Cisco | Networking Academy®
Mind Wide Open™

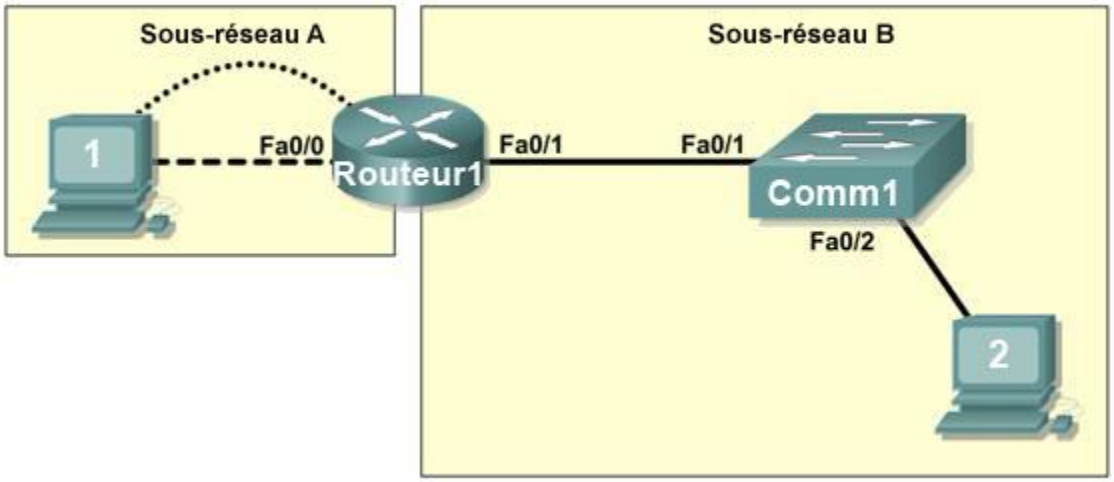
CCNA Exploration 4.0

Commutation de réseau local et réseau local sans fil

Manuel des travaux pratiques du participant

Travaux pratiques 1.3.1 : révision des concepts d'Exploration 1

Diagramme de topologie



Objectifs pédagogiques

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

- Créer une topologie logique selon les besoins d'un réseau
- Créer des sous-réseaux pour satisfaire les besoins en hôtes
- Configurer la topologie physique
- Configurer la topologie logique
- Vérifier la connectivité réseau
- Configurer et vérifier les mots de passe

Scénario

Au cours de ces travaux pratiques, vous allez concevoir et configurer un réseau routé de petite taille et vérifier la connectivité sur plusieurs périphériques réseau. Pour ce faire, vous devez créer et affecter deux blocs de sous-réseaux, connecter les hôtes et les périphériques réseau et configurer les ordinateurs hôtes ainsi qu'un routeur Cisco pour une connectivité réseau de base. Le commutateur Comm1 est configuré par défaut. Nous allons employer des commandes courantes pour tester et documenter le réseau. Nous utiliserons le sous-réseau zéro.

Tâche 1 : conception de la topologie logique d'un réseau local

Étape 1 : conception d'un modèle d'adressage IP

D'après le bloc d'adresses IP de **192.168.7.0 /24**, concevez un modèle d'adressage IP satisfaisant les exigences suivantes :

Sous-réseau	Nombre d'hôtes
Sous-réseau A	110
Sous-réseau B	54

Nous utiliserons le sous-réseau zéro. Les calculatrices de sous-réseau ne sont pas autorisées. Créez les plus petits sous-réseaux possibles satisfaisant les exigences en matière d'hôtes. Affectez le premier sous-réseau utilisable au sous-réseau A.

Sous-réseau A	
Spécification	**Saisie du participant**
Nombre de bits dans le sous-réseau	
Masque IP (binaire)	
Nouveau masque IP (décimal)	
Nombre maximal de sous-réseaux utilisables (y compris le sous-réseau 0)	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau IP	
Première adresse hôte IP	
Dernière adresse hôte IP	

Sous-réseau B	
Spécification	**Saisie du participant**
Nombre de bits dans le sous-réseau	
Masque IP (binaire)	
Nouveau masque IP (décimal)	
Nombre maximal de sous-réseaux utilisables (y compris le sous-réseau 0)	
Nombre d'hôtes utilisables par sous-réseau	
Adresse réseau IP	
Première adresse hôte IP	
Dernière adresse hôte IP	

Les ordinateurs hôtes utilisent la première adresse IP utilisable du sous-réseau. Le routeur du réseau utilise la dernière adresse IP utilisable du sous-réseau.

Étape 2 : inscription des informations d'adresse IP de chaque périphérique

Périphérique	Adresse IP	Masque	Passerelle
Hôte 1			
Routeur1-Fa0/0			
Hôte 2			
Routeur1-Fa0/1			

Tableau 1. Affectations d'adresses IP

Avant de poursuivre, vérifiez vos adresses IP en compagnie du formateur.

Tâche 2 : configuration de la topologie physique

Étape 1 : câblage du réseau

Reportez-vous à la figure et au tableau ci-dessous pour connaître les câbles nécessaires.

Câblage	Type de câble
Câble LAN entre l'hôte 1 et l'interface Fa0/0 de Routeur1	Croisé
Câble LAN entre Comm1 et l'interface Fa0/1 de Routeur1	Droit
Câble LAN entre Comm1 et l'hôte 2	Droit
Câble console entre l'hôte 1 et Routeur1	À paires inversées

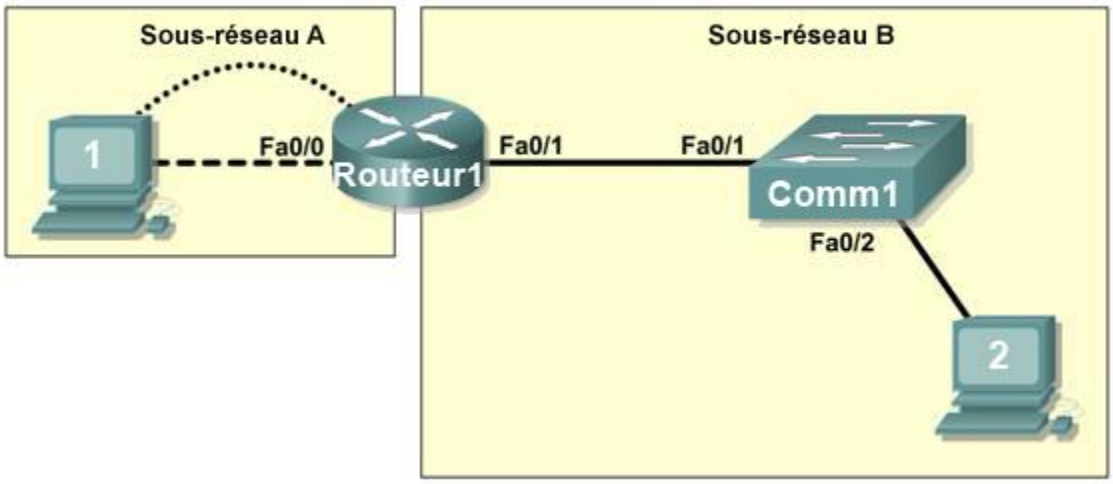


Figure 1. Câblage du réseau

Étape 2 : connexion physique des périphériques des travaux pratiques

Reliez les périphériques réseau comme indiqué dans la figure 1. S'ils ne le sont pas déjà, mettez tous les périphériques sous tension.

Étape 3 : inspection des connexions réseau

Vérifiez visuellement les connexions.

Tâche 3 : configuration de la topologie logique

Étape 1 : configuration des ordinateurs hôtes

Configurez l'adresse IP statique, le masque de sous-réseau et la passerelle pour chaque ordinateur hôte.

Remarque : les instructions suivantes concernent Windows XP. Pour configurer les hôtes à l'aide de systèmes d'exploitation différents, reportez-vous au manuel du système d'exploitation.

Pour configurer l'hôte, cliquez sur **Démarrer > Panneau de configuration > Connexions réseau > Connexion au réseau local**. Dans la fenêtre Propriétés de Connexion au réseau local, sélectionnez **Protocole Internet (TCP/IP)** et cliquez sur le bouton **Propriétés**.

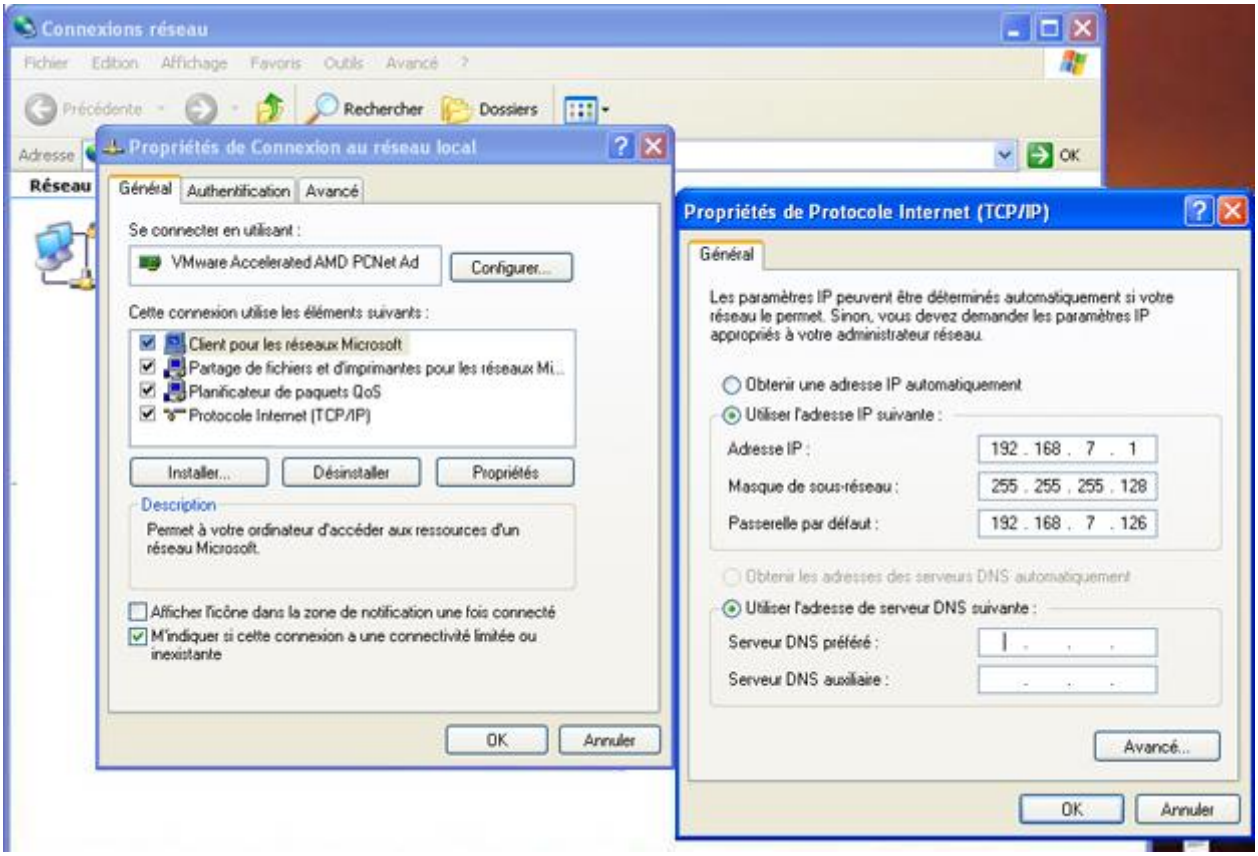


Figure 2. Définition des propriétés pour le protocole Internet (TCP/IP)

Dans la boîte de dialogue Propriétés du protocole Internet TCP/IP de chaque hôte, entrez l'adresse IP, le masque de réseau et la passerelle du Tableau 1.

Après la configuration de chaque ordinateur hôte, ouvrez une fenêtre de commande sur l'hôte en sélectionnant **Démarrer > Exécuter**. Lorsqu'un message vous demande de taper le nom d'un programme, entrez **cmd** dans la zone de texte. Dans la fenêtre de commande, affichez et vérifiez les paramètres réseau de l'hôte avec la commande **ipconfig /all**. Les paramètres doivent correspondre à ceux des tableaux ci-dessous :

Configuration réseau hôte 1	
Adresse IP	192.168.7.1
Masque de sous-réseau	255.255.255.128
Passerelle par défaut	192.168.7.126

Configuration réseau hôte 2	
Adresse IP	192.168.7.129
Masque de sous-réseau	255.255.255.192
Passerelle par défaut	192.168.7.190

Les paramètres des hôtes sont-ils conformes aux tableaux ? _____ Si ce n'est pas le cas, reconfigurez-les comme il convient.

Étape 2 : configuration du Routeur1

Depuis l'hôte 1, établissez une connexion à la console du routeur 1 et une session en mode console. Les instructions concernant la création d'une connexion console à l'aide du logiciel HyperTerminal figurent dans l'annexe 2.

Dans la console du routeur, configurez les éléments suivants :

Tâche	Spécification
Nom du routeur	`Routeur1`
Mot de passe chiffré en mode d'exécution privilégié	`cisco`
Mot de passe d'accès à la console	`class`
Mot de passe d'accès Telnet	`class`
Routeur1-Fa0/0	Indiquez la description. Définissez l'adresse de couche 3.
Routeur1-Fa0/1	Indiquez la description. Définissez l'adresse de couche 3.

Entrez les commandes suivantes sur le routeur :

```
Router>enable
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Routeur1
Routeur1(config)#enable secret class
Routeur1(config)#line console 0
Routeur1(config-line)#password cisco
Routeur1(config-line)#login
Routeur1(config-line)#line vty 0 4
```

```
Routeur1(config-line)#password cisco
Routeur1(config-line)#login
Routeur1(config-line)#interface fa0/0
Routeur1(config-if)#ip address 192.168.7.126  255.255.255.128
Routeur1(config-if)#no shutdown
Routeur1(config-if)#description connection to hôte1
Routeur1(config-if)#interface fa0/1
Routeur1(config-if)#description connection to comm1
Routeur1(config-if)#ip address 192.168.7.190 255.255.255.192
Routeur1(config-if)#no shutdown
Routeur1(config-if)#end
Routeur1#
```

Tâche 4 : vérification de la connectivité réseau

Étape 1 : vérification de la connectivité réseau à l'aide de la commande ping

Vous pouvez vérifier la connectivité réseau à l'aide de la commande **ping**.

Remarque : si vous n'obtenez pas de résultats en interrogeant les ordinateurs hôtes via la commande ping, désactivez provisoirement le pare-feu sur l'ordinateur et relancez le test. Pour désactiver un pare-feu Windows, sélectionnez **Démarrer > Panneau de configuration > Pare-feu Windows**, choisissez **Désactivé**, puis **OK**.

Pour vérifier la connectivité avec chaque périphérique réseau, servez-vous du tableau ci-dessous. Lorsque le test n'est pas concluant, faites le nécessaire pour établir la connectivité.

De	À	Adresse IP	Résultats de la requête ping
Hôte 1	Adresse IP de la carte réseau	192.168.7.1	
Hôte 1	Routeur1, Fa0/0	192.168.7.126	
Hôte 1	Routeur1, Fa0/1	192.168.7.190	
Hôte 1	Hôte 2	192.168.7.129	
Hôte 2	Adresse IP de la carte réseau	192.168.7.129	
Hôte 2	Routeur1, Fa0/1	192.168.7.190	
Hôte 2	Routeur1, Fa0/0	192.168.7.126	
Hôte 2	Hôte 1	192.168.7.1	

Outre la commande **ping**, quelles sont les autres commandes Windows permettant d'afficher les délais et les interruptions dans le transfert vers la destination ? _____

Tâche 5 : vérification des mots de passe

Étape 1 : envoi d'une requête Telnet depuis l'hôte 2 au routeur et vérification du mot de passe Telnet

Vous devez être en mesure d'accéder à l'interface Fast Ethernet du routeur via Telnet.

Dans une fenêtre de commande sur l'hôte 2, tapez :

```
telnet 192.168.7.190
```

Lorsqu'un message vous invite à entrer le mot de passe Telnet, tapez **cisco** et appuyez sur Entrée.

La requête Telnet a-t-elle abouti ? _____

Étape 2 : vérification de la définition du mot de passe secret actif

Depuis la session Telnet, entrez en mode d'exécution privilégié et vérifiez qu'il est protégé par un mot de passe :

```
Router>enable
```

Avez-vous été invité à entrer le mot de passe secret actif ? _____

Étape 3 : vérification de la protection de la console par un mot de passe

Mettez fin à la connexion console de l'hôte 1 au routeur puis rétablissez-la pour vérifier que la console est protégée par un mot de passe.

En fonction du client Telnet que vous utilisez, vous pouvez généralement terminer la session avec Ctrl-]. Lorsque la session est rétablie, un message doit vous demander le mot de passe de la console avant que vous ne puissiez accéder à l'interface de ligne de commande.

Tâche 6 : remarques générales

En quoi l'accès Telnet et l'accès à la console sont-ils différents ? Dans quel cas peut-il être judicieux de définir des mots de passe différents sur ces deux ports d'accès ?

_____

_____

Pourquoi le commutateur entre l'hôte 2 et le routeur ne nécessite-t-il pas de configuration avec une adresse IP pour acheminer les paquets ?

_____

_____

Tâche 7 : remise en état

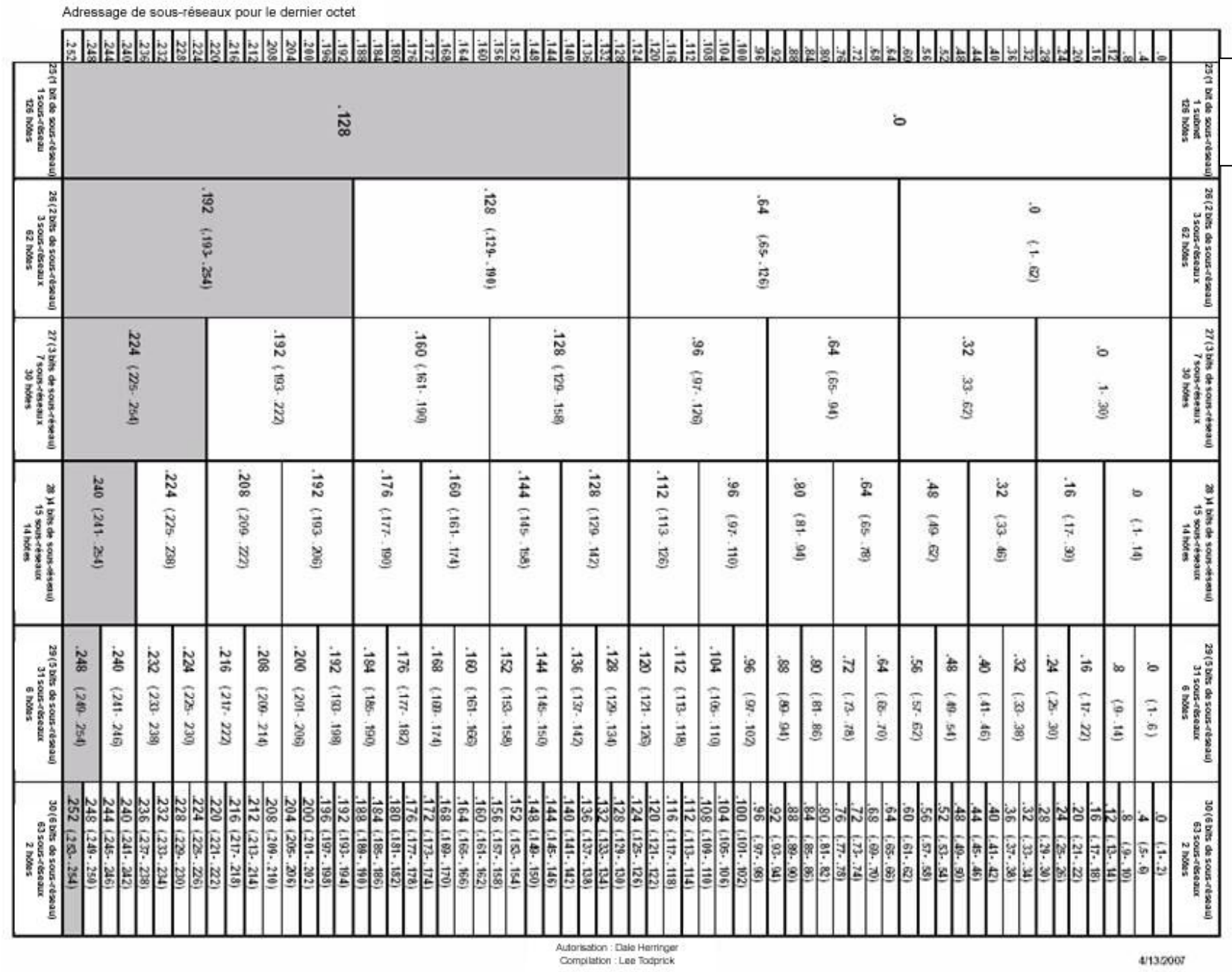
Sauf indication contraire de votre formateur, effacez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Configuration finale du routeur 1

```
Routeur1#show run
<partie du résultat omise>
!
hostname Routeur1
!
enable secret class
!
!
 interface FastEthernet0/0
 description connection to hôte1
 ip address 192.168.7.126 255.255.255.128
```

```
 no shutdown
!
interface FastEthernet0/1
 description connection to comm1
 ip address 192.168.7.190 255.255.255.192
 no shutdown
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Annexe 1 : diagramme du sous-réseau pour le dernier octet



1 subnet should be 1 sous-réseau

Annexe 2 : création d'une session en mode console du routeur à l'aide du logiciel HyperTerminal

Tâche 1 : connexion d'un routeur et d'un ordinateur à l'aide d'un câble console

Étape 1 : configuration d'une connexion physique de base

Connectez le câble console (à paires inversées) au port de console du routeur. Connectez l'autre extrémité du câble au port COM 1 de l'ordinateur hôte avec un adaptateur DB-9 ou DB-25.

Étape 2 : mise sous tension des périphériques

Si ce n'est déjà fait, mettez l'ordinateur et le routeur sous tension.

Tâche 2 : configuration d'HyperTerminal en vue d'ouvrir une session en mode console avec un routeur Cisco IOS

Étape 1 : démarrage de l'application HyperTerminal

Démarrez le programme HyperTerminal en cliquant sur **Démarrer > Programmes > Accessoires > Communications > HyperTerminal**.

Étape 2 : configuration d'HyperTerminal

Figure 3. Fenêtre de configuration du nom de session dans HyperTerminal

Dans la fenêtre Description de la connexion, entrez un nom de session dans le champ Nom. Sélectionnez une icône ou conservez l'icône par défaut. Cliquez sur **OK**.

Figure 4. Type de connexion HyperTerminal

Entrez COM 1 dans le champ Se connecter en utilisant, puis cliquez sur **OK**. (Selon le PC que vous utilisez, il peut s'avérer nécessaire d'utiliser un port COM différent. Si COM 1 ne fonctionne pas, essayez systématiquement les ports COM supplémentaires jusqu'à ce que vous réussissiez.)

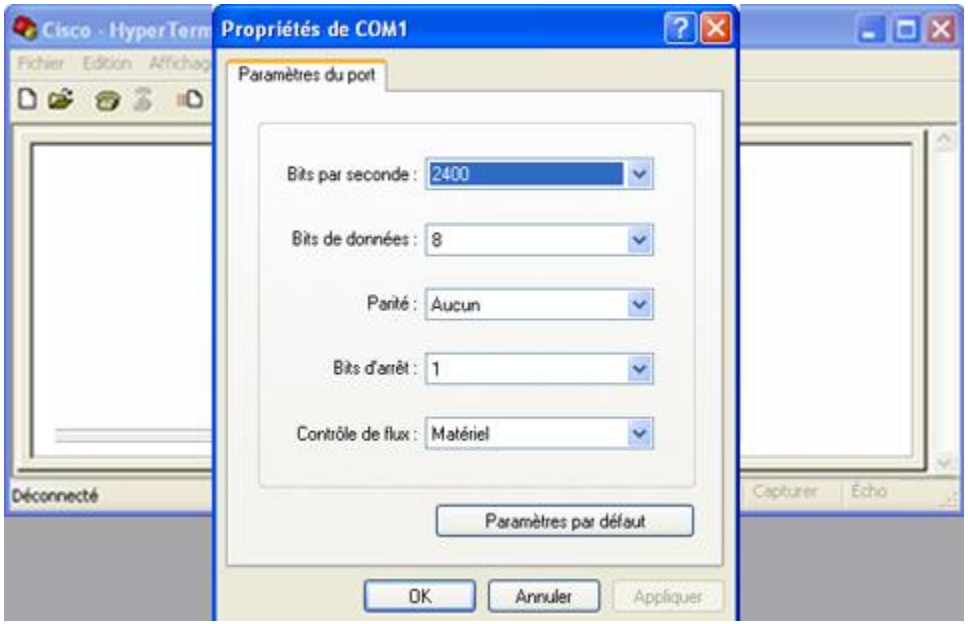


Figure 5. Paramètres du port COM1 dans HyperTerminal

Comme indiqué dans la figure 3, remplacez les paramètres du port par les valeurs suivantes, puis cliquez sur **OK** :

Paramètre	**Valeur**
Bits par seconde	**9600**
Bits de données	**8**
Parité	**aucune**
Bits d'arrêt	**1**
Contrôle de flux	**aucune**

Lorsque la fenêtre de la session HyperTerminal s'affiche, appuyez sur **Entrée**. Le routeur doit répondre. Cela indique que la connexion a été établie. En l'absence de connexion, recherchez les causes du problème. Par exemple, vérifiez que le routeur est sous tension. Assurez-vous que le câble est bien connecté au port COM 1 du PC et au port de console du routeur. S'il n'y a toujours pas de connexion, demandez de l'aide au formateur.

Étape 3 : fermeture d'HyperTerminal

Lorsque vous avez terminé, fermez la session HyperTerminal en sélectionnant **Fichier > Quitter**. Lorsque vous êtes invité à enregistrer la session, cliquez sur **Oui**. Attribuez un nom à la session.

Étape 4 : reconnexion de la session HyperTerminal

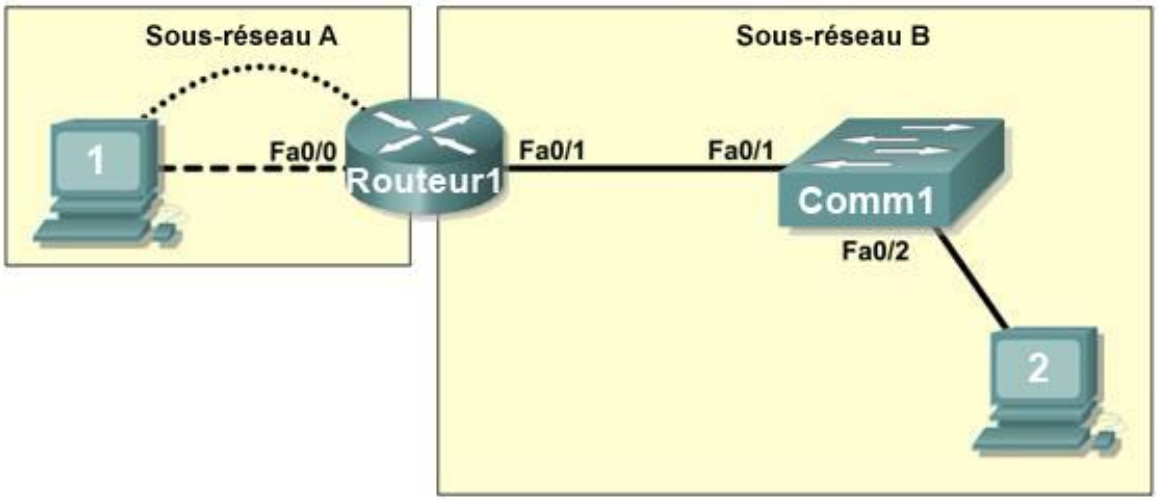
Rouvrez la session HyperTerminal, comme indiqué à l'étape 1 de la tâche 2. Cette fois, cliquez sur **Annuler** lorsque la fenêtre Description de la connexion s'affiche (voir Figure 3).

Cliquez sur **Fichier > Ouvrir**. Sélectionnez la session enregistrée, puis cliquez sur **Ouvrir**. Employez cette étape pour reconnecter la session HyperTerminal à un périphérique Cisco sans avoir à reconfigurer une nouvelle session.

Lorsque vous avez terminé, quittez HyperTerminal.

Travaux pratiques 1.3.2 : révision des concepts d'Exploration 1 : exercice

Diagramme de topologie



Objectifs pédagogiques

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

- Créer une topologie logique selon les besoins d'un réseau
- Créer des sous-réseaux pour satisfaire les besoins en hôtes
- Configurer la topologie physique
- Configurer la topologie logique
- Vérifier la connectivité réseau
- Configurer et vérifier les mots de passe

Scénario

Au cours de ces travaux pratiques, vous allez concevoir et configurer un réseau routé de petite taille et vérifier la connectivité sur plusieurs périphériques réseau. Pour ce faire, vous devez créer et affecter deux blocs de sous-réseaux, connecter les hôtes et les périphériques réseau et configurer les ordinateurs hôtes ainsi qu'un routeur Cisco pour une connectivité réseau de base. Le commutateur Comm1 est configuré par défaut. Nous allons employer des commandes courantes pour tester et documenter le réseau. Nous utiliserons le sous-réseau zéro.

Tâche 1 : conception de la topologie logique d'un réseau local

Étape 1 : conception d'un modèle d'adressage IP

D'après le bloc d'adresses IP de **192.168.30.0 /27**, concevez un modèle d'adressage IP satisfaisant les exigences suivantes :

Sous-réseau	Nombre d'hôtes
Sous-réseau A	7
Sous-réseau B	14

Nous utiliserons le sous-réseau zéro. Les calculatrices de sous-réseau ne sont pas autorisées. Créez le plus petit nombre possible de sous-réseaux satisfaisant les exigences en matière d'hôtes. Affectez le premier sous-réseau utilisable au sous-réseau A.

Sous-réseau A	
Spécification	**Saisie du participant**
Nombre de bits dans le sous-réseau	
Masque IP (binaire)	
Nouveau masque IP (décimal)	
Nombre maximal de sous-réseaux utilisables (y compris le sous-réseau 0)	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau IP	
Première adresse hôte IP	
Dernière adresse hôte IP	

Sous-réseau B	
Spécification	**Saisie du participant**
Nombre de bits dans le sous-réseau	
Masque IP (binaire)	
Nouveau masque IP (décimal)	
Nombre maximal de sous-réseaux utilisables (y compris le sous-réseau 0)	
Nombre d'hôtes utilisables par sous-réseau	
Adresse de sous-réseau IP	
Première adresse hôte IP	
Dernière adresse hôte IP	

Les ordinateurs hôtes utilisent la première adresse IP du sous-réseau. Le routeur du réseau utilise la dernière adresse IP du sous-réseau.

Étape 2 : inscription des informations d'adresse IP de chaque périphérique

Périphérique	Adresse IP	Masque	Passerelle
Hôte 1			
Routeur1-Fa0/0			
Hôte 2			
Routeur1-Fa0/1			

Avant de poursuivre, vérifiez vos adresses IP en compagnie du formateur.

Tâche 2 : configuration de la topologie physique

Étape 1 : détermination des besoins en câbles

D'après la figure 1, identifiez chaque type de câble requis et documentez-le dans le tableau.

Câblage correct	Type de câble
Câble LAN entre l'hôte 1 et l'interface Fa0/0 de Routeur1	
Câble LAN entre Comm1 et l'interface Fa0/1 de Routeur1	
Câble LAN entre Comm1 et l'hôte 2	
Câble console entre l'hôte 1 et Routeur1	

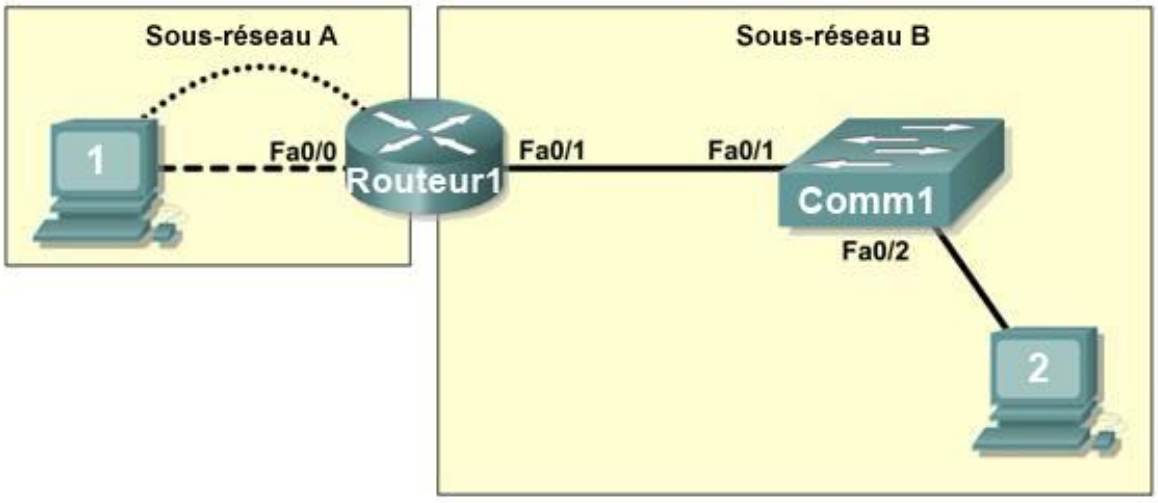


Figure 1. Câblage du réseau

Étape 2 : connexion physique des périphériques des travaux pratiques

Reliez les périphériques réseau comme indiqué dans la figure 1. S'ils ne le sont pas déjà, mettez tous les périphériques sous tension.

Étape 3 : inspection des connexions réseau

Après avoir câblé les périphériques réseau, vérifiez les connexions.

Tâche 3 : configuration de la topologie logique

Étape 1 : configuration des ordinateurs hôtes

Configurez l'adresse IP statique, le masque de sous-réseau et la passerelle pour chaque ordinateur hôte. Après avoir configuré chaque ordinateur hôte, affichez et vérifiez les paramètres réseau de l'hôte à l'aide de la commande **ipconfig /all**.

Configuration réseau hôte 1	
Adresse physique	
Adresse IP	
Masque de sous-réseau	
Passerelle par défaut	

Configuration réseau hôte 2	
Adresse physique	
Adresse IP	
Masque de sous-réseau	
Passerelle par défaut	

Étape 2 : configuration du Routeur1

Depuis l'hôte 1, établissez une connexion à la console du routeur 1 et configurez les éléments suivants :

Tâche	Spécification
Nom du routeur	`Routeur1`
Mot de passe chiffré en mode d'exécution privilégié	`class`
Mot de passe d'accès à la console	`cisco`
Mot de passe d'accès Telnet	`cisco`
Routeur1-Fa0/0	Indiquez la description. Définissez l'adresse de couche 3.
Routeur1-Fa0/1	Indiquez la description. Définissez l'adresse de couche 3.

Tâche 4 : vérification de la connectivité réseau

Étape 1 : vérification de la connectivité réseau à l'aide de la commande ping

Vous pouvez vérifier la connectivité réseau à l'aide de la commande **ping**.

Remarque : si vous n'obtenez pas de résultats en interrogeant les ordinateurs hôtes via la commande ping, vérifiez l'existence d'un programme de pare-feu exécuté sur les hôtes. Si un pare-feu est exécuté sur l'hôte, désactivez-le provisoirement et relancez le test. Pour désactiver un pare-feu Windows, sélectionnez **Démarrer > Panneau de configuration > Pare-feu Windows**, choisissez **Désactivé**, puis **OK**.

Pour vérifier la connectivité avec chaque périphérique réseau, servez-vous du tableau ci-dessous. Lorsque le test n'est pas concluant, faites le nécessaire pour établir la connectivité.

De	À	Adresse IP	Résultats de la requête ping
Hôte 1	Adresse IP de la carte réseau		
Hôte 1	Routeur1, Fa0/0		
Hôte 1	Routeur1, Fa0/1		
Hôte 1	Hôte 2		
Hôte 2	Adresse IP de la carte réseau		
Hôte 2	Routeur1, Fa0/1		
Hôte 2	Routeur1, Fa0/0		
Hôte 2	Hôte 1		

Outre la commande **ping**, quelles sont les autres commandes Windows permettant d'afficher les délais et les interruptions dans le transfert vers la destination ? _____

Tâche 5 : vérification des mots de passe

Étape 1 : envoi d'une requête Telnet depuis l'hôte 2 au routeur et vérification du mot de passe Telnet

Vous devez être en mesure d'accéder à l'interface Fast Ethernet du routeur via Telnet.

Étape 2 : vérification de la définition du mot de passe secret actif

Depuis la session Telnet, entrez en mode d'exécution privilégié et vérifiez qu'il est protégé par un mot de passe.

Étape 3 : vérification de la protection de la console par un mot de passe

Mettez fin à la connexion console de l'hôte 1 au routeur puis rétablissez-la pour vérifier que la console est protégée par un mot de passe.

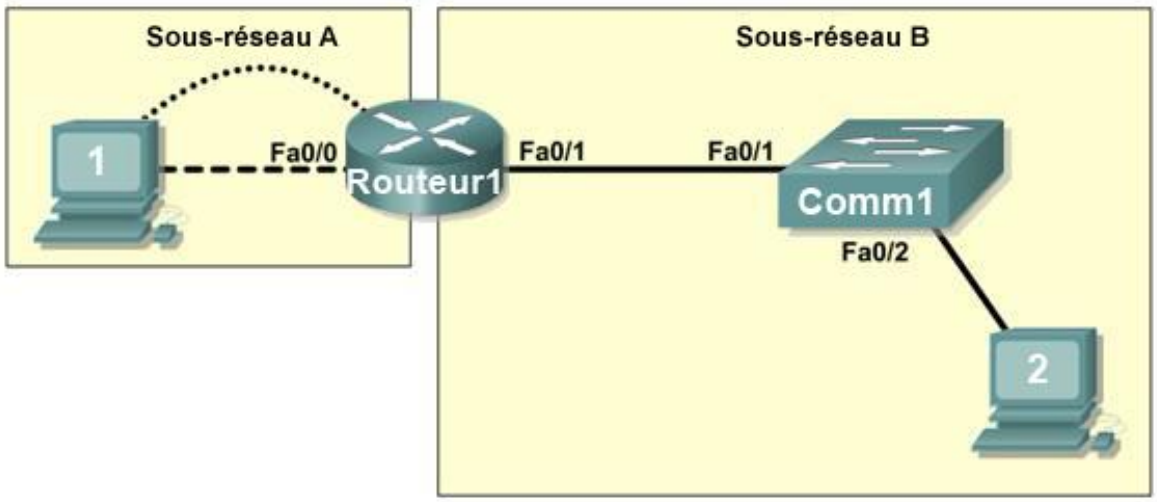
En fonction du client Telnet que vous utilisez, vous pouvez généralement terminer la session avec Ctrl-].

Tâche 6 : remise en état

Sauf indication contraire de votre formateur, effacez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 1.3.3 : dépannage d'un petit réseau

Diagramme de topologie



Objectifs pédagogiques

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

- Vérifier qu'une conception par écrit satisfait les besoins du réseau énoncés
- Installer un réseau conformément au diagramme de topologie
- Supprimer la configuration initiale et recharger un routeur pour revenir aux paramètres par défaut
- Charger les routeurs avec les scripts fournis
- Détecter rapidement les communications impossibles
- Réunir des informations sur la partie mal configurée du réseau, ainsi que toute autre erreur
- Analyser les informations pour déterminer pourquoi la communication n'est pas possible
- Proposer des solutions pour résoudre les erreurs de réseau
- Mettre en place des solutions pour résoudre les erreurs de réseau

Scénario

Au cours de ces travaux pratiques, vous allez découvrir la configuration complète d'un réseau routé de petite taille. La configuration contient des erreurs de conception et de configuration s'opposant aux exigences énoncées et empêchant toute communication de bout en bout. Vous allez examiner la conception donnée, puis identifier et corriger toutes les erreurs de conception. Vous câblerez ensuite le

réseau, configurerez les hôtes et chargerez des configurations sur le routeur. Enfin, vous résoudrez les problèmes de connectivité pour déterminer où surviennent les erreurs et vous les corrigerez à l'aide des commandes appropriées. Lorsque toutes les erreurs seront corrigées, chaque hôte devrait pouvoir communiquer avec tous les autres éléments du réseau configurés et avec l'autre hôte.

Tâche 1 : examen de la topologie logique d'un réseau local

Le bloc d'adresses IP de 172.16.30.0 /23 est divisé en sous-réseaux pour répondre aux exigences suivantes :

Sous-réseau	Nombre d'hôtes
Sous-réseau A	174
Sous-réseau B	60

Spécifications et exigences supplémentaires :

- Nous utiliserons le sous-réseau zéro.
- Utilisez le plus petit nombre de sous-réseaux satisfaisant les besoins en hôtes en conservant le plus grand bloc en réserve à des fins ultérieures.
- Affectez le premier sous-réseau utilisable au sous-réseau A.
- Les ordinateurs hôtes utilisent la première adresse IP utilisable du sous-réseau. Le routeur du réseau utilise la dernière adresse d'hôte utilisable du réseau.

En fonction de ces exigences, la topologie suivante vous est fournie :

Sous-réseau A	
Spécification	**Valeur**
Masque IP (décimal)	255.255.255.0
Adresse IP	172.16.30.0
Première adresse hôte IP	172.16.30.1
Dernière adresse hôte IP	172.16.30.254

Sous-réseau B	
Spécification	**Valeur**
Masque IP (décimal)	255.255.255.128
Adresse IP	172.16.31.0
Première adresse hôte IP	172.16.31.1
Dernière adresse hôte IP	172.16.31.126

Examinez chacune des valeurs dans les tableaux ci-dessus et vérifiez que cette topologie satisfait toutes les exigences et spécifications. Certaines de ces valeurs sont-elles incorrectes ? _____

Si oui, corrigez les valeurs dans le tableau ci-dessus et indiquez les valeurs corrigées ci-dessous :

_____

_____

Créez un tableau de configuration semblable au suivant à l'aide des valeurs corrigées :

Périphérique	Adresse IP	Masque	Passerelle
Hôte 1	172.16.30.1	255.255.255.0	172.16.30.254
Routeur1–Fa0/0	172.16.30.254	255.255.255.0	S/O
Hôte 2	172.16.31.1	255.255.255.128	172.16.31.126
Routeur1–Fa0/1	172.16.31.126	255.255.255.128	S/O

Tâche 2 : câblage, suppression et rechargement des routeurs

Étape 1 : câblage du réseau

Installez un réseau similaire à celui du diagramme de topologie.

Étape 2 : suppression de la configuration sur chaque routeur

Effacez la configuration du routeur à l'aide de la commande **erase startup-config** et rechargez le routeur. Répondez **non** si une fenêtre vous demande d'enregistrer les modifications.

Tâche 3 : configuration des ordinateurs hôtes

Étape 1 : configuration des ordinateurs hôtes

Configurez l'adresse IP statique, le masque de sous-réseau et la passerelle pour chaque ordinateur hôte d'après le tableau de configuration créé à la tâche 1. Après avoir configuré chaque ordinateur hôte, affichez et vérifiez les paramètres réseau de l'hôte à l'aide de la commande **ipconfig /all**.

Tâche 4 : chargement du routeur à l'aide des scripts fournis

```
enable
!
config term
!
hostname Routeur1
!
enable secret class
!
no ip domain-lookup
!
 interface FastEthernet0/0
 description connection to hôte1
 ip address 172.16.30.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description connection to comm1
 ip address 192.16.31.1 255.255.255.192
 duplex auto
 speed auto
!
!
line con 0
```

```
 password cisco
 login
line vty 0
 login
line vty 1 4
 password cisco
 login
!
end
```

Tâche 5 : identification des problèmes de connectivité

Étape 1 : utilisation de la commande ping pour tester la connectivité réseau

Pour tester la connectivité de chaque périphérique réseau, servez-vous du tableau ci-dessous.

De	À	Adresse IP	Résultats de la requête ping
Hôte 1	Adresse IP de la carte réseau	172.16.30.1	
Hôte 1	Routeur1, Fa0/0	172.16.30.254	
Hôte 1	Routeur1, Fa0/1	172.16.31.126	
Hôte 1	Hôte 2	172.16.31.1	
Hôte 2	Adresse IP de la carte réseau	172.16.30.1	
Hôte 2	Routeur1, Fa0/1	172.16.31.126	
Hôte 2	Routeur1, Fa0/0	172.16.30.254	
Hôte 2	Hôte 1	172.16.30.1	

Tâche 6 : dépannage des connexions réseau

Étape 1 : début du dépannage sur l'hôte connecté au routeur AGENCE

Est-il possible d'envoyer une requête ping au PC2 depuis l'hôte PC1 ? _____

Est-il possible d'envoyer une requête ping à l'interface fa0/1 du routeur depuis l'hôte PC1 ? _____

Est-il possible d'envoyer une requête ping à la passerelle par défaut depuis l'hôte PC1 ? _____

Est-il possible que l'hôte PC1 s'envoie lui-même une requête ping ? _____

Où est-il le plus logique de commencer le dépannage des problèmes de connexion PC1 ?

_____

_____

Étape 2 : examen du routeur afin de détecter d'éventuelles erreurs de configuration

Commencez par consulter le résumé des informations d'état relatives à chaque interface du routeur.

Avez-vous rencontré des difficultés avec l'état des interfaces ?

_____

_____

Si vous rencontrez des difficultés avec l'état des interfaces, enregistrez les commandes nécessaires pour la correction des erreurs de configuration.

_____

_____

Étape 3 : utilisation des commandes nécessaires pour corriger la configuration du routeur

Étape 4 : affichage du résumé des informations d'état

Si la configuration a été modifiée à l'étape précédente, consultez le résumé des informations d'état relatives aux interfaces du routeur.

Les informations sur le résumé de l'état des interfaces indiquent-elles des erreurs de configuration sur le routeur 1 ? _____

Si la réponse est **oui**, dépannez l'état des interfaces.

La connectivité a-t-elle été restaurée ? _____

Étape 5 : vérification de la configuration logique

Examinez l'état complet de Fa 0/0 et 0/1. Les informations concernant les adresses IP et le masque de sous-réseau de l'état de l'interface sont-elles cohérentes avec le tableau de configuration ? _____

Si le tableau de configuration et la configuration de l'interface du routeur sont différents, enregistrez les commandes nécessaires pour corriger la configuration du routeur.

_____

_____

La connectivité a-t-elle été restaurée ? _____

Pourquoi est-il utile pour un hôte d'envoyer une requête ping à sa propre adresse ?

_____

_____

Tâche 7 : remise en état

Sauf indication contraire de votre formateur, effacez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 2.5.1 : configuration de base d'un commutateur

Topologie

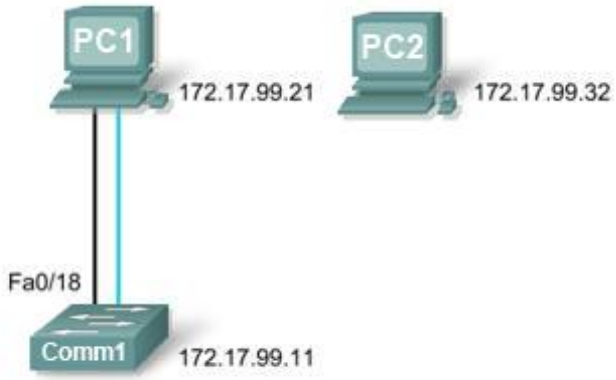


Tableau d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC1	**Carte réseau**	172.17.99.21	255.255.255.0	172.17.99.11
PC2	**Carte réseau**	172.17.99.32	255.255.255.0	172.17.99.11
Comm1	**VLAN 99**	172.17.99.11	255.255.255.0	172.17.99.1

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Supprimer une configuration existante sur un commutateur
- Examiner et vérifier la configuration par défaut
- Créer la configuration de base d'un commutateur, avec un nom et une adresse IP
- Configurer des mots de passe pour sécuriser l'accès à l'interface de ligne de commande
- Configurer les propriétés de vitesse de port et de mode bidirectionnel du commutateur pour une interface
- Configurer la sécurité de base des ports du commutateur
- Gérer la table d'adresses MAC
- Affecter les adresses MAC statiques
- Ajouter et déplacer des hôtes sur un commutateur

Scénario

Au cours de ces travaux pratiques, vous examinerez et configurerez un commutateur de réseau local autonome. Bien qu'un commutateur exécute des fonctions de base dans son état initial par défaut, un administrateur réseau doit modifier de nombreux paramètres pour garantir un réseau local sécurisé et optimisé. Au cours de ces travaux pratiques, vous découvrirez les bases de la configuration d'un commutateur.

Tâche 1 : câblage, suppression et rechargement du commutateur

Étape 1 : câblage d'un réseau

Installez un réseau similaire à celui du diagramme de topologie. Créez une connexion console au commutateur. Si nécessaire, reportez-vous aux Travaux pratiques 1.3.1 pour savoir comment créer une connexion console.

Vous pouvez utiliser n'importe quel commutateur durant les travaux pratiques, pourvu qu'il soit équipé des interfaces indiquées dans la topologie. Le résultat présenté dans ces travaux pratiques provient d'un commutateur 2960. Si vous utilisez d'autres commutateurs, les sorties du commutateur et les descriptions d'interface peuvent être différentes.

Remarque : PC2 n'est pas initialement connecté au commutateur. Il est uniquement utilisé pour la tâche 5.

Étape 2 : suppression de la configuration sur le commutateur

Supprimez la configuration sur le commutateur à l'aide de la procédure de l'annexe 1.

Tâche 2 : vérification de la configuration par défaut du commutateur

Étape 1 : accès au mode privilégié

Vous pouvez accéder à toutes les commandes du commutateur en mode privilégié. Toutefois, étant donné que de nombreuses commandes du mode privilégié configurent des paramètres d'exploitation, l'accès privilégié doit être protégé par un mot de passe pour empêcher une utilisation non autorisée. Vous définirez des mots de passe dans la tâche 3.

Parmi les commandes du mode d'exécution privilégié, on retrouve celles du mode utilisateur, ainsi que la commande **configure** qui donne accès aux autres modes de commande. Accédez au mode d'exécution privilégié en entrant la commande **enable**.

```
Switch>enable
Switch#
```

Notez que l'invite a changé dans la configuration pour représenter le mode d'exécution privilégié.

Étape 2 : examen de la configuration actuelle du commutateur

Examinez le fichier de configuration en cours d'exécution.

```
Switch#show running-config
```

Combien d'interfaces Fast Ethernet le commutateur possède-t-il ? _____

Combien d'interfaces Gigabit Ethernet le commutateur possède-t-il ? _____

Quelle est la plage de valeurs affichée pour les lignes vty ? _____

Examinez le contenu actuel de la mémoire vive non volatile :

```
Switch#show startup-config
startup-config is not present
```

Pourquoi le commutateur donne-t-il cette réponse ?

_____

Examinez les caractéristiques de l'interface virtuelle VLAN1 :

```
Switch#show interface vlan1
```

Une adresse IP est-elle définie sur le commutateur ? _____

Quelle est l'adresse MAC de cette interface de commutateur virtuelle ? _____

Cette interface fonctionne-t-elle ? _____

Affichez maintenant les propriétés IP de l'interface :

```
Switch#show ip interface vlan1
```

Quelle est la sortie affichée ? _____

Étape 3 : affichage des informations Cisco IOS

Examinez les informations de version suivantes que rapporte le commutateur.

```
Switch#show version
```

Quelle version de Cisco IOS le commutateur exécute-t-il ? _____

Quel est le nom de fichier de l'image système ? _____

Quelle est l'adresse MAC de base de ce commutateur ? _____

Étape 4 : examen des interfaces Fast Ethernet

Examinez les propriétés par défaut de l'interface Fast Ethernet utilisée par PC1.

```
Switch#show interface fastethernet 0/18
```

L'interface est-elle activée ou désactivée ? _____

Quel événement pourrait activer une interface ? _____

Quelle est l'adresse MAC de l'interface ? _____

Quels sont les paramètres de vitesse et de mode bidirectionnel de l'interface ? _____

Étape 5 : examen des informations du VLAN (réseau local virtuel)

Examinez les paramètres VLAN par défaut du commutateur.

```
Switch#show vlan
```

Quel est le nom du VLAN 1 ? _____

Quels ports se trouvent dans ce VLAN ? _____

Le VLAN 1 est-il actif ? _____

Quel est le type du VLAN par défaut ? _____

Étape 6 : examen de la mémoire flash

Lancez l'une des commandes suivantes pour examiner le contenu du répertoire flash.

```
Switch#dir flash:
```

ou

```
Switch#show flash
```

Quels sont les fichiers ou les répertoires trouvés ?

_____

Les fichiers comportent une extension de fichier, telle que .bin, à la fin du nom de fichier. Les répertoires n'ont pas d'extension de fichier. Pour examiner les fichiers d'un répertoire, lancez la commande suivante à l'aide du nom de fichier affiché dans le résultat de la commande précédente :

```
Switch#dir flash:c2960-lanbase-mz.122-25.SEE3
```

Le résultat doit être similaire à celui-ci :

```
Directory of flash:/c2960-lanbase-mz.122-25.SEE3/
    6  drwx     4480   Mar 1 1993 00:04:42 +00:00  html
  618  -rwx  4671175   Mar 1 1993 00:06:06 +00:00  c2960-lanbase-mz.122-25.SEE3.bin
  619  -rwx      457   Mar 1 1993 00:06:06 +00:00  info
32514048 bytes total (24804864 bytes free)
```

Quel est le nom du fichier d'image Cisco IOS ? _____

Étape 7 : examen du fichier de configuration initiale

Pour afficher le contenu du fichier de configuration initiale, lancez la commande **show startup-config** en mode d'exécution privilégié.

```
Switch#show startup-config
startup-config is not present
```

Pourquoi ce message apparaît-il ? _____

Apportez une modification à la configuration du commutateur, puis enregistrez-la. Saisissez les commandes suivantes :

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Comm1
Comm1(config)#exit
Comm1#
```

Pour enregistrer le contenu du fichier de configuration en cours dans la mémoire vive non volatile, exécutez la commande **copy running-config startup-config.**

```
Switch#copy running-config startup-config
Destination filename [startup-config]?  (Entrée)
Building configuration...
[OK]
```

Remarque : il est plus facile d'entrer cette commande à l'aide de l'abréviation **copy run start**.

Affichez maintenant le contenu de la mémoire vive non volatile à l'aide de la commande **show startup-config**.

```
Comm1#show startup-config
Using 1170 out of 65536 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Comm1
!
<résultat omis>
```

La configuration actuelle a été écrite dans la mémoire vive non volatile.

Tâche 3 : création d'une configuration de commutateur de base

Étape 1 : attribution d'un nom au commutateur

Dans la dernière étape de la tâche précédente, vous avez configuré le nom d'hôte. Voici un rappel des commandes utilisées.

```
Comm1#configure terminal
Comm1(config)#hostname Comm1
Comm1(config)#exit
```

Étape 2 : définition des mots de passe d'accès

Passez en mode de configuration de ligne pour la console. Définissez le mot de passe de connexion **cisco**. Configurez également les lignes vty 0 à 15 avec le mot de passe **cisco**.

```
Comm1#configure terminal
Tapez les commandes de configuration (une par ligne). Lorsque vous avez
terminé, revenez au mode de configuration globale en saisissant la commande
exit ou en appuyant sur Ctrl-Z.

Comm1(config)#line console 0
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#line vty 0 15
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#exit
```

Pourquoi la commande **login** est-elle requise ? _____

Étape 3 : définition des mots de passe de mode de commande

Définissez class comme mot de passe secret actif. Ce mot de passe protège l'accès au mode d'exécution privilégié.

```
Comm1(config)#enable secret class
```

Étape 4 : configuration de l'adresse de couche 3 du commutateur

Avant de pouvoir gérer Comm1 à distance depuis PC1, vous devez affecter une adresse IP au commutateur. Dans la configuration par défaut du commutateur, la gestion du commutateur est contrôlée par le VLAN 1. Toutefois, pour la configuration de commutateur de base, il est recommandé de modifier le VLAN de gestion par un VLAN autre que le VLAN 1. Le chapitre suivant explique les raisons et les implications de cette opération.

Pour des raisons de gestion, vous utiliserez le VLAN 99. Cette sélection est arbitraire et ne vous oblige en aucun cas à toujours utiliser le VLAN 99.

Vous commencerez par créer le nouveau VLAN 99 sur le commutateur. Ensuite, vous définirez 172.17.99.11 comme adresse IP du commutateur avec le masque de sous-réseau 255.255.255.0 sur l'interface VLAN 99 virtuelle interne.

```
Comm1(config)#vlan 99
Comm1(config-vlan)#exit
Comm1(config)#interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down

Comm1(config-if)#ip address 172.17.99.11 255.255.255.0
Comm1(config-if)#no shutdown
Comm1(config-if)#exit
Comm1(config)#
```

Notez que l'interface VLAN 99 est désactivée même si vous avez entré la commande **no shutdown**. L'interface est actuellement désactivée car aucun port de commutation n'est affecté au VLAN 99.

Affectez tous les ports utilisateur au VLAN 99.

```
Comm1#configure terminal
Comm1(config)#interface range fa0/1 - 24
Comm1(config-if-range)#switchport access vlan 99
Comm1(config-if-range)#exit
Comm1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

L'exploration complète des VLAN n'est pas au programme de ces travaux pratiques. Ce point est étudié de façon détaillée dans le chapitre suivant. Toutefois, pour établir une connectivité entre l'hôte et le commutateur, les ports utilisés par l'hôte doivent se trouver dans le même VLAN que le commutateur. Dans le résultat ci-dessus, notez que l'interface du VLAN 1 est désactivée car aucun des ports n'est affecté au VLAN 1. Au bout de quelques secondes, le VLAN 99 est activé, car au moins un port est désormais affecté au VLAN 99.

Étape 5 : définition de la passerelle par défaut du commutateur

Comm1 est un commutateur de couche 2 ; il prend donc des décisions de transmission basées sur l'en-tête de couche 2. Si plusieurs réseaux sont connectés à un commutateur, vous devez indiquer comment le commutateur transmet les trames interréseau, car le chemin doit être déterminé à la couche 3. Pour ce faire, il convient de spécifier une adresse de passerelle par défaut pointant vers un routeur ou un commutateur de couche 3. Même si cette activité n'inclut aucune passerelle IP externe, supposons que vous connectiez finalement le réseau local à un routeur pour l'accès externe. En partant du principe que l'interface du réseau local sur le routeur est 172.17.99.1, définissez la passerelle par défaut pour le commutateur.

```
Comm1(config)#ip default-gateway 172.17.99.1
Comm1(config)#exit
```

Étape 6 : vérification des paramètres LAN de gestion

Vérifiez les paramètres d'interface sur le VLAN 99.

```
Comm1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is EtherSVI, address is 001b.5302.4ec1 (bia 001b.5302.4ec1)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:06, output 00:03:23, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4 packets input, 1368 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     1 packets output, 64 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Quelle est la bande passante définie sur cette interface ? _____

Quels sont les états du VLAN ? Le VLAN 1 est _____ Le protocole de ligne est _____

Quelle est la stratégie de file d'attente ? _____

Étape 7 : configuration de l'adresse IP et de la passerelle par défaut pour PC1

Définissez 172.17.99.21 comme adresse IP de PC1, avec le masque de sous-réseau 255.255.255.0. Configurez une passerelle par défaut 172.17.99.11. (Si nécessaire, reportez-vous aux Travaux pratiques 1.3.1 pour configurer la carte réseau.)

Étape 8 : vérification de la connectivité

Pour vérifier que l'hôte et le commutateur sont correctement configurés, envoyez une requête ping à l'adresse IP du commutateur (172.17.99.11) depuis PC1.

La requête ping a-t-elle abouti ? _____

Si la réponse est non, dépannez la configuration de l'hôte et du commutateur. Notez que plusieurs tentatives peuvent être nécessaires pour que les requêtes ping aboutissent.

Étape 9 : configuration des paramètres de vitesse de port et de mode bidirectionnel pour une interface Fast Ethernet

Configurez les paramètres de vitesse et de mode bidirectionnel sur Fast Ethernet 0/18. Utilisez la commande end pour repasser en mode d'exécution privilégié lorsque vous aurez terminé.

```
Comm1#configure terminal
Comm1(config)#interface fastethernet 0/18
Comm1(config-if)#speed 100
Comm1(config-if)#duplex full
Comm1(config-if)#end
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Le protocole de ligne pour les interfaces FastEthernet 0/18 et VLAN 99 sera temporairement désactivé.

Par défaut, l'interface Ethernet du commutateur est dotée de la fonction de détection automatique ; elle négocie donc automatiquement les paramètres optimaux. Vous devez définir manuellement la vitesse et le mode bidirectionnel uniquement si un port doit fonctionner à une certaine vitesse et en mode bidirectionnel. La configuration manuelle des ports peut entraîner des décalages de mode bidirectionnel pouvant considérablement détériorer les performances.

Vérifiez les nouveaux paramètres de vitesse et de mode bidirectionnel sur l'interface Fast Ethernet.

```
Comm1#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001b.5302.4e92 (bia 001b.5302.4e92)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     265 packets input, 52078 bytes, 0 no buffer
     Received 265 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 32 multicast, 0 pause input
     0 input packets with dribble condition detected
     4109 packets output, 342112 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Étape 10 : enregistrement de la configuration

Vous avez terminé la configuration de base du commutateur. Sauvegardez maintenant le fichier de configuration en cours dans la mémoire vive non volatile pour être certain de conserver les modifications apportées en cas de réamorçage du système ou de coupure de courant.

```
Comm1#copy running-config startup-config
Destination filename [startup-config]?[Entrée] Building configuration...
[OK]
Comm1#
```

Étape 11 : examen du fichier de configuration initiale

Pour voir la configuration qui est stockée en mémoire vive non volatile, exécutez la commande **show startup-config** en mode d'exécution privilégié.

```
Comm1#show startup-config
```

Est-ce que toutes les modifications saisies ont été enregistrées dans le fichier ? _____

Tâche 4 : gestion de la table d'adresses MAC

Étape 1 : enregistrement des adresses MAC des hôtes

Déterminez et enregistrez les adresses (physiques) de couche 2 des cartes réseau PC à l'aide des commandes suivantes :

Démarrer > Exécuter > cmd > ipconfig /all

PC1 : _____

PC2 : _____

Étape 2 : détermination des adresses MAC que le commutateur a acquises

Affichez les adresses MAC à l'aide de la commande **show mac-address-table** en mode d'exécution privilégié.

```
Comm1#show mac-address-table
```

Combien y a-t-il d'adresses dynamiques ? _____

Combien y a-t-il d'adresses MAC au total ? _____

Les adresses MAC dynamiques correspondent-elles aux adresses MAC de l'hôte ? _____

Étape 3 : énumération des options show mac-address-table

```
Comm1#show mac-address-table ?
```

Combien d'options sont disponibles pour la commande **show mac-address-table** ? _____

Affichez uniquement les adresses MAC de la table qui ont été acquises de façon dynamique.

```
Comm1#show mac-address-table address <Adresse MAC PC1>
```

Combien y a-t-il d'adresses dynamiques ? _____

Étape 4 : suppression de la table d'adresses MAC

Pour supprimer les adresses MAC existantes, utilisez la commande **clear mac-address-table** du mode d'exécution privilégié.

```
Comm1#clear mac-address-table dynamic
```

Étape 5 : vérification des résultats

Vérifiez que la table d'adresses MAC a été supprimée.

```
Comm1#show mac-address-table
```

Combien y a-t-il d'adresses MAC statiques ? _____

Combien y a-t-il d'adresses dynamiques ? _____

Étape 6 : nouvel examen de la table MAC

Il est fort probable qu'une application exécutée sur votre PC1 a déjà envoyé une trame de la carte réseau à Comm1. Consultez une nouvelle fois la table d'adresses MAC en mode d'exécution privilégié pour voir si Comm1 a de nouveau acquis l'adresse MAC pour PC1.

```
Comm1#show mac-address-table
```

Combien y a-t-il d'adresses dynamiques ? _____

Pourquoi est-ce différent du dernier affichage ? _____

_____

Si, pour l'instant, Comm1 n'a pas de nouveau acquis l'adresse MAC pour PC1, envoyez une requête ping à l'adresse IP du VLAN 99 du commutateur depuis PC1 et répétez l'étape 6.

Étape 7 : configuration d'une adresse MAC statique

Pour indiquer les ports auxquels un hôte peut se connecter, vous pouvez créer un mappage statique de l'adresse MAC de l'hôte à un port.

Configurez une adresse MAC statique sur l'interface Fast Ethernet 0/18 en utilisant l'adresse enregistrée pour PC1 à l'étape 1 de cette tâche. L'adresse MAC **00e0.2917.1884** est utilisée à titre d'exemple uniquement. Vous devez utiliser l'adresse MAC de votre PC1, qui est différente de celle utilisée ici comme exemple.

```
Comm1(config)#mac-address-table static 00e0.2917.1884 interface fastethernet
0/18 vlan 99
```

Étape 8 : vérification des résultats

Vérifiez les entrées de la table d'adresses MAC.

```
Comm1#show mac-address-table
```

Combien y a-t-il d'adresses MAC au total ? _____

Combien y a-t-il d'adresses statiques ? _____

Étape 9 : suppression de l'entrée MAC statique

Pour effectuer la tâche suivante, il est nécessaire de supprimer l'entrée de la table d'adresses MAC statiques. Passez en mode de configuration et supprimez la commande en insérant **no** devant la chaîne de commandes.

Remarque : l'adresse MAC 00e0.2917.1884 est utilisée uniquement dans l'exemple. Utilisez l'adresse MAC pour votre PC1.

```
Comm1(config)#no mac-address-table static 00e0.2917.1884 interface
fastethernet 0/18 vlan 99
```

Étape 10 : vérification des résultats

Vérifiez que l'adresse MAC statique a été supprimée.

```
Comm1#show mac-address-table
```

Combien y a-t-il d'adresses MAC statiques au total ? _____

Tâche 5 : configuration de la sécurité des ports

Étape 1 : configuration d'un deuxième hôte

Un deuxième hôte est nécessaire pour cette tâche. Définissez 172.17.99.32 comme adresse IP de PC2, avec le masque de sous-réseau 255.255.255.0 et la passerelle par défaut 172.17.99.11. Ne connectez pas encore ce PC au commutateur.

Étape 2 : vérification de la connectivité

Vérifiez que la configuration de PC1 et du commutateur est toujours correcte en envoyant une requête ping à l'adresse IP du VLAN 99 du commutateur depuis l'hôte.

Les requêtes ping ont-elles abouti ? _____

Si la réponse est non, dépannez les configurations de l'hôte et du commutateur.

Étape 3 : copie des adresses MAC de l'hôte

Notez les adresses MAC de l'étape 1 de la tâche 4.

PC1_____

PC2_____

Étape 4 : détermination des adresses MAC que le commutateur a acquises

Affichez les adresses MAC acquises à l'aide de la commande **show mac-address-table** en mode d'exécution privilégié.

```
Comm1#show mac-address-table
```

Combien y a-t-il d'adresses dynamiques ? _____

Les adresses MAC correspondent-elles aux adresses MAC de l'hôte ? _____

Étape 5 : énumération des options de sécurité des ports

Étudiez les options permettant de définir la sécurité des ports sur l'interface Fast Ethernet 0/18.

```
Comm1# configure terminal
Comm1(config)#interface fastethernet 0/18
Comm1(config-if)#switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
  <cr>

Comm1(config-if)#switchport port-security
```

Étape 6 : configuration de la sécurité d'un port d'accès

Configurez le port du commutateur Fast Ethernet 0/18 de sorte qu'il accepte deux périphériques uniquement, acquière les adresses MAC de ces périphériques de façon dynamique et bloque le trafic issu d'hôtes non valides en cas de violation.

```
Comm1(config-if)#switchport mode access
Comm1(config-if)#switchport port-security
Comm1(config-if)#switchport port-security maximum 2
Comm1(config-if)#switchport port-security mac-address sticky
Comm1(config-if)#switchport port-security violation protect
Comm1(config-if)#exit
```

Étape 7 : vérification des résultats

Affichez les paramètres de sécurité des ports.

```
Comm1#show port-security
```

Combien d'adresses sécurisées sont autorisées sur Fast Ethernet 0/18 ?_____

Quelle est la mesure de sécurité appliquée à ce port ?_____

Étape 8 : examen du fichier de configuration en cours

```
Comm1#show running-config
```

Y a-t-il des instructions répertoriées qui reflètent directement la mise en œuvre de la sécurité de la configuration en cours ?

_____

Étape 9 : modification des paramètres de sécurité d'un port

Sur l'interface Fast Ethernet 0/18, faites passer le nombre d'adresses MAC maximum pour la sécurité des ports à 1 et paramétrez la désactivation en cas de violation.

```
Comm1(config-if)#switchport port-security maximum 1
Comm1(config-if)#switchport port-security violation shutdown
```

Étape 10 : vérification des résultats

Affichez les paramètres de sécurité des ports.

```
Comm1#show port-security
```

Les paramètres de sécurité des ports ont-ils été modifiés pour refléter les modifications de l'étape 9 ?

_____

Envoyez une requête ping à l'adresse du VLAN 99 du commutateur depuis PC1 pour vérifier la connectivité et actualiser la table d'adresses MAC. Désormais, l'adresse MAC pour PC1 doit respecter la configuration en cours.

```
Comm1#show run
Building configuration...

<résultat omis>
!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00e0.2917.1884
 speed 100
 duplex full
!
<résultat omis>
```

Étape 11 : introduction d'un hôte non autorisé

Déconnectez PC1 et connectez PC2 au port Fast Ethernet 0/18. Envoyez une requête ping à l'adresse du VLAN 99 172.17.99.11 depuis le nouvel hôte. Attendez que le voyant de liaison orange devienne vert. Une fois vert, il est presque immédiatement désactivé.

Consignez toute observation utile :

_____

_____

Étape 12 : affichage des informations sur la configuration des ports

Pour afficher les informations de configuration pour le seul port Fast Ethernet 0/18, entrez la commande suivante en mode d'exécution privilégié :

```
Comm1#show interface fastethernet 0/18
```

Quel est l'état de cette interface ?

Fast Ethernet 0/18 est _____ Le protocole de ligne est _____

Étape 13 : réactivation du port

Si une violation de sécurité a lieu et que le port est désactivé, vous pouvez utiliser la commande **no shutdown** pour le réactiver. Toutefois, tant que l'hôte non autorisé est relié à Fast Ethernet 0/18, tout trafic issu de l'hôte désactive le port. Reconnectez PC1 à Fast Ethernet 0/18, et entrez les commandes suivantes sur le commutateur :

```
Comm1# configure terminal
```

```
Comm1(config)#interface fastethernet 0/18
Comm1(config-if)# no shutdown
Comm1(config-if)#exit
```

Remarque : certaines versions IOS peuvent nécessiter une commande **shutdown** manuelle avant la saisie de la commande **no shutdown**.

Étape 14 : remise en état

Sauf indication contraire, effacez la configuration sur les commutateurs, mettez l'ordinateur hôte et les commutateurs hors tension, puis retirez et stockez les câbles.

Annexe 1

Effacement et rechargement du commutateur

Dans la plupart des travaux pratiques d'Exploration 3, il est nécessaire de commencer avec un commutateur non configuré. L'utilisation d'un commutateur comportant déjà une configuration peut produire des résultats imprévisibles. Ces instructions indiquent comment préparer le commutateur avant de commencer les travaux pratiques. Elles concernent le commutateur 2960 ; toutefois, la procédure est identique pour les commutateurs 2900 et 2950.

Étape 1 : accès au mode d'exécution privilégié en tapant la commande enable

Si le système vous demande un mot de passe, entrez class. Si cela ne fonctionne pas, demandez de l'aide au formateur.

```
Switch>enable
```

Étape 2 : suppression du fichier d'informations de la base de données VLAN

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Entrée]
Delete flash:vlan.dat? [confirm] [Entrée]
```

S'il n'y a pas de fichier VLAN, le message suivant s'affiche :

```
%Error deleting flash:vlan.dat (No such file or directory)
```

Étape 3 : suppression, dans la mémoire vive non volatile, du fichier de configuration initiale du commutateur

```
Switch#erase startup-config
```

Vous obtenez le message suivant :

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]

Press Enter to confirm.
```

La réponse suivante doit s'afficher :

```
Erase of nvram: complete
```

Étape 4 : vérification de la suppression des informations du VLAN

Vérifiez que la configuration VLAN a été supprimée à l'étape 2 à l'aide de la commande show vlan.

Si les informations relatives au VLAN ont été supprimées à l'étape 2, passez à l'étape 5 et redémarrez le commutateur à l'aide de la commande **reload**.

Si les informations de la configuration VLAN précédente (autres que celles du VLAN 1 de gestion par défaut) sont toujours présentes, vous devez mettre le commutateur hors tension puis sous tension (redémarrage matériel) plutôt que d'entrer la commande **reload**. Pour le redémarrage matériel du commutateur, ôtez le cordon d'alimentation de l'arrière du commutateur ou débranchez-le, puis rebranchez-le.

Étape 5 : redémarrage du logiciel

Remarque : cette étape n'est pas nécessaire si le commutateur a été redémarré à l'aide du démarrage matériel.

À l'invite du mode d'exécution privilégié, entrez la commande **reload**.

```
Switch(config)#reload
```

Vous obtenez le message suivant :

```
System configuration has been modified. Save? [yes/no]:
```

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

```
Proceed with reload? [confirm] [Entrée]
```

La première ligne de la réponse est la suivante :

```
Reload requested by console.
```

Après le rechargement du commutateur, la ligne suivante s'affiche :

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

```
Press RETURN to get started! [Entrée]
```

Travaux pratiques 2.5.2 : gestion des fichiers de configuration et du système d'exploitation du commutateur

Diagramme de topologie

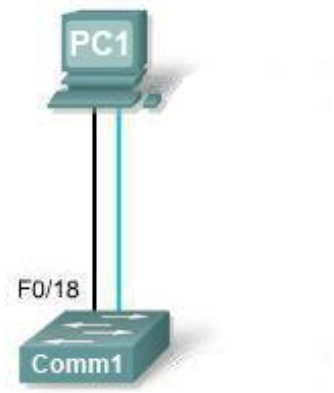


Tableau d'adressage

Périphérique	Nom d'hôte / Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC 1	Hôte A	172.17.99.21	255.255.255.0	172.17.99.1
Comm1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1

Objectifs pédagogiques

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

- Créer et enregistrer une configuration de commutateur de base
- Configurer un serveur TFTP sur le réseau
- Sauvegarder le logiciel Cisco IOS du commutateur sur un serveur TFTP puis le restaurer
- Sauvegarder la configuration de commutateur sur un serveur TFTP
- Configurer un commutateur pour charger une configuration à partir d'un serveur TFTP
- Mettre à niveau le logiciel Cisco IOS à partir d'un serveur TFTP
- Récupérer le mot de passe pour un commutateur 2960 (gamme 2900)

Scénario

Au cours de ces travaux pratiques, vous examinerez et configurerez un commutateur de réseau local autonome. Bien qu'un commutateur exécute des fonctions de base dans son état initial par défaut, un administrateur réseau doit modifier de nombreux paramètres pour garantir un réseau local sécurisé et optimisé. Au cours de ces travaux pratiques, vous découvrirez les bases de la configuration d'un commutateur.

Tâche 1 : câblage et initialisation du réseau

Étape 1 : câblage d'un réseau

Installez un réseau similaire à celui du diagramme de topologie. Créez une connexion console au commutateur. Si nécessaire, reportez-vous aux Travaux pratiques 1.3.1. Le résultat présenté dans ces travaux pratiques provient d'un commutateur 2960. Si vous utilisez d'autres commutateurs, les sorties du commutateur et les descriptions d'interface peuvent être différentes.

Étape 2 : suppression de la configuration sur le commutateur

Configurez une connexion console au commutateur et effacez la configuration existante. Si nécessaire, reportez-vous aux Travaux pratiques 2.5.1, Annexe 1.

Étape 3 : création d'une configuration de base

Utilisez les commandes suivantes pour configurer un nom d'hôte, des mots de passe d'accès à la ligne et le mot de passe secret actif.

```
Switch#configure terminal
Switch(config)#hostname ALSwitch
ALSwitch(config)#exit
ALSwitch(config)#line con 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#exit
```

Créez le VLAN 99 et affectez-lui des ports utilisateur à l'aide des commandes indiquées ci-dessous. Repassez en mode d'exécution privilégié lorsque vous avez terminé.

```
ALSwitch(config)#vlan 99
ALSwitch(config-vlan)#name user
ALSwitch(config-vlan)#exit
ALSwitch(config)#interface vlan 99
ALSwitch(config-if)#ip address 172.17.99.11 255.255.255.0
ALSwitch(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan99, changed state to up
ALSwitch(config-if)#exit
ALSwitch(config)#interface fa0/18
ALSwitch(config-if)#switchport access vlan 99
ALSwitch(config-if)#end
ALSwitch#
```

Étape 4 : configuration de l'hôte relié au commutateur

Configurez l'hôte pour qu'il utilise l'adresse IP, le masque et la passerelle par défaut identifiés dans le tableau d'adressage présenté au début des travaux pratiques. Cet hôte joue le rôle de serveur TFTP dans ces travaux pratiques.

Étape 5 : vérification de la connectivité

Pour vérifier que l'hôte et le commutateur sont correctement configurés, envoyez une requête ping à l'adresse IP du commutateur configurée pour le VLAN 99 à partir de l'hôte.

La requête ping a-t-elle abouti ? _____

Si la réponse est non, dépannez les configurations de l'hôte et du commutateur.

Tâche 2 : démarrage et configuration du serveur TFTP

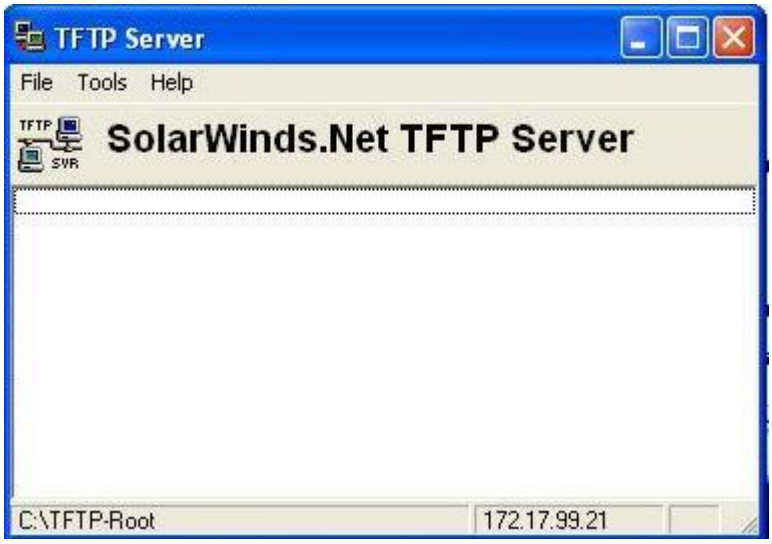
Étape 1 : démarrage et configuration du serveur TFTP

Le serveur TFTP présenté dans ces travaux pratiques est le serveur Solar Winds, disponible à l'adresse http://www.solarwinds.com/products/freetools/free_tftp_server.aspx. Si cette URL ne fonctionne plus, utilisez le moteur de recherche de votre choix pour rechercher « solar winds free tftp download ».

Ce serveur peut être différent de celui utilisé dans cette classe. Dans ce cas, veuillez vérifier avec le formateur les instructions d'emploi du serveur TFTP en question.

Démarrez le serveur sur l'hôte en sélectionnant **Démarrer > Tous les programmes > SolarWinds 2003 Standard Edition > TFTP Server.**

Le serveur doit démarrer, acquérir l'adresse IP de l'interface Ethernet et utiliser le répertoire C:\TFTP-Root par défaut.



Lorsque le serveur TFTP fonctionne et présente la configuration appropriée des adresses sur la station de travail, copiez le fichier Cisco IOS du commutateur sur le serveur TFTP.

Étape 2 : vérification de la connectivité au serveur TFTP

Vérifiez que le serveur TFTP fonctionne et qu'une requête ping peut lui être envoyée à partir du commutateur.

Quelle est l'adresse IP du serveur TFTP ? _____

```
Switch#ping 172.17.99.21

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.17.99.21 , timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1006
ms
Switch#
```

Tâche 3 : sauvegarde du fichier Cisco IOS sur un serveur TFTP

Étape 1 : identification du nom de fichier Cisco IOS

Déterminez le nom exact du fichier d'image à enregistrer. À partir de la session en mode console, entrez **show flash**.

```
Switch#show flash

Directory of flash:/
   2  -rwx         556   Mar 8 1993 22:46:45 +00:00  vlan.dat
   5  drwx         192   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX
32514048 bytes total (26527232 bytes free)
```

Quels sont le nom et la taille de l'image Cisco IOS stockée en mémoire flash ? _____

_____

Remarque : si le fichier se trouve dans un sous-répertoire, comme c'est le cas dans le résultat présenté ci-dessus, vous ne pouvez pas immédiatement voir le nom de fichier. Pour afficher le nom de fichier Cisco IOS, utilisez la commande **cd** pour passer du répertoire courant du commutateur au répertoire Cisco IOS :

```
Switch#cd flash:/c2960-lanbase-mz.122-25.FX
Switch#show flash
Directory of flash:/c2960-lanbase-mz.122-25.FX/
    6  drwx        4160   Mar 1 1993 00:03:36 +00:00  html
  368  -rwx     4414921   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX.bin
  369  -rwx         429   Mar 1 1993 00:04:53 +00:00  info
32514048 bytes total (26527232 bytes free)
```

Quels sont le nom et la taille de l'image Cisco IOS stockée en mémoire flash ? _____

_____

Quels attributs peuvent être identifiés à partir des codes du nom de fichier Cisco IOS ? _____

_____

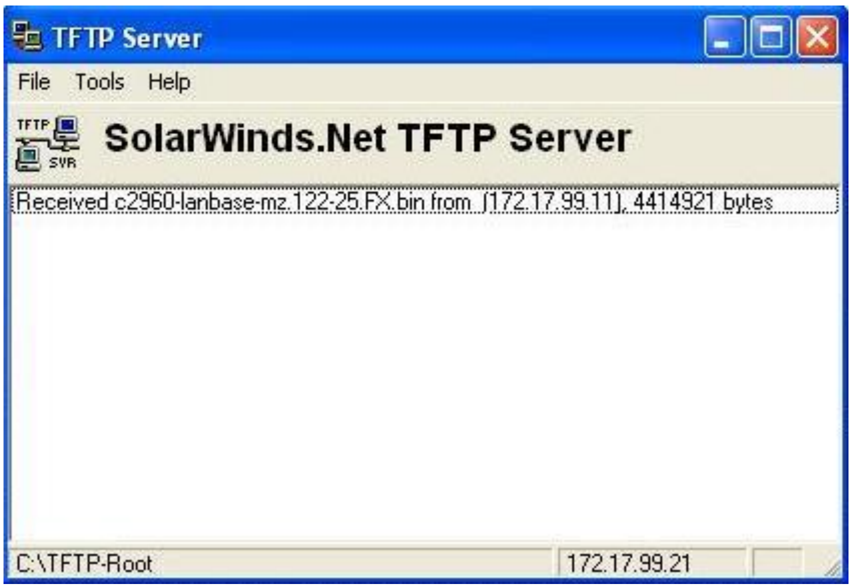
À partir du mode d'exécution privilégié, entrez la commande **copy flash tftp**. À l'invite, entrez d'abord le nom du fichier d'image Cisco IOS, puis l'adresse IP du serveur TFTP. Veillez à inclure le chemin complet si le fichier se trouve dans un sous-répertoire.

```
Switch#copy flash tftp
Source filename []?c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin
```

```
Address or name of remote host []? 172.17.99.21
Destination filename [c2960-lanbase-mz.122-25.FX.bin]? [Entrée]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!<résultat omis>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
4414921 bytes copied in 10.822 secs (407958 bytes/sec)
Switch#
```

Étape 2 : vérification du transfert vers le serveur TFTP

Vérifiez le transfert vers le serveur TFTP en examinant le fichier journal. Sur le serveur TFTP SolarWinds, le transfert peut être vérifié à partir de la fenêtre de commande, comme illustré ci-dessous :



Vérifiez la taille de l'image flash dans le répertoire racine du serveur. Le chemin vers le serveur racine s'affiche dans la fenêtre de commande du serveur : C:\TFTP-root.

Trouvez ce répertoire sur le serveur en utilisant le gestionnaire de fichiers et examinez la liste détaillée du fichier. La longueur du fichier dans la commande **show flash** doit être identique à celle du fichier stocké sur le serveur TFTP. Si les fichiers ne sont pas de taille équivalente, consultez votre formateur.

Tâche 4 : restauration du fichier Cisco IOS sur le commutateur à partir d'un serveur TFTP

Étape 1 : vérification de la connectivité

Vérifiez que le serveur TFTP fonctionne, et envoyez une requête ping à l'adresse IP du serveur TFTP depuis le commutateur.

Quelle est l'adresse IP du serveur TFTP ? ______________________________

```
Switch#ping 172.17.99.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.21 , timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1006
ms
Switch#
```

Si les requêtes ping échouent, dépannez les configurations du serveur et du commutateur.

Étape 2 : identification du nom de fichier Cisco IOS sur le serveur et du nom de chemin complet de la destination pour le commutateur

Quel est le nom de fichier du répertoire racine du serveur TFTP qui sera copié sur le commutateur ?

_____

Quel est le nom du chemin de destination pour le fichier Cisco IOS sur le commutateur ?

_____

Quelle est l'adresse IP du serveur TFTP ? _____

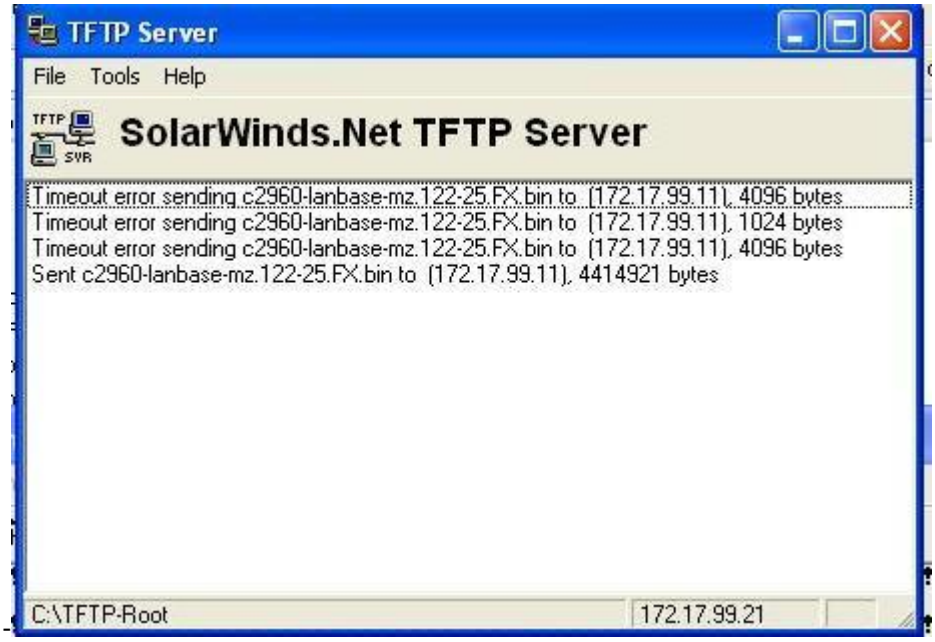
Étape 3 : téléchargement du logiciel Cisco IOS du serveur vers le commutateur

Remarque : il est important que ce processus ne soit pas interrompu.

En mode d'exécution privilégié, copiez le fichier du serveur TFTP sur la mémoire flash.

```
Switch#copy tftp flash
Address or name of remote host []? 172.17.99.21
Source filename []? c2960-lanbase-mz.122-25.FX.bin
Destination filename [c2960-lanbase-mz.122-25.FX.bin]? c2960-lanbase-
mz.122-25.F
X/c2960-lanbase-mz.122-25.FX.bin
%Warning:There is a file already existing with this name
Do you want to over write? [confirm] [Entrée]
Accessing tftp://172.17.99.21 /c2960-lanbase-mz.122-25.FX.bin...
Loading c2960-lanbase-mz.122-25.FX.bin from 172.17.99.21  (via
Vlan1):!!!!!!!!!!!!!!!!!!
<résultat omis>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4414921 bytes]

4414921 bytes copied in 43.964 secs (100421 bytes/sec)
Switch#
```

L'écran de résultat du serveur doit être similaire à celui-ci :



La taille du fichier téléchargé est-elle identique à celle du fichier enregistré sur le répertoire racine TFTP ?

_____

Étape 4 : test de l'image Cisco IOS restaurée

Vérifiez que l'image du commutateur est correcte. Pour cela, rechargez le commutateur et observez le processus de démarrage pour vous assurer qu'il n'y a pas d'erreurs de mémoire flash. En l'absence d'erreur, le logiciel Cisco IOS du commutateur doit avoir démarré correctement. Pour vérifier de façon plus approfondie l'image Cisco IOS stockée en mémoire flash, lancez la commande **show version** qui affiche des informations similaires à celles-ci :

```
System image file is "flash:c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin"
```

Tâche 5 : sauvegarde et restauration d'un fichier de configuration à partir d'un serveur TFTP

Étape 1 : copie du fichier de configuration initiale sur le serveur TFTP

Vérifiez que le serveur TFTP fonctionne et qu'une requête ping peut lui être envoyée à partir du commutateur.

Quelle est l'adresse IP du serveur TFTP ? _____

En mode d'exécution privilégié, entrez la commande copy **running-config startup-config** pour vous assurer que le fichier de configuration en cours est enregistré dans le fichier de configuration initiale.

```
ALSwitch#copy running-config startup-config
Destination filename [startup-config]?[Entrée] Building
configuration...
[OK]
```

Sauvegardez le fichier de configuration enregistré sur le serveur TFTP avec la commande **copy startup-config tftp**. À l'invite, entrez l'adresse IP du serveur TFTP :

```
AlSwitch#copy startup-config tftp
Address or name of remote host []? 172.17.99.21
Destination filename [alswitch-confg]? [Entrée]
!!
1452 bytes copied in 0.445 secs (3263 bytes/sec)#
```

Étape 2 : vérification du transfert vers le serveur TFTP

Vérifiez le transfert vers le serveur TFTP en affichant la fenêtre de commande sur le serveur TFTP. Le résultat doit être similaire à celui-ci :

```
Received alswitch-confg from (172.17.99.11), 1452 bytes
```

Vérifiez que le fichier alswitch-confg se trouve dans le répertoire C:\TFTP-root du serveur TFTP.

Étape 3 : restauration du fichier de configuration initiale à partir du serveur TFTP

Pour restaurer le fichier de configuration initiale, le fichier de configuration initiale existant doit être effacé et le commutateur rechargé.

```
AlSwitch#erase nvram
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
AlSwitch#
AlSwitch#reload
Proceed with reload? [confirm] [Entrée]
```

Lorsque le commutateur est rechargé, vous devez rétablir la connectivité entre le commutateur et le serveur TFTP pour que la configuration puisse être restaurée. Pour ce faire, configurez le VLAN 99 avec l'adresse IP appropriée et affectez le port Fast Ethernet 0/18 au VLAN 99. Lorsque vous avez terminé, repassez en mode d'exécution privilégié.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 99
Switch(config-if)#ip address 172.17.99.11 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/18
Switch(config-if)#switchport access vlan 99
Switch(config-if)#end
Switch#
```

Une fois que le VLAN 99 est activé, vérifiez la connectivité en envoyant une requête ping au serveur depuis le commutateur.

```
Switch#ping 172.17.99.21
```

Si la requête ping échoue, dépannez la configuration du serveur et du commutateur. Restaurez la configuration à partir du serveur TFTP avec la commande **copy tftp startup-config**.

Remarque : il est important que ce processus ne soit pas interrompu.

```
Switch#copy tftp startup-config
Address or name of remote host []? 172.17.99.21
Source filename []? alswitch-confg
Destination filename [startup-config]? [Entrée]
Accessing tftp://172.17.99.21 /alswitch-confg...
Loading alswitch-confg from 172.17.99.21  (via Vlan99): !
[OK - 1452 bytes]
1452 bytes copied in 9.059 secs (160 bytes/sec)
Switch#
00:21:37: %SYS-5-CONFIG_NV_I: Nonvolatile storage configured from
tftp://172.17.99.21 /alswitch-confg by console
Switch#
```

L'opération a-t-elle réussi ? _____

Étape 4 : vérification du fichier de configuration initiale restauré

En mode d'exécution privilégié, rechargez de nouveau le commutateur. Lorsque le rechargement est terminé, le commutateur doit afficher l'invite ALSwitch. Tapez la commande **show startup-config** pour vérifier que la configuration restaurée est complète, notamment les mots de passe secret actif et d'accès à la ligne.

Tâche 6 : mise à niveau du logiciel Cisco IOS du commutateur

Remarque : pour ces travaux pratiques, le formateur ou le participant doit placer une combinaison d'image Cisco IOS et du fichier d'archive HTML (tar) dans le répertoire du serveur TFTP par défaut. Ce fichier doit être téléchargé par le formateur à partir du centre de logiciel en ligne Cisco Connection. Dans le cadre de ces travaux pratiques, le fichier c2960-lanbase-mz.122-25.FX.tar est référencé à des fins pédagogiques uniquement. Il a la même racine de nom de fichier que l'image en cours. Cependant, pour les besoins de ces travaux pratiques, nous supposerons que c'est une mise à jour. La version de mise à jour du logiciel Cisco IOS inclut les fichiers image binaire et de nouveaux fichiers HTML pour prendre en charge les modifications de l'interface Web.

Ces travaux pratiques nécessitent également l'enregistrement d'une copie du fichier de configuration actuelle en tant que sauvegarde.

Étape 1 : détermination de la séquence d'amorçage en cours pour le commutateur

Utilisez la commande **show boot** pour afficher les paramètres des variables d'environnement d'amorçage.

```
ALSwitch#show boot
BOOT path-list : flash:c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : no
HELPER path-list    :
Auto upgrade        : yes
NVRAM/Config file
      buffer size:   65536
ALSwitch#
```

Déterminez s'il y a suffisamment de mémoire pour inclure plusieurs fichiers d'image :

```
ALSwitch#sh flash
Directory of flash:/
    2  -rwx         616   Mar 1 1993 06:39:02 +00:00  vlan.dat
    4  -rwx           5   Mar 1 1993 10:14:07 +00:00  private-
config.text
    5  drwx         192   Mar 1 1993 00:04:53 +00:00  c2960-lanbase-
mz.122-25.FX
  370  -rwx        1281   Mar 1 1993 10:14:07 +00:00  config.text

32514048 bytes total (26524672 bytes free)
ALSwitch#
```

Notez que sur cette plateforme, environ 6 Mo seulement sont utilisés, et il reste approximativement 26,5 Mo d'espace disponible ; la mémoire est donc largement suffisante pour plusieurs images. S'il n'y a pas suffisamment d'espace pour plusieurs images, vous devez remplacer l'image existante par la nouvelle ; vous devez donc vérifier que le serveur TFTP contient une sauvegarde du fichier Cisco IOS existant avant de commencer la mise à niveau.

Étape 2 : préparation de la nouvelle image

Si le commutateur a suffisamment de mémoire libre comme indiqué dans la dernière étape, utilisez la commande **rename** pour renommer le fichier Cisco IOS existant avec le même nom et avec l'extension .old :

```
ALSwitch#rename flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-
25.FX.bin flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.old
```

Vérifiez que le changement de nom a réussi :

```
ALSwitch#dir flash:/c2960-lanbase-mz.122-25.FX/
```

```
Directory of flash:/c2960-lanbase-mz.122-25.FX/
    6  drwx        4160   Mar 1 1993 00:03:36 +00:00  html
  368  -rwx     4414921   Mar 1 1993 03:26:51 +00:00  c2960-lanbase-
mz.122-25.FX.old
  369  -rwx         429   Mar 1 1993 00:04:53 +00:00  info
32514048 bytes total (26524672 bytes free)
```

Utilisez la commande **delete** pour supprimer les fichiers HTML existants. Si vous insérez ***** dans la commande à la place d'un nom de fichier spécifique, tous les fichiers du répertoire sont supprimés.

```
ALSwitch#delete flash:/c2960-lanbase-mz.122-25.FX/html/*
```

Étape 3 : extraction de la nouvelle image Cisco IOS et des nouveaux fichiers HTML vers la mémoire flash

Entrez la commande suivante pour placer la nouvelle image Cisco IOS et les nouveaux fichiers HTML dans le répertoire cible de la mémoire flash :

```
ALSwitch#archive tar /x tftp://172.17.99.21/c2960-lanbase-mz.122-
25.FX.tar flash:/c2960-lanbase-mz.122-25.FX

ALSwitch(config)#ip http server
```

Étape 4 : association du nouveau fichier d'amorçage

Entrez la commande **boot** avec le nom de fichier de la nouvelle image à l'invite du mode de configuration globale. Lorsque vous avez terminé, repassez en mode d'exécution privilégié et enregistrez la configuration.

```
ALSwitch(config)#boot system flash:/c2960-lanbase-mz.122-25.FX/c2960-
lanbase-mz.122-25.FX.bin
ALSwitch(config)# end
ALSwitch#copy running-config startup-config
```

Étape 5 : redémarrage du commutateur

Redémarrez le commutateur à l'aide de la commande **reload** pour voir si le nouveau logiciel Cisco IOS a été chargé. Utilisez la commande **show version** pour voir le nom du fichier Cisco IOS.

Quel était le nom du fichier Cisco IOS à partir duquel le commutateur s'est amorcé ? _____

_____ _____

Était-ce le nom de fichier approprié ? _____

Si le nom de fichier Cisco IOS est à présent correct, supprimez le fichier de sauvegarde de la mémoire flash à l'aide de la commande suivante du mode d'exécution privilégié :

```
ALSwitch(config)#delete flash:/c2960-lanbase-mz.122-25.FX/c2960-lanbase-
mz.122-25.FX.old
```

Tâche 7 : récupération des mots de passe sur Catalyst 2960

Étape 1 : réinitialisation du mot de passe de console

Demandez à un autre participant de modifier les mots de passe de console et vty sur le commutateur. Enregistrez les modifications dans le fichier startup-config et rechargez le commutateur.

Ensuite, sans connaître les mots de passe, essayez d'accéder au commutateur.

Étape 2 : récupération de l'accès au commutateur

Vérifiez que le PC est connecté au port de console et qu'une fenêtre HyperTerminal est ouverte. Mettez le commutateur hors tension. Remettez-le sous tension tout en maintenant enfoncé le bouton **MODE** situé sur la face avant du commutateur au moment de la mise sous tension. Relâchez le bouton **MODE** lorsque la LED SYST arrête de clignoter et reste allumée.

Le résultat suivant doit s'afficher :

```
The system has been interrupted prior to initializing the flash files
system. The following commands will initialize the flash files system,
and finish loading the operating system software:
flash_init
load_helper
boot
```

Pour initialiser le système de fichiers et finir de charger le système d'exploitation, entrez les commandes suivantes :

```
switch:flash_init
switch:load_helper
switch:dir flash:
```

Remarque : n'oubliez pas de taper les deux points (:) après **flash** dans la commande **dir flash**:.

Tapez **rename flash:config.text flash:config.old** pour renommer le fichier de configuration. Ce fichier contient la définition du mot de passe.

Étape 3 : redémarrage du système

Tapez la commande **boot** pour amorcer le système. Entrez **n** lorsque le système vous invite à poursuivre le dialogue de configuration, et **y** lorsqu'il vous demande si vous souhaitez terminer l'installation automatique.

Pour renommer le fichier de configuration avec son nom d'origine, tapez la commande **rename flash:config.old flash:config.text** à l'invite du mode d'exécution privilégié.

Copiez le fichier de configuration en mémoire :

```
Switch#copy flash:config.text system:running-config
Source filename [config.text]?[Entrée]
Destination filename [running-config][Entrée]
```

Le fichier de configuration est à présent rechargé. Modifiez les anciens mots de passe inconnus en procédant comme suit :

```
ALSwitch#configure terminal
ALSwitch(config)#no enable secret
ALSwitch(config)#enable secret class
ALSwitch(config)#line console 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#exit
ALSwitch(config)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#end
ALSwitch#copy running-config startup-config
Destination filename [startup-config]?[Entrée] Building
configuration...
[OK]
ALSwitch#
```

Mettez fin à la connexion console puis rétablissez-la pour vérifier que les nouveaux mots de passe ont été configurés. Si ce n'est pas le cas, recommencez la procédure.

Après avoir réalisé les étapes précédentes, déconnectez-vous en tapant **exit**, puis mettez tous les périphériques hors tension. Retirez et rangez les câbles et l'adaptateur.

Travaux pratiques 2.5.3 : gestion des fichiers de configuration et du système d'exploitation du commutateur – Confirmation

Diagramme de topologie

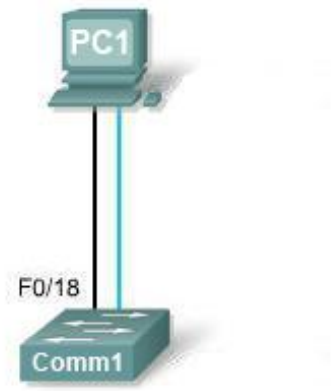


Tableau d'adressage

Périphérique	Nom d'hôte / Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC 1	Hôte A	172.17.99.21	255.255.255.0	172.17.99.1
Comm1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1

Objectifs pédagogiques

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

- Créer et enregistrer une configuration de commutateur de base
- Configurer un serveur TFTP sur le réseau
- Sauvegarder le logiciel Cisco IOS du commutateur sur un serveur TFTP puis le restaurer
- Sauvegarder la configuration de commutateur sur un serveur TFTP
- Configurer un commutateur pour charger une configuration à partir d'un serveur TFTP
- Mettre à niveau le logiciel Cisco IOS à partir d'un serveur TFTP
- Récupérer le mot de passe pour un commutateur Cisco 2960 (gamme 2900)

Scénario

Au cours de ces travaux pratiques, vous étudierez des procédures de gestion de fichiers et de récupération de mots de passe sur un commutateur Catalyst Cisco.

Tâche 1 : câblage et initialisation du réseau

Étape 1 : câblage d'un réseau

Installez un réseau similaire à celui du diagramme de topologie. Ensuite, créez une connexion console au commutateur. Si nécessaire, reportez-vous aux Travaux pratiques 1.3.1. Le résultat présenté dans ces travaux pratiques provient d'un commutateur 2960. Si vous utilisez d'autres commutateurs, les sorties du commutateur et les descriptions d'interface peuvent être différentes.

Étape 2 : suppression de la configuration sur le commutateur

Configurez une connexion console au commutateur. Supprimez la configuration sur le commutateur.

Étape 3 : création d'une configuration de base

Configurez le commutateur avec le nom d'hôte et les mots de passe d'accès suivants. Puis, activez des mots de passe secrets sur le commutateur.

Nom d'hôte	Mot de passe de console	Mot de passe Telnet	Mot de passe de commande
ALSwitch	cisco	cisco	class

Créez le VLAN 99. Affectez l'adresse IP 172.17.99.11 à cette interface. Affectez le port Fast Ethernet 0/18 à ce VLAN.

Étape 4 : configuration de l'hôte relié au commutateur

Configurez l'hôte pour qu'il utilise l'adresse IP, le masque et la passerelle par défaut identifiés dans le tableau d'adressage. Cet hôte joue le rôle de serveur TFTP dans ces travaux pratiques.

Étape 5 : vérification de la connectivité

Pour vérifier que l'hôte et le commutateur sont correctement configurés, envoyez une requête ping à l'adresse IP du commutateur à partir de l'hôte.

La requête ping a-t-elle abouti ? _____

Si la réponse est non, dépannez les configurations de l'hôte et du commutateur.

Tâche 2 : démarrage et configuration du serveur TFTP

Étape 1 : démarrage et configuration du serveur TFTP

Le serveur TFTP qui a été utilisé pour développer ces travaux pratiques est le serveur Solar Winds, disponible à l'adresse http://www.solarwindssoftware.com/toolsets/tools/tftp-server.aspx.

Les travaux pratiques de votre classe peuvent utiliser un serveur TFTP différent. Dans ce cas, vérifiez avec le formateur les instructions d'emploi du serveur TFTP en question.

Démarrez le serveur sur l'hôte à l'aide du menu Démarrer : **Démarrer > Tous les programmes > SolarWinds 2003 Standard Edition > TFTP Server.**

Le serveur doit démarrer et acquérir l'adresse IP de l'interface Ethernet. Il utilise le répertoire C:\TFTP-Root par défaut.

Étape 2 : vérification de la connectivité au serveur TFTP

Vérifiez que le serveur TFTP fonctionne et qu'une requête ping peut lui être envoyée à partir du commutateur.

Tâche 3 : sauvegarde du fichier Cisco IOS sur le serveur TFTP

Étape 1 : identification du nom de fichier Cisco IOS

Déterminez le nom exact du fichier d'image à enregistrer.

Notez que si le fichier se trouve dans un sous-répertoire, comme c'est le cas dans le résultat présenté ci-dessus, vous ne pouvez pas immédiatement voir le nom de fichier. Pour afficher le nom de fichier Cisco IOS, passez d'abord du répertoire courant du commutateur au répertoire Cisco IOS.

Examinez le résultat du commutateur, puis répondez aux questions suivantes.

Quels sont le nom et la taille de l'image Cisco IOS stockée en mémoire flash ?

_____

Quels attributs peuvent être identifiés à partir des codes du nom de fichier Cisco IOS ?

_____

Étape 2 : en mode d'exécution privilégié, copie du fichier d'image sur le serveur TFTP

Étape 3 : vérification du transfert vers le serveur TFTP

Vérifiez le transfert vers le serveur TFTP en examinant le fichier journal. Avec le serveur TFTP SolarWinds, vous pouvez vérifier le transfert, depuis la fenêtre de commande ou le fichier journal du serveur, dans le fichier suivant :

C:\Program Files\SolarWinds\2003 Standard Edition\TFTP-Server.log.

Vérifiez que la taille de l'image flash apparaît dans le répertoire racine du serveur. Le chemin vers le serveur racine s'affiche dans la fenêtre de commande du serveur :

C:\TFTP-root

Utilisez le gestionnaire de fichiers pour trouver ce répertoire sur le serveur et examinez la liste détaillée du fichier. La taille du fichier indiquée par la commande **show flash** doit être identique à celle du fichier stocké sur le serveur TFTP. Si les fichiers ne sont pas de taille équivalente, consultez votre formateur.

Tâche 4 : restauration du fichier Cisco IOS sur le commutateur à partir d'un serveur TFTP

Étape 1 : vérification de la connectivité

Vérifiez que le serveur TFTP fonctionne, et envoyez une requête ping à l'adresse IP du serveur TFTP depuis le commutateur.

Si les requêtes ping échouent, dépannez les configurations du serveur et du commutateur.

Étape 2 : identification du nom de fichier Cisco IOS sur le serveur et du nom de chemin complet de la destination pour le commutateur

Quel est le nom de fichier du répertoire racine du serveur TFTP qui sera copié sur le commutateur ?

_____

Quel est le nom du chemin de destination pour le fichier IOS sur le commutateur ?

_____

Quelle est l'adresse IP du serveur TFTP ? _____

Étape 3 : téléchargement du logiciel Cisco IOS du serveur vers le commutateur

Remarque : il est important que ce processus ne soit pas interrompu.

En mode d'exécution privilégié, copiez le fichier du serveur TFTP sur la mémoire flash.

La taille du fichier téléchargé est-elle identique à celle du fichier enregistré sur le répertoire racine TFTP ?

_____

Étape 4 : test de l'image Cisco IOS restaurée

Vérifiez que l'image du commutateur est correcte. Pour ce faire, rechargez l'image du commutateur et observez le processus de démarrage. Confirmez qu'il n'y a pas d'erreurs de mémoire flash. En l'absence d'erreur, le logiciel Cisco IOS du commutateur doit avoir démarré correctement. Pour vérifier de façon plus approfondie l'image Cisco IOS stockée en mémoire flash, lancez la commande qui affiche la version Cisco IOS.

Tâche 5 : sauvegarde et restauration d'un fichier de configuration à partir d'un serveur TFTP

Étape 1 : copie du fichier de configuration initiale sur le serveur TFTP

Vérifiez que le serveur TFTP fonctionne et qu'une requête ping peut lui être envoyée à partir du commutateur. Enregistrez la configuration actuelle.

Sauvegardez le fichier de configuration enregistré dans le serveur TFTP.

Étape 2 : vérification du transfert vers le serveur TFTP

Vérifiez le transfert vers le serveur TFTP en affichant la fenêtre de commande sur le serveur TFTP. Le résultat doit être similaire à celui-ci :

```
Received alswitch-confg from (172.17.99.11), 1452 bytes
```

Vérifiez que le fichier alswitch-confg se trouve dans le répertoire C:\TFTP-root du serveur TFTP.

Étape 3 : restauration du fichier de configuration initiale à partir du serveur TFTP

Pour restaurer le fichier de configuration initiale, effacez d'abord le fichier de configuration initiale existant, puis rechargez le commutateur.

Lorsque le commutateur est rechargé, vous devez rétablir la connectivité entre le commutateur et le serveur TFTP pour que la configuration puisse être restaurée. Pour ce faire, reconfigurez le VLAN 99 avec l'adresse IP appropriée et affectez le port Fast Ethernet 0/18 à ce VLAN (reportez-vous à la tâche 1).

Une fois que le VLAN 99 est activé, vérifiez la connectivité en envoyant une requête ping au serveur depuis le commutateur.

Si la requête ping échoue, dépannez la configuration du serveur et du commutateur. Restaurez la configuration à partir du serveur TFTP en copiant le fichier alswitch-confg du serveur sur le commutateur.

Remarque : il est important que ce processus ne soit pas interrompu.

L'opération a-t-elle réussi ? _____

Étape 4 : vérification du fichier de configuration initiale restauré

En mode d'exécution privilégié, rechargez de nouveau le routeur. Lorsque le rechargement est terminé, le commutateur doit afficher l'invite ALSwitch. Examinez la configuration en cours pour vérifier que la configuration restaurée est complète, notamment les mots de passe secret actif et d'accès.

Tâche 6 : mise à niveau du logiciel Cisco IOS du commutateur

Remarque : pour ces travaux pratiques, le formateur ou le participant doit placer une combinaison d'image Cisco IOS et du fichier d'archive HTML (tar) dans le répertoire du serveur TFTP par défaut. Ce fichier doit être téléchargé par le formateur à partir du centre de logiciel en ligne Cisco Connection. Dans le cadre de ces travaux pratiques, le fichier c2960-lanbase-mz.122-25.FX.tar est référencé à des fins pédagogiques uniquement. Il a la même racine de nom de fichier que l'image en cours. Cependant, pour les besoins de ces travaux pratiques, nous supposerons que ce fichier est une mise à jour. La version de mise à jour du logiciel Cisco IOS inclut les fichiers image binaire et de nouveaux fichiers HTML pour prendre en charge les modifications de l'interface Web.

Ces travaux pratiques nécessitent également l'enregistrement d'une copie du fichier de configuration actuelle en tant que sauvegarde.

Étape 1 : détermination de la séquence d'amorçage en cours pour le commutateur et vérification de la mémoire disponible

Déterminez s'il y a suffisamment de mémoire pour inclure plusieurs fichiers d'image. Supposons que les nouveaux fichiers requièrent autant d'espace que les fichiers en cours dans la mémoire flash.

La capacité mémoire est-elle suffisante pour stocker des fichiers HTML et Cisco IOS supplémentaires ? _____

Étape 2 : préparation de la nouvelle image

Si le commutateur a suffisamment de mémoire libre comme indiqué dans la dernière étape, renommez le fichier Cisco IOS existant avec le même nom et avec l'extension .old :

Vérifiez que le changement de nom a réussi.

Par précaution, désactivez l'accès aux pages HTML du commutateur, puis supprimez les fichiers HTML existants de la mémoire flash.

Étape 3 : extraction de la nouvelle image Cisco IOS et des nouveaux fichiers HTML vers la mémoire flash

Entrez la commande suivante pour placer la nouvelle image Cisco IOS et les nouveaux fichiers HTML dans le répertoire cible de la mémoire flash :

```
ALSwitch#archive tar /x tftp://172.17.99.21/c2960-lanbase-mz.122-
25.FX.tar flash:/c2960-lanbase-mz.122-25.FX
```

Réactivez le serveur HTTP sur le commutateur.

Étape 4 : association du nouveau fichier d'amorçage

Entrez la commande boot system avec le nom de fichier de la nouvelle image à l'invite du mode de configuration, puis enregistrez la configuration.

Étape 5 : redémarrage du commutateur

Redémarrez le commutateur à l'aide de la commande **reload** pour voir si le nouveau logiciel Cisco IOS a été chargé. Utilisez la commande **show version** pour voir le nom du fichier Cisco IOS.

Quel était le nom du fichier Cisco IOS à partir duquel le commutateur s'est amorcé ? _____

_____

Était-ce le nom de fichier approprié ? _____

Si le nom de fichier Cisco IOS est maintenant correct, supprimez le fichier de sauvegarde (avec l'extension .old) de la mémoire flash.

Tâche 7 : récupération des mots de passe sur Catalyst 2960

Étape 1 : réinitialisation du mot de passe de console

Demandez à un autre participant de modifier les mots de passe de console, vty et secret actif sur le commutateur. Enregistrez les modifications dans le fichier startup-config et rechargez le commutateur.

Ensuite, sans connaître les mots de passe, essayez d'accéder au mode d'exécution privilégié sur le commutateur.

Étape 2 : récupération de l'accès au commutateur

Les procédures détaillées de récupération des mots de passe sont disponibles dans la documentation d'assistance en ligne Cisco. Dans le cas présent, vous les trouverez dans la section de dépannage du guide de configuration du logiciel du commutateur Catalyst 2960. Suivez les procédures pour restaurer l'accès au commutateur.

Après avoir réalisé les étapes précédentes, déconnectez-vous en tapant **exit**, puis mettez tous les périphériques hors tension. Retirez et rangez les câbles et l'adaptateur.

Annexe 1 : récupération des mots de passe sur Catalyst 2960

Récupération d'un mot de passe perdu ou oublié

La configuration par défaut du commutateur permet à un utilisateur final disposant d'un accès physique au commutateur de récupérer un mot de passe perdu en interrompant le processus d'amorçage pendant la mise en route et en saisissant un nouveau mot de passe. Pour utiliser ces procédures de récupération, il est nécessaire de disposer d'un accès physique au commutateur.

Remarque Sur ces commutateurs, un administrateur système peut désactiver certaines de ces fonctionnalités en permettant à un utilisateur final de réinitialiser un mot de passe en acceptant simplement de rétablir la configuration par défaut. En tant qu'utilisateur final, si vous essayez de réinitialiser un mot de passe alors que la récupération de mots de passe a été désactivée, un message d'état vous en avertit pendant le processus de récupération.

Les sections suivantes décrivent la récupération d'un mot de passe de commutateur oublié ou perdu :

- Procédure avec la récupération de mots de passe activée
- Procédure avec la récupération de mots de passe désactivée

La commande de configuration globale **service password-recovery** vous permet d'activer ou de désactiver la récupération de mots de passe. Suivez les étapes de cette procédure si vous avez oublié ou perdu le mot de passe de commutateur.

Étape 1 Connectez un terminal ou un ordinateur doté d'un logiciel d'émulation de terminal au port de console du commutateur.

Étape 2 Affectez la valeur 9600 bauds au débit de la ligne sur le logiciel d'émulation.

Étape 3 Mettez le commutateur hors tension. Reconnectez le cordon d'alimentation au commutateur et, dans les 15 secondes suivantes, appuyez sur le bouton **Mode** tandis que la LED système clignote en vert. Continuez à appuyer sur le bouton **Mode** jusqu'à ce que la LED système devienne orange, puis vert fixe ; vous pouvez alors relâcher le bouton **Mode**.

Plusieurs lignes d'informations sur le logiciel apparaissent avec les instructions, vous indiquant si la procédure de récupération de mots de passe a été désactivée ou non.

- Si vous voyez apparaître un message commençant par :

```
The system has been interrupted prior to initializing the flash
file system. The
following commands will initialize the flash file system
```

accédez à la section « Procédure avec la récupération de mots de passe activée » et suivez les étapes correspondantes.

- Si vous voyez apparaître un message commençant par :

```
The password-recovery mechanism has been triggered, but is
currently disabled.
```

accédez à la section « Procédure avec la récupération de mots de passe désactivée » et suivez les étapes correspondantes.

Étape 4 Après avoir récupéré le mot de passe, rechargez le commutateur :

```
Switch> reload

Proceed with reload? [confirm] y
```

Procédure avec la récupération de mots de passe activée

Si le mécanisme de récupération de mots de passe est activé, le message suivant apparaît :

```
The system has been interrupted prior to initializing the flash
file system. The following
commands will initialize the flash file system, and finish
loading the operating system
software:

flash_init
load_helper
boot
```

Étape 1 Initialisez le système de fichiers flash :

```
switch: flash_init
```

Étape 2 Si vous avez affecté une valeur différente de 9600 au débit du port de console, il a été réinitialisé à ce débit particulier. Modifiez le débit de la ligne du logiciel d'émulation pour qu'il corresponde à celui du port de console du commutateur.

Étape 3 Chargez les fichiers d'aide :

```
switch: load_helper
```

Étape 4 Affichez le contenu de la mémoire flash :

```
switch: dir flash:
```

Le système de fichiers du commutateur apparaît :

```
Directory of flash:
   13  drwx         192   Mar 01 1993 22:30:48  c2960-lanbase-
mz.122-25.FX
   11  -rwx        5825   Mar 01 1993 22:31:59  config.text
   18  -rwx         720   Mar 01 1993 02:21:30  vlan.dat

16128000 bytes total (10003456 bytes free)
```

Étape 5 Renommez le fichier de configuration en config.text.old.

Ce fichier contient la définition du mot de passe.

```
switch: rename flash:config.text flash:config.text.old
```

Étape 6 Amorcez le système :

```
switch: boot
```

Vous êtes invité à démarrer le programme de configuration. Entrez **N** à l'invite :

```
Continue with the configuration dialog? [yes/no]: N
```

Étape 7 À l'invite du commutateur, passez en mode d'exécution privilégié :

```
Switch> enable
```

Étape 8 Rétablissez le nom d'origine du fichier de configuration :

```
Switch# rename flash:config.text.old flash:config.text
```

Étape 9 Copiez le fichier de configuration en mémoire :

```
Switch# copy flash:config.text system:running-config
Source filename [config.text]?
Destination filename [running-config]?
```

Appuyez sur **Entrée** pour confirmer.

Le fichier de configuration est à présent rechargé et vous pouvez modifier le mot de passe.

Étape 10 Passez en mode de configuration globale :

```
Switch# configure terminal
```

Étape 11 Modifiez le mot de passe :

```
Switch (config)# enable secret password
```

Le mot de passe secret peut être composé de 1 à 25 caractères alphanumériques, commencer par un nombre, tenir compte des majuscules, autoriser les espaces mais ignorer les espaces de début.

Étape 12 Repassez en mode d'exécution privilégié :

```
Switch (config)# exit
Switch#
```

Étape 13 Écrivez la configuration en cours dans le fichier de configuration initiale :

```
Switch# copy running-config startup-config
```

Le nouveau mot de passe se trouve désormais dans la configuration initiale.

Remarque Via cette procédure, votre interface de commutateur virtuelle peut rester désactivée. Vous pouvez afficher l'interface dont l'état est désactivé en exécutant la commande d'exécution privilégiée **show running-config**. Pour réactiver l'interface, exécutez la commande de configuration globale **interface vlan** *id-vlan* et spécifiez l'ID de VLAN de l'interface désactivée. Lorsque le commutateur est en mode de configuration d'interface, exécutez la commande **no shutdown**.

Étape 14 Rechargez le commutateur :

```
Switch# reload
```

Procédure avec la récupération de mots de passe désactivée

Si le mécanisme de récupération de mots de passe est désactivé, le message suivant apparaît :

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default
configuration (y/n)?
```

Attention Si vous rétablissez les résultats de la configuration par défaut pour le commutateur, toutes les configurations existantes sont perdues. Nous vous recommandons de contacter votre administrateur système pour vérifier s'il existe un commutateur de sauvegarde et des fichiers de configuration VLAN.

- Si vous saisissez **n** (non), le processus d'amorçage normal continue comme si le bouton **Mode** n'avait pas été activé ; vous ne pouvez pas accéder à l'invite boot loader et vous ne pouvez pas saisir de nouveau mot de passe. Le message suivant apparaît :

```
Press Enter to continue........
```

- Si vous saisissez **y** (oui), le fichier de configuration dans la mémoire flash et le fichier de base de données VLAN sont supprimés. Lors du chargement de la configuration par défaut, vous pouvez réinitialiser le mot de passe.

Étape 1 Choisissez de continuer la récupération du mot de passe et de perdre la configuration existante :

```
Would you like to reset the system back to the default
configuration (y/n)? Y
```

Étape 2 Chargez les fichiers d'aide :

```
Switch: load_helper
```

Étape 3 Affichez le contenu de la mémoire flash :

```
switch: dir flash:
```

Le système de fichiers du commutateur apparaît :

```
Directory of flash:
13  drwx         192   Mar 01 1993 22:30:48 c2960-lanbase-
mz.122-25.FX.0

16128000 bytes total (10003456 bytes free)
```

Étape 4 Amorcez le système :

```
Switch: boot
```

Vous êtes invité à démarrer le programme de configuration. Pour poursuivre la récupération de mots de passe, saisissez **N** à l'invite :

```
Continue with the configuration dialog? [yes/no]: N
```

Étape 5 À l'invite du commutateur, passez en mode d'exécution privilégié :

```
Switch> enable
```

Étape 6 Passez en mode de configuration globale :

```
Switch# configure terminal
```

Étape 7 Modifiez le mot de passe :

```
Switch (config)# enable secret mot de passe
```

Le mot de passe secret peut être composé de 1 à 25 caractères alphanumériques, commencer par un nombre, tenir compte des majuscules, autoriser les espaces mais ignorer les espaces de début.

Étape 8 Repassez en mode d'exécution privilégié :

```
Switch (config)# exit
Switch#
```

Étape 9 Écrivez la configuration en cours dans le fichier de configuration initiale :

```
Switch# copy running-config startup-config
```

Le nouveau mot de passe se trouve désormais dans la configuration initiale.

Remarque Via cette procédure, votre interface de commutateur virtuelle peut rester désactivée. Vous pouvez afficher l'interface dont l'état est désactivé en exécutant la commande d'exécution privilégiée **show running-config**. Pour réactiver l'interface, exécutez la commande de configuration globale **interface vlan** *id-vlan* et spécifiez l'ID de VLAN de l'interface désactivée. Lorsque le commutateur est en mode de configuration d'interface, exécutez la commande **no shutdown**.

Étape 10 Vous devez maintenant reconfigurer le commutateur. Si l'administrateur système a accès au commutateur de sauvegarde et aux fichiers de configuration VLAN, utilisez-les.

Travaux pratiques 3.5.1 : configuration de base de réseaux locaux virtuels

Diagramme de topologie

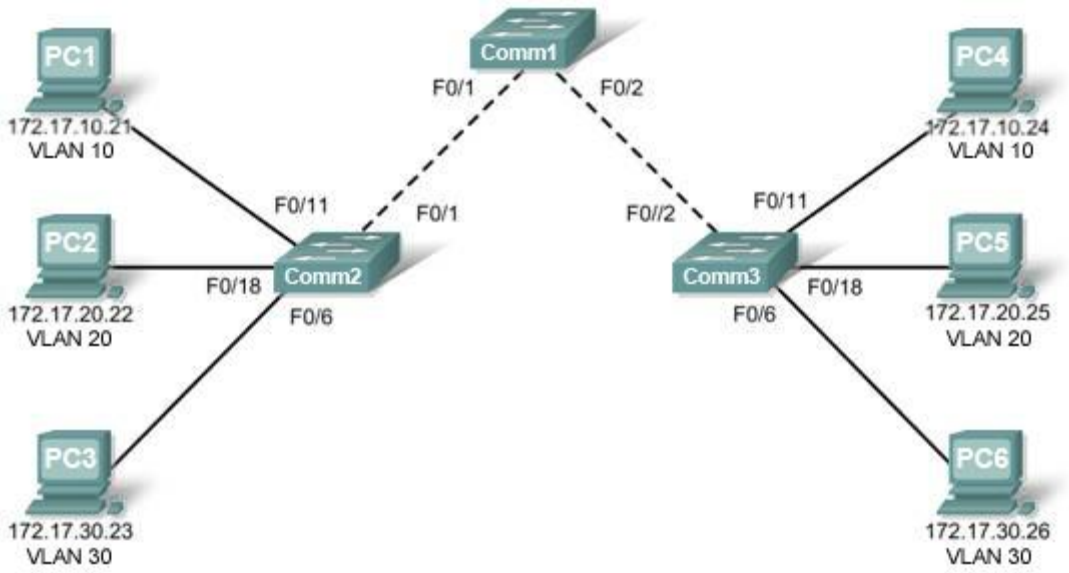


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 99**	172.17.99.11	255.255.255.0	N/D
Comm2	**VLAN 99**	172.17.99.12	255.255.255.0	N/D
Comm3	**VLAN 99**	172.17.99.13	255.255.255.0	N/D
PC1	**Carte réseau**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**Carte réseau**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**Carte réseau**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**Carte réseau**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**Carte réseau**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**Carte réseau**	172.17.30.26	255.255.255.0	172.17.30.1

Affectation initiale des ports (Commutateurs 2 et 3)

Ports	Affectation	Réseau
Fa0/1 – 0/5	Agrégations 802.1q (VLAN 99 natif)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Invité (par défaut)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculté/Personnel	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Participants	172.17.20.0 /24

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Supprimer la configuration initiale et recharger un commutateur pour revenir aux paramètres par défaut
- Exécuter des tâches de configuration de base sur un commutateur
- Créer des réseaux locaux virtuels
- Affecter des ports de commutateur à un réseau local virtuel
- Ajouter, déplacer et modifier les ports
- Vérifier la configuration VLAN
- Activer l'agrégation sur les connexions entre commutateurs
- Vérifier la configuration de l'agrégation
- Enregistrer la configuration VLAN

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Vous pouvez utiliser n'importe quel commutateur durant les travaux pratiques, pourvu qu'il soit équipé des interfaces indiquées dans la topologie.

Remarque : si vous utilisez les commutateurs 2900 ou 2950, les résultats peuvent être différents. Certaines commandes peuvent également être différentes ou non disponibles.

Étape 2 : suppression des configurations existantes sur les commutateurs et initialisation de tous les ports désactivés

Si nécessaire, reportez-vous aux Travaux pratiques 2.5.1, Annexe 1, pour consulter la procédure de suppression des configurations des commutateurs.

Il est recommandé de désactiver tous les ports non utilisés sur les commutateurs. Désactivez tous les ports sur les commutateurs :

```
Switch#config term
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Tâche 2 : configuration de base des commutateurs

Étape 1 : configuration des commutateurs conformément aux instructions suivantes

- Configurez le nom d'hôte du commutateur.
- Désactivez la recherche DNS.
- Configurez le mot de passe **class** pour le mode d'exécution.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.

Étape 2 : réactivation des ports utilisateur sur Comm2 et Comm3

```
Comm2(config)#interface range fa0/6, fa0/11, fa0/18
Comm2(config-if-range)#switchport mode access
Comm2(config-if-range)#no shutdown

Comm3(config)#interface range fa0/6, fa0/11, fa0/18
Comm3(config-if-range)#switchport mode access
Comm3(config-if-range)#no shutdown
```

Tâche 3 : configuration et activation des interfaces Ethernet

Étape 1 : configuration des ordinateurs

Vous pouvez réaliser ces travaux pratiques à l'aide de deux ordinateurs uniquement. Il suffit de modifier l'adressage IP des deux ordinateurs devant réaliser un test. Par exemple, pour tester la connectivité entre PC1 et PC2, configurez les adresses IP pour ces ordinateurs en vous référant au tableau d'adressage au début des travaux pratiques. Vous pouvez aussi configurer les six ordinateurs avec les adresses IP et les passerelles par défaut.

Tâche 4 : configuration des réseaux locaux virtuels sur le commutateur

Étape 1 : création de réseaux locaux virtuels sur le commutateur Comm1

Utilisez la commande **vlan** *id-vlan* en mode de configuration globale pour ajouter un réseau local virtuel pour le commutateur Comm1. Quatre réseaux locaux virtuels sont configurés pour ces travaux pratiques : VLAN 10 (faculté/personnel) ; VLAN 20 (participants) ; VLAN 30 (invité) et VLAN 99 (direction). Après avoir créé le réseau local virtuel, vous pouvez utiliser le mode de configuration vlan pour nommer le réseau local virtuel via la commande **name** *nom vlan*.

```
Comm1(config)#vlan 10
Comm1(config-vlan)#name faculté/personnel
Comm1(config-vlan)#vlan 20
Comm1(config-vlan)#name participants
Comm1(config-vlan)#vlan 30
Comm1(config-vlan)#name invité
Comm1(config-vlan)#vlan 99
Comm1(config-vlan)#name direction
Comm1(config-vlan)#end
Comm1#
```

Étape 2 : vérification de la création des réseaux locaux virtuels pour Comm1

Utilisez la commande **show vlan brief** pour vérifier que les réseaux locaux virtuels ont été créés.

```
Comm1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
```

```
10   faculté/personnel                  active
20   participants                       active
30   invité                             active
99   direction                          active
```

Étape 3 : configuration et affectation d'un nom aux réseaux locaux virtuels pour les commutateurs Comm2 et Comm3

Créez et nommez les réseaux locaux virtuels 10, 20, 30 et 99 pour les commutateurs Comm2 et Comm3 à l'aide des commandes de l'étape 1. Vérifiez la configuration correcte avec la commande **show vlan brief**.

Quels sont les ports actuellement affectés aux quatre réseaux locaux virtuels que vous avez créés ?

_____

Étape 4 : affectation des ports de commutateur aux réseaux locaux virtuels sur Comm2 et Comm3

Reportez-vous au tableau d'affectation des ports de la page 1. Les ports sont affectés aux réseaux locaux virtuels en mode de configuration d'interface, via la commande **switchport access vlan** *id-vlan*. Vous pouvez affecter chaque port individuellement ou utiliser la commande **interface range** pour simplifier cette tâche, comme indiqué ici. Les commandes sont indiquées pour Comm3 uniquement mais vous devez configurer Comm2 et Comm3 de la même façon. Enregistrez votre configuration lorsque vous avez terminé.

```
Comm3(config)#interface range fa0/6-10
Comm3(config-if-range)#switchport access vlan 30
Comm3(config-if-range)#interface range fa0/11-17
Comm3(config-if-range)#switchport access vlan 10
Comm3(config-if-range)#interface range fa0/18-24
Comm3(config-if-range)#switchport access vlan 20
Comm3(config-if-range)#end
Comm3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Étape 4 : détermination des ports ayant été ajoutés

Utilisez la commande **show vlan id** *numéro-vlan* sur Comm2 pour identifier les ports affectés au VLAN 10.

Quels sont les ports affectés au VLAN 10 ?

_____

Remarque : la commande **show vlan id** *nom-vlan* affiche les mêmes résultats.

Vous pouvez également afficher les informations d'affectation VLAN à l'aide de la commande **show interfaces** *interface* **switchport**.

Étape 5 : affectation d'un réseau local virtuel de gestion

Un réseau local virtuel de gestion est un réseau local virtuel que vous configurez pour accéder aux fonctions de gestion d'un commutateur. Si vous ne définissez aucun autre réseau local virtuel, le VLAN 1 fait office de réseau local virtuel de gestion. Affectez une adresse IP et un masque de sous-réseau au réseau local virtuel de gestion. Un commutateur peut être géré via HTTP, Telnet, SSH ou SNMP. Étant donné que la première configuration d'un commutateur Cisco présente le VLAN 1 comme réseau local virtuel par défaut, il n'est pas recommandé d'utiliser le VLAN 1 comme réseau local virtuel de gestion. Vous ne souhaitez pas qu'un utilisateur arbitraire se connectant à un commutateur soit dirigé par défaut vers le réseau local virtuel de gestion. N'oubliez pas que vous avez configuré le réseau local virtuel de gestion en tant que VLAN 99 précédemment dans ces travaux pratiques.

En mode de configuration d'interface, utilisez la commande **ip address** pour affecter l'adresse IP de gestion aux commutateurs.

```
Comm1(config)#interface vlan 99
Comm1(config-if)#ip address 172.17.99.11 255.255.255.0
Comm1(config-if)#no shutdown

Comm2(config)#interface vlan 99
Comm2(config-if)#ip address 172.17.99.12 255.255.255.0
Comm2(config-if)#no shutdown

Comm3(config)#interface vlan 99
Comm3(config-if)#ip address 172.17.99.13 255.255.255.0
Comm3(config-if)#no shutdown
```

L'affectation d'une adresse de gestion permet la communication IP entre les commutateurs, ainsi que la connexion aux commutateurs de n'importe quel hôte connecté à un port affecté au VLAN 99. Étant donné que le VLAN 99 est configuré en tant que réseau local virtuel de gestion, tout port affecté à ce réseau local virtuel est considéré comme un port de gestion et doit être sécurisé pour contrôler les périphériques autorisés à se connecter à ce port.

Étape 6 : configuration de l'agrégation et du réseau local virtuel natif pour les ports agrégés sur tous les commutateurs

Les agrégations sont des connexions entre les commutateurs leur permettant d'échanger des informations pour tous les réseaux locaux virtuels. Par défaut, un port agrégé appartient à tous les réseaux locaux virtuels, contrairement à un port d'accès qui ne peut appartenir qu'à un seul réseau local virtuel. Si le commutateur prend en charge l'encapsulation VLAN ISL et 802.1Q, les agrégations doivent spécifier la méthode utilisée. Étant donné que le commutateur 2960 ne prend en charge que l'agrégation 802.1Q, il n'est pas spécifié dans ces travaux pratiques.

Un réseau local virtuel natif est affecté à un port agrégé 802.1Q. Dans la topologie, le réseau local virtuel natif est le VLAN 99. Un port agrégé 802.1Q prend en charge le trafic provenant de plusieurs réseaux locaux virtuels (trafic étiqueté), ainsi que le trafic ne provenant pas d'un réseau local virtuel (trafic non étiqueté). Le port agrégé 802.1Q place le trafic non étiqueté sur le réseau local virtuel natif. Le trafic non étiqueté est généré par un ordinateur connecté à un port de commutateur configuré avec le réseau local virtuel natif. Une des spécifications IEEE 802.1Q pour les réseaux locaux virtuels natifs consiste à conserver la compatibilité amont avec le trafic non étiqueté commun aux scénarios de réseau local existants. Pour les besoins de ces travaux pratiques, un réseau local virtuel natif fait office d'identificateur commun aux extrémités d'un lien agrégé. Il est recommandé d'utiliser un réseau local virtuel autre que le VLAN 1 comme réseau local virtuel natif.

Utilisez la commande **interface range** en mode de configuration globale pour simplifier la configuration de l'agrégation.

```
Comm1(config)#interface range fa0/1-5
Comm1(config-if-range)#switchport mode trunk
Comm1(config-if-range)#switchport trunk native vlan 99
Comm1(config-if-range)#no shutdown
Comm1(config-if-range)#end

Comm2(config)# interface range fa0/1-5
Comm2(config-if-range)#switchport mode trunk
Comm2(config-if-range)#switchport trunk native vlan 99
Comm2(config-if-range)#no shutdown
Comm2(config-if-range)#end
```

```
Comm3(config)# interface range fa0/1-5
Comm3(config-if-range)#switchport mode trunk
Comm3(config-if-range)#switchport trunk native vlan 99
Comm3(config-if-range)#no shutdown
Comm3(config-if-range)#end
```

Vérifiez que les agrégations ont été configurées via la commande **show interface trunk**.

```
Comm1#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99

Port      Vlans allowed on trunk
Fa0/1       1-4094
Fa0/2       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,99
Fa0/2       1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,99
Fa0/2       1,10,20,30,99
```

Étape 7 : vérification de la communication entre les commutateurs

À partir de Comm1, envoyez une requête ping à l'adresse de gestion sur Comm2 et Comm3.

```
Comm1#ping 172.17.99.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
```

```
Comm1#ping 172.17.99.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Étape 8 : envoi d'une requête ping à plusieurs hôtes à partir de PC2

Envoyez une requête ping de l'hôte PC2 à l'hôte PC1 (172.17.10.21). La tentative de requête ping a-t-elle abouti ? _____

Envoyez une requête ping de l'hôte PC2 à l'adresse IP 172.17.99.12 du commutateur VLAN 99.
La tentative de requête ping a-t-elle abouti ? _____

Étant donné que ces hôtes se trouvent sur des sous-réseaux différents et sur des réseaux locaux virtuels différents, ils ne peuvent pas communiquer sans un périphérique de couche 3 qui les achemine entre les différents sous-réseaux.

Envoyez une requête ping de l'hôte PC2 à l'hôte PC5. La tentative de requête ping a-t-elle abouti ?

_____

Étant donné que PC2 se trouve sur le même réseau local virtuel et le même sous-réseau que PC5, la requête ping a abouti.

Étape 9 : transfert de PC1 vers le même réseau local virtuel que PC2

Le port connecté à PC2 (Comm2 Fa0/18) est affecté au VLAN 20, et le port connecté à PC1 (Comm2 Fa0/11) est affecté au VLAN 10. Affectez de nouveau le port Comm2 Fa0/11 au VLAN 20. Vous n'avez pas besoin de supprimer un port d'un réseau local virtuel pour modifier son appartenance au réseau local virtuel. Après avoir réaffecté le port à un nouveau réseau local virtuel, il est automatiquement supprimé de son ancien réseau local virtuel.

```
Comm2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Comm2(config)#interface fastethernet 0/11
Comm2(config-if)#switchport access vlan 20
Comm2(config-if)#end
```

Envoyez une requête ping de l'hôte PC2 à l'hôte PC1. La tentative de requête ping a-t-elle abouti ?

_____

Même si les ports utilisés par PC1 et PC2 se trouvent sur le même réseau local virtuel, leurs sous-réseaux sont différents. Ils ne peuvent donc pas communiquer directement.

Étape 10 : modification de l'adresse IP et du réseau de PC1

Remplacez l'adresse IP de PC1 par 172.17.20.22. Le masque de sous-réseau et la passerelle par défaut peuvent rester identiques. Envoyez de nouveau une requête ping de l'hôte PC2 à l'hôte PC1, en utilisant la nouvelle adresse IP affectée.

La tentative de requête ping a-t-elle abouti ? _____

Pourquoi ?

_____

_____

Tâche 5 : enregistrement des configurations des commutateurs

Sur chaque commutateur, il est conseillé de capturer la configuration courante dans un fichier texte et de l'enregistrer pour pouvoir la réutiliser.

Tâche 6 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 3.5.2 : configuration avancée de réseaux locaux virtuels

Diagramme de topologie

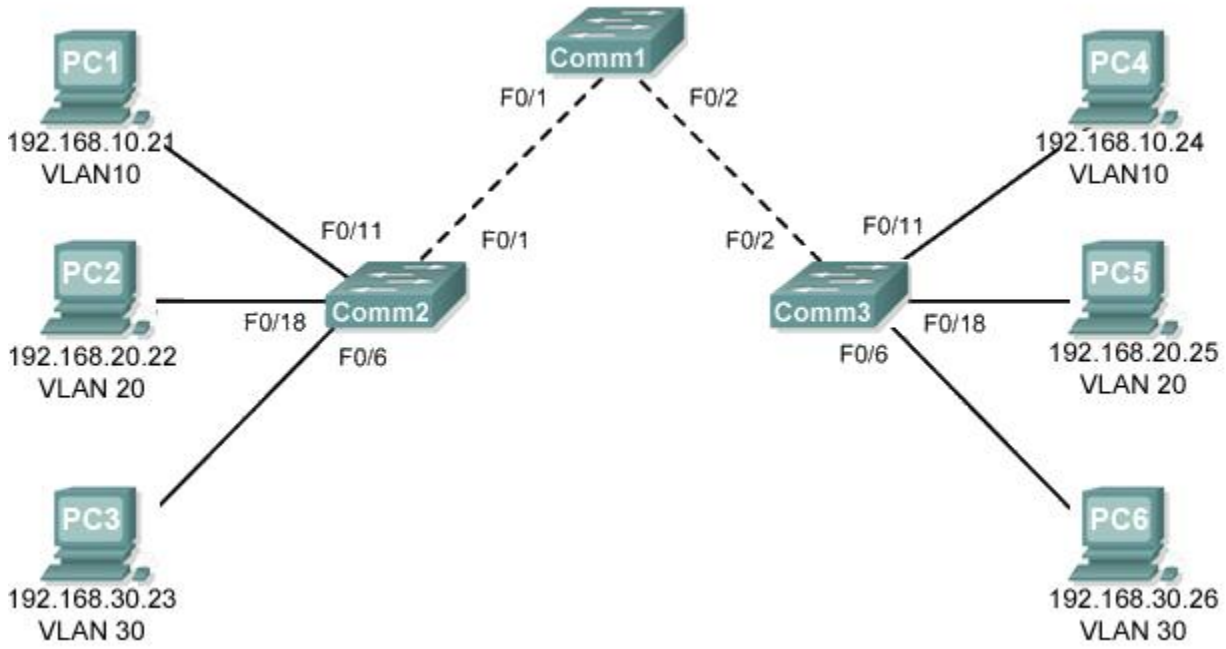


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 56**	192.168.56.11	255.255.255.0	N/D
Comm2	**VLAN 56**	192.168.56.12	255.255.255.0	N/D
Comm3	**VLAN 56**	192.168.56.13	255.255.255.0	N/D
PC1	**Carte réseau**	192.168.10.21	255.255.255.0	192.168.10.1
PC2	**Carte réseau**	192.168.20.22	255.255.255.0	192.168.20.1
PC3	**Carte réseau**	192.168.30.23	255.255.255.0	192.168.30.1
PC4	**Carte réseau**	192.168.10.24	255.255.255.0	192.168.10.1
PC5	**Carte réseau**	192.168.20.25	255.255.255.0	192.168.20.1
PC6	**Carte réseau**	192.168.30.26	255.255.255.0	192.168.30.1

Affectation initiale des ports (Commutateurs 2 et 3)

Ports	Affectation	Réseau
Fa0/1 – 0/5	Agrégations 802.1q (VLAN 56 natif)	192.168.56.0 /24
Fa0/6 – 0/10	VLAN 30 – Invité (par défaut)	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculté/Personnel	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Participants	192.168.20.0 /24

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Supprimer la configuration initiale et recharger un commutateur pour revenir aux paramètres par défaut
- Exécuter des tâches de configuration de base sur un commutateur
- Créer des réseaux locaux virtuels
- Affecter des ports de commutateur à un réseau local virtuel
- Ajouter, déplacer et modifier les ports
- Vérifier la configuration VLAN
- Activer l'agrégation sur les connexions entre commutateurs
- Vérifier la configuration de l'agrégation
- Enregistrer la configuration VLAN

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Étape 2 : suppression des configurations existantes sur les commutateurs et initialisation de tous les ports désactivés

Tâche 2 : configuration de base des commutateurs

Étape 1 : configuration des commutateurs conformément aux instructions suivantes

- Configurez le nom d'hôte du commutateur.
- Désactivez la recherche DNS.
- Configurez le mot de passe **class** pour le mode d'exécution.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.

Étape 2 : réactivation des ports utilisateur sur Comm2 et Comm3

Tâche 3 : configuration et activation des interfaces Ethernet

Étape 1 : configuration des ordinateurs

Configurez les interfaces Ethernet des six ordinateurs avec les adresses IP et les passerelles par défaut à partir du tableau d'adressage au début des travaux pratiques.

Tâche 4 : configuration des réseaux locaux virtuels sur le commutateur

Étape 1 : création de réseaux locaux virtuels sur le commutateur Comm1

Étape 2 : vérification de la création des réseaux locaux virtuels pour Comm1

Étape 3 : configuration, affectation d'un nom et vérification des réseaux locaux virtuels pour les commutateurs Comm2 et Comm3

Étape 4 : affectation des ports de commutateur aux réseaux locaux virtuels sur Comm2 et Comm3

Étape 5 : détermination des ports ayant été ajoutés au VLAN 10 sur Comm2

Étape 6 : configuration du VLAN 56 de gestion sur chaque commutateur

Étape 7 : configuration de l'agrégation et du réseau local virtuel natif pour les ports agrégés sur les trois commutateurs, vérification de la configuration des agrégations

Étape 8 : vérification de la communication entre Comm1, Comm2 et Comm3

Étape 9 : envoi d'une requête ping à plusieurs hôtes à partir de PC2 et résultat

Étape 10 : transfert de PC1 vers le même réseau local virtuel que PC2 ; PC1 peut-il envoyer une requête ping à PC2 ?

Étape 11 : remplacement de l'adresse IP de PC1 par 192.168.10.22 ; PC1 peut-il envoyer une requête ping à PC2 ?

Remplacez l'adresse IP de PC1 par 192.168.10.22. Le masque de sous-réseau et la passerelle par défaut peuvent rester identiques. Envoyez de nouveau une requête ping de l'hôte PC2 à l'hôte PC1, en utilisant la nouvelle adresse IP affectée. La tentative de requête ping a-t-elle abouti ? Oui.

Pourquoi ?

Tâche 5 : enregistrement des configurations des commutateurs

Sur chaque commutateur, il est conseillé de capturer la configuration courante dans un fichier texte et de l'enregistrer pour pouvoir la réutiliser.

Tâche 6 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 3.5.3 : dépannage des configurations de réseaux locaux virtuels

Diagramme de topologie

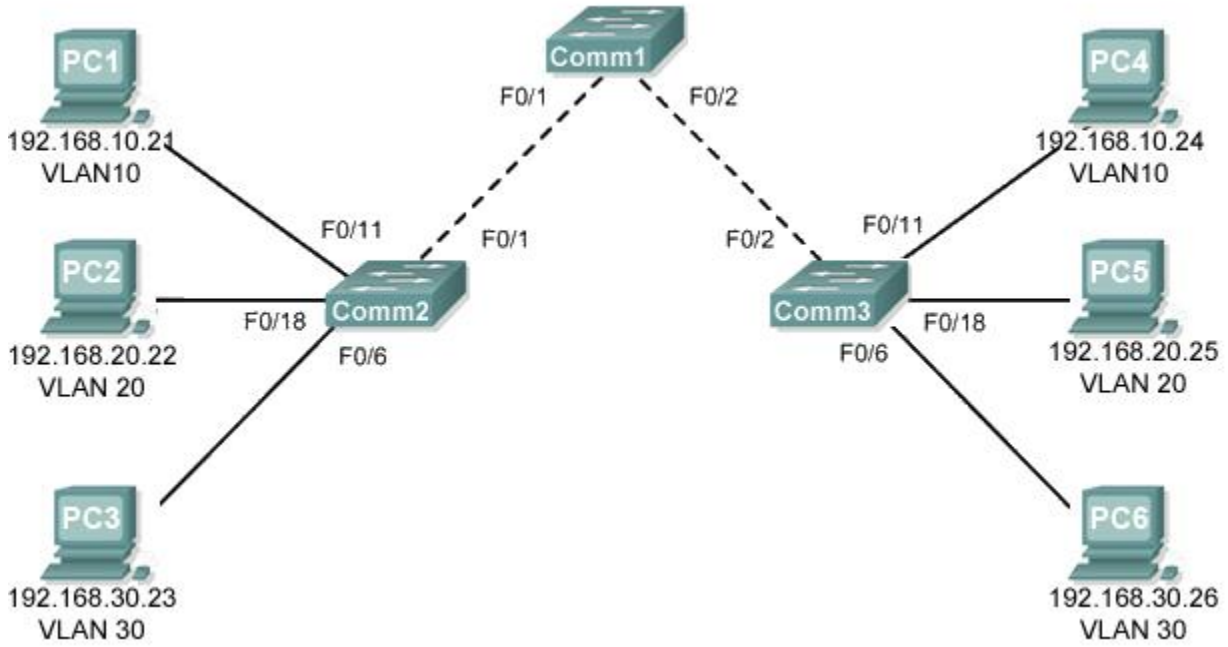


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 56**	192.168.56.11	255.255.255.0	N/D
Comm2	**VLAN 56**	192.168.56.12	255.255.255.0	N/D
Comm3	**VLAN 56**	192.168.56.13	255.255.255.0	N/D
PC1	**Carte réseau**	192.168.10.21	255.255.255.0	192.168.10.1
PC2	**Carte réseau**	192.168.20.22	255.255.255.0	192.168.20.1
PC3	**Carte réseau**	192.168.30.23	255.255.255.0	192.168.30.1
PC4	**Carte réseau**	192.168.10.24	255.255.255.0	192.168.10.1
PC5	**Carte réseau**	192.168.20.25	255.255.255.0	192.168.20.1
PC6	**Carte réseau**	192.168.30.26	255.255.255.0	192.168.30.1

Affectation initiale des ports (Commutateurs 2 et 3)

Ports	Affectation	Réseau
Fa0/1 – 0/5	Agrégations 802.1q (VLAN 56 natif)	192.168.56.0 /24
Fa0/6 – 0/10	VLAN 30 – Invité (par défaut)	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculté/Personnel	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Participants	192.168.20.0 /24

Objectif pédagogique

Mettre en pratique les compétences de base en matière de dépannage des réseaux locaux virtuels

Scénario

Au cours de ces travaux pratiques, vous allez dépanner un environnement de réseau local virtuel dont la configuration est incorrecte. Chargez ou demandez à votre formateur de charger les configurations ci-dessous dans votre installation destinée aux travaux pratiques. Votre objectif est de localiser et de corriger toutes les erreurs dans les configurations et d'établir une connectivité de bout en bout. Votre configuration finale doit correspondre au diagramme de la topologie et au tableau d'adressage. Tous les mots de passe sont **cisco**, sauf le mot de passe secret actif qui est **class**.

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Étape 2 : suppression des configurations existantes sur les commutateurs et initialisation de tous les ports désactivés

Étape 3 : importation des configurations ci-dessous

Commutateur 1

```
hostname Comm1
no ip domain-lookup
enable secret class
!
!
interface range FastEthernet0/1-5
 switchport mode trunk
!
interface range FastEthernet0/6-24
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan56
 ip address 192.168.56.11 255.255.255.0
 no ip route-cache
!
line con 0
 logging synchronous
line vty 0 4
 no login
line vty 5 15
 password cisco
 login
!
end
```

Commutateur 2

```
hostname Comm2
no ip domain-lookup
enable secret class
```

```
!
vlan 10,20,30,56
!
interface FastEthernet0/1-5
 switchport trunk native vlan 56
 switchport mode access
!
interface range FastEthernet0/6-10
 switchport access vlan 30
 switchport mode access
!
interface range FastEthernet0/11-17
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/18-24
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.56.12 255.255.255.0
 no ip route-cache
 shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Commutateur 3

```
hostname Comm3
no ip domain-lookup
enable secret cisco
!
vlan 10,20,30
!
interface range FastEthernet0/1-5
 switchport trunk native vlan 56
 switchport mode trunk
!
interface range FastEthernet0/6-10
 switchport mode access
!
interface range FastEthernet0/11-17
 switchport mode access
```

```
!
interface range FastEthernet0/18-24
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan56
 no ip route-cache
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Tâche 2 : dépannage et réparation des configurations de réseaux locaux virtuels

Tâche 3 : enregistrement des configurations des commutateurs

Sur chaque commutateur, capturez la configuration courante dans un fichier texte et enregistrez-la pour pouvoir la réutiliser :

Tâche 4 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 4.4.1 : configuration de base du protocole VTP

Diagramme de topologie

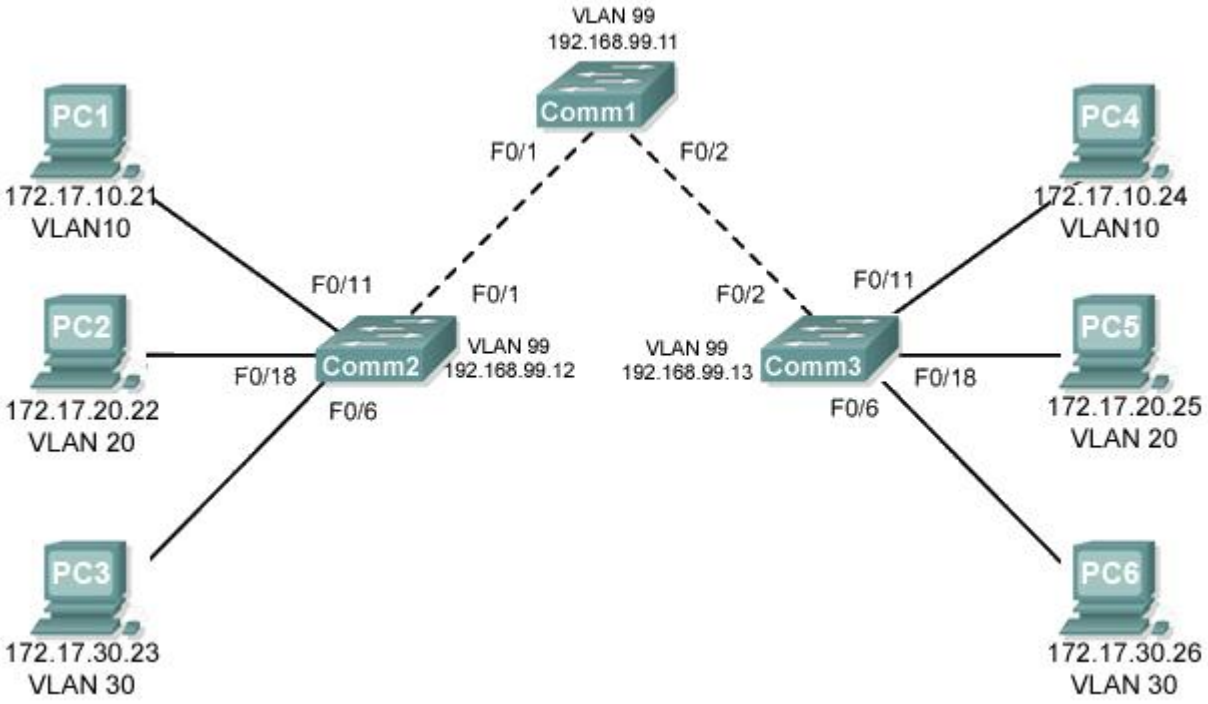


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 99**	172.17.99.11	255.255.255.0	N/D
Comm2	**VLAN 99**	172.17.99.12	255.255.255.0	N/D
Comm3	**VLAN 99**	172.17.99.13	255.255.255.0	N/D
PC1	**Carte réseau**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**Carte réseau**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**Carte réseau**	172.17.30.23	255.255.255.0	172.17.30.1
PC4	**Carte réseau**	172.17.10.24	255.255.255.0	172.17.10.1
PC5	**Carte réseau**	172.17.20.25	255.255.255.0	172.17.20.1
PC6	**Carte réseau**	172.17.30.26	255.255.255.0	172.17.30.1

Affectation des ports (Commutateurs 2 et 3)

Ports	Affectation	Réseau
Fa0/1 – 0/5	Agrégations 802.1q (VLAN 99 natif)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Invité (par défaut)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculté/Personnel	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Participants	172.17.20.0 /24

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Supprimer la configuration initiale et recharger un commutateur pour revenir aux paramètres par défaut
- Exécuter des tâches de configuration de base sur un commutateur
- Configurer le protocole VTP (VLAN Trunking Protocol) sur tous les commutateurs
- Activer l'agrégation sur les connexions entre commutateurs
- Vérifier la configuration de l'agrégation
- Modifier les modes VTP et en observer les conséquences
- Créer des réseaux locaux virtuels sur le serveur VTP et distribuer ces informations VLAN aux commutateurs du réseau
- Expliquer les différences de fonctionnement entre le mode transparent, le mode serveur et le mode client VTP
- Attribuer des ports de commutateur aux réseaux locaux virtuels
- Enregistrer la configuration VLAN
- Activer l'élagage VTP sur le réseau
- Expliquer la manière dont l'élagage réduit le trafic de diffusion inutile sur le réseau local

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Vous pouvez utiliser n'importe quel commutateur durant les travaux pratiques, pourvu qu'il soit équipé des interfaces indiquées dans la topologie. Les résultats présentés dans ces travaux pratiques proviennent des commutateurs 2960. Les autres types de commutateur peuvent produire des résultats différents. Si vous utilisez des commutateurs plus anciens, certaines commandes peuvent être différentes ou indisponibles.

Vous remarquerez dans le tableau d'adressage que les ordinateurs ont été configurés avec une adresse IP de passerelle par défaut. Cette adresse peut correspondre à l'adresse IP du routeur local qui n'est pas inclus dans ce scénario des travaux pratiques. La passerelle par défaut et le routeur sont nécessaires pour que les ordinateurs de différents réseaux locaux virtuels puissent communiquer. Ce point est traité dans un prochain chapitre.

Configurez les connexions console pour les trois commutateurs.

Étape 2 : suppression des configurations actuelles des commutateurs

Si nécessaire, reportez-vous aux Travaux pratiques 2.5.1, Annexe 1, pour consulter la procédure de suppression des configurations des commutateurs et des réseaux locaux virtuels. Utilisez la commande **show vlan** pour confirmer que seuls les réseaux locaux virtuels par défaut existent et que tous les ports sont affectés au VLAN 1.

```
Comm1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Étape 3 : désactivation de tous les ports à l'aide de la commande shutdown

```
Comm1(config)#interface range fa0/1-24
Comm1(config-if-range)#shutdown
Comm1(config-if-range)#interface range gi0/1-2
Comm1(config-if-range)#shutdown

Comm2(config)#interface range fa0/1-24
Comm2(config-if-range)#shutdown
Comm2(config-if-range)#interface range gi0/1-2
Comm2(config-if-range)#shutdown

Comm3(config)#interface range fa0/1-24
Comm3(config-if-range)#shutdown
Comm3(config-if-range)#interface range gi0/1-2
Comm3(config-if-range)#shutdown
```

Étape 4 : réactivation des ports utilisateur sur Comm2 et Comm3

Configurez les ports utilisateur en mode access. Reportez-vous au diagramme de topologie pour déterminer les ports connectés aux périphériques des utilisateurs finaux.

```
Comm2(config)#interface fa0/6
Comm2(config-if)#switchport mode access
Comm2(config-if)#no shutdown
Comm2(config-if)#interface fa0/11
Comm2(config-if)#switchport mode access
Comm2(config-if)#no shutdown
Comm2(config-if)#interface fa0/18
Comm2(config-if)#switchport mode access
Comm2(config-if)#no shutdown
```

```
Comm3(config)#interface fa0/6
Comm3(config-if)#switchport mode access
Comm3(config-if)#no shutdown
Comm3(config-if)#interface fa0/11
Comm3(config-if)#switchport mode access
Comm3(config-if)#no shutdown
Comm3(config-if)#interface fa0/18
Comm3(config-if)#switchport mode access
Comm3(config-if)#no shutdown
```

Tâche 2 : configuration de base des commutateurs

Configurez les commutateurs Comm1, Comm2 et Comm3 conformément aux instructions suivantes et enregistrez toutes vos configurations :

- Configurez le nom d'hôte du commutateur comme indiqué dans la topologie.
- Désactivez la recherche DNS.
- Configurez le mot de passe **class** pour le mode d'exécution.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.

(Résultats pour Comm1)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Comm1
Comm1(config)#enable secret class
Comm1(config)#no ip domain-lookup
Comm1(config)#line console 0
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#line vty 0 15
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
Comm1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Tâche 3 : configuration des interfaces Ethernet sur les ordinateurs hôtes

Configurez les interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 et PC6 avec les adresses IP et les passerelles par défaut indiquées dans le tableau d'adressage au début des travaux pratiques.

Vérifiez que PC1 peut envoyer une requête ping à PC4, que PC2 peut envoyer une requête ping à PC5, et que PC3 peut faire de même à PC6.

Tâche 4 : configuration du protocole VTP sur les commutateurs

Le protocole VTP permet à l'administrateur réseau de contrôler les instances des réseaux locaux virtuels sur le réseau en créant des domaines VTP. Dans chaque domaine VTP, un ou plusieurs commutateurs sont configurés en tant que serveurs VTP. Les réseaux locaux virtuels sont alors créés sur le serveur VTP et élargis aux autres commutateurs du domaine. La définition du mode de fonctionnement, du domaine et du mot de passe font partie des tâches de configuration VTP courantes. Au cours de ces travaux pratiques, vous utiliserez Comm1 comme serveur VTP, Comm2 et Comm3 étant configurés comme clients VTP ou en mode transparent VTP.

Étape 1 : vérification des paramètres VTP courants sur les trois commutateurs

```
Comm1#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Comm2#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Comm3#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Notez que les trois commutateurs sont en mode serveur. Le mode serveur est le mode VTP par défaut pour la plupart des commutateurs Catalyst.

Étape 2 : configuration du mode de fonctionnement, du nom de domaine et du mot de passe VTP sur les trois commutateurs

Configurez le nom de domaine VTP **Lab4** et le mot de passe VTP **cisco** pour les trois commutateurs**.** Configurez Comm1 en mode serveur, Comm2 en mode client et Comm3 en mode transparent.

```
Comm1(config)#vtp mode server
Le périphérique est déjà en mode SERVEUR VTP.
Comm1(config)#vtp domain Lab4
Remplacement du nom de domaine VTP NULL par Lab4
Comm1(config)#vtp password cisco
Définition du mot de passe cisco de la base de données du réseau local
virtuel du périphérique
Comm1(config)#end

Comm2(config)#vtp mode client
Définition du périphérique en mode CLIENT VTP
Comm2(config)#vtp domain Lab4
Remplacement du nom de domaine VTP NULL par Lab4
Comm2(config)#vtp password cisco
Définition du mot de passe cisco de la base de données du réseau local
virtuel du périphérique
Comm2(config)#end

Comm3(config)#vtp mode transparent
Définition du périphérique en mode TRANSPARENT VTP
Comm3(config)#vtp domain Lab4
Remplacement du nom de domaine VTP NULL par Lab4
Comm3(config)#vtp password cisco
Définition du mot de passe cisco de la base de données du réseau local
virtuel du périphérique
Comm3(config)#end
```

Remarque : le nom de domaine VTP peut être appris par un commutateur client à partir d'un commutateur serveur, mais uniquement si le domaine du commutateur client a l'état Null. Il n'apprend pas de nouveau nom si un nom a déjà été défini. Pour cela, il est recommandé de configurer manuellement le nom de domaine sur tous les commutateurs pour s'assurer qu'il est correctement configuré. Les commutateurs de différents domaines VTP n'échangent pas les informations VLAN.

Étape 3 : configuration de l'agrégation et du réseau local virtuel natif pour les ports agrégés sur les trois commutateurs

Utilisez la commande **interface range** en mode de configuration globale pour simplifier cette tâche.

```
Comm1(config)#interface range fa0/1-5
Comm1(config-if-range)#switchport mode trunk
Comm1(config-if-range)#switchport trunk native vlan 99
Comm1(config-if-range)#no shutdown
Comm1(config-if-range)#end

Comm2(config)# interface range fa0/1-5
Comm2(config-if-range)#switchport mode trunk
Comm2(config-if-range)#switchport trunk native vlan 99
Comm2(config-if-range)#no shutdown
Comm2(config-if-range)#end
```

```
Comm3(config)# interface range fa0/1-5
Comm3(config-if-range)#switchport mode trunk
Comm3(config-if-range)#switchport trunk native vlan 99
Comm3(config-if-range)#no shutdown
Comm3(config-if-range)#end
```

Étape 4 : configuration de la sécurité des ports sur les commutateurs de couche d'accès Comm2 et Comm3

Configurez les ports fa0/6, fa0/11 et fa0/18 afin qu'ils autorisent uniquement un seul hôte et qu'ils apprennent l'adresse MAC de l'hôte de manière dynamique.

```
Comm2(config)#interface fa0/6
Comm2(config-if)#switchport port-security
Comm2(config-if)#switchport port-security maximum 1
Comm2(config-if)#switchport port-security mac-address sticky
Comm2(config-if)#interface fa0/11
Comm2(config-if)#switchport port-security
Comm2(config-if)#switchport port-security maximum 1
Comm2(config-if)#switchport port-security mac-address sticky
Comm2(config-if)#interface fa0/18
Comm2(config-if)#switchport port-security
Comm2(config-if)#switchport port-security maximum 1
Comm2(config-if)#switchport port-security mac-address sticky
Comm2(config-if)#end
```

```
Comm3(config)#interface fa0/6
Comm3(config-if)#switchport port-security
Comm3(config-if)#switchport port-security maximum 1
Comm3(config-if)#switchport port-security mac-address sticky
Comm3(config-if)#interface fa0/11
Comm3(config-if)#switchport port-security
Comm3(config-if)#switchport port-security maximum 1
Comm3(config-if)#switchport port-security mac-address sticky
Comm3(config-if)#interface fa0/18
Comm3(config-if)#switchport port-security
Comm3(config-if)#switchport port-security maximum 1
Comm3(config-if)#switchport port-security mac-address sticky
Comm3(config-if)#end
```

Étape 5 : configuration des réseaux locaux virtuels sur le serveur VTP

Quatre réseaux locaux virtuels supplémentaires sont requis dans ces travaux pratiques :

- VLAN 99 (direction)
- VLAN 10 (faculté/personnel)
- VLAN 20 (participants)
- VLAN 30 (invité)

Configurez ces réseaux sur le serveur VTP.

```
Comm1(config)#vlan 99
Comm1(config-vlan)#name direction
Comm1(config-vlan)#exit
Comm1(config)#vlan 10
Comm1(config-vlan)#name faculté/personnel
Comm1(config-vlan)#exit
Comm1(config)#vlan 20
Comm1(config-vlan)#name participants
Comm1(config-vlan)#exit
Comm1(config)#vlan 30
Comm1(config-vlan)#name invité
Comm1(config-vlan)#exit
```

Vérifiez que les réseaux locaux virtuels ont été créés sur Comm1 via la commande **show vlan brief**.

Étape 6 : vérification de la distribution sur Comm2 et Comm3 des réseaux locaux virtuels créés sur Comm1

Utilisez la commande **show vlan brief** sur Comm2 et Comm3 pour déterminer si le serveur VTP a élargi la configuration des réseaux locaux virtuels à tous les commutateurs.

```
Comm2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
10   faculté/personnel                  active
20   participants                       active
30   invité                             active
99   direction                          active

Comm3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Les mêmes réseaux locaux virtuels sont-ils configurés sur tous les commutateurs ? _____

Expliquez ici pourquoi Comm2 et Comm3 ont des configurations de réseaux locaux virtuels différentes.

_____

_____

_____

Étape 7 : création d'un réseau local virtuel sur les commutateurs 2 et 3

```
Comm2(config)#vlan 88
La configuration d'un réseau local virtuel %VTP n'est pas autorisée lorsque
le périphérique est en mode CLIENT.

Comm3(config)#vlan 88
Comm3(config-vlan)#name test
Comm3(config-vlan)#
```

Pourquoi est-il impossible de créer un réseau local virtuel sur Comm2, alors que cela est possible sur Comm3 ? _____

_____

Supprimez le VLAN 88 de Comm3.

```
Comm3(config)#no vlan 88
```

Étape 8 : configuration manuelle des réseaux locaux virtuels

Configurez les quatre réseaux locaux virtuels identifiés à l'étape 5 sur le commutateur Comm3.

```
Comm3(config)#vlan 99
Comm3(config-vlan)#name direction
Comm3(config-vlan)#exit
Comm3(config)#vlan 10
Comm3(config-vlan)#name faculté/personnel
Comm3(config-vlan)#exit
Comm3(config)#vlan 20
Comm3(config-vlan)#name participants
Comm3(config-vlan)#exit
Comm3(config)#vlan 30
Comm3(config-vlan)#name invité
Comm3(config-vlan)#exit
```

Un des avantages de VTP est illustré ici. La configuration manuelle est fastidieuse et présente des risques d'erreur, et toute erreur introduite ici peut empêcher la communication au sein du réseau local virtuel. En outre, ces types d'erreurs peuvent être difficiles à résoudre.

Étape 9 : configuration de l'adresse de l'interface de gestion sur les trois commutateurs

```
Comm1(config)#interface vlan 99
Comm1(config-if)#ip address 172.17.99.11 255.255.255.0
Comm1(config-if)#no shutdown
```

```
Comm2(config)#interface vlan 99
Comm2(config-if)#ip address 172.17.99.12 255.255.255.0
Comm2(config-if)#no shutdown

Comm3(config)#interface vlan 99
Comm3(config-if)#ip address 172.17.99.13 255.255.255.0
Comm3(config-if)#no shutdown
```

Vérifiez que les commutateurs sont configurés correctement en envoyant des requêtes ping entre eux. À partir de Comm1, envoyez une requête ping à l'interface de gestion sur Comm2 et Comm3. À partir de Comm2, envoyez une requête ping à l'interface de gestion sur Comm3.

Les requêtes ping ont-elles abouti ? _____

Dans le cas contraire, corrigez les configurations des commutateurs et réessayez.

Étape 10 : affectation des ports de commutateur aux réseaux locaux virtuels

Reportez-vous au tableau d'affectation des ports au début des travaux pratiques pour affecter les ports aux réseaux locaux virtuels. Utilisez la commande **interface range** pour simplifier cette tâche. Les affectations des ports ne sont pas configurées via VTP. Elles doivent être configurées sur chaque commutateur de manière manuelle ou dynamique via un serveur VMPS. Les commandes sont décrites pour Comm3 uniquement mais les commutateurs Comm2 et Comm1 doivent également être configurés de la même façon. Enregistrez la configuration lorsque vous avez terminé.

```
Comm3(config)#interface range fa0/6-10
Comm3(config-if-range)#switchport access vlan 30
Comm3(config-if-range)#interface range fa0/11-17
Comm3(config-if-range)#switchport access vlan 10
Comm3(config-if-range)#interface range fa0/18-24
Comm3(config-if-range)#switchport access vlan 20
Comm3(config-if-range)#end
Comm3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
Comm3#
```

Tâche 5 : configuration de l'élagage VTP sur les commutateurs

L'élagage VTP permet à un serveur VTP de supprimer le trafic de diffusion IP pour des réseaux locaux virtuels spécifiques et de le remplacer par des commutateurs ne présentant aucun port dans ce réseau local virtuel. Par défaut, toutes les monodiffusions et diffusions inconnues d'un réseau local virtuel sont transmises à l'ensemble du réseau local virtuel. Tous les commutateurs du réseau reçoivent l'ensemble des diffusions, même lorsque peu d'utilisateurs sont connectés à ce réseau local virtuel. L'élagage VTP est utilisé pour éliminer ou élaguer ce trafic inutile. L'élagage préserve la bande passante du réseau local car il est inutile de transmettre les diffusions aux commutateurs qui n'en ont pas besoin.

L'élagage est configuré sur le commutateur de serveur via la commande **vtp pruning** en mode de configuration globale. La configuration est élargie aux commutateurs client. Cependant, comme Comm3 est en mode transparent, l'élagage VTP doit être configuré localement sur ce commutateur.

Confirmez la configuration de l'élagage VTP sur chaque commutateur à l'aide de la commande **show vtp status**. Le mode d'élagage VTP doit être activé sur chaque commutateur.

```
Comm1#show vtp status
VTP Version                     : 2
Configuration Revision          : 17
Maximum VLANs supported locally : 255
```

```
Number of existing VLANs          : 9
VTP Operating Mode                : Server
VTP Domain Name                   : Lab4
VTP Pruning Mode                  : Enabled
<résultat omis>
```

Tâche 6 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 4.4.2 : configuration avancée du protocole VTP

Topologie

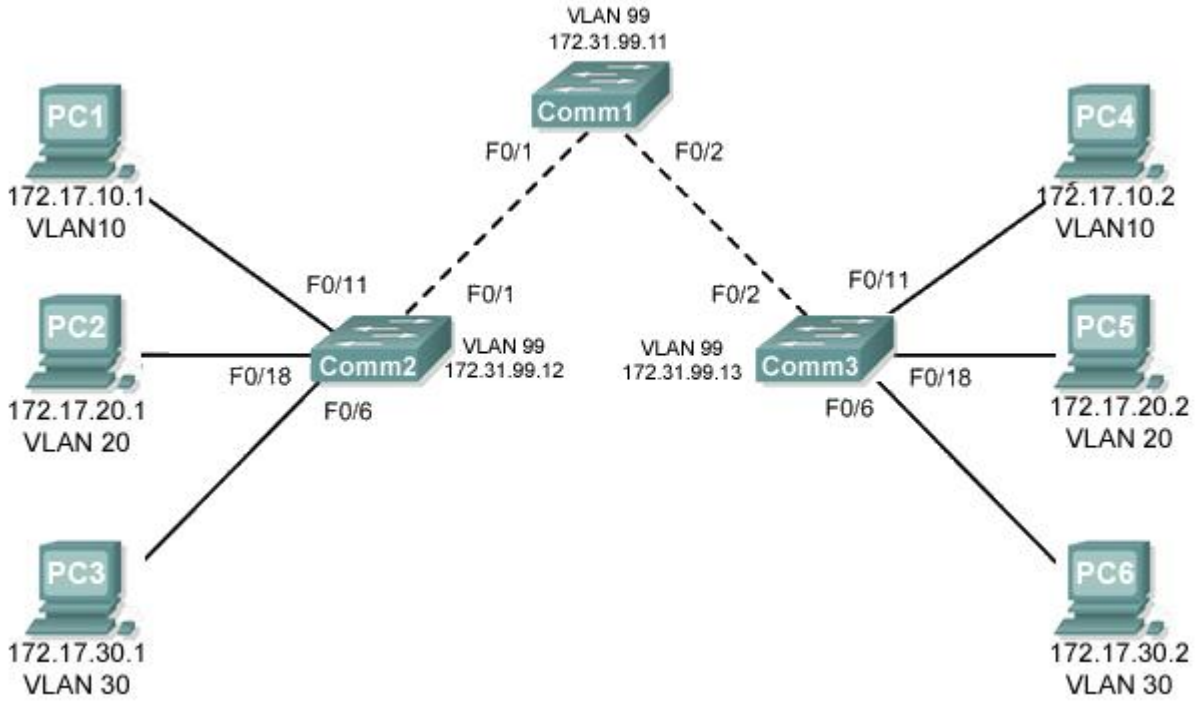


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 99**	172.31.99.11	255.255.255.0	N/D
Comm2	**VLAN 99**	172.31.99.12	255.255.255.0	N/D
Comm3	**VLAN 99**	172.31.99.13	255.255.255.0	N/D
PC1	**Carte réseau**	172.31.10.1	255.255.255.0	
PC2	**Carte réseau**	172.31.20.1	255.255.255.0	
PC3	**Carte réseau**	172.31.30.1	255.255.255.0	
PC4	**Carte réseau**	172.31.10.2	255.255.255.0	
PC5	**Carte réseau**	172.31.20.2	255.255.255.0	
PC6	**Carte réseau**	172.31.30.2	255.255.255.0	

Affectation des ports (Commutateurs 2 et 3)

Ports	Affectation	Réseau
Fa0/1 – 0/5	Agrégations 802.1q	
Fa0/11 – 0/17	VLAN 10 – Ingénierie	172.31.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Ventes	172.31.20.0 /24
Fa0/6 – 0/10	VLAN 30 – Administration	172.31.30.0 /24
Aucun	VLAN 99 – Direction	172.31.99.0 /24

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Supprimer la configuration initiale et recharger un commutateur pour revenir aux paramètres par défaut
- Exécuter des tâches de configuration de base sur un commutateur
- Configurer le protocole VTP (VLAN Trunking Protocol) sur tous les commutateurs
- Activer l'agrégation sur les connexions entre commutateurs
- Vérifier la configuration de l'agrégation
- Modifier les modes VTP et en observer les conséquences
- Créer des réseaux locaux virtuels sur le serveur VTP et distribuer ces informations VLAN aux commutateurs du réseau
- Expliquer les différences de fonctionnement entre le mode transparent, le mode serveur et le mode client VTP
- Attribuer des ports de commutateur aux réseaux locaux virtuels
- Enregistrer la configuration VLAN

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Étape 2 : suppression des configurations actuelles des commutateurs

Étape 3 : désactivation de tous les ports à l'aide de la commande shutdown

Étape 4 : réactivation des ports utilisateur sur Comm2 et Comm3 et définition du mode access (reportez-vous au diagramme de topologie pour déterminer les ports connectés aux périphériques des utilisateurs finaux)

Tâche 2 : configuration de base des commutateurs

Configurez les commutateurs Comm1, Comm2 et Comm3 conformément aux instructions suivantes et enregistrez toutes vos configurations :

- Configurez le nom d'hôte du commutateur comme indiqué dans la topologie.
- Désactivez la recherche DNS.
- Configurez le mot de passe **class** pour le mode d'exécution.

- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.

Tâche 3 : configuration des interfaces Ethernet sur les ordinateurs hôtes

Configurez les interfaces Ethernet de PC1 à PC6 avec les adresses IP indiquées dans le tableau d'adressage au début des travaux pratiques.

Tâche 4 : configuration du protocole VTP sur les commutateurs

Étape 1 : vérification des paramètres VTP courants sur les trois commutateurs

Étape 2 : configuration du mode de fonctionnement, du nom de domaine et du mot de passe VTP sur les trois commutateurs

Étape 3 : configuration de l'agrégation et du réseau local virtuel natif pour les ports agrégés sur les trois commutateurs

Configurez les ports Fa0/1 à Fa0/5 en mode d'agrégation. Configurez le VLAN 99 en tant que réseau local virtuel natif pour ces agrégations. Vous pouvez utiliser la commande **interface range** pour simplifier cette tâche. N'oubliez pas d'activer les interfaces agrégées.

Étape 4 : configuration de la sécurité des ports d'accès Comm2 et Comm3

Configurez les ports Fa0/6, Fa0/11 et Fa0/18 sur Comm2 et Comm3 afin d'autoriser la connexion de deux hôtes au maximum et de permettre l'apprentissage des adresses MAC des hôtes de manière dynamique.

Étape 5 : configuration des réseaux locaux virtuels sur le serveur VTP

Lorsque vous avez terminé, vérifiez que les quatre réseaux locaux virtuels ont été créés sur Comm1.

Étape 6 : vérification de la distribution sur Comm2 et Comm3 des réseaux locaux virtuels créés sur Comm1

Étape 7 : configuration de l'adresse de l'interface de gestion sur les trois commutateurs conformément au tableau d'adressage fourni au début des travaux pratiques

Affectez ces adresses au réseau local virtuel d'administration réseau (VLAN 99).

Vérifiez que les commutateurs sont configurés correctement en envoyant des requêtes ping entre eux. À partir de Comm1, envoyez une requête ping à l'interface de gestion sur Comm2 et Comm3. À partir de Comm2, envoyez une requête ping à l'interface de gestion sur Comm3.
Si la réponse est non, dépannez les configurations des commutateurs et résolvez les problèmes.

Étape 8 : affectation des ports de commutateur aux réseaux locaux virtuels

Reportez-vous au tableau d'affectation des ports au début des travaux pratiques pour affecter les ports aux réseaux locaux virtuels.

Étape 9 : vérification du fonctionnement des agrégations

Tâche 5 : configuration de l’élagage VTP sur les commutateurs

L’élagage VTP permet à un serveur VTP de supprimer le trafic de diffusion IP pour des réseaux locaux virtuels spécifiques et de le remplacer par des commutateurs ne présentant aucun port dans ce réseau local virtuel. Par défaut, toutes les monodiffusions et diffusions inconnues d’un réseau local virtuel sont transmises à l’ensemble du réseau local virtuel. Tous les commutateurs du réseau reçoivent l’ensemble des diffusions, même lorsque peu d’utilisateurs sont connectés à ce réseau local virtuel. L’élagage VTP élimine ou élague ce trafic inutile. L’élagage préserve la bande passante du réseau local car il est inutile de transmettre les diffusions aux commutateurs qui n’en ont pas besoin.

Configurez l’élagage sur le commutateur serveur, qui sera ensuite élargi aux commutateurs client. Cependant, comme Comm3 est en mode transparent, l’élagage VTP doit être également configuré localement sur ce commutateur.

Confirmez la configuration de l’élagage VTP sur chaque commutateur à l’aide de la commande **show vtp status**. Le mode d’élagage VTP doit avoir la valeur « Activé » sur chaque commutateur.

Tâche 6 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 4.4.3 : dépannage de la configuration du protocole VTP

Diagramme de topologie

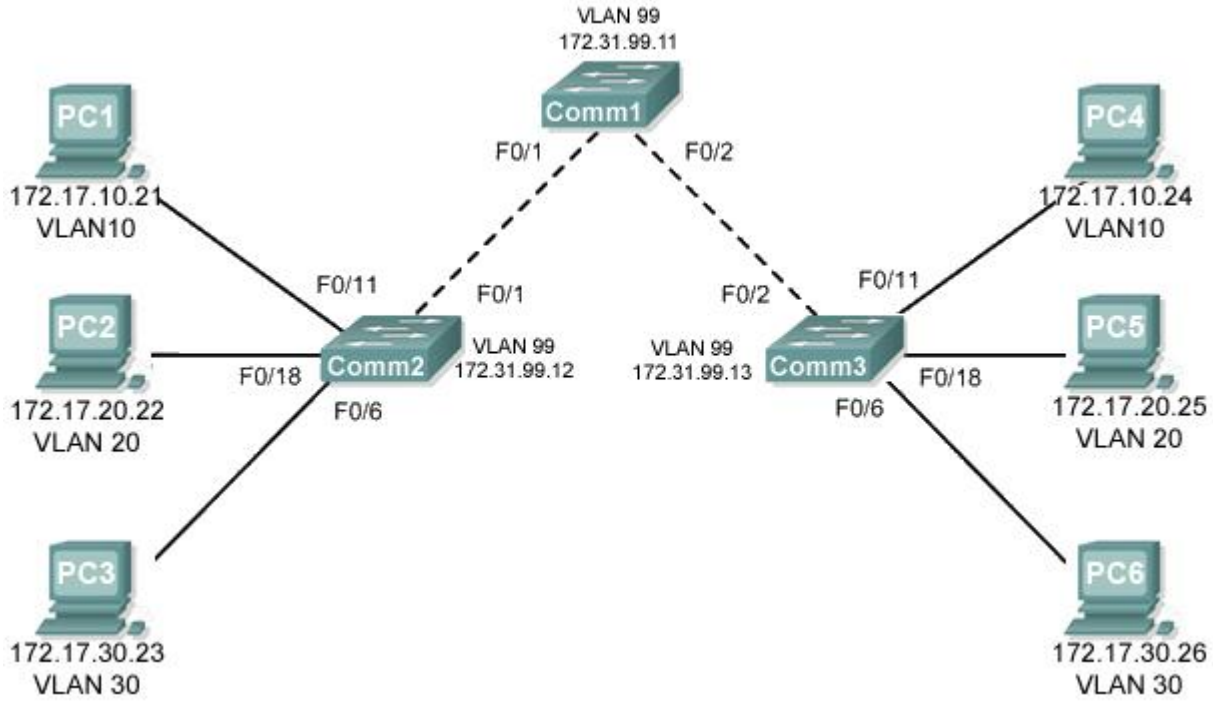


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau
Comm1	**VLAN 99**	172.17.99.11	255.255.255.0
Comm2	**VLAN 99**	172.17.99.12	255.255.255.0
Comm3	**VLAN 99**	172.17.99.13	255.255.255.0
PC1	**Carte réseau**	172.17.10.21	255.255.255.0
PC2	**Carte réseau**	172.17.20.22	255.255.255.0
PC3	**Carte réseau**	172.17.30.23	255.255.255.0
PC4	**Carte réseau**	172.17.10.24	255.255.255.0
PC5	**Carte réseau**	172.17.20.25	255.255.255.0
PC6	**Carte réseau**	172.17.30.26	255.255.255.0

Affectation des ports (Commutateurs 2 et 3)

Ports	Affectation	Réseau
Fa0/1 – 0/5	Agrégations 802.1q (VLAN 99 natif)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Invité (par défaut)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculté/Personnel	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Participants	172.17.20.0 /24

Objectifs

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

- Installer un réseau conformément au diagramme de topologie
- Supprimer la configuration initiale et les fichiers vlan.dat et recharger les commutateurs pour revenir aux paramètres par défaut
- Charger les commutateurs avec les scripts fournis
- Rechercher et corriger toutes les erreurs de configuration
- Enregistrer le réseau corrigé

Scénario

Le protocole VTP (VLAN Trunking Protocol), s'il est configuré correctement, permet de créer des configurations de réseaux locaux virtuels uniformes sur votre réseau commuté. Au cours de ces travaux pratiques, vous utiliserez les scripts fournis pour configurer Comm1 comme serveur VTP, Comm2 et Comm3 étant configurés comme clients VTP. Le nom de domaine VTP est Lab3_4 et le mot de passe VTP est cisco. Toutefois, il existe un certain nombre d'erreurs dans cette configuration que vous devez dépanner et corriger avant de restaurer la connectivité de bout en bout au sein du réseau local virtuel.

Toutes les erreurs sont résolues lorsque les mêmes réseaux locaux virtuels sont configurés sur les trois commutateurs et que vous pouvez envoyer une requête ping entre deux hôtes du même réseau local virtuel ou entre deux commutateurs.

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Vous pouvez utiliser n'importe quel commutateur durant les travaux pratiques, pourvu qu'il soit équipé des interfaces indiquées dans le diagramme de topologie. Les résultats présentés dans ces travaux pratiques proviennent des commutateurs 2960. Les autres types de commutateur peuvent produire des résultats différents. Si vous utilisez des commutateurs plus anciens, certaines commandes peuvent être différentes ou indisponibles.

Configurez les connexions console pour les trois commutateurs.

Étape 2 : suppression des configurations actuelles des commutateurs

Supprimez les configurations des commutateurs et des réseaux locaux virtuels sur les trois commutateurs et rechargez-les avant de restaurer l'état par défaut. Utilisez la commande **show vlan** pour confirmer que seuls les réseaux locaux virtuels par défaut existent et que tous les ports sont affectés au VLAN 1.

Étape 3 : configuration des interfaces Ethernet sur les ordinateurs hôtes

Configurez les interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 et PC6 avec les adresses IP indiquées dans le tableau d'adressage au début des travaux pratiques. Il n'est pas nécessaire de configurer les passerelles par défaut pour ces travaux pratiques.

Tâche 2 : chargement des commutateurs avec les scripts fournis

Configuration de Comm1

```
enable
!
config term
hostname Comm1
enable secret class
no ip domain-lookup
!
vtp mode server
vtp domain Lab4_3
vtp password Cisco
!
vlan 99
name direction
exit
!
vlan 10
name Faculté/Personnel
exit
!
vlan 20
name Participants
exit
!
vlan 30
name Invité
exit
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode access
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface range FastEthernet0/6-24
shutdown
!
interface GigabitEthernet0/1
shutdown
```

```
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan99
 ip address 179.17.99.11 255.255.255.0
  no shutdown
!
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 no login
line vty 1 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Configuration de Comm2

```
hostname Comm2
!
enable secret class
no ip domain-lookup
!
vtp mode client
vtp domain Lab4
!
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode access
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface range FastEthernet0/6- 10
```

```
 switchport access vlan 10
!
switchport mode access
!
interface range FastEthernet0/11- 17
 switchport access vlan 20
switchport mode access
!
interface range FastEthernet0/18- 24
 switchport access vlan 30
 switchport mode access
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
ip http server
!
line con 0
  password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
```

Configuration de Comm3

```
hostname Comm3
!
enable secret class
no ip domain-lookup
!
vtp mode client
vtp domain Lab4
!
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
```

```
 switchport trunk native vlan 99
 switchport mode trunk
!
interface range FastEthernet0/6- 10
 switchport access vlan 30
 switchport mode access
!
interface range FastEthernet0/11- 17
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/18- 24
 switchport access vlan 20
 switchport mode access
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end
```

Tâche 3 : dépannage et correction des erreurs de configuration et de protocole VTP

Lorsque toutes les erreurs sont corrigées, vous devez pouvoir envoyer une requête ping de PC1 à PC4, de PC2 à PC5 et de PC3 à PC6. Vous devez pouvoir envoyer une requête ping aux interfaces de gestion de Comm1 à Comm2 et Comm3.

Tâche 4 : enregistrement de la configuration des commutateurs

Lorsque vous avez terminé le dépannage, capturez les résultats de la commande **show run** et enregistrez-les dans un document texte pour chaque commutateur.

Tâche 5 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 5.5.1 : protocole STP - Notions de base

Diagramme de topologie

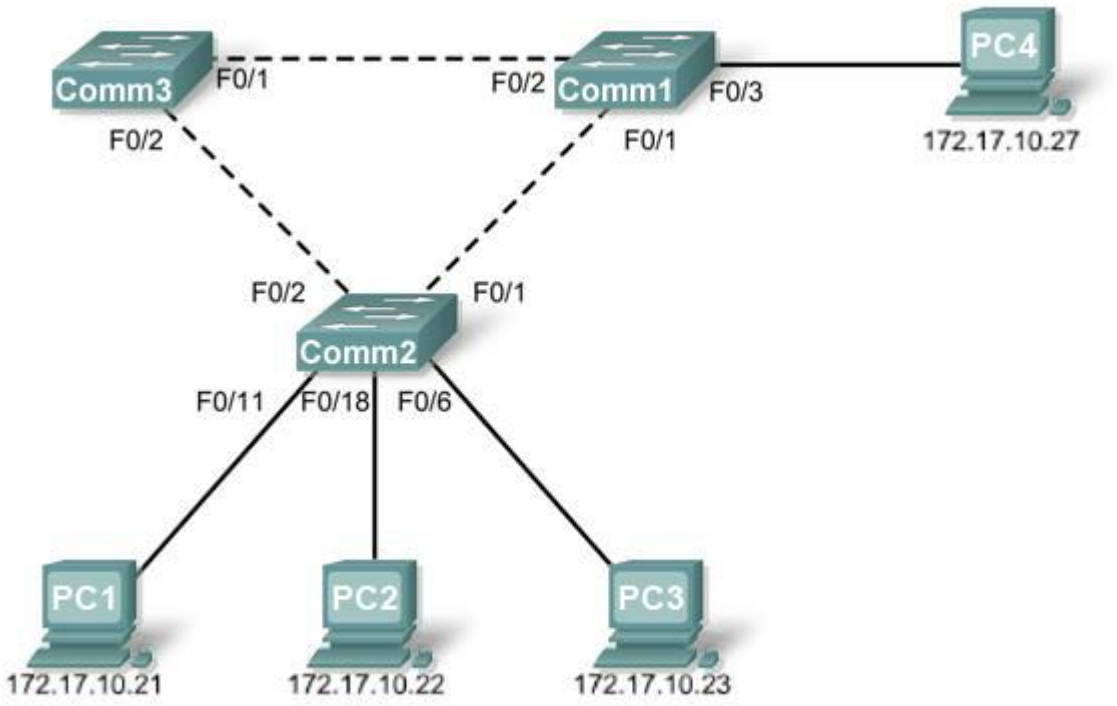


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 1**	172.17.10.1	255.255.255.0	N/D
Comm2	**VLAN 1**	172.17.10.2	255.255.255.0	N/D
Comm3	**VLAN 1**	172.17.10.3	255.255.255.0	N/D
PC1	**Carte réseau**	172.17.10.21	255.255.255.0	172.17.10.254
PC2	**Carte réseau**	172.17.10.22	255.255.255.0	172.17.10.254
PC3	**Carte réseau**	172.17.10.23	255.255.255.0	172.17.10.254
PC4	**Carte réseau**	172.17.10.27	255.255.255.0	172.17.10.254

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Supprimer la configuration initiale et recharger la configuration par défaut, pour revenir aux paramètres par défaut pour un commutateur
- Exécuter des tâches de configuration de base sur un commutateur
- Observer et expliquer le comportement par défaut du protocole Spanning Tree (STP, 802.1D)
- Observer la réponse à une modification de la topologie Spanning Tree

Tâche 1 : configuration de base des commutateurs

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Vous pouvez utiliser n'importe quel commutateur durant les travaux pratiques, pourvu qu'il soit équipé des interfaces indiquées dans le diagramme de topologie. Les résultats présentés dans ces travaux pratiques proviennent des commutateurs Cisco 2960. Les autres modèles de commutateur peuvent produire des résultats différents.

Configurez les connexions console pour les trois commutateurs.

Étape 2 : suppression des configurations actuelles des commutateurs

Videz la mémoire vive non volatile, supprimez le fichier vlan.dat et rechargez les commutateurs. Reportez-vous aux Travaux pratiques 2.5.1 pour consulter la procédure. Une fois le rechargement fini, utilisez la commande du mode d'exécution privilégié **show vlan** pour confirmer que seuls les réseaux locaux virtuels par défaut existent et que tous les ports sont affectés au VLAN 1.

```
Comm1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Étape 3 : configuration des paramètres de commutateur de base

Configurez les commutateurs Comm1, Comm2 et Comm3 en fonction des instructions suivantes :

- Configurez le nom d'hôte du commutateur.
- Désactivez la recherche DNS.
- Configurez le mot de passe **class** pour le mode d'exécution.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.

(Résultats pour Comm1)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Comm1
Comm1(config)#enable secret class
Comm1(config)#no ip domain-lookup
Comm1(config)#line console 0
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#line vty 0 15
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
Comm1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Tâche 2 : préparation du réseau

Étape 1 : désactivation de tous les ports à l'aide de la commande shutdown

Vérifiez que l'état initial des ports de commutateur est inactif via la commande **shutdown**. Utilisez la commande **interface-range** pour simplifier cette tâche.

```
Comm1(config)#interface range fa0/1-24
Comm1(config-if-range)#shutdown
Comm1(config-if-range)#interface range gi0/1-2
Comm1(config-if-range)#shutdown

Comm2(config)#interface range fa0/1-24
Comm2(config-if-range)#shutdown
Comm2(config-if-range)#interface range gi0/1-2
Comm2(config-if-range)#shutdown

Comm3(config)#interface range fa0/1-24
Comm3(config-if-range)#shutdown
Comm3(config-if-range)#interface range gi0/1-2
Comm3(config-if-range)#shutdown
```

Étape 2 : réactivation des ports utilisateur sur Comm1 et Comm2 en mode access

Reportez-vous au diagramme de topologie pour déterminer les ports de commutateur activés sur Comm2 pour l'accès des périphériques des utilisateurs finaux. Ces trois ports seront configurés en mode access et activés via la commande **no shutdown**.

```
Comm1(config)#interface fa0/3
Comm1(config-if)#switchport mode access
Comm1(config-if)#no shutdown

Comm2(config)#interface range fa0/6, fa0/11, fa0/18
Comm2(config-if-range)#switchport mode access
Comm2(config-if-range)#no shutdown
```

Étape 3 : activation des ports agrégés sur Comm1, Comm2 et Comm3

Un seul réseau local virtuel est utilisé dans ces travaux pratiques. Cependant, l'agrégation a été activée sur toutes les liaisons entre les commutateurs pour que des réseaux locaux virtuels supplémentaires puissent être ajoutés ultérieurement.

```
Comm1(config-if-range)#interface range fa0/1, fa0/2
Comm1(config-if-range)#switchport mode trunk
Comm1(config-if-range)#no shutdown

Comm2(config-if-range)#interface range fa0/1, fa0/2
Comm2(config-if-range)#switchport mode trunk
Comm2(config-if-range)#no shutdown

Comm3(config-if-range)#interface range fa0/1, fa0/2
Comm3(config-if-range)#switchport mode trunk
Comm3(config-if-range)#no shutdown
```

Étape 4 : configuration de l'adresse de l'interface de gestion sur les trois commutateurs

```
Comm1(config)#interface vlan1
Comm1(config-if)#ip address 172.17.10.1 255.255.255.0
Comm1(config-if)#no shutdown

Comm2(config)#interface vlan1
Comm2(config-if)#ip address 172.17.10.2 255.255.255.0
Comm2(config-if)#no shutdown

Comm3(config)#interface vlan1
Comm3(config-if)#ip address 172.17.10.3 255.255.255.0
Comm3(config-if)#no shutdown
```

Vérifiez que les commutateurs sont configurés correctement en envoyant des requêtes ping entre eux. À partir de Comm1, envoyez une requête ping à l'interface de gestion sur Comm2 et Comm3. À partir de Comm2, envoyez une requête ping à l'interface de gestion sur Comm3.

Les requêtes ping ont-elles abouti ? _____

Dans le cas contraire, corrigez les configurations des commutateurs et réessayez.

Tâche 3 : configuration des ordinateurs hôtes

Configurez les interfaces Ethernet de PC1, PC2, PC3 et PC4 avec l'adresse IP, le masque de sous-réseau et la passerelle indiqués dans le tableau d'adressage au début des travaux pratiques.

Tâche 4 : configuration du protocole Spanning Tree

Étape 1 : examen de la configuration par défaut du protocole STP 802.1D

Sur chaque commutateur, affichez la table Spanning Tree via la commande **show spanning-tree**. La sélection racine varie en fonction de l'ID de pont de chaque commutateur des travaux pratiques, ce qui donne des résultats différents.

```
Comm1#show spanning-tree


VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0019.068d.6980  Il s'agit de l'adresse MAC du commutateur racine

              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0019.068d.6980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.4    P2p
Fa0/3            Desg FWD 19        128.5    P2p

Comm2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0019.068d.6980
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     001b.0c68.2080
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/11            Desg FWD 19        128.11   P2p
Fa0/18            Desg FWD 19        128.18   P2p


Comm3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0019.068d.6980
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     001b.5303.1700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
```

Étape 2 : examen des résultats

L'identificateur de pont (ID de pont) enregistré dans l'unité BPDU Spanning Tree inclut la priorité du pont, l'extension de l'ID système et l'adresse MAC. On appelle ***priorité de l'ID de pont*** la combinaison ou l'ajout de la priorité du pont et de l'extension de l'ID système. L'extension de l'ID système correspond toujours au numéro du réseau local virtuel. Par exemple, l'extension de l'ID système pour le VLAN 100 est 100. Si la valeur 32768 est utilisée pour la priorité de pont par défaut, la ***priorité de l'ID de pont*** pour le VLAN 100 est 32868 (32768 + 100).

La commande **`show spanning-tree`** affiche la valeur de la ***priorité de l'ID de pont***. Remarque : la valeur « priorité » entre parenthèses représente la valeur de la priorité du pont, suivie par la valeur de l'extension de l'ID système.

Répondez aux questions suivantes à partir des résultats.

1. Quelle est la priorité de l'ID de pont pour les commutateurs Comm1, Comm2 et Comm3 sur le VLAN 1 ?
   a. Comm1 _____
   b. Comm2 _____
   c. Comm3 _____
2. Quel commutateur représente la racine Spanning Tree du VLAN 1 ? _____
3. Sur Comm1, quels sont les ports Spanning Tree à l'état de blocage sur le commutateur racine ? _____
4. Sur Comm3, quel est le port Spanning Tree à l'état de blocage ? _____
5. Comment le commutateur racine est-il choisi via STP ? _____
6. Étant donné que les priorités de pont sont toutes identiques, quel autre élément le commutateur utilise-t-il pour déterminer la racine ? _____

Tâche 5 : observation de la réponse à une modification de la topologie STP 802.1D

Observons maintenant les conséquences de la simulation d'une liaison rompue.

Étape 1 : placement des commutateurs en mode de débogage Spanning Tree via la commande `debug spanning-tree events`

```
Comm1#debug spanning-tree events
Le débogage des événements Spanning Tree est activé
```

```
Comm2#debug spanning-tree events
Le débogage des événements Spanning Tree est activé

Comm3#debug spanning-tree events
Le débogage des événements Spanning Tree est activé
```

Étape 2 : désactivation intentionnelle du port Fa0/1 sur Comm1

```
Comm1(config)#interface fa0/1
Comm1(config-if)#shutdown
```

Étape 3 : enregistrement des résultats de débogage à partir de Comm2 et Comm3

```
Comm2#
1w2d: STP: VLAN0001 we are the spanning tree root
Comm2#
1w2d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
1w2d: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
Comm2#
1w2d: STP: VLAN0001 heard root 32769-0019.068d.6980 on Fa0/2
1w2d:      supersedes 32769-001b.0c68.2080
1w2d: STP: VLAN0001 new root is 32769, 0019.068d.6980 on port Fa0/2, cost 38
1w2d: STP: VLAN0001 sent Topology Change Notice on Fa0/2

Comm3#
1w2d: STP: VLAN0001 heard root 32769-001b.0c68.2080 on Fa0/2
1w2d: STP: VLAN0001 Fa0/2 -> listening
Comm3#
1w2d: STP: VLAN0001 Topology Change rcvd on Fa0/2
1w2d: STP: VLAN0001 sent Topology Change Notice on Fa0/1
Comm3#
1w2d: STP: VLAN0001 Fa0/2 -> learning
Comm3#
1w2d: STP: VLAN0001 sent Topology Change Notice on Fa0/1
1w2d: STP: VLAN0001 Fa0/2 -> forwarding
```

Lorsque la liaison de Comm2 connecté au commutateur racine est désactivée, quelle est la conclusion initiale à propos de la racine Spanning Tree ?_____

Dès que Comm2 reçoit de nouvelles informations sur Fa0/2, quelle nouvelle conclusion tire-t-il ?_____

Le port Fa0/2 sur Comm3 était à l'état de blocage avant que la liaison entre Comm2 et Comm1 ne soit désactivée. Quels sont ses états après une modification topologique ?

_____

Étape 4 : examen des modifications apportées à la topologie Spanning Tree via la commande `show spanning-tree`

```
Comm2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
```

```
  Root ID    Priority    32769
             Address     0019.068d.6980
             Cost        38
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     001b.0c68.2080
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/11            Desg FWD 19        128.11    P2p
Fa0/18            Desg FWD 19        128.18    P2p


Comm3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0019.068d.6980
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     001b.5303.1700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

Répondez aux questions suivantes à partir des résultats.

1. Quelles sont les modifications apportées au transfert du trafic via Comm2 ? _____
2. Quelles sont les modifications apportées au transfert du trafic via Comm3 ?_____

Tâche 6 : via la commande show run, enregistrement de la configuration de chaque commutateur

```
Comm1#show run
!<résultat omis>
!
hostname Comm1
!
!
interface FastEthernet0/1
```

```
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode access
!
! <output omitted>
!
interface Vlan1
 ip address 172.17.10.1 255.255.255.0
!
end
```

```
Comm2#show run
!<résultat omis>
!
hostname Comm2
!
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
! <résultat omis>
!
interface FastEthernet0/6
 switchport mode access
!
interface FastEthernet0/11
 switchport mode access
!
interface FastEthernet0/18
 switchport mode access
!
!
interface Vlan1
 ip address 172.17.10.2 255.255.255.0
!
end
```

```
Comm3#show run
!<résultat omis>
!
hostname Comm3
!
!
interface FastEthernet0/1
 switchport mode trunk
!
```

```
interface FastEthernet0/2
 switchport mode trunk
!
!
! <résultat omis>
!
interface Vlan1
 ip address 172.17.10.3 255.255.255.0
!
end
```

Tâche 7 : remise en état

Supprimez les configurations et rechargez les configurations par défaut pour les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 5.5.2 : protocole STP - Travaux pratiques avancés

Diagramme de topologie

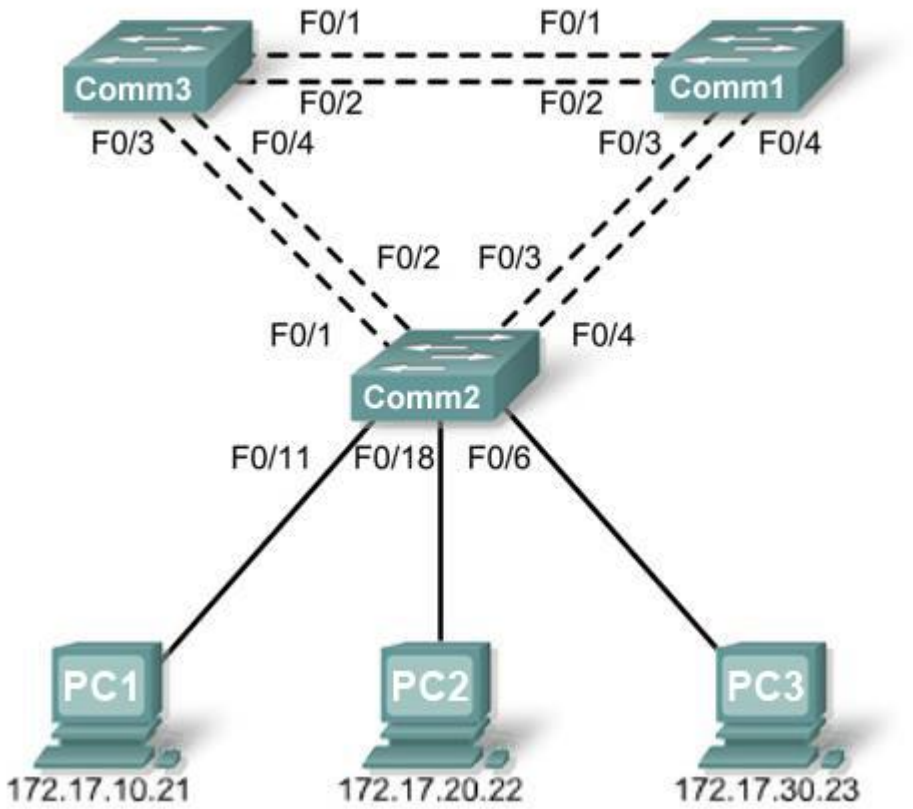


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 99**	172.17.99.11	255.255.255.0	N/D
Comm2	**VLAN 99**	172.17.99.12	255.255.255.0	N/D
Comm3	**VLAN 99**	172.17.99.13	255.255.255.0	N/D
PC1	**Carte réseau**	172.17.10.21	255.255.255.0	172.17.10.12
PC2	**Carte réseau**	172.17.20.22	255.255.255.0	172.17.20.12
PC3	**Carte réseau**	172.17.30.23	255.255.255.0	172.17.30.12

Affectations des ports – Commutateur 2

Ports	Affectation	Réseau
Fa0/1 – 0/4	Agrégations 802.1q (VLAN 99 natif)	172.17.99.0 /24
Fa0/5 – 0/10	VLAN 30 – Invité (par défaut)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculté/Personnel	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Participants	172.17.20.0 /24

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Supprimer la configuration initiale et recharger la configuration par défaut, pour revenir aux paramètres par défaut pour un commutateur
- Exécuter des tâches de configuration de base sur un commutateur
- Configurer le protocole VTP (VLAN Trunking Protocol) sur tous les commutateurs
- Observer et expliquer le comportement par défaut du protocole Spanning Tree (STP, 802.1D)
- Modifier l'emplacement de la racine Spanning Tree
- Observer la réponse à une modification de la topologie Spanning Tree
- Expliquer les limites du protocole STP 802.1D dans la prise en charge de la continuité du service
- Configurer le protocole STP rapide (802.1W)
- Observer et expliquer les améliorations offertes par le protocole STP rapide

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Vous pouvez utiliser n'importe quel commutateur durant les travaux pratiques, pourvu qu'il soit équipé des interfaces indiquées dans le diagramme de topologie. Les résultats présentés dans ces travaux pratiques proviennent des commutateurs Cisco 2960. Les autres modèles de commutateur peuvent produire des résultats différents.

Configurez les connexions console pour les trois commutateurs.

Étape 2 : suppression des configurations actuelles des commutateurs

Videz la mémoire vive non volatile, supprimez le fichier vlan.dat et rechargez les commutateurs. Reportez-vous aux Travaux pratiques 2.5.1 pour consulter la procédure. Une fois le rechargement fini, utilisez la commande du mode d'exécution privilégié **show vlan** pour confirmer que seuls les réseaux locaux virtuels par défaut existent et que tous les ports sont affectés au VLAN 1.

```
Comm1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
```

```
                                                Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                Gig1/1, Gig1/2
1002 fddi-default                   active
1003 token-ring-default             active
1004 fddinet-default                active
1005 trnet-default                  active
```

Étape 3 : désactivation de tous les ports à l'aide de la commande shutdown

Vérifiez que l'état initial des ports de commutateur est inactif via la commande **shutdown**. Utilisez la commande **interface-range** pour simplifier cette tâche.

```
Comm1(config)#interface range fa0/1-24
Comm1(config-if-range)#shutdown
Comm1(config-if-range)#interface range gi0/1-2
Comm1(config-if-range)#shutdown

Comm2(config)#interface range fa0/1-24
Comm2(config-if-range)#shutdown
Comm2(config-if-range)#interface range gi0/1-2
Comm2(config-if-range)#shutdown

Comm3(config)#interface range fa0/1-24
Comm3(config-if-range)#shutdown
Comm3(config-if-range)#interface range gi0/1-2
Comm3(config-if-range)#shutdown
```

Étape 4 : réactivation des ports utilisateur sur Comm2 en mode access

Reportez-vous au diagramme de topologie pour déterminer les ports de commutateur activés sur Comm2 pour l'accès des périphériques des utilisateurs finaux. Ces trois ports seront configurés en mode access et activés via la commande **no shutdown**.

```
Comm2(config)#interface range fa0/6, fa0/11, fa0/18
Comm2(config-if-range)#switchport mode access
Comm2(config-if-range)#no shutdown
```

Tâche 2 : configuration de base des commutateurs

Configurez les commutateurs Comm1, Comm2 et Comm3 en fonction des instructions suivantes :

- Configurez le nom d'hôte du commutateur.
- Désactivez la recherche DNS.
- Configurez le mot de passe **class** pour le mode d'exécution.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.

(Résultats pour Comm1)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Switch(config)#hostname Comm1
Comm1(config)#enable secret class
Comm1(config)#no ip domain-lookup
Comm1(config)#line console 0
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#line vty 0 15
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
Comm1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Tâche 3 : configuration des ordinateurs hôtes

Configurez les interfaces Ethernet de PC1, PC2 et PC3 avec l'adresse IP, le masque de sous-réseau et la passerelle indiqués dans le tableau d'adressage au début des travaux pratiques.

Tâche 4 : configuration des réseaux locaux virtuels

Étape 1 : configuration du protocole VTP

Configurez le protocole VTP sur les trois commutateurs à l'aide du tableau suivant. N'oubliez pas que les mots de passe et les noms de domaine VTP tiennent compte des majuscules. Le mode de fonctionnement par défaut est Serveur.

Nom du commutateur	Mode de fonctionnement VTP	Domaine VTP	Mot de passe VTP
Comm1	**Serveur**	**Lab5**	**cisco**
Comm2	**Client**	**Lab5**	**cisco**
Comm3	**Client**	**Lab5**	**cisco**

```
Comm1(config)#vtp mode server
Le périphérique est déjà en mode SERVEUR VTP.
Comm1(config)#vtp domain Lab5
Remplacement du nom de domaine VTP NULL par Lab5
Comm1(config)#vtp password cisco
Définition du mot de passe cisco de la base de données du réseau local
virtuel du périphérique
Comm1(config)#end

Comm2(config)#vtp mode client
Définition du périphérique en mode CLIENT VTP
Comm2(config)#vtp domain Lab5
Remplacement du nom de domaine VTP NULL par Lab5
Comm2(config)#vtp password cisco
Définition du mot de passe cisco de la base de données du réseau local
```

```
virtuel du périphérique
Comm2(config)#end

Comm3(config)#vtp mode client
Définition du périphérique en mode CLIENT VTP
Comm3(config)#vtp domain Lab5
Remplacement du nom de domaine VTP NULL par Lab5
Comm3(config)#vtp password cisco
Définition du mot de passe cisco de la base de données du réseau local
virtuel du périphérique
Comm3(config)#end
```

Étape 2 : configuration des liens agrégés et du réseau local virtuel natif

Configurez les ports agrégés et le réseau local virtuel natif. Pour chaque commutateur, configurez les ports Fa0/1 à Fa0/4 en tant que ports agrégés. Désignez le VLAN 99 en tant que réseau local virtuel natif pour ces agrégations. Utilisez la commande **interface range** en mode de configuration globale pour simplifier cette tâche. N'oubliez pas que ces ports ont été désactivés lors d'une étape précédente et qu'ils doivent être réactivés via la commande **no shutdown**.

```
Comm1(config)#interface range fa0/1-4
Comm1(config-if-range)#switchport mode trunk
Comm1(config-if-range)#switchport trunk native vlan 99
Comm1(config-if-range)#no shutdown
Comm1(config-if-range)#end

Comm2(config)# interface range fa0/1-4
Comm2(config-if-range)#switchport mode trunk
Comm2(config-if-range)#switchport trunk native vlan 99
Comm2(config-if-range)#no shutdown
Comm2(config-if-range)#end

Comm3(config)# interface range fa0/1-4
Comm3(config-if-range)#switchport mode trunk
Comm3(config-if-range)#switchport trunk native vlan 99
Comm3(config-if-range)#no shutdown
Comm3(config-if-range)#end
```

Étape 3 : configuration du serveur VTP avec les réseaux locaux virtuels

Le protocole VTP permet de configurer des réseaux locaux virtuels sur le serveur VTP et de leur attribuer les clients VTP du domaine. Cela permet de garantir la cohérence de la configuration VLAN sur le réseau.

Configurez les réseaux locaux virtuels suivants sur le serveur VTP :

VLAN	Nom VLAN
VLAN 99	**direction**
VLAN 10	**faculté-personnel**
VLAN 20	**participants**
VLAN 30	**invité**

```
Comm1(config)#vlan 99
Comm1(config-vlan)#name direction
Comm1(config-vlan)#exit
Comm1(config)#vlan 10
Comm1(config-vlan)#name faculté-personnel
Comm1(config-vlan)#exit
Comm1(config)#vlan 20
Comm1(config-vlan)#name participants
Comm1(config-vlan)#exit
Comm1(config)#vlan 30
Comm1(config-vlan)#name invité
Comm1(config-vlan)#exit
```

Étape 4 : vérification des réseaux locaux virtuels

Exécutez la commande **show vlan brief** sur Comm2 et Comm3 pour vérifier que les quatre réseaux locaux virtuels ont été répartis sur les commutateurs client.

```
Comm2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,
Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,
Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
10   faculté/personnel                 active
20   participants                      active
30   invité                            active
99   direction                         active

Comm3#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,
Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,
Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
10   faculté/personnel                 active
20   participants                      active
30   invité                            active
99   direction                         active
```

Étape 5 : configuration de l'adresse de l'interface de gestion sur les trois commutateurs

```
Comm1(config)#interface vlan99
Comm1(config-if)#ip address 172.17.99.11 255.255.255.0
Comm1(config-if)#no shutdown

Comm2(config)#interface vlan99
Comm2(config-if)#ip address 172.17.99.12 255.255.255.0
Comm2(config-if)#no shutdown

Comm3(config)#interface vlan99
Comm3(config-if)#ip address 172.17.99.13 255.255.255.0
Comm3(config-if)#no shutdown
```

Vérifiez que les commutateurs sont configurés correctement en envoyant des requêtes ping entre eux. À partir de Comm1, envoyez une requête ping à l'interface de gestion sur Comm2 et Comm3. À partir de Comm2, envoyez une requête ping à l'interface de gestion sur Comm3.

Les requêtes ping ont-elles abouti ? _____

Dans le cas contraire, corrigez les configurations des commutateurs et réessayez.

Étape 6 : attribution des ports de commutateur aux réseaux locaux virtuels

Affectez des ports aux réseaux locaux virtuels sur Comm2. Reportez-vous au tableau d'affectation des ports fourni au début des travaux pratiques.

```
Comm2(config)#interface range fa0/5-10
Comm2(config-if-range)#switchport access vlan 30
Comm2(config-if-range)#interface range fa0/11-17
Comm2(config-if-range)#switchport access vlan 10
Comm2(config-if-range)#interface range fa0/18-24
Comm2(config-if-range)#switchport access vlan 20
Comm2(config-if-range)#end
Comm2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
Comm2#
```

Tâche 5 : configuration du protocole Spanning Tree

Étape 1 : examen de la configuration par défaut du protocole STP 802.1D

Sur chaque commutateur, affichez la table Spanning Tree via la commande **show spanning-tree**. Les résultats sont présentés pour Comm1 uniquement. La sélection racine varie en fonction de l'ID de pont de chaque commutateur des travaux pratiques.

```
Comm1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0019.068d.6980
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0019.068d.6980
```

```
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.4    P2p
Fa0/3            Desg FWD 19        128.5    P2p
Fa0/4            Desg FWD 19        128.6    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0019.068d.6980
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0019.068d.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.4    P2p
Fa0/3            Desg FWD 19        128.5    P2p
Fa0/4            Desg FWD 19        128.6    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     0019.068d.6980
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0019.068d.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.4    P2p
Fa0/3            Desg FWD 19        128.5    P2p
Fa0/4            Desg FWD 19        128.6    P2p

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    32798
             Address     0019.068d.6980
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     0019.068d.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.4    P2p
Fa0/3            Desg FWD 19        128.5    P2p
Fa0/4            Desg FWD 19        128.6    P2p

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0019.068d.6980
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32867  (priority 32768 sys-id-ext 99)
             Address     0019.068d.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.4    P2p
Fa0/3            Desg FWD 19        128.5    P2p
Fa0/4            Desg FWD 19        128.6    P2p
```

Notez que chaque commutateur comporte cinq instances Spanning Tree. La configuration STP par défaut sur les commutateurs Cisco est PVST+ (Per-VLAN Spanning Tree), ce qui crée un Spanning Tree distinct pour chaque réseau local virtuel (pour le VLAN 1 et pour tout réseau local virtuel configuré par l'utilisateur).

Examinez le Spanning Tree du VLAN 99 pour les trois commutateurs :

```
Comm1#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0019.068d.6980
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32867  (priority 32768 sys-id-ext 99)
             Address     0019.068d.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.4    P2p
Fa0/3            Desg FWD 19        128.5    P2p
Fa0/4            Desg FWD 19        128.6    P2p

Comm2#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    32867
              Address     0019.068d.6980   Il s'agit de l'adresse MAC du commutateur racine
(Comm1 dans ce cas)
              Cost        19
              Port        3 (FastEthernet0/3)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     001b.0c68.2080
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p

Comm3#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    32867
              Address     0019.068d.6980  Il s'agit de l'adresse MAC du commutateur racine
(Comm1 dans ce cas)
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     001b.5303.1700
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

Étape 2 : examen des résultats

Répondez aux questions suivantes à partir des résultats.

1. Quelle est la priorité de l'ID de pont pour les commutateurs Comm1, Comm2 et Comm3 sur le VLAN 99 ?
    a. Comm1 _____
    b. Comm2 _____
    c. Comm3 _____
2. Quelle est la priorité de l'ID de pont pour Comm1 sur les VLAN 10, 20, 30 et 99 ?
    a. VLAN 10 _____
    b. VLAN 20_____
    c. VLAN 30_____
    d. VLAN 99_____
3. Quel commutateur représente la racine Spanning Tree du VLAN 99 ? _____
4. Sur le VLAN 99, quels sont les ports Spanning Tree à l'état de blocage sur le commutateur racine ? _____
5. Sur le VLAN 99, quels sont les ports Spanning Tree à l'état de blocage sur les commutateurs non-racine ? _____
6. Comment le commutateur racine est-il choisi via STP ? _____
7. Étant donné que les priorités de pont sont toutes identiques, quel autre élément le commutateur utilise-t-il pour déterminer la racine ? _____

Tâche 6 : optimisation du protocole STP

Étant donné qu'il existe une instance distincte du Spanning Tree pour chaque réseau local virtuel actif, une sélection racine distincte est réalisée pour chaque instance. Si les priorités de commutateur par défaut sont utilisées dans la sélection racine, la même racine est sélectionnée pour chaque Spanning Tree, comme nous l'avons déjà constaté. Cela peut diminuer les performances de la conception. Voici les principales raisons de contrôler la sélection du commutateur racine :

- Le commutateur racine est responsable de la génération des unités BPDU dans STP 802.1D et correspond au point central pour le trafic de contrôle du Spanning Tree. Le commutateur racine doit être capable de gérer cette charge de traitement supplémentaire.
- L'emplacement de la racine définit les chemins commutés actifs du réseau. Un emplacement aléatoire peut mener vers des chemins inefficaces. La racine se trouve idéalement sur la couche de distribution.
- Examinez la topologie utilisée dans ces travaux pratiques. Sur les six agrégations configurées, seules deux acheminent le trafic. Même si cette configuration évite les boucles, elle entraîne une perte de ressources. Étant donné que la racine peut être définie sur la base du réseau local virtuel, certains ports peuvent bloquer un réseau local virtuel tout en assurant la transmission pour un autre. Cette configuration est illustrée ci-dessous.

Dans cet exemple, la sélection racine utilisant les valeurs par défaut a entraîné une sous-utilisation des agrégations de commutateur disponibles. Par conséquent, il est nécessaire de forcer un autre commutateur à devenir le commutateur racine pour le VLAN 99, pour imposer le partage des charges entre les agrégations.

La sélection du commutateur racine est réalisée en modifiant la priorité Spanning Tree pour le réseau local virtuel. Comme le commutateur racine par défaut peut varier dans votre environnement de travaux pratiques, nous configurerons Comm1 et Comm3 en tant que commutateurs racine pour les réseaux locaux virtuels spécifiques. La priorité par défaut, comme vous avez pu le constater, est 32768 plus l'ID de VLAN. Le nombre le plus faible indique une priorité plus élevée pour la sélection racine. Affectez la valeur 4096 au VLAN 99 sur Comm3.

```
Comm3(config)#spanning-tree vlan 99 ?
  forward-time  Définit le délai de transmission du Spanning Tree
  hello-time    Définit l'intervalle Hello du Spanning Tree
  max-age       Définit l'âge maximum du Spanning Tree
  priority      Définit la priorité de pont du Spanning Tree
  root          Configure le commutateur en tant que racine
  <cr>

Comm3(config)#spanning-tree vlan 99 priority ?
  <0-61440>  Priorité de pont en incréments de 4096

Comm3(config)#spanning-tree vlan 99 priority 4096
Comm3(config)#exit
```

Affectez la valeur 4096 pour la priorité des VLAN 1, 10, 20 et 30 sur Comm1. Là encore, le nombre le plus faible indique une priorité plus élevée pour la sélection racine.

```
Comm1(config)#spanning-tree vlan 1 priority 4096
Comm1(config)#spanning-tree vlan 10 priority 4096
Comm1(config)#spanning-tree vlan 20 priority 4096
Comm1(config)#spanning-tree vlan 30 priority 4096
Comm1(config)#exit
```

Faites en sorte que les commutateurs aient un peu de temps pour recalculer le Spanning Tree, puis vérifiez l'arborescence du VLAN 99 sur le commutateur Comm1 et le commutateur Comm3.

```
Comm1#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    4195
              Address     001b.5303.1700   Il s'agit désormais de l'adresse MAC de Comm3
(le nouveau commutateur racine)
              Cost        19
              Port        3 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32867  (priority 32768 sys-id-ext 99)
              Address     0019.068d.6980
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.3    P2p
Fa0/2            Altn BLK 19        128.4    P2p
Fa0/3            Desg FWD 19        128.5    P2p
Fa0/4            Desg FWD 19        128.6    P2p
```

```
Comm3#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    4195
              Address     001b.5303.1700
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4195   (priority 4096 sys-id-ext 99)
              Address     001b.5303.1700
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
```

Quel commutateur correspond à la racine du VLAN 99 ? _____

Sur le VLAN 99, quels sont les ports Spanning Tree à l'état de blocage sur le nouveau commutateur racine ? _____

Sur le VLAN 99, quels sont les ports Spanning Tree à l'état de blocage sur l'ancien commutateur racine ? _____

Comparez le Spanning Tree du VLAN 99 sur Comm3 ci-dessus à celui du VLAN 10 sur Comm3.

```
Comm3#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     0019.068d.6980
              Cost        19
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778   (priority 32768 sys-id-ext 10)
              Address     001b.5303.1700
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

Notez que Comm3 peut désormais utiliser les quatre ports pour le trafic du VLAN 99 s'ils ne sont pas bloqués à l'autre extrémité de l'agrégation. Cependant, la topologie Spanning Tree d'origine, avec trois des quatre ports Comm3 en mode blocage, est toujours en place pour les quatre autres réseaux locaux virtuels actifs. En configurant les groupes de réseaux locaux virtuels pour utiliser différentes agrégations comme leur chemin de transmission principal, la redondance des agrégations de basculement est conservée, sans avoir à laisser les agrégations totalement inutilisées.

Tâche 7 : observation de la réponse à une modification de la topologie STP 802.1D

Pour observer une continuité sur le réseau local lors d'une modification de la topologie, commencez par reconfigurer PC3, qui est connecté au port Fa0/6 de Comm2, avec l'adresse IP 172.17.99.23 255.255.255.0. Réaffectez ensuite le port Fa0/6 de Comm2 au VLAN 99. Cela vous permet d'envoyer des requêtes ping continues sur le réseau local à partir de l'hôte.

```
Comm2(config)# interface fa0/6
Comm2(config-if)#switchport access vlan 99
```

Vérifiez que les commutateurs peuvent envoyer des requêtes ping à l'hôte.

```
Comm2#ping 172.17.99.23
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.17.99.23, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1007 ms

Comm1#ping 172.17.99.23

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.23, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1007 ms
```

Placez Comm1 en mode de débogage des événements Spanning Tree pour contrôler les modifications lors du changement topologique.

```
Comm1#debug spanning-tree events
Le débogage des événements Spanning Tree est activé
```

Ouvrez une fenêtre de commande sur PC3 et envoyez une requête ping continue à l'interface de gestion Comm1 avec la commande **ping –t 172.17.99.11**. Déconnectez les agrégations sur Fa0/1 et Fa0/3 de Comm1. Contrôlez les requêtes ping. Ces dernières dépasseront le délai d'attente lorsque la connectivité sur le réseau local sera interrompue. Dès que la connectivité est rétablie, mettez fin aux requêtes ping en appuyant sur Ctrl+C.

Une version raccourcie des résultats de débogage sur Comm1 est présentée ci-dessous (plusieurs lignes ont été omises par souci de concision).

```
Comm1#debug spanning-tree events
Le débogage des événements Spanning Tree est activé
Comm1#
6d08h: STP: VLAN0099 new root port Fa0/2, cost 19
6d08h: STP: VLAN0099 Fa0/2 -> listening
6d08h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
6d08h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
6d08h: STP: VLAN0099 sent Topology Change Notice on Fa0/2
6d08h: STP: VLAN0030 Topology Change rcvd on Fa0/2
6d08h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down
```

```
6d08h: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
6d08h: STP: VLAN0001 Topology Change rcvd on Fa0/4
6d08h: STP: VLAN0099 Fa0/2 -> learning
6d08h: STP: VLAN0099 sent Topology Change Notice on Fa0/2
6d08h: STP: VLAN0099 Fa0/2 -> forwarding
6d08h: STP: VLAN0001 Topology Change rcvd on Fa0/4
```

N'oubliez pas que lorsque les ports sont en mode écoute et apprentissage, ils ne transmettent pas les trames et le réseau local est essentiellement désactivé. Le recalcul du Spanning Tree peut durer jusqu'à 50 secondes, ce qui représente une interruption significative des services réseau. Les résultats des requêtes ping continues indiquent la durée d'interruption réelle. Dans ce cas, elle était de 30 secondes environ. Tandis que le protocole STP 802.1D empêche la formation de boucles de commutation, cette longue durée de restauration est considérée comme un inconvénient majeur entravant la disponibilité des réseaux locaux actuels.

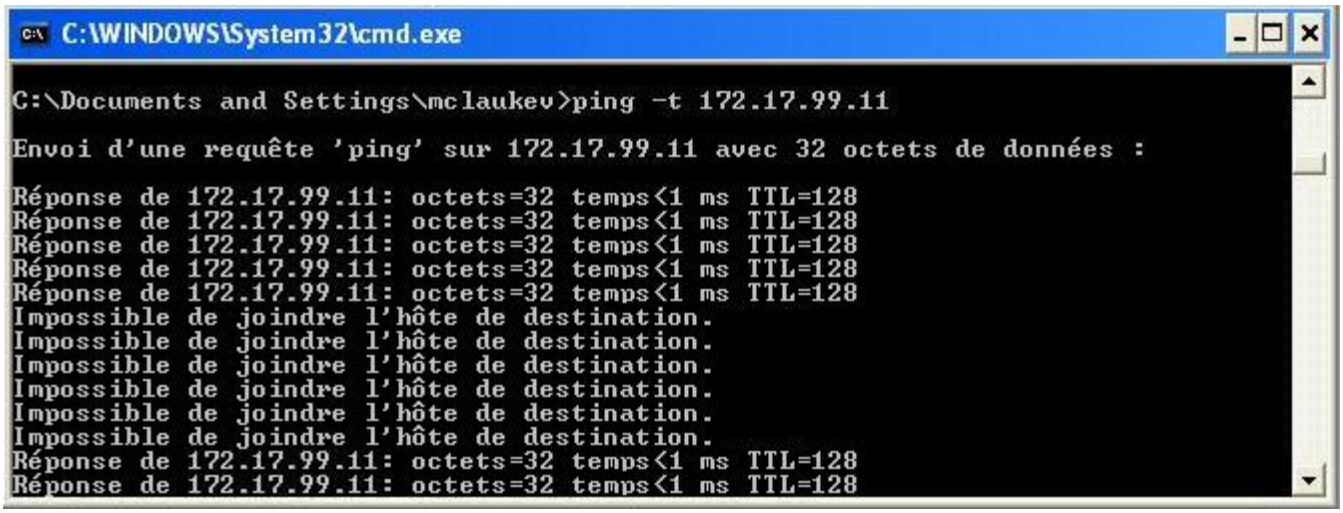


Figure 1. Ces requêtes ping connaissent un délai de connectivité de 30 secondes lors du recalcul du Spanning Tree.

Tâche 8 : configuration du protocole Spanning Tree rapide PVST

Cisco a développé plusieurs fonctionnalités pour résoudre les délais de convergence lente associés au protocole STP standard. PortFast, UplinkFast et BackboneFast sont des fonctionnalités qui, lorsqu'elles sont configurées correctement, peuvent réduire considérablement le délai requis pour restaurer la connectivité. L'intégration de ces fonctionnalités requiert une configuration manuelle, qui doit être réalisée avec soin. La solution sur le long terme est STP rapide (RSTP), 802.1w, qui intègre ces fonctionnalités parmi d'autres. RSTP-PVST est configuré comme suit :

```
Comm1(config)#spanning-tree mode rapid-pvst
```

Configurez les trois commutateurs de cette manière.

Exécutez la commande **show spanning-tree summary** pour vérifier que RSTP est activé.

Tâche 9 : observation du délai de convergence de RSTP

Commencez par restaurer les agrégations que vous avez déconnectées dans la Tâche 7, si ce n'est déjà fait (ports Fa0/1 et Fa0/3 sur Comm1). Suivez ensuite les étapes de la Tâche 7 :

- Définissez le PC3 hôte pour envoyer des requêtes ping continues sur le réseau.
- Activez le débogage des événements Spanning Tree sur le commutateur Comm1.
- Déconnectez les câbles connectés aux ports Fa0/1 et Fa0/3.
- Observez le délai nécessaire au rétablissement d'un Spanning Tree stable.

Voici les résultats partiels du débogage :

```
Comm1#debug spanning-tree events
Le débogage des événements Spanning Tree est activé
Comm1#
6d10h: RSTP(99): updt rolesroot port Fa0/3 is going down
6d10h: RSTP(99): Fa0/2 is now root port
```

La connectivité a été restaurée ; l'interruption a duré moins d'une seconde

```
6d10h: RSTP(99): syncing port Fa0/1
6d10h: RSTP(99): syncing port Fa0/4
6d10h: RSTP(99): transmitting a proposal on Fa0/1
6d10h: RSTP(99): transmitting a proposal on Fa0/4
6d10h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down
6d10h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
```

Le délai de restauration avec RSTP activé a été inférieur à une seconde et aucune requête ping n'a été abandonnée.

Tâche 10 : remise en état

Supprimez les configurations et rechargez les configurations par défaut pour les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Configurations finales

Commutateur Comm1

```
hostname Comm1
!
enable secret class
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 4096
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 4096
spanning-tree vlan 30 priority 4096
!
interface FastEthernet0/1
```

```
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
(configuration des autres ports omise- tous les ports non utilisés sont à
l'arrêt)
!
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no ip route-cache
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Commutateur Comm2

```
hostname Comm2
!
enable secret class
!
```

```
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 30
!
interface FastEthernet0/6
 switchport access vlan 30
!
interface FastEthernet0/7
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 30
!
interface FastEthernet0/11
 switchport access vlan 10
!
interface FastEthernet0/12
 switchport access vlan 10
!
interface FastEthernet0/13
 switchport access vlan 10
!
interface FastEthernet0/14
 switchport access vlan 10
!
interface FastEthernet0/15
 switchport access vlan 10
!
interface FastEthernet0/16
 switchport access vlan 10
!
interface FastEthernet0/17
```

```
 switchport access vlan 10
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
!
interface FastEthernet0/20
switchport access vlan 20
!
interface FastEthernet0/21
 switchport access vlan 20
!
interface FastEthernet0/22
 switchport access vlan 20
!
interface FastEthernet0/23
 switchport access vlan 20
!
interface FastEthernet0/24
 switchport access vlan 20
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no ip route-cache
!
line con 0
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Commutateur Comm3

```
hostname Comm3
!
enable secret class
!
no ip domain-lookup
!
```

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 99 priority 4096
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
(configuration des autres ports omise- tous les ports non utilisés sont à
l'arrêt)
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no ip route-cache
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Travaux pratiques 5.5.3 : dépannage du protocole STP

Diagramme de topologie

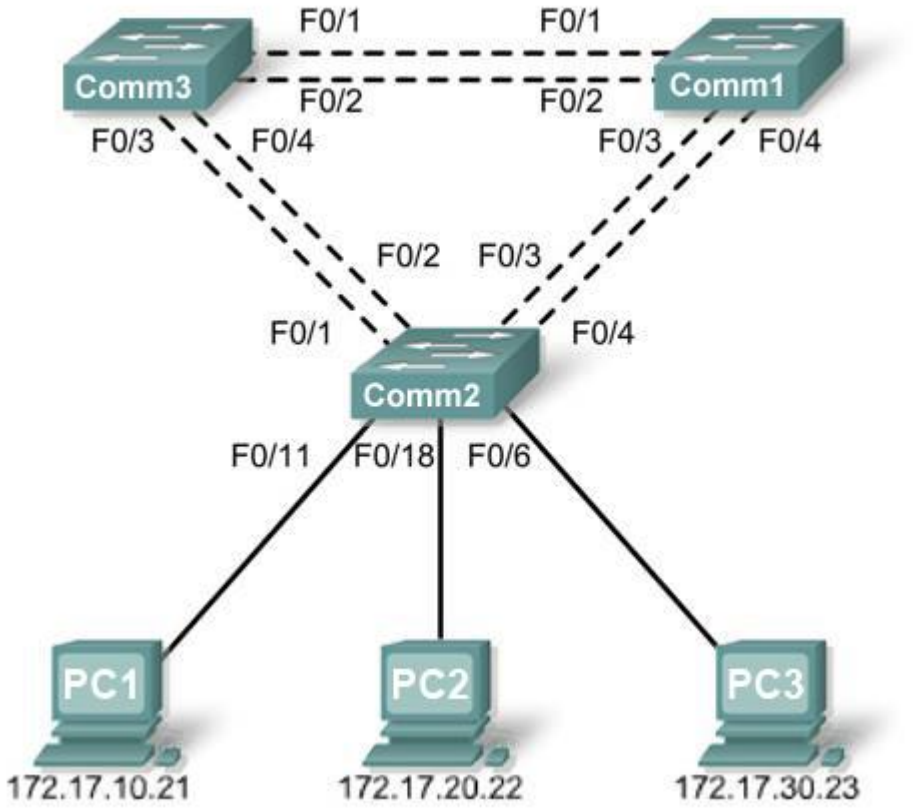


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 99**	172.17.99.11	255.255.255.0	N/D
Comm2	**VLAN 99**	172.17.99.12	255.255.255.0	N/D
Comm3	**VLAN 99**	172.17.99.13	255.255.255.0	N/D
PC1	**Carte réseau**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**Carte réseau**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**Carte réseau**	172.17.30.23	255.255.255.0	172.17.30.1

Affectations des ports – Commutateur 2

Ports	Affectation	Réseau
Fa0/1 – 0/4	Agrégations 802.1q (VLAN 99 natif)	172.17.99.0 /24
Fa0/5 – 0/10	VLAN 30 – Invité (par défaut)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculté/Personnel	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Participants	172.17.20.0 /24

Objectifs pédagogiques

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

- Analyser un problème de congestion sur un réseau local commuté redondant
- Reconnaître les fonctionnalités pour l'équilibrage de charge par réseau local virtuel avec PVST
- Modifier la configuration STP par défaut pour optimiser la bande passante disponible
- Vérifier que l'objectif des modifications a été atteint

Scénario

Vous êtes responsable du fonctionnement du réseau local commuté redondant illustré dans le diagramme de topologie. Vous et les utilisateurs avez observé une latence accrue pendant les heures de pointe et votre analyse montre que des agrégations sont encombrées. Sur les six agrégations configurées, seules trois acheminent des paquets dans la configuration STP par défaut en cours d'exécution. Pour résoudre ce problème, les agrégations disponibles doivent être utilisées de manière plus efficace. La fonctionnalité PVST+ des commutateurs Cisco fournit la flexibilité requise pour répartir le trafic entre commutateurs à l'aide des six agrégations.

Ces travaux pratiques sont terminés lorsque toutes les agrégations filaires acheminent le trafic et que les trois commutateurs participent à l'équilibrage de charge par réseau local virtuel pour les trois réseaux locaux virtuels des utilisateurs.

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Vous pouvez utiliser n'importe quel commutateur durant les travaux pratiques, pourvu qu'il soit équipé des interfaces indiquées dans le diagramme de topologie. Les résultats présentés dans ces travaux pratiques proviennent des commutateurs Cisco 2960. Les autres modèles de commutateur peuvent produire des résultats différents.

Configurez les connexions console pour les trois commutateurs.

Étape 2 : suppression des configurations actuelles des commutateurs

Videz la mémoire vive non volatile, supprimez le fichier vlan.dat et rechargez les commutateurs.

Étape 3 : chargement des commutateurs avec le script suivant :

Configuration de Comm1

```
hostname Comm1
enable secret class
no ip domain-lookup
!
vtp mode server
vtp domain Lab5
vtp password cisco
!
vlan 99
name Direction
exit
!
vlan 10
name Faculté/Personnel
exit
!
vlan 20
name Participants
exit
!
vlan 30
name Invité
exit
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface range FastEthernet0/5-24
shutdown
!
interface GigabitEthernet0/1
shutdown
```

```
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 password cisco
 login
line vty 0
 no login
line vty 1 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Configuration de Comm2

```
hostname Comm2
!
enable secret class
no ip domain-lookup
!
vtp mode client
vtp domain Lab5
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
```

```
interface range FastEthernet0/5- 10
 switchport access vlan 30
 switchport mode access
!
interface range FastEthernet0/11- 17
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/18- 24
 switchport access vlan 20
 switchport mode access
!
interface fa0/6
no shutdown
interface fa0/11
no shutdown
interface fa0/18
no shutdown
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
```

Configuration de Comm3

```
hostname Comm3
!
enable secret class
no ip domain-lookup
!
vtp mode client
vtp domain Lab5
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
```

```
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface range FastEthernet0/5- 10
 switchport access vlan 30
 switchport mode access
!
interface range FastEthernet0/11- 17
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/18- 24
 switchport access vlan 20
 switchport mode access
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end
```

Tâche 2 : configuration des ordinateurs hôtes

Configurez les interfaces Ethernet de PC1, PC2 et PC3 avec l'adresse IP, le masque de sous-réseau et la passerelle indiqués dans le tableau d'adressage.

Tâche 3 : identification de l'état initial de l'ensemble des agrégations

Sur chaque commutateur, affichez la table Spanning Tree via la commande **show spanning-tree**. Notez les ports de transmission sur chaque commutateur et identifiez les agrégations inutilisées dans la configuration par défaut. Vous pouvez utiliser votre topologie réseau pour documenter l'état initial de tous les ports agrégés.

Tâche 4 : modification du Spanning Tree pour réaliser l'équilibrage de charge

Modifiez la configuration Spanning Tree de manière à utiliser les six agrégations. Supposons que les trois réseaux locaux utilisateur (10, 20 et 30) acheminent un trafic égal. La solution idéale doit comprendre un ensemble différent de ports de transmission pour chaque réseau local virtuel utilisateur. Il faut, au minimum, que chacun des trois réseaux locaux virtuels utilisateur présente un commutateur différent en tant que racine du Spanning Tree.

Tâche 5 : enregistrement de la configuration des commutateurs

Lorsque vous avez terminé de configurer la solution, capturez les résultats de la commande **show run** et enregistrez-les dans un fichier texte pour chaque commutateur.

Tâche 6 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 6.4.1 : routage de base entre réseaux locaux virtuels

Diagramme de topologie

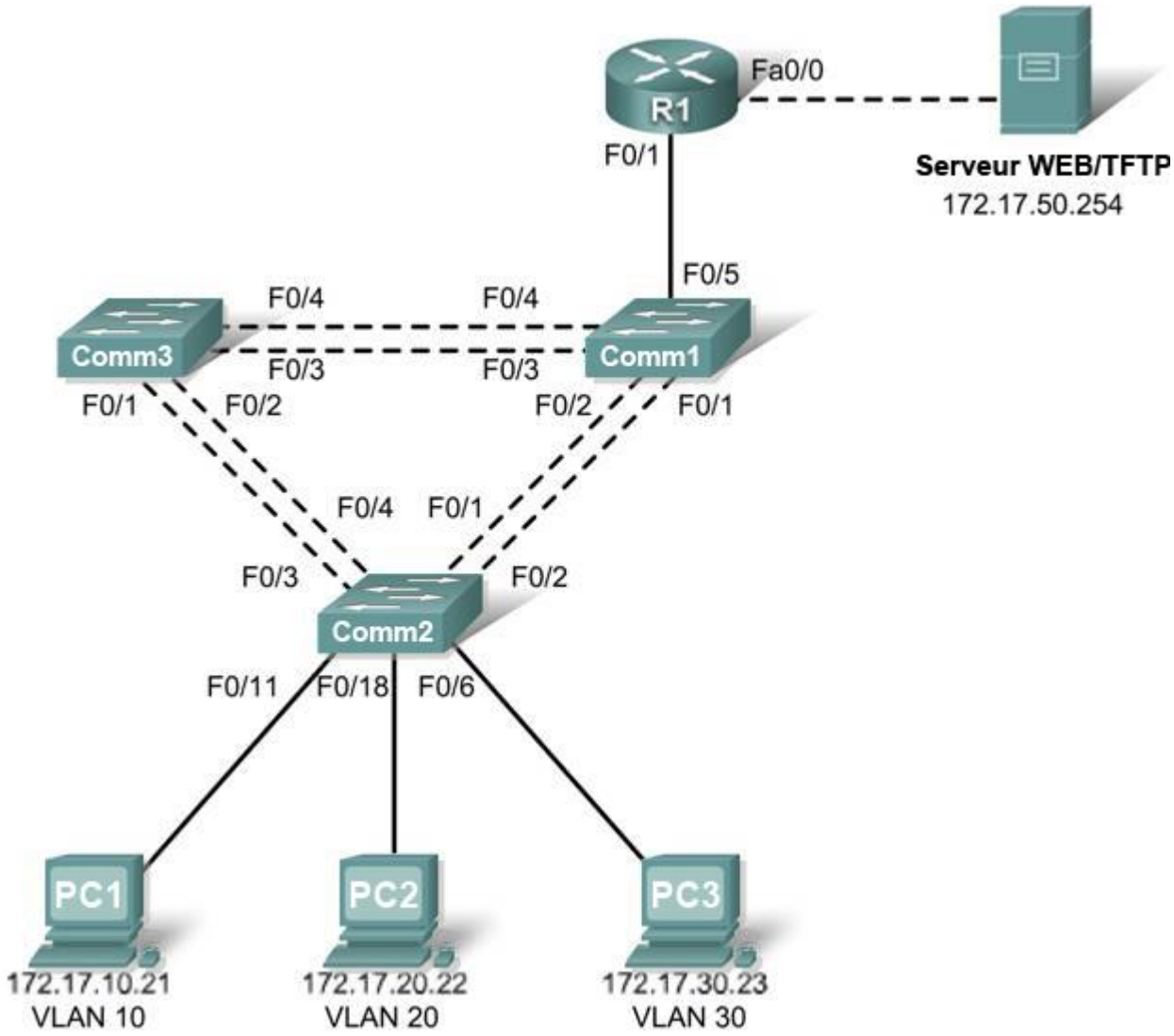


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 99**	172.17.99.11	255.255.255.0	172.17.99.1
Comm2	**VLAN 99**	172.17.99.12	255.255.255.0	172.17.99.1
Comm3	**VLAN 99**	172.17.99.13	255.255.255.0	172.17.99.1

R1	**Fa 0/0**	172.17.50.1	255.255.255.0	N/D
R1	**Fa 0/1**	Voir Tableau de configuration des interfaces		N/D
PC1	**Carte réseau**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**Carte réseau**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**Carte réseau**	172.17.30.23	255.255.255.0	172.17.30.1
Serveur	**Carte réseau**	172.17.50.254	255.255.255.0	172.17.50.1

Affectations des ports – Commutateur 2

Ports	Affectation	Réseau
Fa0/1 – 0/4	Agrégations 802.1q (VLAN 99 natif)	172.17.99.0 /24
Fa0/5 – 0/10	VLAN 30 – Invité (par défaut)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculté/Personnel	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 - Participants	172.17.20.0 /24

Tableau de configuration des interfaces – Routeur 1

Interface	Affectation	Adresse IP
Fa0/1.1	VLAN 1	172.17.1.1 /24
Fa0/1.10	VLAN 10	172.17.10.1 /24
Fa0/1.20	VLAN 20	172.17.20.1 /24
Fa0/1.30	VLAN 30	172.17.30.1 /24
Fa0/1.99	VLAN 99	172.17.99.1 /24

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Réinitialiser les configurations et restaurer un commutateur et un routeur à l'état par défaut
- Exécuter des tâches de configuration de base sur un routeur et un réseau local commuté
- Configurer des VLAN et le protocole VTP (VLAN Trunking Protocol) sur tous les commutateurs
- Montrer et expliquer l'effet des frontières de couche 3 imposées par la création des VLAN
- Configurer un routeur pour prendre en charge les agrégations 802.1q sur une interface Fast Ethernet
- Configurer un routeur avec des sous-interfaces correspondant aux VLAN configurés
- Montrer et expliquer le routage entre réseaux locaux virtuels

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Les résultats présentés dans ces travaux pratiques proviennent de commutateurs 2960 et d'un routeur 1841. Vous pouvez utiliser n'importe quel commutateur ou routeur durant les travaux pratiques, pourvu qu'ils soient équipés des interfaces indiquées dans le diagramme de topologie. Les autres types de périphérique peuvent produire des résultats différents. Notez que les interfaces réseaux Ethernet (10 Mo) sur les routeurs ne prennent pas en charge les agrégations et que les programmes IOS Cisco antérieurs à la version 12.3 ne prennent pas toujours en charge les agrégations sur les interfaces de routeur Fast Ethernet.

Configurez les connexions console pour les trois commutateurs et le routeur.

Étape 2 : suppression des configurations actuelles des commutateurs

Videz la mémoire vive non volatile, supprimez le fichier vlan.dat et rechargez les commutateurs. Reportez-vous aux Travaux pratiques 2.2.1 pour plus d'informations sur la procédure. Une fois le rechargement fini, utilisez la commande **show vlan** pour confirmer que seuls les réseaux locaux virtuels par défaut existent et que tous les ports sont affectés au VLAN 1.

```
Comm1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15,Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19,Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23,Fa0/24
                                                 Gig1/1, Gig1/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Étape 3 : désactivation de tous les ports à l'aide de la commande shutdown

Vérifiez que l'état initial des ports de commutateur est inactif en désactivant tous les ports. Utilisez la commande **interface range** pour simplifier cette tâche.

```
Comm1(config)#interface range fa0/1-24
Comm1(config-if-range)#shutdown
Comm1(config-if-range)#interface range gi0/1-2
Comm1(config-if-range)#shutdown

Comm2(config)#interface range fa0/1-24
Comm2(config-if-range)#shutdown
Comm2(config-if-range)#interface range gi0/1-2
Comm2(config-if-range)#shutdown

Comm3(config)#interface range fa0/1-24
Comm3(config-if-range)#shutdown
Comm3(config-if-range)#interface range gi0/1-2
Comm3(config-if-range)#shutdown
```

Étape 4 : réactivation des ports utilisateur actifs sur Comm2 en mode access

```
Comm2(config)#interface fa0/6
Comm2(config-if)#switchport mode access
Comm2(config-if)#no shutdown
Comm2(config-if)#interface fa0/11
Comm2(config-if)#switchport mode access
Comm2(config-if)#no shutdown
Comm2(config-if)#interface fa0/18
Comm2(config-if)#switchport mode access
Comm2(config-if)#no shutdown
```

Tâche 2 : configuration de base des commutateurs

Configurez les commutateurs Comm1, Comm2 et Comm3 en fonction du tableau d'adressage et des instructions suivantes :

- Configurez le nom d'hôte du commutateur.
- Désactivez la recherche DNS.
- Définissez **class** comme mot de passe secret actif.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.
- Configurez la passerelle par défaut sur chaque commutateur.

Résultats pour Comm1

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Comm1
Comm1(config)#enable secret class
Comm1(config)#no ip domain-lookup
Comm1(config)#ip default-gateway 172.17.99.1
Comm1(config)#line console 0
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#line vty 0 15
Comm1(config-line)#password cisco
Comm1(config-line)#login
Comm1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
Comm1#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
```

Tâche 3 : configuration des interfaces Ethernet sur les ordinateurs hôtes

Configurez les interfaces Ethernet de PC1, PC2, PC3 et le serveur TFTP/Web distant avec les adresses IP issues du tableau d'adressage.

Tâche 4 : configuration du protocole VTP sur les commutateurs

Étape 1 : configuration du protocole VTP sur les trois commutateurs à l'aide du tableau suivant (n'oubliez pas que les mots de passe et les noms de domaine VTP tiennent compte des majuscules)

Nom du commutateur	Mode de fonctionnement VTP	Domaine VTP	Mot de passe VTP
Comm1	**Serveur**	**Lab6**	**cisco**
Comm2	**Client**	**Lab6**	**cisco**
Comm3	**Client**	**Lab6**	**cisco**

Comm1 :

```
Comm1(config)#vtp mode server
Le périphérique est déjà en mode SERVEUR VTP.
Comm1(config)#vtp domain Lab6
Remplacement du nom de domaine VTP NULL par Lab6
Comm1(config)#vtp password cisco
Définition du mot de passe cisco de la base de données du réseau local
virtuel du périphérique
Comm1(config)#end
```

Comm2 :

```
Comm2(config)#vtp mode client
Définition du périphérique en mode CLIENT VTP
Comm2(config)#vtp domain Lab6
Remplacement du nom de domaine VTP NULL par Lab6
Comm2(config)#vtp password cisco
Définition du mot de passe cisco de la base de données du réseau local
virtuel du périphérique
Comm2(config)#end
```

Comm3 :

```
Comm3(config)#vtp mode client
Définition du périphérique en mode CLIENT VTP
Comm3(config)#vtp domain Lab6
Remplacement du nom de domaine VTP NULL par Lab6
Comm3(config)#vtp password cisco
Définition du mot de passe cisco de la base de données du réseau local
virtuel du périphérique
Comm3(config)#end
```

Étape 2 : configuration des ports d'agrégation et désignation du réseau local virtuel natif pour les agrégations

Configurez les ports Fa0/1 à Fa0/5 comme ports d'agrégation et désignez VLAN 99 comme réseau local virtuel natif pour ces agrégations. Utilisez la commande **interface range** en mode de configuration globale pour simplifier cette tâche.

```
Comm1(config)#interface range fa0/1-4
Comm1(config-if-range)#switchport mode trunk
Comm1(config-if-range)#switchport trunk native vlan 99
Comm1(config-if-range)#no shutdown
Comm1(config-if-range)#end

Comm2(config)# interface range fa0/1-4
Comm2(config-if-range)#switchport mode trunk
Comm2(config-if-range)#switchport trunk native vlan 99
Comm2(config-if-range)#no shutdown
Comm2(config-if-range)#end

Comm3(config)# interface range fa0/1-4
Comm3(config-if-range)#switchport mode trunk
Comm3(config-if-range)#switchport trunk native vlan 99
Comm3(config-if-range)#no shutdown
Comm3(config-if-range)#end
```

Étape 3 : configuration des réseaux locaux virtuels sur le serveur VTP

Configurez les réseaux locaux virtuels suivants sur le serveur VTP :

VLAN	Nom VLAN
VLAN 99	**direction**
VLAN 10	**faculté-personnel**
VLAN 20	**participants**
VLAN 30	**invité**

```
Comm1(config)#vlan 99
Comm1(config-vlan)#name direction
Comm1(config-vlan)#exit
Comm1(config)#vlan 10
Comm1(config-vlan)#name faculté-personnel
Comm1(config-vlan)#exit
Comm1(config)#vlan 20
Comm1(config-vlan)#name participants
Comm1(config-vlan)#exit
Comm1(config)#vlan 30
Comm1(config-vlan)#name invité
Comm1(config-vlan)#exit
```

Vérifiez que les réseaux locaux virtuels ont été créés sur Comm1 via la commande **show vlan brief**.

Étape 4 : vérification de la distribution sur Comm2 et Comm3 des réseaux locaux virtuels créés sur Comm1

Exécutez la commande **show vlan brief** sur Comm2 et Comm3 pour vérifier que les quatre réseaux locaux virtuels ont été répartis sur les commutateurs clients.

```
Comm2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                 Gi0/2
10   faculté/personnel                 active
20   participants                      active
30   invité                            active
99   direction                         active
```

Étape 5 : configuration de l'adresse de l'interface de gestion sur les trois commutateurs

```
Comm1(config)#interface vlan 99
Comm1(config-if)#ip address 172.17.99.11 255.255.255.0
Comm1(config-if)#no shutdown

Comm2(config)#interface vlan 99
Comm2(config-if)#ip address 172.17.99.12 255.255.255.0
Comm2(config-if)#no shutdown

Comm3(config)#interface vlan 99
Comm3(config-if)#ip address 172.17.99.13 255.255.255.0
Comm3(config-if)#no shutdown
```

Vérifiez que les commutateurs sont configurés correctement en envoyant des requêtes ping entre eux. À partir de Comm1, envoyez une requête ping à l'interface de gestion sur Comm2 et Comm3. À partir de Comm2, envoyez une requête ping à l'interface de gestion sur Comm3.

Les requêtes ping ont-elles abouti ? _____

Dans le cas contraire, corrigez les configurations des commutateurs et réessayez.

Étape 6 : affectation des ports de commutateur aux réseaux locaux virtuels sur Comm2

Reportez-vous au tableau d'affectation des ports au début des travaux pratiques pour affecter les ports aux réseaux locaux virtuels sur Comm2.

```
Comm2(config)#interface range fa0/5-10
Comm2(config-if-range)#switchport access vlan 30
Comm2(config-if-range)#interface range fa0/11-17
Comm2(config-if-range)#switchport access vlan 10
Comm2(config-if-range)#interface range fa0/18-24
Comm2(config-if-range)#switchport access vlan 20
Comm2(config-if-range)#end
Comm2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Étape 7 : vérification de la connectivité entre les réseaux locaux virtuels

Ouvrez des fenêtres de commande sur les trois hôtes connectés à Comm2. Envoyez une requête ping de PC1 (172.17.10.21) vers PC2 (172.17.20.22). Envoyez une requête ping de PC2 vers PC3 (172.17.30.23).

Les requêtes ping ont-elles abouti ? _____

Pourquoi ? _____

_____

_____

Tâche 5 : configuration du routeur et du LAN du serveur distant

Étape 1 : suppression de la configuration du routeur et rechargement

```
Router#erase nvram:
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
Erase of nvram: complete
Router#reload
System configuration has been modified. Save? [yes/no]: no
```

Étape 2 : création d'une configuration de base sur le routeur

- Configurez le routeur avec le nom d'hôte R1.
- Désactivez la recherche DNS.
- Configurez le mot de passe **cisco** pour le mode d'exécution.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.

Étape 3 : configuration de l'interface d'agrégation sur R1

Vous avez constaté que la connectivité entre les réseaux locaux virtuels demande d'établir le routage au niveau de la couche réseau, tout comme la connectivité entre deux réseaux distants. Il existe plusieurs options pour configurer le routage entre des réseaux locaux virtuels.

La première est une approche un peu brutale. Un périphérique de couche 3, au choix un routeur ou un commutateur compatible couche 3, est connecté à un commutateur LAN avec plusieurs connexions dont une distincte pour chaque réseau local virtuel qui demande une connectivité entre réseaux locaux virtuels. Tous les ports de commutation utilisés par le périphérique de couche 3 sont configurés dans un réseau local virtuel séparé sur le commutateur. Une fois les adresses IP affectées aux interfaces sur le périphérique de couche 3, la table de routage contient les routes connectées directement à tous les réseaux locaux virtuels et le routage entre réseaux locaux virtuels est activé. Les limites de cette méthode sont le manque de ports Fast Ethernet sur les routeurs, la sous-utilisation des ports sur les commutateurs de couche 3 et les routeurs, le câblage important et le degré élevé de configuration manuelle. La topologie utilisée dans ces travaux pratiques n'emploie pas cette méthode.

Il existe une autre méthode qui consiste à créer une ou plusieurs connexions Fast Ethernet entre le périphérique de couche 3 (le routeur) et le commutateur de la couche de distribution puis à configurer ces connexions en tant qu'agrégations dot1q. De cette manière, tout le trafic entre réseaux locaux virtuels pourra transiter par le périphérique de routage sur une seule agrégation. Toutefois, cela demande que l'interface de couche 3 soit configurée avec plusieurs adresses IP. Vous pouvez le faire en créant des interfaces virtuelles, appelées « sous-interfaces », sur l'un des ports du routeur Fast Ethernet puis en les configurant comme compatibles dot1q.

La configuration avec sous-interfaces requiert les étapes suivantes :

- Passer en mode de configuration de sous-interface
- Établir une encapsulation des agrégations
- Associer un VLAN avec la sous-interface
- Affecter une adresse IP à la sous-interface depuis le VLAN

Les commandes à utiliser sont les suivantes :

```
R1(config)#interface fastethernet 0/1
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/1.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 172.17.1.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Notez les points suivants dans cette configuration :

- L'interface physique est activée par la commande **no shutdown**, car les interfaces de routeur sont inactives par défaut. Les interfaces virtuelles sont actives par défaut.
- La sous-interface peut utiliser tout nombre en 32 bits mais il est conseillé d'affecter le numéro de VLAN au numéro d'interface, comme dans cet exemple.
- Le réseau local virtuel natif est spécifié sur le périphérique de couche 3 pour être cohérent avec les commutateurs. Sinon, VLAN 1 sera le réseau local virtuel natif par défaut et la communication ne passera pas entre le routeur et le VLAN de gestion sur les commutateurs.

Étape 4 : configuration de l'interface réseau du serveur sur R1

```
R1(config)# interface FastEthernet0/0
R1(config-if)#ip address 172.17.50.1 255.255.255.0
R1(config-if)#description server interface
R1(config-if)#no shutdown
R1(config-if)#end
```

Nous avons maintenant six réseaux configurés. Contrôlez que vous pouvez router des paquets vers les six réseaux en vérifiant la table de routage sur R1.

```
R1#show ip route
<résultat omis>

Gateway of last resort is not set

     172.17.0.0/24 is subnetted, 6 subnets
C       172.17.50.0 is directly connected, FastEthernet0/1
C       172.17.30.0 is directly connected, FastEthernet0/0.30
C       172.17.20.0 is directly connected, FastEthernet0/0.20
```

```
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.1.0 is directly connected, FastEthernet0/0.1
C       172.17.99.0 is directly connected, FastEthernet0/0.99
```

Si votre table de routage ne contient pas les six réseaux, corrigez votre configuration et réglez le problème avant de continuer.

Étape 5 : vérification du routage entre réseaux locaux virtuels

Depuis PC1, vérifiez que vous pouvez envoyer une requête ping au serveur distant (172.17.50.254) et aux deux autres hôtes (172.17.20.22 et 172.17.30.23). Plusieurs requêtes ping peuvent être nécessaires avant que le chemin de bout en bout ne s'établisse.

Les requêtes ping ont-elles abouti ? _____

Dans le cas contraire, corrigez la configuration. Vérifiez que les passerelles par défaut ont été définies sur tous les PC et tous les commutateurs. Si un des hôtes est entré en hibernation, l'interface connectée risque d'être désactivée.

Tâche 6 : remarques générales

Dans la Tâche 5, il était conseillé de configurer VLAN 99 comme réseau local virtuel natif dans la configuration d'interface du routeur Fa0/0.99. Pourquoi les paquets provenant du routeur ou des hôtes ne pourraient-ils pas atteindre les interfaces de gestion du commutateur si le VLAN natif restait le VLAN par défaut ?

_____

_____

_____

_____

Tâche 7 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Configurations finales

Routeur 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.17.50.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
```

```
 no shutdown
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1
 ip address 172.17.1.1 255.255.255.0
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 172.17.30.1 255.255.255.0
!
interface FastEthernet0/1.99
 encapsulation dot1Q 99 native
 ip address 172.17.99.1 255.255.255.0
!
<résultat omis - interfaces séries non configurées>
!
line con 0
line aux 0
line vty 0 4
 login
 password cisco
!
```

Commutateur 1

```
!
hostname Comm1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
```

```
 switchport mode trunk
!
interface FastEthernet0/5
 no shutdown
!
<résultat omis – tous les autres ports sont à l'arrêt>
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no shutdown
!
ip default-gateway 172.17.99.1
ip http server
!
line con 0
 logging synchronous
line vty 0 4
 login
 password cisco
line vty 5 15
 login
 password cisco
!
end
```

Commutateur 2

```
!
hostname Comm2
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
```

```
 switchport access vlan 30
 switchport mode access
!
 interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 30
!
interface FastEthernet0/8
 switchport access vlan 30
!
interface FastEthernet0/9
 switchport access vlan 30
!
interface FastEthernet0/10
 switchport access vlan 30
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
!
 interface FastEthernet0/13
 switchport access vlan 10
!
interface FastEthernet0/14
 switchport access vlan 10
!
interface FastEthernet0/15
 switchport access vlan 10
!
interface FastEthernet0/16
 switchport access vlan 10
!
interface FastEthernet0/17
 switchport access vlan 10
!
interface FastEthernet0/18
 switchport access vlan 20
!
interface FastEthernet0/19
 switchport access vlan 20
!
interface FastEthernet0/20
 switchport access vlan 20
!
interface FastEthernet0/21
 switchport access vlan 20
!
interface FastEthernet0/22
 switchport access vlan 20
```

```
!
interface FastEthernet0/23
 switchport access vlan 20
!
interface FastEthernet0/24
 switchport access vlan 20
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
ip default-gateway 172.17.99.1
ip http server
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Commutateur 3

```
!
hostname Comm3
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
```

```
!
interface FastEthernet0/5
 shutdown
!
<résultat omis – tous les autres ports sont à l'arrêt>
!
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no shutdown
!
ip default-gateway 172.17.99.1
ip http server
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Travaux pratiques 6.4.2 : routage avancé entre réseaux locaux virtuels

Diagramme de topologie

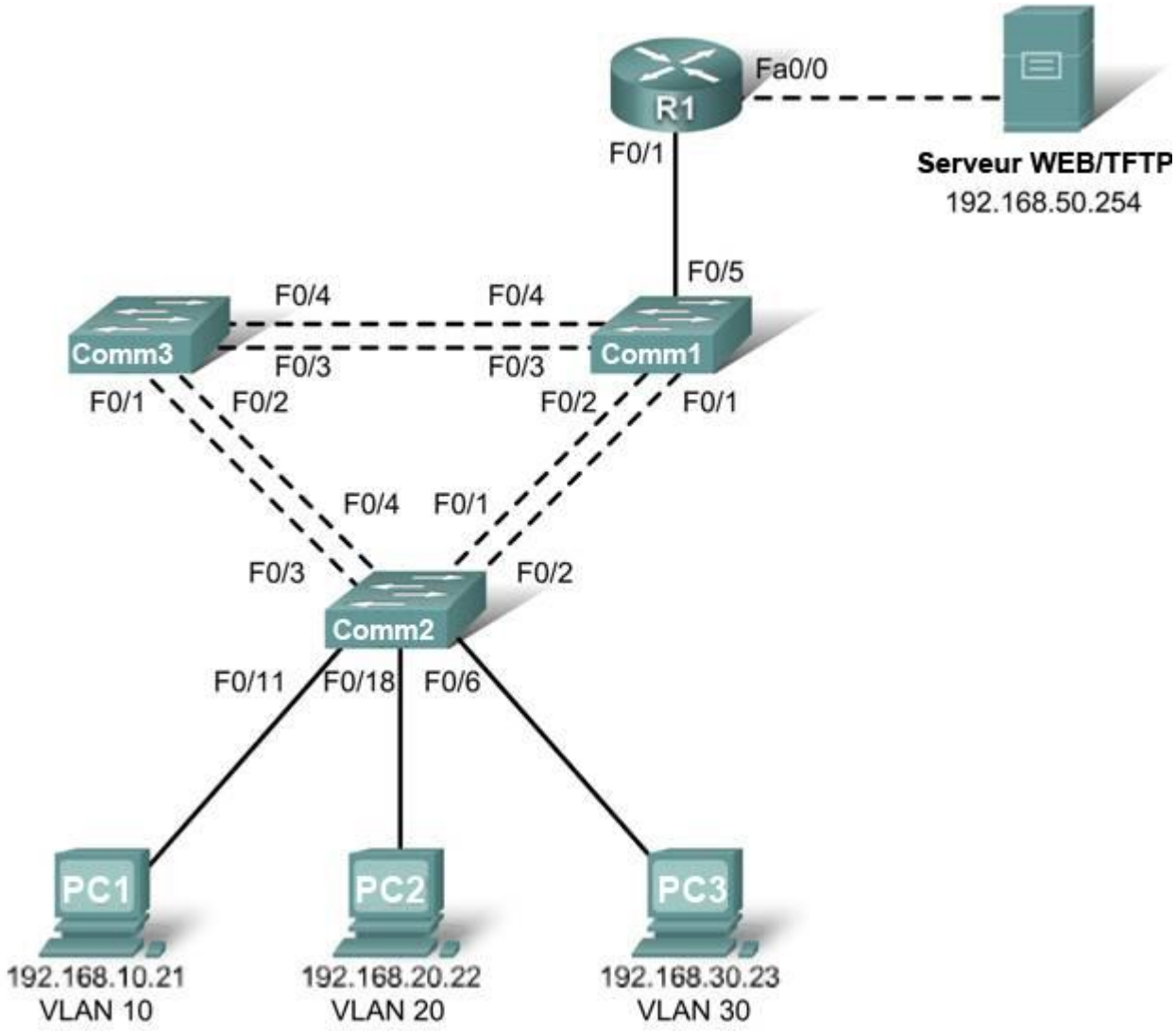


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 99**	192.168.99.11	255.255.255.0	192.168.99.1
Comm2	**VLAN 99**	192.168.99.12	255.255.255.0	192.168.99.1
Comm3	**VLAN 99**	192.168.99.13	255.255.255.0	192.168.99.1

R1	**Fa 0/0**	192.168.50.1	255.255.255.0	S/O
R1	**Fa 0/1**	Voir Tableau de configuration des sous-interfaces		S/O
PC1	**Carte réseau**	192.168.10.21	255.255.255.0	192.168.10.1
PC2	**Carte réseau**	192.168.20.22	255.255.255.0	192.168.20.1
PC3	**Carte réseau**	192.168.30.23	255.255.255.0	192.168.30.1
Serveur	**Carte réseau**	192.168.50.254	255.255.255.0	192.168.50.1

Affectations des ports – Commutateur 2

Ports	Affectation	Réseau
Fa0/1 – 0/4	Agrégations 802.1q (VLAN 99 natif)	192.168.99.0 /24
Fa0/5 – 0/10	VLAN 30 – Ventes	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – R&D	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Ingénierie	192.168.20.0 /24

Tableau de configuration des sous-interfaces – Routeur 1

Interface de routeur	Affectation	Adresse IP
Fa0/0.1	VLAN 1	192.168.1.1
Fa0/0.10	VLAN 10	192.168.10.1
Fa0/0.20	VLAN 20	192.168.20.1
Fa0/0.30	VLAN 30	192.168.30.1
Fa0/0.99	VLAN 99	192.168.99.1

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Réinitialiser les configurations et restaurer un commutateur et un routeur à l'état par défaut
- Exécuter des tâches de configuration de base sur un routeur et un réseau local commuté
- Configurer des VLAN et le protocole VTP (VLAN Trunking Protocol) sur tous les commutateurs
- Configurer un routeur pour prendre en charge les agrégations 802.1q sur une interface Fast Ethernet
- Configurer un routeur avec des sous-interfaces correspondant aux VLAN configurés
- Expliquer le routage entre réseaux locaux virtuels

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Les résultats présentés dans ces travaux pratiques proviennent de commutateurs 2960 et d'un routeur 1841. Vous pouvez utiliser n'importe quel commutateur ou routeur durant les travaux pratiques, pourvu qu'ils soient équipés des interfaces indiquées dans le diagramme de topologie. Les autres types

de périphérique peuvent produire des résultats différents. Notez que les interfaces réseaux Ethernet (10 Mo) sur les routeurs ne prennent pas en charge les agrégations et que les programmes IOS Cisco antérieurs à la version 12.3 ne prennent pas toujours en charge les agrégations sur les interfaces de routeur Fast Ethernet.

Configurez les connexions console pour les trois commutateurs et le routeur.

Étape 2 : suppression des configurations actuelles des commutateurs

Videz la mémoire vive non volatile, supprimez le fichier vlan.dat et rechargez les commutateurs. Reportez-vous aux Travaux pratiques 2.2.1 pour plus d'informations sur la procédure. Une fois le rechargement fini, utilisez la commande **show vlan** pour confirmer que seuls les réseaux locaux virtuels par défaut existent et que tous les ports sont affectés au VLAN 1.

Étape 3 : désactivation de tous les ports à l'aide de la commande shutdown

Vérifiez que l'état initial des ports de commutateur est inactif en désactivant tous les ports. Utilisez la commande **interface-range** pour simplifier cette tâche.

Étape 4 : réactivation des ports utilisateur actifs sur Comm2 en mode access

Activez les ports Fa0/6, Fa0/11 et Fa0/18 sur Comm2 à l'aide de la commande **no shutdown** puis configurez-les comme ports d'accès.

Tâche 2 : configuration de base des commutateurs

Configurez les commutateurs Comm1, Comm2 et Comm3 en fonction du tableau d'adressage et des instructions suivantes :

- Configurez le nom d'hôte du commutateur.
- Désactivez la recherche DNS.
- Configurez le mot de passe **class** pour le mode d'exécution.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.
- Configurez la passerelle par défaut sur chaque commutateur.

Tâche 3 : configuration des interfaces Ethernet sur le serveur et les ordinateurs hôtes

Configurez les interfaces Ethernet de PC1, PC2, PC3 et le serveur TFTP/Web distant avec les adresses IP issues du tableau d'adressage. Connectez ces périphériques avec les câbles et les interfaces appropriés.

Tâche 4 : configuration du protocole VTP sur les commutateurs

Étape 1 : configuration du protocole VTP sur les trois commutateurs

Utilisez le tableau suivant pour configurer les commutateurs. N'oubliez pas que les mots de passe et les noms de domaine VTP tiennent compte des majuscules.

Nom du commutateur	Mode de fonctionnement VTP	Domaine VTP	Mot de passe VTP
Comm1	**Serveur**	**Lab6**	**cisco**
Comm2	**Client**	**Lab6**	**cisco**
Comm3	**Client**	**Lab6**	**cisco**

Étape 2 : configuration des ports d'agrégation et désignation du réseau local virtuel natif pour les agrégations

Configurez les ports Fa0/1 à Fa0/5 comme ports d'agrégation et désignez VLAN 99 comme réseau local virtuel natif pour ces agrégations. Utilisez la commande **interface range** en mode de configuration globale pour simplifier cette tâche.

Étape 3 : configuration des réseaux locaux virtuels sur le serveur VTP

Configurez les réseaux locaux virtuels suivants sur le serveur VTP :

VLAN	Nom VLAN
VLAN 99	**Direction**
VLAN 10	**R&D**
VLAN 20	**Ingénierie**
VLAN 30	**Ventes**

Vérifiez que les réseaux locaux virtuels ont été créés sur Comm1 via la commande **show vlan brief**.

Étape 4 : vérification de la distribution sur Comm2 et Comm3 des réseaux locaux virtuels créés sur Comm1

Exécutez la commande **show vlan brief** sur Comm2 et Comm3 pour vérifier que les quatre réseaux locaux virtuels ont été répartis sur les commutateurs clients.

Étape 5 : configuration de l'adresse de l'interface Direction sur les trois commutateurs

Reportez-vous au tableau d'adressage au début des travaux pratiques pour affecter l'adresse IP de Direction aux trois commutateurs.

Vérifiez que les commutateurs sont configurés correctement en envoyant des requêtes ping entre eux. À partir de Comm1, envoyez une requête ping à l'interface Direction sur Comm2 et Comm3. À partir de Comm2, envoyez une requête ping à l'interface Management sur Comm3.

Les requêtes ping ont-elles abouti ? _____

Si la réponse est non, dépannez les configurations des commutateurs et résolvez les problèmes.

Étape 6 : affectation des ports de commutateur aux réseaux locaux virtuels sur Comm2

Reportez-vous au tableau d'affectation des ports au début des travaux pratiques pour affecter les ports aux réseaux locaux virtuels sur Comm2.

Étape 7 : vérification de la connectivité entre les réseaux locaux virtuels

Ouvrez des fenêtres de commande sur les trois hôtes connectés à Comm2. Envoyez une requête ping de PC1 (192.168.10.21) vers PC2 (192.168.20.22). Envoyez une requête ping de PC2 vers PC3 (192.168.30.23).

Les requêtes ping ont-elles abouti ? _____

Pourquoi ? _____

_____

Tâche 5 : configuration du routeur

Étape 1 : suppression de la configuration du routeur et rechargement

Étape 2 : création d'une configuration de base sur le routeur

- Configurez le routeur avec le nom d'hôte R1.
- Désactivez la recherche DNS.
- Configurez le mot de passe **class** pour le mode d'exécution.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.

Étape 3 : configuration de l'interface d'agrégation sur R1

Configurez l'interface Fa0/1 sur R1 avec cinq sous-interfaces, une pour chaque VLAN identifié dans le tableau de configuration des sous-interfaces au début des travaux pratiques. Configurez ces sous-interfaces avec l'encapsulation dot1q et utilisez la première adresse dans chaque sous-réseau VLAN sur la sous-interface du routeur. Désignez VLAN 99 comme le VLAN natif sur sa sous-interface. N'affectez pas d'adresse IP à l'interface physique mais n'oubliez pas de l'activer. Reportez les sous-interfaces et leurs adresses IP respectives dans le tableau des sous-interfaces.

Étape 4 : configuration de l'interface réseau du serveur sur R1

Reportez-vous au tableau d'adressage et configurez Fa0/0 avec l'adresse IP et le masque appropriés.

Étape 5 : vérification de la configuration du routage

À cette étape, six réseaux doivent être configurés sur R1. Contrôlez que vous pouvez router des paquets vers les six réseaux en vérifiant la table de routage sur R1.

Si votre table de routage ne contient pas les six réseaux, corrigez votre configuration et réglez le problème avant de continuer.

Étape 6 : vérification du routage entre réseaux locaux virtuels

Depuis PC1, vérifiez que vous pouvez envoyer une requête ping au serveur distant (192.168.50.254) et aux deux autres hôtes (192.168.20.22 et 192.168.30.23). Plusieurs requêtes ping peuvent être nécessaires avant que le chemin de bout en bout ne s'établisse.

Les requêtes ping ont-elles abouti ? _____

Dans le cas contraire, corrigez la configuration. Vérifiez que les passerelles par défaut ont été définies sur tous les PC et tous les commutateurs. Si un des hôtes est entré en hibernation, l'interface connectée risque d'être désactivée.

À cette étape, vous devez pouvoir envoyer une requête ping à n'importe quel nœud des six réseaux configurés sur votre réseau local, y compris aux interfaces de gestion des commutateurs.

Tâche 6 : remise en état

Supprimez les configurations et rechargez les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 6.4.3 : dépannage du routage entre réseaux locaux virtuels

Diagramme de topologie

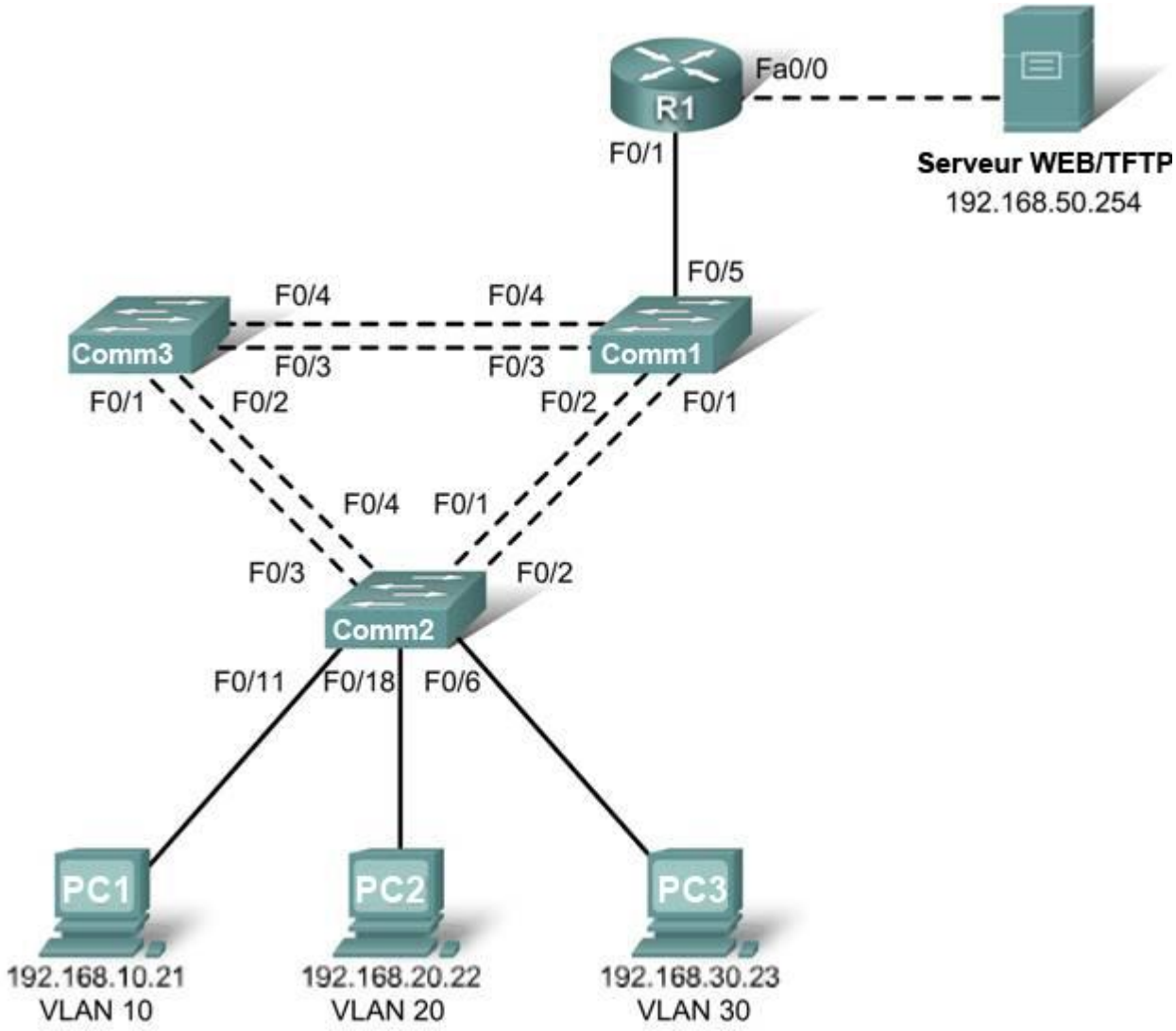


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Comm1	**VLAN 99**	192.168.99.11	255.255.255.0	192.168.99.1
Comm2	**VLAN 99**	192.168.99.12	255.255.255.0	192.168.99.1
Comm3	**VLAN 99**	192.168.99.13	255.255.255.0	192.168.99.1

R1	**Fa 0/0**	192.168.50.1	255.255.255.0	S/O
R1	**Fa 0/1**	Voir Tableau de configuration des sous-interfaces		S/O
PC1	**Carte réseau**	192.168.10.21	255.255.255.0	192.168.10.1
PC2	**Carte réseau**	192.168.20.22	255.255.255.0	192.168.20.1
PC3	**Carte réseau**	192.168.30.23	255.255.255.0	192.168.30.1
Serveur	**Carte réseau**	192.168.50.254	255.255.255.0	192.168.50.1

Affectations des ports – Commutateur 2

Ports	Affectation	Réseau
Fa0/1 – 0/4	Agrégations 802.1q (VLAN 99 natif)	192.168.99.0 /24
Fa0/5 – 0/10	VLAN 30 – Ventes	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – R&D	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Ingénierie	192.168.20.0 /24

Tableau de configuration des sous-interfaces – Routeur 1

Interface de routeur	Affectation	Adresse IP
Fa0/0.1	VLAN 1	192.168.1.1
Fa0/0.10	VLAN 10	192.168.10.1
Fa0/0.20	VLAN 20	192.168.20.1
Fa0/0.30	VLAN 30	192.168.30.1
Fa0/0.99	VLAN 99	192.168.99.1

Objectifs pédagogiques

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

- Installer un réseau conformément au diagramme de topologie
- Effacer les configurations existantes et restaurer les commutateurs et le routeur à leur état par défaut
- Charger les commutateurs et le routeur avec des scripts fournis
- Rechercher et corriger toutes les erreurs de configuration
- Enregistrer le réseau corrigé

Scénario

Le réseau a été conçu et configuré pour prendre en charge cinq réseaux locaux virtuels et un réseau de serveurs séparé. Le routage entre réseaux locaux virtuels est assuré par un routeur externe avec une configuration de type « router-on-a-stick » et le réseau de serveurs est routé via une interface Fast Ethernet séparée. Toutefois, cela ne fonctionne pas comme prévu et les plaintes des utilisateurs n'ont pas permis d'identifier la cause des problèmes. Vous devez d'abord trouver ce qui ne fonctionne pas comme prévu puis analyser les configurations actuelles afin de déterminer la source des problèmes et les corriger.

À l'issue de ces travaux pratiques, vous pourrez prouver la connectivité IP entre chacun des réseaux locaux virtuels de l'utilisateur et le réseau de serveurs externes d'une part, et entre le réseau local virtuel de gestion des commutateurs et le réseau de serveurs d'autre part.

Tâche 1 : préparation du réseau

Étape 1 : installation d'un réseau similaire à celui du diagramme de topologie

Les résultats présentés dans ces travaux pratiques proviennent de commutateurs 2960 et d'un routeur 1841. Vous pouvez utiliser n'importe quel commutateur ou routeur durant les travaux pratiques, pourvu qu'ils soient équipés des interfaces indiquées dans le diagramme de topologie. Les autres types de périphérique peuvent produire des résultats différents. Notez que les interfaces réseaux Ethernet (10 Mo) sur les routeurs ne prennent pas en charge les agrégations et que les programmes IOS Cisco antérieurs à la version 12.3 ne prennent pas toujours en charge les agrégations sur les interfaces de routeur Fast Ethernet.

Configurez les connexions console pour les trois commutateurs et le routeur.

Étape 2 : suppression des configurations actuelles des commutateurs

Supprimez les configurations de commutateur sur les trois commutateurs et rechargez-les pour restaurer l'état par défaut. Utilisez la commande **show vlan** pour confirmer que seuls les réseaux locaux virtuels par défaut existent et que tous les ports sont affectés au VLAN 1.

Étape 3 : configuration des interfaces Ethernet sur les ordinateurs hôtes et le serveur

Configurez les interfaces Ethernet de PC1, PC2 et PC3 et le serveur avec les adresses IP et les passerelles par défaut indiquées dans le tableau d'adressage.

Tâche 2 : chargement du routeur et des commutateurs avec des scripts fournis

Configuration du routeur 1

```
hostname R1
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.50.1 255.255.255.192
!
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1.10
 encapsulation dot1Q 11
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/1.30
 ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet0/1.99
 encapsulation dot1Q 99 native
 ip address 192.168.99.1 255.255.255.0
```

```
!
line con 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
 login
!
end
```

Configuration du commutateur 1

```
hostname Comm1
!
vtp mode server
vtp domain lab6_3
vtp password cisco
!
vlan 99
name Direction
exit
!
vlan 10
name R&D
exit
!
vlan 30
name Ventes
exit
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
 shutdown
!
!
interface range FastEthernet0/5 - 24
 shutdown
!
```

```
interface Vlan99
 ip address 192.168.99.11 255.255.255.0
 no shutdown
!
exit
!
ip default-gateway 192.168.99.1
!
line con 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
 login
!
line vty 5 15
 password cisco
 login
!
end
```

Configuration du commutateur 2

```
!
hostname Comm2
no ip domain-lookup
enable secret class
!
vtp mode client
vtp domain lab6_3
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
 interface range FastEthernet0/5 - 11
 switchport access vlan 30
 switchport mode access
!
interface range FastEthernet0/12 - 17
 switchport access vlan 10
```

```
!
interface range FastEthernet0/18 -24
 switchport mode access
 switchport access vlan 20
!
interface Vlan99
 ip address 192.168.99.12 255.255.255.0
 no shutdown
exit
!
ip default-gateway 192.168.99.1
ip http server
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Configuration du commutateur 3

```
!
hostname Comm3
!
enable secret class
!
vtp mode client
vtp domain lab6_3
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
```

```
 no shutdown
!
interface range FastEthernet0/5 - 24
 shutdown
 exit
!
ip default-gateway 192.168.99.1
!
line con 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
 login
!
line vty 5 15
 password cisco
 login
!
end
```

Tâche 3 : dépannage et correction des erreurs de configuration et problèmes entre réseaux locaux virtuels

Commencez par identifier ce qui fonctionne et ce qui ne fonctionne pas. Quel est l'état des interfaces ? Quels hôtes peuvent envoyer une requête ping aux autres hôtes ? Quels hôtes peuvent envoyer une requête ping au serveur ? Quelles routes devraient apparaître dans la table de routage de R1 ? Qu'est-ce qui peut empêcher un réseau configuré d'entrer dans la table de routage ?

Une fois toutes les erreurs corrigées, vous devez pouvoir envoyer une requête ping au serveur distant depuis n'importe quel ordinateur ou commutateur. De plus, vous devez pouvoir échanger des requêtes ping entre les trois ordinateurs et vers les interfaces de gestion des commutateurs depuis n'importe quel ordinateur.

Tâche 4 : enregistrement de la configuration du réseau

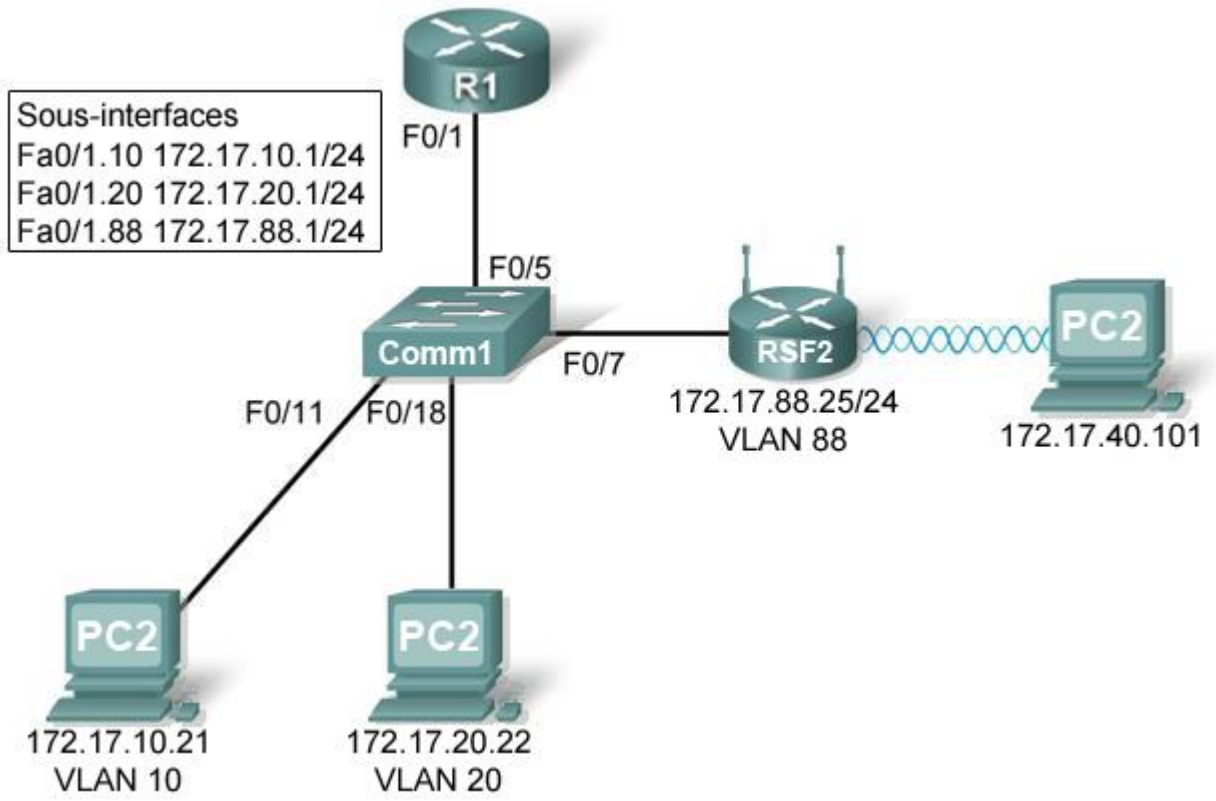
Une fois les problèmes résolus, capturez la sortie de la commande **show run** exécutée sur le routeur et les trois commutateurs puis enregistrez-la dans un fichier texte.

Tâche 5 : remise en état

Supprimez les configurations et rechargez les commutateurs et le routeur. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage approprié et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (LAN de votre site ou Internet).

Travaux pratiques 7.5.1 : configuration de l'accès sans fil au réseau local

Diagramme de topologie



Objectifs pédagogiques

- Configurer les options de l'onglet Linksys Setup
- Configurer les options de l'onglet Linksys Wireless
- Configurer les options de l'onglet Linksys Administration
- Configurer les options de l'onglet Linksys Security
- Ajouter une connectivité sans fil à un PC
- Tester la connectivité

Présentation

Au cours de cette activité, vous allez configurer un routeur sans fil Linksys qui donnera une capacité d'accès à distance à vos PC ainsi qu'une connectivité sans fil avec la sécurité du protocole WEP.

Tâche 1 : chargement des configurations de départ

Étape 1 : chargement des configurations de R1

```
hostname R1
!
interface FastEthernet0/0
 ip address 172.17.50.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 no ip address
 no shutdown
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1.88
 encapsulation dot1Q 88
 ip address 172.17.88.1 255.255.255.0
!
```

Étape 2 : chargement des configurations de Comm2

```
hostname Comm2
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/7
 switchport access vlan 88
 switchport mode access
 no shutdown
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 no shutdown
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
 no shutdown
!
```

Tâche 2 : branchement et connexion du routeur sans fil

Pour configurer les paramètres du routeur sans fil, nous utiliserons son interface utilisateur graphique Web. Pour accéder à cette interface utilisateur, entrez l'adresse IP sans fil/réseau du routeur dans votre navigateur Web. L'adresse par défaut d'origine est 192.168.1.1

Étape 1 : établissement de la connectivité physique

Connectez un câble direct entre le PC et l'un des ports réseau du routeur sans fil. Le routeur sans fil fournira une adresse IP au PC en utilisant des configurations DHCP par défaut.

Étape 2 : ouverture du navigateur Web

Étape 3 : ouverture de l'utilitaire Web du routeur sans fil

- Tapez l'URL http://192.168.1.1 dans votre navigateur.

Les droits d'accès par défaut sont un nom d'utilisateur vide et le mot de passe suivant : **admin**. Notez que cela est risqué car cette valeur par défaut d'origine est connue d'un large public. Nous définirons donc un mot de passe individuel ultérieurement.

Étape 4 : connexion

- Laissez vide la zone du nom d'utilisateur et entrez le mot de passe suivant : admin.

Tâche 3 : configuration des options de l'onglet Linksys Setup

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

- Par défaut, la page de démarrage est l'écran de configuration. Dans les menus situés en haut de la page, vous remarquez que vous êtes dans la section Setup et sous l'onglet Basic Setup.
- Dans l'écran Setup associé au routeur Linksys, cherchez l'option **Internet Connection Type** dans la section **Internet Setup** de la page. Cliquez sur le menu déroulant et sélectionnez **Static IP** dans la liste.

Étape 2 : configuration de la passerelle par défaut, du masque de sous-réseau et de l'adresse IP de VLAN 88 pour RSFRSF2

- Pour l'adresse IP Internet, entrez 172.17.88.25.
- Pour le masque de sous-réseau, entrez 255.255.255.0.
- Pour la passerelle par défaut, entrez 172.17.88.1.

Remarque : habituellement, dans un réseau domestique ou de PME, cette adresse IP est affectée par le FAI via DHCP ou PPPoE (les particularités de PPPoE ne sont pas abordées dans ce cours).

Étape 3 : configuration des paramètres IP du routeur

- Sur la même page, recherchez l'option **Network Setup**. Dans les champs de la section **Router IP**, entrez les informations suivantes :
  - Pour l'adresse IP, entrez 172.17.40.1. Pour le masque de sous-réseau, entrez 255.255.255.0.
- Dans la zone **DHCP Server Setting**, vérifiez que le serveur DHCP est activé.

Étape 4 : enregistrement des paramètres

Cliquez sur le bouton **Save Settings** situé en bas de l'écran **Setup**.

Notez que l'intervalle d'adresses IP du pool DHCP change pour correspondre aux paramètres IP du routeur. Ces adresses sont utilisées pour les clients sans fil et les clients qui se connectent au commutateur interne du routeur sans fil. Les clients recevront une adresse IP et un masque ainsi que l'adresse IP du routeur à utiliser comme passerelle.

Étape 5 : reconnexion de RSFRSF2

Puisque nous avons modifié l'adresse IP et le pool DHCP du routeur, nous devons nous y reconnecter avec la nouvelle adresse que nous venons de configurer.

- Reconnectez-vous au routeur. Vous aurez besoin d'obtenir une nouvelle adresse IP du routeur via DHCP ou d'en définir une autre manuellement.
- Reconnectez-vous à l'interface de configuration du routeur à l'aide de l'adresse IP 172.17.88.1 (reportez-vous à la Tâche 1 si besoin).

Tâche 4 : configuration des options de l'onglet Linksys Wireless

Étape 1 : définition du nom de réseau (SSID)

- Cliquez sur l'onglet **Wireless**.
- Sous **Network Name (SSID)**, remplacez le nom de réseau **Default** par **WRS_LAN**.
- Cliquez sur **Save Settings**.

Étape 2 : définition du mode de sécurité

- Cliquez sur **Wireless Security**. Cette option est située à côté de **Basic Wireless Settings** dans l'onglet principal **Wireless**.
- Dans la zone **Security Mode**, remplacez **Disabled** par **WEP**.
- En utilisant le chiffrement par défaut en 40/64 bits, remplacez **Key1** par **1234567890**.
- Cliquez sur **Save Settings**.

Tâche 5 : configuration des options de l'onglet Linksys Administration

Étape 1 : définition du mot de passe du routeur

- Cliquez sur l'onglet **Administration**.
- Sous **Router Access**, entrez le mot de passe **cisco123**. Entrez à nouveau le même mot de passe pour le confirmer.

Étape 2 : activation de la gestion à distance

- Sous **Remote Access**, activez l'option **Remote Management**.
- Cliquez sur **Save Settings**.
- Un message vous demandera peut-être de vous reconnecter. Utilisez alors le nouveau mot de passe **cisco123** sans entrer de nom d'utilisateur.

Tâche 6 : configuration des options de l'onglet Linksys Security

Par défaut, les requêtes ping envoyées à l'interface sans fil/réseau de RSF2 (172.17.40.1) depuis des sources situées sur son interface de réseau WAN (par exemple PC1 et PC2) seront bloquées pour des raisons de sécurité définies par le routeur sans fil. Toutefois, pour vérifier la connectivité, nous aurons besoin de les autoriser.

Étape 1 : autorisation des requêtes Internet anonymes

- Cliquez sur l'onglet **Security**.
- Sous **Internet Filter**, décochez la case **Filter Anonymous Internet Requests**.

Tâche 7 : ajout d'une connectivité sans fil à un PC

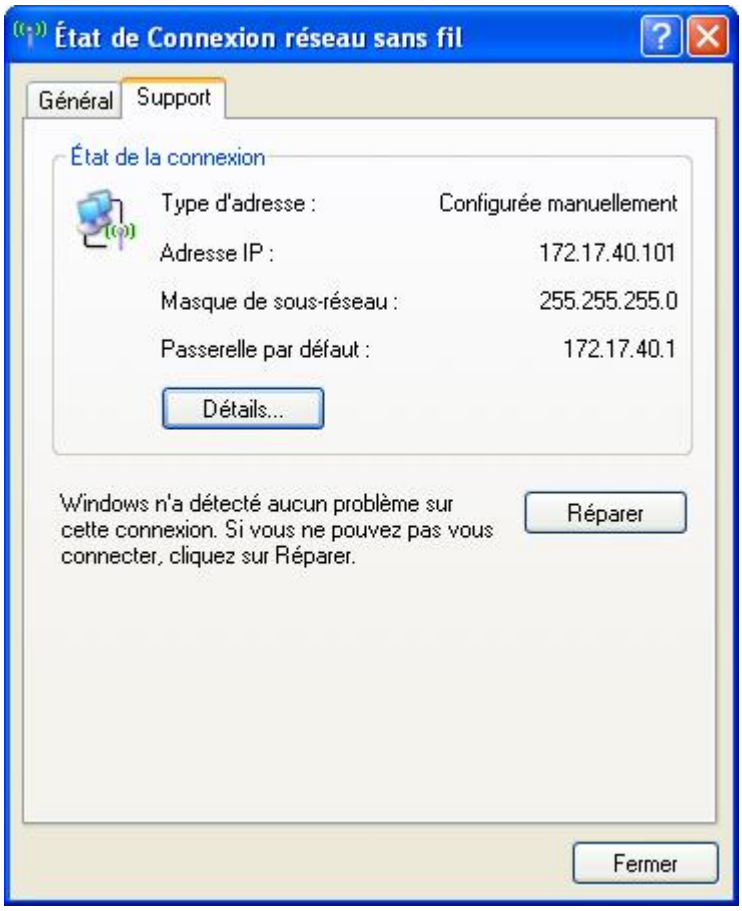
Étape 1 : déconnexion de la liaison Ethernet entre PC3 et RSF2

Étape 2 : connexion du routeur sans fil à l'aide de Windows XP

- Cherchez l'icône Wireless Network Connection dans votre barre des tâches ou sélectionnez **Démarrer > Paramètres > Panneau de configuration > Connexions réseau**.
- Sélectionnez **Wireless Network Connection**.
- Cliquez sur le menu **File** et sélectionnez **Status**.
- Cliquez sur **View Wireless Networks**.
- Cherchez le SSID « WRS_LAN » dans la liste des réseaux disponibles et connectez-vous à ce réseau.
- À l'invite de saisie de la clé WEP, entrez **1234567890** (voir la Tâche 3) puis cliquez sur **Connect**.

Étape 3 : vérification de la connexion

- Dans la fenêtre **Status**, sélectionnez l'onglet **Support**.
- Vérifiez que PC3 a reçu une adresse IP du pool d'adresses DHCP de RSF2 ou a été configuré manuellement.



Tâche 8 : test de la connectivité

Étape 1 : envoi d'une requête ping à l'interface sans fil/réseau de RSF2

- Sur l'ordinateur PC3, cliquez sur **Démarrer ->Exécuter**.
- Tapez **cmd** puis appuyez sur Entrée. Ceci ouvre une fenêtre d'invite de commande.
- À l'invite de commande, tapez **ping 172.17.40.1** et appuyez sur Entrée.

Étape 2 : envoi d'une requête ping à l'interface Fa0/1.88 de R1

- À l'invite de commande, tapez **ping 172.17.88.1** et appuyez sur Entrée.

Étape 3 : envoi d'une requête ping depuis PC3 vers PC1 et PC2

- À l'invite de commande, tapez **ping 172.17.10.21** pour envoyer une requête ping à PC1, et appuyez sur Entrée.
- Puis tapez ping 172.17.20.22 pour PC2, et appuyez sur Entrée.

Travaux pratiques 7.5.2 : configuration avancée sans fil

Diagramme de topologie

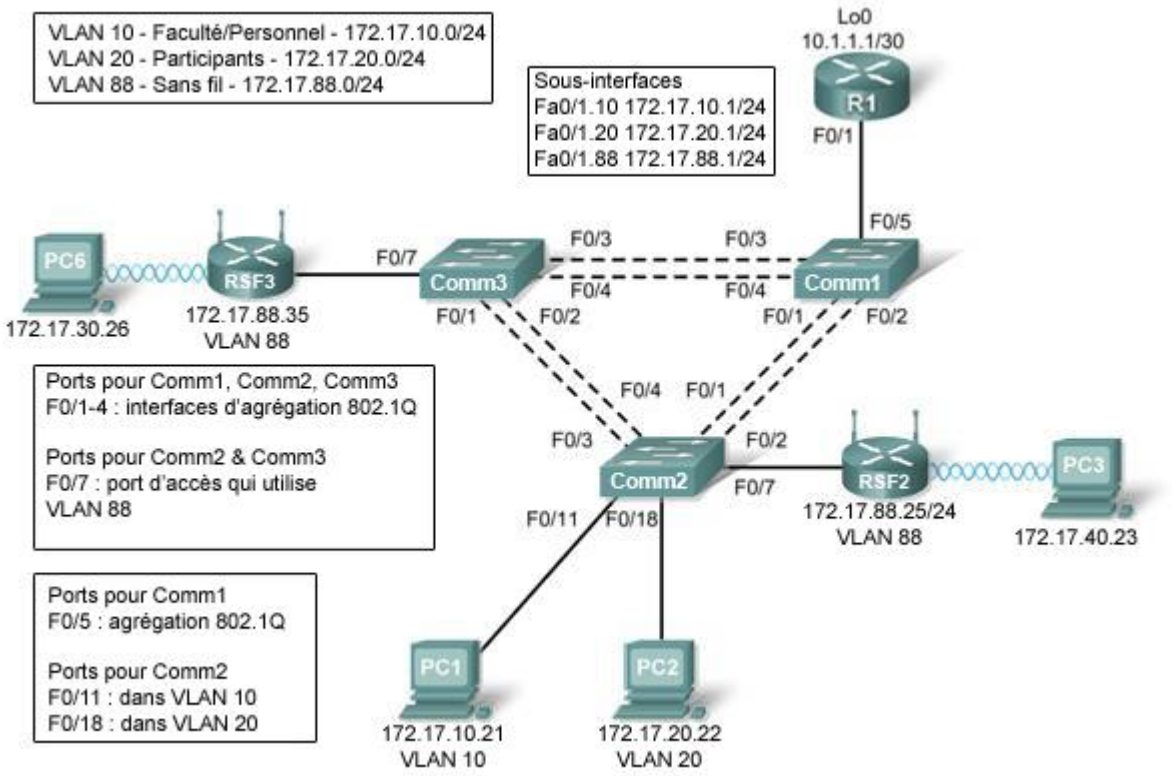


Tableau d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/1.10**	172.17.10.1	255.255.255.0	S/O
	Fa0/1.20	172.17.20.1	255.255.255.0	S/O
	Fa0/1.88	172.17.88.1	255.255.255.0	S/O
	Lo0	10.1.1.1	255.255.255.252	S/O
RSF2	**Réseau étendu**	172.17.88.25	255.255.255.0	172.17.88.1
	Réseau local/sans fil	172.17.40.1	255.255.255.0	S/O
RSF3	**Réseau étendu**	172.17.88.35	255.255.255.0	172.17.88.1

	Réseau local/sans fil	172.17.30.1	255.255.255.0	S/O
PC1	**Carte réseau**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**Carte réseau**	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 Linksys WRT300N
- Configurer les paramètres IP d'un Linksys WRT300N
- Configurer DHCP sur un Linksys WRT300N
- Configurer des routes statiques sur des routeurs standard Cisco et sur un WRT300N
- Changer le mode réseau et le canal réseau correspondant sur un WRT300N
- Activer le chiffrement WEP et désactiver les diffusions de SSID
- Activer un filtre MAC sans fil
- Configurer les restrictions d'accès sur un WRT300N
- Configurer le mot de passe de gestion de routeur d'un WRT300N
- Activer la journalisation sur un WRT300N
- Mettre à niveau le progiciel du WRT300N
- Utiliser les procédures de diagnostic, sauvegarde, restauration et confirmation d'un routeur WRT300N

Scénario

Vous allez configurer un routeur Linksys WRT300N, la sécurité des ports d'un commutateur Cisco et des routes statiques sur plusieurs périphériques. Notez bien les procédures utilisées pour vous connecter au réseau sans fil car certaines étapes demanderont de déconnecter des clients qui devront se reconnecter une fois les changements effectués.

Tâche 1 : exécution des configurations de routeur de base

Configurez le routeur R1 conformément aux instructions suivantes :

- Nom d'hôte du routeur
- Recherche DNS désactivée
- Mot de passe du mode d'exécution
- Fast Ethernet 0/1 et Fast Ethernet 0/0, ainsi que les sous-interfaces
- Loopback0
- Journalisation synchrone, exec-timeout et le nom de login **cisco** sur le port de console

Tâche 2 : configuration des interfaces des commutateurs

Réglez les commutateurs sur le mode Transparent, effacez les données des réseaux locaux virtuels et créez les VLAN 10, 20 et 88.

<pour les trois commutateurs>

```
!
vtp mode transparent
no vlan 2-1001
vlan 10,20,88
!
```

Étape 1 : configuration des interfaces des ports des commutateurs Comm1, Comm2 et Comm3

Configurez les interfaces des commutateurs Comm1, Comm2 et Comm3 selon les connexions du diagramme de topologie.

Sur les connexions entre deux commutateurs, configurez des agrégations.

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

Configurez la connexion entre Comm2 et le PC1, dans le VLAN 10, et la connexion du PC2 dans le VLAN 20.

Configurez la connexion entre Comm1 et R1 en tant qu'agrégation.

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

Comm1

```
!
interface FastEthernet 0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
```

Comm2

```
!
interface FastEthernet 0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/7
 switchport mode access
 switchport access vlan 88
 no shutdown
!
```

Comm3

```
!
interface FastEthernet 0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet 0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdwn
!
interface FastEthernet 0/7
 switchport mode access
 switchport access vlan 88
 no shutdown
```

```
!
interface FastEthernet 0/11
 switchport mode access
 switchport access vlan 11
 no shutdown
!
interface FastEthernet 0/18
 switchport mode access
 switchport access vlan 20
 no shutdown
!
```

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

Exécutez la commande **show ip interface trunk** sur Comm1 et la commande **show vlan command** sur Comm2, pour contrôler que les commutateurs agrègent correctement le trafic et que les réseaux locaux virtuels existent bien.

Comm1#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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,88
Fa0/2       none          <-- bloqué par Spanning Tree
Fa0/3       1,10,20,88
Fa0/4       1,10,20,88
Fa0/5       1,10,20,88>
```

Comm2#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, veillez à enregistrer la configuration en cours dans la mémoire vive non volatile du routeur et des commutateurs.

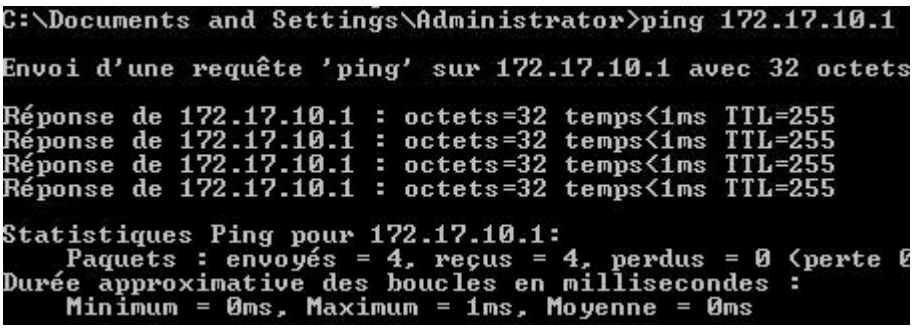
Étape 3 : configuration des interfaces Ethernet de PC1 et PC2

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 tapez ping 172.17.x.x



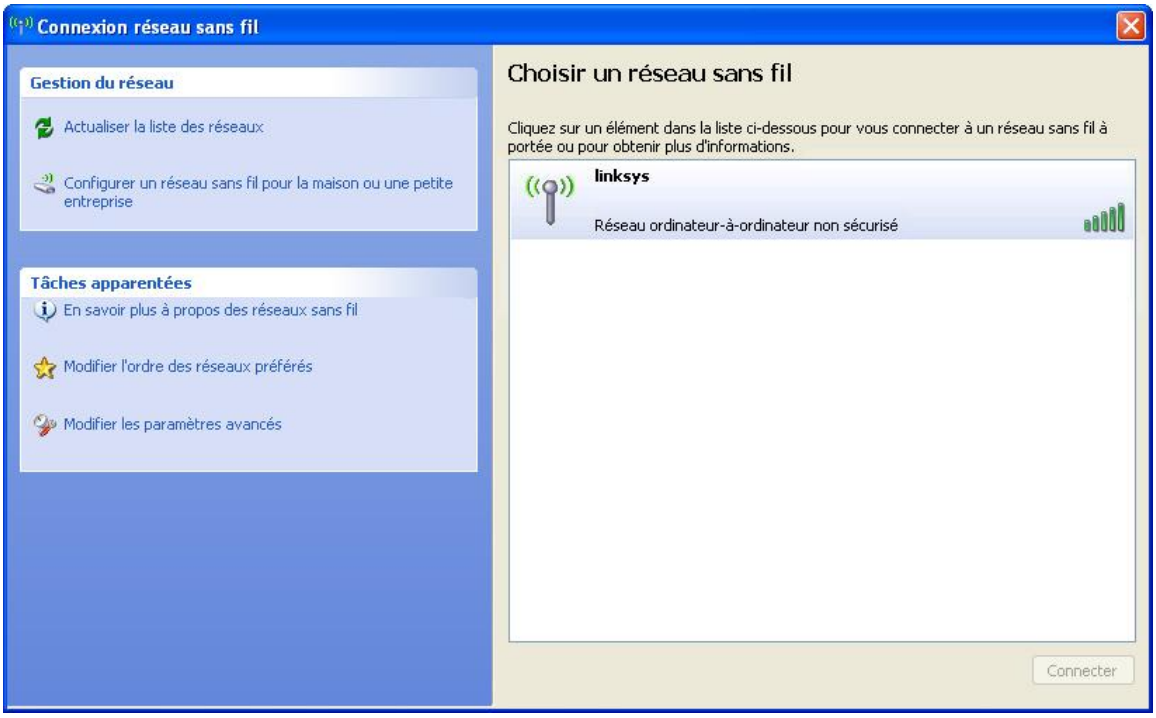
Tâche 3 : connexion au routeur Linksys WRT300N

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 du routeur sans fil à l'aide de Windows XP

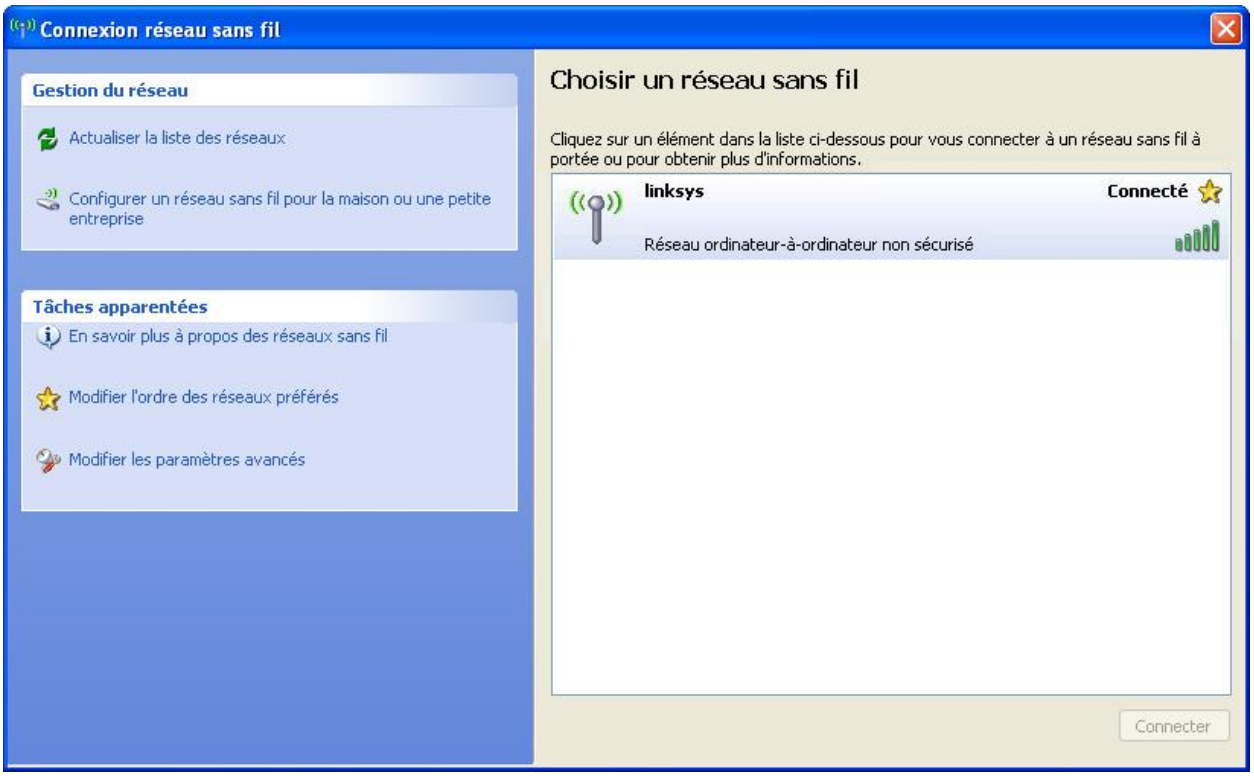
Cherchez l'icône Connexion réseau sans fil dans votre barre des tâches ou sélectionnez **Démarrer > Paramètres > Panneau de configuration > Connexions réseau**. Cliquez à l'aide du bouton droit sur l'icône et sélectionnez Afficher les réseaux sans fil disponibles.

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
```

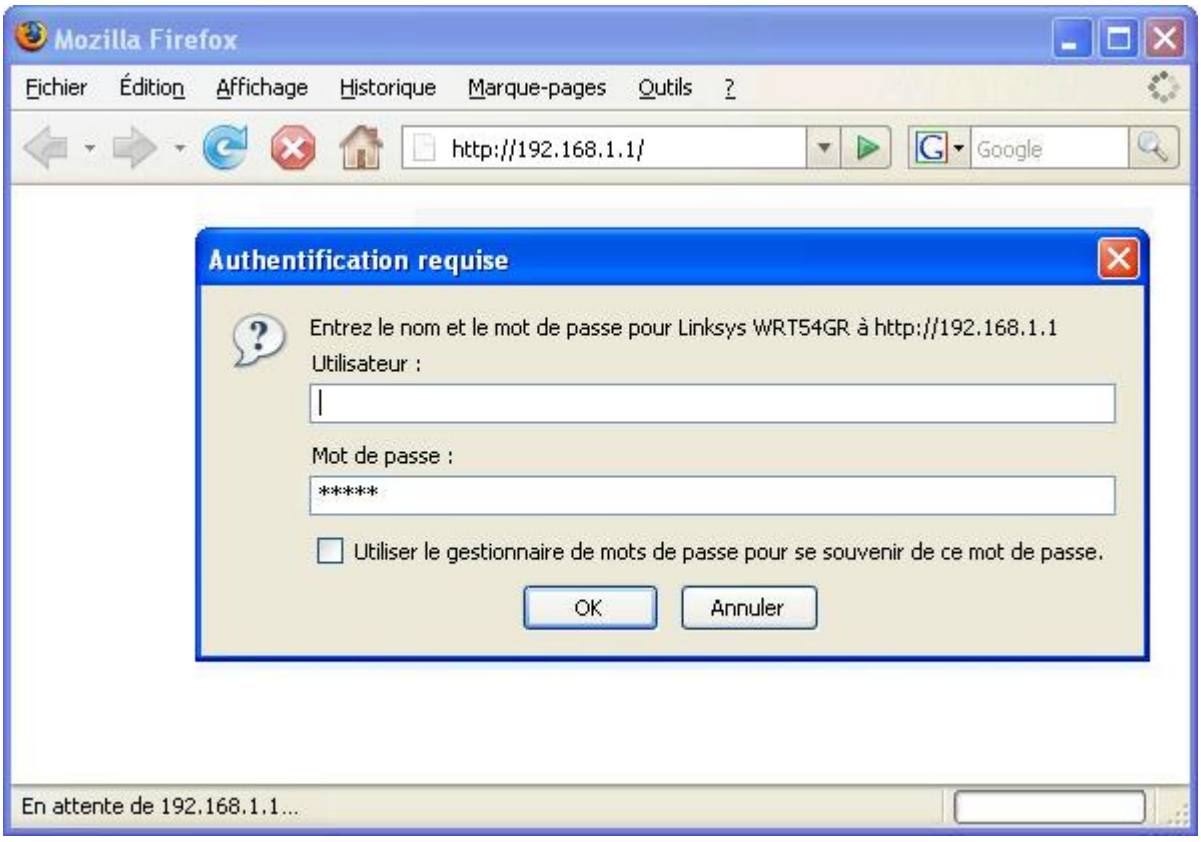
Tâche 4 : configuration du WRT300N à l'aide de l'utilitaire Web

Étape 1 : accès à l'URL par défaut

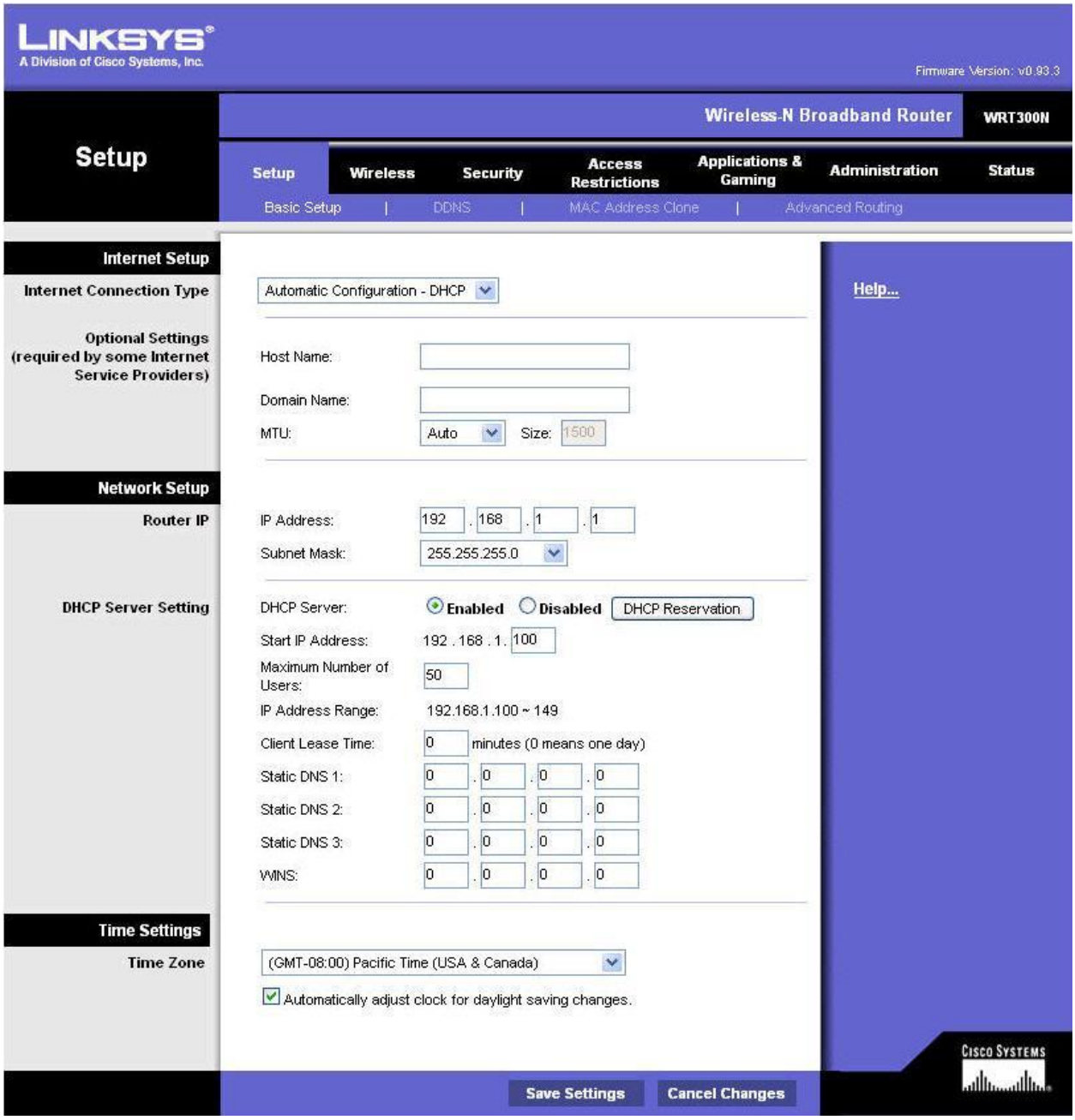
Ouvrez votre navigateur Web habituel et tapez l'adresse **http://192.168.1.1**. Il s'agit de l'URL par défaut du routeur WRT300N.

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.



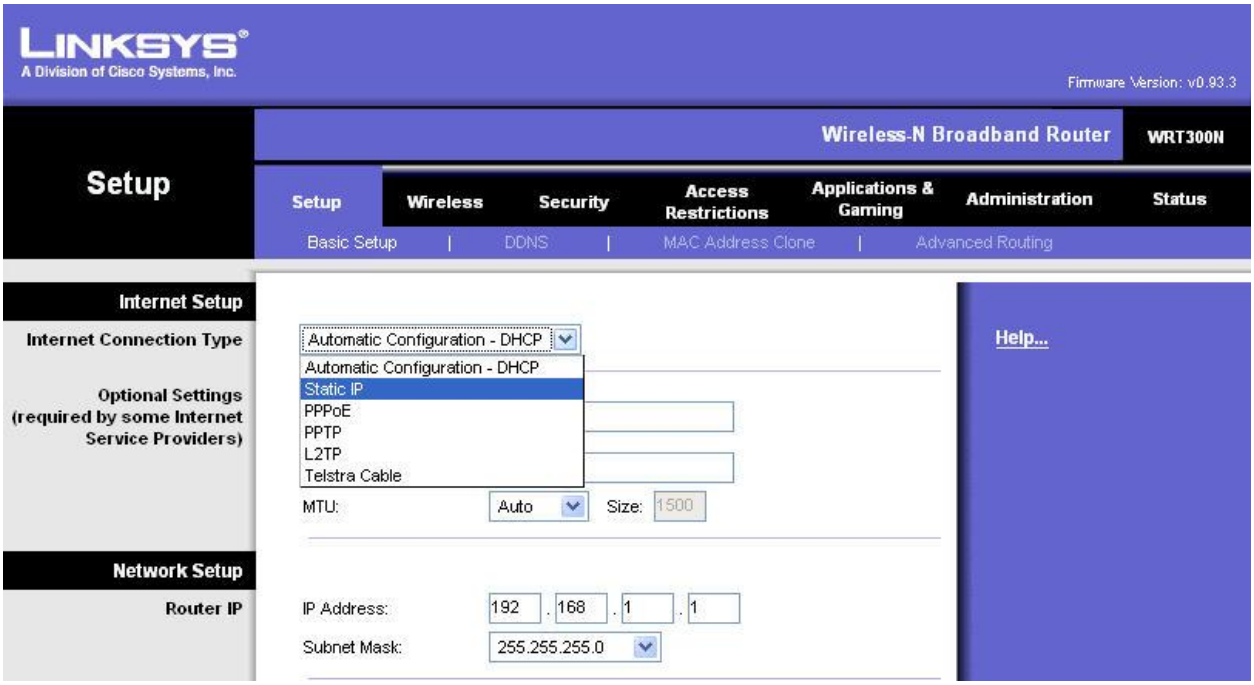
Vous devez voir s'afficher la page par défaut de l'utilitaire Web du routeur Linksys WRT300N.

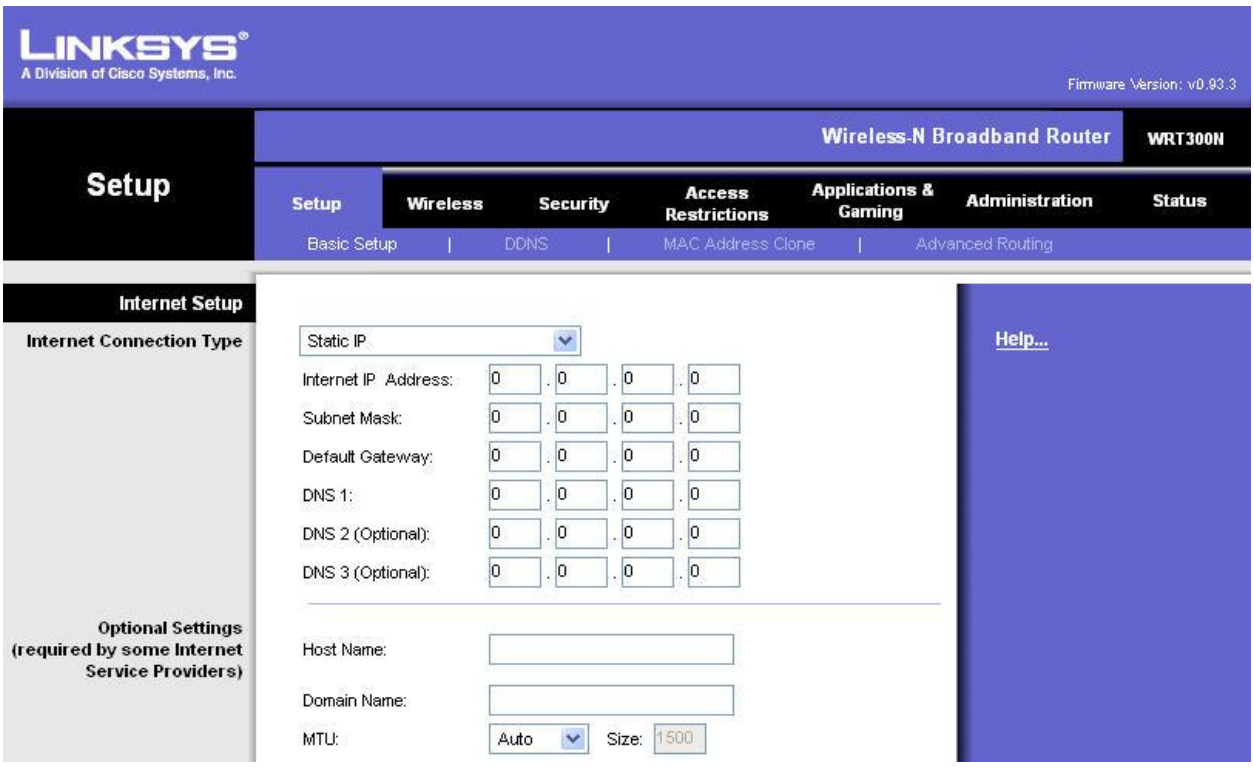


Tâche 5 : configuration des paramètres IP du Linksys WRT300N

Pour mieux comprendre les paramètres qui suivent, regardez le WRT300N comme un routeur Cisco basé sur l'IOS avec deux interfaces séparées. L'une des deux interfaces, celle qui est configurée sous Internet Setup, agit comme une connexion avec les commutateurs et l'intérieur du réseau. L'autre interface, configurée sous Network Setup, agit comme une connexion avec les clients sans fil, PC6 et PC3.

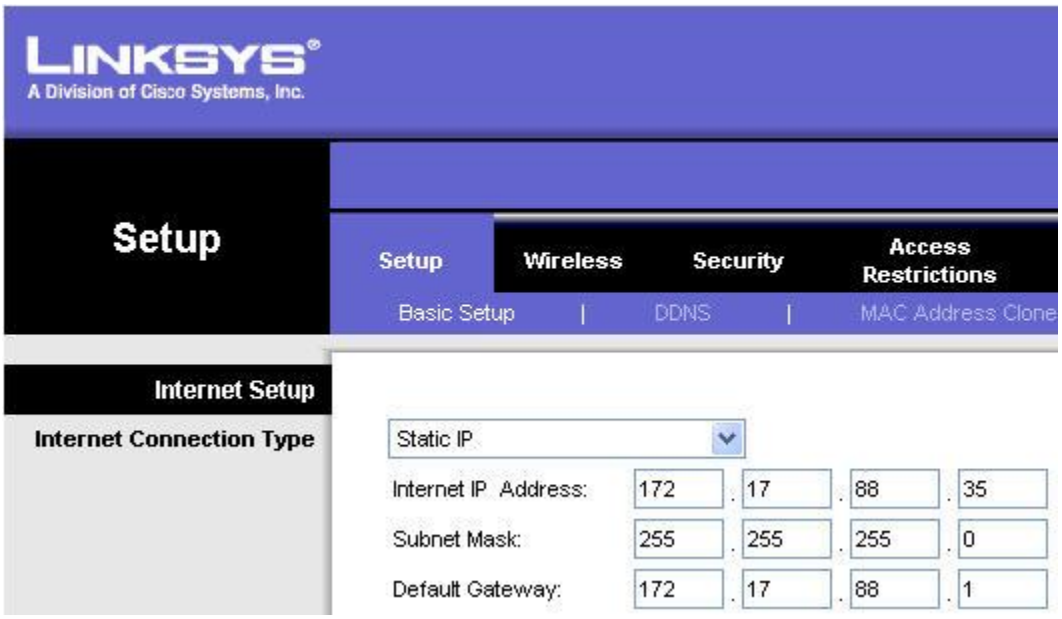
Étape 1 : définition du type de connexion Internet sur IP statique



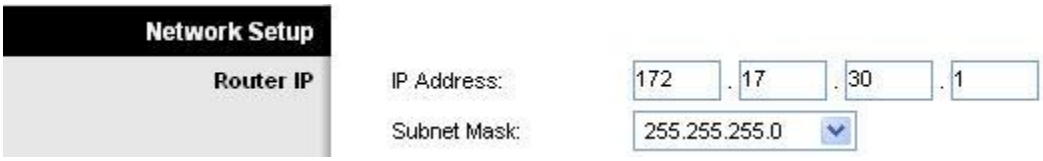


Étape 2 : définition des paramètres d'adresse IP dans Internet Setup

- Pour le paramètre Internet IP Address, tapez 172.17.88.35.
- Pour le paramètre Subnet Mask, tapez 255.255.255.0.
- Pour le paramètre Default Gateway, tapez l'adresse IP du VLAN 88 Fa 0/1 de R1 : 172.17.88.1.

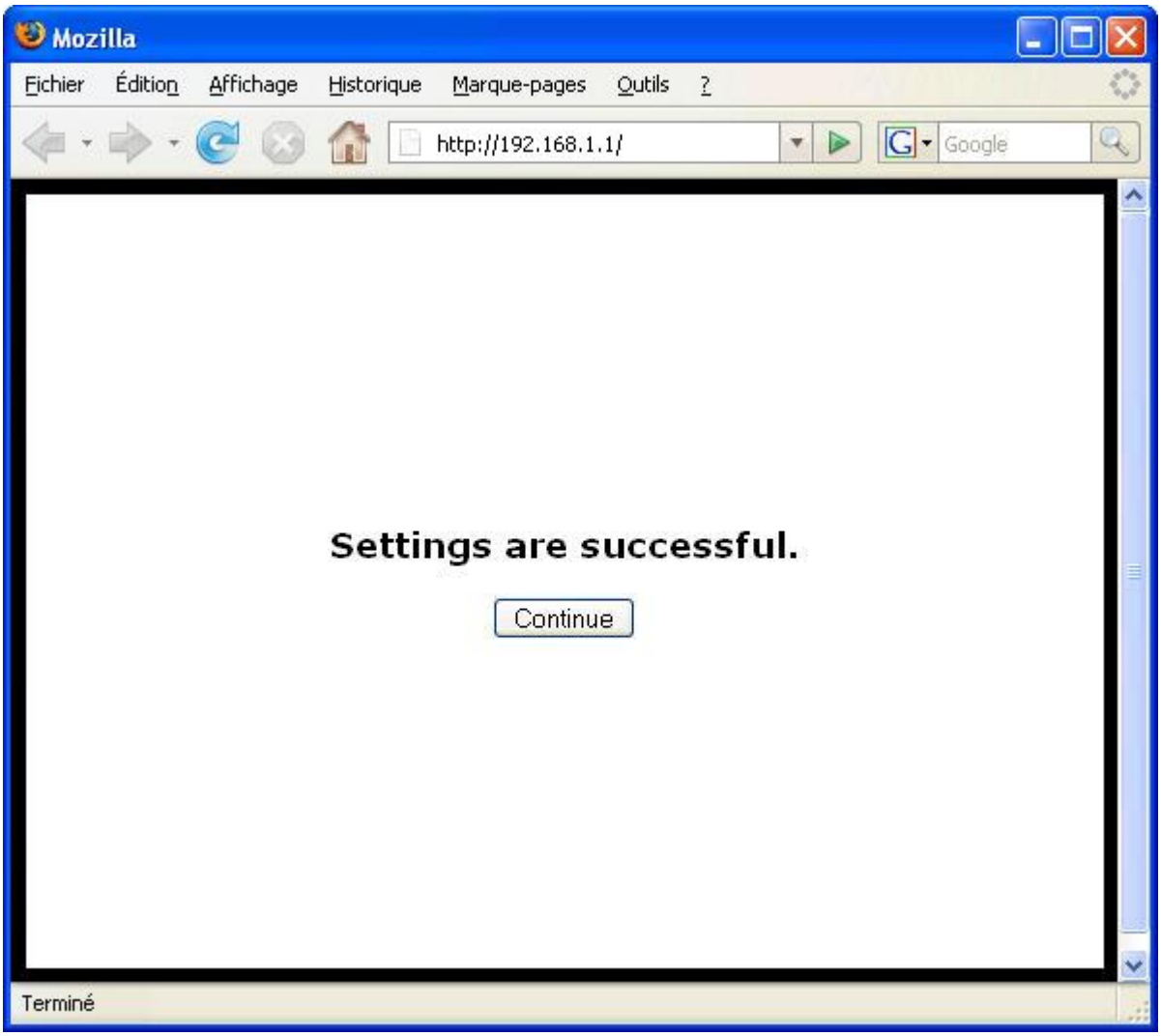


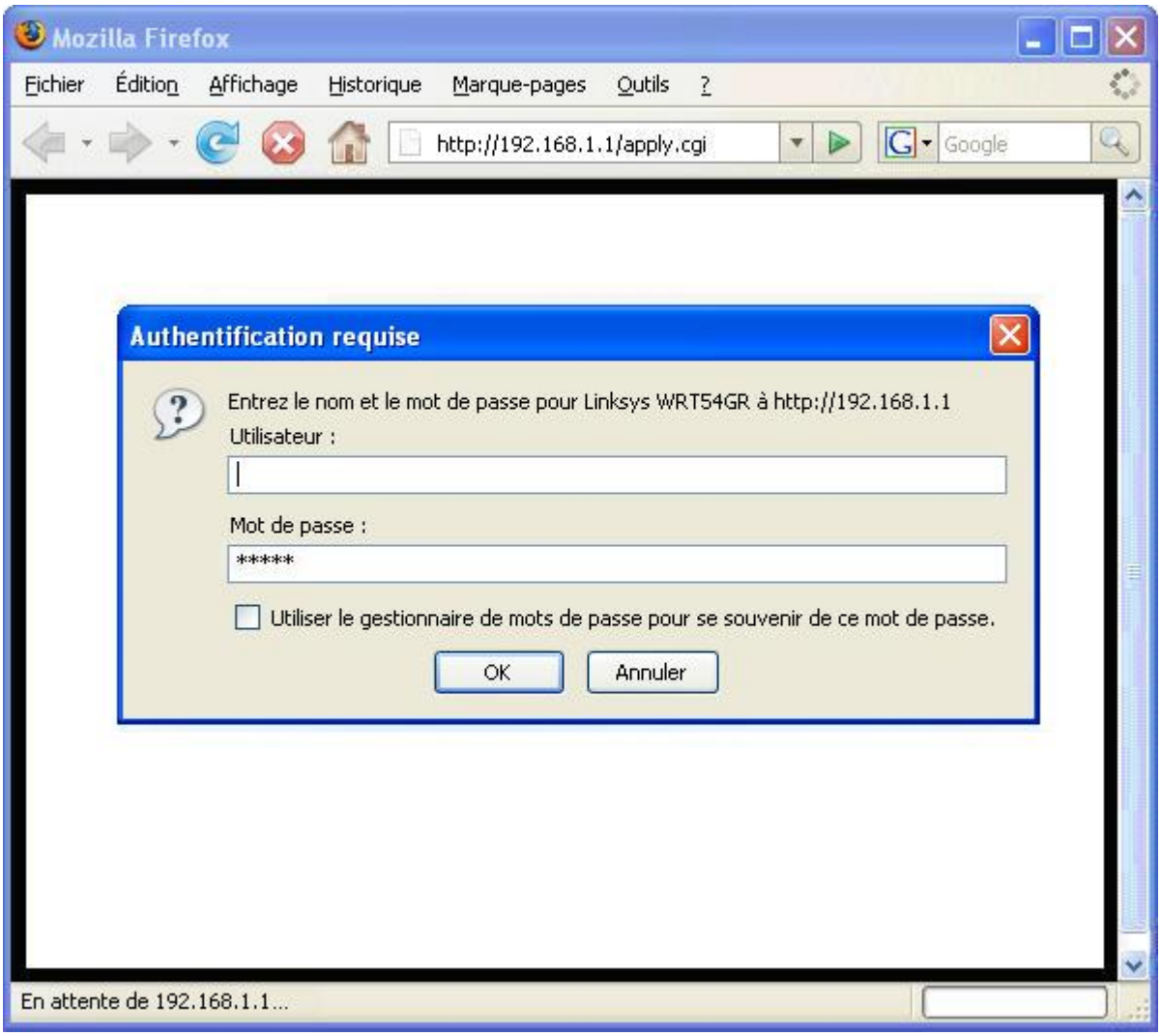
Étape 3 : configuration de l'adresse IP (172.17.30.1)



Étape 4 : enregistrement des paramètres

Cliquez sur **Save Settings**. L'écran suivant apparaît. Cliquez sur **Continue**. Si vous n'êtes pas redirigé vers la nouvelle URL de l'utilitaire Web (**http://172.17.30.1**), entrez cette adresse comme vous l'avez fait à l'étape 1 de la Tâche 4.





Étape 5 : vérification des nouvelles adresses IP

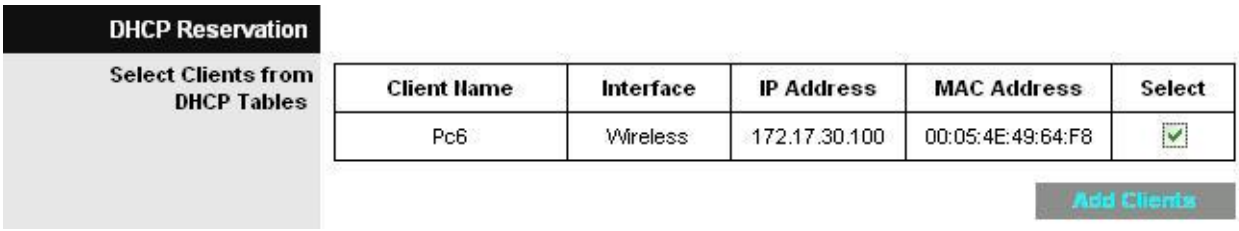
Revenez à l'invite de commande et examinez les nouvelles adresses IP. Tapez la commande **ipconfig**.

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

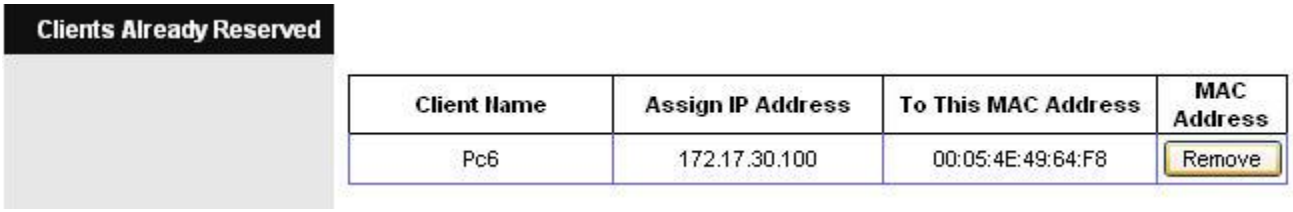
Tâche 6 : configuration des paramètres DHCP et des paramètres horaires du routeur

Étape 1 : affectation d'un lien DHCP statique à Pc6

Cliquez sur **DHCP Reservations** et recherchez Pc6 dans la liste des clients DHCP actuels. Cliquez sur **Add Clients**.

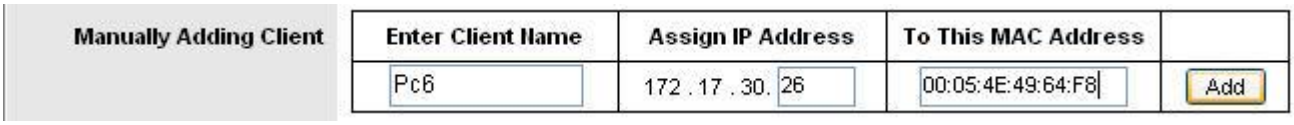


Le client Pc6, c'est-à-dire l'ordinateur ayant l'adresse MAC 00:05:4E:49:64:F8, aura la même adresse IP, 172.17.30.100, chaque fois qu'il demandera une adresse via DHCP. Ceci n'est qu'une des manières d'établir rapidement un lien permanent entre un client et une adresse DHCP. Vous allez maintenant affecter à Pc6 l'adresse IP du diagramme de topologie au lieu de celle qu'il a reçue initialement. Cliquez sur **Remove** pour affecter la nouvelle adresse.



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 le client Pc6 se connectera au routeur, il recevra l'adresse IP 172.17.30.26 via DHCP. Enregistrez les modifications.

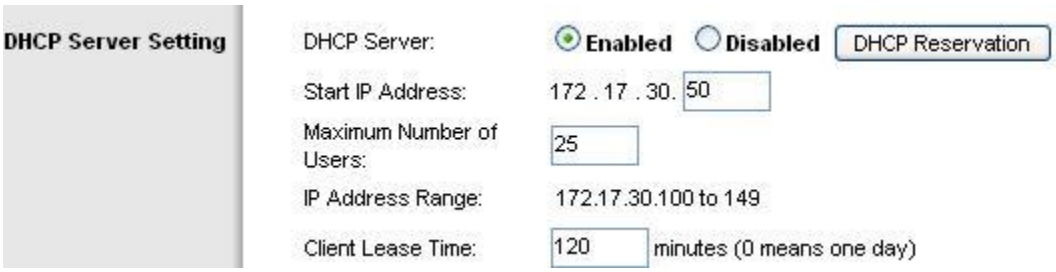


Étape 3 : vérification du changement d'adresse IP statique

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 6, Étape 5, que cette modification a été prise en compte.

Étape 4 : configuration du serveur DHCP

Réglez l'adresse de départ sur 50, le nombre maximum d'utilisateurs sur 25 et la durée d'utilisation sur 2 heures (120 minutes).

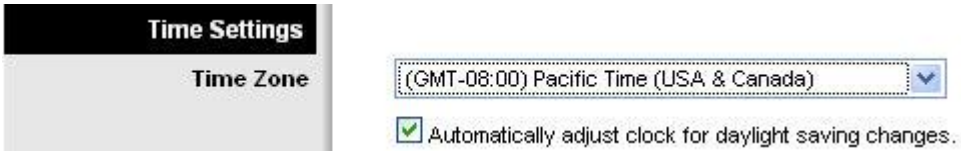


Avec ces paramètres, un PC qui se connectera sans fil à ce routeur et qui demandera une adresse IP via DHCP recevra une adresse comprise entre 172.17.30.50 et 74. Seuls 25 clients pourront obtenir une adresse IP en même temps et pour une durée de deux heures au plus, après quoi ils devront en demander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



Étape 6 : enregistrement des paramètres

Tâche 7 : paramètres sans fil de base

Étape 1 : définition du mode réseau

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 le champ Network Name (SSID), entrez RSF3. Dans le champ Standard Channel, entrez 6 – 2.437 GHZ, et désactivez l'option SSID Broadcast.

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

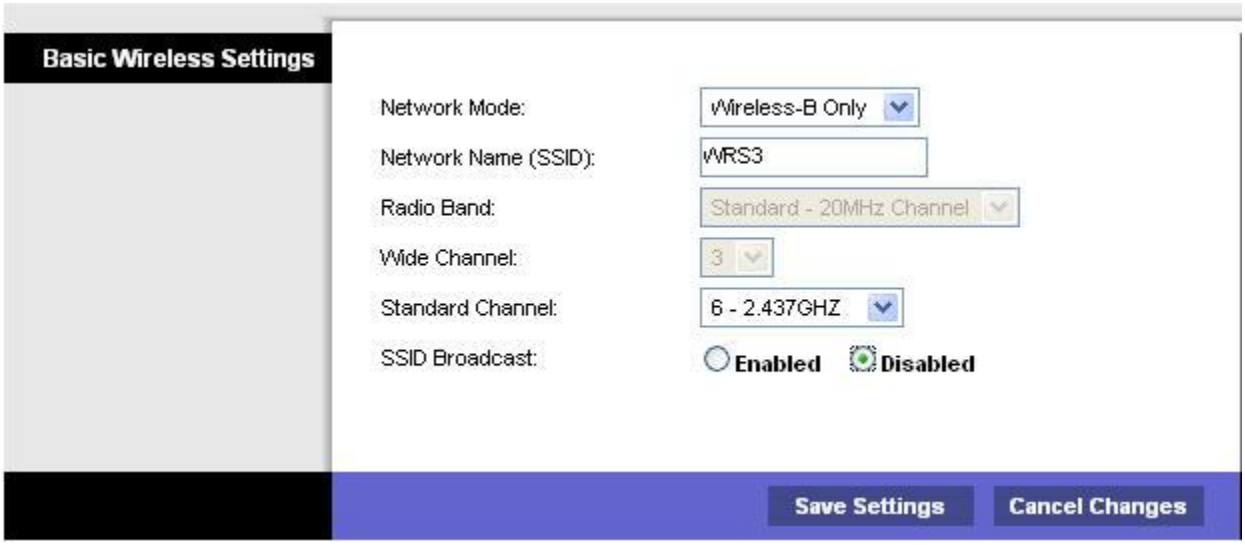
_____

_____

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

_____

_____



Étape 3 : enregistrement des paramètres

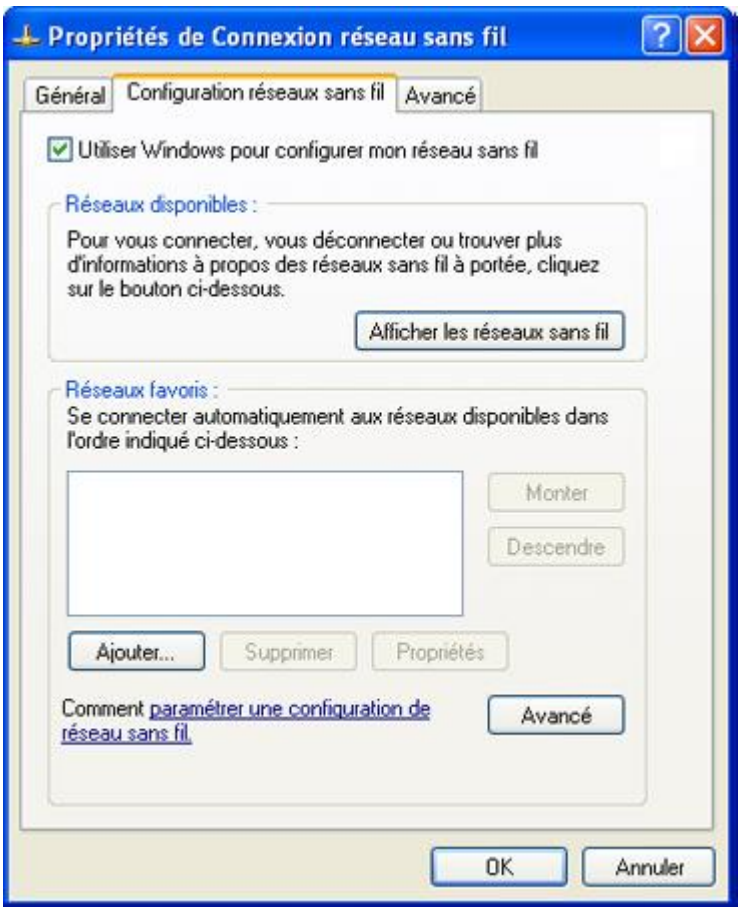
Étape 4 : vérification de la non-diffusion du SSID du routeur

Regardez la liste des réseaux sans fil (voir la Tâche 3, Étape 1). Le SSID du routeur sans fil est-il affiché ?_____

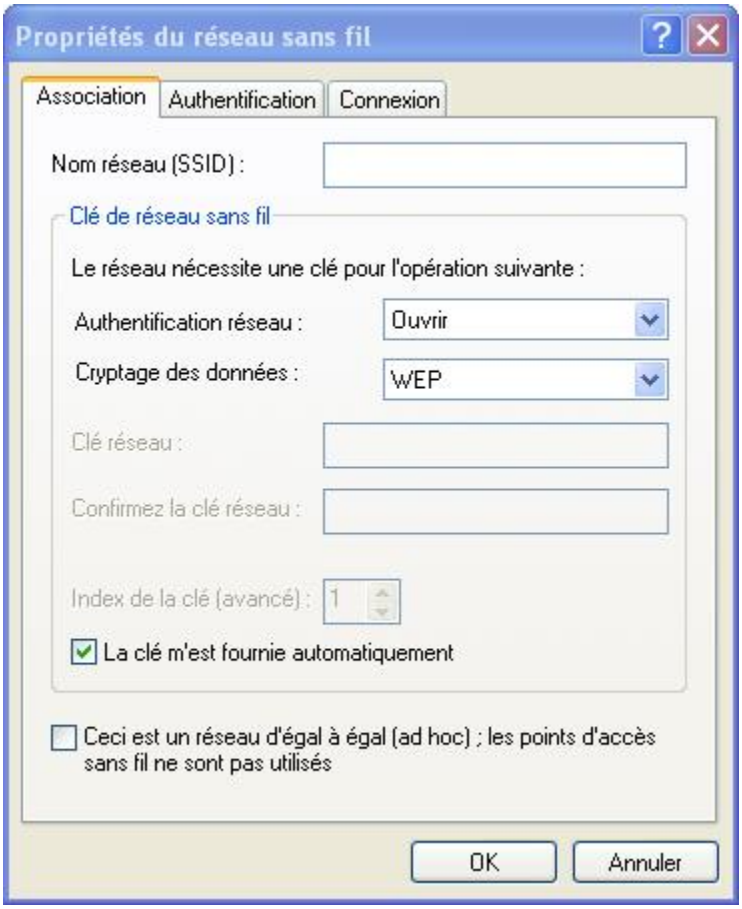
Étape 5 : reconnexion au réseau sans fil

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 RSF3 dans le champ Nom réseau (SSID) et sélectionnez Désactivé pour l'option Cryptage des données. Cliquez sur OK, puis une nouvelle fois sur OK. 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 5, Étape 3. Pour le vérifier, tapez **ipconfig** à l'invite de commande.

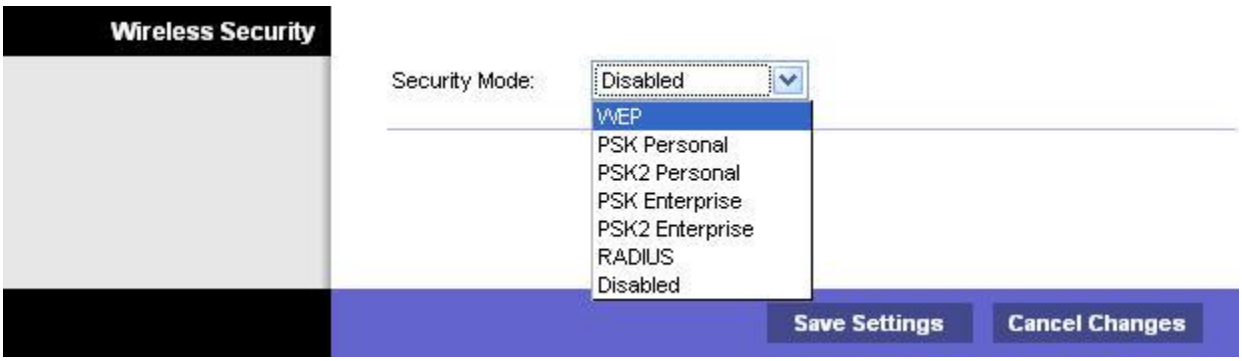
```
Adresse IP. . . . . . . . . . . . : 192.168.1.100
Masque de sous-réseau . . . . . . : 255.255.255.0
Passerelle par défaut . . . . . . : 192.168.1.1
```

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 : saisie de la clé WEP

La sécurité d'un réseau est égale à celle du point le plus vulnérable et un routeur sans fil est l'endroit idéal pour s'y introduire afin de l'endommager. 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. Il existe des outils de sécurité plus avancés, WPA et WPA-2, mais ils ne sont pas pris en charge actuellement sur ce routeur. Les filtres Wireless MAC sont plus sûrs mais parfois trop complexes à utiliser pour sécuriser votre réseau. Nous en parlerons dans la tâche qui suit.

Ajoutez la clé WEP 1234567890.

Étape 5 : enregistrement des paramètres

Vous allez être déconnecté du réseau.

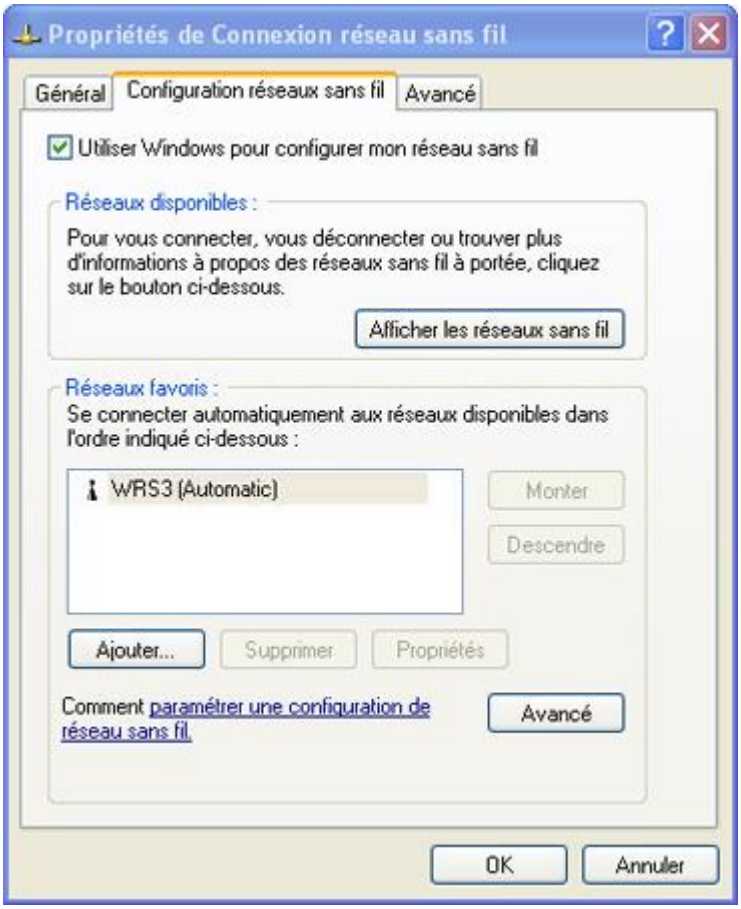
Étape 6 : configuration de Windows pour l'utilisation de l'authentification WEP

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 RSF3 et cliquez sur **Propriétés**.

Pour l'option Cryptage des données, choisissez WEP.

- Décochez la case La clé m'est fournie automatiquement.
- Tapez la clé de réseau 1234567890, qui était initialement configurée sur le routeur.
- Cliquez sur OK puis à nouveau sur OK.

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).
- Retrouvez la section Wireless puis l'onglet Wireless MAC Filter.
- Cochez la case Enabled.
- Sélectionnez **Prevent PCs listed below from accessing the wireless network**.
- Entrez l'adresse MAC 00:05:4E:49:64:87.

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

Étape 2 : sélection de la liste des clients sans fil

La zone **Wireless Client List** répertorie tout ce qui est actuellement connecté au routeur via une connexion sans fil. Remarquez l'option **Save to MAC filter list**. Quand vous cochez 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 ?

_____

_____

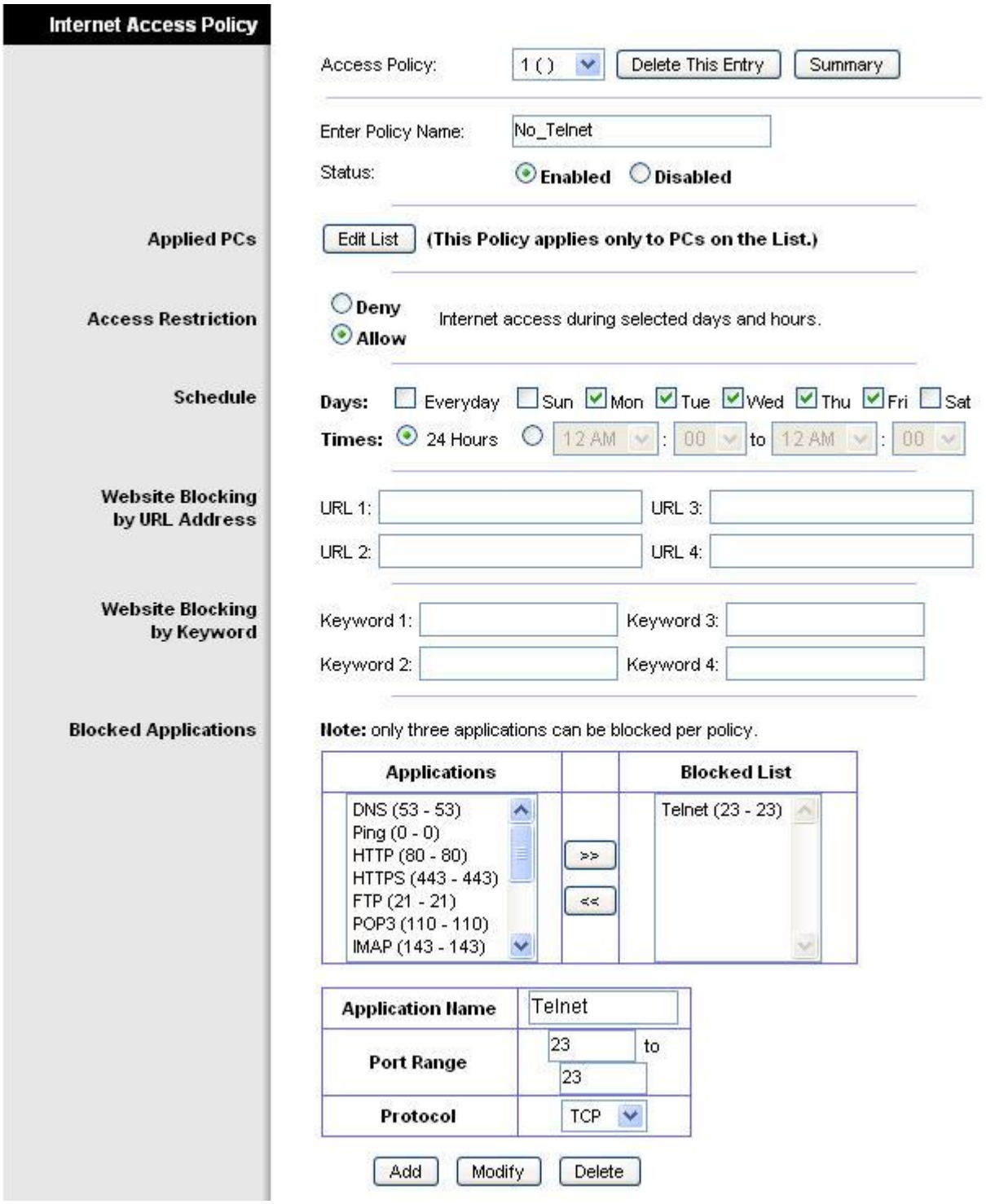
Tâche 10 : définition des restrictions d'accès

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

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

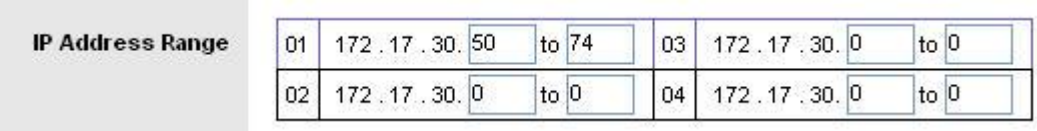
- Enter Policy Name : No_Telnet
- Status : Enabled
- Internet access during... : Allow
- Days : cochez de Monday à Friday.
- Blocked List : ajoutez Telnet.



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.



Enregistrez les paramètres de restriction d'accès.

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

Étape 1 : configuration de l'accès au Web

Recherchez 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.

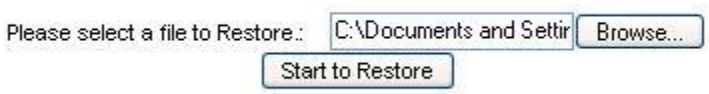
Dans la zone **Web Utility Access via Wireless,** sélectionnez Enabled. Si vous avez désactivé cette option, l'utilitaire Web ne sera pas accessible aux clients connectés sans fil. La désactivation de l'accès est une autre forme de sécurité qui demande à l'utilisateur de se connecter directement au routeur 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.

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

Étape 2 : restauration de la configuration

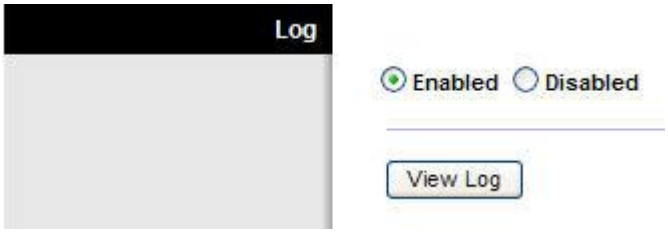
Si vos paramètres se perdent ou s'altèrent par accident ou malveillance, vous pouvez les restaurer depuis une configuration fonctionnelle à l'aide de l'option **Restore Configurations** située dans la section Backup and Restore.

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** et activez la journalisation. Vous pouvez maintenant consulter le journal du routeur.



Étape 4 : enregistrement des paramètres et arrêt de la connexion sans fil avec le routeur

Étape 5 : branchement d'un câble Ethernet sur l'un des ports réseau du routeur sans fil et connexion

Étape 6 : ouverture de l'interface Web du routeur

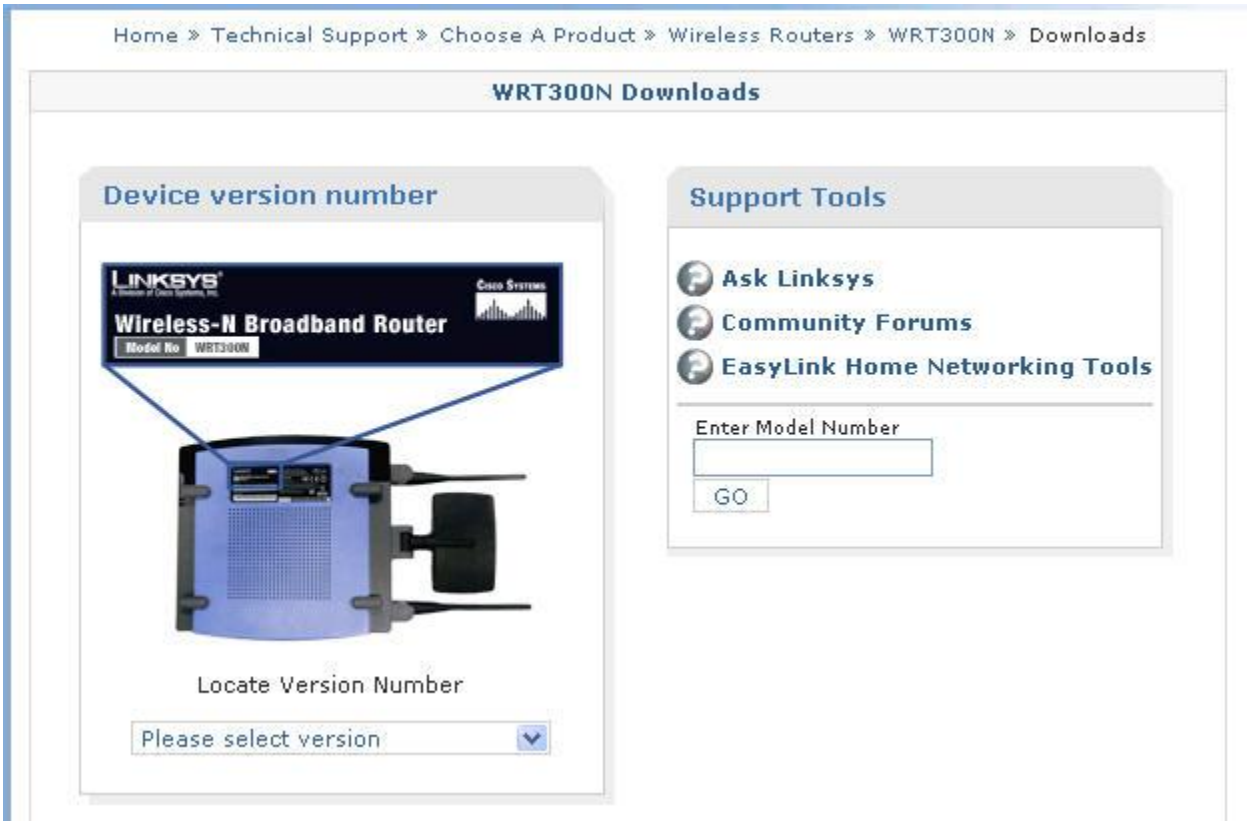
Étape 7 : recherche de la section Administration

Étape 8 : mise à jour du progiciel

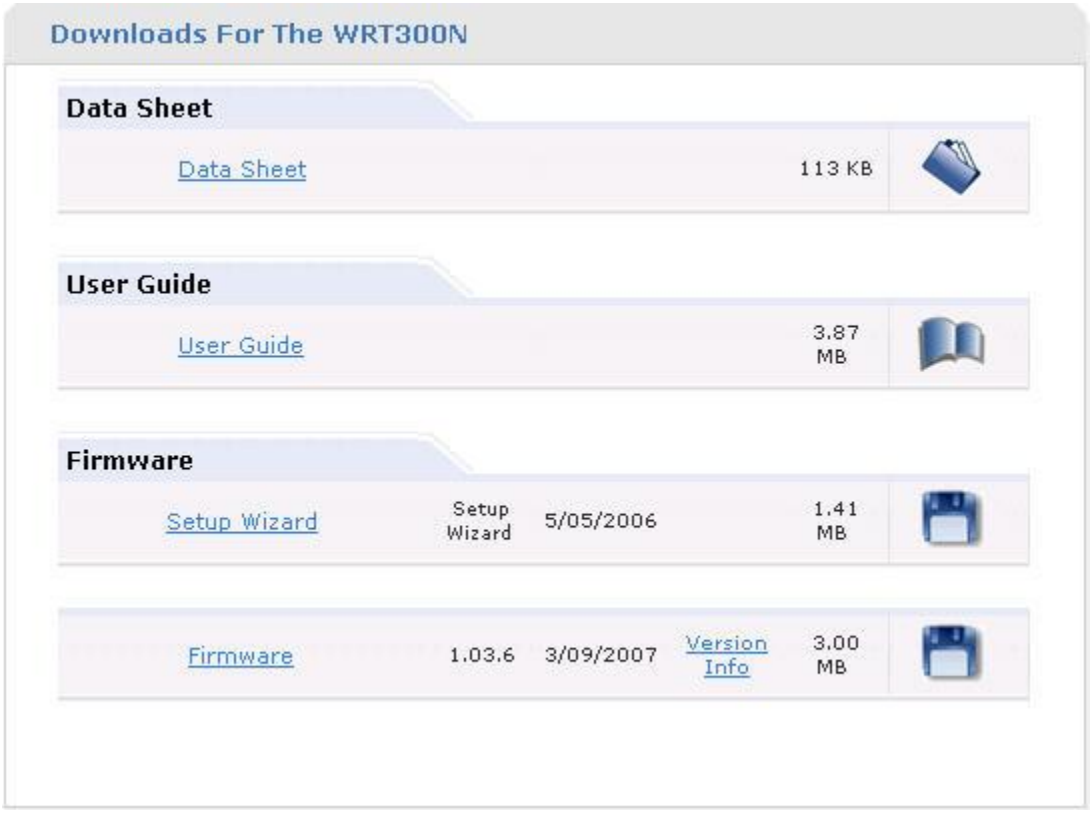
Accédez à la page :

http://www.linksys.com/servlet/Satellite?c=L_CASupport_C2&childpagename=US%2FLayout&cid=1166859841746&pagename=Linksys%2FCommon%2FVisitorWrapper&lid=4174637314B274&displaypage=download

Sélectionnez la version du routeur. Des instructions pour identifier la version sont disponibles sur le site Web de Linksys.

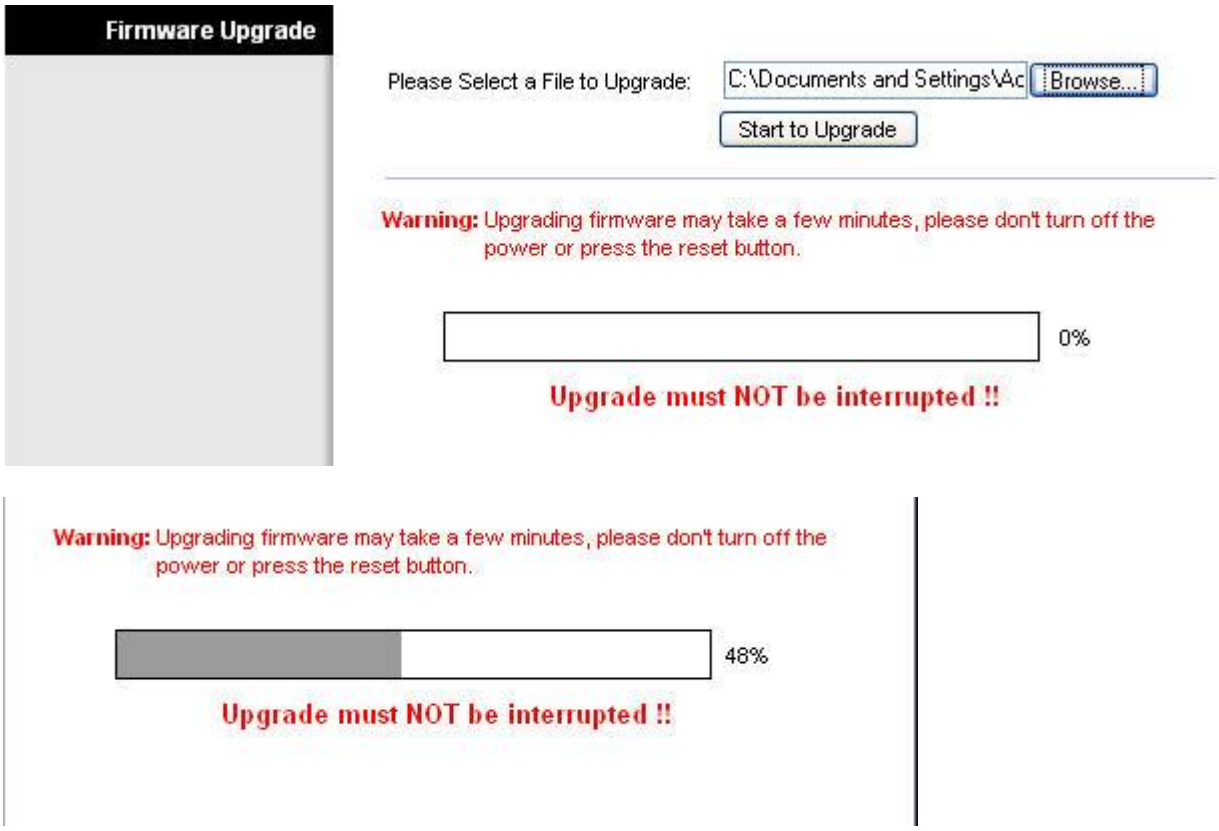


Cliquez sur **Firmware** ou sur l'icône de sauvegarde. Enregistrez le fichier sur le disque à l'invite.



Avant de procéder à la mise à niveau, notez la version du progiciel indiquée dans l'angle supérieur droit de l'écran.

Recherchez la section **Administration**. Cliquez sur **Upgrade Firmware**. Recherchez le fichier que vous venez de télécharger. Cliquez sur **Start to Upgrade**. La mise à niveau ne doit pas être interrompue. Veillez à ne pas éteindre l'appareil.

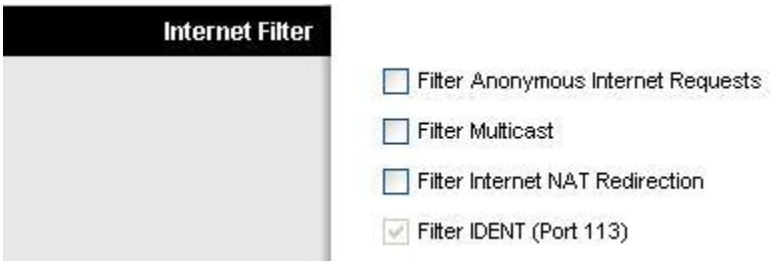


Une fois la mise à niveau terminée, vérifiez la nouvelle version du progiciel installée sur l'appareil.

Tâche 12 : établissement et vérification de la connectivité totale

Étape 1 : filtrage des requêtes Internet anonymes

Dans la section **Security**, décochez **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 RSF3 (172.17.30.1) depuis les nœuds connectés à son port WAN.



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

Dans la section **Setup**, cliquez sur l'onglet **Advanced Routing**. Désactivez la traduction d'adresses de réseau (NAT).

Étape 3 : connexion à RSF2

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

- Pour l'adresse IP, entrez 172.17.88.25.
- Pour le masque de sous-réseau, entrez 255.255.255.0.

Pour le paramètre Default Gateway, tapez l'adresse IP du VLAN 88 Fa 0/1 de R1 : 172.17.88.1.

Pour Network Setup, entrez l'adresse IP 172.17.30.1.

Établissez un lien statique entre l'adresse MAC de PC3 et l'adresse DHCP 172.17.40.23 (voir : Tâche 6, Étape 2).

Pour le SSID du réseau sans fil, entrez RSF2 (voir : Tâche 7, Étape 2).

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

```
R1config)#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 : reprise des étapes 1 et 2 pour RSF2

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.

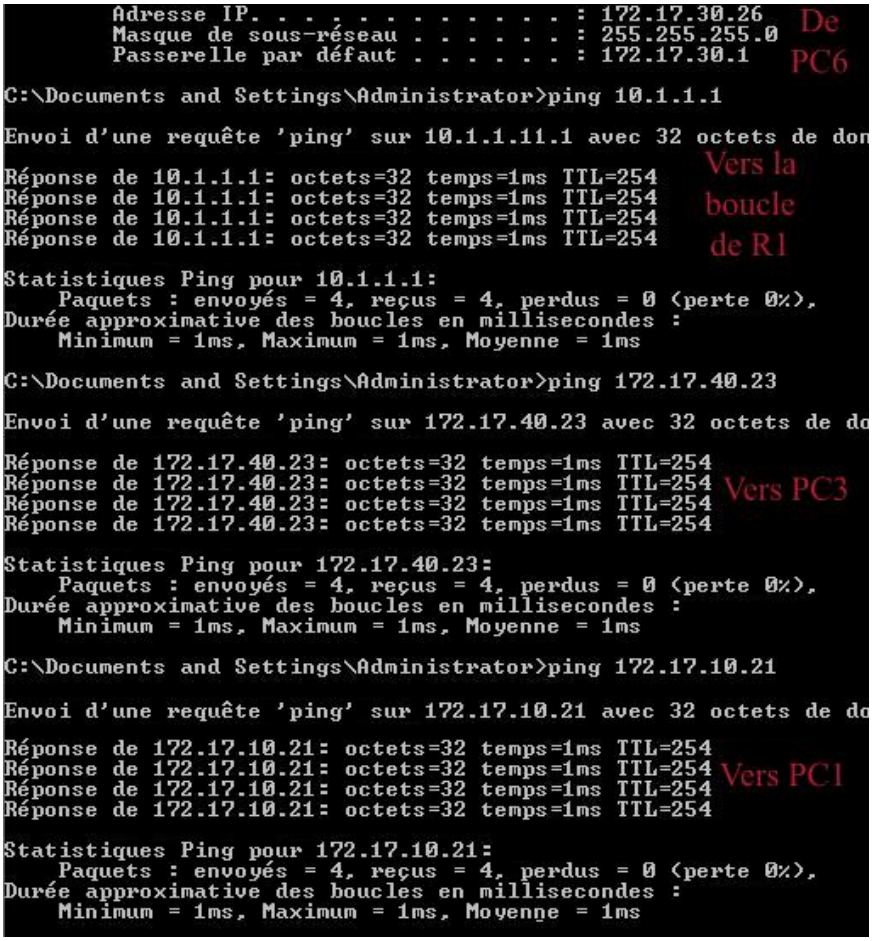
```
R1#sh ip route
<résultat omis>

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
     10.0.0.0/24 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.



Tâche 13 : configuration du routage

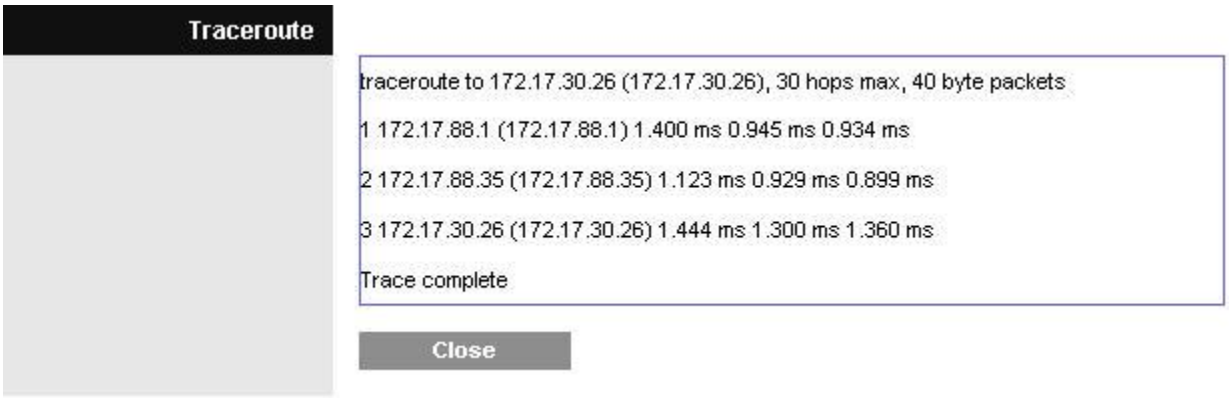
Étape 1 : utilisation de Traceroute pour voir la connexion réseau

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 RSF2 (172.17.88.25) vers la passerelle par défaut de RSF2 (172.17.88.1). Ensuite, R1 envoie le paquet à l'interface WAN de RSF3 (172.17.88.35) où RSF3 le prend en charge.

Vous pouvez le vérifier dans l'onglet **Diagnostics** de la section Administration. Dans le champ Traceroute Test, entrez l'adresse IP de PC6 à PC6, 172.17.30.26.

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

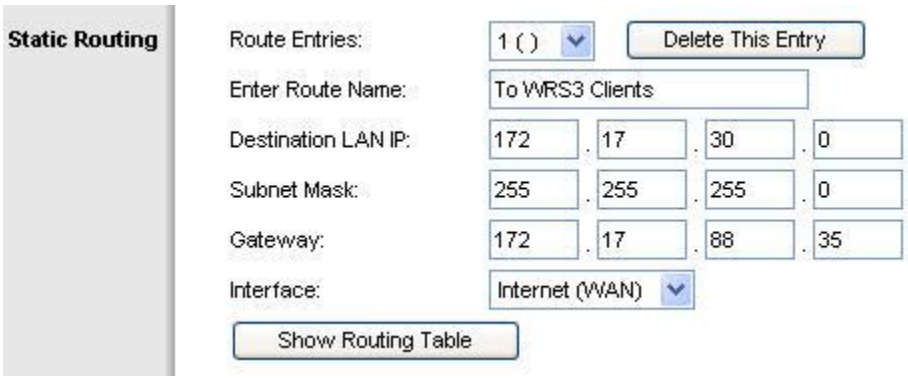


Si RSF2 savait qu'il pouvait accéder au réseau 172.17.30.0 depuis l'adresse 172.17.88.35, il enverrait le paquet directement à cette adresse IP. Alors dites-le lui !

Étape 2 : configuration d'une nouvelle route

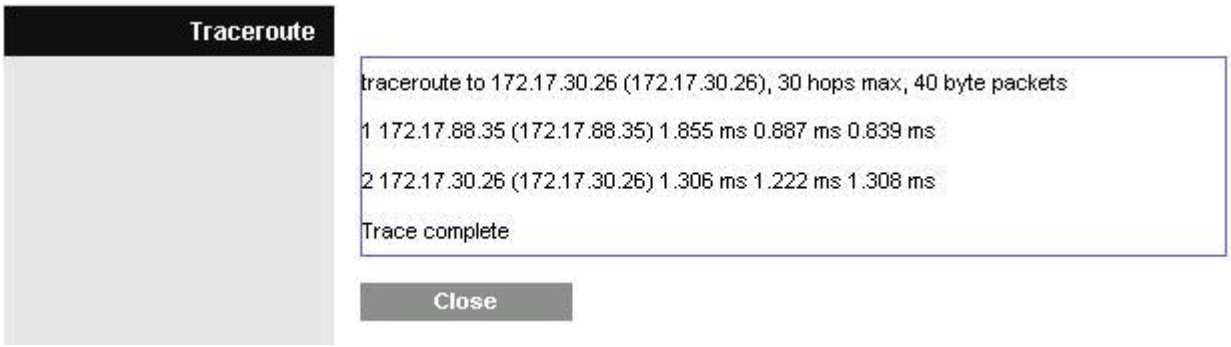
Dans la section **Setup**, cliquez sur l'onglet **Advanced Routing**. Pour la section Static Routing, entrez les paramètres suivants :

- Dans le champ **Route Name**, entrez **To RSF2 Clients**.
- Dans le champ **Destination LAN IP**, entrez l'adresse du réseau situé derrière RSF2 : 172.17.40.0
- Entrez le masque de sous-réseau /24.
- Entrez l'adresse de passerelle 172.17.88.35.
- Dans le champ Interface, entrez Internet (WAN).



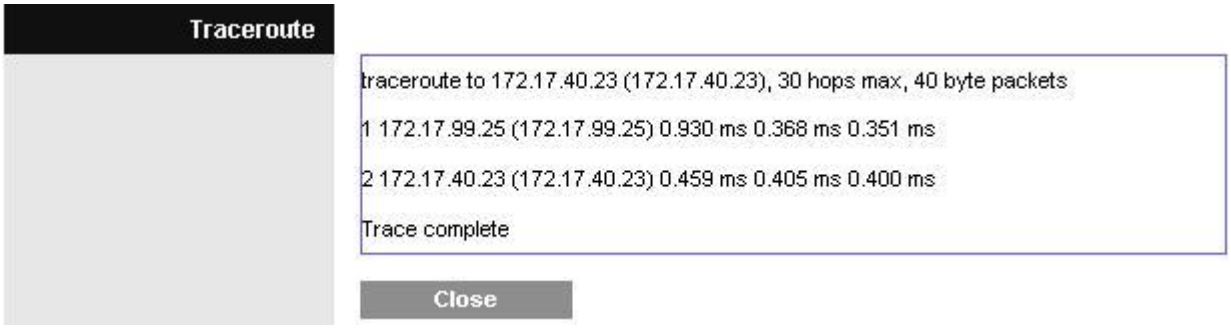
Étape 3 : vérification de la nouvelle route

Dans 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 RSF2 va directement à RSF3 sans passer par R1.

Faites la même chose pour RSF3 avec le réseau 172.17.40.0/24 en pointant vers l'interface WAN de RSF2 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 Comm2. Configurez le port de commutateur 11 de PC1, activez la sécurité des ports et activez les adresses permanentes MAC dynamiques.

Étape 2 : configuration de la sécurité des ports de PC2

Répétez l'étape 1 pour le port de commutateur 18.

```
Comm2

!
interface FastEthernet 0/11
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security mac-address sticky
 no shutdown
!
!
interface FastEthernet 0/18
 switchport mode access
 switchport access vlan 20
 switchport port-security
 switchport port-security mac-address sticky
 no shutdown
!
```

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

Étape 4 : vérification de la sécurité des ports

```
Comm1#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

Comm1#sh port-security int fa 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
```

Annexe

Configurations

Hostname R1

```
!
enable secret class
!
no ip domain lookup
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1.88
 encapsulation dot1Q 88
 ip address 172.17.88.1 255.255.255.0
!
!
ip route 172.17.30.0 255.255.255.0 172.17.88.35
ip route 172.17.40.0 255.255.255.0 172.17.88.25
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 password cisco
line aux 0
line vty 0 4
!
!
end
```

Hostname Comm1

```
!
!
vtp mode transparent
!
!
```

```
vlan 10,20,88
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

Hostname Comm2

```
!
!
vtp mode transparent
!
vlan 10,20,88
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
!
interface FastEthernet0/7
 switchport mode access
 switchport access vlan 88
!
!
! PC1 and PC2's MAC address will appear after 'sticky' on ports 11
! and 18 respectively, after traffic traverses them
!
!

interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky ffff.ffff.ffff
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky ffff.ffff.ffff
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

Hostname Comm3

```
!
vtp mode transparent
!
vlan 10,20,88
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
!
interface FastEthernet0/7
 switchport mode access
 switchport access vlan 88
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
!
end
```

Travaux pratiques 7.5.3 : résolution des incidents liés au WRT300N sans fil

Diagramme de topologie

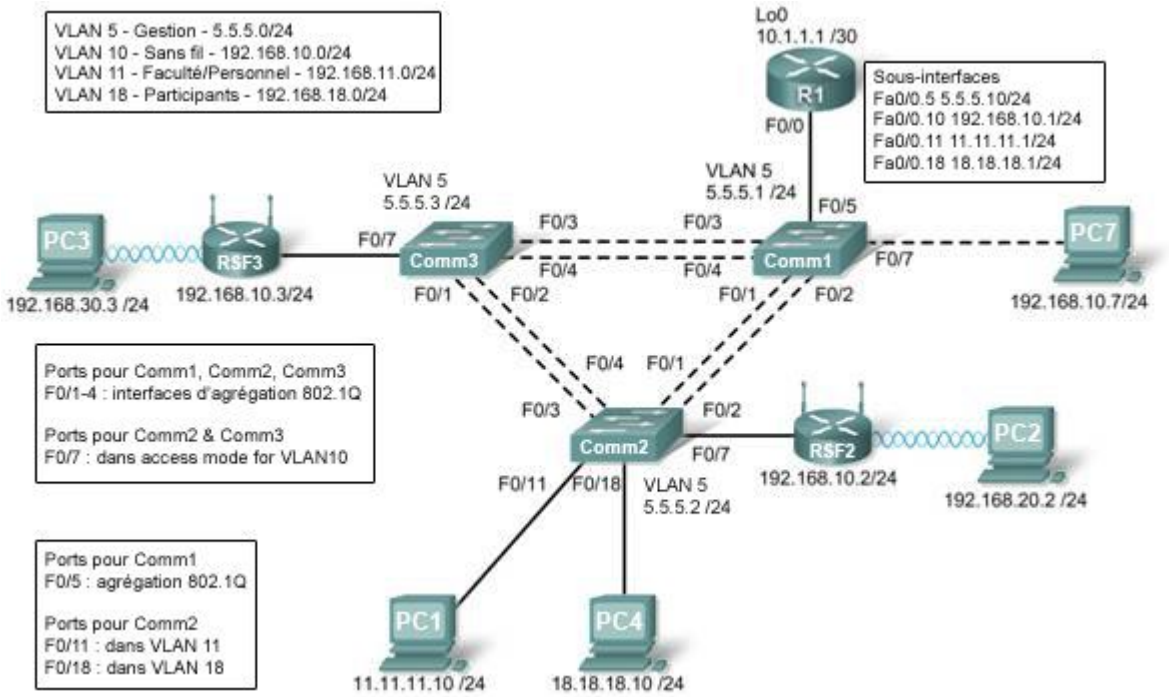


Tableau d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/1.5**	5.5.5.10	255.255.255.0	S/O
	Fa0/1.10	192.168.10.1	255.255.255.0	S/O
	Fa0/1.11	11.11.11.1	255.255.255.0	S/O
	Fa0/1.18	18.18.18.1	255.255.255.0	S/O
	Lo0	10.1.1.1	255.255.255.252	S/O
RSF2	**Réseau étendu**	192.168.10.2	255.255.255.0	192.168.10.1
	Réseau local/sans fil	192.168.20.1	255.255.255.0	S/O
RSF3	**Réseau étendu**	192.168.10.3	255.255.255.0	192.168.10.1
	Réseau local/sans fil	192.168.30.1	255.255.255.0	S/O

PC1	**Carte réseau**	11.11.11.10	255.255.255.0	11.11.11.1
PC4	**Carte réseau**	18.18.18.10	255.255.255.0	18.18.18.1
Comm1	**VLAN 5**	5.5.5.1	255.255.255.0	S/O
Comm2	**VLAN 5**	5.5.5.2	255.255.255.0	S/O
Comm3	**VLAN 5**	5.5.5.3	255.255.255.0	S/O

Scénario

Un réseau simple et un réseau sans fil ont été configurés d'une manière incorrecte. Vous devez rechercher et corriger les erreurs de configuration sur la base des spécifications de réseau minimales fournies par votre entreprise.

Voici les configurations que vous devez charger dans le routeur et dans les commutateurs.

Configuration de R1

```
hostname R1
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1.5
 encapsulation dot1Q 5
 ip address 5.5.5.10 255.255.255.0
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.11.1 255.255.255.0
!
interface FastEthernet0/1.18
 encapsulation dot1Q 18
 ip address 18.18.18.1 255.255.255.0
!
ip route 192.168.20.0 255.255.255.0 192.168.10.2
ip route 192.168.30.0 255.255.255.0 192.168.10.3
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

Configuration du commutateur 1

```
hostname Comm1
!
vtp mode transparent
!
vlan 5,10-11
vlan 18
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan5
 ip address 5.5.5.1 255.255.255.0
 no shutdown
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
End
```

Configuration du commutateur 2

```
hostname Comm2
!
vtp mode transparent
ip subnet-zero
!
vlan 5,10-11,18
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode access
```

```
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode access
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode access
!
interface FastEthernet0/7
switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 switchport mode trunk
!
interface FastEthernet0/11
 switchport access vlan 11
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0336.5b1e.33fa
!
interface FastEthernet0/18
 switchport access vlan 18
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 022c.ab13.22fb
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan5
 ip address 5.5.5.2 255.255.255.0
 no shutdown
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
End
```

Configuration du commutateur 3

```
hostname Comm3
!
vtp mode transparent
!
vlan 5,10-11,18
!
```

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,10,11,18
 switchport mode trunk
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan5
 ip address 6.6.6.3 255.255.255.0
 no shutdown
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
end
```

Spécifications de réseau du routeur sans fil

En corrigeant la configuration de RSF2 et RSF3, vérifiez que les conditions suivantes sont satisfaites :

1. Connexions via les adresses IP indiquées dans le diagramme de topologie.
2. Plus de 30 clients peuvent obtenir une adresse IP simultanément via DHCP.
3. Un client peut obtenir une adresse DHCP pour au moins deux heures.
4. Les clients qui utilisent à la fois les modes réseau sans fil B et G peuvent se connecter mais pas les clients N.
5. Les clients sans fil doivent s'authentifier avec le protocole WEP et la clé 5655545251.
6. Le trafic entre PC2 et PC3 doit emprunter la route la plus économique.
7. Les requêtes ping provenant des ports WAN externes des routeurs Linksys et dirigées vers les adresses IP réseau local/sans fil (192.168.30.1) doivent aboutir.
8. Le protocole DHCP ne doit pas délivrer d'adresses IP comprises dans un intervalle incluant les adresses de PC2 et PC3.
9. Les deux réseaux sans fil ne doivent pas interférer l'un avec l'autre.

Solution réseau sans fil