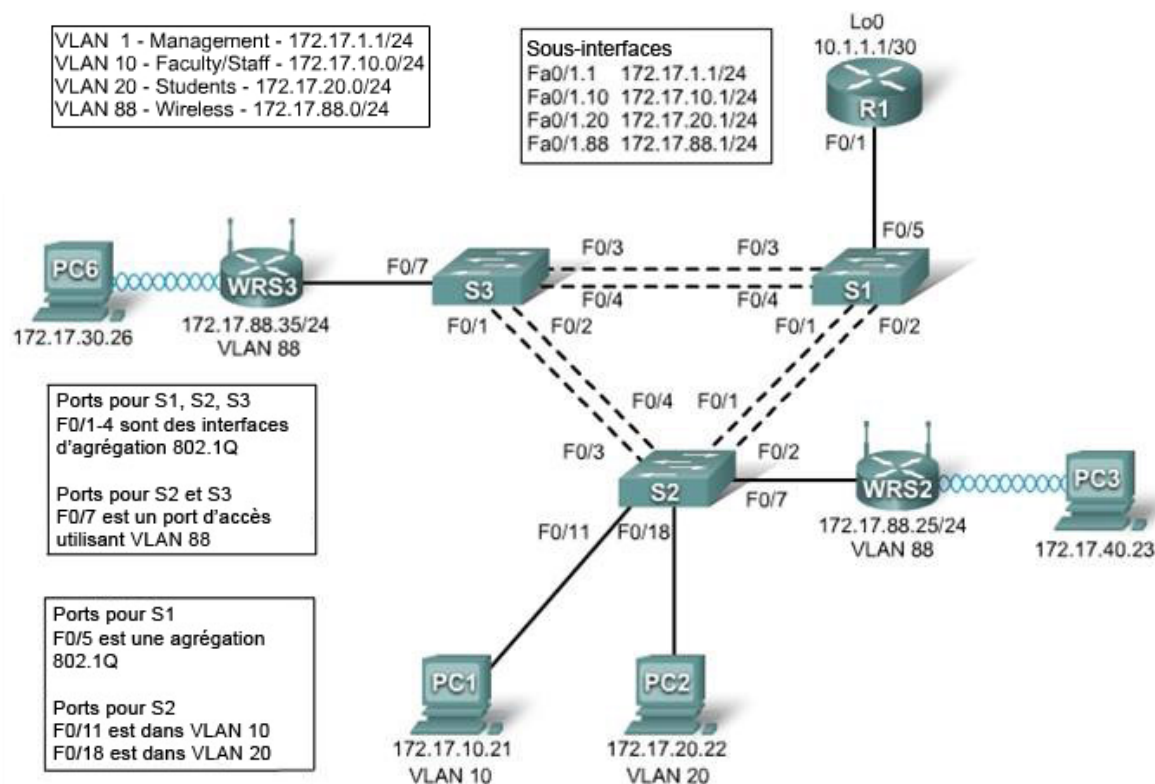


## Travaux pratiques 7.5.2 : Configuration avancée d'un routeur sans fil WRT300N

### Schéma de topologie



## Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
<b>R1</b>	<b>Fa0/1.1</b>	172.17.1.1	255.255.255.0	S/O
	<b>Fa0/1.10</b>	172.17.10.1	255.255.255.0	S/O
	<b>Fa0/1.20</b>	172.17.20.1	255.255.255.0	S/O
	<b>Fa0/1.88</b>	172.17.88.1	255.255.255.0	S/O
	<b>Lo0</b>	10.1.1.1	255.255.255.252	S/O
<b>WRS2</b>	<b>WAN</b>	172.17.88.25	255.255.255.0	172.17.88.1
	<b>LAN/Wireless</b>	172.17.40.1	255.255.255.0	S/O
<b>WRS3</b>	<b>WAN</b>	172.17.88.35	255.255.255.0	172.17.88.1
	<b>LAN/Wireless</b>	172.17.30.1	255.255.255.0	S/O
<b>PC1</b>	<b>Carte réseau</b>	172.17.10.21	255.255.255.0	172.17.10.1
<b>PC2</b>	<b>Carte réseau</b>	172.17.20.22	255.255.255.0	172.17.20.1

## Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Configurer les données de réseau VLAN des ports d'un commutateur et la sécurité des ports
- Opérer la réinitialisation matérielle d'un routeur Linksys WRT300N
- Connecter un routeur sans fil et vérifier sa connectivité
- Ouvrir l'utilitaire Web d'un routeur Linksys WRT300N
- Configurer les paramètres IP d'un routeur Linksys WRT300N
- Configurer DHCP sur un routeur Linksys WRT300N
- Configurer des routes statiques sur des routeurs standard Cisco et sur un routeur WRT300N
- Changer le mode réseau et le canal réseau correspondant sur un routeur WRT300N
- Activer le chiffrement WEP et désactiver les diffusions de SSID
- Activer un filtre MAC sans fil
- Configurer les restrictions d'accès sur un routeur WRT300N
- Configurer le mot de passe de gestion d'un routeur WRT300N
- Activer la journalisation sur un routeur WRT300N
- Mettre à niveau le progiciel du routeur WRT300N
- Utiliser les procédures de diagnostic, sauvegarde, restauration et confirmation d'un routeur WRT300N

## Scénario

Dans le cadre de ces travaux pratiques, vous allez configurer un périphérique Linksys WRT300N, la sécurité des ports sur un commutateur Cisco et des routes statiques sur plusieurs périphériques. Notez les procédures utilisées pour connecter les clients à un réseau sans fil, car certaines modifications impliquent la déconnexion de clients. Ces clients devront être reconnectés après des modifications de la configuration.

### Tâche 1 : exécution des configurations de routeur de base

#### Étape 1: connexion physique des périphériques selon le schéma de topologie

#### Étape 2: configuration de R1 conformément aux instructions suivantes

- Configurez le nom d'hôte du routeur.
- Désactivez la recherche DNS.
- Définissez **cisco** comme mot de passe du mode d'exécution privilégié.
- Configurez l'interface FastEthernet 0/1 et ses sous-interfaces.
- Configurez Loopback0.
- Configurez la journalisation synchrone, la commande exec-timeout et le mot de passe **cisco** sur le port de console.

### Tâche 2 : configuration des interfaces des commutateurs

Configurez les noms d'hôte sur les commutateurs S1, S2 et S3. Réglez les commutateurs sur le mode Transparent, effacez les données des réseaux locaux virtuels et créez les VLAN 10, 20 et 88.

#### Étape 1: configuration des interfaces de port des commutateurs S1, S2 et S3

Configurez les interfaces des commutateurs S1, S2, and S3 selon les connexions du schéma de topologie.

Configurez les connexions entre deux commutateurs, configurez des agrégations.

Configurez les connexions à un routeur sans fil en tant que mode d'accès pour le VLAN 88.

Configurez la connexion entre S2 et PC1 dans le VLAN 10, et la connexion de PC2 dans le VLAN 20.

Configurez la connexion entre S1 et R1 en tant qu'agrégation.

Autorisez le trafic de tous les réseaux locaux virtuels entre les interfaces d'agrégation.

#### Étape 2: vérification des réseaux locaux virtuels et de l'agrégation

Exécutez la commande **show ip interface trunk** sur S1 et la commande **show vlan command** sur S2 pour contrôler que les commutateurs agrègent correctement le trafic et que les réseaux locaux virtuels existent bien.

# **S1#show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1
Fa0/3	on	802.1q	trunking	1
Fa0/4	on	802.1q	trunking	1
Fa0/5	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094
Fa0/2	1-4094
Fa0/3	1-4094
Fa0/4	1-4094
Fa0/5	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,88
Fa0/2	1,10,20,88
Fa0/3	1,10,20,88
Fa0/4	1,10,20,88
Fa0/5	1,10,20,88

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,88
Fa0/2	none
Fa0/3	1,10,20,88
Fa0/4	1,10,20,88
Fa0/5	1,10,20,88

←-- bloqué par STP, varie en fonction de la racine

# **S2#show vlan**

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/8, Fa0/9 Fa0/10, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gi0/1, Gi0/2
10	VLAN0010	active	Fa0/11
20	VLAN0020	active	Fa0/18
88	VLAN0088	active	Fa0/7
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Lorsque vous avez terminé, veuillez à enregistrer la configuration en cours dans la mémoire vive non volatile du routeur et des commutateurs.

### Étape 3: configuration des interfaces Ethernet de PC1 et PC2

Configurez les interfaces Ethernet des ordinateurs PC1 et PC2 avec les adresses IP et les passerelles par défaut indiquées dans le tableau d'adressage du début des travaux pratiques.

### Étape 4: vérification des configurations des ordinateurs

Envoyez une requête ping à la passerelle par défaut depuis les PC : 172.17.10.1 pour PC1 et 172.17.20.1 pour PC2.

Sélectionnez **Démarrer -> Exécuter ->** tapez **cmd**, puis **ping 172.17.x.x**

```
C:\Documents and Settings\Administrator>ping 172.17.10.1

Envoi d'une requête 'ping' sur 172.17.10.1 avec 32 octets

Réponse de 172.17.10.1 : octets=32 temps<1ms TTL=255
Réponse de 172.17.10.1 : octets=32 temps<1ms TTL=255
Réponse de 172.17.10.1 : octets=32 temps<1ms TTL=255
Réponse de 172.17.10.1 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 172.17.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%)
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

## Tâche 3 : connexion au routeur Linksys WRT300N WRS3

Vérifiez avec le formateur que le routeur sans fil a toujours ses paramètres d'usine. Dans le cas contraire, vous devez opérer une réinitialisation matérielle du routeur. Pour cela, recherchez le bouton de réinitialisation à l'arrière du routeur. À l'aide d'un stylo ou d'un autre instrument fin, maintenez enfoncé le bouton de réinitialisation pendant 5 secondes. Le routeur doit retrouver ses paramètres d'origine.

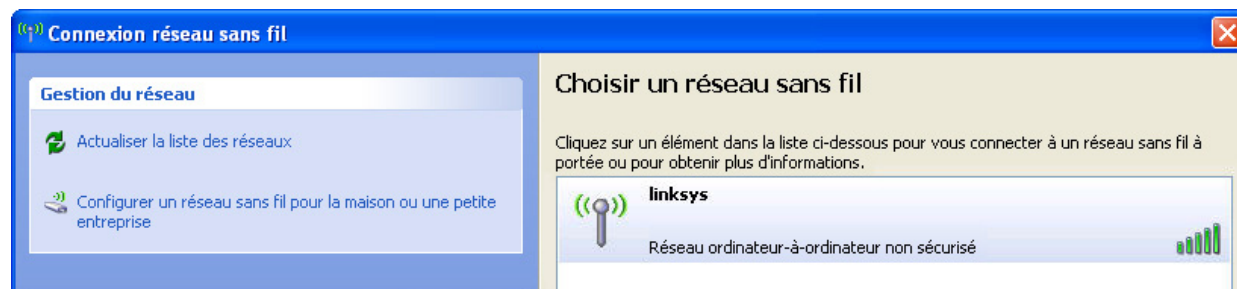
### Étape 1: connexion au routeur sans fil

Lorsque la configuration par défaut du routeur sans fil est rétablie, celui-ci diffuse le SSID par défaut « linksys ». Étape 1: connexion du routeur sans fil à l'aide de Windows XP

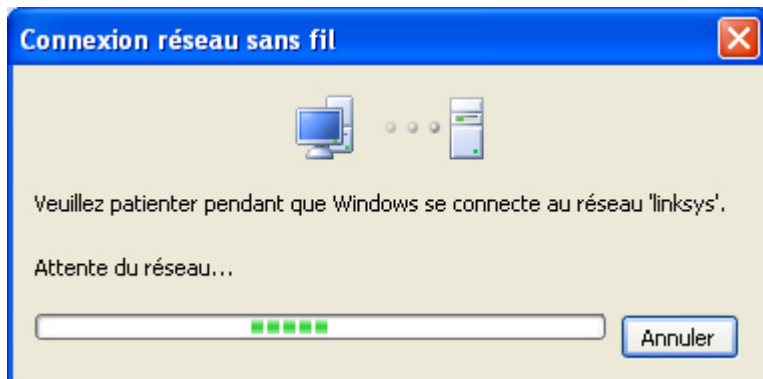
Remarque : avant de tenter d'établir une connexion au routeur WRS3, assurez-vous que le cordon d'alimentation du routeur WRS2 est débranché. Si les deux routeurs sans fil sont sous tension, le PC détectera deux réseaux sans fil avec le SSID « linksys », et il sera difficile de distinguer le routeur auquel vous tentez de vous connecter.

Cherchez l'icône Connexion réseau sans fil dans votre barre des tâches ou sélectionnez **Démarrer > Paramètres > Panneau de configuration > Connexions réseau**. Cliquez à l'aide du bouton droit sur l'icône et sélectionnez **Afficher les réseaux sans fil disponibles**.

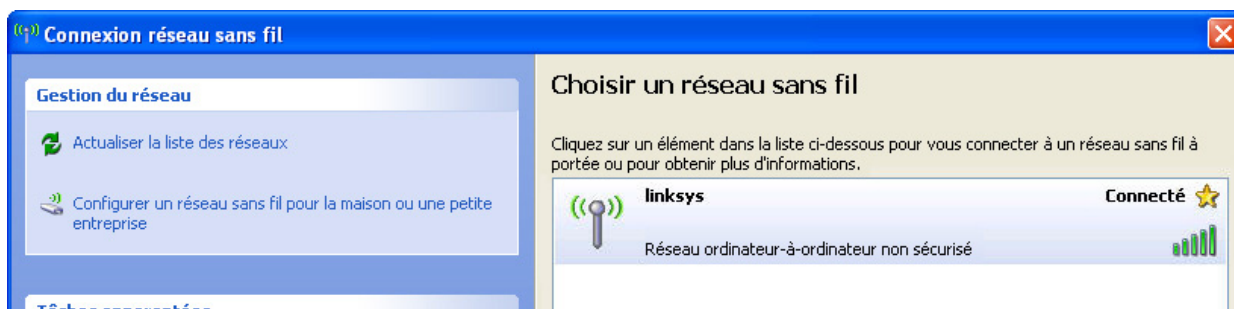
L'écran suivant apparaît. Notez que le SSID d'origine du routeur est « Linksys ».



Sélectionnez **Linksys**, puis cliquez sur **Connecter**.



La connexion s'établit après quelques instants.



## Étape 2: vérification des paramètres de connectivité

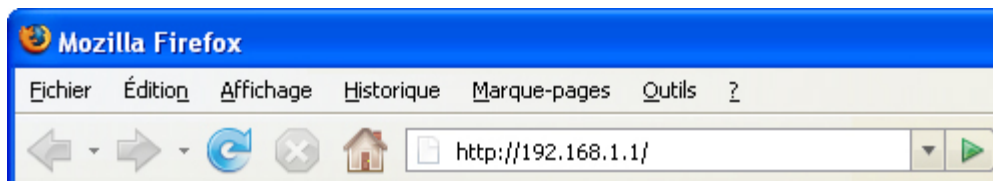
Pour vérifier les paramètres de connectivité, sélectionnez **Démarrer > Exécuter** puis tapez **cmd**. À l'invite de commande, tapez la commande **ipconfig** pour afficher les caractéristiques du périphérique réseau. Notez l'adresse IP de la passerelle par défaut. Il s'agit de l'adresse par défaut de tout routeur Linksys WRT300N.

```
Adresse IP. . . . . : 192.168.1.100
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 192.168.1.1
```

## Tâche 4 : configuration de WRS3 à l'aide de l'utilitaire Web

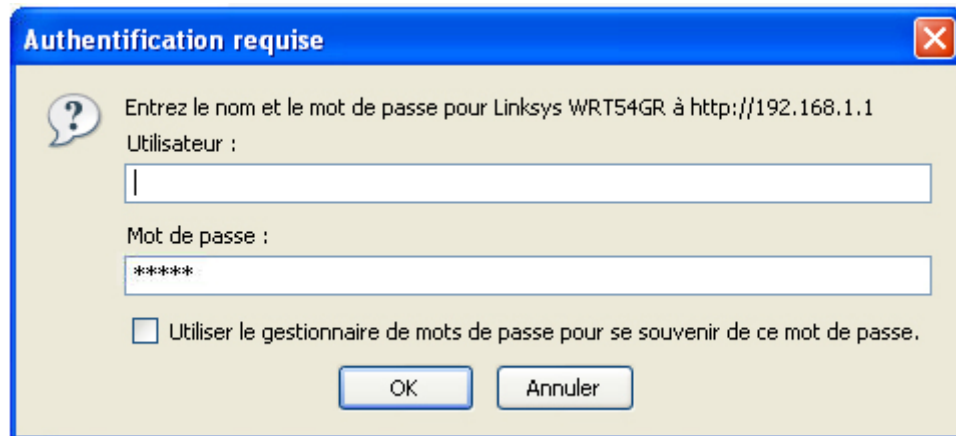
### Étape 1: ouverture de l'URL par défaut

Dans votre navigateur Web, accédez à <http://192.168.1.1>. Il s'agit de l'URL par défaut du routeur WRT300N.



## Étape 2: saisie des informations d'authentification

Un message vous demande de saisir un nom d'utilisateur et un mot de passe. Entrez le mot de passe par défaut du routeur WRT300N **admin** et laissez vide le champ du nom d'utilisateur.



Vous devez voir s'afficher la page par défaut de l'utilitaire Web du routeur Linksys WRT300N.

## Tâche 5 : configuration des paramètres IP pour le routeur Linksys WRT300N

Le meilleur moyen de comprendre la différence entre les options **Internet Setup** et **Network Setup** est de considérer que le routeur WRT300N est similaire à un routeur Cisco IOS avec deux interfaces séparées. Une de ces interfaces, celle configurée sous **Internet Setup**, agit comme la connexion aux commutateurs et au reste du réseau. Cette connexion aboutit éventuellement à Internet, bien qu'il n'y ait pas de connexion à Internet dans notre topologie. L'autre interface, configurée sous **Network Setup**, agit comme l'interface se connectant aux clients, à la fois sans fil et câblés.

## Étape 1: définition du type de connexion Internet sur IP statique

**LINKSYS®**  
A Division of Cisco Systems, Inc.

Firmware Version: v0.93.3

**Wireless-N Broadband Router WRT300N**

**Setup**

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

**Internet Setup**

Internet Connection Type

Optional Settings  
(required by some Internet Service Providers)

Static IP

MTU: Auto Size: 1500

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

[Help...](#)

## Étape 2: définition des paramètres d'adresse IP pour Internet Setup

- Dans Internet IP Address, tapez **172.17.88.35**.
- Dans Subnet Mask, tapez **255.255.255.0**.
- Dans Default Gateway, tapez **172.17.88.1** (l'adresse IP du VLAN 88 FastEthernet 0/1 de R1).

**LINKSYS®**  
A Division of Cisco Systems, Inc.

**Setup**

Setup | Wireless | Security | Access Restrictions

Basic Setup | DDNS | MAC Address Clone

**Internet Setup**

Internet Connection Type

Static IP

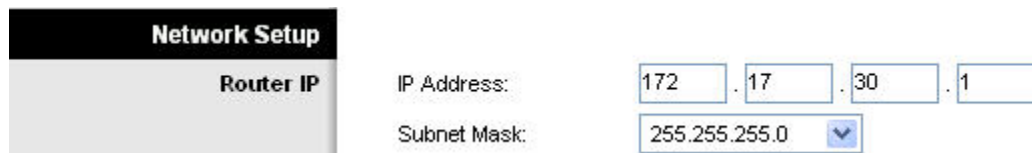
Internet IP Address: 172 . 17 . 88 . 35

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 172 . 17 . 88 . 1



### Étape 3: configuration de l'adresse IP (172.17.30.1)



The screenshot shows the 'Network Setup' window with the 'Router IP' tab selected. The 'IP Address' field is configured with the values 172, 17, 30, and 1. The 'Subnet Mask' field is set to 255.255.255.0 with a dropdown arrow.

### Étape 4: enregistrement des paramètres.

Cliquez sur **Save Settings**. Vous êtes invité à cliquer sur **Continue**. Puisque vous êtes connecté sans fil, vous ne serez pas redirigé vers la nouvelle URL de l'utilitaire Web (<http://172.17.30.1>).

Pour que les modifications apportées à l'adresse IP entrent en vigueur, le PC doit libérer son ancienne adresse IP et acquérir dynamiquement une nouvelle adresse à partir du réseau 172.17.30.0/24.

### Étape 5: libération de l'ancienne adresse IP dans Network Setup

À l'invite de commande, utilisez la commande **ipconfig /release** pour libérer l'adresse DHCP actuelle. Pour obtenir une nouvelle adresse IP dans le nouveau réseau, émettez la commande **ipconfig /renew**. Une nouvelle adresse IP doit être extraite du réseau 172.17.30.0/24.

### Étape 6 : affichage des paramètres de configuration IP du PC

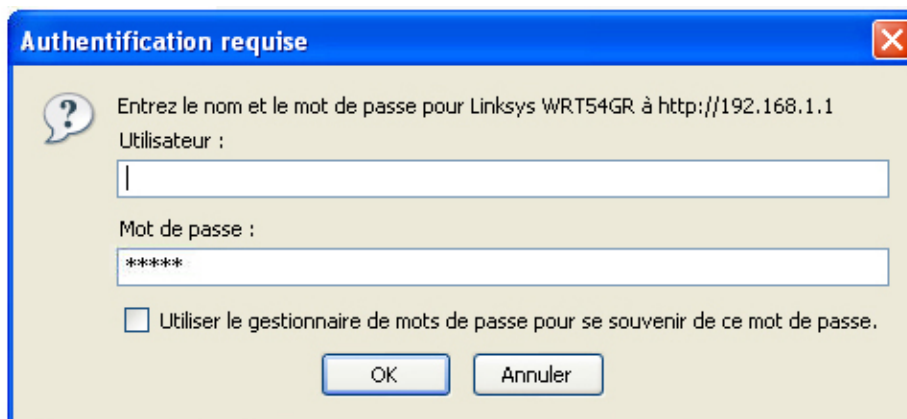
Accédez à l'invite de commande et tapez la commande **ipconfig**. Si l'adresse n'a pas été mise à jour (réseau 172.17.30.0/24), vous devrez libérer et renouveler l'adresse IP sur le client.

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : cisco.com
IP Address. . . . . : 172.17.30.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.17.30.1
```

### Étape 7 : ouverture de la nouvelle URL et entrée des informations d'authentification

Dans votre navigateur Web habituel, accédez à <http://172.17.30.1>. Il s'agit de la nouvelle URL pour le routeur WRT300N. Entrez le nom d'utilisateur et le mot de passe par défaut lorsque le système vous y invite.



The screenshot shows an 'Authentication required' dialog box. It contains a question mark icon and the text: 'Entrez le nom et le mot de passe pour Linksys WRT54GR à http://192.168.1.1'. Below this, there are input fields for 'Utilisateur :' and 'Mot de passe :'. The password field shows '\*\*\*\*\*'. There is a checkbox labeled 'Utiliser le gestionnaire de mots de passe pour se souvenir de ce mot de passe.' and two buttons at the bottom: 'OK' and 'Annuler'.

## Tâche 6 : configuration des paramètres DHCP et des paramètres horaires du routeur

### Étape 1 : affectation d'un lien DHCP statique à PC6

Dans la page **Basic Setup** de la section **Network Setup**, cliquez sur **DHCP Reservations**. Recherchez PC6 dans la liste des clients DHCP actuels. (Notez que votre PC peut avoir un nom différent.) Activez la case à cocher sur la ligne correspondant au PC, puis cliquez sur **Add Clients**.

DHCP Reservation					
Select Clients from DHCP Tables	Client Name	Interface	IP Address	MAC Address	Select
	Pc6	Wireless	172.17.30.100	00:05:4E:49:64:F8	<input checked="" type="checkbox"/>

**Add Clients**

Le client PC6, c'est-à-dire l'ordinateur ayant l'adresse MAC 00:05:4E:49:64:F8, aura la même adresse IP, 172.17.30.100, chaque fois qu'il demandera une adresse via DHCP. Ceci n'est qu'une des manières d'établir rapidement un lien permanent entre un client et une adresse DHCP. Vous allez maintenant affecter à PC6 l'adresse IP du schéma de topologie au lieu de celle qu'il a reçue initialement. Cliquez sur **Remove** pour affecter la nouvelle adresse.

Clients Already Reserved			
Client Name	Assign IP Address	To This MAC Address	MAC Address
Pc6	172.17.30.100	00:05:4E:49:64:F8	<b>Remove</b>

### Étape 2 : affectation de l'adresse 172.17.30.26 à PC6

Si vous entrez l'adresse de PC6 dans la zone Manually Adding Client, chaque fois que PC6 se connectera au routeur sans fil, il recevra l'adresse IP 172.17.30.26 via DHCP. Enregistrez les modifications.

Manually Adding Client			
Enter Client Name	Assign IP Address	To This MAC Address	
Pc6	172.17.30.26	00:05:4E:49:64:F8	<b>Add</b>

### Étape 3 : vérification du changement d'adresse IP statique

Puisque nous avons déjà une adresse IP de DHCP, nous n'obtiendrons pas la nouvelle adresse, 172.17.30.26, avant la reconnexion. Nous vérifierons plus tard dans la Tâche 7, Étape 6, que cette modification a été prise en compte.

#### Étape 4 : configuration du serveur DHCP

Attribuez la valeur 50 à l'adresse de début, 25 au nombre maximal d'utilisateurs et 2 heures (120 minutes) à la durée d'utilisation.

**DHCP Server Setting**

DHCP Server: ☒ Enabled ☐ Disabled [DHCP Reservation](#)

Start IP Address: 172.17.30.50

Maximum Number of Users: 25

IP Address Range: 172.17.30.100 to 149

Client Lease Time: 120 minutes (0 means one day)

Avec ces paramètres, un PC qui se connectera sans fil à ce routeur et qui demandera une adresse IP via DHCP recevra une adresse comprise entre 172.17.30.50 et 74. Seuls 25 clients pourront obtenir une adresse IP en même temps et pour une durée de deux heures au plus, après quoi ils devront en demander une autre.

Remarque : le champ IP Address Range s'actualise uniquement quand vous cliquez sur **Save Settings**.

#### Étape 5 : configuration du fuseau horaire du routeur

En bas de la page Basic Setup, choisissez le fuseau qui correspond à votre zone géographique.

**Time Settings**

Time Zone: (GMT-08:00) Pacific Time (USA & Canada) ▼

☒ Automatically adjust clock for daylight saving changes.

#### Étape 6: enregistrement des paramètres

Cliquez sur **Save Settings**. Vous êtes invité à cliquer sur **Continue**.

### Tâche 7 : paramètres sans fil de base

#### Étape 1 : ouverture de la page Wireless et définition du mode réseau sous l'onglet Basic Wireless Settings

Le routeur Linksys WRT300N vous permet de choisir le mode réseau à utiliser. Les modes les plus courants actuellement sont Wireless-G pour les clients et BG-Mixed pour les routeurs. Quand un routeur fonctionne en mode BG-Mixed, il peut accepter les clients en modes B et G. Si un client en mode B se connecte, le routeur doit descendre au niveau B, le plus lent. Pour ces travaux pratiques, nous allons considérer que tous les clients sont en mode B et donc choisir le mode Wireless-B Only.

## Étape 2 : configuration des autres paramètres

Dans **Network Name (SSID)**, tapez WRS3\_[numéro], où le numéro est un numéro d'ID unique qui vous a été communiqué par le formateur. Dans **Standard Channel**, sélectionnez le canal qui vous a été attribué par le formateur, puis désactivez SSID Broadcast.

Pourquoi est-il souhaitable que le canal sans fil ne soit pas le canal par défaut ?

---

---

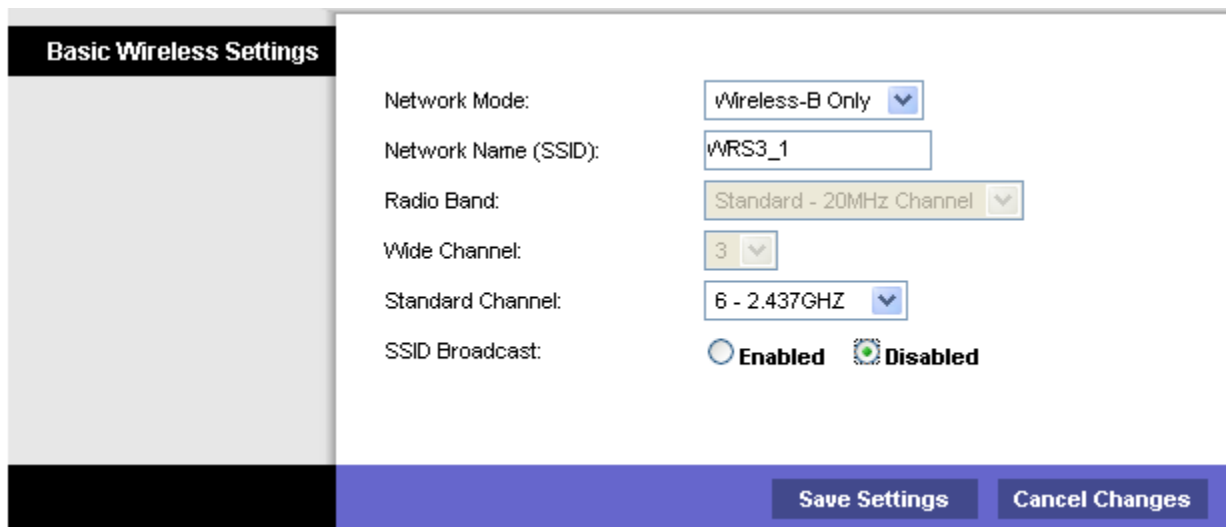
Pourquoi est-il conseillé de désactiver l'option SSID Broadcast ?

---

---

---

---



## Étape 3 : enregistrement des paramètres

Cliquez sur le lien **Save Settings** pour enregistrer toutes les modifications. Cliquez sur **Continue** pour passer à la tâche suivante.

## Étape 4 : vérification de la non-diffusion du SSID du routeur

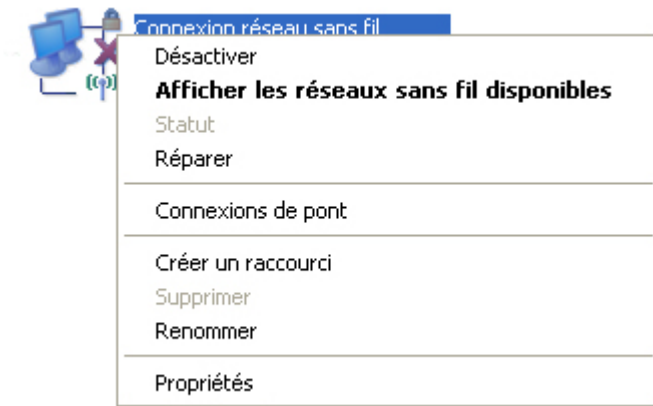
Recherchez les réseaux sans fil disponibles. Cherchez l'icône Connexion réseau sans fil dans votre barre des tâches ou sélectionnez **Démarrer > Paramètres > Panneau de configuration > Connexions réseau**. Cliquez avec le bouton droit sur l'icône et sélectionnez Afficher les réseaux sans fil disponibles.

Le SSID du routeur sans fil apparaît-il ?

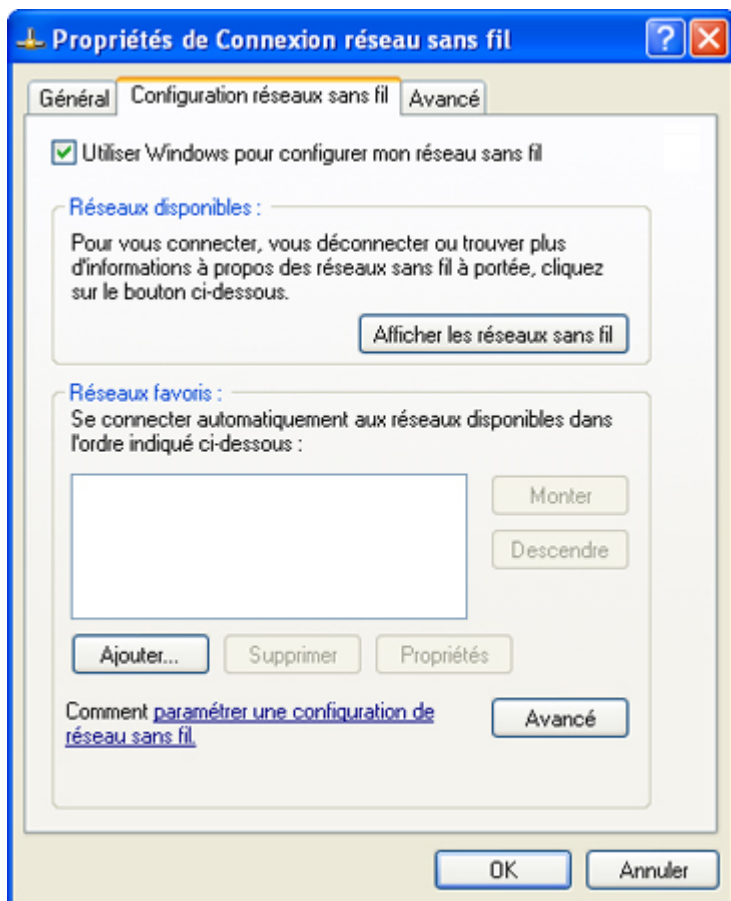
---

## Étape 5 : reconnexion au réseau sans fil

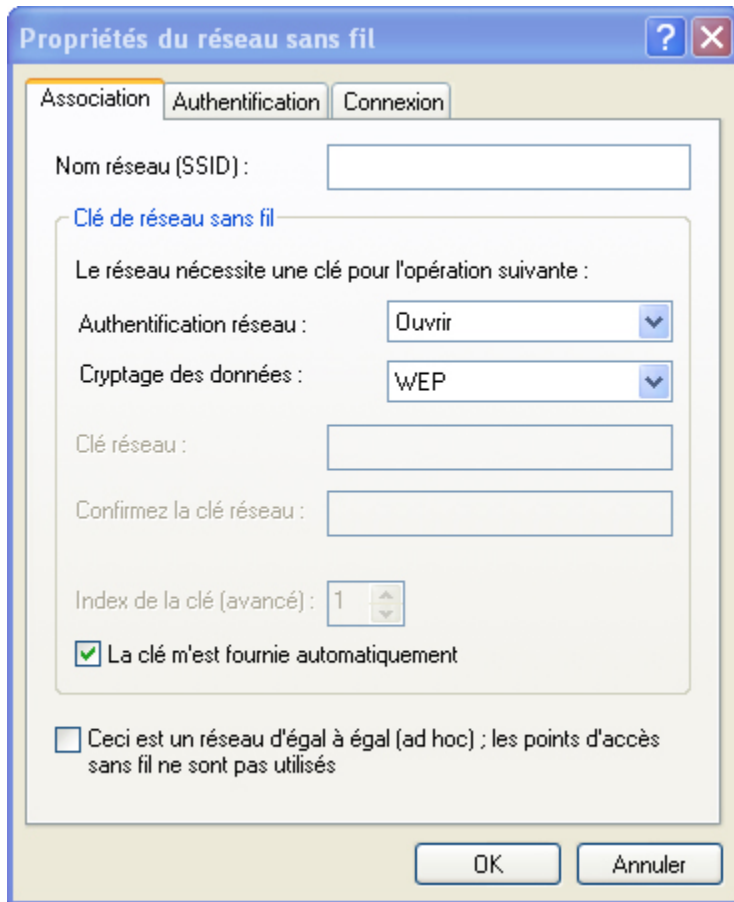
Sélectionnez **Démarrer > Panneau de configuration > Connexions réseau**, cliquez avec le bouton droit sur l'icône Connexion réseau sans fil, puis sélectionnez Propriétés.



Sous l'onglet Configuration réseaux sans fil, sélectionnez **Ajouter**.



Sous l'onglet **Association**, entrez WRS3\_[numéro] dans le champ Nom réseau (SSID) et sélectionnez **Disabled** pour l'option Chiffrement des données. Cliquez sur **OK** à deux reprises. Windows doit à présent tenter de se reconnecter au routeur sans fil.



### Étape 6: vérification des paramètres

À présent que vous êtes reconnecté au réseau, vous utilisez les nouveaux paramètres DHCP que vous avez configurés à la Tâche 6, Étape 2. Pour le vérifier, tapez **ipconfig** à l'invite de commande de PC6.

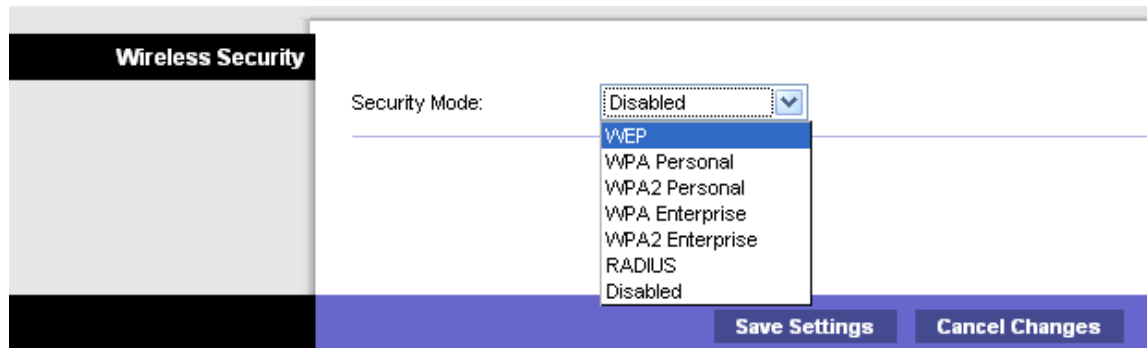
```
Adresse IP. . . . . : 192.168.1.100
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 192.168.1.1
```

## Tâche 8 : activation de la sécurité sans fil

Étape 1 : reconnexion à la page de configuration du routeur (<http://172.17.30.1>)

Étape 2 : ouverture de la page Wireless et sélection de l'onglet Wireless Security

Étape 3 : option Security Mode réglée sur WEP

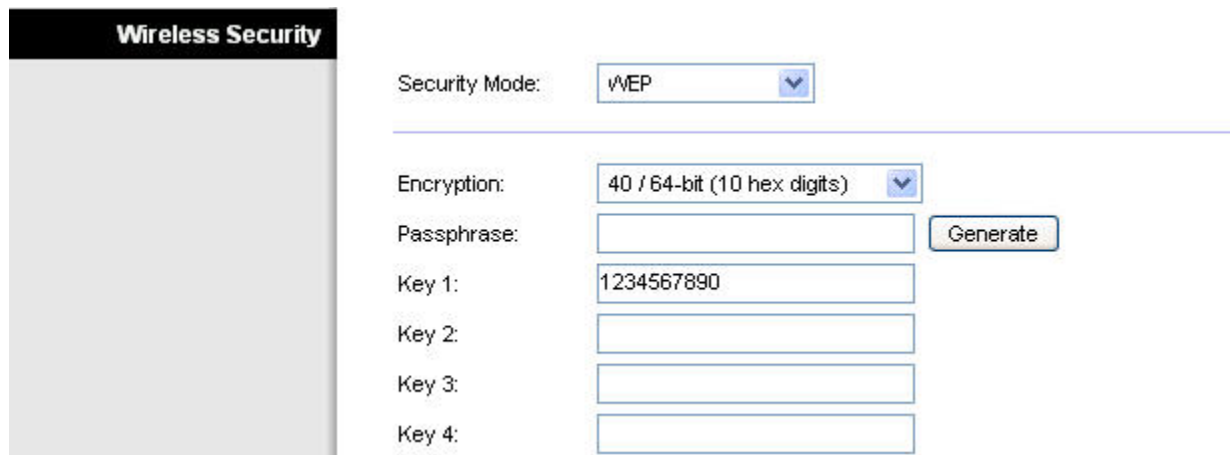


Étape 4 : entrée de la clé WEP

Un réseau n'est pas plus sécurisé que son point le plus vulnérable, un routeur sans fil est donc un point de départ très pratique pour quelqu'un souhaitant endommager votre réseau. Si vous ne diffusez pas le SSID du réseau et que vous demandez une clé WEP pour se connecter au routeur, vous ajoutez quelques degrés de sécurité.

Malheureusement, il existe des outils capables d'identifier les réseaux même s'ils ne diffusent pas leur SSID, et des outils capables de percer à jour un chiffrement de clé WEP.

Ajoutez la clé WEP **1234567890** comme Key 1.



## Étape 5 : enregistrement des paramètres

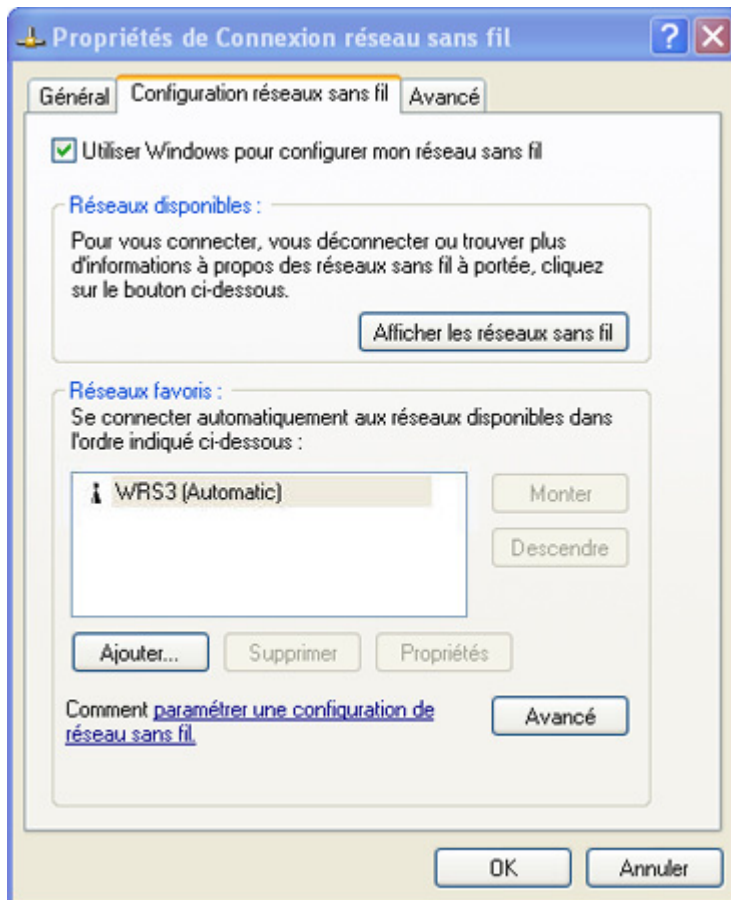
Maintenant que WRS3 a été configuré avec la sécurité WEP et que PC6 n'est pas configuré avec WEP, vous allez être déconnecté du réseau.

## Étape 6: configuration de Windows pour l'utilisation de l'authentification WEP

Ouvrez à nouveau la page Connexions réseau, puis cliquez avec le bouton droit sur l'icône **Connexion réseau sans fil**. Sous l'onglet Configuration réseaux sans fil, recherchez le réseau WRS3 et cliquez sur **Propriétés**.

- Pour l'option Chiffrement des données, choisissez **WEP**.
- Désactivez la case This Key Is Provided For Me.
- Tapez la clé réseau **1234567890** qui était initialement configurée sur le routeur.
- Cliquez sur **OK** à deux reprises.

Windows doit maintenant se reconnecter au réseau.





## Tâche 9 : configuration d'un filtre Wireless MAC

### Étape 1 : ajout d'un filtre Mac

- Revenez à la page de l'utilitaire Web du routeur (<http://172.17.30.1>).
- Accédez à la page Wireless, puis à l'onglet Wireless MAC Filter.
- Activez la case à cocher Enabled.
- Sélectionnez **Prevent PCs listed below from accessing the wireless network**.
- Entrez l'adresse MAC 00:05:4E:49:64:87.
- Cliquez sur **Save Settings**.

Les clients ayant l'adresse MAC 00:05:4E:49:64:87 ne pourront plus accéder au réseau sans fil.

**Access Restriction**

☒ Enabled ☐ Disabled

☒ Prevent PCs listed below from accessing the wireless network.  
☐ Permit PCs listed below to access the wireless network.

**MAC Address Filter List**

Wireless Client List

MAC 01:	00:05:4E:49:64:87	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00

### Étape 2 : sélection de la liste des clients sans fil

La zone **Wireless Client List** répertorie toutes les personnes actuellement connectées au routeur via une connexion sans fil. Remarquez la présence de l'option **Save to MAC filter list**. Quand vous sélectionnez cette option, l'adresse MAC du client visé s'ajoute automatiquement à la liste des adresses MAC afin de permettre ou interdire l'accès au réseau sans fil.

Connaissez-vous une manière fiable de réserver l'accès au réseau sans fil aux clients de votre choix uniquement ?

---

---

---

Pourquoi cela n'est-il pas possible dans les grands réseaux ?

---

---

---

Connaissez-vous une manière facile d'ajouter des adresses MAC si toutes les personnes à qui vous voulez autoriser l'accès sont déjà connectées au réseau sans fil ?

---

---

---

## Tâche 10 : définition des restrictions d'accès

Configurez une restriction d'accès capable d'empêcher les accès Telnet entre le lundi et le vendredi pour les utilisateurs ayant obtenu une adresse DHCP issue du pool prédéfini (172.17.30.50 – 74).

### Étape 1 : sélection de l'onglet Access Restrictions

Sous l'onglet Access Restrictions, entrez les valeurs suivantes :

- Enter Policy Name : No\_Telnet
- Status : **Enabled**
- Access Restriction : **Allow**
- Schedule : désactivez la case à cocher **Everyday** et activez les cases à cocher de **Lundi** à **Vendredi**
- Blocked Applications : ajoutez **Telnet** à Blocked List

**Internet Access Policy**

Access Policy: 1 ( ) Delete This Entry Summary

---

Enter Policy Name: No\_Telnet

Status: ☒ **Enabled** ☐ **Disabled**

---

**Applied PCs**

**Access Restriction**

**Schedule**

**Website Blocking by URL Address**

**Website Blocking by Keyword**

**Blocked Applications**

Edit List **(This Policy applies only to PCs on the List.)**

☐ **Deny** Internet access during selected days and hours.

☒ **Allow**

---

**Days:** ☐ Everyday ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

**Times:** ☒ 24 Hours ☐ 12 AM : 00 to 12 AM : 00

---

URL 1:  URL 3:

URL 2:  URL 4:

---

Keyword 1:  Keyword 3:

Keyword 2:  Keyword 4:

---

**Note:** only three applications can be blocked per policy.

Applications		Blocked List
<div style="border: 1px solid black; padding: 2px;">                     DNS (53 - 53)                      Ping (0 - 0)                      HTTP (80 - 80)                      HTTPS (443 - 443)                      FTP (21 - 21)                      POP3 (110 - 110)                      IMAP (143 - 143)                 </div>	<div style="border: 1px solid black; padding: 2px; margin: 2px;">&gt;&gt;</div> <div style="border: 1px solid black; padding: 2px; margin: 2px;">&lt;&lt;</div>	<div style="border: 1px solid black; padding: 2px;">                     Telnet (23 - 23)                 </div>

---

<b>Application Name</b>	<span style="border: 1px solid black; padding: 2px;">Telnet</span>	
<b>Port Range</b>	<div style="border: 1px solid black; padding: 2px; display: inline-block; width: 40px; text-align: center;">23</div> to <div style="border: 1px solid black; padding: 2px; display: inline-block; width: 40px; text-align: center;">23</div>	
<b>Protocol</b>	<span style="border: 1px solid black; padding: 2px;">TCP</span>	

Add
Modify
Delete

## Étape 2 : définition de la plage d'adresses IP

Appliquez cette configuration à tous ceux qui utilisent une adresse DHCP par défaut comprise dans l'intervalle 172.17.30.50 – 74.

Cliquez sur le bouton **Edit List** situé en haut de la fenêtre et entrez la plage d'adresses IP. Enregistrez les paramètres.

IP Address Range					
01	172 . 17 . 30 .	50	to	74	
02	172 . 17 . 30 .	0	to	0	
03	172 . 17 . 30 .	0	to	0	
04	172 . 17 . 30 .	0	to	0	

Cliquez sur le bouton **Save Settings** pour enregistrer les paramètres de restriction d'accès. Cliquez sur **Close** pour fermer la fenêtre et passer à la tâche suivante.

## Tâche 11 : gestion et sécurisation de l'utilitaire Web du routeur

### Étape 1 : configuration de l'accès au Web

Accédez à la section **Administration**. Remplacez le mot de passe du routeur par **cisco**.

Dans **Web Utility Access**, sélectionnez HTTP et HTTPS. La sélection de l'accès HTTPS permet à un administrateur réseau de gérer le routeur via l'adresse <https://172.17.30.1> avec SSL, une forme de protocole HTTP plus sécurisée. Si vous choisissez cette option, vous devrez accepter des certificats.

Web Access	
Web Utility Access:	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS
Web Utility Access via Wireless:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Dans la zone **Web Utility Access via Wireless**, sélectionnez **Enabled**. Si vous avez désactivé cette option, l'utilitaire Web ne sera pas accessible aux clients connectés sans fil. La désactivation de l'accès est une autre forme de sécurité qui demande à l'utilisateur de se connecter directement au routeur avant de changer les paramètres. Toutefois, dans ce scénario de travaux pratiques, vous configurez le routeur via l'accès sans fil et désactiver l'accès n'est donc pas approprié.

Cliquez sur le bouton **Save Settings** dans la partie inférieure de la fenêtre de configuration. Vous pouvez être invité à entrer le mot de passe configuré. Entrez **cisco** comme mot de passe, puis reconnectez-vous.

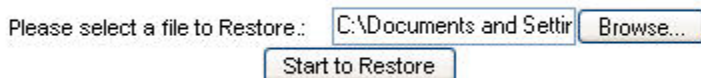
À présent, sauvegardez votre configuration en cliquant sur le bouton **Backup Configurations**. Enregistrez le fichier sur votre bureau à l'invite.

Backup and Restore	
<input type="button" value="Backup Configurations"/>	<input type="button" value="Restore Configurations"/>

## Étape 2 : restauration de la configuration

Si vos paramètres se perdent ou sont modifiés par accident ou malveillance, vous pouvez les restaurer depuis une configuration fonctionnelle à l'aide de l'option **Restore Configurations** située dans la section **Backup and Restore**.

Cliquez maintenant sur le bouton **Restore Configuration**. Dans la fenêtre Restore Configurations, recherchez le fichier de configuration que vous venez de sauvegarder. Cliquez sur le bouton **Start to Restore**. Les paramètres antérieurs doivent se restaurer.



## Étape 3 : activation de la journalisation

Sélectionnez l'onglet **Log** de la section **Administration**, puis activez la journalisation. Vous pouvez maintenant consulter le journal du routeur.



## Étape 4 : enregistrement des paramètres

### Tâche 12 : création et vérification de l'ensemble des connexions

#### Étape 1 : filtrage des requêtes Internet anonymes

Dans la page **Security**, désactivez la case à cocher **Filter Anonymous Internet Requests**. Une fois cette option désactivée, vous pouvez adresser une requête ping à l'adresse IP sans fil/réseau local interne de WRS3 (172.17.30.1) depuis les nœuds connectés à son port WAN. N'oubliez pas d'enregistrer vos paramètres en cliquant sur **Save**.



## Étape 2 : désactivation de la traduction d'adresses de réseau (NAT)

Dans la page **Setup**, cliquez sur l'onglet **Advanced Routing**. Désactivez NAT. N'oubliez pas d'enregistrer vos paramètres en cliquant sur **Save**.



## Étape 3 : connexion à WRS2

Maintenant que WRS3 a été configuré, il ne diffuse plus le SSID par défaut linksys. Mettez en marche le routeur sans fil WRS2 et effectuez des configurations similaires. Passez en revue les étapes précédentes pour connecter PC3 à WRS2 via une connexion sans fil.

Définissez les paramètres d'adresse IP dans la section Internet Setup.

- Dans Internet IP, tapez **172.17.88.25**.
- Dans Subnet Mask, tapez **255.255.255.0**.

Dans Default Gateway, tapez **172.17.88.1** (l'adresse IP du VLAN 88 FastEthernet 0/1 de R1).

Dans Network Setup IP, tapez **172.17.40.1**.

Établissez un lien statique entre l'adresse MAC de PC3 et l'adresse DHCP **172.17.40.23**.

Remplacez le SSID sans fil par **WRS2\_[numéro]**.

## Étape 4 : attribution de routes statiques vers les réseaux 172.17.30.0 et 172.17.40.0 à R1

```
R1(config)#ip route 172.17.30.0 255.255.255.0 172.17.88.35  
R1(config)#ip route 172.17.40.0 255.255.255.0 172.17.88.25
```

## Étape 5 : répétition des étapes 1 et 2 pour WRS2

Désactivez la case à cocher Filter anonymous Internet requests.

Désactivez NAT.

## Étape 6: vérification de la connectivité

Vérifiez que le routeur R1 dispose de routes vers les nœuds PC3 et PC6 et qu'il peut leur adresser des requêtes ping.

**R1#sh ip route**

<résultat omis>

Gateway of last resort is not set

```
      172.17.0.0/24 is subnetted, 5 subnets
S       172.17.40.0 [1/0] via 172.17.88.25
S       172.17.30.0 [1/0] via 172.17.88.35
C       172.17.20.0 is directly connected, FastEthernet0/1.20
C       172.17.10.0 is directly connected, FastEthernet0/1.10
C       172.17.88.0 is directly connected, FastEthernet0/1.88
      10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback0
```

**R1#ping 172.17.30.26**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.17.30.26, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

**R1#ping 172.17.40.23**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.17.40.23, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Vérifiez que PC3 et PC6 peuvent envoyer une requête ping à la boucle de R1.

Vérifiez que PC3 et PC6 peuvent mutuellement s'adresser des requêtes ping.

Vérifiez que PC3 et PC6 peuvent adresser des requêtes ping à PC1 et PC2.

```
Adresse IP. . . . . : 172.17.30.26
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 172.17.30.1

C:\Documents and Settings\Administrator>ping 10.1.1.1

Envoi d'une requête 'ping' sur 10.1.1.11.1 avec 32 octets de données

Réponse de 10.1.1.1: octets=32 temps=1ms TTL=254
Réponse de 10.1.1.1: octets=32 temps=1ms TTL=254
Réponse de 10.1.1.1: octets=32 temps=1ms TTL=254
Réponse de 10.1.1.1: octets=32 temps=1ms TTL=254

Statistiques Ping pour 10.1.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Documents and Settings\Administrator>ping 172.17.40.23

Envoi d'une requête 'ping' sur 172.17.40.23 avec 32 octets de données

Réponse de 172.17.40.23: octets=32 temps=1ms TTL=254
Réponse de 172.17.40.23: octets=32 temps=1ms TTL=254
Réponse de 172.17.40.23: octets=32 temps=1ms TTL=254
Réponse de 172.17.40.23: octets=32 temps=1ms TTL=254

Statistiques Ping pour 172.17.40.23:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Documents and Settings\Administrator>ping 172.17.10.21

Envoi d'une requête 'ping' sur 172.17.10.21 avec 32 octets de données

Réponse de 172.17.10.21: octets=32 temps=1ms TTL=254
Réponse de 172.17.10.21: octets=32 temps=1ms TTL=254
Réponse de 172.17.10.21: octets=32 temps=1ms TTL=254
Réponse de 172.17.10.21: octets=32 temps=1ms TTL=254

Statistiques Ping pour 172.17.10.21:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

De  
PC6

Vers la  
boucle  
de R1

Vers PC3

Vers PC1

## Tâche 13 : configuration du routage

### Étape 1 : utilisation de Traceroute pour voir la connexion réseau

R1 étant la passerelle par défaut, le routeur Linksys passe par lui pour accéder à un réseau qu'il ne sait pas comment joindre. Ceci vaut aussi pour les clients des autres routeurs Linksys.

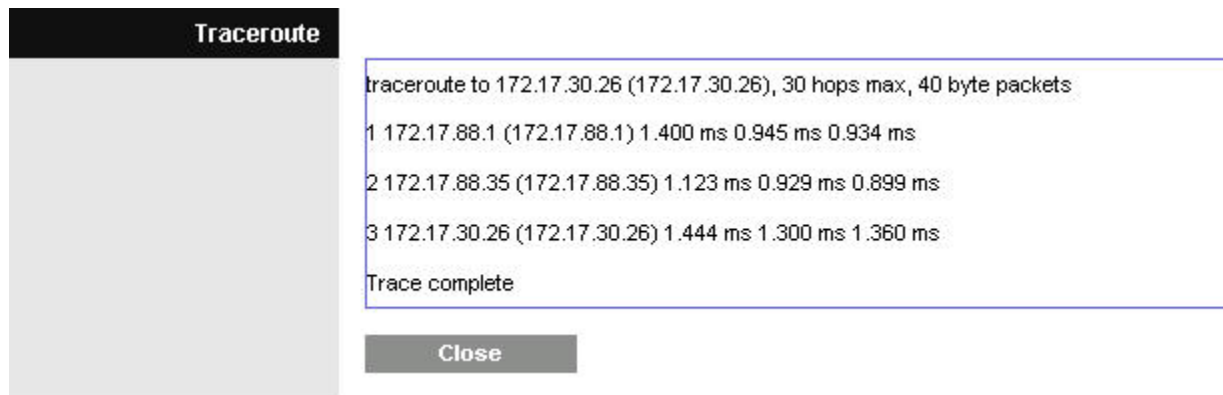
Un paquet envoyé par PC3 à PC6 atteint d'abord la passerelle par défaut 172.17.40.1, puis il est envoyé à l'interface WAN de WRS2 (172.17.88.25) vers la passerelle par défaut de WRS2 (172.17.88.1). Ensuite, R1 envoie le paquet à l'interface WAN de WRS3 (172.17.88.35) où WRS3 le prend en charge.

Sur WRS2, vous pouvez le vérifier sous l'onglet **Diagnostics** de la section Administration. Dans le champ Traceroute Test, entrez l'adresse IP de PC6, 172.17.30.26.

Traceroute Test	IP or URL Address:	<input type="text" value="172.17.30.26"/>
		<input type="button" value="Start to Traceroute"/>



Ensuite cliquez sur Start to Traceroute. Un message instantané apparaît.



Si WRS2 savait qu'il pouvait accéder au réseau 172.17.30.0 depuis l'adresse 172.17.88.35, il enverrait le paquet directement à cette adresse IP. Alors dites-le lui !

## Étape 2 : configuration d'une nouvelle route

Sur WRS2, dans la page **Setup**, cliquez sur l'onglet **Advanced Routing**. Pour la section Static Routing, entrez les paramètres suivants :

- Dans le champ **Route Name**, entrez **To WRS3 Clients**.
- Dans le champ **Destination LAN IP**, entrez l'adresse du réseau situé derrière WRS3 : **172.17.30.0**.
- Entrez **255.255.255.0** comme masque de sous-réseau.
- Entrez **172.17.88.35** comme passerelle.
- Dans le champ Interface, sélectionnez **Internet (WAN)**.
- Enregistrez vos paramètres.

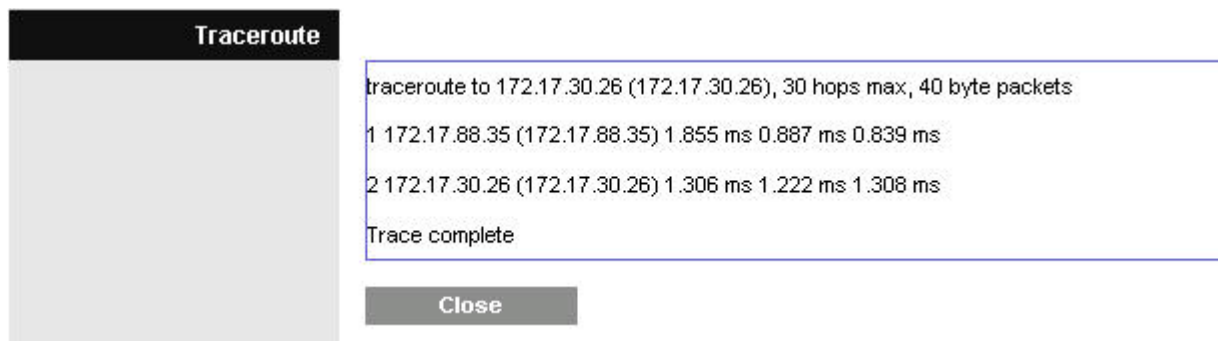
The screenshot shows the "Static Routing" configuration page. It has a "Route Entries" section with a dropdown menu showing "1 ()" and a "Delete This Entry" button. Below this, there are fields for "Enter Route Name:", "Destination LAN IP:", "Subnet Mask:", "Gateway:", and "Interface:". The values entered are:

- Enter Route Name: To WRS3 Clients
- Destination LAN IP: 172 . 17 . 30 . 0
- Subnet Mask: 255 . 255 . 255 . 0
- Gateway: 172 . 17 . 88 . 35
- Interface: Internet (WAN)

At the bottom, there is a "Show Routing Table" button.

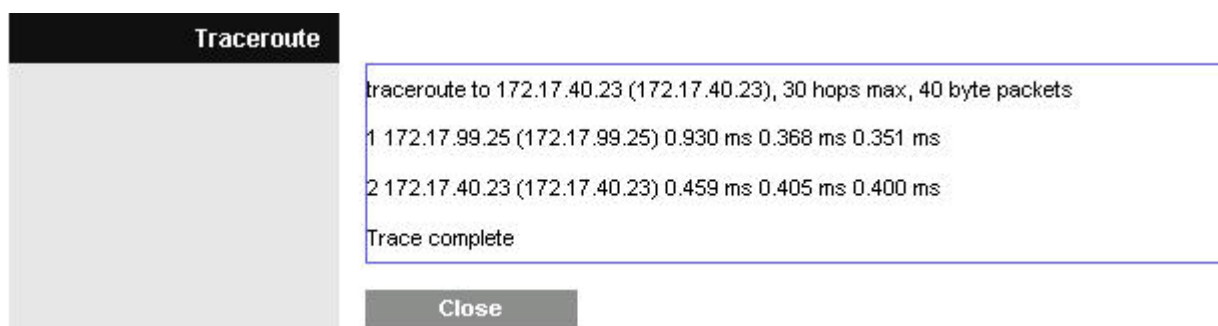
### Étape 3 : vérification de la nouvelle route

Sous l'onglet **Diagnostics** de la section Administration, entrez à nouveau l'adresse IP de PC3 dans le champ Traceroute Test. Cliquez sur **Start to Traceroute** pour afficher la route.



Notez que WRS2 va directement à WRS3 sans passer par R1.

Faites la même chose pour WRS3 avec le réseau 172.17.40.0/24 en pointant vers l'interface WAN de WRS2 à l'adresse 172.17.88.25.



## Tâche 14 : configuration de la sécurité des ports

### Étape 1 : configuration de la sécurité des ports de PC1

Connectez-vous au commutateur S2. Configurez le port de commutateur PC1, activez la sécurité des ports de l'interface FastEthernet 0/11 et activez les adresses permanentes MAC dynamiques.

### Étape 2 : configuration de la sécurité des ports de PC2

Répétez l'opération pour FastEthernet 0/18.

### Étape 3 : création de trafic entre les ports via une requête ping entre PC1 et PC2

#### Étape 4 : vérification de la sécurité du port

**S2#show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
----	-----	----	-----	-----
10	0006.5b1e.33fa	SecureSticky	Fa0/11	-
20	0001.4ac2.22ca	SecureSticky	Fa0/18	-

Total Addresses in System (excluding one mac per port) : 0  
Max Addresses limit in System (excluding one mac per port) : 6272

**S2#show port-security interface FastEthernet 0/11**

Port Security : Enabled  
Port Status : Secure-up  
Violation Mode : Shutdown  
Aging Time : 0 mins  
Aging Type : Absolute  
SecureStatic Address Aging : Disabled  
Maximum MAC Addresses : 1  
Total MAC Addresses : 1  
Configured MAC Addresses : 0  
Sticky MAC Addresses : 1  
Last Source Address:Vlan : 0006.5b1e.33fa:10  
Security Violation Count : 0

### Tâche 15 : restauration des paramètres par défaut des routeurs WRT300N

#### Étape 1 : suppression des paramètres des deux routeurs WRT300N

Pour rétablir les paramètres par défaut des deux routeurs WRT300N, accédez à la page Administration, cliquez sur **Factory Defaults**, puis sur le bouton **Restore All Settings**.