS CONTROLI	LER WIRELESS	S SECURITY N	IANAGEMENT	COMMANDS		
Controller	Interfaces			Ne	w		
General Inventory	Interface Name	VLAN Identifier	IP Address	Interface Type			
Interfaces	ap-manager	100	172.16.100.100	Static	Edit		
Internal DHCP Server	management	untagged	172.16.1.100	Static	Edit		
Mobility Management Mobility Groups Mobility Statistics	virtual	N/A	1.1.1.1	Static	Edit		
Ports							
Master Controller Mode							
Network Time Protocol							
QoS Profiles							
e				🥑 Internet			

Figure 3-1: Interface Configuration Page

Click the **New...** link to create a new interface. Give the new interface a name of VLAN2 and VLAN number 2. Click **Apply** to submit the parameters.

🖉 Cisco - Microsoft Internet Ex	plorerX							
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> i	ools Help 🥂							
🔇 Back 🔻 🕥 👻 😰 🏠 🔎 Search 👷 Favorites 🛛 🧔 🗸 🍒 🚍								
Address 🙆 https://172.16.1.100/s	screens/frameset.html 🔽 🎅 Go 🛛 Links 🎽							
CISCO SYSTEMS	Save Configuration Ping Logout Refresh							
	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS							
Controller	Interfaces > New < Back Apply							
General	Interface Name VLAN2							
Inventory								
Interfaces	VLAN Id 2							
Internal DHCP Server								
Mobility Management Mobility Groups Mobility Statistics								
Ports								
Master Controller Mode								
Network Time Protocol								
QoS Profiles								
I Cone	📄 📄 👘 Internet							

Figure 3-2: Creating a New VLAN Interface

On the next page, configure the IP address shown in the diagram. Also configure this on physical port 1, since that is the port trunked to the switch. After you have entered in all the changes, click **Apply**. Click **OK** to the warning box that comes up. This warning says that there may be a temporary connectivity loss on the APs while changes are applied.

🖉 Cisco - Microsoft Internet Exp	plorer						_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ools <u>H</u> elp						
🔇 Back 🝷 🕘 👻 😰 🐔	🔎 Search 📌 Favorites 🤞	3 🔗 😪 🕞					-
Address 🙆 https://172.16.1.100/s	creens/frameset.html				•	🔁 Go	Links »
CISCO SYSTEMS				Save Configur	ation Ping	Logout	Refresh
	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	т сом	IMANDS
Controller	Interfaces > Edit				< Back	Appl	у
General							
Inventory	General Informatio	n					
Interfaces	Interface Name	VLAN2					
Internal DHCP Server	Tubuda a Addus a						
Mobility Management			_		-		
Mobility Statistics	VLAN Identifier	2					
Ports	IP Address	172	.16.2.100]			
Master Controller Mode	Netmask	255	.255.255.0]			
Network Time Protocol	Gateway	172	.16.2.1				
QoS Profiles	Physical Informatio	in					
	Port Number	1			-		
	Configuration				-		
	Quarantine						
	DHCP Information				_		
	Primary DHCP Server	. 172	.16.2.1				
	Secondary DHCP Ser	ver]			
	Access Control List				-		
	ACL Name	non	e 💌				
	Note: Changing the Inte temporarily disabled and some clients.	rface parameters I thus may result	causes the WL in loss of conn	ANs to be ectivity for	-		
j Done					🔹 🚺 🕐 Inte	rnet	

Figure 3-3: Configuring VLAN Interface Properties

The new interface should appear in the interfaces list. Do the same configuration steps for VLAN 3.

🖉 Cisco - Microsoft Internet Exp	blorer						
File Edit View Favorites Tools Help							
🔇 Back 🔻 🕥 🖌 📓 🐔 🔎 Search 👷 Favorites 🖗 🖗							
Address 🙆 https://172.16.1.100/s	creens/frameset.html			~	🔁 Go 🛛 Links 🂙		
CISCO SYSTEMS			Save Configura	ation Ping	Logout Refresh		
	MONITOR WLANS CONTROLL	ER WIRELE	SS SECURITY	MANAGEMEN	T COMMANDS		
Controller	Interfaces				New		
General	- · · · ·	VLAN	70.111	Interface			
Inventory	Interface Name	Identifier	IP Address	Туре			
Interfaces	ap-manager	100	172.16.100.100	Static <u>E</u>	dit		
Internal DHCP Server	management	untagged	172.16.1.100	Static <u>E</u>	dit		
Mobility Management	virtual	N/A	1.1.1.1	Static <u>E</u>	<u>idit</u>		
Mobility Groups Mobility Statistics	vlan2	2	172.16.2.100	Dynamic <u>E</u>	dit <u>Remove</u>		
Ports							
Master Controller Mode							
Network Time Protocol							
QoS Profiles							
🕘 Done				💙 Inte	rnet //.		

Figure 3-4: Verify Existing VLAN Interfaces

🖉 Cisco - Microsoft Internet Exp	olorer						_ 🗆 X
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ools <u>H</u> elp						
🚱 Back 🝷 💮 👻 🖹 🐔	🔎 Search 🛭 👷 Favorites 🤄) 🔝 🌜 🗟					
Address 🙆 https://172.16.1.100/s	creens/frameset.html				•	🔁 Go	Links »
CISCO SYSTEMS				ave Configur	ation Ping	Logout	Refresh
	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	т сом	IMANDS
Controller	Interfaces > Edit			1	< Back	Appl	y
General							
Inventory	General Information	1					
Interfaces	Interface Name	VLAN3					
Internal DHCP Server	Interface Address						
Mobility Management Mobility Groups			_				
Mobility Statistics	VLAN Identifier	3					
Ports	IP Address	172	16.3.100				
Master Controller Mode	Netmask	255	255.255.0				
Network Time Protocol	Gateway	172	16.3.1				
QoS Profiles	Physical Information	n					
	Port Number	1					
	Configuration						
	Quarantine						
	DHCP Information						
	Primary DHCP Server	172	16.3.1				
	Secondary DHCP Serv	er 🗌					
	Access Control List						
	ACL Name	non	e 💌				
	Note: Changing the Inter temporarily disabled and some clients.	face parameters thus may result	causes the WL in loss of conn	ANs to be ectivity for			
Done					🔹 Inte	rnet	

Figure 3-5: Configuring the VLAN 3 Interface

Make sure both interfaces appear in the interface table.

🖉 Cisco - Microsoft Internet Exp	blorer				
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ools <u>H</u> elp				2
🔇 Back 🝷 🕘 🖌 💽 🐔 🔒	🔎 Search 🛛 👷 Favorites 🛛 🤣 🕶 🕯	\$ B			
Address 🙆 https://172.16.1.100/s	creens/frameset.html			•	🕑 🔁 Go 🛛 Links 🂙
CISCO SYSTEMS			Save Configur	ation Ping	Logout Refresh
	MONITOR WLANS CONTRO		ESS SECURITY	MANAGEMEI	NT COMMANDS
Controller	Interfaces				New
General				T-4	
Inventory	Interface Name	Identifier	IP Address	Туре	
Interfaces	ap-manager	100	172.16.100.100	Static	Edit
Internal DHCP Server	management	untagged	172.16.1.100	Static	Edit
Mobility Management	virtual	N/A	1.1.1.1	Static	Edit
Mobility Groups	vlan2	2	172.16.2.100	Dynamic	Edit Remove
Mobility Statistics	vlan3	3	172.16.3.100	Dynamic	<u>Edit</u> <u>Remove</u>
Ports					
Master Controller Mode					
Network Time Protocol					
QUS Promes					
Cone				🕎 Int	ernet //

Figure 3-6: Verifying VLAN Interfaces on the WLAN Controller

Step 4

Now, you can configure the WLANs corresponding to these VLANs. To do this, first click the **WLANs** link at the top of the page. This will show you all configured WLANs.



Figure 4-1: Viewing Existing WLANs

On the existing one, click **Edit** on the right of it. Remove the layer 2 security and change the interface to VLAN2. This will associate this WLAN with the correct VLAN.

🖉 Cisco - Microsoft Internet Ex	plorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u>	Iools <u>H</u> elp	🥂 🖉
🔾 Back 🝷 🕘 👻 📓 🐔	🔎 Search 👷 Favorites 🛛 🕢 🌜 📄	
Address 🙆 https://172.16.1.100/s	/screens/frameset.html	🔽 🄁 Go 🛛 Links 🌺
CISCO SYSTEMS		Save Configuration Ping Logout Refresh
	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	F COMMANDS HELP
WLANs	WLANs > Edit	< Back Apply
WLANS	WLAN ID 1	
WLANS AP Groups VLAN	WLAN SSID ccnppod	
	General Policies	Security Policies
	Radio Policy All	Laver 2 Security
	Admin Status 🔽 Enabled	
	Session Timeout (secs) 0	
	Quality of Service (QoS) Silver (best effort) 💌	Layer 3 Security None 🔹
	WMM Policy Disabled 💌	🗌 Web Policy *
	7920 Phone Support 🛛 🗌 Client CAC Limit 🔲 AP CAC Limit	
	Broadcast SSID 🔽 Enabled	* web policy count to word in continuing with
	Aironet IE 🛛 🗹 Enabled	IPsec and L2TP.
	Allow AAA Override 🛛 Enabled	** When client exclusion is enabled, a timeout
	Client Exclusion 🔽 Enabled ** 60	value of zero means infinity(will require administrative override to reset excluded
	Timeout Value (secs) DHCP Server 🗌 Override	clients) *** CKIP is not supported by 10xx APs
	DHCP Addr. Assignment 🗌 Required	
	Interface Name vlan2 💽	
	MFP Version Required 1	
	Generation Global MFP Disabled)	
	H-REAP Local Switching 🗌	
	* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.	
	Radius Servers	
	Authentication Servers Accounting Servers	-1
, (C) Done		

Figure 4-2: Edit the Configuration for WLAN 1

Click **Apply** and click **OK** to the warning box that comes up.



Figure 4-3: WLAN 1 without a Security Policy

Click New... and configure a WLAN for VLAN 3. Use the SSID "ccnplab".

🖉 Cisco - Microsoft Internet Ex	plorer							
<u>File Edit View Favorites I</u>	File Edit View Favorites Tools Help							
G Back ▼ G ▼ 🗶 🖁 G / >> Search 👷 Favorites 🚱 💋 ▼ G / Search 👷 Favorites 🚱 🖉 ♥ 🚱 🖻								
Aguress en https://172.16.1.100/	screens/rranesec.num					Save	Configuration Pin	
			WIRELESS	SECURITY		COMMANDS		g Logodt Konosh
WLANs	WLANs > New	COMINCELER	WINCELESS	Secondin	HANAGEMENT	COMMANDO	< Back	Apply
WLANS WLANS	WLAN ID	2 💌						
AP Groups VLAN	WLAN SSID	ccnplab						
Done								Internet

Figure 4-4: Adding a New SSID for WLAN 2

On this WLAN, configure the layer 2 security as Static WEP and use a 40 bit WEP key. Make the key index 2 and use a key of "cisco". Also, set the administrative status of the WLAN to enabled and change the interface name to VLAN3. When you are done, click Apply and you should see both WLANs in the WLAN list.

🛃 Cisco - Microsoft Internet Exp	plorer								_ 8	×
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u>	ools <u>H</u> elp									,
😋 Back 🔹 🕘 👻 😰 🐔	🔎 Search 🛭 👷 Favorites 🛛 🦑) 🔝 - 🕹 🖃								
Address 🙆 https://172.16.1.100/s	creens/frameset.html								💌 🄁 Go Links	»
CISCO SYSTEMS									Ping Logout Refresh	h
	MONITOR WLANS (CONTROLLER WIRELESS	SECURITY MANAGEME	NT COMMANDS	HELP					
WLANS	MERION Lanc									•
71211110	WLAN ID	2								
WLANs WLANs	WLAN SSID	conplab								
AP Groups VLAN	General Policies				Se	ecurity Policies				
	Radio Policy	All				Laver 2 Security	Static WER	-		
	Admin Status	Enabled				Edifor 2 booding	MAC Filtering			
	Session Timeout (secs) 0								
	Quality of Service (Qo	S) Silver (best effort) 💌				Layer 3 Security	None	1		
	WMM Policy	Disabled 💌					🔲 Web Policy *			
	7920 Phone Support	🗌 Client CAC Limit 📗	P CAC Limit							
	Broadcast SSID	🔽 Enabled				* Web Deliev expost by	a used in combination with	IRcoo		
	Aironet IE	🔽 Enabled				and L2TP.	e used in combination with	I IFSEC		
	Allow AAA Override	Enabled				** When client exclusion	on is enabled, a timeout v	alue of		
	Client Exclusion	Enabled ** 60	Value (secs)			reset excluded clients)	require autilitistrative of ted by LOVY ARE	vernue to		
	DHCP Server	Override	vulue (3003)			CKIP is not suppor	ted by Ioxx AFS			
	DHCP Addr. Assignmer	nt 🔲 Required								
	Interface Name	vlan3 💌								
	MFP Version Required	1								
	MFP Signature Generation	☑ (Global MFP Disabled)							
	H-REAP Local Switching	g 🗆								
	* H-REAP Local Switchi	ing not supported with IPSEC,	L2TP, PPTP, CRANITE and F	ORTRESS authenticati	ions.					
	Radius Servers									
		Authentication Servers	Accounting Servers							
	Server 1	none -	none 💌							
	Server 2	none 💌	none 💌							
	Server 3	none 💌	none 💌							
	Static WEP Parameters									
	802.11 Data Encryption	n Current Key: 40 bits V	EP Static Key (Key Index =	2)						
		Type Key Size Key	Index Encryption Key	Kev	Eormat					
		WEP 40 bits + 2 +	cisco	TASC						
	Allow Shared-Key	Enabled	, .		_					
Dama .	Authentication								Takaunak	•
Uoné Doné									1 Internet	

Figure 4-5: Configuring VLAN Association and Authentication for VLAN 3



Figure 4-6: Verifying Final WLAN Configuration

At this point, if you have a computer with a wireless card installed you should be able to see both SSIDs and connect to the WLANs/VLANs associated with them. Notice that each WLAN exists in a separate subnet, because each WLAN is in a separate VLAN.