IT Essentials 5.0

10.2.4.10 Travaux pratiques – Configuration de la sécurité sans fil

Introduction

Imprimez et faites ces travaux pratiques.

Au cours de ce TP, vous allez configurer et tester les paramètres sans fil du routeur Linksys E2500.

Matériel conseillé

- Deux ordinateurs exécutant Windows 7, Windows Vista, ou Windows XP
- Une carte réseau Ethernet installée sur l'ordinateur 1
- Une carte réseau sans fil installée sur l'ordinateur 2
- Un routeur sans fil Linksys E2500
- Un câble de raccordement Ethernet

Étape 1

Demandez à l'instructeur de vous fournir les informations suivantes. Vous en aurez besoin pour ce TP.

Informations de connexion par défaut : Nom d'utilisateur (s'il y a lieu) : _	
Mot de passe :	
Paramètres sans fil de base : Nom de réseau (SSID) :	

Mode réseau :

Canal : _____

Important : utilisez uniquement les informations de configuration indiquées par l'instructeur.

Remarque : sauf indication contraire, utilisez l'ordinateur 1 pour toutes les instructions de ce TP.

Étape 2

Connectez l'ordinateur 1 à l'un des ports **Ethernet** du routeur sans fil, à l'aide d'un câble de raccordement Ethernet.

Branchez l'alimentation du routeur sans fil. Démarrez l'ordinateur et ouvrez une session en tant qu'Administrateur.

Étape 3

Ouvrez l'invite de commandes.

Tapez ipconfig.

Quelle est l'adresse IP de l'ordinateur ?

Quelle est la passerelle par défaut de l'ordinateur ?

Ouvrez Internet Explorer et connectez-vous au routeur sans fil.

Tapez « admin » dans le champ « Password: ».

L'écran de configuration s'affiche.

Cliquez sur l'onglet Wireless.

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	Gu	est Access	Wireless MAC Filter	
Configuration View	Manual Manual Network Mode: Network Name Channel Width: Channel:	Wi-Fi Protected (SSID): Ci A	Setup™ isabled ▼ sco55842 D MHz Only uto (DFS) ▼			<u>Help</u>	
2.4 GHz Wireless Settings	SSID Broadcas Network Mode: Network Name Channel Width: Channel: SSID Broadcas	t: D (SSD): 22 A t: O	Enabled D MHz Only uto Enabled D Salation	bled v			
			Save Se	ttings	Cancel Change	s	

Dans l'onglet Wireless, cliquez sur **Basic Wireless Settings** si cette option n'est pas déjà sélectionnée.

cisco.						Firmwa	e Version: 1.0.0
						Linksys E2500	E2500
Wireless	Setup	Wireless	s Security	Access Policy	Applications & Gaming	Administration	Status
	Basic Wireless	Settings	Wireless Securit	y I 🤇	Guest Access	Wireless MAC Filter	
Configuration View							
	🖲 Manual 🔘	Wi-Fi Protec	cted Setup™			<u>Help</u>	
5 GHz Wireless Settings	Network Mode:		Disabled	-			
	Network Name	(SSID):	Cisco55842				
	Channel Width:		20 MHz Only	v			
	Channel:		Auto (DFS)]			
	SSID Broadcas	t	Enabled 🖲 Dis	abled			
2.4 GHz Wireless Settings	Network Mode		Mixed	•			
	Network Name	(SSID):	Cisco1				
	Channel Width:		20 MHz Only	•			
	Channel:		6 - 2.437GHZ 🔻				
	SSID Broadcas	t	Enabled O Dis	abled			
						a en ante	
			Save S	ettings	Cancel Change	s	

Spécifiez les informations suivantes pour les paramètres sans fil 2,4 GHz, sauf si l'instructeur donne des indications contraires :

Network Mode : **Mixed**

Network Name (SSID) : **Cisco#**, où # est un nombre attribué par l'instructeur Channel : **#**, où # est un nombre attribué par l'instructeur SSID Broadcast : **Enabled**

Cliquez sur **Save Settings > Continue**.

Cliquez sur le sous-onglet Wireless Security.

Étape 5

L'écran « Wireless Security » apparaît.

cisco.								FI	rmware Version: 1.0.02
								Linksys E25	00 E2500
Wireless	Setup	Wirele	ss	Security	Access Policy	Application Gaming	ns& g	Administration	Status
	Basic Wireless	s Settings	j.	Wireless Security	G	uest Access	<u>(</u> 1	Wireless MAC Filter	
5 GHz Wireless Security									
	Security Mode	c.	Dis	abled		×		<u>Help</u>	
2.4 GHz Wireless Security	Security Mode	C	WF	A2 Personal		•			
	Passphrase:		C!s	coL@b102410					
				Save Se	ttings 👆	Cancel Ch	ange	s	

Spécifiez les informations suivantes pour les paramètres de sécurité sans fil 2,4 GHz, sauf si l'instructeur donne d'autres indications :

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

Cliquez sur Save Settings > Continue.

Laissez Internet Explorer ouvert et connectez-vous au routeur Linksys.

Étape 6

Ouvrez une session sur l'ordinateur 2, à savoir l'ordinateur sans fil, en tant qu'Administrateur.

Connectez-vous au réseau sans fil. Si le système vous demande une clé de sécurité ou une phrase de passe, tapez : C!scoL&b102410

Ouvrez l'invite de commandes.

Tapez ipconfig /all.

Quelle est l'adresse IP de la carte réseau sans fil ?

Quelle est l'adresse physique de la carte réseau sans fil ?

Tapez ping AdresselP. Où AdresselP est l'adresse IP de l'ordinateur 1.

La requête ping a-t-elle abouti?

Laissez la fenêtre d'invite de commandes ouverte.

Étape 7

Assurez-vous qu'Internet Explorer est actif sur l'ordinateur 1.

Dans l'onglet Wireless, cliquez sur Guest Access.

cisco.						Firmwa	ire Version: 1.0.02
						Linksys E2500	E2500
Wireless	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status
	Basic Wireless	s Settings 🛛 🛔	Wireless Security	G	uest Access	Wireless MAC Filter	
Guest Access	Guest Acces giving them a Allow Guest A Guest Networ Guest Passwr Total Guests A SSID Broadca Your guests opening a We	s provides visit access to your k ccess: k Name: Ci ord: g ulowed: 5 st: st: st: should connec b browser and	tors to your homo computers or pe yes O no sco1-guest uest Enabled O Disc to your wireless entering the gue	e with Inte rsonal dat abled s network est passw	change Listed above by rord.	s	

Pourquoi autoriser un accès invité ?

ululu cisco.						Firmwa	re Version: 1.0.02		
						Linksys E2500	E2500		
Wireless	Setup	Wireless	Securit	y Access Policy	Applications & Gaming	Administration	Status		
	Basic Wir	eless Settings 🛛 🛔	Wireless S	ecurity Gi	uest Access	Wireless MAC Filter			
Wireless MAC Filter									
	C Enab	ed 🖲 Disabled				Help			
	Prevent PCs listed below from accessing the wireless network. Permit PCs listed below to access the wireless network.								
MAC Address Filter List	Wire	less Client List							
	MAC 01:	00:00:00:00:00:00	MAC 17:	00:00:00:00:00:00	00				
	MAC 02:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:00	00				
	MAC 03:	00:00:00:00:00:00	MAC 19:	00:00:00:00:00:00	00				

Sous l'onglet Wireless, cliquez sur Wireless MAC Filter.

Étape 8

L'écran « Wireless MAC Filter » apparaît.

cisco.						Firmw	are Version: 1.0.02
						Linksys E2500	E2500
Wireless	Setup	Wireless	Securi	ty Access Policy	Applications & Gaming	& Administration	Status
	Basic Wir	eless Settings	Wireless S	ecurity Gu	uest Access	Wireless MAC Filter	
Wireless MAC Filter							
	Enable	ed 🔘 Disabled				<u>Help</u>	
	Preve	ent PCs listed below it PCs listed below t	from accessi o access the	ing the wireless ne wireless network.	etwork.		
MAC Address Filter List	Wire	less Client List					
	MAC 01:	00:00:00:00:00:00	MAC 17:	00:00:00:00:00:0	10		
	MAC 02:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:0	10		
	MAC 03:	00:00:00:00:00:00	MAC 19:	00:00:00:00:00:0	10		

Sélectionnez Enabled > Prevent et cliquez sur Wireless Client List.

L'écran « Wireless Client List » apparaît.

cisco.						
Wireless Client List Sort By	IP Address 🔻					
	Client Name	Interface	IP Address	MAC Address	Status	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		

Cochez la case Save to MAC Address Filter List pour l'ordinateur 2.

Cliquez sur **Add**.

Quelle adresse MAC apparaît à présent ?

Cliquez sur **Save Settings > Continue**.

Étape 9

Sur l'ordinateur 2 :

Dans la fenêtre d'invite de commandes, tapez **ping** *AdresselP*, où *AdresselP* est l'adresse IP de l'ordinateur 1.

La requête ping a-t-elle abouti?

Sur l'ordinateur 1, cliquez sur le **navigateur** afin de l'activer.

Cliquez sur **Administration** dans la barre d'onglets principale.

L'écran Administration apparaît.

			Linksys E2500	E2500
Administration	Setup Wireles	s Security Access Applications & Ad	Iministration S	itatus
	Management Log	Diagnostics Factory Defaults Firmw	are Upgrade	
Management				
Router Access	Router Password: Re-Enter to Confirm:		<u>Help</u>	
Local Management Access	Access via:	W HTTP HTTPS		
	Access via Wireless:	Enabled Disabled		
Remote Management Access	Remote Management:	Enabled Isabled		
	Access via:	HTTP HTTPS		
	Remote Upgrade:	Enabled Disabled		
	Allowed Remote IP Address:	Any IP Address		
		0.0.0.0 to 0		
	Remote Management Port:	8080		
Advanced features	SIP ALG:	© Enabled		
UPnP	UPnP:	Enabled Oisabled		
	Allow Users to Configure:	Enabled Disabled		
	Allow Users to Disable Internet Access:	© Enabled		
Back Up and Restore	Back Up Configuration	Restore Configuration	-	
		Save Settings Cancel Changes		

Sélectionnez le mot de passe du routeur et tapez **ITEv5.0**. Tapez le même mot de passe dans le champ Re-enter to Confirm.

Cliquez sur **Cancel Changes**. N'enregistrez pas le nouveau mot de passe.

Cliquez sur **Security** dans la barre d'onglets principale.

L'écran du pare-feu apparaît.

uluilu cisco.						Firmur	are Version: 1.0.02	
						Linksys E2500	E2500	
Security	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status	
Firowall	Firewall	VPN Passthrou	ıgh					
Thewan	IPv6 SPI Firewa Protection:	<u>Help</u>						
	IPv4 SPI Firewa Protection:							
Internet Filter	Internet Filter							
	Filter Multic	ast net NAT Redirectio	on for IPv4 Intern	et				
	Only Filter IDENT	Г (Port 113)						
Web Filter	Dana -	laura 🔲 é até	er 🔲 Castin					
	Proxy	Java 🖂 Activ	COOKIES	5				
			Save	Settings	Cancel Change	s		

Par défaut, la valeur de SPI Firewall Protection est Enabled.

Quels filtres Internet sont disponibles ?

Quels filtres Web sont disponibles ?

Cliquez sur Applications & Gaming dans la barre d'onglets principale.

L'écran « Applications & Gaming » apparaît.

cisco.							Firmware	Version: 1.0.02
							Linksys E2500	E2500
Applications & Gaming	Setup	Wireless	Security	Access Policy	Applicati Gami	ons&	Administration	Status
Cunning	Single Port Forwarding	1	Port Range Forwarding	1	Port Range Triggering	I.	DMZ ^{IPv6} Firewall	QoS
Single Port Forwarding								
Application Name	External Port	Internal Port	Protocol	To IP Add	iress	Enabled	Help	
None 🔻	1	1	11	192.168.1	. 0			
None 🔻			11	192 . 168 . 1	. 0			
None 🔻				192 . 168 . 1	I. 0			
None 🔻			32443	192 . 168 . 1	I. 0			
None 🔻			1 <u></u> 1	192 . 168 . 1	0			
	0	0	Both 🔻	192.168.1	I. 0			
	0	0	Both 🔻	192 . 168 . 1	I. 0			
	0	0	Both 🔻	192.168.1	. 0			

Cliquez sur Single Port Forwarding.

cisco.							Firmware	Version: 1.0.02
							Linksys E2500	E2500
Applications & Gaming	Setup	Wireless	Security	Access Policy	Application Gaming	s &	Administration	Status
	Single Port Forwarding		Port Range Forwarding		ort Range Triggering			
Single Port Forwarding								
Application Name	External Port	Internal Port	Protocol	To IP Add	ress E	Enabled	Help	
None 🔻	11 1		11	192.168.1.	0			
None				192.168.1.	0		-	
Telnet v				192.168.1.	0			
DNS			22442	192, 168, 1	0			
TFTP		1000	1	192 168 1	0			
HTTP	0	0	Both 🔻	192 168 1	0			
NNTP	0	0	Both V	400 400 4	0		-	
SNMP	U IIII	U	Doul •	192.168.1.	. •			
PPTP	0	0	Both 🔻	192.168.1.	0			

Pour activer la redirection depuis un port défini vers un ordinateur spécifique, sélectionnez **Application Name > FTP**.

Tapez le dernier octet de l'adresse IP de l'ordinateur, puis cochez la case **Enabled**.

			Single Port Forwarding	E.	Port Range Forwarding	I Po Ti	ort Range riggering	I Di	z I	IPv6 Firewall	QoS
Single Port	Forwa	rding									
Applic	Application Nam		External Port	Internal Port	Protocol	To IP Address		Enabled		Help	
	FTP	•	21	21	тср	192 . 168 . 1.	2				
	None	-			·	192 . 168 . 1.	0				
	None	•			1	192 . 168 . 1.	0				
	None	•	19220	1000	1000	192 . 168 . 1.	0				
	None	•	82224	222	8 <u>000</u> 9	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				
-		-1	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				
					Save	Settings	Cancel Ct	nanges			

Cliquez sur **Cancel Changes**. N'enregistrez pas le nouveau paramètre.

Cliquez sur Port Range Triggering.

L'écran « Port Range Triggering » apparaît.

uluilu cisco									949 - E	
									Firmware	Version: 1.0.02
						- 20		Lii	nksys E2500	E2500
Applications & Gaming	Setup	Wireless		Security	Access Policy	Applica Garr	tions & ning	Admini	stration	Status
ş	Single Port Forwarding			rt Range warding		Port Range Triggering				
Port Range Triggering							00			
	Applicatio	n Name	Trigg	gered Range	Forwar	ded Range	Enabled		Help	
			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				
			0	to 0	0	to 0				
			0	to 0	0	to 0				
								-		
				Save Se	ttings	Cancel	Changes			

Pour ouvrir un port bloqué, tapez **IRC** dans le champ Application Name. Tapez ensuite **6660 to 7000** dans les champs Triggered Range et **113 to 113** dans les champs Forwarded Range, puis cochez la case **Enabled**.

cisco.										Firmware	Version: 1.0.02
									L	inksys E2500	E2500
Applications &	Setup	Wireless	ess Security		Acces Policy	Access Applications & Policy Gaming		tions & ning	Administration St		Status
Canning	Single Port Forwarding	I.	Port Forw	Range varding	ų.	Р 1	ort Range Triggering	I.	DMZ	l IPv6 Firewall	QoS
Port Range Triggering											
	Applicatio	n Name	Trigge	ered Range	Forwa	rde	d Range	Enabled		Help	
	IRC		6660	to 7000	113	to	113	V			
			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				
			0	to 0	0	to	0				
				Save S	ettings		Cancel	Changes	•		

Cliquez sur **Cancel Changes**. N'enregistrez pas le nouveau paramètre.

Cliquez sur Access Policy.

L'écran des contrôles parentaux apparaît.

Access Policy	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status
	Parental Control	s	() ()	ă și și și și și	19 		
Parental Controls							
	Parental Controls	<u>Help</u>					
Target Devices	Restrict Internet						
	Add Remov	Rename	-				
Schedule	Block Internet Ac						
	Never A	Always Spe	ecific times	414			
	Weekends	Midnight	to 7:00▼ to 7:00	AM 👻			
Block Specific Sites	URL 1:						
	URL 2:						
	URL 3:						
	URL 4:						
	URL 5:			_			
	URL 8:						
			Save	Settings	Cancel Changes	s (1999)	

Sélectionnez **Enabled > Add**.

La fenêtre « Set up parental controls for » s'affiche.

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

Sélectionnez un nom d'ordinateur, **BRAXTON-PC > OK**.

Access Policy	Setup	Wireless	Security	Access Policy	Applications & Gaming	Administration	Status
	Parental Controls				-		
Parental Controls							
	Parental Controls:	<u>Help</u>					
Target Devices	Restrict Internet ac						
	BRAXTON-PC						
	Add Remove	Rename					
Schedule	Block Internet Acco						
	School nights	5:30 PM	✓ to 7:00	AM 👻			
	Weekends	8:00 PM	▼ to 7:00	AM 🔻			
Block Specific Sites	URL 1: WWW.						
	URL 2:						
	URL 3:						
	URL 4:						
	URL 5:			-			
	URL 6:			-			
	URL 7:			-			
	URL 8:						
			Save S	Settings	Cancel Changes	. In	
					44		

L'écran des contrôles parentaux réapparaît.

Planifiez les horaires de blocage de l'accès Internet.

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

Block Specific Sites : tapez l'URL du site Web.

Cliquez sur Cancel Changes.

Étape 15

Sur l'ordinateur 1, cliquez sur l'onglet Wireless.

Cliquez sur Wireless MAC Filter > Disabled > Save Settings > Continue.

Cliquez sur Wireless Security > Disabled > Save Settings > Continue.

Cliquez sur Basic Wireless Settings > Disabled > Save Settings > Continue.