IT Essentials 5.0 10.2.4.10 Lab - Configure Wireless Security

Introduction

Print and complete this lab.

In this lab, you will configure and test the wireless settings on the Linksys E2500.

Recommended Equipment

- Two computers with Windows 7 or Windows Vista or Windows XP
- An Ethernet NIC installed in computer 1
- A Wireless NIC installed in computer 2
- Linksys E2500 Wireless Router
- Ethernet patch cable

Step 1

Ask the instructor for the following information that is used during the lab.

Default Login Information: User Name (if any) _____

Password _____

Basic Wireless Settings:

Network Name (SSID) _____

Network Mode: _____

Channel: _____

Important: Only use configurations assigned by the instructor.

Note: Use computer 1 for all lab instructions unless stated.

Step 2

Connect computer 1 to an Ethernet ports on the wireless router with an Ethernet patch cable.

Plug in the power of the wireless router. Boot the computer and log in as an administrator.

Step 3

Open the command prompt.

Type ipconfig.

What is the IP address for the computer?

What is the default gateway for the computer?

Step 4

Open Internet Explorer and connect to the wireless router.

Type "admin" in the "Password:" field.

The "Setup screen" appears.

Click Wireless tab.

cisco.						Firmwar	e Version: 1.0.02
						Linksys E2500	E2500
Wireless	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status
	Basic Wireless 5	Settings	Wireless Security	Gu	est Access	Wireless MAC Filter	
Configuration View	🖲 Manual 🔘	Wi-Fi Protected	i Setup™			<u>Help</u>	
5 GHz Wireless Settings	Network Mode: Network Name (Channel Width: Channel: SSID Broadcast:	SSID): Ci	isabled visco55842 0 MHz Only uto (DFS) visco (DFS) Enabled Disa	• •			
2.4 GHz Wireless Settings	Network Mode: Network Name (Channel Width: Channel: SSID Broadcast:	SSID):	0 MHz Only uto v Enabled © Disa	• •			
			Save Se	ttings	Cancel Change	s	

Under the Wireless tab, click **Basic Wireless Settings** if it is not selected.

cisco.							Firmwa	ire Version: 1.0.02
							Linksys E2500	E2500
Wireless	Setup Wire	eless	Security	Acces Policy			Administration	Status
	Basic Wireless Settings	• 1	Wireless Security	<u>_</u> 1_	Guest Access	đ	Wireless MAC Filter	
Configuration View								
5 GHz Wireless Settings	◉ Manual © Wi-Fi P			11			<u>Help</u>	
o Gilz Witeless Settings	Network Mode: Network Name (SSID):	12	Disabled Cisco55842					
	Channel Width:	1	20 MHz Only		-			
	Channel:	1	Auto (DFS) 💌					
	SSID Broadcast:	0	Enabled 🔘 Disa	abled				
.4 GHz Wireless Settings	Network Mode:	l.	Mixed	•				
	Network Name (SSID):	Ī	Cisco1					
	Channel Width:		20 MHz Only		•]			
	Channel:		6 - 2.437GHZ 🔻					
	SSID Broadcast:		Enabled 🔘 Disa	abled				
			International Action of Action	The second s	BERTHER STREET			
			Save Se	ttings	Cancel Cl	ange	S	

Enter the following information for the 2.4 GHz wireless settings, unless stated otherwise by the instructor:

Network Mode: Mixed

Network Name (SSID): **Cisco#**, where # is a number assigned by the instructor Channel: **#**, where # is a number assigned by the instructor SSID Broadcast: **Enabled**

Click Save Settings > Continue.

Click the Wireless Security sub-tab.

Step 5

The "Wireless Security" screen appears.

ululu cisco.						Firmwa	re Version: 1.0.02
						Linksys E2500	E2500
Wireless	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status
	Basic Wireless	Settings	Wireless Security	I G	uest Access	Wireless MAC Filter	
5 GHz Wireless Security							
	Security Mode:	[Disabled		•	<u>Help</u>	
2.4 GHz Wireless Security							
	Security Mode:	1	WPA2 Personal		-		
	Passphrase:	C	lscoL@b102410				
			Save Se	ttings 👆	Cancel Change	s	

Enter the following information for the 2.4 GHz wireless security settings, unless stated otherwise by the instructor:

Security Mode: **WPA2 Personal**. Passphrase: **C!scoL&b102410**

Click Save Settings > Continue.

Keep Internet Explorer open to the Linksys router.

Step 6

Log in to computer 2, the wireless computer, as the administrator.

Connect to the wireless network. If asked for a security key or passphase enter: C!scoL&b102410

Open the command prompt.

Type ipconfig /all.

What is the IP address of the wireless NIC?

What is the physical address of the wireless NIC?

Type ping IPaddress. Where IPaddress is the IP address of computer 1.

Was the ping successful?

Keep the command prompt window open.

Step 7

From computer 1, make sure Internet Explorer is active.

Under the Wireless tab, click Guest Access.

						Linksys E2500	E250
Wireless	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status
				Gu	est Access		
	Allow Guest Ad Guest Network Guest Passwo Total Guests A SSID Broadcas	Name: C rd: g llowed: t. @	yes © no isco1-guest uest 5 ▼ Enabled © Disc		Change		
			t to your wireless d entering the gu				

Why would you allow guest access?

uluilu cisco								Firmwai	e Version: 1.0.02
								Linksys E2500	E2500
Wireless	Setup	Wirel	ess Se	ecurity	Access Policy	Application Gamin		Administration	Status
	Basic Wir	eless Settings	l Wirele	ess Security	Gi	uest Access	1	Wireless MAC Filter	
Wireless MAC Filter	C Enab	ed 🖲 Disab	led					Help	
		ent PCs listed b it PCs listed be							
MAC Address Filter List	Wire	less Client List							
	MAC 01:	0:00:00:00:00	0:00 MAG	17: 00:00	:00:00:00:0	0			
	MAC 02:	0:00:00:00:00	0:00 MAC	18: 00:00	:00:00:00:0	00			
	MAC 03:	00:00:00:00:00	0:00 MAC	19: 00:00	:00:00:00:0	00			

Under the Wireless tab, click Wireless MAC Filter.

Step 8

The "Wireless MAC Filter" screen appears.

CISCO.						Firmwar	e Version: 1.0.
						Linksys E2500	E2500
Wireless	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status
	Basic Wir	eless Settings 🛛 🛔	Wireless Sec	urity Gu	est Access	Wireless MAC Filter	
Wireless MAC Filter	6						
	Enable	led Oisabled				<u>Help</u>	
		ent PCs listed below hit PCs listed below to	Charles and the second second		twork.		
MAC Address Filter List	© Perm		Charles and the second second		twork.		
NAC Address Filter List	© Perm	nit PCs listed below to	o access the wi				
MAC Address Filter List	© Perm	nit PCs listed below to	MAC 17: 0	eless network.	0		

Select Enabled > Prevent > click Wireless Client List.

The "Wireless Client List" screen appears.

cisco.						
Wireless Client List Sort By	IP Address 🔹					
	Client Name	Interface	IP Address	MAC Address	<mark>Status</mark>	Save to MAC Address Filter List
	Braxton-PC	Wireless-G	192.168.1.29	00:13:CE:8A:3C:14	Connected	
	Add	Refresh	Clo	ose		I internet

Select Save to MAC Address Filter List check box for computer 2.

Click Add.

What MAC address is now listed?

Click Save Settings > Continue.

Step 9

From computer 2:

In the command prompt window type **ping** *IPaddress*. Where *IPaddress* is the IP address of computer 1.

Was the ping successful?

Step 10

From computer 1, click the **browser** so it is activated.

Click Administration on the main tab bar.

The "Management" screen appears.

				Linksys E2500	E2500
Administration	Setup Wireles	s Secu	rity Access Applications & Policy Gaming	Administration	Status
	Management Log	Diagno	stics Factory Defaults	Firmware Upgrade	
Management					
Router Access	Router Password:			<u>Help</u>	
	Re-Enter to Confirm:	••••••	•••••		
ocal Management Access	Access via:	ИТТР	HTTPS		
	Access via Wireless:	Enabled	Disabled		
Remote Management	Remote Management:	C Enabled	Disabled		
Access	Access via:		HTTPS		
	Remote Upgrade:	C Enabled	Disabled		
	Allowed Remote IP Address:	Any IP Ad	dress		
		00.0	0.0.0 to 0		
	Remote Management Port:	8080			
Advanced features	SIP ALG:	C Enabled	Disabled		
UPnP	UPnP:	Enabled	© Disabled		
	Allow Users to Configure:	Enabled	O Disabled		
	Allow Users to Disable Internet Access:	C Enabled	Disabled		
Back Up and Restore	Back Up Configuration	R	lestore Configuration	_	
			Save Settings Cancel Chang		

Highlight the Router Password and type ITEv5.0. Type the same password in Re-Enter to Confirm.

Click Cancel Changes. Do not save the new password.

Click **Security** on the main tab bar.

Step 11

The "Firewall" screen appears.

						Linksys E2500	E250
Security	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status
Firewall Internet Filter	Firewall I IPv6 SPI Firewe Protection: IPv4 SPI Firewe Protection: IPv6 SPI Firewe Protection:) all () I	Enabled 💿 Dis Enabled 💿 Dis			Help	
Web Filter	Filter Intern Only	net NAT Redirecti					

By default, SPI Firewall Protection is Enabled.

What Internet Filters are available?

What Web Filters are available?

Click Applications & Gaming on the main tab bar.

Step 12

The "Applications & Gaming" screen appears.

ابدار cisco								Firmware	e Version: 1.0.02
								Linksys E2500	E2500
Applicat Gam		Setup	Wireless	Security	Access Policy	Applicati Gami		Administration	Status
Gail	illig	Single Port Forwarding		Port Range Forwarding		Port Range Triggering	1	DMZ IPv6 Firewall	QoS
Single Por	t Forwarding								
Appli	cation Name	External Port	Internal Port	Protocol	To IP Ad	Idress	Enable	d <u>Help</u>	
	None -				192.168.	1. 0	1		
	None 🔻		[192 . 168 .	1. 0			
	None 🔻	() ()			192 . 168 .	1. 0			
	None 🔻	2000			192 . 168 .	1. 0			
	None 🔻		120		192 . 168 .	1. 0			
		0	0	Both 🔻	192 . 168 .	1. 0			
		0	0	Both 🔻	192 . 168 .	1. 0			
		0	0	Both 🔻	192 . 168 .	1. 0			

Click Single Port Forwarding.

cisco.								Firmwa	ire Version: 1.0.02
								Linksys E2500	E2500
Applicatio Gamir		Setup	Wireless	Security	Access Policy	Applicati Gami		Administration	Status
Canin	ig	Single Port Forwarding	ţ.	Port Range Forwarding		Port Range Triggering	I	DMZ IPv6 Firewall	QoS
Single Port F	orwarding								
Applicat	ion Name	External Port	Internal Port	Protocol	To IP Ad	dress	Enable	d <u>Help</u>	
	None 🔻			 .	192.168.	1. 0			
	None	[- ee]			192 . 168 .	1. 0			
	SMTP				192.168.	1. 0			
1	ONS	2000		192220	192.168.	1. 0			
F	FFTP Finger		10		192.168.	1. 0			
	HTTP POP3	0	0	Both 🔻	192 . 168 .	1. 0	0		
	NNTP SNMP	0	0	Both 👻	192 . 168 .	1. 0			
	PPTP	0	0	Both 🔻	192 . 168 .	1. 0			

To forward an otherwise blocked port to a specific computer, select Application Name > FTP.

	i i i						
	Forwarding						
Applic	ation Name	External Port	Internal Port	Protocol	To IP Address	Enabled	Help
	FTP 🔻	21	21	TCP	192 . 168 . 1. 2		
	None 🔻	(<u>— e—</u> e —)			192 . 168 . 1. 0		
	None 🔻	2000			192 . 168 . 1. 0		
	None 🔻	1000	112		192 . 168 . 1. 0		
	None 🔻				192 . 168 . 1. 0		
		0	0	Both 🔻	192.168.1.0		
		0	0	Both 🔻	192.168.1.0		
		0	0	Both 🔻	192.168.1.0		
		0	0	Both 🔻	192 . 168 . 1. 0		
		0	0	Both 🔻	192.168.1.0		
		0	0	Both 🔻	192 . 168 . 1. ⁰		
		0	0	Both 🔻	192.168.1.0		
		0	0	Both 🔻	192.168.1. ⁰		
		0	0	Both 🔻	192 . 168 . 1. 0		
		0	0	Both 🔻	192.168.1.0		
		0	0	Both 🔻	192 . 168 . 1. 0		
		0	0	Both 🔻	192.168.1.0		
		0	0	Both 🔻	192.168.1.0		
		0	0	Both 💌	192 . 168 . 1. 0		
		0	0	Both 🔻	192.168.1.0		
	- 11						

Type the last octet of the IP address for the computer and then click **Enabled** checkbox.

Click Cancel Changes. Do not save the new setting.

Click Port Range Triggering.

Step 13

The "Port Range Triggering" screen appears.

								Links	ys E2500	E2500
Applications & Gaming	Setup	Wireless	less Security		Access Applications & Policy Gaming		Administration		Status	
	Single Port Forwarding	ţ,		rt Range warding	đ	Port Range Triggering		DMZ	IPv6 Firewall	Qo!
Port Range Triggering	Applicatio	n Name	Trigg	gered Range	Forwa	rded Range	Enabled		<u>Help</u>	
			0	to 0	0	to 0				
	a de la companya de l		0	to 0	0	to 0				
	-		0	to 0	0	to 0				
	1		0	to 0	0	to 0				
			0	to 0	0	to 0				
			0	to 0	0	to 0				
			0	to 0	0	to 0				
			0	to 0	0	to 0				
	. J		0	to 0	0	to 0				

To open an otherwise blocked port, type in the application name **IRC**. Then type the Triggered Range **6660 to 7000**, Forwarded Range **113 to 113** and then click **Enabled** checkbox.

cisco.												Firmware	Version	1.0.02
										L	inksy	s E2500	E2	500
Applications & Gaming	Setup	Wireless	Se	ecur	ity	Acces Policy		Applica Garr		Admin	istrat	ion	State	ıs
Gaming	Single Port Forwarding	I,	Port Forw			1		ort Range Friggering	I	DMZ	1	IPv6 Firewall	Ŀ	QoS
Port Range Triggering													-	
	Applicatio	n Name	Trigge	ered	Range	Forwa	rde	d Range	Enabled		H	<u>elp</u>		
	IRC		6660	to	7000	113	to	113						
]	0	to	0	0	to	0						
],	0	to	0	0	to	0						
			0	to	0	0	to	0						
			0	to	0	0	to	0						
)	0	to	0	0	to	0						
			0	to	0	0	to	0						
			0	to	0	0	to	0						
			0	to	0	0	to	0						
	1]	0	to	0	0	to	0						
				1	Save Se	ttings	11	Cancel	Changes	lin.				

Click Cancel Changes. Do not save the new setting.

Click Access Policy.

Step 14

The "Parental Controls" screen appears.

Access Policy	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status
	Parental Controls						
Parental Controls							
	Parental Controls	:	Enabled 🔘 🛛	isabled		<u>Help</u>	
Target Devices	Restrict Internet a	access on				_	
			_				
	Add Remov	Rename]				
Schedule	Block Internet Ac	cess					
	Never O A	lways 🔘 Spe	cific times				
	School nights	9:00 PM		AM -			
	Weekends	Midnight	* to 7:00	AM 👻			
Block Specific Sites	URL 1:						
	BOADDAN			-			
	URL 2:			-			
	URL 3:			-			
	URL 4:						
	URL 5:						
	URL 6:						
	URL 7:						
	URL 8:						
			Save	Settings	Cancel Change	s	

Select Enable > Add.

The "Set up parental control for:" window opens.

iliiilii cisco.		
Parental Controls	Set up parental controls for: Student01 BRAXTON-PC	

Select a computer name, **Computer2 > OK**.

Access Policy	Setup	Wireless S	iecurity	Access Policy	Applications & Gaming	Administration	Status
	Parental Controls						
Parental Controls							
	Parental Controls:	Enab	led 🔘 Disa	bled		<u>Help</u>	
Target Devices	Restrict Internet ad	ccess on					
	BRAXTON-PC						
	Add Remove	Rename					
	Add	Rename					
Schedule	Block Internet Acc	ess ways 💿 Specific	timos				
	School nights	5:30 PM -	All Contractions	1 🔻			
	Weekends	8:00 PM 👻	to 7:00 AM	1 -			
Block Specific Sites	URL 1: WWW.					_	
	URL 2:						
	URL 3:						
	URL 4:						
	URL 5:						
	URL 6:						
	URL 7:						
	URL 8:						
					BRIDDELT BURDLE STORE STORE		
			Save Set	tings	Cancel Change		

The "Parental Controls" screen re-appears.

Set a schedule to block Internet access.

Select Specific times. School nights: 5:30 PM to 7:00AM Weekends: 8:00 PM to 7:00 AM

Block specific sites: type in the website URL.

Click Cancel Changes.

Step 15

From computer 1, click Wireless tab.

Click Wireless MAC Filter > Disable > Save Settings > Continue.

Click Wireless Security > Disable > Save Settings > Continue.

Click Basic Wireless Settings > Disable > Save Settings > Continue.