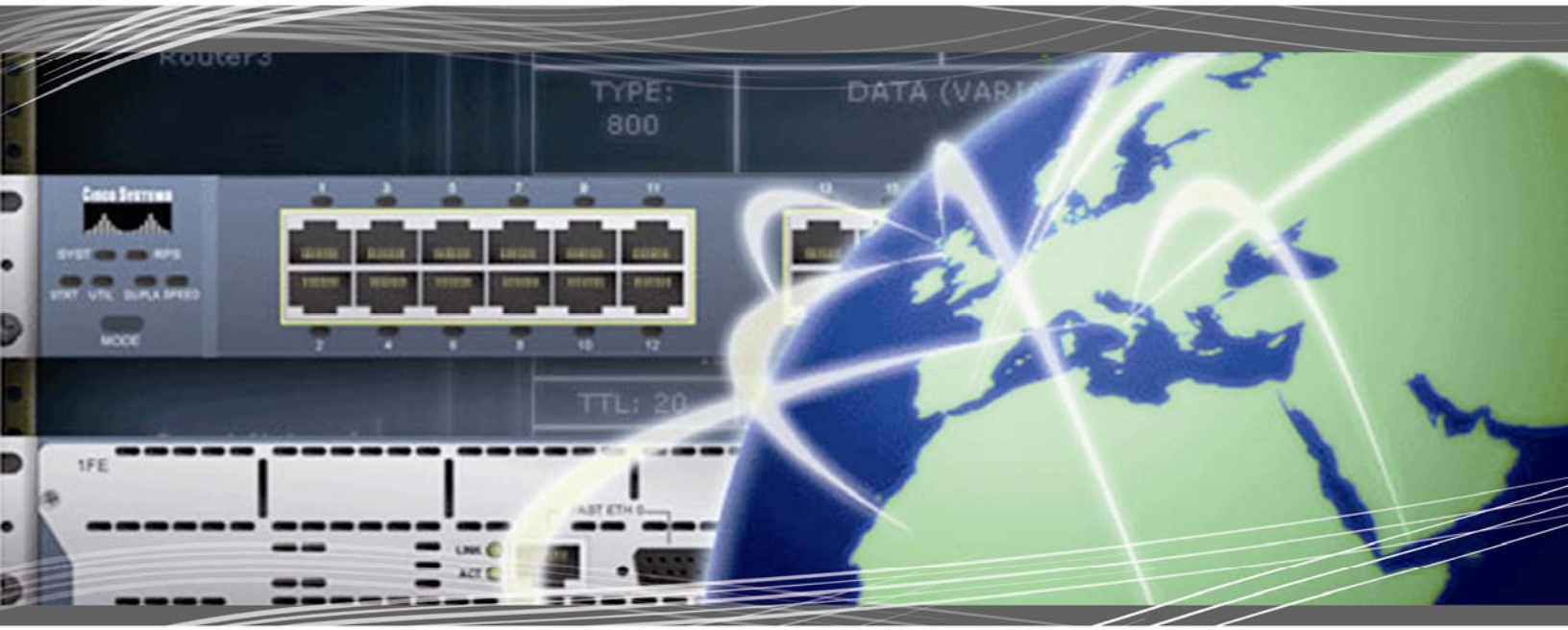
Cisco | Networking Academy®
Mind Wide Open™



CCNA Exploration 4.0

Accès au réseau étendu

Manuel de travaux pratiques Packet Tracer du participant

Exercice PT 1.5.1 : exercice d'intégration des compétences Packet Tracer

Diagramme de topologie

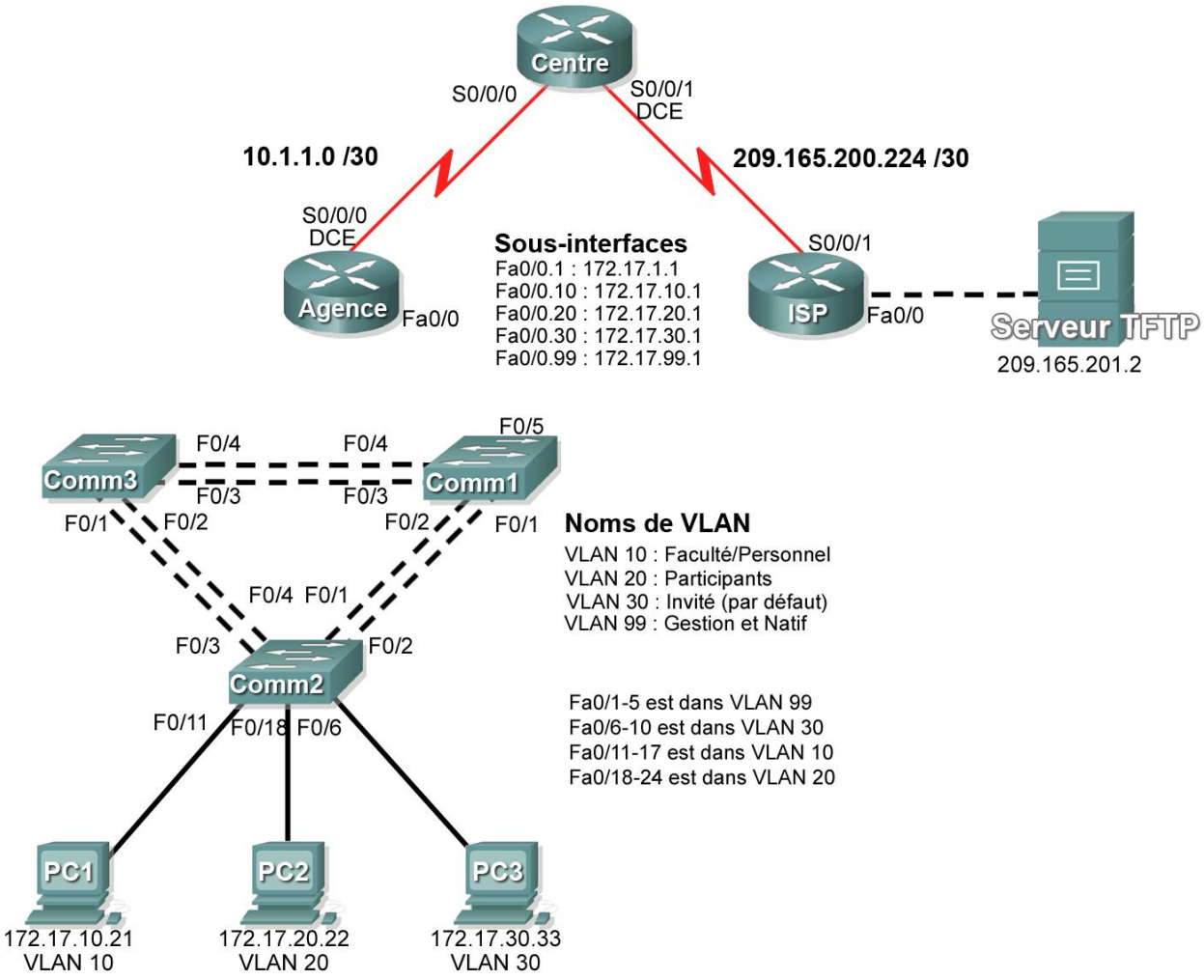


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
FAI	**S0/0/1**	209.165.200.225	255.255.255.252	N/D
	Fa0/0	209.165.201.1	255.255.255.252	N/D
CENTRE	**S0/0/0**	10.1.1.2	255.255.255.252	N/D
	S0/0/1	209.165.200.226	255.255.255.252	N/D
AGENCE	**S0/0/0**	10.1.1.1	255.255.255.252	N/D
	Fa0/0.1	172.17.1.1	255.255.255.0	N/D
	Fa0/0.10	172.17.10.1	255.255.255.0	N/D
	Fa0/0.20	172.17.20.1	255.255.255.0	N/D
	Fa0/0.30	172.17.30.1	255.255.255.0	N/D
	Fa0/0.99	172.17.99.1	255.255.255.0	N/D
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
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 Web	**Carte réseau**	209.165.201.2	255.255.255.252	209.165.201.1

Objectifs pédagogiques

- Configurer le routage statique et par défaut
- Ajouter et connecter le routeur AGENCE
- Ajouter et connecter les commutateurs
- Ajouter et connecter les PC
- Effectuer une configuration de périphérique de base
- Configurer le routage OSPF
- Configurer le STP
- Configurer le VTP
- Configurer des réseaux locaux virtuels
- Vérifier la connectivité de bout en bout

Présentation

Cet exercice aborde plusieurs des compétences que vous avez acquises lors des trois premiers cours Exploration : construction d'un réseau, application d'un schéma d'adressage, configuration du routage, de réseaux locaux virtuels, de STP et de VTP et test de la connectivité. Revoyez ces compétences avant de poursuivre. En outre, cet exercice vous offre l'occasion de réviser les bases du programme Packet Tracer. Packet Tracer est intégré à l'ensemble de ce cours. Afin de mener à bien ce cours, vous devez savoir comment naviguer dans l'environnement Packet Tracer. Utilisez les didacticiels pour réviser les bases de Packet Tracer, si nécessaire. Les didacticiels se trouvent dans le menu **Help** (Aide) de Packet Tracer.

Remarque : plus de 150 éléments sont évalués au cours de cet exercice. Par conséquent, vous ne verrez peut-être pas le pourcentage augmenter à chaque fois que vous entrerez une commande. Le mot de passe d'exécution utilisateur est **cisco** et le mot de passe d'exécution privilégié est **class**.

Tâche 1 : configuration du routage statique et par défaut

Étape 1. Configuration du routage statique de FAI à CENTRE

Utilisez le diagramme de topologie pour configurer FAI avec des routes statiques vers tous les réseaux. Chaque réseau est accessible via S0/0/1 à partir de FAI. Le paramètre d'interface de sortie vous permet de configurer des routes statiques vers les réseaux suivants :

- 10.1.1.0/30
- 172.17.1.0/24
- 172.17.10.0/24
- 172.17.20.0/24
- 172.17.30.0/24
- 172.17.99.0/24

Étape 2. Configuration du routage par défaut de CENTRE à FAI

Configurez une route par défaut sur CENTRE à l'aide du paramètre d'interface de sortie pour envoyer tout le trafic par défaut vers FAI.

Étape 3. Test de la connectivité au serveur Web

CENTRE doit maintenant être en mesure d'envoyer une requête ping au serveur Web à l'adresse 209.165.201.2.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 4 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : ajout et connexion du routeur AGENCE

Étape 1. Ajout du routeur AGENCE

Cliquez sur **Custom Made Devices** et ajoutez un routeur 1841 à la topologie. à partir de l'onglet **Config**, modifiez les champs Display Name et Hostname en AGENCE. Les noms affichés sont sensibles à la casse.

Étape 2. Connexion de AGENCE à CENTRE

- Connectez AGENCE à CENTRE.
- Configurez la liaison entre AGENCE et CENTRE.
- Utilisez une fréquence d'horloge de **64 000** bits/s.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 8 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : ajout et connexion des commutateurs

Reportez-vous à la topologie pour les emplacements, les noms de commutateurs et les interfaces.

Étape 1. Ajout des commutateurs Comm1, Comm2 et Comm3 à l'aide du modèle 2960

Étape 2. Connexion de Comm1 à AGENCE

Étape 3. Connexion de Comm1 à Comm2

Étape 4. Connexion de Comm1 à Comm3

Étape 5. Connexion de Comm2 à Comm3

Étape 6. Vérification des résultats

Votre taux de réalisation doit être de 28 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : ajout et connexion des PC

Utilisez les interfaces indiquées dans le diagramme de topologie et la table d'adressage.

Étape 1. Ajout de PC1, PC2 et PC3

Étape 2. Connexion de PC1, PC2 et PC3 à Comm2

Étape 3. Configuration des PC

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 41 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 5 : configuration de base d'un périphérique

Étape 1. Configuration des commandes de base sur AGENCE, Comm1, Comm2 et Comm3

Les commandes de configuration de base doivent inclure le nom d'hôte, le mot de passe d'exécution privilégié, la bannière, la console et les lignes vty.

Étape 2. Configuration des sous-interfaces Fast Ethernet sur AGENCE

Pensez à configurer l'encapsulation 802.1q et les paramètres de réseaux locaux virtuels pour chaque sous-interface. Le troisième octet de l'adresse de chaque sous-interface correspond au numéro de réseau local virtuel (VLAN). Par exemple, la sous-interface Fa0/0.30 utilise l'adresse IP 172.17.**30**.1 et appartient au VLAN 30. VLAN 99 est le VLAN natif.

Étape 3. Configuration des commutateurs

- Configurez l'interface de VLAN 99.
- Configurez la passerelle par défaut.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 60 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 6 : configuration du routage OSPF

Étape 1. Configuration d'OSPF sur CENTRE et propagation de la route par défaut

- Configurez OSPF à l'aide de l'ID de processus 1.
- Utilisez la zone 0 d'OSPF
- Ajoutez uniquement le réseau partagé avec AGENCE.
- Transmettez les informations de route par défaut aux voisins OSPF.

Étape 2. Configuration d'OSPF sur AGENCE

- Configurez OSPF à l'aide de l'ID de processus 1.
- Utilisez la zone 0 d'OSPF
- Ajoutez tous les réseaux routés par AGENCE.

Étape 3. Désactivation des mises à jour OSPF sur les interfaces adéquates à la fois sur CENTRE et sur AGENCE

Désactivez les mises à jour OSPF sur toutes les interfaces de réseau local et vers FAI.

Étape 4. Test de connectivité

AGENCE doit maintenant être en mesure d'envoyer une requête ping au serveur Web à l'adresse 209.165.201.2.

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 69 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 7 : configuration du protocole STP

Étape 1. Définition de Comm1 comme pont racine

Définissez les priorités à 4096.

Étape 2. Vérification que Comm1 est le pont racine

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 72 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 8 : configuration du protocole VTP

Étape 1. Configuration du mode VTP sur les trois commutateurs

Configurez Comm1 en tant que serveur. Configurez Comm2 et Comm3 en tant que clients.

Étape 2. Configuration du nom de domaine VTP sur les trois commutateurs

Utilisez **CCNA** comme nom de domaine VTP.

Étape 3. Configuration du mot de passe de domaine VTP sur les trois commutateurs

Utilisez **cisco** comme mot de passe de domaine VTP.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 77 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 9 : configuration de l'agrégation

Étape 1. Configuration de l'agrégation sur Comm1, Comm2 et Comm3

Configurez les interfaces adéquates dans le mode d'agrégation et définissez VLAN 99 comme VLAN natif.

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 94 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 10 : configuration des réseaux locaux virtuels

Étape 1. Configuration de Comm1 avec des réseaux locaux virtuels.

Les noms des réseaux locaux virtuels sont sensibles à la casse. Ajoutez les quatre réseaux locaux virtuels et donnez-leur des noms suivant les indications suivantes :

- VLAN 10 : **Enseignants/personnel**
- VLAN 20 : **Étudiants**
- VLAN 30 : **Invité(défaut)**
- VLAN 99 : **Gestion&natif**

Étape 2. Vérification que Comm2 et Comm3 ont reçu de Comm1 les configurations VLAN.

Étape 3. Configuration pour l'accès des ports reliés aux PC sur Comm2 et affectation de chaque port au réseau local virtuel qui convient.

Étape 4. Vérification des résultats.

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 11 : vérification de la connectivité de bout en bout

Étape 1. Vérification que PC1, PC2 et PC3 peuvent envoyer des requêtes ping l'un vers l'autre.

Étape 2. Vérification que PC1, PC2 et PC3 peuvent envoyer une requête ping vers le serveur Web.

Exercice PT 2.1.7 : dépannage d'une interface série

Diagramme de topologie

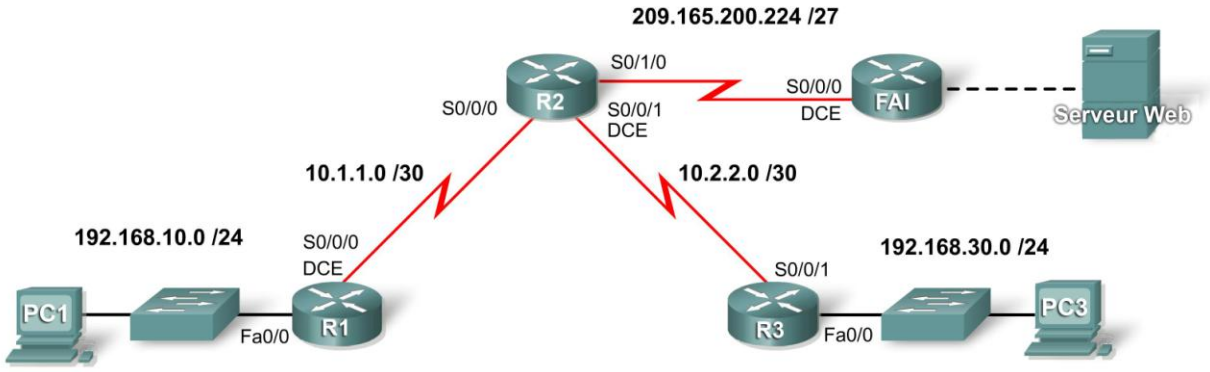


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	Fa0/0Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0S0/1/0	209.165.200.225	255.255.255.224
R3	Fa0/0Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0S0/0/0	10.2.2.2	255.255.255.252
FAI	S0/0/0S0/0/0	209.165.200.226	255.255.255.224
	Fa0/0Fa0/0	209.165.200.1	255.255.255.252
Serveur Web	Carte réseau	209.165.200.2	255.255.255.252
PC1	Carte réseau	192.168.10.10	255.255.255.0
PC3	Carte réseau	192.168.30.10	255.255.255.0

Objectifs pédagogiques

- Tester la connectivité
- Étudier les problèmes de connectivité en recueillant des données
- Mettre en place la solution et tester la connectivité

Présentation

Dans cet exercice, vous avez accès uniquement à la ligne de commande sur PC1 et PC3. Pour résoudre les problèmes sur les routeurs et pour mettre en œuvre les solutions, vous devez utiliser une connexion Telnet à partir de PC1 ou PC3. L'exercice est terminé lorsque vous obtenez 100 % et lorsque PC1 peut envoyer une requête ping à PC3.

Tâche 1 : test de la connectivité

Étape 1 : utilisation de la commande ping pour tester la connectivité de bout en bout

Attendez que les voyants orange de liaison sur Comm1 et sur Comm3 passent au vert. Envoyez ensuite une requête ping à PC3 à partir de la ligne de commande sur PC1. Ce ping doit échouer.

Étape 2 : utilisation de traceroute pour rechercher le point où la connectivité échoue

Sur la ligne de commande sur PC1, utilisez la commande **tracert** pour identifier l'origine de l'échec de la connectivité.

```
Packet Tracer PC Command Line 1.0
PC>tracert 192.168.30.10
```

Quittez la commande **tracert** à l'aide de la combinaison de touches Ctrl-C. Quel est le dernier routeur qui réponde à la commande **tracert** ? _____

Étape 3 : description des symptômes du problème

_____

_____

Tâche 2 : collecte de données sur le problème

Étape 1 : accès au dernier routeur qui réponde au paquet traceroute

Utilisez une connexion Telnet pour accéder au dernier routeur ayant répondu à **tracert**. Définissez **cisco** comme mot de passe Telnet et **class** comme mot de passe enable.

Étape 2 : utilisation de commandes de dépannage pour rechercher la raison pour laquelle ce routeur ne transfère pas la trace au saut suivant

Isolez les problèmes spécifiques avec l'interface série à l'aide des commandes suivantes :

- **show ip interface brief**
- **show interface serial**
- **show controllers serial**

La commande **show ip interface brief** indique si une interface a été configurée correctement et si elle a été mise en service correctement à l'aide de la commande **no shutdown**.

La commande **show interface serial** donne plus d'informations sur l'interface qui est en échec. Elle renvoie l'un des cinq états possibles :

- L'interface série x est down (désactivée) et le protocole de ligne est down (désactivé)
- L'interface série x est up (activée) et le protocole de ligne est down (désactivé)
- L'interface série x est up (activée) et le protocole de ligne est up (activé) (en boucle)
- L'interface série x est up (activée) et le protocole de ligne est down (désactivé)
- L'interface série x est administratively down (désactivée au niveau administratif) et le protocole de ligne est down (désactivé)

La commande **show interface serial** indique également le type d'encapsulation utilisée sur l'interface. Pour cet exercice, tous les routeurs doivent utiliser une encapsulation HDLC.

La commande **show controllers serial** indique l'état des canaux de l'interface et signale la présence ou l'absence d'un câble.

Vous devrez peut-être contrôler également la configuration sur le routeur connecté pour détecter le problème.

Étape 3 : description du problème et solutions proposées

Quelles sont des raisons possibles d'un échec de liaison série ?

_____

_____

_____

Tâche 3 : mise en œuvre de la solution et test de la connectivité

Étape 1 : modifications selon la solution proposée à la tâche 2

Étape 2 : utilisation de la commande ping pour tester la connectivité de bout en bout

À partir de la ligne de commande du routeur ou de PC1, utilisez les commandes **ping** et **tracert** pour tester la connectivité vers PC3.

Si la requête ping échoue, revenez à la tâche 2 pour poursuivre la recherche de problèmes. Vous devrez peut-être commencer votre dépannage à partir de PC3.

Étape 3 : vérification des résultats

Cliquez sur **Check Results**, puis **cliquez** sur l'onglet **Connectivity Tests**. Le test de connectivité doit maintenant réussir.

Étape 4 : résumé des résultats de vos recherches

Problème 1 : _____

Solution 1 : _____

Problème 2 : _____

Solution 2 : _____

Problème 3 : _____

Solution 3 : _____

Exercice PT 2.3.4 : configuration d'encapsulations point à point

Diagramme de topologie

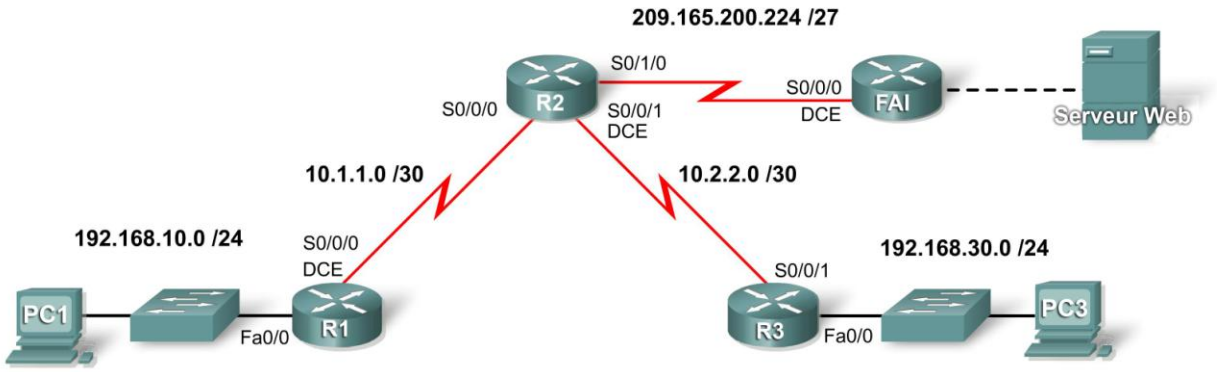


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
R2	**S0/0/0**	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
	S0/1/0	209.165.200.225	255.255.255.252	N/D
R3	**Fa0/0**	192.168.30.1	255.255.255.0	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
FAI	**S0/0/0**	209.165.200.226	255.255.255.252	N/D
	Fa0/0	209.165.200.1	255.255.255.252	N/D
Serveur Web	**Carte réseau**	209.165.200.2	255.255.255.252	209.165.200.1
PC1	**Carte réseau**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**Carte réseau**	192.168.30.10	255.255.255.0	192.168.30.1

Objectifs pédagogiques

- Vérifier les configurations de routage
- Configurer la méthode d'encapsulation PPP
- Configurer la méthode d'encapsulation HDLC

Tâche 1 : vérification des configurations de routage

Étape 1. Affichage des configurations en cours de tous les routeurs

Prenez note des configurations de routage, à la fois statique et dynamique. Vous allez configurer les deux types de routage dans l'exercice d'intégration des compétences Packet Tracer à la fin de ce chapitre.

Étape 2. Test de la connectivité entre les PC et le serveur Web

1. Ouvrez une ligne de commande à partir de PC1.
2. Envoyez la commande **ping 209.165.200.2**
3. Répétez cette étape pour PC3.

Les deux commandes **ping** doivent réussir. Veillez à accorder suffisamment de temps à STP et OSPF pour converger.

Tâche 2 : configuration de la méthode d'encapsulation PPP

Étape 1. Configuration de R1 pour utiliser l'encapsulation PPP avec R2

```
R1(config)#interface serial0/0/0
R1(config-if)#encapsulation ppp
```

Étape 2. Configuration de R2 pour utiliser l'encapsulation PPP avec R1 et R3

Étape 3. Configuration de R3 pour utiliser l'encapsulation PPP avec R2

Étape 4. Test de la connectivité entre les PC et le serveur Web

Pourquoi OSPF doit-il converger après la modification d'encapsulation ?

_____

_____

_____

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 67 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration de la méthode d'encapsulation HDLC

Étape 1. Configuration de FAI pour utiliser l'encapsulation HDLC avec R2

```
FAI(config)#interface serial0/0/0
FAI(config-if)#encapsulation hdlc
FAI(config-if)#no shutdown
```

Étape 2. Configuration de R2 pour utiliser l'encapsulation HDLC avec FAI

```
R2(config)#interface serial 0/1/0
R2(config-if)#encapsulation hdlc
R2(config-if)#no shutdown
```

Remarque : même si la vérification des résultats indique 100 %, les tests de connectivité échouent si vous ne configurez pas la commande **no shutdown** sur R2 et FAI.

Étape 3. Test de la connectivité entre les PC et le serveur Web

Utilisez une unité de données simple Packet Tracer pour vérifier la connectivité. Le test doit réussir.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Exercice PT 2.4.6 : configuration de l'authentification PAP et CHAP

Diagramme de topologie

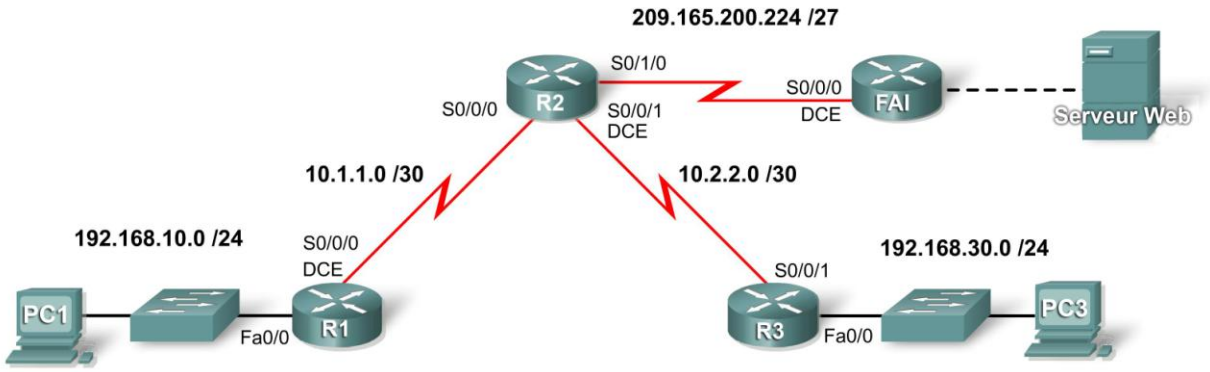


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
FAI	S0/0/0	209.165.200.226	255.255.255.252
	Fa0/0	209.165.200.1	255.255.255.252
Serveur Web	Carte réseau	209.165.200.2	255.255.255.252
PC1	Carte réseau	192.168.10.10	255.255.255.0
PC3	Carte réseau	192.168.30.10	255.255.255.0

Objectifs pédagogiques

- Configurer le routage OSPF
- Configurer l'authentification PAP entre R1 et R2
- Configurer l'authentification CHAP entre R3 et R2

Présentation

L'encapsulation PPP permet deux types d'authentification différents : PAP (Password Authentication Protocol ou protocole d'authentification du mot de passe) et CHAP (Challenge Handshake Authentication Protocol ou protocole d'authentification à échanges confirmés). PAP utilise un mot de passe sous forme de texte en clair, tandis que CHAP fait appel à une empreinte numérique à sens unique qui offre plus de sécurité que PAP. Au cours de cet exercice, vous allez configurer à la fois les types PAP et CHAP et examiner la configuration de routage OSPF.

Tâche 1 : configuration du routage OSPF

Étape 1 : activation du protocole OSPF sur R1

Avec un paramètre *process-ID* de **1**, activez le routage OSPF à l'aide de la commande **router ospf 1**.

Étape 2 : configuration des instructions réseau sur R1

En mode de configuration du routeur, ajoutez tous les réseaux connectés à R1 à l'aide de la commande **network**. Le paramètre *area-id* OSPF est de **0** pour toutes les instructions **network** dans cette topologie.

```
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
```

Étape 3 : configuration des instructions réseau sur R2 et R3

Répétez les étapes 1 et 2 pour les routeurs R2 et R3. Consultez la table d'adressage pour déterminer les instructions correctes. Sur R2, n'annoncez *pas* le réseau 209.165.202.224/30. Vous allez configurer une route par défaut à la prochaine étape.

Étape 4 : définition et redistribution de la route par défaut OSPF

- Sur R2, créez une route statique par défaut vers FAI à l'aide de la commande **ip route 0.0.0.0 0.0.0.0 s0/1/0**.
- À l'invite du routeur, envoyez la commande **default-information originate** pour inclure la route statique dans les mises à jour OSPF envoyées depuis R2.

Étape 5 : vérification de la connectivité de bout en bout

À ce stade de la configuration, tous les périphériques doivent être en mesure d'envoyer des requêtes ping vers tous les emplacements.

Cliquez sur **Check Results**, puis cliquez sur l'onglet **Connectivity Tests**. L'état doit avoir la valeur « correct » pour les deux tests. Les tables de routage de R1, R2 et R3 doivent être complètes. R1 et R3 doivent avoir une route par défaut comme indiqué dans la table de routage de R1 ci-dessous :

```
R1#show ip route
Codes : C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
<résultat omis>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:03:59, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
O    192.168.30.0/24 [110/129] via 10.1.1.2, 00:02:19, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 10.1.1.2, 00:02:19, Serial0/0/0
```

Étape 6 : vérification des résultats

Votre taux de réalisation doit être de 40 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration de l'authentification PAP

Étape 1 : configuration de R1 pour utiliser l'authentification PAP avec R2

- Sur R1 en mode de configuration globale, entrez la commande **username R2 password cisco123**. Cette commande permet au routeur distant R2 de se connecter à R1 en utilisant le mot de passe **cisco123.**
- Modifiez le type d'encapsulation en PPP sur l'interface s0/0/0 de R1 à l'aide de la commande **encapsulation ppp**.
- Sur l'interface série, configurez l'authentification PAP à l'aide de la commande **ppp authentication pap**.
- Configurez le nom d'utilisateur et le mot de passe qui seront envoyés à R2 à l'aide de la commande **ppp pap sent-username R1 password cisco123**. Packet Tracer n'évalue pas la commande **ppp pap sent-username R1 password cisco123** mais celle-ci est nécessaire pour configurer l'authentification PAP.
- Revenez en mode d'exécution privilégié et lancez la commande **show ip interface brief** pour remarquer que la liaison entre R1 et R2 s'est désactivée.

```
R1(config)#username R2 password cisco123
R1(config)#interface s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password cisco123
R1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            10.1.1.1        YES manual up                    down
Serial0/0/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Étape 2 : configuration de R2 pour utiliser l'authentification PAP avec R1

Répétez l'étape 1 pour R2, en utilisant la liaison série vers R1.

N'oubliez pas que le nom utilisé dans la commande **username** *nom* **password** *motdepasse* est toujours le nom du routeur distant, alors que dans la commande **ppp pap sent-username** *nom* **password** *motdepasse*, il s'agit du nom du routeur source.

Remarque : Packet Tracer active la liaison, mais sur un équipement réel vous devez utiliser les commandes **shutdown** puis **no shutdown** sur l'interface pour forcer une nouvelle authentification de PAP. Vous pouvez aussi simplement recharger les routeurs.

Étape 3 : test de la connectivité entre PC1 et le serveur Web

Lancez la commande **show ip interface brief** pour voir que la liaison entre R1 et R2 est maintenant activée. L'accès au serveur Web à partir de R1 doit maintenant être rétabli. Pour le tester, envoyez un paquet ping de PC1 au serveur Web.

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual administratively down down
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            10.1.1.2        YES manual up                    up
Serial0/0/1            10.2.2.1        YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Étape 4 : vérification des résultats

Votre taux de réalisation doit être de 70 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration de l'authentification CHAP

Étape 1 : configuration de R3 pour utiliser l'authentification CHAP avec R2

- En mode de configuration globale pour R3, entrez la commande **username R2 password cisco123**.
- Sur l'interface s0/0/1, lancez les commandes **encapsulation ppp** et **ppp authentication chap**, ce qui permet d'activer l'encapsulation PPP et l'authentification CHAP.
- Lancez la commande **show ip interface brief** pour voir que la liaison entre R2 et R3 s'est désactivée.

```
R3(config)#username R2 password cisco123
R3(config)#interface s0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#ppp authentication chap
```

Étape 2 : configuration de R2 pour utiliser l'authentification CHAP avec R3

Répétez l'étape 1 utilisée pour R2, en changeant le nom en R3, puisque R3 est le routeur distant.

Étape 3 : test de la connectivité entre PC3 et le serveur Web

À l'aide de la commande **show ip interface brief**, vous pouvez voir que la liaison entre R2 et R3 est maintenant activée et que PC3 peut envoyer une requête ping au serveur Web.

Étape 4 : vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Exercice 2.5.1 : configuration de base du protocole PPP

Diagramme de topologie

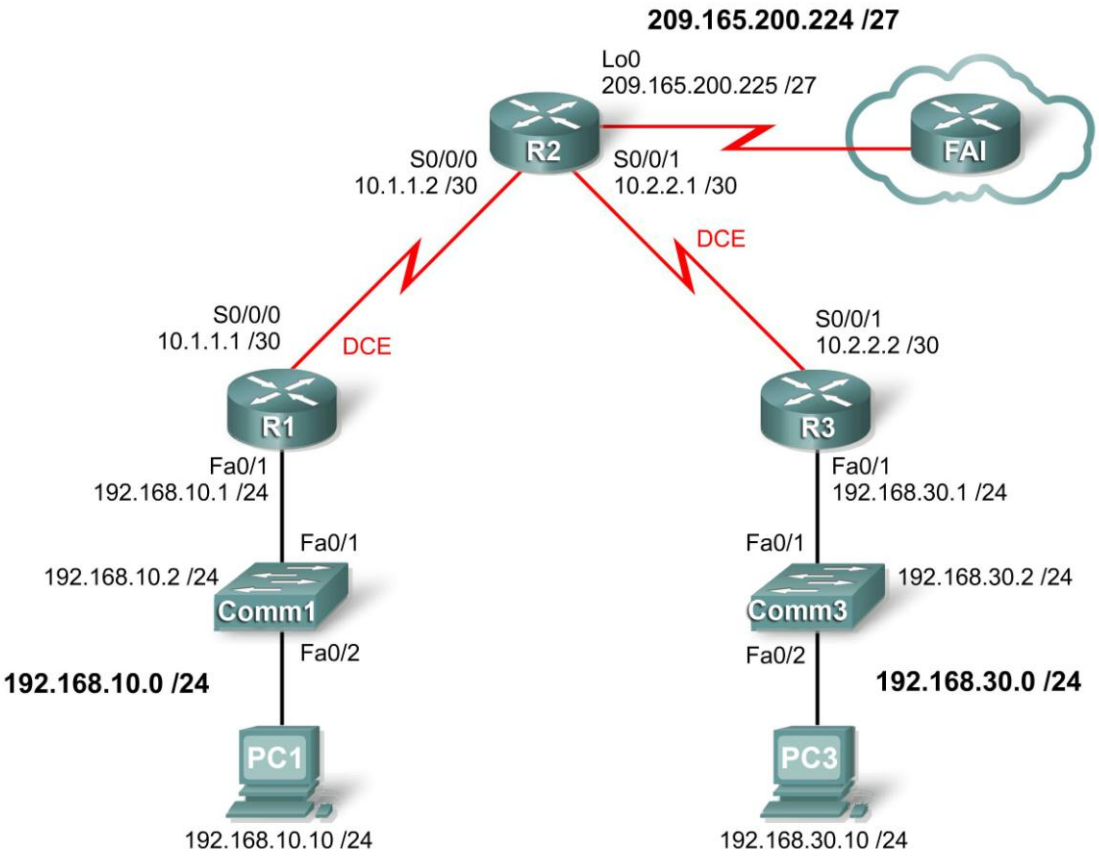


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/1**	192.168.10.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
R2	**Lo0**	209.165.200.225	255.255.255.224	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
R3	**Fa0/1**	192.168.30.1	255.255.255.0	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
PC1	**Carte réseau**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**Carte réseau**	192.168.30.10	255.255.255.0	192.168.30.1

Objectifs pédagogiques

- Configurer le routage OSPF sur tous les routeurs
- Configurer l'encapsulation PPP sur toutes les interfaces série
- Interrompre et restaurer volontairement l'encapsulation PPP
- Configurer les authentifications CHAP et PAP PPP
- Interrompre et restaurer volontairement les authentifications CHAP et PAP PPP

Présentation

Dans le cadre de ces travaux pratiques, vous allez apprendre à configurer une encapsulation PPP sur des liaisons série en utilisant le réseau illustré dans le diagramme de topologie. Vous allez également apprendre à restaurer l'encapsulation HDLC par défaut sur les liaisons série. Enfin, vous allez configurer l'authentification PAP PPP et l'authentification CHAP PPP.

Tâche 1 : configuration du protocole OSPF sur les routeurs

Étape 1. Activation du routage OSPF sur R1, R2 et R3

Lancez la commande **router ospf** avec un ID de processus de 1 pour entrer en mode de configuration du routeur. Pour chaque routeur, annoncez tous les réseaux reliés.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#

R2(config)#router ospf 1
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#network 209.165.200.224 0.0.0.31 area 0
R2(config-router)#

R3(config)#router ospf 1
R3(config-router)#network 10.2.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.30.0 0.0.0.255 area 0
R3(config-router)#
```

Étape 2. Vérification de la connectivité totale du réseau

Utilisez les commandes **show ip route** et **ping** pour vérifier la connectivité.

```
R1#show ip route

<résultat omis>

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:02:22, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
O    192.168.30.0/24 [110/129] via 10.1.1.2, 00:00:08, Serial0/0/0
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.225 [110/65] via 10.1.1.2, 00:02:22, Serial0/0/0

R1#ping 192.168.30.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
R1#

R2#show ip route

<résultat omis>

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/65] via 10.1.1.1, 00:02:31, Serial0/0/0
O    192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:20, Serial0/0/1
     209.165.200.0/27 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, Loopback0

R2#ping 192.168.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R2#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R2#

R3#show ip route

<résultat omis>

     10.0.0.0/30 is subnetted, 2 subnets
O       10.1.1.0 [110/128] via 10.2.2.1, 00:00:34, Serial0/0/1
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/129] via 10.2.2.1, 00:00:34, Serial0/0/1
C    192.168.30.0/24 is directly connected, FastEthernet0/1
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.225 [110/65] via 10.2.2.1, 00:00:34, Serial0/0/1

R3#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R3#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
R3#
```

Tâche 2 : configuration de l'encapsulation PPP sur les interfaces série

Étape 1. Utilisation de la commande show interface pour vérifier si HDLC est l'encapsulation série par défaut

HDLC est le protocole d'encapsulation série par défaut sur les routeurs Cisco. Lancez la commande **show interface** sur l'une des interfaces série pour afficher l'encapsulation actuelle.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set

<résultat omis>
```

Si vous vérifiez toutes les interfaces série actives, l'encapsulation est définie sur HDLC.

Étape 2. Modification du protocole d'encapsulation des interfaces série de HDLC en PPP

Modifiez le type d'encapsulation de la liaison entre R1 et R2 et observez les effets.

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#
*Aug 17 19:02:53.412: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from F
ULL to DOWN, Neighbor Down: Interface down or detached
R1(config-if)#

R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#
```

Que se passe-t-il lorsqu'une extrémité de la liaison série est encapsulée avec PPP et l'autre extrémité avec HDLC ?

Que se passe-t-il lorsque l'encapsulation PPP est configurée aux deux extrémités de la liaison série ?

Étape 3. Modification de l'encapsulation de HDLC en PPP aux deux extrémités de la liaison série entre R2 et R3

```
R2(config)#interface serial0/0/1
R2(config-if)#encapsulation ppp
R2(config-if)#
*Aug 17 20:02:08.080: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
 to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:02:13.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
*Aug 17 20:02:58.564: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:03:03.644: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
*Aug 17 20:03:46.988: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
```

```
 state to down
R3(config)#interface serial 0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#
*Aug 17 20:04:27.152: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:04:30.952: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from L
OADING to FULL, Loading Done
```

Quand le protocole de ligne de la liaison série s'active-t-il et la contiguïté OSPF est-elle restaurée ?

Étape 4. Vérification que le protocole d'encapsulation est désormais PPP sur les interfaces série

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<résultat omis>

R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<résultat omis>

R2#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<résultat omis>
R3#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<résultat omis>
```

Tâche 3 : interruption et restauration de l'encapsulation PPP

Étape 1. Retour des deux interfaces série de R2 à leur encapsulation HDLC par défaut

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:36:48.432: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from FULL
 to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:36:49.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to down
R2(config-if)#
*Aug 17 20:36:51.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to up
R2(config-if)#interface serial 0/0/1
*Aug 17 20:37:14.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to down
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:37:17.368: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
 to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:37:18.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
*Aug 17 20:37:20.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:37:44.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
```

Pourquoi est-il utile de briser volontairement une configuration ?

_____

_____

Pourquoi les deux interfaces série se désactivent-elles, puis se réactivent puis se désactivent de nouveau ?

_____

_____

Voyez-vous une autre manière de passer l'encapsulation d'une interface série de PPP à l'encapsulation HDLC par défaut, sans faire appel à la commande encapsulation hdlc ? (Indice : cela concerne la commande **no**).

_____

_____

_____

_____

_____

Étape 2. Retour des deux interfaces série de R2 à l'encapsulation PPP

```
R2(config)#interface s0/0/0
R2(config-if)#encapsulation ppp
*Aug 17 20:53:06.612: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to up
R2(config-if)#interface s0/0/1
*Aug 17 20:53:10.856: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOAD
ING to FULL, Loading Done
R2(config-if)#encapsulation ppp
*Aug 17 20:53:23.332: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:53:24.916: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
R2(config-if)#
```

Tâche 4 : configuration de l'authentification PPP

Étape 1. Configuration de l'authentification PAP PPP sur la liaison série entre R1 et R2

```
R1(config)#username R2 password cisco
R1(config)#int s0/0/0
R1(config-if)#ppp authentication pap
R1(config-if)#
*Aug 22 18:58:57.367: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to down
*Aug 22 18:58:58.423: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from F
ULL to DOWN, Neighbor Down: Interface down or detached
R1(config-if)#ppp pap sent-username R1 password cisco
```

Que se passe-t-il lorsque l'authentification PAP PPP est configurée à une seule extrémité de la liaison série ?

_____

_____

```
R2(config)#username R1 password cisco
R2(config)#interface Serial0/0/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R2 password cisco
R2(config-if)#
*Aug 23 16:30:33.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to up
*Aug 23 16:30:40.815: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOAD
ING to FULL, Loading Done
```

Que se passe-t-il lorsque l'authentification PAP PPP est configurée aux deux extrémités de la liaison série ?

_____

Étape 2. Configuration de l'authentification CHAP PPP sur la liaison série entre R2 et R3

Avec une authentification PAP, le mot de passe n'est pas chiffré. Cela est évidemment mieux que de n'utiliser aucune identification, mais il est encore nettement préférable de chiffrer le mot de passe envoyé sur la liaison. Avec CHAP, les mots de passe sont chiffrés.

```
R2(config)#username R3 password cisco
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 23 18:06:00.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
R2(config-if)#
*Aug 23 18:06:01.947: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
 to DOWN, Neighbor Down: Interface down or detached
R2(config-if)#
R3(config)#username R2 password cisco
*Aug 23 18:07:13.074: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
R3(config)#int s0/0/1
R3(config-if)#
*Aug 23 18:07:22.174: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from L
OADING to FULL, Loading Done
R3(config-if)#ppp authentication chap
R3(config-if)#
```

Remarquez que le protocole de ligne de l'interface série 0/0/1 voit son état passer à « UP » même avant que l'interface ne soit configurée pour l'authentification CHAP. Savez-vous pourquoi cela se produit ?

_____

_____

Tâche 5 : interruption et restauration volontaire de l'authentification CHAP PPP

Étape 1. Interruption de l'authentification CHAP PPP

Sur la liaison série entre R2 et R3, modifiez le protocole d'authentification de l'interface série 0/0/1 en PAP.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ppp authentication pap
R2(config-if)#^Z
R2#
*Aug 24 15:45:47.039: %SYS-5-CONFIG_I: Configured from console by console
R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#reload
```

La modification du protocole d'authentification en PAP sur l'interface série 0/0/1 a-t-elle pour effet d'interrompre l'authentification entre R2 et R3 ?

_____

Étape 2. Restauration de l'authentification CHAP PPP sur la liaison série

Remarquez qu'il n'est pas nécessaire de recharger le routeur pour que cette modification prenne effet.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 24 15:50:00.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
R2(config-if)#
*Aug 24 15:50:07.467: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
R2(config-if)#
```

Étape 3. Interruption volontaire de l'authentification CHAP PPP en modifiant le mot de passe sur R3

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#username R2 password ciisco
R3(config)#^Z
R3#
*Aug 24 15:54:17.215: %SYS-5-CONFIG_I: Configured from console by console
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
```

Après le rechargement, quel est l'état du protocole de ligne sur l'interface série 0/0/1 ?

_____

Étape 4. Restauration de l'authentification CHAP PPP en modifiant le mot de passe sur R3

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#username R2 password cisco
R3(config)#
*Aug 24 16:11:10.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3(config)#
*Aug 24 16:11:19.739: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config)#
```

Remarquez que la liaison est à nouveau active. Testez la connectivité en lançant une commande ping de PC1 à PC3.

Exercice 2.5.2 : configuration avancée du protocole PPP

Topologie

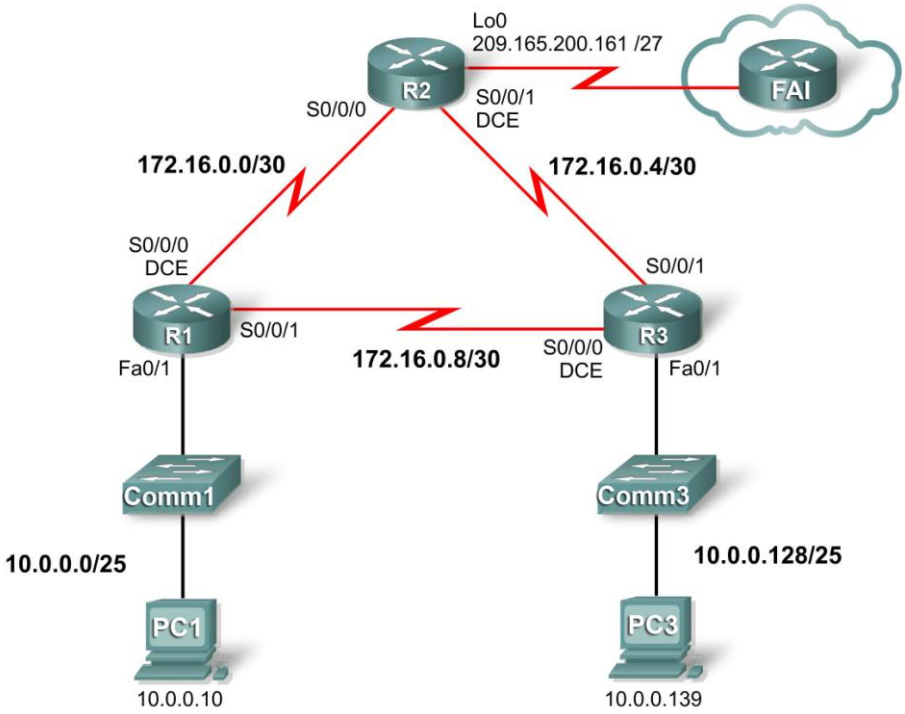


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/1**	10.0.0.1	255.255.255.128	N/D
	S0/0/0	172.16.0.1	255.255.255.252	N/D
	S0/0/1	172.16.0.9	255.255.255.252	N/D
R2	**Lo0**	209.165.200.161	255.255.255.224	N/D
	S0/0/0	172.16.0.2	255.255.255.252	N/D
	S0/0/1	172.16.0.5	255.255.255.252	N/D
R3	**Fa0/1**	10.0.0.129	255.255.255.128	N/D
	S0/0/0	172.16.0.10	255.255.255.252	N/D
	S0/0/1	172.16.0.6	255.255.255.252	N/D
PC1	**Carte réseau**	10.0.0.10	255.255.255.128	10.0.0.1
PC3	**Carte réseau**	10.0.0.139	255.255.255.128	10.0.0.129

Objectifs pédagogiques

- Configurer et activer des interfaces
- Configurer le routage OSPF sur tous les routeurs
- Configurer l'encapsulation PPP sur toutes les interfaces série
- Configurer l'authentification CHAP PPP

Présentation

Au cours de cet exercice, vous allez configurer une encapsulation PPP sur des liaisons série en utilisant le réseau illustré dans le diagramme de topologie. Vous allez également configurer l'authentification CHAP PPP. Si vous avez besoin d'aide, reportez-vous à l'exercice ou aux travaux pratiques de configuration PPP de base ; essayez cependant d'en faire le plus possible par vous-même.

Tâche 1 : configuration et activation d'adresses série et Ethernet

Étape 1. Configuration des interfaces sur R1, R2 et R3

Le système d'adressage est indiqué sur la topologie et dans la table d'adressage. Certaines adresses d'interfaces sont fournies mais pour certaines interfaces, seul le réseau est indiqué. Dans les cas où vous disposez uniquement de l'adresse réseau, vous pouvez utiliser toute adresse valide sur le réseau indiqué pour permettre une évaluation correcte dans Packet Tracer.

Configurez les interfaces pour R1, R2 et R3 en fonction de la topologie. Aux extrémités DCE des liaisons série, la fréquence d'horloge est de 64 000 bits/s.

Étape 2. Vérification de l'adressage IP et des interfaces

Vérifiez que toutes les interfaces sont actives à la fois au niveau physique et sur la couche liaison de données. Chaque routeur connecté directement doit être en mesure d'envoyer une requête ping aux autres.

Étape 3. Configuration des interfaces Ethernet de PC1 et PC3

Étape 4. Test de connectivité entre les PC

Les PC devraient-ils être capables de s'envoyer des requêtes ping à ce stade ? Peuvent-ils envoyer des requêtes ping sur leurs passerelles par défaut ?

Tâche 2 : configuration du protocole OSPF sur les routeurs

Étape 1. Configuration du routage OSPF sur les routeurs

Pour la configuration du routage OSPF, utilisez une id de zone de 1.

Étape 2. Vérification de la connectivité totale du réseau

Tous les routeurs doivent disposer de routes vers tous les réseaux et doivent être en mesure d'envoyer des requêtes ping vers tous les périphériques.

Tâche 3 : configuration de l'encapsulation PPP sur les interfaces série

Étape 1. Configuration de PPP sur les interfaces série des trois routeurs

L'encapsulation actuelle est définie sur HDLC sur toutes les liaisons série. Afin de configurer l'authentification par la suite, l'encapsulation doit être définie sur PPP.

Étape 2. Vérification que toutes les interfaces série utilisent l'encapsulation PPP

Si les encapsulations des interfaces série connectées ne correspondent pas, la liaison se désactive. Faites en sorte que l'encapsulation PPP soit définie sur toutes les interfaces.

Tâche 4 : configuration de l'authentification CHAP PPP

Le mot de passe pour l'authentification CHAP est cisco.

Étape 1. Configuration de l'authentification CHAP PPP sur toutes les liaisons série

Étape 2. Vérification de l'authentification CHAP PPP sur toutes les liaisons série

Les routeurs peuvent-ils tous communiquer entre eux ? PC1 peut-il envoyer une requête ping à PC3 ?

Exercice 2.5.3 : dépannage de la configuration PPP

Diagramme de topologie

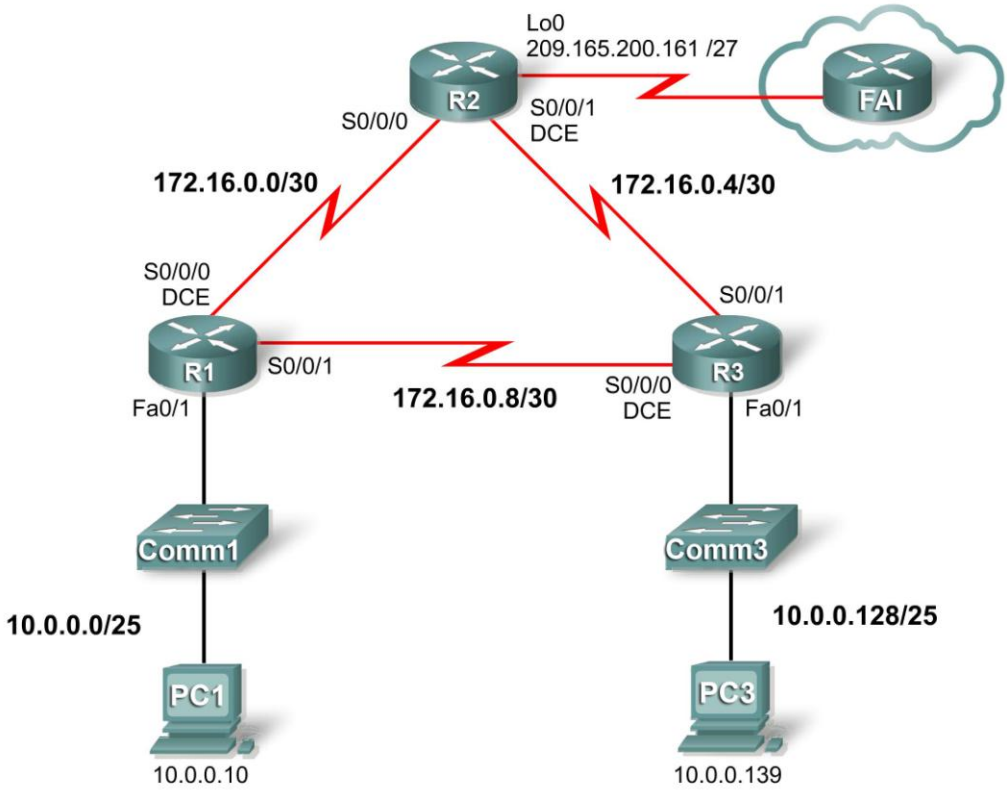


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/1**	10.0.0.1	255.255.255.128	N/D
	S0/0/0	172.16.0.1	255.255.255.252	N/D
	S0/0/1	172.16.0.9	255.255.255.252	N/D
R2	**Lo0**	209.165.200.161	255.255.255.224	N/D
	S0/0/0	172.16.0.2	255.255.255.252	N/D
	S0/0/1	172.16.0.5	255.255.255.252	N/D
R3	**Fa0/1**	10.0.0.129	255.255.255.128	N/D
	S0/0/0	172.16.0.10	255.255.255.252	N/D
	S0/0/1	172.16.0.6	255.255.255.252	N/D
PC1	**Carte réseau**	10.0.0.10	255.255.255.128	10.0.0.1
PC3	**Carte réseau**	10.0.0.139	255.255.255.128	10.0.0.129

Objectifs pédagogiques

- Trouver et corriger les erreurs de réseau
- Documenter le réseau corrigé

Scénario

Les routeurs de votre société ont été configurés par un ingénieur réseau sans expérience. De nombreuses erreurs de configuration ont entraîné des problèmes de connectivité. Votre supérieur vous a demandé de dépanner et de corriger les erreurs de configuration et de rapporter par écrit votre travail. En utilisant vos connaissances de PPP et des méthodes de test standard, trouvez et corrigez les erreurs. Vérifiez que toutes les liaisons série utilisent l'authentification CHAP PPP et que tous les réseaux sont accessibles.

Tâche 1 : recherche et correction des erreurs de réseau

- Réglez toutes les fréquences d'horloge sur **64000**.
- Utilisez **cisco** pour tous les mots de passe CHAP.

Tâche 2 : description du réseau corrigé

Exercice PT 2.6.1 : exercice d'intégration des compétences Packet Tracer

Diagramme de topologie

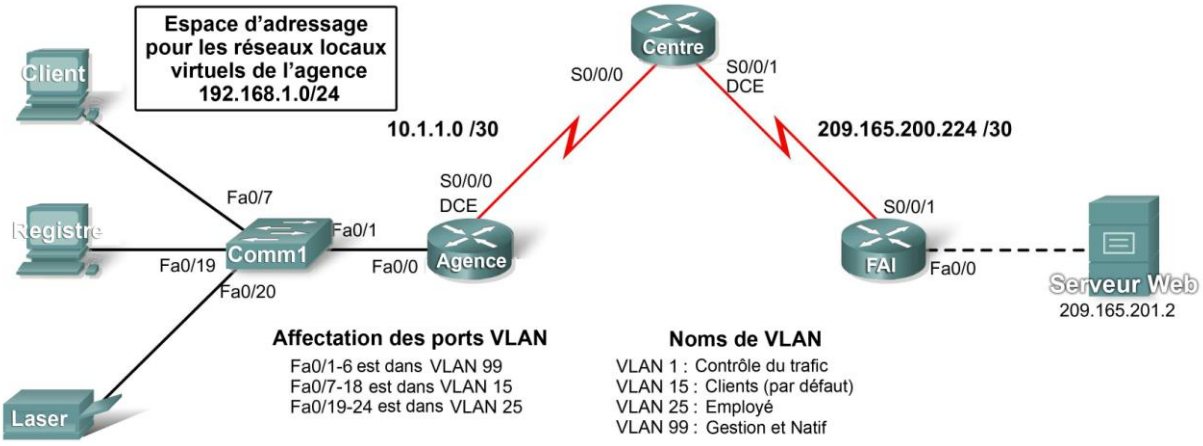


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
CENTRE	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	209.165.200.226	255.255.255.252	N/D
FAI	S0/0/1	209.165.200.225	255.255.255.252	N/D
	Fa0/0	209.165.201.1	255.255.255.252	N/D
AGENCE	Fa0/0.1			N/D
	Fa0/0.15			N/D
	Fa0/0.25			N/D
	Fa0/0.99			N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
Comm1	VLAN2			
Client	Carte réseau			
Registre	Carte réseau			
Laser	Carte réseau			
Serveur Web	Carte réseau	209.165.201.2	255.255.255.252	209.165.201.1

Objectifs pédagogiques

- Configurer le routage statique et par défaut
- Ajouter et connecter un routeur
- Concevoir et documenter un schéma d'adressage
- Ajouter et connecter des périphériques dans un espace d'adressage
- Configurer des paramètres de base de périphérique
- Configurer l'encapsulation PPP avec CHAP
- Configurer le routage OSPF
- Configurer des réseaux locaux virtuels
- Vérifier la connectivité

Tâche 1 : configuration du routage statique et par défaut

Étape 1. Configuration du routage statique de FAI à CENTRE

Utilisez les mots de passe **cisco** et **class** pour accéder aux modes d'exécution des interfaces de commande en ligne des routeurs. Configurez deux routes statiques sur FAI à l'aide de l'argument d'interface de sortie vers les réseaux suivants :

- 10.1.1.0/30
- 192.168.1.0/24

Étape 2. Configuration du routage par défaut de CENTRE à FAI

Configurez une route par défaut sur CENTRE à l'aide de l'argument d'interface de sortie pour envoyer tout le trafic par défaut vers FAI.

Étape 3. Test de la connectivité au serveur Web

CENTRE doit maintenant être en mesure d'envoyer une requête ping au serveur Web à l'adresse 209.165.201.2.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 4 %. Si ce n'est pas le cas, cliquez sur **Check Results** (Vérifier les résultats) pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : ajout et connexion d'un routeur

Étape 1. Ajout du routeur AGENCE

Cliquez sur Custom Made Devices et ajoutez un routeur 1841 à la topologie. à partir de l'onglet Config, modifiez le champ Display Name en AGENCE. Les noms affichés sont sensibles à la casse. Ne modifiez pas le nom d'hôte tout de suite.

Étape 2. Connexion de AGENCE à CENTRE

Choisissez le câble qui convient et connectez AGENCE à CENTRE conformément aux interfaces indiquées dans la topologie.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 9 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets. Si vous avez modifié le nom d'hôte à l'étape 2, votre pourcentage sera plus élevé.

Tâche 3 : conception et description d'un schéma d'adressage

Étape 1. Conception d'un schéma d'adressage

À l'aide de la topologie et des spécifications suivantes, concevez un schéma d'adressage :

- L'adressage est fourni pour toutes les liaisons WAN.
- Pour les réseaux locaux virtuels raccordés à AGENCE, utilisez l'espace d'adressage 192.168.1.0/24. Affectez les sous-réseaux dans l'ordre suivant pour tous les réseaux locaux virtuels, en commençant par ceux ayant les besoins les plus importants en termes d'hôtes.
    - VLAN 15 a besoin d'espace pour 100 hôtes _____
    - VLAN 25 a besoin d'espace pour 50 hôtes _____
    - VLAN 1 a besoin d'espace pour 20 hôtes _____
    - VLAN 99 a besoin d'espace pour 20 hôtes _____

Étape 2. Documentation du schéma d'adressage

- Procédez comme suit pour compléter la table d'adressage. Vous ajouterez les périphériques qui restent dans la prochaine tâche.
    - Attribuez la première adresse de chaque réseau local virtuel à la sous-interface de AGENCE correspondante. Les numéros de sous-interface correspondent aux numéros de réseaux locaux virtuels (VLAN).
    - Attribuez la deuxième adresse de VLAN 99 à Comm1.
    - Attribuez la deuxième adresse de VLAN 15 au PC Client.
    - Attribuez la deuxième adresse de VLAN 25 au PC Registre.
    - Attribuez la dernière adresse de VLAN 25 à l'imprimante laser.
- Veillez à enregistrer pour chaque adresse le masque de sous-réseau et la passerelle par défaut qui conviennent.

Tâche 4 : ajout et connexion des périphériques dans l'espace d'adressage

Étape 1. Ajout de Comm1, du PC Client, du PC Registre et de l'imprimante laser dans l'espace d'adressage 192.168.1.0/24

- Comm1 est un commutateur 2960. Ajoutez-le à la topologie et modifiez le nom affiché en Comm1. Les noms affichés sont sensibles à la casse. Ne modifiez pas le nom d'hôte tout de suite.
- Les PC et l'imprimante apparaissent dans End Devices. Ajoutez deux PC et une imprimante. Modifiez les noms affichés pour les PC et l'imprimante en fonction de la topologie.

Étape 2. Connexion de Comm1 à AGENCE

Choisissez le câble qui convient et connectez Comm1 à AGENCE conformément aux interfaces indiquées dans la topologie.

Étape 3. Connexion du PC Client, du PC Registre et de l'imprimante laser à Comm1

Choisissez le câble qui convient et connectez les PC et l'imprimante à Comm1 conformément aux interfaces indiquées dans la topologie.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 22 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets. Si vous avez modifié le nom d'hôte de Comm1 à l'étape 1, votre pourcentage sera plus élevé.

Tâche 5 : configuration de paramètres de base de périphérique

Étape 1. Configuration de AGENCE et de Comm1

À l'aide de votre documentation, procédez à la configuration de base de AGENCE et de Comm1, notamment l'adressage. Utilisez **cisco** comme mot de passe de ligne et **class** comme mot de passe secret. Réglez la fréquence d'horloge sur 64 000. Les parties de la configuration de base qui sont évaluées sont les suivantes :

- Les noms d'hôte, sensibles à la casse.
- L'adressage de l'interface et son activation. Le réglage de la fréquence d'horloge sur 64 000 bits/s.
- Pour l'interface Fa0/0.99, la configuration de VLAN 99 en tant que réseau local virtuel natif.
- La création et l'adressage de l'interface VLAN 99 sur Comm1. L'activation de VLAN 99 est effectuée après la configuration de l'agrégation, un peu plus loin dans cet exercice.

Étape 2. Configuration des autres périphériques

À l'aide de votre documentation, configurez les PC et l'imprimante avec l'adressage qui convient.

Étape 3. Test de connectivité entre AGENCE et CENTRE

CENTRE doit maintenant être en mesure d'envoyer une requête ping vers AGENCE. Comm1 pourra envoyer une requête ping seulement lorsque l'agrégation sera configurée.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 63 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 6 : configuration de l'encapsulation PPP avec l'authentification CHAP

Étape 1. Configuration de CENTRE pour utiliser PPP avec CHAP pour la liaison vers AGENCE

Le mot de passe pour l'authentification CHAP est **cisco123.** La liaison se désactive.

Étape 2. Configuration de AGENCE pour utiliser PPP avec CHAP pour la liaison vers CENTRE

Le mot de passe pour l'authentification CHAP est **cisco123.** La liaison est réactivée.

Étape 3. Test de connectivité entre AGENCE et CENTRE

L'activation des interfaces par Packet Tracer peut prendre un peu plus de temps qu'avec un équipement réel. Une fois les interfaces activées, CENTRE doit être en mesure d'envoyer une requête ping vers AGENCE.

Étape 4. Vérification des résultats.

Votre taux de réalisation doit être de 71 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 7 : configuration du routage OSPF

Étape 1. Configuration d'OSPF sur CENTRE

- Configurez OSPF à l'aide de l'ID de processus 1.
- Ajoutez uniquement le réseau partagé avec AGENCE.
- Transmettez les informations de route par défaut aux voisins OSPF.
- Désactivez les mises à jour OSPF vers FAI.

Étape 2. Configuration d'OSPF sur AGENCE

- Configurez OSPF à l'aide de l'ID de processus 1.
- Ajoutez tous les réseaux actifs routés par AGENCE.
- Désactivez les mises à jour OSPF vers les réseaux locaux virtuels.

Étape 3. Test de la connectivité au serveur Web

AGENCE doit maintenant être en mesure d'envoyer une requête ping au serveur Web à l'adresse 209.165.201.2.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 86 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 8 : configuration des réseaux locaux virtuels

Étape 1. Ajout des réseaux locaux virtuels à Comm1

Les noms des réseaux locaux virtuels sont sensibles à la casse. Ajoutez les quatre réseaux locaux virtuels et donnez-leur des noms en fonction des indications suivantes :

- VLAN 15 ; son nom est **Clients(défaut)**
- VLAN 25 ; son nom est **Employés**
- VLAN 99 ; son nom est **Direction&natif**

Étape 2. Attribution des ports aux réseaux locaux virtuels adéquats et activation de l'interface VLAN 99

- À l'aide des affectations de ports des réseaux locaux virtuels indiquées dans le diagramme de topologie, configurez les ports d'accès reliés aux périphériques d'extrémité et affectez chacun d'eux au réseau local virtuel qui convient.
- Activez l'agrégation sur le port Fa0/1 et configurez-le pour utiliser VLAN 99 en tant que réseau local virtuel natif.
- Activez l'interface VLAN 99, si nécessaire. Elle devrait déjà être active.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 9 : vérification de la connectivité

Étape 1. Vérification que le PC Client, le PC Registre et l'imprimante laser peuvent s'envoyer des requêtes ping

Étape 2. Vérification que le PC Client, le PC Registre et l'imprimante laser peuvent envoyer des requêtes ping au serveur Web

Exercice PT 3.2.2 : configuration Frame Relay de base avec mappages statiques

Diagramme de topologie

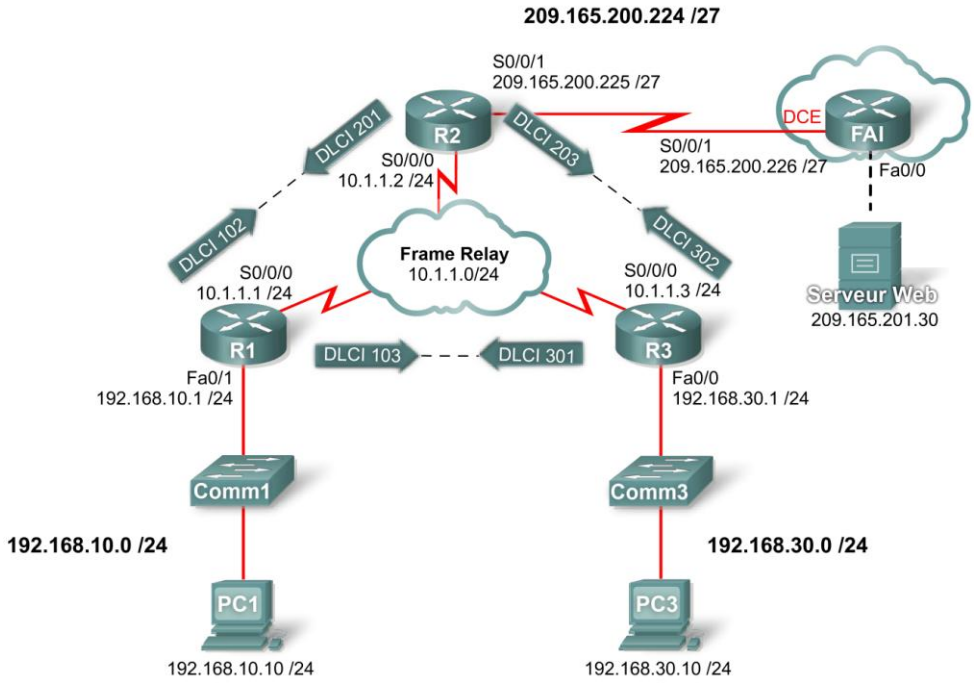


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**Fa0/0Fa0/0**	192.168.10.1	255.255.255.0
	S0/0/1S0/0/1	10.10.10.1	255.255.255.0
R2	**S0/0/0S0/0/0**	10.10.10.2	255.255.255.0
	S0/0/1S0/0/1	209.165.200.225	255.255.255.224
R3	**Fa0/0Fa0/0**	192.168.30.1	255.255.255.0
	S0/0/0S0/0/0	10.10.10.3	255.255.255.0
FAI	**S0/0/1S0/0/1**	209.165.200.226	255.255.255.224

Objectifs pédagogiques

- Configurer Frame Relay
- Configurer des cartes Frame Relay statiques
- Configurer le type de LMI de Frame Relay

Présentation

Au cours de cet exercice, vous allez configurer Frame Relay sur les interfaces série 0/0/0 des routeurs R1, R2 et R3. Vous allez également configurer deux cartes Frame Relay statiques sur chaque routeur pour atteindre les deux autres routeurs. Bien que le type de LMI soit détecté automatiquement sur les routeurs, vous allez affecter le type de manière statique en configurant l'interface LMI.

Les routeurs R1, R2 et R3 ont été préconfigurés avec des noms d'hôte et des adresses IP sur toutes les interfaces. Les interfaces Fast Ethernet sur les routeurs R1 et R3 sont actifs, et l'interface S0/0/1 de R2 est active.

Tâche 1 : configuration de Frame Relay

Étape 1. Configuration de l'encapsulation Frame Relay sur l'interface série 0/0/0 de R1

```
R1(config)#interface serial0/0/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown
```

Étape 2. Configuration de l'encapsulation Frame Relay sur les interfaces série 0/0/0 de R2 et de R3

Étape 3. Test de connectivité

À partir de la ligne de commande sur PC1, vérifiez la connectivité vers l'hôte PC3, à l'adresse 192.168.30.10, à l'aide de la commande **ping**.

La requête ping de PC1 à PC3 doit échouer car le routeur R1 ne sait pas où se trouve le réseau 192.168.30.0. R1 doit être configuré avec une carte Frame Relay afin de lui permettre de trouver la destination du prochain saut pour atteindre le réseau.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 40 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration des cartes Frame Relay statiques

Étape 1. Configuration des cartes statiques sur R1, R2 et R3

Chaque routeur a besoin de deux cartes statiques pour atteindre les autres routeurs. Les identificateurs DLCI (identificateurs de connexion de liaison de données) permettant d'atteindre ces routeurs sont les suivants :

Routeur R1 :

- Pour atteindre le routeur R2, utilisez le DCLI 102 situé à l'adresse IP 10.10.10.2.
- Pour atteindre le routeur R3, utilisez le DCLI 103 situé à l'adresse IP 10.10.10.3.

Routeur R2 :

- Pour atteindre le routeur R1, utilisez le DCLI 201 situé à l'adresse IP 10.10.10.1.
- Pour atteindre le routeur R3, utilisez le DCLI 203 situé à l'adresse IP 10.10.10.3.

Routeur R3 :

- Pour atteindre le routeur R1, utilisez le DCLI 301 situé à l'adresse IP 10.10.10.1.
- Pour atteindre le routeur R3, utilisez le DCLI 302 situé à l'adresse IP 10.10.10.2.

Les routeurs doivent également prendre en charge le protocole RIP. Par conséquent, le mot de passe **broadcast** est obligatoire.

Sur le routeur R1, configurez les cartes Frame Relay statiques comme suit :

```
R1(config-if)#frame-relay map ip 10.10.10.2 102 broadcast
R1(config-if)#frame-relay map ip 10.10.10.3 103 broadcast
```

Configurez les routeurs R2 et R3 à l'aide des informations précédentes.

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 80 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration du type de LMI de Frame Relay

Le nuage Frame Relay contient des commutateurs qui utilisent ANSI comme type de LMI. Par conséquent, toutes les liaisons Frame Relay doivent être configurées manuellement pour utiliser ANSI.

Étape 1. Configuration du type de LMI ANSI sur R1, R2 et R3

Entrez les commandes suivantes sur l'interface série de chaque routeur.

```
R1(config-if)#interface s0/0/0
R1(config-if)#frame-relay lmi-type ansi
```

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Étape 3. Test de connectivité

Il est possible de terminer l'exercice avec 100 % tout en n'ayant pas de connectivité. PC1 et PC3 doivent maintenant être en mesure d'envoyer des requêtes ping l'un vers l'autre et vers le serveur Web. Si ce n'est pas le cas, vérifiez que vous avez saisi toutes les commandes exactement comme indiqué dans les étapes précédentes.

Exercice PT 3.6.1 : exercice d'intégration des compétences Packet Tracer

Diagramme de topologie

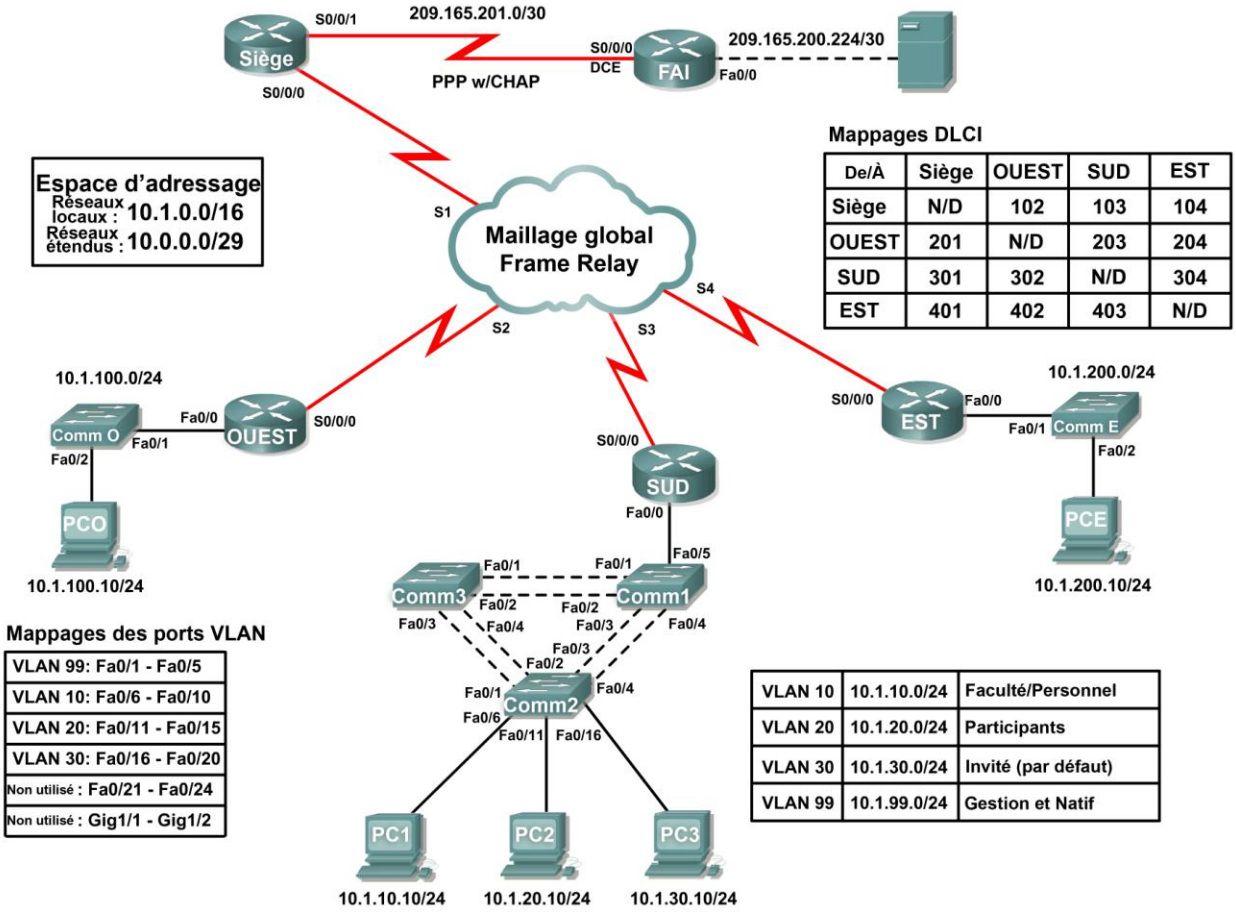


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
SIÈGE	**S0/0/1**	209.165.201.2	255.255.255.252
	S0/0/0	10.0.0.1	255.255.255.248
OUEST	**S0/0/0**	10.0.0.2	255.255.255.248
	Fa0/0	10.1.100.1	255.255.255.0
SUD	**S0/0/0**	10.0.0.3	255.255.255.248
	Fa0/0.10	10.1.10.1	255.255.255.0
	Fa0/0.20	10.1.20.1	255.255.255.0
	Fa0/0.30	10.1.30.1	255.255.255.0
	Fa0/0.99	10.1.99.1	255.255.255.0
EST	**S0/0/0**	10.0.0.4	255.255.255.248
	Fa0/0	10.1.200.1	255.255.255.0
FAI	**S0/0/0**	209.165.201.1	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Serveur Web	**Carte réseau**	209.165.200.226	255.255.255.252
Comm1	**VLAN99**	10.1.99.11	255.255.255.0
Comm2	**VLAN99**	10.1.99.12	255.255.255.0
Comm3	**VLAN99**	10.1.99.13	255.255.255.0

Objectifs pédagogiques

- Configurer PPP avec CHAP
- Configurer un Frame Relay à maillage global
- Configurer le routage statique et par défaut
- Configurer et tester le routage entre réseaux locaux virtuels
- Configurer le protocole VTP et l'agrégation sur des commutateurs
- Configurer des réseaux locaux virtuels sur un commutateur
- Configurer et vérifier l'interface VLAN 99
- Configurer un commutateur comme racine pour toutes les arborescences complètes
- Attribuer des ports à des réseaux locaux virtuels
- Tester la connectivité de bout en bout

Présentation

Cet exercice vous permet de mettre en pratique différentes compétences, notamment la configuration de Frame Relay, de PPP avec CHAP, d'un routage statique et par défaut, du protocole VTP et des réseaux locaux virtuels. Étant donné que près de 150 composants sont évalués au cours de cet exercice, vous ne verrez peut-être pas le pourcentage augmenter à chaque fois que vous configurerez une commande évaluée. Vous pouvez à tout moment cliquer sur **Check Results** et **Assessment Items** pour voir si vous avez entré correctement une commande évaluée.

Tâche 1 : configuration de PPP avec CHAP entre les périphériques

Étape 1. Configuration et activation de l'interface série 0/0/1 sur SIÈGE

Étape 2. Configuration de l'encapsulation PPP sur SIÈGE pour la liaison partagée avec FAI

Étape 3. Configuration de l'authentification CHAP sur SIÈGE

Entrez le mot de passe **cisco**.

Étape 4. Vérification de la connectivité entre SIÈGE et FAI

La liaison entre SIÈGE et FAI doit maintenant être active, et vous devez être en mesure d'envoyer une requête vers FAI. Cependant, cela peut prendre quelques minutes dans Packet Tracer pour que la liaison s'active. Pour accélérer le processus, basculez entre les modes Simulation et Realtime (Temps réel) trois ou quatre fois.

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 4 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration d'un Frame Relay à maillage global

Le diagramme de topologie représenté plus haut et la table ci-dessous indiquent tous deux les mappages DLCI utilisés dans cette configuration Frame Relay à maillage global. Lisez ce tableau de gauche à droite. Par exemple, les mappages DLCI à configurer sur SIÈGE sont les suivants : 102 vers OUEST, 103 vers SUD et 104 vers EST.

	Mappages DLCI			
De/vers	**SIÈGE**	**OUEST**	**SUD**	**EST**
SIÈGE	N/D	102	103	104
OUEST	201	N/D	203	204
SUD	301	302	N/D	304
EST	401	402	403	N/D

Remarque : SIÈGE, OUEST et SUD utilisent tous l'encapsulation Frame Relay par défaut **cisco**. Cependant, EST utilise le type d'encapsulation IETF.

Étape 1. Configuration et activation de l'interface série 0/0/0 sur SIÈGE

Configurez l'interface à l'aide des informations suivantes :

- adresse IP ;
- encapsulation Frame Relay ;
- mappages vers OUEST, SUD et EST (EST utilise l'encapsulation IETF) ;
- la trame LMI est du type ANSI.

Étape 2. Configuration et activation de l'interface série 0/0/0 sur OUEST

Configurez l'interface à l'aide des informations suivantes :

- adresse IP ;
- encapsulation Frame Relay ;
- mappages vers SIÈGE, SUD et EST (EST utilise l'encapsulation IETF) ;
- la trame LMI est du type ANSI.

Étape 3. Configuration et activation de l'interface série 0/0/0 sur SUD

Configurez l'interface à l'aide des informations suivantes :

- adresse IP ;
- encapsulation Frame Relay ;
- mappages vers SIÈGE, OUEST et EST (EST utilise l'encapsulation IETF) ;
- la trame LMI est du type ANSI.

Étape 4. Configuration et activation de l'interface série 0/0/0 sur EST

Configurez l'interface à l'aide des informations suivantes :

- adresse IP ;
- encapsulation Frame Relay avec IETF ;
- mappages vers SIÈGE, OUEST et SUD ;
- la trame LMI est du type ANSI.

Remarque : Packet Tracer n'évalue pas vos instructions de cartes. Vous devez cependant configurer les commandes. La connectivité complète entre les routeurs Frame Relay doit maintenant être établie.

Étape 5. Vérification de la connectivité entre les routeurs Frame Relay

La carte sur SIÈGE doit ressembler à ce qui suit. Vérifiez que tous les routeurs disposent de cartes complètes.

```
Serial0/0/0 (up): ip 10.0.0.2 dlci 102, static, broadcast, CISCO, status
defined, active
Serial0/0/0 (up): ip 10.0.0.3 dlci 103, static, broadcast, CISCO, status
defined, active
Serial0/0/0 (up): ip 10.0.0.4 dlci 104, static, broadcast, IETF, status
defined, active
```

Vérifiez que SIÈGE, OUEST, SUD et EST peuvent envoyer des requêtes ping l'un vers l'autre.

Étape 6. Vérification des résultats

Votre taux de réalisation doit être de 28 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration du routage statique et par défaut

Cette topologie n'utilise aucun protocole de routage. Tout le routage est effectué par le biais de routage statique et par défaut.

Étape 1. Configuration des routes statiques et par défaut sur SIÈGE

- SIÈGE a besoin de six routes statiques vers les six réseaux locaux distants de la topologie. Utilisez l'argument *next-hop-ip* dans la configuration de route statique.
- SIÈGE a également besoin d'une route par défaut. Utilisez l'argument *exit-interface* dans la configuration de la route par défaut.

Étape 2. Configuration des routes statiques et par défaut sur OUEST

- OUEST a besoin de cinq routes statiques vers les cinq réseaux locaux distants de la topologie. Utilisez l'argument *next-hop-ip* dans la configuration de route statique.
- OUEST a également besoin d'une route par défaut. Utilisez l'argument *next-hop-ip* dans la configuration de la route par défaut.

Étape 3. Configuration des routes statiques et par défaut sur SUD

- SUD a besoin de deux routes statiques vers les deux réseaux locaux distants de la topologie. Utilisez l'argument *next-hop-ip* dans la configuration de route statique.
- SUD a également besoin d'une route par défaut. Utilisez l'argument *next-hop-ip* dans la configuration de la route par défaut.

Étape 4. Configuration des routes statiques et par défaut sur EST

- EST a besoin de cinq routes statiques vers les cinq réseaux locaux distants de la topologie. Utilisez l'argument *next-hop-ip* dans la configuration de route statique.
- EST a également besoin d'une route par défaut. Utilisez l'argument *next-hop-ip* dans la configuration de la route par défaut.

Étape 5. Vérification de la connectivité des réseaux locaux EST et OUEST vers le serveur Web

- Tous les routeurs doivent maintenant être en mesure d'envoyer une requête ping au serveur Web.
- Le PC OUEST (PC-O) et le PC EST (PC-E) doivent maintenant être en mesure d'envoyer des requêtes ping l'un vers l'autre et vers le serveur Web.

Étape 6. Vérification des résultats

Votre taux de réalisation doit être de 43 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : configuration et test du routage entre réseaux locaux virtuels

Étape 1. Configuration du routage entre réseaux locaux virtuels sur SUD

À l'aide de la table d'adressage, activez l'interface Fast Ethernet 0/0 sur SUD et configurez le routage entre réseaux locaux virtuels. Le numéro de sous-interface correspond au numéro de réseau local virtuel (VLAN). VLAN 99 est le réseau local virtuel natif.

Étape 2. Test du routage entre réseaux locaux virtuels sur SUD

SIÈGE, OUEST et EST doivent maintenant être en mesure d'envoyer des requêtes ping vers toutes les sous-interfaces de SUD.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 56 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets. Les routeurs sont maintenant entièrement configurés.

Tâche 5 : configuration du protocole VTP et de l'agrégation sur les commutateurs

Étape 1. Configuration des paramètres VTP sur Comm1, Comm2 et Comm3

- Comm1 est le serveur. Comm2 et Comm3 sont des clients.
- Le nom de domaine est **CCNA**.
- Le mot de passe est **cisco**.

Étape 2. Configuration de l'agrégation sur Comm1, Comm2 et Comm3

Les ports d'agrégation de Comm1, Comm2 et Comm3 sont tous les ports reliés à un autre commutateur ou à un routeur. Définissez tous les ports d'agrégation en mode d'agrégation et affectez VLAN 99 comme réseau local virtuel natif.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 81 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 6 : configuration des réseaux locaux virtuels sur le commutateur

Étape 1. Création des réseaux locaux virtuels et attribution de noms

Créez les réseaux locaux virtuels suivants sur Comm1 uniquement et attribuez-leur des noms :

- VLAN 10, nom = **Faculté/Personnel**
- VLAN 20, nom = **Participants**
- VLAN 30, nom = **Invité (par défaut)**
- VLAN 99, nom = **Gestion et Natif**

Étape 2. Vérification que les réseaux locaux virtuels sont envoyés vers Comm2 et Comm3

Quelle commande affiche les informations suivantes ? _____

```
VTP Version                     : 2
Configuration Revision          : 8
Maximum VLANs supported locally : 64
Number of existing VLANs        : 9
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xF5 0x50 0x30 0xB6 0x91 0x74 0x95 0xD9
Configuration last modified by 0.0.0.0 at 3-1-93 00:12:30
```

Quelle commande affiche les informations suivantes ? _____

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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
10   Faculté/Personnel                 active
20   Participants                      active
30   Invité(par défaut)                active
99   Gestione et Natif                 active
<résultat omis>
```

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 84 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 7 : configuration et vérification de VLAN 99

Étape 1. Exécution des étapes suivantes sur Comm1, Comm2 et Comm3

- Configurez et activez VLAN 99.
- Configurez la passerelle par défaut.
- Vérifiez que Comm1, Comm2 et Comm3 peuvent maintenant envoyer des requêtes ping vers SUD à l'adresse 10.1.99.1.

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 92 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 8 : configuration de Comm1 comme racine pour toutes les instances Spanning Tree

Étape 1. Configuration de Comm1 comme pont racine pour toutes les instances Spanning Tree, y compris les VLAN 1, 10, 20, 30 et 99

Remarquez que Comm3 a remporté la guerre des racines et est actuellement le pont racine pour toutes les instances Spanning Tree. Définissez la priorité à 4096 sur Comm1 pour toutes les arborescences complètes.

Étape 2. Vérification que Comm1 est maintenant le pont racine pour toutes les instances Spanning Tree

Seuls les résultats pour VLAN 1 sont affichés ci-dessous. Cependant, Comm1 doit être la racine de toutes les instances Spanning Tree. Quelle commande affiche les informations suivantes ?

_____

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     00D0.BC79.4B57
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4097  (priority 4096 sys-id-ext 1)
             Address     00D0.BC79.4B57
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/5            Desg FWD 19        128.3    Shr
<résultat omis>
```

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 96 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 9 : affectation des ports aux réseaux locaux virtuels

Étape 1. Affectation de ports sur Comm2 aux réseaux locaux virtuels

Packet Tracer évalue uniquement les ports reliés à PC1, PC2 et PC3.

- Configurez le port en mode d'accès.
- Affectez le port à son réseau local virtuel.

Les mappages de port des réseaux locaux virtuels sont les suivants :

- VLAN 99 : Fa0/1 – Fa0/5
- VLAN 10 : Fa0/6 – Fa0/10
- VLAN 20 : Fa0/11 – Fa0/15
- VLAN 30 : Fa0/16 – Fa0/20
- Non utilisés : Fa0/21 – Fa0/24 ; Gig1/1 ; Gig1/2

Par sécurité, désactivez les ports non utilisés.

Étape 2. Vérification des affectations des ports aux réseaux locaux virtuels

Quelle commande a été utilisée pour obtenir les résultats suivants présentant les affectations des réseaux locaux virtuels ?

_____

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig1/1, Gig1/2
10   Faculté/Personnel                 active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/10
20   Participants                      active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
30   Invité(par défaut)                active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20
99   Gestion et Natif                  active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 10 : test de la connectivité de bout en bout

Il est possible que Packet Tracer mette un certain temps à converger. Cependant, PC1, PC2 et PC3 parviendront finalement à envoyer des requêtes ping. Testez la connectivité vers PC-O, vers PC-E et vers le serveur Web. Si nécessaire, alternez entre les modes Simulation et Realtime (Temps réel) pour accélérer la convergence.

Exercice PT 4.3.2 : configuration de l'authentification OSPF

Diagramme de topologie

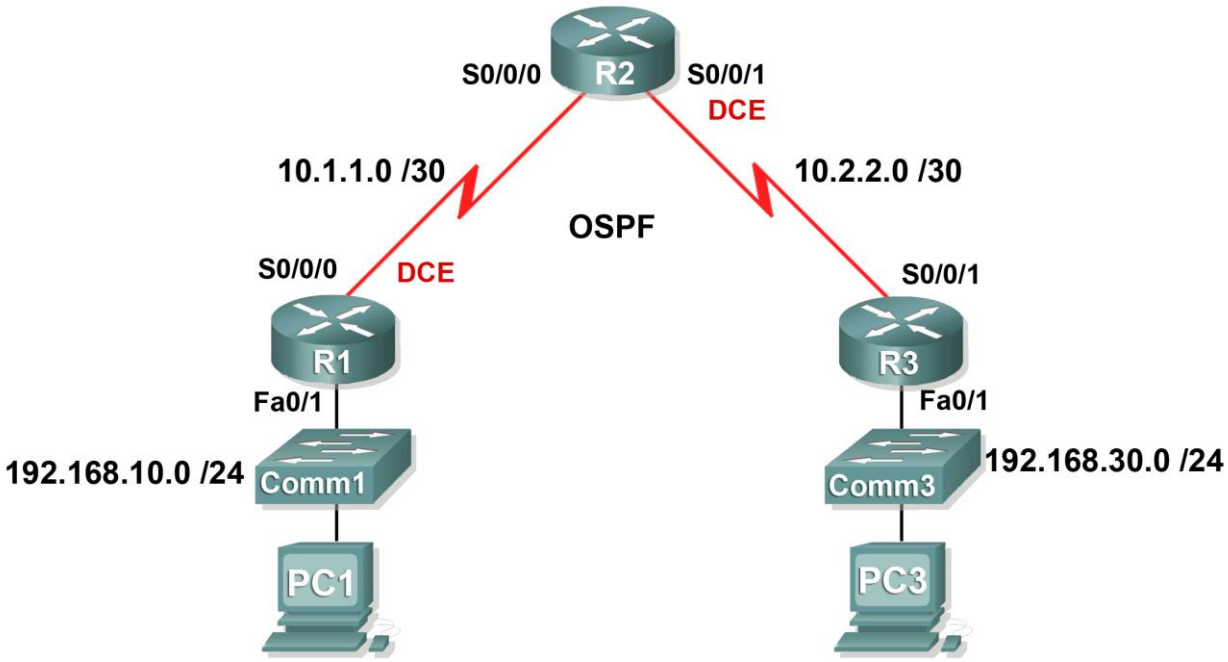


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
PC1	**Carte réseau**	192.168.10.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0

Objectifs pédagogiques

- Configurer une authentification simple OSPF
- Configurer une authentification MD5 OSPF
- Tester la connectivité

Présentation

Cet exercice porte sur l'authentification simple OSPF et sur l'authentification MD5 (message digest 5) OSPF. Vous pouvez activer l'authentification dans OSPF pour échanger des informations de mise à jour du routage de manière sécurisée. Si vous configurez une authentification simple, le mot de passe est envoyé sur le réseau sous forme de texte en clair. L'authentification simple est utilisée lorsque les périphériques d'une zone ne prennent pas en charge l'authentification MD5, qui est plus sûre. Si vous configurez une authentification MD5, le mot de passe n'est pas envoyé sur le réseau. MD5 est considéré comme le mode d'authentification OSPF le plus sûr. Lorsque vous configurez l'authentification, vous devez utiliser le même type d'authentification pour l'intégralité de la zone. Dans cet exercice, vous allez configurer une authentification simple entre R1 et R2, puis une authentification MD5 entre R2 et R3.

Tâche 1 : configuration d'une authentification simple OSPF

Étape 1. Configuration d'une authentification simple OSPF sur R1

Pour activer une authentification simple sur R1, passez en mode de configuration du routeur à l'aide de la commande **router ospf 1** à l'invite de configuration globale. Envoyez ensuite la commande **area 0 authentication** pour activer l'authentification.

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
Down: Interface down or detached
```

Finalement, un message s'affiche et indique que la contiguïté avec R2 est désactivée. R1 perd toutes les routes OSPF de sa table de routage jusqu'à ce qu'il parvienne à authentifier les routes avec R2. Bien que vous n'ayez pas encore configuré de mot de passe, R1 demande à ses voisins d'utiliser l'authentification dans les mises à jour et les messages de routage OSPF.

La commande **area 0 authentication** active l'authentification pour toutes les interfaces de la zone 0. Cette commande est suffisante pour R1, car il n'a pas besoin de prendre en charge d'autre type d'authentification.

Pour configurer R1 avec un mot de passe d'authentification simple, passez en mode de configuration d'interface pour la liaison avec R2. Envoyez alors la commande **ip ospf authentication-key cisco123**. Cette commande définit le mot de passe d'authentification **cisco123**.

```
R1(config-router)#interface S0/0/0
R1(config-if)#ip ospf authentication-key cisco123
```

Étape 2. Configuration d'une authentification simple OSPF sur R2

Vous avez configuré l'authentification sur R1 pour toute la zone. R2 pouvant prendre en charge à la fois l'authentification simple et l'authentification MD5, les commandes sont saisies au niveau de l'interface.

Passez en mode de configuration d'interface pour S0/0/0. Précisez que vous utilisez une authentification simple à l'aide de la commande **ip ospf authentication**. Envoyez alors la commande **ip ospf authentication-key cisco123** pour définir le mot de passe d'authentification **cisco123**.

```
R2(config)#interface S0/0/0
R2(config-if)#ip ospf authentication
R2(config-if)#ip ospf authentication-key cisco123
00:07:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done
```

Une fois ces tâches de configuration terminées, vous devez finalement voir un message indiquant que la contiguïté est rétablie entre R1 et R2. Les routes OSPF sont réinstallées dans la table de routage.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 50 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration d'une authentification MD5 OSPF

Étape 1. Configuration d'une authentification MD5 OSPF sur R3

Pour activer une authentification MD5 sur R3, passez en mode de configuration du routeur à l'aide de la commande **router ospf 1** à l'invite de configuration globale. Envoyez ensuite la commande **area 0 authentication message-digest** pour activer l'authentification.

```
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
Down: Interface down or detached
```

Finalement, un message s'affiche et indique que la contiguïté avec R2 est désactivée. R3 perd toutes les routes OSPF de sa table de routage jusqu'à ce qu'il parvienne à authentifier les routes avec R2.

Pour configurer R3 avec le mot de passe d'authentification MD5, passez en mode de configuration d'interface pour la liaison avec R2. Envoyez alors la commande **ip ospf message-digest-key 1 md5 cisco123**. Cette commande définit le mot de passe d'authentification OSPF **cisco123**, protégé par l'algorithme MD5.

```
R3(config-router)#interface S0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 cisco123
```

Étape 2. Configuration d'une authentification MD5 OSPF sur R2

Sur R2, passez en mode de configuration d'interface pour la liaison avec R3. Envoyez la commande **ip ospf authentication message-digest** pour activer l'authentification MD5. Cette commande est nécessaire sur R2 car ce routeur utilise deux types d'authentification.

Envoyez alors la commande **ip ospf message-digest-key 1 md5 cisco123** pour définir le mot de passe d'authentification.

```
R2(config)#interface S0/0/1
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 cisco123
00:13:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Serial0/0/1 from
EXCHANGE to FULL, Exchange Done
```

Après l'envoi de cette commande, attendez quelques instants que les routeurs convergent. Vous devez voir un message sur R2 et R3 indiquant que la contiguïté de voisins est rétablie. Vous pouvez confirmer que R2 a réinstallé les routes OSPF et que R3 est un voisin OSPF de R2.

```
R2#show ip route
<résultat omis>

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/65] via 10.1.1.1, 00:06:13, Serial0/0/0
O    192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:07, Serial0/0/1
```

```
R2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.10.1      1   FULL/-          00:00:32    10.1.1.1        Serial0/0/0
192.168.30.1      1   FULL/-          00:00:37    10.2.2.2        Serial0/0/1
```

Étape 3. Vérification des résultats

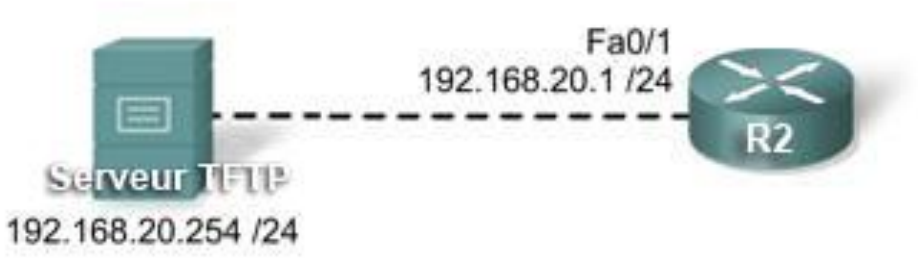
Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : test de la connectivité

L'authentification doit maintenant être correctement configurée sur les trois routeurs. Par conséquent, PC1 doit maintenant être en mesure d'envoyer une requête ping à PC3. Cliquez sur **Check Results**, puis sur **Connectivity Tests** pour voir si cela fonctionne.

Exercice PT 4.5.4 : utilisation d'un serveur TFTP pour mettre à niveau une image ISO Cisco

Diagramme de topologie



Objectifs pédagogiques

- Vérifier l'image IOS Cisco actuelle
- Configurer l'accès au serveur TFTP
- Télécharger une nouvelle image IOS Cisco
- Configurer la commande **boot system**
- Tester la nouvelle image IOS Cisco

Présentation

Dans cet exercice, vous allez configurer l'accès au serveur TFTP et télécharger une image IOS Cisco plus récente et plus évoluée. Packet Tracer simule la mise à niveau de l'image IOS Cisco sur un routeur mais ne simule pas la sauvegarde de celle-ci sur le serveur TFTP. De plus, même si l'image vers laquelle vous mettez à niveau est plus évoluée, cette simulation Packet Tracer ne fera pas apparaître des commandes plus évoluées. Le même ensemble de commandes Packet Tracer sera toujours actif.

Tâche 1 : vérification de l'image IOS Cisco actuelle

Étape 1. Utilisation de la commande show version pour vérifier l'image actuellement chargée dans la mémoire vive

```
R2#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbase-mz.123-14.T7.bin"
<résultat omis>
```

L'image actuellement chargée dans la mémoire vive ne prend pas en charge SSH ni de nombreuses autres fonctions évoluées.

Étape 2. Utilisation de la commande show flash pour vérifier les images actuellement disponibles en mémoire Flash

```
R2#show flash

System flash directory:
File  Length   Name/status
  1   13832032 c1841-ipbase-mz.123-14.T7.bin
[13832032 bytes used, 18682016 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)
```

Une seule image IOS Cisco est disponible. Afin de pouvoir utiliser SSH ainsi que des fonctions de sécurité supplémentaires, vous devez mettre à niveau l'image vers une version plus évoluée.

Tâche 2 : configuration de l'accès au serveur TFTP

R2 doit établir une connexion avec un serveur TFTP qui dispose de l'image IOS Cisco dont vous avez besoin.

Étape 1. Connexion de R2 au serveur TFTP

L'interface correcte est indiquée dans le diagramme de topologie.

Étape 2. Configuration d'une adresse IP pour R2

L'adressage IP correct est indiqué dans le diagramme de topologie.

Étape 3. Configuration de l'adressage IP et d'une passerelle par défaut pour le serveur TFTP

L'adressage IP correct est indiqué dans le diagramme de topologie.

Étape 4. Test de connectivité

R2 doit être en mesure d'envoyer une requête ping au serveur TFTP. Si ce n'est pas le cas, vérifiez le câblage et l'adressage.

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 80 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : téléchargement d'une nouvelle image IOS Cisco

Étape 1. Vérification des images IOS Cisco présentes sur le serveur TFTP

Cliquez sur le serveur TFTP puis sur l'onglet **Config**. Remarquez que plusieurs images sont disponibles. Vous allez télécharger l'image c1841-ipbasek9-mz.124-12.bin sur R2.

Étape 2. Téléchargement de l'image c1841-ipbasek9-mz.124-12.bin sur R2

- Sur R2, lancez le processus de téléchargement à l'aide de la commande **copy tftp flash**.
- Entrez l'adresse IP du serveur TFTP.
- Entrez le nom de fichier complet de l'image IOS Cisco

```
R2#copy tftp flash
Address or name of remote host []? 192.168.20.254
Source filename []? c1841-ipbasek9-mz.124-12.bin
Destination filename [c1841-ipbasek9-mz.124-12.bin]? Entrée
Accessing tftp://192.168.20.254/c1841-ipbasek9-mz.124-12.bin...
Loading c1841-ipbasek9-mz.124-12.bin from 192.168.20.254:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
[OK - 16599160 bytes]

16599160 bytes copied in 13.047 secs (284682 bytes/sec)
R2#
```

Étape 3. Vérification que la nouvelle image est maintenant dans la mémoire Flash

```
R2#show flash

System flash directory:
File  Length   Name/status
  1   13832032 c1841-ipbase-mz.123-14.T7.bin
  2   16599160 c1841-ipbasek9-mz.124-12.bin
[30431192 bytes used, 2082856 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)

R2#
```

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 90 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : configuration de la commande boot system

Par défaut, la séquence d'amorçage du routeur charge la première image IOS Cisco de la liste en mémoire Flash. Une manière de s'assurer que le routeur charge la nouvelle image consiste à configurer la commande **boot system flash**. Sur R2, entrez la commande suivante :

```
R2(config)#boot system flash c1841-ipbasek9-mz.124-12.bin
```

Cette commande fait maintenant partie de la configuration en cours. Cependant, la configuration doit également être enregistrée en mémoire vive non volatile. Si ce n'est pas fait, la configuration sera écrasée au prochain rechargement du routeur.

```
R2(config)#end
R2#copy running-config startup-config
```

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 5 : test de la nouvelle image

Rechargez R2 et attendez qu'il redémarre. Lorsque le routeur recharge, vérifiez que la nouvelle image est dans la mémoire vive à l'aide de la commande **show version**.

```
R2#reload
Proceed with reload? [confirm] [Entrée]

%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
<résultat omis>

R2>show version
Cisco IOS Software, 1841 Software (C1841-IPBASEK9-M), Version 12.4(12),
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbasek9-mz.124-12.bin"
<résultat omis>
```

Exercice PT 4.7.1 : exercice d'intégration des compétences Packet Tracer

Diagramme de topologie

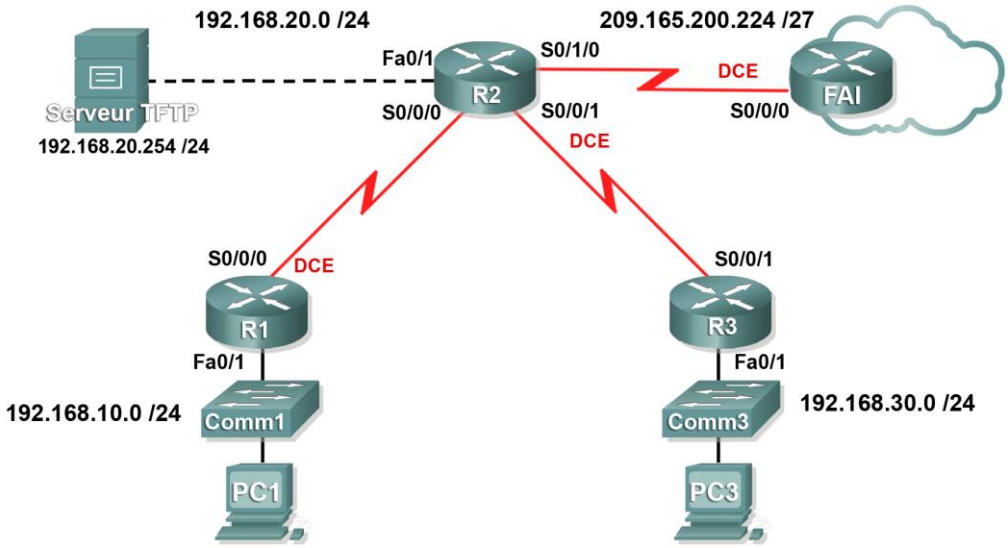


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
FAI	**S0/0/0**	209.165.200.226	255.255.255.252
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255255.255.252
R2	**Fa0/1**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
PC1	**Carte réseau**	192.168.10.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0
Serveur TFTP	**Carte réseau**	192.168.20.254	255.255.255.255

Objectifs pédagogiques

- Configurer le routage
- Configurer l'authentification OSPF
- Mettre à niveau l'image IOS Cisco

Présentation

Cet exercice est une révision globale du chapitre portant sur le routage OSPF, l'authentification et la mise à niveau de l'image IOS Cisco.

Tâche 1 : configuration du routage

Étape 1. Configuration d'une route par défaut vers FAI

Sur R2, configurez une route par défaut vers FAI à l'aide de l'argument d'interface de sortie.

Étape 2. Configuration du routage OSPF entre R1, R2 et R3

Configurez le routage OSPF sur les trois routeurs. Utilisez l'ID de processus 1. Désactivez les mises à jour OSPF sur les interfaces appropriées.

Étape 3. Création de la route par défaut

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 59 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration de l'authentification OSPF

Étape 1. Configuration de l'authentification MD5 entre R1, R2 et R3

Configurez l'authentification MD5 OSPF entre R1, R2 et R3 en utilisant la valeur de clé **1** et le mot de passe **cisco123**.

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 91 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : mise à niveau de l'image IOS Cisco

Étape 1. Copie d'une image plus récente en mémoire Flash de R2 à partir du serveur TFTP

Consultez l'onglet Config du serveur TFTP afin d'identifier le nom de l'image IOS Cisco la plus récente. Copiez ensuite celle-ci dans la mémoire Flash de R2.

Étape 2. Configuration de R2 pour démarrer avec la nouvelle image

Étape 3. Enregistrement de la configuration et rechargement

Vérifiez que la nouvelle image est chargée dans la mémoire vive.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Exercice PT 5.2.8 : configuration de listes de contrôle d'accès standard

Diagramme de topologie

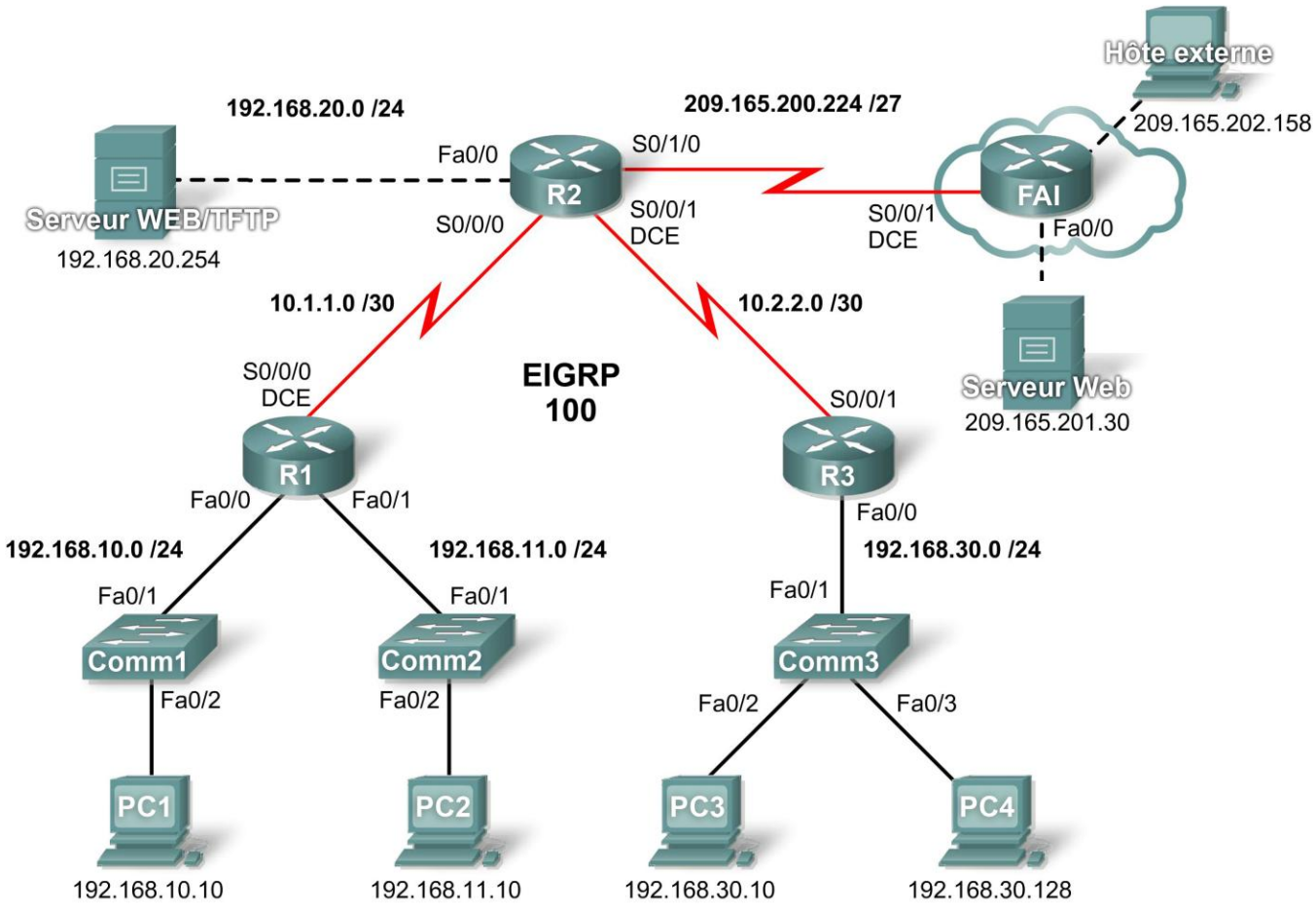


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**S0/0/0**	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	**S0/0/1**	10.2.2.2	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
FAI	**S0/0/1**	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	**Carte réseau**	192.168.10.10	255.255.255.0
PC2	**Carte réseau**	192.168.11.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0
PC4	**Carte réseau**	192.168.30.128	255.255.255.0
Serveur TFTP/Web	**Carte réseau**	192.168.20.254	255.255.255.0
Serveur Web	**Carte réseau**	209.165.201.30	255.255.255.224
Hôte externe	**Carte réseau**	209.165.202.158	255.255.255.224

Objectifs pédagogiques

- Étudier la configuration actuelle du réseau
- Évaluer une stratégie de réseau et planifier la mise en œuvre de listes de contrôle d'accès
- Configurer des listes de contrôle d'accès standard numérotées
- Configurer des listes de contrôle d'accès standard nommées

Présentation

Les listes de contrôle d'accès standard sont des scripts de configuration du routeur qui définissent si celui-ci autorise ou refuse des paquets en fonction de l'adresse source. Cet exercice porte principalement sur la définition de critères de filtrage, la configuration de listes de contrôle d'accès standard, l'application de ces listes aux interfaces des routeurs, ainsi que sur la vérification et le test de leur mise en œuvre. Les routeurs sont déjà configurés, notamment les adresses IP et le routage EIGRP. Le mot de passe d'exécution utilisateur est **cisco** et le mot de passe d'exécution privilégié est **class**.

Tâche 1 : étude de la configuration actuelle du réseau

Étape 1. Affichage de la configuration en cours sur les routeurs

Affichez les configurations en cours sur les trois routeurs à l'aide de la commande **show running-config** en mode d'exécution privilégié. Remarquez que les interfaces et le routage sont entièrement configurés. Comparez les configurations d'adresses IP à la table d'adressage ci-dessus. Aucune liste de contrôle d'accès ne doit être configurée sur les routeurs à ce stade.

Aucune configuration du routeur FAI n'est nécessaire au cours de cet exercice. Considérez que vous n'êtes pas responsable du routeur FAI et que celui-ci est configuré et entretenu par l'administrateur FAI.

Étape 2. Vérification que tous les périphériques ont accès à tous les autres emplacements

Avant d'appliquer des listes de contrôle d'accès à un réseau, il est important de vérifier que vous disposez d'une connectivité complète. Si vous ne testez pas la connectivité de votre réseau avant d'appliquer une liste de contrôle d'accès, le dépannage sera plus difficile.

Pour tester la connectivité, vous pouvez afficher la table de routage de chaque périphérique et vérifier que tous les réseaux y sont présents. Sur R1, R2 et R3, lancez la commande **show ip route**. Vous devez voir que chaque périphérique dispose de routes connectées vers les réseaux reliés et de routes dynamiques vers tous les autres réseaux distants. Tous les périphériques ont accès à tous les autres emplacements.

Bien que la table de routage soit utile pour évaluer l'état du réseau, vous pouvez cependant tester la connectivité à l'aide de la commande **ping**. Effectuez les tests suivants :

- À partir de PC1, envoyez une requête ping à PC2.
- À partir de PC2, envoyez une requête ping à Hôte externe.
- À partir de PC4, envoyez une requête ping au serveur Web/TFTP.

Tous ces tests de connectivité doivent réussir.

Tâche 2 : évaluation d'une stratégie de réseau et planification de la mise en œuvre de listes de contrôle d'accès

Étape 1. Évaluation de la stratégie pour les réseaux locaux de R1

- Le réseau 192.168.10.0/24 a accès à tous les emplacements, à l'exception du réseau 192.168.11.0/24.
- Le réseau 192.168.11.0/24 a accès à toutes les destinations, à l'exception des réseaux connectés à FAI.

Étape 2. Planification de la mise en œuvre des listes de contrôle d'accès pour les réseaux locaux de R1

- Deux listes de contrôle d'accès permettent de mettre en œuvre intégralement la stratégie de sécurité pour les réseaux locaux de R1.
- La première liste de contrôle d'accès sur R1 refuse le trafic du réseau 192.168.10.0/24 vers le réseau 192.168.11.0/24 mais autorise tout autre trafic.
- Cette première liste, appliquée en sortie sur l'interface Fa0/1, surveille tout le trafic envoyé vers le réseau 192.168.11.0.
- La seconde liste de contrôle d'accès sur R2 refuse au réseau 192.168.11.0/24 l'accès à FAI mais autorise tout autre trafic.
- Le trafic sortant de l'interface S0/1/0 est contrôlé.
- Classez les instructions des listes de contrôle d'accès par ordre décroissant de spécificité. Le refus de l'accès d'un trafic réseau à un autre réseau est prioritaire sur l'autorisation de tout autre trafic.

Étape 3. Évaluation de la stratégie pour le réseau local de R3

- Le réseau 192.168.30.0/10 a accès à toutes les destinations.
- L'hôte 192.168.30.128 n'est pas autorisé à accéder hors du réseau local.

Étape 4. Planification de la mise en œuvre des listes de contrôle d'accès pour le réseau local de R3

- Une liste de contrôle d'accès permet de mettre en œuvre intégralement la stratégie de sécurité pour le réseau local de R3.
- La liste de contrôle d'accès est placée sur R3 et refuse à l'hôte 192.168.30.128 l'accès hors du réseau local mais autorise le trafic en provenance de tous les autres hôtes du réseau local.
- Si elle est appliquée en entrée sur l'interface Fa0/0, cette liste de contrôle d'accès surveille tout trafic essayant de quitter le réseau 192.168.30.0/10.
- Classez les instructions des listes de contrôle d'accès par ordre décroissant de spécificité. Le refus de l'accès de l'hôte 192.168.30.128 est prioritaire sur l'autorisation de tout autre trafic.

Tâche 3 : configuration de listes de contrôle d'accès standard numérotées

Étape 1. Définition du masque générique

Le masque générique d'une instruction de liste de contrôle d'accès détermine la proportion d'une adresse de destination ou d'une adresse source IP qui doit être vérifiée. Un bit à 0 indique que cette valeur doit correspondre dans l'adresse, tandis qu'un bit à 1 ignore cette valeur dans l'adresse. N'oubliez pas que les listes de contrôle d'accès standard peuvent uniquement contrôler les adresses source.

- Étant donné que la liste de contrôle d'accès sur R1 refuse tout trafic du réseau 192.168.10.0/24, toute adresse IP source commençant par 192.168.10 est refusée. Le dernier octet de l'adresse IP pouvant être ignoré, le masque générique qui convient est 0.0.0.255. Chaque octet de ce masque peut être considéré comme « contrôler, contrôler, contrôler, ignorer ».
- La liste de contrôle d'accès sur R2 refuse également le trafic du réseau 192.168.11.0/24. Vous pouvez appliquer le même masque générique, 0.0.0.255.

Étape 2. Définition des instructions

- Les listes de contrôle d'accès sont configurées en mode de configuration globale.
- Pour les listes de contrôle d'accès standard, utilisez un nombre entre 1 et 99. Le nombre **10** est utilisé pour cette liste sur R1 afin de rappeler que celle-ci surveille le réseau 192.168.**10**.0.
- Sur R2, la liste d'accès **11 refuse** tout trafic en provenance du réseau 192.168.**11**.0 vers tout réseau FAI. Par conséquent, l'option **deny** est configurée avec le réseau **192.168.11.0** et le masque générique **0.0.0.255**.
- Tout autre trafic doit être autorisé à l'aide de l'option **permit** en raison du refus implicite (« deny any ») à la fin des listes de contrôle d'accès. L'option **any** indique tout hôte source.

Configurez ce qui suit sur R1 :

```
R1(config)#access-list 10 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit any
```

Remarque : Packet Tracer évalue une configuration de liste de contrôle d'accès seulement lorsque toutes les instructions sont saisies dans l'ordre correct.

Créez maintenant une liste de contrôle d'accès sur R2 pour refuser le réseau 192.168.11.0 et autoriser tous les autres réseaux. Utilisez le numéro **11** pour cette liste de contrôle d'accès. Configurez ce qui suit sur R2 :

```
R2(config)#access-list 11 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 11 permit any
```

Étape 3. Application des instructions aux interfaces

Sur R1, passez en mode de configuration pour l'interface Fa0/1.

Lancez la commande **ip access-group 10 out** pour appliquer la liste de contrôle d'accès standard en sortie de l'interface.

```
R1(config)#interface fa0/1
R1(config-if)#ip access-group 10 out
```

Sur R2, passez en mode de configuration pour l'interface S0/1/0.

Lancez la commande **ip access-group 11 out** pour appliquer la liste de contrôle d'accès standard en sortie de l'interface.

```
R2(config)#interface s0/1/0
R2(config-if)#ip access-group 11 out
```

Étape 4. Vérification et test des listes de contrôle d'accès

Une fois les listes de contrôle d'accès configurées et appliquées, PC1 (192.168.10.10) ne doit pas être en mesure d'envoyer de requête ping à PC2 (192.168.11.10) car la liste de contrôle d'accès est appliquée en sortie de Fa0/1 sur R1.

PC2 (192.168.11.10) ne doit pas être en mesure d'envoyer de requête ping au serveur Web (209.165.201.30) ni à Hôte externe (209.165.202.158) mais doit pouvoir le faire vers toutes les autres destinations, car la liste de contrôle d'accès est appliquée en sortie de l'interface S0/1/0 sur R2. Cependant, PC2 ne peut pas envoyer de requête ping à PC1 car la liste de contrôle d'accès 10 sur R1 empêche la réponse d'écho de PC1 à PC2.

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 67 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : configuration d'une liste de contrôle d'accès standard nommée

Étape 1. Définition du masque générique

- La stratégie d'accès pour R3 indique que l'hôte à l'adresse 192.168.30.128 ne doit pas pouvoir accéder hors du réseau local. Tous les autres hôtes du réseau 192.168.30.0 doivent pouvoir accéder à tous les autres emplacements.
- Pour vérifier un seul hôte, il est nécessaire de vérifier l'intégralité de l'adresse IP. Le mot de passe **host** permet cela.
- Tous les paquets ne correspondant pas à l'instruction relative à l'hôte sont autorisés.

Étape 2. Définition des instructions

- Sur R3, passez en mode de configuration globale.
- Créez une liste de contrôle d'accès nommée NO_ACCESS à l'aide de la commande **ip access-list standard NO_ACCESS**. Vous passez en mode de configuration de liste de contrôle d'accès. Toutes les instructions permit et deny sont configurées à partir de ce mode de configuration.
- Refusez le trafic en provenance de l'hôte 192.168.30.128 à l'aide de l'option **host**.
- Autorisez tout autre trafic à l'aide de **permit any**.

Configurez la liste de contrôle d'accès nommée suivante sur R3 :

```
R3(config)#ip access-list standard NO_ACCESS
R3(config-std-nacl)#deny host 192.168.30.128
R3(config-std-nacl)#permit any
```

Étape 3. Application des instructions à l'interface correcte

Sur R3, passez en mode de configuration pour l'interface Fa0/0.

Lancez la commande **ip access-group NO_ACCESS in** pour appliquer la liste de contrôle d'accès nommée en entrée de l'interface. Avec cette commande, tout le trafic entrant sur l'interface Fa0/0 en provenance du réseau local 192.168.30.0/24 est contrôlé par rapport à la liste de contrôle d'accès.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group NO_ACCESS in
```

Étape 4. Vérification et test des listes de contrôle d'accès

Cliquez sur **Check Results**, puis sur **Connectivity Tests**. Les tests suivants doivent échouer :

- PC1 vers PC2
- PC2 vers Hôte externe
- PC2 vers Serveur Web
- Toutes les requêtes ping en provenance de/vers PC4, sauf entre PC3 et PC4.

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Exercice PT 5.3.4 : configuration de listes de contrôle d'accès étendues

Diagramme de topologie

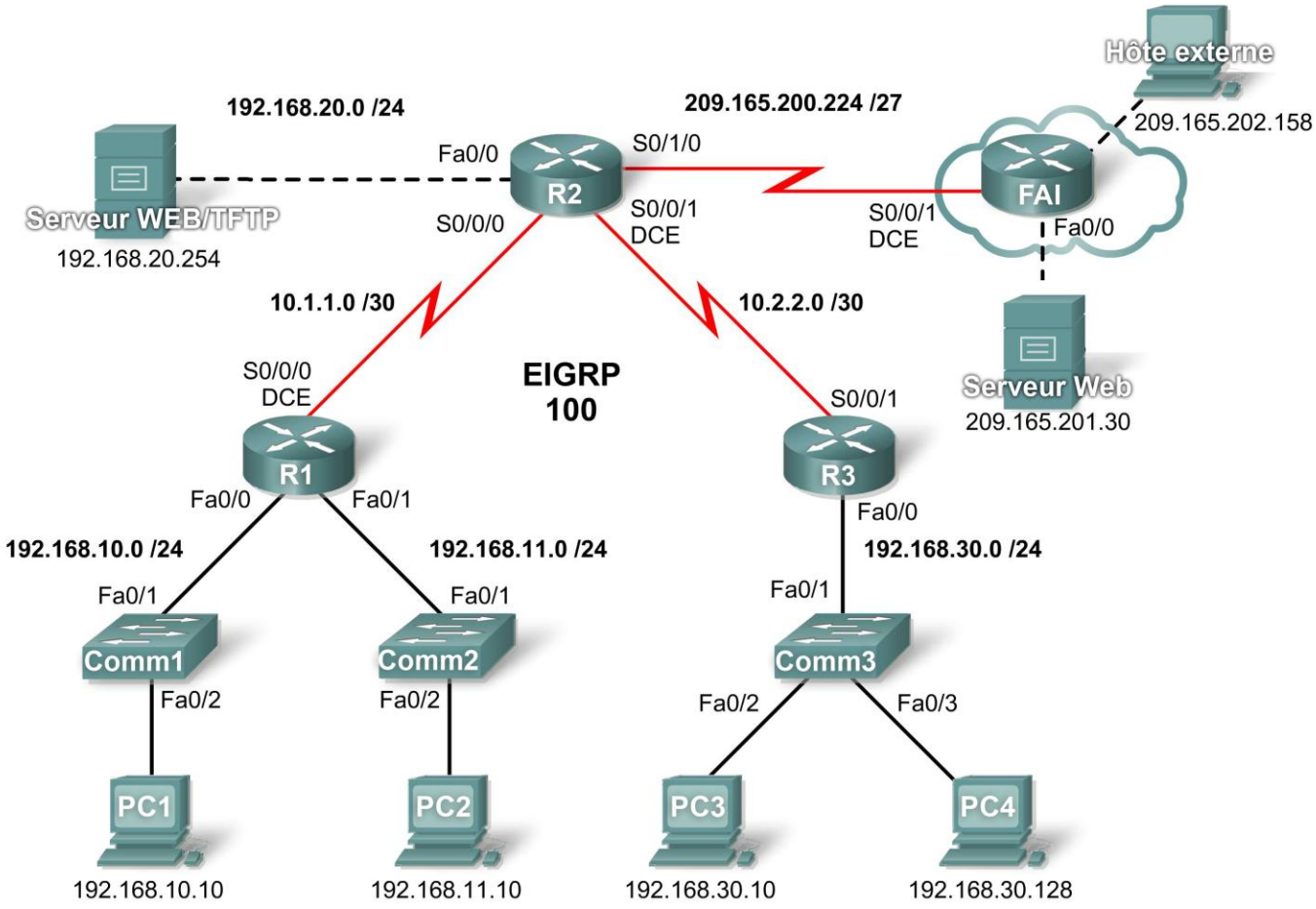


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**S0/0/0**	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.2	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	**S0/0/1**	10.2.2.1	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
FAI	**S0/0/1**	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	**Carte réseau**	192.168.10.10	255.255.255.0
PC2	**Carte réseau**	192.168.11.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0
PC4	**Carte réseau**	192.168.30.128	255.255.255.0
Serveur TFTP/Web	**Carte réseau**	192.168.20.254	255.255.255.0
Serveur Web	**Carte réseau**	209.165.201.30	255.255.255.224
Hôte externe	**Carte réseau**	209.165.202.158	255.255.255.224

Objectifs pédagogiques

- Étudier la configuration actuelle du réseau
- Évaluer une stratégie de réseau et planifier la mise en œuvre de listes de contrôle d'accès
- Configurer des listes de contrôle d'accès étendues numérotées
- Configurer des listes de contrôle d'accès étendues nommées

Présentation

Les listes de contrôle d'accès étendues sont des scripts de configuration du routeur qui définissent si celui-ci autorise ou refuse des paquets selon l'adresse source ou de destination, ainsi qu'en fonction de protocoles ou de ports. Les listes de contrôle d'accès étendues offrent une meilleure souplesse et une plus grande précision que les listes de contrôle d'accès standard. Cet exercice porte principalement sur la définition de critères de filtrage, la configuration de listes de contrôle d'accès étendues, l'application de ces listes aux interfaces des routeurs, ainsi que sur la vérification et le test de leur mise en œuvre. Les routeurs sont déjà configurés, notamment les adresses IP et le routage EIGRP. Le mot de passe d'exécution utilisateur est **cisco** et le mot de passe d'exécution privilégié est **class**.

Tâche 1 : étude de la configuration actuelle du réseau

Étape 1. Affichage de la configuration en cours sur les routeurs

Affichez les configurations en cours sur les trois routeurs à l'aide de la commande **show running-config** en mode d'exécution privilégié. Remarquez que les interfaces et le routage sont entièrement configurés. Comparez les configurations d'adresses IP à la table d'adressage ci-dessus. Aucune liste de contrôle d'accès ne doit être configurée sur les routeurs à ce stade.

Aucune configuration du routeur FAI n'est nécessaire au cours de cet exercice. Il est supposé que vous n'êtes pas responsable du routeur FAI et que celui-ci est configuré et entretenu par l'administrateur FAI.

Étape 2. Vérification que tous les périphériques ont accès à tous les autres emplacements

Avant d'appliquer des listes de contrôle d'accès à un réseau, il est important de vérifier que vous disposez d'une connectivité complète. Si vous ne testez pas la connectivité de votre réseau avant d'appliquer une liste de contrôle d'accès, le dépannage sera plus difficile.

Afin de garantir la connectivité sur tout le réseau, utilisez les commandes **ping** et **tracert** entre les différents périphériques réseau pour vérifier les connexions.

Tâche 2 : évaluation d'une stratégie de réseau et planification de la mise en œuvre de listes de contrôle d'accès

Étape 1. Évaluation de la stratégie pour les réseaux locaux de R1

- Pour le réseau 192.168.10.0/24, bloquez l'accès Telnet vers tous les emplacements et l'accès TFTP au serveur Web/TFTP d'entreprise à l'adresse 192.168.20.254. Tout autre accès est autorisé.
- Pour le réseau 192.168.11.0/24, autorisez l'accès TFTP et l'accès Web au serveur Web/TFTP d'entreprise à l'adresse 192.168.20.254. Bloquez tout autre trafic en provenance du réseau 192.168.11.0/24 vers le réseau 192.168.20.0/24. Tout autre accès est autorisé.

Étape 2. Planification de la mise en œuvre des listes de contrôle d'accès pour les réseaux locaux de R1

- Deux listes de contrôle d'accès permettent de mettre en œuvre intégralement la stratégie de sécurité pour les réseaux locaux de R1.
- La première liste prend en charge la première partie de la stratégie et est configurée sur R1 et appliquée en entrée de l'interface Fast Ethernet 0/0.
- La seconde liste prend en charge la seconde partie de la stratégie et est configurée sur R1 et appliquée en entrée de l'interface Fast Ethernet 0/1.

Étape 3. Évaluation de la stratégie pour le réseau local de R3

- L'accès aux adresses IP du réseau 192.168.20.0/24 est bloqué pour toutes les adresses IP du réseau 192.168.30.0/24.
- La première moitié du réseau 192.168.30.0/24 a accès à toutes les destinations.
- La seconde moitié du réseau 192.168.30.0/24 a accès aux réseaux 192.168.10.0/24 et 192.168.11.0/24.
- La seconde moitié du réseau 192.168.30.0/24 dispose d'un accès Web et ICMP à toutes les autres destinations.
- Tout autre accès est implicitement refusé.

Étape 4. Planification de la mise en œuvre des listes de contrôle d'accès pour le réseau local de R3

Cette étape requiert la configuration d'une liste de contrôle d'accès sur R3, appliquée en entrée de l'interface Fast Ethernet 0/0.

Étape 5. Évaluation de la stratégie pour le trafic en provenance d'Internet via le fournisseur de services Internet (FAI)

- Les hôtes externes peuvent établir une session Web avec le serveur Web interne uniquement sur le port 80.
- Seules les sessions TCP établies sont autorisées en entrée.
- Seules les réponses ping sont autorisées via R2.

Étape 6. Planification de la mise en œuvre des listes de contrôle d'accès pour le trafic en provenance d'Internet via le fournisseur de services Internet (FAI)

Cette étape requiert la configuration d'une liste de contrôle d'accès sur R2, appliquée en entrée de l'interface Serial 0/1/0.

Tâche 3 : configuration de listes de contrôle d'accès étendues numérotées

Étape 1. Définition des masques génériques

Deux listes de contrôle d'accès sont nécessaires pour appliquer la stratégie de contrôle d'accès sur R1. Ces deux listes doivent être conçues pour refuser un réseau de classe C complet. Vous allez configurer un masque générique correspondant à tous les hôtes de chacun de ces réseaux de classe C.

Par exemple, pour l'intégralité du sous-réseau de 192.168.10.0/24 à associer, le masque générique est 0.0.0255. Cela peut être considéré comme « contrôler, contrôler, contrôler, ignorer » et correspond par définition au réseau 192.168.10.0/24 dans sa totalité.

Étape 2. Configuration de la première liste de contrôle d'accès étendue pour R1

En mode de configuration globale, configurez la première liste de contrôle d'accès avec le numéro 110. Vous souhaitez tout d'abord bloquer le trafic Telnet vers tout emplacement pour toutes les adresses IP du réseau 192.168.10.0/24.

Lorsque vous écrivez l'instruction, vérifiez que vous vous trouvez bien en mode de configuration globale.

```
R1(config)#access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
```

Bloquez ensuite pour toutes les adresses IP du réseau 192.168.10.0/24 l'accès TFTP à l'hôte à l'adresse 192.168.20.254.

```
R1(config)#access-list 110 deny udp 192.168.10.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Enfin, autorisez tout autre trafic.

```
R1(config)#access-list 110 permit ip any any
```

Étape 3. Configuration de la seconde liste de contrôle d'accès étendue pour R1

Configurez la seconde liste de contrôle d'accès avec le numéro 111. Autorisez l'accès www à l'hôte ayant l'adresse 192.168.20.254 à toute adresse IP du réseau 192.168.11.0/24.

```
R1(config)#access-list 111 permit tcp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq www
```

Autorisez ensuite l'accès TFTP à l'hôte ayant l'adresse 192.168.20.254 à toutes les adresses IP du réseau 192.168.11.0/24.

```
R1(config)#access-list 111 permit udp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Bloquez tout autre trafic en provenance du réseau 192.168.11.0/24 vers le réseau 192.168.20.0/24.

```
R1(config)#access-list 111 deny ip 192.168.11.0 0.0.0.255 192.168.20.0
0.0.0.255
```

Enfin, autorisez tout autre trafic. Cette instruction garantit que le trafic en provenance d'autres réseaux n'est pas bloqué.

```
R1(config)#access-list 111 permit ip any any
```

Étape 4. Vérification de la configuration des listes de contrôle d'accès

Pour confirmer les configurations sur R1, lancez la commande **show access-lists**. Le résultat doit être similaire à celui-ci :

```
R1#show access-lists
Extended IP access list 110
   deny tcp 192.168.10.0 0.0.0.255 any eq telnet
   deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
   permit ip any any
Extended IP access list 111
   permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
   permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
   deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
   permit ip any any
```

Étape 5. Application des instructions aux interfaces

Pour appliquer une liste de contrôle d'accès à une interface, passez en mode de configuration d'interface. Configurez la commande **ip access-group** *numéro-liste-accès* {**in** | **out**} pour appliquer la liste de contrôle d'accès à l'interface.

Chaque liste de contrôle d'accès filtre le trafic entrant. Appliquez la liste 110 à l'interface Fast Ethernet 0/0 et la liste 111 à l'interface Fast Ethernet 0/1.

```
R1(config)#interface fa0/0
R1(config-if)#ip access-group 110 in
R1(config-if)#interface fa0/1
R1(config-if)#ip access-group 111 in
```

Vérifiez que les listes de contrôle d'accès apparaissent dans la configuration en cours de R1 et qu'elles ont été appliquées aux interfaces correctes.

Étape 6. Test des listes de contrôle d'accès configurées sur R1

Une fois les listes de contrôle d'accès configurées et appliquées, il est très important de tester si le trafic est bloqué ou autorisé comme prévu.

- À partir de PC1, essayez d'obtenir un accès Telnet à n'importe quel périphérique. Cette opération doit être bloquée.
- À partir de PC1, essayez d'accéder au serveur Web/TFTP d'entreprise via le protocole HTTP. Cette opération doit être autorisée.

- À partir de PC2, essayez d'accéder au serveur Web/TFTP via le protocole HTTP. Cette opération doit être autorisée.
- À partir de PC2, essayez d'accéder au serveur Web externe via le protocole HTTP. Cette opération doit être autorisée.

En vous basant sur vos connaissances des listes de contrôle d'accès, réalisez quelques tests de connectivité supplémentaires à partir de PC1 et de PC2.

Étape 7. Vérification des résultats

Packet Tracer ne prenant pas en charge le test de l'accès TFTP, vous ne pourrez pas vérifier cette stratégie. Cependant, votre taux de réalisation doit être de 50 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : configuration d'une liste de contrôle d'accès étendue numérotée pour R3

Étape 1. Définition du masque générique

La stratégie d'accès pour la moitié inférieure des adresses IP du réseau 192.168.30.0/24 requiert les conditions suivantes :

- Refus de l'accès au réseau 192.168.20.0/24
- Autorisation de l'accès vers toutes les autres destinations

La moitié supérieure des adresses IP du réseau 192.168.30.0/24 possède les restrictions suivantes :

- Autorisation de l'accès à 192.168.10.0 et à 192.168.11.0
- Refus de l'accès à 192.168.20.0
- Autorisation des accès Web et ICMP vers tous les autres emplacements

Pour définir le masque générique, réfléchissez aux bits qui doivent être testés pour que la liste de contrôle d'accès corresponde aux adresses IP 0-127 (moitié inférieure) ou 128-255 (moitié supérieure).

Rappelez-vous qu'une manière de déterminer le masque générique consiste à soustraire le masque réseau normal de 255.255.255.255. Le masque normal pour les adresses IP 0-127 et 128-255 dans le cas d'une adresse de classe C est 255.255.255.128. En utilisant la méthode par soustraction, voici le masque générique qui convient :

```
   255.255.255.255
 - 255.255.255.128
-----------------
     0. 0. 0.127
```

Étape 2. Configuration des listes de contrôle d'accès étendues sur R3

Sur R3, passez en mode de configuration globale et configurez la liste de contrôle d'accès avec le numéro de liste d'accès 130.

La première instruction empêche l'hôte 192.168.30.0/24 d'accéder à toutes les adresses du réseau 192.168.30.0/24.

```
R3(config)#access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255
```

La seconde instruction permet à la moitié inférieure du réseau 192.168.30.0/24 d'accéder à toutes les autres destinations.

```
R3(config)#access-list 130 permit ip 192.168.30.0 0.0.0.127 any
```

Les instructions suivantes autorisent explicitement la moitié supérieure du réseau 192.168.30.0/24 à accéder aux réseaux et aux services permis par la stratégie réseau.

```
R3(config)#access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0
0.0.0.255
R3(config)# access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0
0.0.0.255
R3(config)# access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www
R3(config)# access-list 130 permit icmp 192.168.30.128 0.0.0.127 any
R3(config)# access-list 130 deny ip any any
```

Étape 3. Application de l'instruction à l'interface

Pour appliquer une liste de contrôle d'accès à une interface, passez en mode de configuration d'interface. Configurez la commande **ip access-group** *numéro-liste-accès* {**in** | **out**} pour appliquer la liste de contrôle d'accès à l'interface.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group 130 in
```

Étape 4. Vérification et test des listes de contrôle d'accès

Une fois la liste de contrôle d'accès configurée et appliquée, il est très important de tester si le trafic est bloqué ou autorisé comme prévu.

- À partir de PC3, envoyez une requête ping au serveur Web/TFTP. Cette opération doit être bloquée.
- À partir de PC3, envoyez une requête ping vers tout autre périphérique. Cette opération doit être autorisée.
- À partir de PC4, envoyez une requête ping au serveur Web/TFTP. Cette opération doit être bloquée.
- À partir de PC4, ouvrez une session Telnet vers R1 à l'adresse 192.168.10.1 ou 192.168.11.1. Cette opération doit être autorisée.
- À partir de PC4, envoyez une requête ping à PC1 et à PC2. Cette opération doit être autorisée.
- À partir de PC4, ouvrez une session Telnet vers R2 à l'adresse 10.2.2.2. Cette opération doit être bloquée.

Une fois que les tests ont donné les résultats attendus, lancez la commande d'exécution privilégiée **show access-lists** sur R3 pour vérifier que les instructions de liste de contrôle d'accès ont des correspondances.

En vous basant sur vos connaissances des listes de contrôle d'accès, réalisez d'autres tests pour vérifier que chaque instruction correspond au trafic correct.

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 75 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 5 : configuration d'une liste de contrôle d'accès étendue nommée

Étape 1. Configuration d'une liste de contrôle d'accès étendue nommée sur R2

Rappelez-vous que la stratégie sur R2 doit être conçue pour filtrer le trafic Internet. R2 ayant une connexion au fournisseur de services (FAI), il constitue le meilleur emplacement pour la liste de contrôle d'accès.

Configurez une liste de contrôle d'accès nommée FIREWALL sur R2 à l'aide de la commande **ip access-list extended** *nom*. Cette commande place le routeur en mode de configuration de liste de contrôle d'accès nommée. Remarquez que l'invite du routeur est différente.

```
R2(config)#ip access-list extended FIREWALL
R2(config-ext-nacl)#
```

En mode de configuration de liste de contrôle d'accès, ajoutez les instructions de filtrage du trafic décrites dans la stratégie :

- Les hôtes externes peuvent établir une session Web avec le serveur Web interne uniquement sur le port 80.
- Seules les sessions TCP établies sont autorisées en entrée.
- Les réponses ping sont autorisées via R2.

```
R2(config-ext-nacl)#permit tcp any host 192.168.20.254 eq www
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#deny ip any any
```

Une fois la liste de contrôle d'accès configurée sur R2, lancez la commande **show access-lists** pour vérifier que la liste contient les instructions correctes.

Étape 2. Application de l'instruction à l'interface

Lancez la commande **ip access-group** *nom* {**in** | **out**} pour appliquer la liste de contrôle d'accès en entrée de l'interface de R2 reliée à FAI.

```
R3(config)#interface s0/1/0
R3(config-if)#ip access-group FIREWALL in
```

Étape 3. Vérification et test des listes de contrôle d'accès

Réalisez les tests suivants pour vous assurer que la liste de contrôle d'accès fonctionne comme prévu :

- À partir de Outside Host, ouvrez une page Web sur le serveur Web/TFTP interne. Cette opération doit être autorisée.
- À partir de Outside Host, envoyez une requête ping au serveur Web/TFTP interne. Cette opération doit être bloquée.
- À partir de Outside Host, envoyez une requête ping à PC1. Cette opération doit être bloquée.
- À partir de PC1, envoyez une requête ping au serveur Web à l'adresse 209.165.201.30. Cette opération doit être autorisée.
- À partir de PC1, ouvrez une page Web sur le serveur Web externe. Cette opération doit être autorisée.

Une fois que les tests ont donné les résultats attendus, lancez la commande d'exécution privilégiée **show access-lists** sur R2 pour vérifier que les instructions de liste de contrôle d'accès ont des correspondances.

En vous basant sur vos connaissances des listes de contrôle d'accès, réalisez d'autres tests pour vérifier que chaque instruction correspond au trafic correct.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Exercice PT 5.5.1 : listes de contrôle d'accès de base

Diagramme de topologie

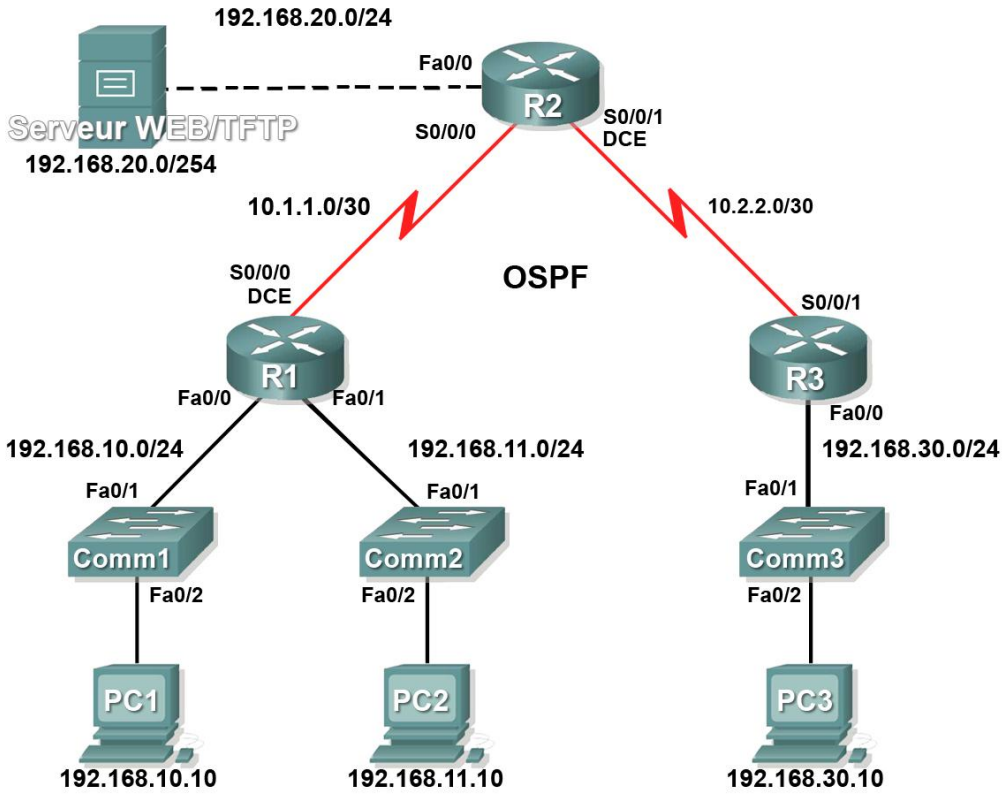


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/D
	Fa0/1	192.168.11.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
R2	**Fa0/0**	192.168.20.1	255.255.255.0	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
	Lo0	209.165.200.225	255.255.255.224	N/D
R3	**Fa0/0**	192.168.30.1	255.255.255.0	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D

Table d'adressage à la page suivante

Table d'adressage (suite)

Comm1	**VLAN 1**	192.168.10.2	255.255.255.0	192.168.10.1
Comm2	**VLAN 1**	192.168.11.2	255.255.255.0	192.168.11.1
Comm3	**VLAN 1**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**Carte réseau**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**Carte réseau**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**Carte réseau**	192.168.30.10	255.255.255.0	192.168.30.1
Serveur Web	**Carte réseau**	192.168.20.254	255.255.255.0	192.168.20.1

Objectifs pédagogiques

- Réaliser des configurations de base de routeurs et de commutateurs
- Configurer une liste de contrôle d'accès standard
- Configurer une liste de contrôle d'accès étendue
- Contrôler l'accès aux lignes vty avec une liste de contrôle d'accès standard
- Dépanner des listes de contrôle d'accès

Présentation

Au cours de cet exercice, vous allez concevoir, appliquer, tester et dépanner des configurations de listes d'accès.

Tâche 1 : configurations de base de routeurs et de commutateurs

Configurez les routeurs et commutateurs R1, R2, R3, Comm1, Comm2 et Comm3 en suivant les directives suivantes :

- Configurez les noms d'hôte relatifs au diagramme de topologie.
- Désactivez la recherche DNS.
- Configurez **class** comme mot de passe secret de mode d'exécution.
- Configurez une **bannière de message du jour**.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.
- Configurez les adresses IP et les masques sur tous les périphériques. Fréquence d'horloge à **64000**.
- Activez le protocole OSPF en utilisant l'ID de processus 1 sur tous les routeurs pour tous les réseaux.
- Configurez une interface de bouclage sur R2.
- Configurez les adresses IP de l'interface VLAN 1 sur chaque commutateur.
- Configurez chaque commutateur avec la passerelle par défaut adéquate.
- Vérifiez l'ensemble de la connectivité IP à l'aide de la commande **ping**.

Tâche 2 : configuration d'une liste de contrôle d'accès standard

Les listes de contrôle d'accès standard peuvent filtrer le trafic en fonction de l'adresse IP source uniquement. Au cours de cette tâche, vous allez configurer une liste de contrôle d'accès standard qui bloque le trafic en provenance du réseau 192.168.11.0 /24. Cette liste de contrôle d'accès s'applique en entrée à l'interface série R3. N'oubliez pas que chaque liste de contrôle d'accès possède une instruction « deny all » implicite qui entraîne le blocage de tout trafic qui ne correspond pas à une instruction de la liste de contrôle d'accès. C'est pourquoi vous devez ajouter l'instruction **permit any** à la fin de la liste de contrôle d'accès.

Étape 1. Création de la liste de contrôle d'accès

En mode de configuration globale, créez une liste de contrôle d'accès nommée standard appelée **std-1**.

```
R3(config)#ip access-list standard std-1
```

En mode de configuration d'une liste de contrôle d'accès standard, ajoutez une instruction qui refuse tous les paquets ayant une adresse source 192.168.11.0 /24 et imprimez un message sur la console pour chaque paquet correspondant.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255
```

Autorisez tout autre trafic.

```
R3(config-std-nacl)#permit any
```

Étape 2. Application de la liste de contrôle d'accès

Appliquez la liste de contrôle d'accès std-1 comme filtre à des paquets entrant dans R3 via l'interface série 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group std-1 in
```

Étape 3. Test de la liste de contrôle d'accès

Testez la liste de contrôle d'accès en envoyant une requête ping de PC2 à PC3. Étant donné que la liste de contrôle d'accès est conçue pour bloquer le trafic ayant des adresses source provenant du réseau 192.168.11.0 /24, PC2 (192.168.11.10) ne doit pas pouvoir envoyer de requête ping à PC3.

En mode d'exécution privilégié sur R3, envoyez la commande **show access-lists**. Le résultat généré est similaire à ce qui suit. Chaque ligne de la liste de contrôle d'accès possède un compteur associé indiquant le nombre de paquets ayant suivi la règle.

```
Standard IP access list std-1
    deny 192.168.11.0 0.0.0.255 (3 match(es))
    permit any
```

Tâche 3 : configuration d'une liste de contrôle d'accès étendue

Lorsque vous recherchez une plus grande finesse, utilisez une liste de contrôle d'accès étendue. Les listes de contrôle d'accès étendues filtrent le trafic en ne s'appuyant pas uniquement sur l'adresse source. Les listes de contrôle d'accès étendues filtrent en fonction du protocole, des adresses IP source et de destination, ainsi que des numéros de port source et de destination.

Une stratégie supplémentaire s'appliquant à ce réseau stipule que les périphériques du réseau local 192.168.10.0/24 sont uniquement autorisés à atteindre des réseaux internes. Les ordinateurs de ce réseau local ne sont pas autorisés à accéder à Internet. L'accès de ces utilisateurs à l'adresse IP 209.165.200.225 doit donc être bloqué. Une liste de contrôle d'accès étendue est nécessaire car cette exigence doit mettre en œuvre la source et la destination.

Au cours de cette tâche, vous allez configurer une liste de contrôle d'accès étendue sur R1 qui empêche le trafic en provenance de tout périphérique du réseau 192.168.10.0 /24 d'accéder à l'hôte 209.165.200.255. Cette liste de contrôle d'accès s'applique en sortie de l'interface série 0/0/0 de R1.

Étape 1. Configuration d'une liste de contrôle d'accès étendue nommée

En mode de configuration globale, créez une liste de contrôle d'accès étendue nommée appelée **extend-1**.

```
R1(config)#ip access-list extended extend-1
```

Remarquez que l'invite du routeur change pour indiquer que vous êtes désormais en mode de configuration de liste de contrôle d'accès étendue. À partir de cette invite, ajoutez les instructions nécessaires au blocage du trafic partant du réseau 192.168.10.0 /24 vers l'hôte. Utilisez le mot clé **host** lorsque vous définissez la destination.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

N'oubliez pas que le refus global implicite (« deny all ») bloque tout autre trafic sans l'instruction supplémentaire **permit**. Ajoutez l'instruction **permit** pour vous assurer qu'aucun autre trafic n'est bloqué.

```
R1(config-ext-nacl)#permit ip any any
```

Étape 2. Application de la liste de contrôle d'accès

Avec les listes de contrôle d'accès standard, la méthode recommandée consiste à placer la liste de contrôle d'accès le plus près possible de la destination. Les listes de contrôle d'accès étendues se trouvent généralement près de la source. Placez la liste de contrôle d'accès **extend-1** sur l'interface série afin de filtrer le trafic sortant.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group extend-1 out
```

Étape 3. Test de la liste de contrôle d'accès

À partir de PC1 ou de tout autre périphérique du réseau 192.168.10.0 /24, envoyez une requête ping à l'interface de bouclage sur R2. Ces requêtes ping doivent échouer car tout le trafic en provenance du réseau 192.168.10.0 /24 est filtré lorsque la destination est 209.165.200.225. Si la destination est n'importe quelle autre adresse, les requêtes ping doivent aboutir. Assurez-vous que c'est bien le cas en envoyant une requête ping à R3 à partir du périphérique réseau 192.168.10.0/24.

Pour vérifier encore cela, lancez la commande **show ip access-list** sur R1 après l'envoi de la requête ping.

Des correspondances doivent exister pour les deux règles de la liste de contrôle d'accès. En effet, la requête ping de PC1 vers l'interface de bouclage de R2 a été refusée tandis que la requête ping vers R3 a été autorisée.

```
R1#show ip access-list
Extended IP access list extend-1
    deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 match(es))
    permit ip any any (4 match(es))
```

Tâche 4 : contrôle de l'accès aux lignes vty à l'aide d'une liste de contrôle d'accès standard

Il est recommandé de restreindre l'accès aux lignes vty du routeur pour une administration à distance. Appliquez une liste de contrôle d'accès aux lignes vty pour restreindre l'accès à des hôtes ou à des réseaux spécifiques. Au cours de cette tâche, vous allez configurer une liste de contrôle d'accès standard pour permettre à des hôtes de deux réseaux d'accéder aux lignes vty. Tous les autres hôtes sont rejetés.

Vérifiez que vous pouvez établir une connexion Telnet vers R2 à partir de R1 et de R3.

Étape 1. Configuration de la liste de contrôle d'accès

Configurez une liste de contrôle d'accès standard nommée sur R2 qui autorise le trafic en provenance de 10.2.2.0/30 et de 192.168.30.0/24. Refusez tout autre trafic. Nommez **Task-4** la liste de contrôle d'accès.

```
R2(config)#ip access-list standard Task-4
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Étape 2. Application de la liste de contrôle d'accès

Accédez au mode de configuration de ligne des lignes vty 0 à 16.

```
R2(config)#line vty 0 16
```

Utilisez la commande **access-class** pour appliquer la liste de contrôle d'accès aux lignes vty dans le sens entrant. Remarquez qu'elle diffère de la commande utilisée pour appliquer des listes de contrôle d'accès à d'autres interfaces.

```
R2(config-line)#access-class Task-4 in
```

Étape 3. Test de la liste de contrôle d'accès

Établissez une connexion Telnet avec R2 à partir de R1. Remarquez que R1 ne possède pas d'adresse IP dans la plage d'adresses répertoriée dans les instructions « permit » de la liste de contrôle d'accès Task-4. Les tentatives de connexion doivent échouer.

À partir de R3, établissez une connexion Telnet avec R2 ou avec tout périphérique du réseau 192.168.30.0/24. Une invite vous demandant le mot de passe de la ligne vty s'affiche.

Pourquoi les tentatives de connexion à partir d'autres réseaux échouent-elles même si ceux-ci ne sont pas spécifiquement répertoriés dans la liste de contrôle d'accès ?

_____

_____

Tâche 5 : dépannage des listes de contrôle d'accès

Lorsqu'une liste de contrôle d'accès n'est pas correctement configurée ou est appliquée à une interface erronée ou dans la mauvaise direction, il est possible que le trafic réseau en soit affecté de manière indésirable.

Étape 1. Test de la liste de contrôle d'accès

Au cours d'une tâche précédente, vous avez créé et appliqué une liste de contrôle d'accès standard nommée sur R3. Pour afficher la liste de contrôle d'accès et son emplacement, utilisez la commande **show running-config**. Vous devez voir qu'une liste de contrôle d'accès nommée **std-1** a été configurée et appliquée en entrée sur Serial 0/0/1. Cette liste de contrôle d'accès a été créée pour empêcher tout trafic réseau avec une adresse source du réseau 192.168.11.0/24 d'accéder au réseau local sur R3.

Pour supprimer la liste de contrôle d'accès, passez en mode de configuration d'interface pour Serial 0/0/1 sur R3.

```
R3(config)#interface serial 0/0/1
```

Exécutez la commande **no ip access-group std-1 in** pour supprimer la liste de contrôle d'accès de l'interface.

```
R3(config-if)#no ip access-group std-1 in
```

Exécutez la commande **show running-config** pour vérifier que la liste de contrôle d'accès a été supprimée de Serial 0/0/1.

Étape 2. Application de la liste de contrôle d'accès std-1 à S0/0/1 en sortie

Pour tester l'importance du sens de filtrage de la liste de contrôle d'accès, appliquez à nouveau la liste de contrôle d'accès **std-1** à l'interface Serial 0/0/1. Désormais, la liste de contrôle d'accès doit filtrer le trafic sortant et non entrant. N'oubliez pas d'utiliser le mot clé **out** lorsque vous appliquez la liste de contrôle d'accès.

```
R3(config-if)#ip access-group std-1 out
```

Étape 3. Test de la liste de contrôle d'accès

Testez la liste de contrôle d'accès en envoyant une requête ping à PC3 à partir de PC2. Une autre solution consiste à envoyer une requête ping étendue à partir de R1. Remarquez que, cette fois-ci, les requêtes ping aboutissent et que les compteurs de la liste de contrôle d'accès n'augmentent pas. Pour vérifier cela, envoyez la commande **show ip access-list** sur R3.

Étape 4. Rétablissement de la configuration d'origine de la liste de contrôle d'accès

Supprimez la liste de contrôle d'accès du sens sortant et appliquez-la à nouveau dans le sens entrant.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group std-1 out
R3(config-if)#ip access-group std-1 in
```

Étape 5. Application de Task-4 en entrée de l'interface série 0/0/0 de R2

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group Task-4 in
```

Étape 6. Test de la liste de contrôle d'accès

Essayez de communiquer avec un périphérique connecté à R2 ou R3 à partir de R1 ou des réseaux qui y sont reliés. Remarquez que toutes les communications sont bloquées. Cependant, les compteurs de la liste de contrôle d'accès n'augmentent pas. Cela est dû au refus global implicite (« deny all ») placé à la fin de chaque liste de contrôle d'accès.

Après expiration des compteurs d'intervalles d'arrêt OSPF, les consoles de R1 et R2 affichent des messages similaires à celui ci :

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Supprimez la liste de contrôle d'accès Task-4 de l'interface.

Exercice PT 5.5.2 : exercice sur les listes de contrôle d'accès

Diagramme de topologie

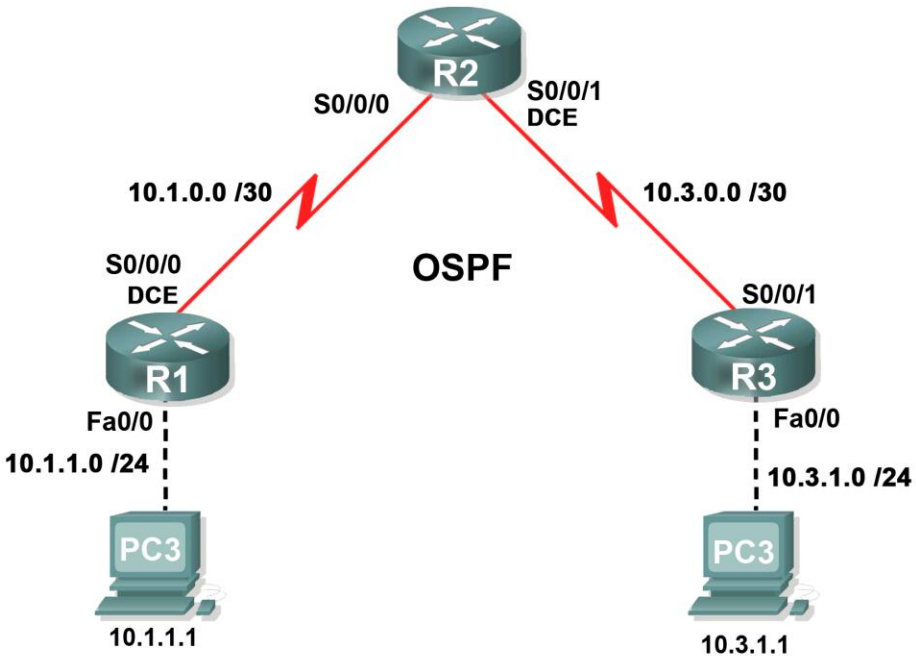


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**S0/0/0**	10.1.0.1	255.255.255.252	N/D
	Fa0/0	10.1.1.254	255.255.255.0	N/D
R2	**S0/0/0**	10.1.0.2	255.255.255.252	N/D
	S0/0/1	10.3.0.1	255.255.255.252	N/D
R3	**S0/0/1**	10.3.0.2	255.255.255.252	N/D
	Fa0/0	10.3.1.254	255.255.255.0	N/D
PC1	**Carte réseau**	10.1.1.1	255.255.255.0	10.1.1.254
PC2	**Carte réseau**	10.3.1.1	255.255.255.0	10.3.1.254

Objectifs pédagogiques

- Effectuer des configurations de base de routeur
- Configurer des listes de contrôle d'accès standard
- Configurer des listes de contrôle d'accès étendues
- Vérifier des listes de contrôle d'accès

Présentation

Au cours de cet exercice, vous allez concevoir, appliquer, tester et dépanner des configurations de listes d'accès.

Tâche 1 : configurations de base de routeurs

Configurez tous les périphériques selon les instructions suivantes :

- Configurez le nom d'hôte du routeur.
- Désactivez la recherche DNS.
- Configurez **class** comme mot de passe secret de mode d'exécution.
- Configurez une **bannière de message du jour**.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.
- Configurez les adresses IP et les masques sur tous les périphériques. La fréquence d'horloge est de **64000**.
- Activez le protocole OSPF en utilisant l'ID de processus 1 sur tous les routeurs pour tous les réseaux.
- Vérifiez l'ensemble de la connectivité IP à l'aide de la commande **ping**.

Tâche 2 : configuration de listes de contrôle d'accès standard

Configurez les listes de contrôle d'accès nommées standard sur les lignes vty de R1 et R3, ce qui permet aux hôtes connectés directement à leurs sous-réseaux Fast Ethernet d'obtenir un accès Telnet. Refusez toutes les autres tentatives de connexion. Nommez ces listes de contrôle d'accès standard **VTY-Local** et appliquez-les à toutes les lignes Telnet. Documentez votre configuration de listes de contrôle d'accès.

_____

_____

_____

_____

_____

_____

_____

Tâche 3 : configuration de listes de contrôle d'accès étendues

En utilisant des listes de contrôle d'accès étendues sur R2, suivez ces instructions :

- Nommez le bloc de listes de contrôle d'accès.
- Empêchez le trafic provenant des sous-réseaux connectés à R1 d'atteindre les sous-réseaux connectés à R3.
- Empêchez le trafic provenant des sous-réseaux connectés à R3 d'atteindre les sous-réseaux connectés à R1.
- Autorisez tout autre trafic.

Documentez votre configuration de listes de contrôle d'accès.

_____

_____

_____

_____

_____

_____

Tâche 4 : vérification des listes de contrôle d'accès

Étape 1. Test de connexion Telnet

- PC1 doit pouvoir établir une connexion Telnet avec R1.
- PC3 doit être capable d'établir une connexion Telnet avec R3.
- R2 doit se voir refuser l'accès Telnet à R1 et à R3.

Étape 2. Test du trafic

Les requêtes ping entre PC1 et PC3 doivent échouer.

Exercice PT 5.6.1 : exercice d'intégration des compétences Packet Tracer

Diagramme de topologie

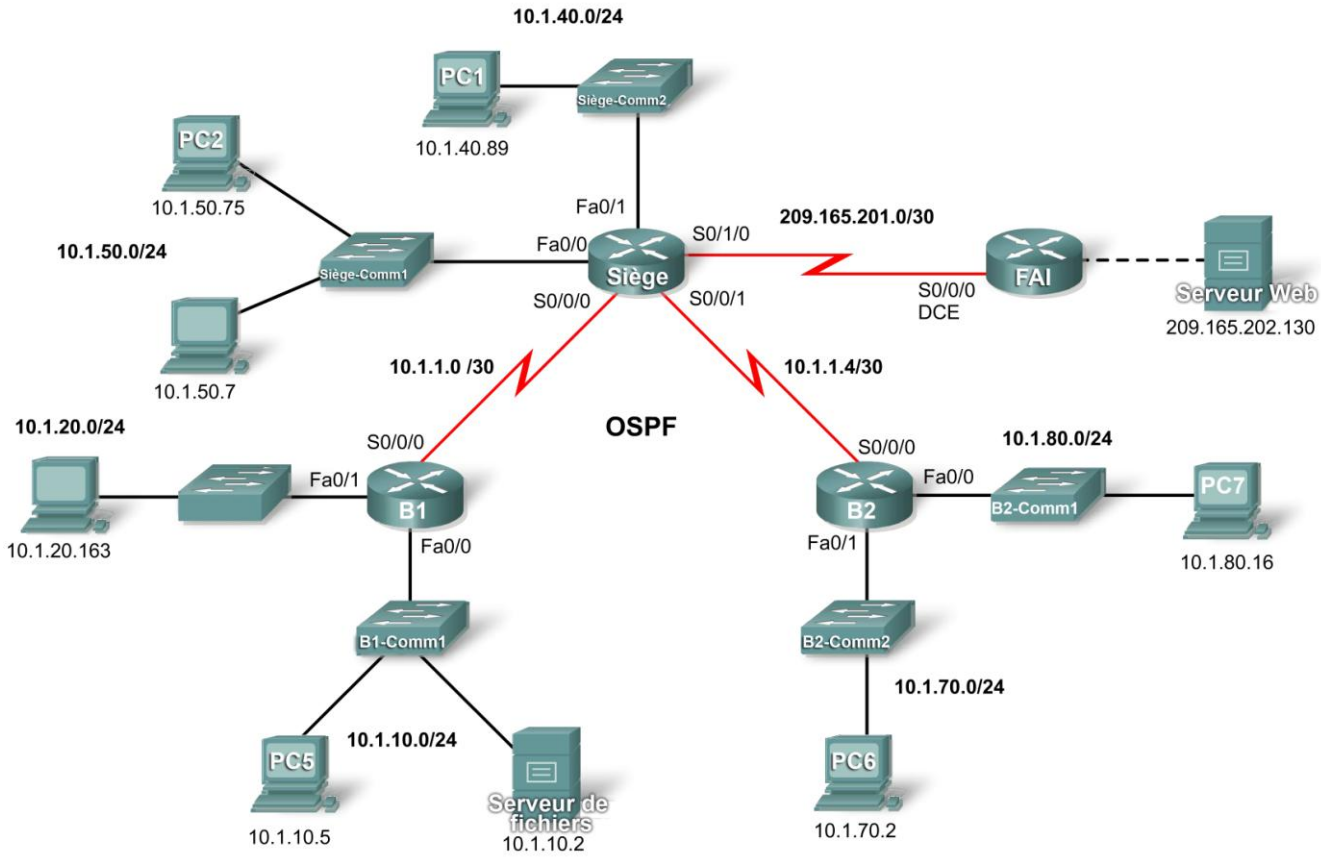


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
SIÈGE	S0/0/0	10.1.1.1	255.255.255.252
	S0/0/1	10.1.1.5	255.255.255.252
	S0/1/0	209.165.201.2	255.255.255.252
	Fa0/0	10.1.50.1	255.255.255.0
	Fa0/1	10.1.40.1	255.255.255.0
B1	S0/0/0	10.1.1.2	255.255.255.252
	Fa0/0	10.1.10.1	255.255.255.0
	Fa0/1	10.1.20.1	255.255.255.0
B2	S0/0/0	10.1.1.6	255.255.255.252
	Fa0/0	10.1.80.1	255.255.255.0
	Fa0/1	10.1.70.1	255.255.255.0
FAI	S0/0/0	209.165.201.1	255.255.255.252
	Fa0/0	209.165.202.129	255.255.255.252
Serveur Web	Carte réseau	209.165.202.130	255.255.255.252

Objectifs pédagogiques

- Configurer le protocole PPP avec l'authentification CHAP
- Configurer le routage par défaut
- Configurer le routage OSPF
- Mettre en œuvre et vérifier plusieurs stratégies de sécurité de listes de contrôle d'accès

Présentation

Au cours de cet exercice, vous allez faire preuve de votre capacité à configurer des listes de contrôle d'accès qui appliquent cinq stratégies de sécurité. Vous allez également configurer le protocole PPP et le routage OSPF. L'adressage IP des périphériques est déjà configuré. Le mot de passe d'exécution utilisateur est **cisco** et le mot de passe d'exécution privilégié est **class**.

Tâche 1 : configuration du protocole PPP avec l'authentification CHAP

Étape 1. Configuration de la liaison entre SIÈGE et B1 pour utiliser l'encapsulation PPP avec l'authentification CHAP

Le mot de passe pour l'authentification CHAP est **cisco123.**

Étape 2. Configuration de la liaison entre SIÈGE et B2 pour utiliser l'encapsulation PPP avec l'authentification CHAP

Le mot de passe pour l'authentification CHAP est **cisco123.**

Étape 3. Vérification du rétablissement de la connectivité entre les routeurs

SIÈGE doit être en mesure d'envoyer une requête ping à B1 et à B2. Quelques minutes peuvent être nécessaires pour que les interfaces se rétablissent. Pour accélérer le processus, vous pouvez alterner entre les modes Realtime (temps réel) et Simulation. Une autre solution permettant de contourner ce comportement de Packet Tracer consiste à utiliser les commandes **shutdown** et **no shutdown** sur les interfaces.

Remarque : il est possible que les interfaces se désactivent de façon aléatoire pendant l'exercice à cause d'un bogue de Packet Tracer. En principe, l'interface se rétablit seule après quelques secondes d'attente.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 29 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration du routage par défaut

Étape 1. Configuration du routage par défaut de SIÈGE vers FAI

Configurez une route par défaut sur SIÈGE en utilisant l'argument *exit interface* pour envoyer tout le trafic par défaut vers FAI.

Étape 2. Test de la connectivité au serveur Web

SIÈGE doit être en mesure d'envoyer une requête ping au serveur Web à l'adresse 209.165.202.130 tant que la requête ping provient de l'interface Serial0/1/0.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 32 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration du routage OSPF

Étape 1. Configuration d'OSPF sur SIÈGE

- Configurez OSPF à l'aide de l'ID de processus 1.
- Annoncez tous les sous-réseaux à l'exception du réseau 209.165.201.0.
- Transmettez les informations de route par défaut aux voisins OSPF.
- Désactivez les mises à jour d'OSPF vers FAI et vers les réseaux locaux de SIÈGE.

Étape 2. Configuration d'OSPF sur B1 et B2

- Configurez OSPF à l'aide de l'ID de processus 1.
- Sur chaque routeur, configurez les sous-réseaux adéquats.
- Désactivez les mises à jour d'OSPF vers les réseaux locaux.

Étape 3. Test de la connectivité dans l'ensemble du réseau

Le réseau doit maintenant avoir une connectivité totale de bout en bout. Chaque périphérique doit être en mesure d'envoyer une requête ping à tout autre périphérique, y compris au serveur Web à l'adresse 209.165.202.130.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 76 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : mise en œuvre de plusieurs stratégies de sécurité de listes de contrôle d'accès

Étape 1. Mise en œuvre de la stratégie de sécurité numéro 1

Empêchez le réseau 10.1.10.0 d'accéder au réseau 10.1.40.0. Tout autre accès à 10.1.40.0 est autorisé. Configurez la liste de contrôle d'accès sur SIÈGE en utilisant la liste de contrôle d'accès numéro 10.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 2. Vérification de la mise en œuvre de la stratégie de sécurité numéro 1

Une requête ping de PC5 à PC1 doit échouer.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 80 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Étape 4. Mise en œuvre de la stratégie de sécurité numéro 2

L'hôte 10.1.10.5 n'est pas autorisé à accéder à l'hôte 10.1.50.7. Tous les autres hôtes sont autorisés à accéder à 10.1.50.7. Configurez la liste de contrôle d'accès sur B1 en utilisant la liste de contrôle d'accès numéro 115.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 5. Vérification de la mise en œuvre de la stratégie de sécurité numéro 2

Une requête ping de PC5 à PC3 doit échouer.

Étape 6. Vérification des résultats

Votre taux de réalisation doit être de 85 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Étape 7. Mise en œuvre de la stratégie de sécurité numéro 3

Les hôtes 10.1.50.1 à 10.1.50.63 ne disposent pas d'un accès Web au serveur Intranet à l'adresse 10.1.80.16. Tout autre accès est autorisé. Configurez la liste de contrôle d'accès sur le routeur adéquat en utilisant la liste de contrôle d'accès numéro 101.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- Sur quel routeur configurer la liste de contrôle d'accès ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 8. Vérification de la mise en œuvre de la stratégie de sécurité numéro 3

Pour tester cette stratégie, cliquez sur PC3, puis sur l'onglet **Desktop,** puis sur **Web Browser**. Pour l'URL, saisissez l'adresse IP du serveur Intranet, 10.1.80.16, puis appuyez sur **Entrée**. Après quelques secondes, vous devez recevoir un message de dépassement de délai d'attente de la requête. PC2 et tout autre PC du réseau doivent être en mesure d'accéder au serveur Intranet.

Étape 9. Vérification des résultats

Votre taux de réalisation doit être de 90 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Étape 10. Mise en œuvre de la stratégie de sécurité numéro 4

Utilisez le nom **NO_FTP** pour configurer une liste de contrôle d'accès nommée qui empêche le réseau 10.1.70.0/24 d'accéder aux services FTP (port 21) du serveur de fichiers à l'adresse 10.1.10.2. Tout autre accès doit être autorisé.

Remarque : les noms sont sensibles à la casse.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- Sur quel routeur configurer la liste de contrôle d'accès ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 11. Vérification des résultats

Packet Tracer ne prenant pas en charge le test de l'accès FTP, vous ne pourrez pas vérifier cette stratégie. Cependant, votre taux de réalisation doit être de 95 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Étape 12. Mise en œuvre de la stratégie de sécurité numéro 5

FAI représentant la connectivité à Internet, configurez une liste de contrôle d'accès nommée appelée **FIREWALL** dans l'ordre suivant :

1. Autorisez uniquement les réponses ping entrantes en provenance du FAI et de toute source au-delà du FAI.
2. Autorisez uniquement les sessions TCP établies à partir du FAI et de toute source au-delà du FAI.
3. Bloquez explicitement tout autre accès entrant à partir du FAI et de toute source au-delà du FAI.

- Utiliser une liste de contrôle d'accès standard ou étendue ? _____
- Sur quel routeur configurer la liste de contrôle d'accès ? _____
- À quelle interface appliquer la liste de contrôle d'accès ? _____
- Dans quel sens appliquer la liste de contrôle d'accès ? _____

_____

_____

_____

_____

_____

Étape 13. Vérification de la mise en œuvre de la stratégie de sécurité numéro 5

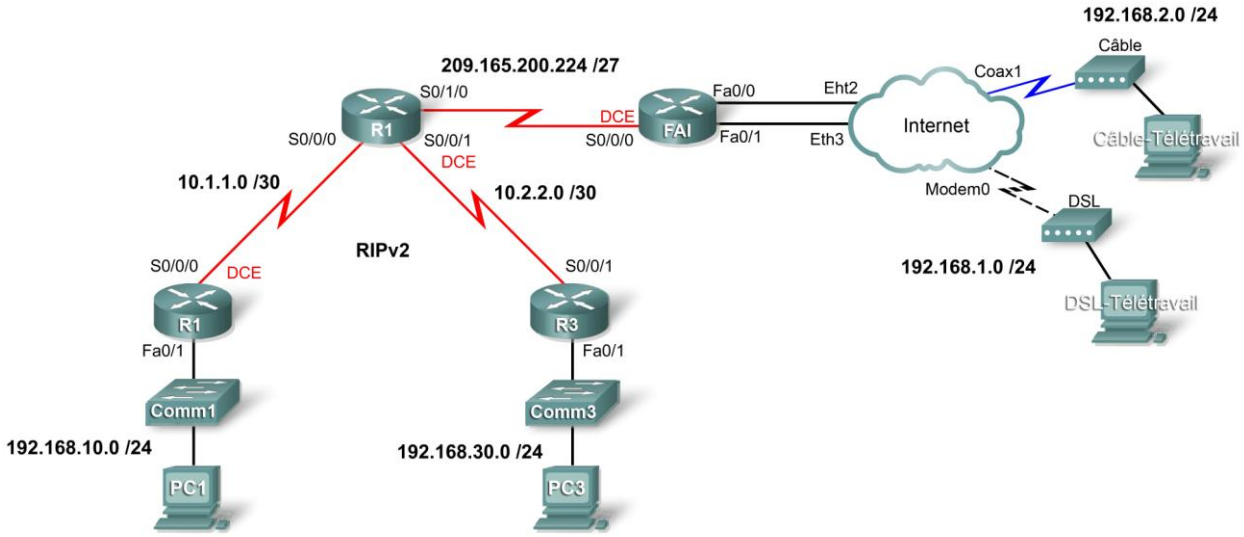
Pour tester cette stratégie, tout PC doit être en mesure d'envoyer une requête ping à FAI ou au serveur Web. Cependant, ni FAI ni le serveur Web ne doivent pouvoir envoyer de requête ping à SIÈGE ou à tout autre périphérique au-delà de la liste de contrôle d'accès **FIREWALL.**

Étape 14. Vérification des résultats

Votre taux de réalisation doit être de 100%. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Exercice PT 6.2.4 : services à large bande

Diagramme de topologie



Objectifs pédagogiques

- Connecter le routeur FAI au nuage Internet
- Ajouter des unités WAN
- Connecter une unité WAN au nuage Internet
- Connecter les PC des télétravailleurs aux unités WAN
- Tester la connectivité

Présentation

Au cours de cet exercice, vous allez prouver votre capacité à ajouter des connexions et des périphériques à large bande à Packet Tracer. Bien que vous ne puissiez pas configurer la liaison DSL et les modems câbles, vous pouvez simuler une connectivité de bout en bout vers les périphériques des télétravailleurs.

Tâche 1 : connexion de FAI au nuage Internet

Étape 1. Établissement des connexions à l'aide des interfaces indiquées dans la topologie

- Connectez Fa0/0 de FAI à Eth2 du nuage Internet.
- Connectez Fa0/1 de FAI à Eth3 du nuage Internet.

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 25 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : ajout d'unités WAN

Étape 1. Ajout d'une liaison DSL et de périphériques à câble

Les périphériques **DSL Modem** et **Cable Modem** se trouvent dans le menu **WAN Emulation**. Installez-les comme vous installeriez tout autre périphérique.

Étape 2. Désignation des unités WAN

À partir de l'onglet Config, modifiez le nom affiché pour chaque unité WAN respectivement en **Cable** et **DSL**.

Tâche 3 : connexion des unités WAN au nuage Internet

Étape 1. Connexion du modem câble au nuage Internet

Choisissez le type de connexion **Coaxial** dans le menu **Connection**.

Étape 2. Connexion du modem DSL au nuage Internet

Choisissez le type de connexion **Phone** dans le menu **Connection**.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 75 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : connexion des PC des télétravailleurs aux unités WAN

Étape 1. Connexion de Câble-Télétravail à Cable

Étape 2. Connexion de DSL-Télétravail à DSL

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 5 : test de la connectivité

Cliquez sur **Check Results** puis sur l'onglet Connectivity Tests pour vérifier que les périphériques des télétravailleurs peuvent communiquer avec les PC internes.

Exercice PT 6.4.1 : exercice d'intégration des compétences Packet Tracer

Diagramme de topologie

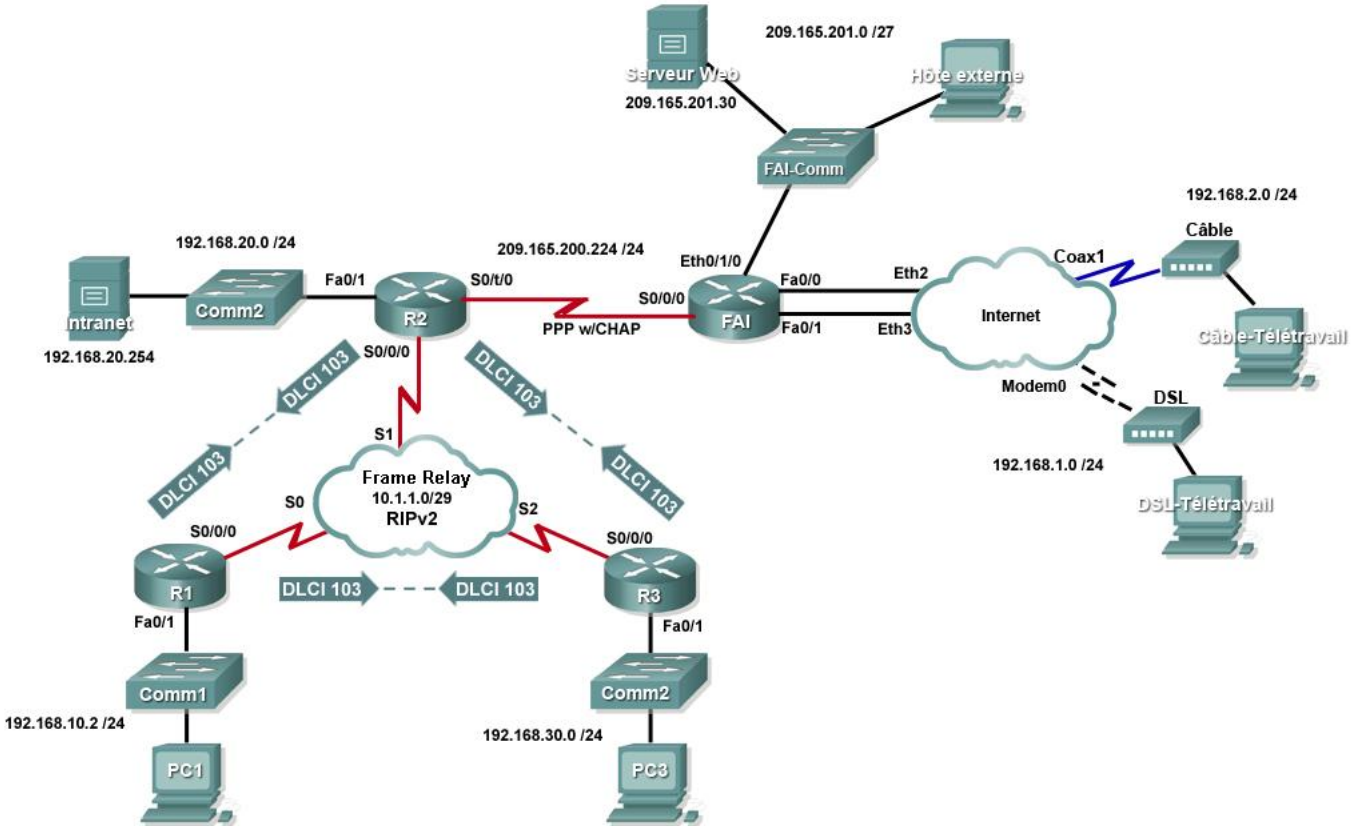


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.248
R2	**Fa0/1**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.248
	S0/1/0	209.165.200.225	255.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/0	10.1.1.3	255.255.255.248
FAI	**S0/0/0**	209.165.200.226	255.255.255.224
	Eth0/1/0	209.165.201.1	255.255.255.224
	Fa0/0	192.168.1.1	255.255.255.0
	Fa0/1	192.168.2.1	255.255.255.0
PC1	**Carte réseau**	192.168.10.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0
Intranet	**Carte réseau**	192.168.20.254	255.255.255.0
DSL-Télétravail	**Carte réseau**	192.168.1.10	255.255.255.0
Câble-Télétravail	**Carte réseau**	192.168.2.10	255.255.255.0
Serveur Web	**Carte réseau**	209.165.201.30	255.255.255.224
Hôte externe	**Carte réseau**	209.165.201.10	255.255.255.224

Objectifs pédagogiques

- Appliquer des configurations de base des routeurs
- Configurer un routage dynamique et un routage par défaut
- Mettre en place des services de télétravail
- Tester la connectivité avant de configurer les listes de contrôle d'accès
- Appliquer des stratégies de listes de contrôle d'accès
- Tester la connectivité après avoir configuré les listes de contrôle d'accès

Présentation

Lors de cet exercice, vous allez configurer une route par défaut ainsi qu'un routage dynamique à l'aide du protocole RIP version 2. Vous allez également ajouter des périphériques à large bande au réseau. Pour finir, vous allez définir des listes de contrôle d'accès sur deux routeurs afin de contrôler le trafic réseau. Packet Tracer étant très précis sur la façon de noter les listes de contrôle d'accès, vous devez configurer les règles de ces listes dans l'ordre donné.

Tâche 1 : application des configurations de base des routeurs

À l'aide des informations du diagramme de topologie et de la table d'adressage, réalisez les configurations de base des périphériques R1, R2 et R3. Les noms d'hôtes sont configurés pour vous.

Incluez les éléments suivants :

- lignes vty et de console ;
- bannières ;
- désactivation de la recherche de nom de domaine ;
- descriptions d'interface.

Tâche 2 : configuration du routage dynamique et du routage par défaut

Étape 1. Configuration du routage par défaut

R2 a besoin d'une route par défaut. Utilisez l'argument *exit-interface* dans la configuration de la route par défaut.

Étape 2. Configuration du routage dynamique

Configurez le protocole RIPv2 sur R1, R2 et R3 pour tous les réseaux disponibles. R2 doit transférer sa configuration réseau par défaut aux autres routeurs. Assurez-vous également d'utiliser la commande **passive-interface** sur toutes les interfaces actives qui ne sont pas utilisées pour le routage.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 59 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : mise en place des services de télétravail

Étape 1. Ajout d'unités WAN

Ajoutez une liaison DSL et un modem câble en suivant le diagramme de topologie.

Étape 2. Désignation des unités WAN

À partir de l'onglet **Config**, modifiez le nom affiché pour chaque unité WAN respectivement en **Cable** et **DSL**.

Étape 3. Connexion des unités WAN

Connectez les unités WAN aux PC et à Internet à l'aide des câbles et des interfaces appropriés.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 86 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : test de la connectivité avant de configurer les listes de contrôle d'accès

À ce stade, toutes les branches de la topologie doivent avoir une connectivité. Le fait d'alterner entre les modes Simulation et Realtime (temps réel) peut accélérer la convergence.

Tâche 5 : application des stratégies de listes de contrôle d'accès

Étape 1. Création et application de la stratégie de sécurité numéro 1

Mettez en œuvre les règles de liste de contrôle d'accès suivantes à l'aide de la liste de contrôle d'accès numéro 101 :

1. Autorisez aux hôtes du réseau 192.168.30.0/24 un accès Web vers toute destination.
2. Autorisez aux hôtes du réseau 192.168.30.0/24 l'envoi de requêtes ping vers toute destination.
3. Refusez tout autre accès provenant du réseau.

Étape 2. Création et application de la stratégie de sécurité numéro 2

FAI représentant la connectivité à Internet, configurez une liste de contrôle d'accès nommée appelée **FIREWALL** dans l'ordre suivant :

1. Autorisez à DSL-Télétravail l'accès Web au serveur Intranet.
2. Autorisez à Câble-Télétravail l'accès Web au serveur Intranet.
3. Autorisez uniquement les réponses ping entrantes en provenance de FAI et de toute source au-delà de FAI.
4. Autorisez uniquement les sessions TCP établies à partir de FAI et de toute source au-delà de FAI.
5. Bloquez explicitement tout autre accès entrant à partir de FAI et de toute source au-delà de FAI.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 6 : test de la connectivité après avoir configuré les listes de contrôle d'accès

Les télétravailleurs ne doivent pas être en mesure d'envoyer des requêtes ping au serveur Intranet mais doivent pouvoir accéder à leur serveur HTTP via le navigateur Web. Cet exercice inclut trois PDU, dont deux doivent échouer et une aboutir. Vérifiez **Connectivity Tests** dans le menu **Check Results** pour vous assurer que les taux de réalisation sont de 100 %.

Exercice PT 7.1.8 : configuration de DHCP avec Easy IP

Diagramme de topologie

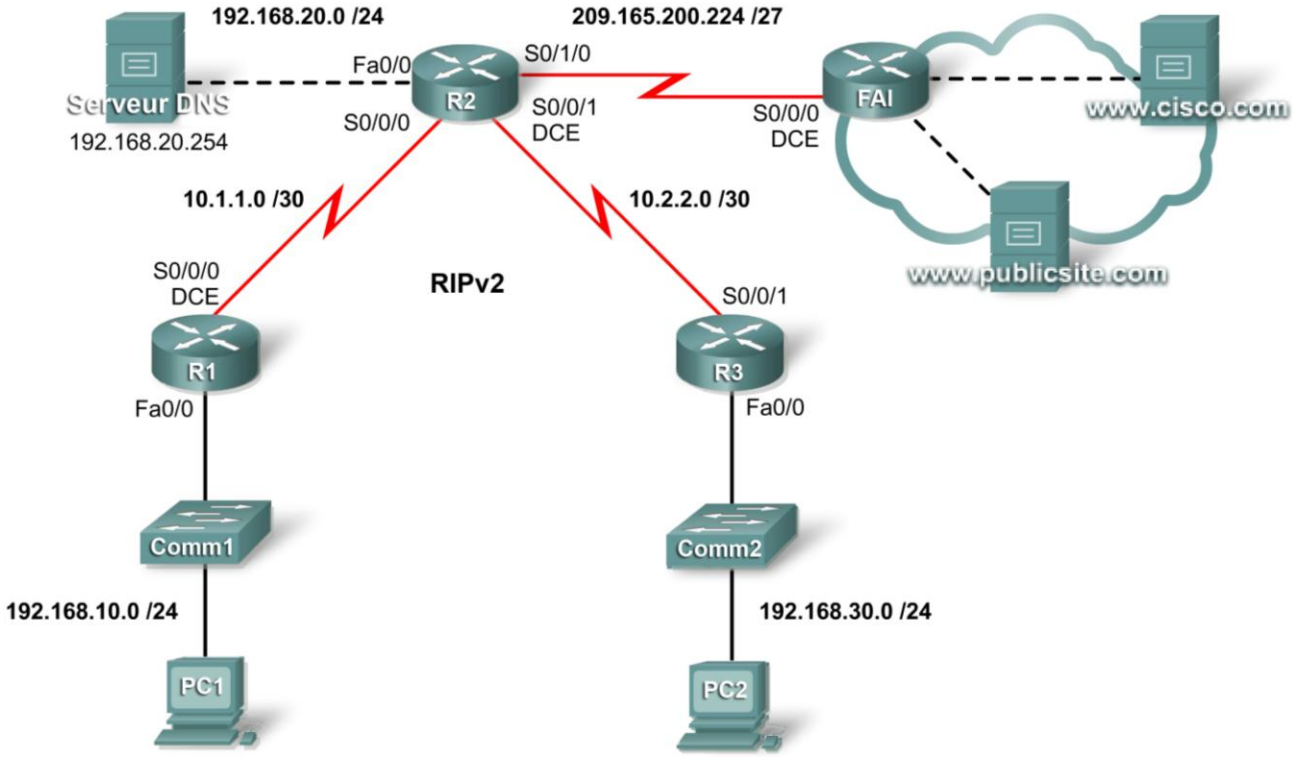


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**Fa0/0**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	225.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

Objectifs pédagogiques

- Configurer des routeurs avec Easy IP
- Vérifier que des PC sont automatiquement configurés avec des informations d'adressage
- Configurer un serveur DNS avec des valeurs DNS
- Tester la connectivité des PC à des noms de domaine

Présentation

Le protocole DHCP attribue dynamiquement des adresses IP et d'autres informations importantes de configuration réseau. Les routeurs Cisco peuvent utiliser en option le jeu de fonctions IOS de Cisco, Easy IP, comme serveur DHCP complet. Par défaut, Easy IP concède des configurations pendant 24 heures. Au cours de cet exercice, vous allez configurer des services DHCP sur deux routeurs et tester votre configuration.

Tâche 1 : configuration de routeurs avec Easy IP

Étape 1. Configuration des adresses exclues pour R1 et R3

Définissez un jeu d'adresses qui sont réservées aux hôtes ayant besoin d'adresses statiques, tels que les serveurs, les routeurs et les imprimantes. Ces adresses ne sont pas incluses dans le pool d'adresses qui peuvent être attribuées aux clients DHCP. Pour R1 et R3, excluez les neuf premières adresses du pool DHCP.

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#

R3(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.9
R3(config)#
```

Étape 2. Configuration du pool d'adresses pour R1

Définissez le pool d'adresses à partir duquel DHCP attribue des adresses à des clients DHCP sur le réseau local de R1. Les adresses disponibles sont toutes des adresses du réseau 192.168.10.0, sauf celles qui ont été exclues à l'étape 1.

Sur R1, nommez le pool d'adresses R1LAN. Précisez le pool d'adresses, la passerelle par défaut et le serveur DNS qui sont attribués à chaque périphérique client ayant besoin d'un service DHCP.

```
R1(config)#ip dhcp pool R1LAN
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#dns-server 192.168.20.254
```

Étape 3. Configuration du pool d'adresses pour R3

Sur R3, nommez le pool d'adresses R3LAN. Précisez le pool d'adresses, la passerelle par défaut et le serveur DNS qui sont attribués à chaque périphérique client ayant besoin d'un service DHCP.

```
R3(config)#ip dhcp pool R3LAN
R3(dhcp-config)#network 192.168.30.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.30.1
R3(dhcp-config)#dns-server 192.168.20.254
```

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 43 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : vérification de la configuration automatique des PC

Étape 1. Configuration de PC1 et de PC3 pour la configuration DHCP

Dans l'onglet **Desktop** de chaque PC, cliquez sur **IP Configuration** puis sélectionnez **DHCP**. Les informations concernant la configuration IP se mettent immédiatement à jour.

Étape 2. Vérification du fonctionnement de DHCP sur les routeurs

Pour vérifier le fonctionnement du protocole DHCP sur les routeurs, lancez la commande show ip dhcp binding. Les résultats doivent montrer une adresse IP liée à chacun des routeurs.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 86 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration d'un serveur DNS avec des valeurs DNS

Étape 1. Configuration du serveur DNS

Pour configurer le système DNS sur le serveur DNS, cliquez sur le bouton **DNS** dans l'onglet **Config**.

Assurez-vous que le système DNS soit actif puis saisissez les valeurs DNS suivantes :

- www.cisco.com 209.165.201.30
- www.publicsite.com 209.165.202.158

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : test de la connectivité des PC aux noms de domaine

Étape 1. Vérification de la connexion de PC1 à des serveurs en utilisant le nom de domaine

Sur PC1, ouvrez le navigateur Web et saisissez **www.cisco.com** sur la ligne d'adresse. La page Web doit s'afficher.

Étape 2. Vérification de la connexion de PC3 à des serveurs en utilisant le nom de domaine

Sur PC3, ouvrez le navigateur Web et saisissez **www.publicsite.com** sur la ligne d'adresse. La page Web doit s'afficher.

Exercice PT 7.2.8 : évolutivité des réseaux avec NAT

Diagramme de topologie

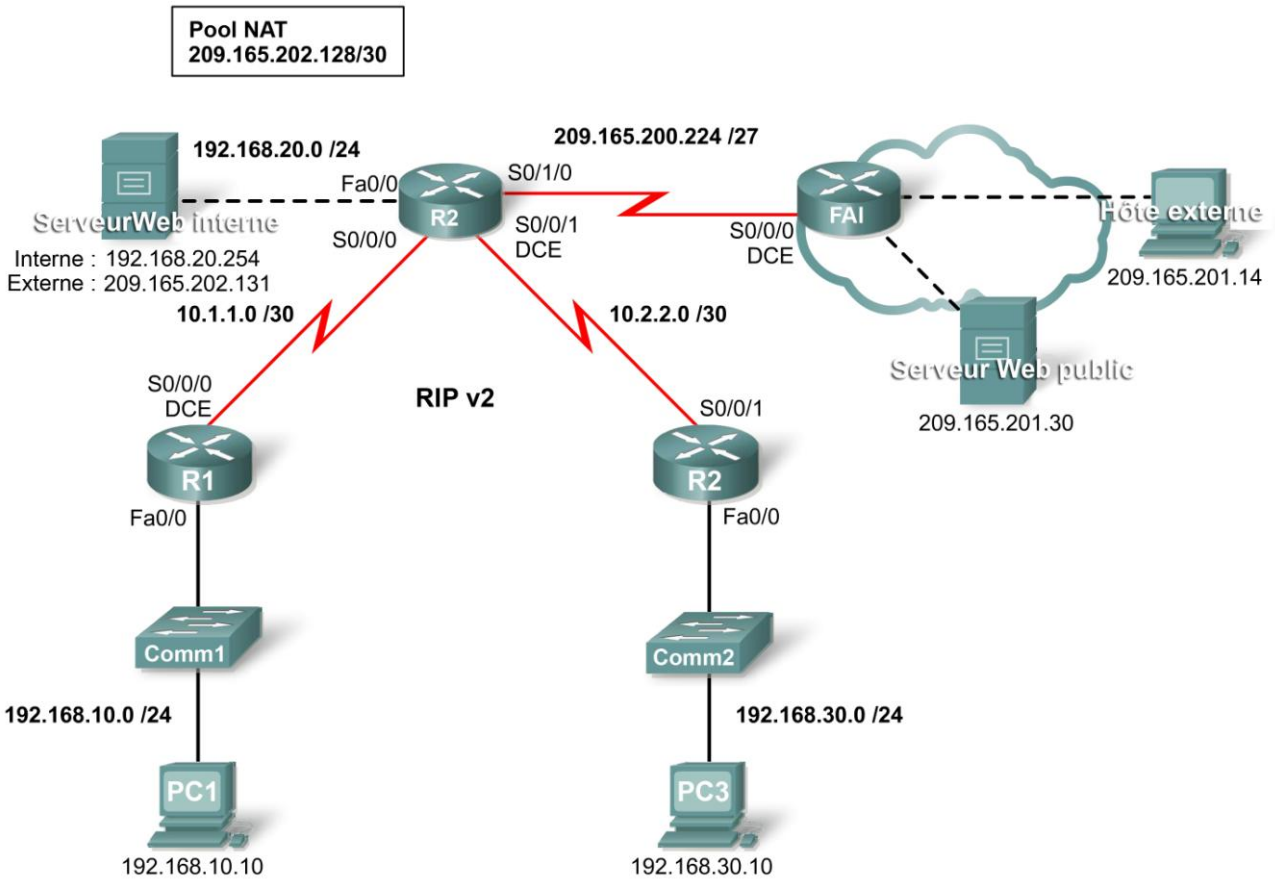


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**Fa0/0**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

Suite de la table d'adressage sur la page suivante

Table d'adressage (suite)

Serveur Web interne	**Carte réseau**	Local : 192.168.20.254	255.255.255.252
	Carte réseau	Global : 209.165.202.131	255.255.255.252
PC1	**Carte réseau**	192.168.10.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0
Hôte externe	**Carte réseau**	209.165.201.14	255.255.255.240
Serveur Web public	**Carte réseau**	209.265.201.30	255.255.255.240

Objectifs pédagogiques

- Configurer une liste de contrôle d'accès pour autoriser la fonction NAT
- Configurer une fonction NAT statique
- Configurer une surcharge NAT dynamique
- Configurer le routeur FAI avec une route statique
- Tester la connectivité

Présentation

La fonction NAT traduit des adresses internes, privées et non routables en adresses publiques routables. Un avantage supplémentaire de la fonction NAT est d'offrir confidentialité et sécurité à un réseau en masquant les adresses IP internes aux réseaux externes. Au cours de cet exercice, vous allez configurer la fonction NAT statique et dynamique.

Tâche 1 : configuration d'une liste de contrôle d'accès pour autoriser la fonction NAT

Étape 1. Création d'une liste de contrôle d'accès standard nommée

Pour définir les adresses internes qui sont traduites en adresses publiques dans le processus NAT, créez une liste de contrôle d'accès standard nommée appelée R2NAT. Cette liste est utilisée dans les étapes suivantes de configuration de la fonction NAT.

```
R2(config)#ip access-list standard R2NAT
R2(config-std-nacl)# permit 192.168.10.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.30.0 0.0.0.255
```

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 11 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration d'une fonction NAT statique

Étape 1. Configuration d'une fonction NAT statique pour un serveur Web interne

Le serveur Web interne doit posséder une adresse IP publique qui ne change jamais afin qu'un accès soit possible de l'extérieur du réseau. La configuration d'une adresse NAT statique permet de configurer le serveur Web avec une adresse interne privée. Le processus NAT mappe alors toujours sur l'adresse privée les paquets utilisant l'adresse publique du serveur.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.202.131
```

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 22 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration d'une surcharge NAT dynamique

Outre l'adresse IP publique attribuée au serveur Web interne, FAI vous a attribué trois adresses publiques. Ces adresses sont mappées sur tous les autres hôtes internes qui accèdent à Internet.

Pour autoriser plus de trois hôtes internes à accéder simultanément à Internet, configurez une surcharge à la fonction NAT pour accepter les hôtes supplémentaires. La surcharge NAT, également appelée traduction d'adresses réseau (PAT, Port Address Translation), utilise les numéros de port pour faire la distinction entre les paquets des différents hôtes auxquels la même adresse IP publique a été attribuée.

Étape 1. Définition du pool d'adresses et configuration de la fonction NAT dynamique

Saisissez les commandes suivantes pour configurer le pool d'adresses publiques qui sont dynamiquement mappées sur les hôtes internes.

La première commande définit le pool de trois adresses publiques qui sont mappées sur des adresses internes.

La seconde commande indique au processus NAT le mappage des adresses dans le pool d'adresses définies dans la liste d'accès que vous avez créée à la tâche 1.

```
R2(config)#ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask
255.255.255.252
R2(config)#ip nat inside source list R2NAT pool R2POOL overload
```

Étape 2. Configuration des interfaces sur R2 pour appliquer la fonction NAT

Dans le mode de configuration d'interface sur R2, configurez chaque interface à l'aide de la commande **ip nat** {**inside** | **outside**}**.** Étant donné que les adresses internes se trouvent sur des réseaux connectés aux interfaces Fa0/0, Serial 0/0/0 et Serial0/0/1, utilisez la commande **ip nat inside** pour configurer ces interfaces. Internet étant connecté à Serial0/1/0, utilisez la commande **ip nat outside** sur cette interface.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 89 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : configuration de FAI avec une route statique

Étape 1. Configuration de FAI avec une route statique vers R2

FAI nécessite une route statique vers les adresses publiques de R2. Pour cela, utilisez la commande suivante :

```
FAI(config)#ip route 209.165.202.128 255.255.255.224 serial0/0/0
```

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 5 : test de la connectivité

Vous devez maintenant être en mesure d'envoyer une requête ping de tout hôte interne vers l'hôte externe ou vers le serveur Web public.

Pour visualiser les effets de NAT sur un paquet spécifique, passez en mode Simulation et observez le paquet qui provient de PC1.

Cliquez sur la zone d'informations en couleur associée à ce paquet lorsqu'il passe de R1 à R2. Si vous cliquez sur **Inbound PDU Details**, vous devez voir que l'adresse source est 192.168.10.10. En cliquant sur **Outbound PDU Details**, vous devez voir que l'adresse source a été traduite en une adresse 209.165.x.x.

Exercice 7.4.1 : configuration de base de DHCP et NAT

Diagramme de topologie

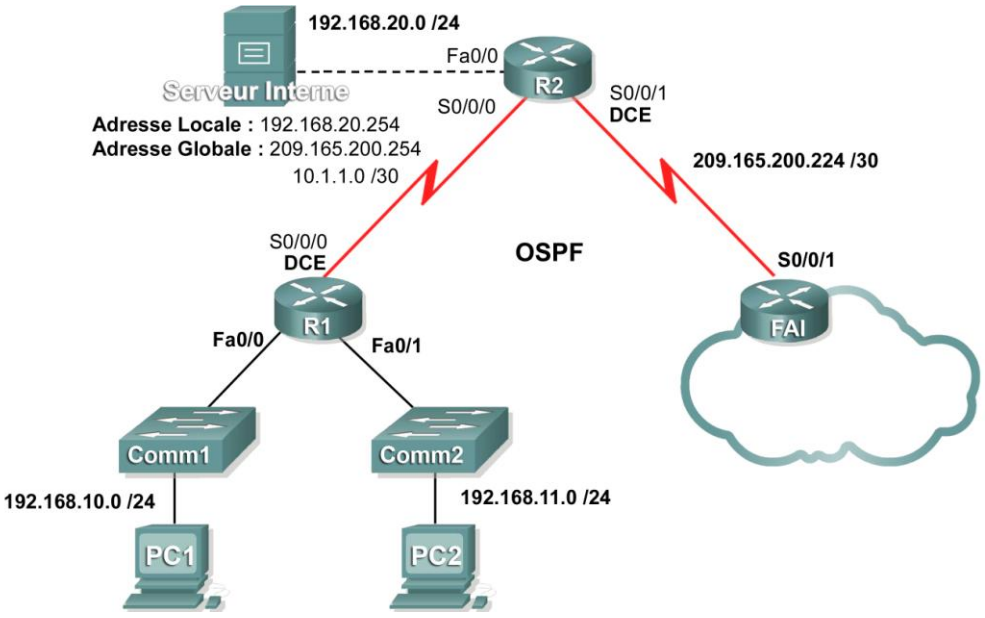


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.1	255.255.255.0
FAI	S0/0/1	209.165.200.226	255.255.255.252

Objectifs pédagogiques

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

- Préparer le réseau
- Effectuer des configurations de base des routeurs
- Configurer un serveur DHCP Cisco IOS
- Configurer le routage statique et par défaut
- Configurer une fonction NAT statique
- Configurer une fonction NAT dynamique avec un pool d'adresses
- Configurer une surcharge NAT

Scénario

Au cours de ces travaux pratiques, vous allez configurer les services IP de la fonction NAT et du protocole DHCP. Le premier routeur est le serveur DHCP. Le second transmet les requêtes DHCP au serveur. Vous allez également établir les configurations NAT statique et dynamique, notamment la surcharge NAT. Lorsque vous aurez terminé les configurations, vérifiez la connectivité entre les adresses internes et externes.

Tâche 1 : configurations de base des routeurs

Configurez les routeurs R1, R2 et FAI selon les instructions suivantes :

- Configurez le nom d'hôte des périphériques.
- Désactivez la recherche DNS.
- Configurez un mot de passe de mode d'exécution privilégié.
- Configurez une bannière du message du jour.
- Configurez un mot de passe pour les connexions de consoles.
- Configurez un mot de passe pour les connexions de terminaux virtuels (vty).
- Configurez des adresses IP sur tous les routeurs. Les PC reçoivent un adressage IP de DHCP plus tard dans l'exercice.
- Activez le protocole OSPF avec l'ID de processus 1 sur R1 et R2. N'annoncez pas le réseau 209.165.200.224/27.

Tâche 2 : configuration d'un serveur DHCP Cisco IOS

Étape 1. Exclusion des adresses attribuées de manière statique

Le serveur DHCP suppose que toutes les adresses IP d'un pool d'adresses DHCP peuvent être affectées à des clients DHCP. Vous devez indiquer les adresses IP que le serveur DHCP ne doit pas affecter aux clients. Ces adresses IP sont généralement des adresses statiques réservées à l'interface de routeur, à l'adresse IP de gestion des commutateurs, aux serveurs et à l'imprimante connectée au réseau local. La commande **ip dhcp excluded-address** empêche le routeur d'attribuer des adresses IP dans la plage configurée. Les commandes suivantes excluent les 10 premières adresses IP de chaque pool pour les réseaux locaux reliés à R1. Ces adresses ne sont alors attribuées à aucun client DHCP.

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Étape 2. Configuration du pool

Créez le pool DHCP à l'aide la de commande **ip dhcp pool** et donnez-lui le nom **R1Fa0**.

```
R1(config)#ip dhcp pool R1Fa0
```

Précisez le sous-réseau à utiliser lors de l'attribution des adresses IP. Les pools DHCP s'associent automatiquement à une interface en fonction de l'instruction réseau. Le routeur fonctionne désormais comme un serveur DHCP et distribue des adresses dans le sous-réseau 192.168.10.0/24 en commençant par 192.168.10.1.

```
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Configurez le routeur par défaut et le serveur de noms de domaine du réseau. Les clients reçoivent ces paramètres via le protocole DHCP, ainsi qu'une adresse IP.

```
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.10.1
```

Remarque : aucun serveur DNS n'est présent sur 192.168.11.5. Vous configurez la commande uniquement dans un objectif d'apprentissage.

```
R1(config)#ip dhcp pool R1Fa1
R1(dhcp-config)#network 192.168.11.0 255.255.255.0
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.11.1
```

Étape 3. Vérification de la configuration de DHCP

Il vous est possible de vérifier la configuration du serveur DHCP de plusieurs façons. La façon la plus simple est de configurer un hôte sur le sous-réseau pour recevoir une adresse IP via le protocole DHCP. Vous pouvez ensuite envoyer des commandes sur le routeur pour obtenir plus d'informations. La commande **show ip dhcp binding** fournit des informations sur toutes les adresses DHCP actuellement attribuées. Par exemple, les résultats suivants montrent que l'adresse IP 192.168.10.11 a été attribuée à l'adresse MAC 3031.632e.3537.6563. La période d'utilisation IP expire le 14 septembre 2007 à 19h33.

```
R1#show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.10.11 0007.EC66.8752 -- Automatic
192.168.11.11 00E0.F724.8EDA -- Automatic
```

Tâche 3 : configuration du routage par défaut et statique

FAI utilise un routage statique pour atteindre tous les réseaux au-delà de R2. Cependant, R2 traduit les adresses privées en adresses publiques avant d'envoyer le trafic à FAI. FAI doit donc être configuré avec les adresses publiques qui font partie de la configuration de la fonction NAT sur R2. Saisissez la route statique suivante sur FAI :

```
FAI(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

Cette route statique inclut toutes les adresses attribuées à R2 pour une utilisation publique.

Configurez une route par défaut sur R2 et propagez la route dans le protocole OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

Attendez quelques secondes que R1 prenne en compte la route par défaut envoyée par R2, puis vérifiez la table de routage de R1. Vous pouvez également effacer la table de routage à l'aide de la commande **clear ip route ***. Une route par défaut pointant vers R2 doit s'afficher dans la table de routage de R1. à partir de R1, envoyez une requête ping à l'interface Serial 0/0/1 sur R2 (209.165.200.225). Les requêtes ping doivent aboutir. Dépannez si elles échouent.

Tâche 4 : configuration de la fonction NAT statique

Étape 1. Mappage statique d'une adresse IP publique vers une adresse IP privée

Le serveur interne relié à R2 est accessible aux hôtes externes au-delà de FAI. Attribuez de façon statique l'adresse IP publique 209.165.200.254 comme l'adresse que NAT utilise pour mapper les paquets sur l'adresse IP privée du serveur interne sur 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Étape 2. Spécification des interfaces NAT internes et externes

Avant de pouvoir appliquer la fonction NAT, précisez les interfaces qui sont à l'intérieur et celles qui sont à l'extérieur.

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

Étape 3. Vérification de la configuration NAT statique

À partir de FAI, envoyez une requête ping à l'adresse IP publique 209.165.200.254.

Tâche 5 : configuration d'une fonction NAT dynamique avec un pool d'adresses

Alors que la fonction NAT statique offre un mappage permanent entre une adresse interne et une adresse publique spécifique, la fonction NAT dynamique mappe des adresses IP privées sur des adresses publiques. Ces adresses IP publiques proviennent d'un pool NAT.

Étape 1. Définition d'un pool d'adresses globales

Créez un pool d'adresses vers lesquelles des adresses source correspondantes sont traduites. La commande suivante crée un pool appelé **MY-NAT-POOL** qui traduit les adresses correspondantes en une adresse IP disponible dans la plage 209.165.200.241 - 209.165.200.246.

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

Étape 2. Création d'une liste de contrôle d'accès étendue permettant d'identifier les adresses internes traduites

```
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Étape 3. Mise en place d'une traduction de source dynamique en reliant le pool à la liste de contrôle d'accès

Un routeur peut posséder plus d'un pool NAT et plusieurs listes de contrôle d'accès. La commande suivante indique au routeur le pool d'adresses à utiliser pour traduire des hôtes que la liste de contrôle d'accès autorise.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

Étape 4. Spécification des interfaces NAT internes et externes

Vous avez déjà précisé les interfaces internes et externes de votre configuration NAT statique. Ajoutez maintenant l'interface série reliée à R1 comme interface interne.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Étape 5. Vérification de la configuration

Envoyez une requête ping à FAI à partir de PC1 et de PC2. Utilisez ensuite la commande **show ip nat translations** sur R2 pour vérifier la fonction NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.241   192.168.10.11      ---                ---
---  209.165.200.242   192.168.11.11      ---                ---
---  209.165.200.254   192.168.20.254     ---                ---
```

Tâche 6 : configuration d'une surcharge NAT

Dans l'exemple précédent, que se passerait-il si vous aviez besoin de plus d'adresses IP publiques que les six autorisées par le pool ?

Par un suivi des numéros de port, la surcharge NAT permet à plusieurs utilisateurs internes de réutiliser une adresse IP publique.

Au cours de cette tâche, vous allez supprimer le pool et l'instruction de mappage configurée dans la tâche précédente. Vous allez ensuite configurer la surcharge NAT sur R2 de telle sorte que les adresses IP internes soient traduites sur l'adresse S0/0/1 de R2 lors de la connexion à tout périphérique externe.

Étape 1. Suppression du pool NAT et de l'instruction de mappage

Utilisez les commandes suivantes pour supprimer le pool NAT et le mappage sur la liste de contrôle d'accès NAT.

```
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

Si vous recevez le message suivant, effacez vos traductions NAT.

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```

Étape 2. Configuration de la fonction PAT sur R2 avec l'adresse IP publique de l'interface Serial 0/0/1

La configuration est similaire à celle de la fonction NAT dynamique, si ce n'est que le mot clé **interface** (et non un pool d'adresses) est utilisé pour identifier l'adresse IP externe. Aucun pool NAT n'est donc défini. Le mot clé **overload** active l'ajout du numéro de port à la traduction.

Puisque vous avez déjà configuré une liste de contrôle d'accès pour identifier les adresses IP internes à traduire, ainsi que les interfaces qui sont internes et celles qui sont externes, vous avez simplement à configurer ce qui suit :

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

Étape 3. Vérification de la configuration

Envoyez une requête ping à FAI à partir de PC1 et de PC2. Utilisez ensuite la commande **show ip nat translations** sur R2 pour vérifier la fonction NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:3 192.168.10.11:3    209.165.200.226:3
209.165.200.226:3
icmp 209.165.200.225:1024192.168.11.11:3    209.165.200.226:3
209.165.200.226:1024
---  209.165.200.254   192.168.20.254     ---                ---
```

Remarque : au cours de la tâche précédente, vous avez pu ajouter le mot clé **overload** à la commande **ip nat inside source list NAT pool MY-NAT-POOL** pour autoriser plus de six utilisateurs simultanés.

Tâche 7 : documentation du réseau

Sur chaque routeur, exécutez la commande **show run** pour accéder aux configurations.

Tâche 1 : préparation du réseau

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

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

Remarque : si vous utilisez un routeur série 1700, 2500 ou 2600, les informations affichées sur le routeur et les descriptions d'interface peuvent apparaître différemment.

Étape 2. Suppression des configurations actuelles des routeurs

Tâche 2 : configurations de base des routeurs

Configurez les routeurs R1, R2 et FAI selon les instructions suivantes :

- Configurez le nom d'hôte des périphériques.
- Désactivez la recherche DNS.
- Configurez un mot de passe de mode d'exécution privilégié.
- Configurez une bannière du message du jour.
- Configurez un mot de passe pour les connexions de consoles.
- Configurez un mot de passe pour les connexions de terminaux virtuels (vty).
- Configurez des adresses IP sur tous les routeurs. Les PC reçoivent un adressage IP de DHCP plus tard dans l'exercice.
- Activez le protocole OSPF avec l'ID de processus 1 sur R1 et R2. N'annoncez pas le réseau 209.165.200.224/27.

Remarque : au lieu de relier un serveur à R2, vous pouvez configurer une interface de bouclage sur R2 pour utiliser l'adresse IP 192.168.20.254/24. Si vous faites cela, vous n'avez pas besoin de configurer l'interface Fast Ethernet.

Tâche 3 : configuration d'un serveur DHCP Cisco IOS

Le logiciel Cisco IOS prend en charge une configuration de serveur DHCP appelée Easy IP. L'objectif de ces travaux pratiques est de faire en sorte que les périphériques des réseaux 192.168.10.0/24 et 192.168.11.0/24 demandent des adresses IP via le protocole DHCP à partir de R2.

Étape 1. Exclusion des adresses attribuées de manière statique

Le serveur DHCP suppose que toutes les adresses IP d'un pool d'adresses DHCP peuvent être affectées à des clients DHCP. Vous devez indiquer les adresses IP que le serveur DHCP ne doit pas affecter aux clients. Ces adresses IP sont généralement des adresses statiques réservées à l'interface du routeur, à l'adresse IP de gestion des commutateurs, aux serveurs et à l'imprimante connectée au réseau local. La commande **ip dhcp excluded-address** empêche le routeur d'attribuer des adresses IP dans la plage configurée. Les commandes suivantes excluent les 10 premières adresses IP de chaque pool pour les réseaux locaux reliés à R1. Ces adresses ne sont alors attribuées à aucun client DHCP.

```
R2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Étape 2. Configuration du pool

Créez le pool DHCP à l'aide la de commande **ip dhcp pool** et donnez-lui le nom **R1Fa0**.

```
R2(config)#ip dhcp pool R1Fa0
```

Précisez le sous-réseau à utiliser lors de l'attribution des adresses IP. Les pools DHCP s'associent automatiquement à une interface en fonction de l'instruction réseau. Le routeur fonctionne désormais comme un serveur DHCP et distribue des adresses dans le sous-réseau 192.168.10.0/24 en commençant par 192.168.10.1.

```
R2(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Configurez le routeur par défaut et le serveur de noms de domaine du réseau. Les clients reçoivent ces paramètres via le protocole DHCP, ainsi qu'une adresse IP.

```
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.10.1
```

Remarque : aucun serveur DNS n'est présent sur 192.168.11.5. Vous configurez la commande uniquement dans un objectif d'apprentissage.

Étant donné que des périphériques du réseau 192.168.11.0/24 demandent également des adresses à R2, un pool séparé doit être créé pour les périphériques du réseau en question. Les commandes sont similaires aux commandes indiquées ci-dessus :

```
R2(config)#ip dhcp pool R1Fa1
R2(dhcp-config)#network 192.168.11.0 255.255.255.0
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.11.1
```

Étape 3. Configuration d'une adresse de diffusion par défaut

Des services réseau tels que le protocole DHCP s'appuient sur des diffusions de couche 2 pour fonctionner. Lorsque les périphériques fournissant ces services existent sur un sous-réseau différent de celui des clients, ils ne peuvent pas recevoir les paquets de diffusion. Puisque le serveur DHCP et les clients DHCP ne se trouvent pas sur le même sous-réseau, configurez R1 pour qu'il transfère les diffusions DHCP à R2, qui est le serveur DHCP, en utilisant la commande de configuration d'interface **ip helper-address**.

Remarquez que la commande **ip helper-address** doit être configurée sur chaque interface impliquée.

```
R1(config)#interface fa0/0
R1(config-if)#ip helper-address 10.1.1.2
R1(config)#interface fa0/1
R1(config-if)#ip helper-address 10.1.1.2
```

Étape 4. Vérification de la configuration de DHCP

Il vous est possible de vérifier la configuration du serveur DHCP de plusieurs façons. La façon la plus simple est de configurer un hôte sur le sous-réseau pour recevoir une adresse IP via le protocole DHCP. Vous pouvez ensuite envoyer des commandes sur le routeur pour obtenir plus d'informations. La commande **show ip dhcp binding** fournit des informations sur toutes les adresses DHCP actuellement attribuées. Par exemple, les résultats suivants montrent que l'adresse IP 192.168.10.11 a été attribuée à l'adresse MAC 3031.632e.3537.6563. La période d'utilisation IP expire le 14 septembre 2007 à 19h33.

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/            Lease expiration        Type
                  Hardware address/
                  User name
192.168.10.11     0063.6973.636f.2d30. Sep 14 2007 07:33 PM    Automatic
                  3031.632e.3537.6563.
                  2e30.3634.302d.566c.
                  31
```

La commande **show ip dhcp pool** affiche des informations sur tous les pools DHCP actuellement configurés sur le routeur. Elle indique que le pool **R1Fa0** est configuré sur R2. Une adresse de ce pool a été louée. Le prochain client demandant une adresse se verra attribuer 192.168.10.12.

```
R2#show ip dhcp pool
Pool R1Fa0 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.10.12        192.168.10.1     - 192.168.10.254    1
```

La commande **debug ip dhcp server events** peut être extrêmement utile pour dépanner des locations de DHCP avec un serveur DHCP Cisco IOS. Voici les informations de débogage sur R1 après la connexion d'un hôte. Remarquez que la partie surlignée montre le DHCP attribuant au client une adresse de 192.168.10.12 et un maque de 255.255.255.0.

```
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
*Sep 13 21:04:18.072:   DHCPD : htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD : remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD : circuit id 00000000
*Sep 13 21:04:18.072: DHCPD : Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD : htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD : remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD : circuit id 00000000
*Sep 13 21:04:18.072: DHCPD : there is no address pool for 192.168.11.1.
*Sep 13 21:04:18.072: DHCPD : Sending notification of DISCOVER:
R1#
*Sep 13 21:04:18.072:   DHCPD : htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD : remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD : circuit id 00000000
*Sep 13 21:04:18.072: DHCPD : Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD : htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD : remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD : circuit id 00000000
R1#
*Sep 13 21:04:20.072: DHCPD : Adding binding to radix tree (192.168.10.12)
*Sep 13 21:04:20.072: DHCPD : Adding binding to hash tree
*Sep 13 21:04:20.072: DHCPD : assigned IP address 192.168.10.12 to client
0063.6973.636f.2d30.3031.632e.3537.6563.2e30.3634.302d.566c.31.
*Sep 13 21:04:20.072: DHCPD : Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.072:  DHCPD : address 192.168.10.12 mask 255.255.255.0
*Sep 13 21:04:20.072:   DHCPD : htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.072:   DHCPD : lease time remaining (secs) = 86400
*Sep 13 21:04:20.076: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.076:  DHCPD : address 192.168.10.12 mask 255.255.255.0
R1#
*Sep 13 21:04:20.076:   DHCPD : htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.076:   DHCPD : lease time remaining (secs) = 86400
```

Tâche 4 : configuration du routage par défaut et statique

FAI utilise un routage statique pour atteindre tous les réseaux au-delà de R2. Cependant, R2 traduit les adresses privées en adresses publiques avant d'envoyer le trafic à FAI. FAI doit donc être configuré avec les adresses publiques qui font partie de la configuration de la fonction NAT sur R2. Saisissez la route statique suivante sur FAI :

```
FAI(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

Cette route statique inclut toutes les adresses attribuées à R2 pour une utilisation publique.

Configurez une route par défaut sur R2 et propagez la route dans le protocole OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209 165 200 225
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

Attendez quelques secondes que R1 prenne en compte la route par défaut envoyée par R2, puis vérifiez la table de routage de R1. Vous pouvez également effacer la table de routage à l'aide de la commande **clear ip route *.** Une route par défaut pointant vers R2 doit s'afficher dans la table de routage de R1. À partir de R1, envoyez une requête ping à l'interface Serial 0/0/1 sur R2 (209.165.200.226). Les requêtes ping doivent aboutir. Dépannez si elles échouent.

Tâche 5 : configuration de la fonction NAT statique

Étape 1. Mappage statique d'une adresse IP publique vers une adresse IP privée

Le serveur interne relié à R2 est accessible aux hôtes externes au-delà de FAI. Attribuez de façon statique l'adresse IP publique 209.165.200.254 comme l'adresse que NAT utilise pour mapper les paquets sur l'adresse IP privée du serveur interne sur 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Étape 2. Spécification des interfaces NAT internes et externes

Avant de pouvoir appliquer la fonction NAT, précisez les interfaces qui sont à l'intérieur et celles qui sont à l'extérieur.

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

Remarque : si vous utilisez un serveur interne simulé, affectez la commande **ip nat inside** à l'interface de bouclage.

Étape 3. Vérification de la configuration NAT statique

À partir de FAI, envoyez une requête ping à l'adresse IP publique 209.165.200.254.

Tâche 6 : configuration d'une fonction NAT dynamique avec un pool d'adresses

Alors que la fonction NAT statique offre un mappage permanent entre une adresse interne et une adresse publique spécifique, la fonction NAT dynamique mappe des adresses IP privées sur des adresses publiques. Ces adresses IP publiques proviennent d'un pool NAT.

Étape 1. Définition d'un pool d'adresses globales

Créez un pool d'adresses vers lesquelles des adresses source correspondantes sont traduites. La commande suivante crée un pool appelé **MY-NAT-POOL** qui traduit les adresses correspondantes en une adresse IP disponible dans la plage 209.165.200.241 - 209.165.200.246.

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

Étape 2. Création d'une liste de contrôle d'accès étendue permettant d'identifier les adresses internes traduites

```
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Étape 3. Mise en place d'une traduction de source dynamique en reliant le pool à la liste de contrôle d'accès

Un routeur peut posséder plus d'un pool NAT et plusieurs listes de contrôle d'accès. La commande suivante indique au routeur le pool d'adresses à utiliser pour traduire des hôtes que la liste de contrôle d'accès autorise.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

Étape 4. Spécification des interfaces NAT internes et externes

Vous avez déjà précisé les interfaces internes et externes de votre configuration NAT statique. Ajoutez maintenant l'interface série reliée à R1 comme interface interne.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Étape 5. Vérification de la configuration

Envoyez une requête ping à FAI à partir de PC1 ou de l'interface Fast Ethernet sur R1 à l'aide de la commande **ping** étendue. Utilisez ensuite les commandes **show ip nat translations** et **show ip nat statistics** sur R2 pour vérifier la fonction NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.241:4 192.168.10.1:4     209.165.200.226:4  209.165.200.226:4
--- 209.165.200.241    192.168.10.1       ---                ---
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 statique, 1 dynamique ; 0 étendu)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 23  Misses: 3
CEF Translated packets: 18, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT pool MY-NAT-POOL refcount 1
 pool MY-NAT-POOL: netmask 255.255.255.248
        start 209.165.200.241 end 209.165.200.246
        type generic, total addresses 6, allocated 1 (16%), misses 0
Queued Packets: 0
```

Pour dépanner tout problème posé par la fonction NAT, utilisez la commande **debug ip nat**. Activez le débogage de la fonction NAT et renvoyez une requête ping à partir de PC1.

```
R2#debug ip nat
IP NAT debugging is on
R2#
*Sep 13 21:15:02.215: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [25]
*Sep 13 21:15:02.231: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [25]
*Sep 13 21:15:02.247: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [26]
*Sep 13 21:15:02.263: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [26]
*Sep 13 21:15:02.275: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [27]
*Sep 13 21:15:02.291: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [27]
*Sep 13 21:15:02.307: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [28]
*Sep 13 21:15:02.323: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [28]
*Sep 13 21:15:02.335: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [29]
*Sep 13 21:15:02.351: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [29]
R2#
```

Tâche 7 : configuration d'une surcharge NAT

Dans l'exemple précédent, que se passerait-il si vous aviez besoin de plus d'adresses IP publiques que les six autorisées par le pool ?

_____

Par un suivi des numéros de port, la surcharge NAT permet à plusieurs utilisateurs internes de réutiliser une adresse IP publique.

Au cours de cette tâche, vous allez supprimer le pool et l'instruction de mappage configurée dans la tâche précédente. Vous allez ensuite configurer la surcharge NAT sur R2 de telle sorte que les adresses IP internes soient traduites sur l'adresse S0/0/1 de R2 lors de la connexion à tout périphérique externe.

Étape 1. Suppression de l'instruction de mappage et de pool NAT

Utilisez les commandes suivantes pour supprimer le pool NAT et le mappage sur la liste de contrôle d'accès NAT.

```
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

Si vous recevez le message suivant, effacez vos traductions NAT.

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```

Étape 2. Configuration de la fonction PAT sur R2 avec l'adresse IP publique de l'interface Serial 0/0/1

La configuration est similaire à celle de la fonction NAT dynamique, si ce n'est que le mot clé **interface** (et non un pool d'adresses) est utilisé pour identifier l'adresse IP externe. Aucun pool NAT n'est donc défini. Le mot clé **overload** active l'ajout du numéro de port à la traduction.

Puisque vous avez déjà configuré une liste de contrôle d'accès pour identifier les adresses IP internes à traduire, ainsi que les interfaces qui sont internes et celles qui sont externes, vous avez simplement à configurer ce qui suit :

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

Étape 3. Vérification de la configuration

Envoyez une requête ping à FAI à partir de PC1 ou de l'interface Fast Ethernet sur R1 à l'aide de la commande **ping** étendue. Utilisez ensuite les commandes **show ip nat translations** et **show ip nat statistics** sur R2 pour vérifier la fonction NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:6 192.168.10.11:6    209.165.200.226:6  209.165.200.226:6
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 statique, 1 dynamique ; 1 étendu)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 48  Misses: 6
CEF Translated packets: 46, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 2] access-list NAT interface Serial0/0/1 refcount 1
Queued Packets: 0
```

Remarque : au cours de la tâche précédente, vous avez pu ajouter le mot clé **overload** à la commande **ip nat inside source list NAT pool MY-NAT-POOL** pour autoriser plus de six utilisateurs simultanés.

Tâche 8 : documentation du réseau

Sur chaque routeur, exécutez la commande **show run** pour accéder aux configurations.

Tâche 9 : remise en état

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

Exercice 7.4.2 : configuration avancée de DHCP et NAT

Diagramme de topologie

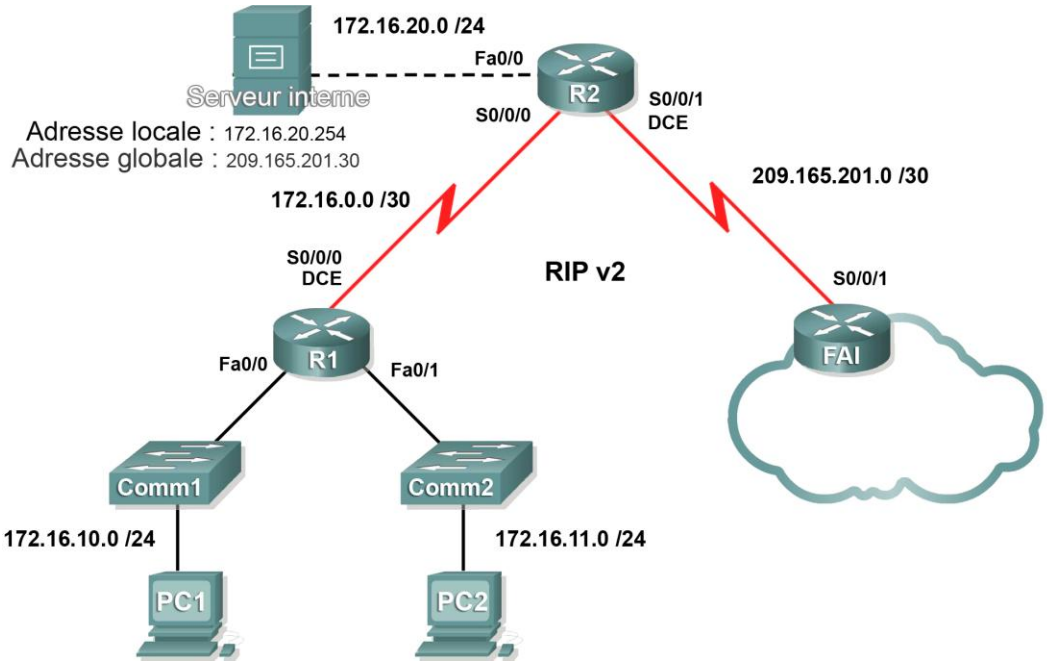


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**S0/0/0**	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	**S0/0/0**	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
FAI	**S0/0/1**	209.165.201.2	255.255.255.252

Objectifs pédagogiques

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

- Préparer le réseau
- Effectuer des configurations de base des routeurs
- Configurer un serveur DHCP Cisco IOS
- Configurer le routage par défaut et statique
- Configurer une fonction NAT statique
- Configurer une fonction NAT dynamique avec un pool d'adresses
- Configurer une surcharge NAT

Scénario

Au cours de ces travaux pratiques, vous allez configurer les services d'adresse IP à l'aide du réseau indiqué dans le diagramme de topologie. Si vous avez besoin d'aide, reportez-vous à l'exercice de configuration de base de NAT et du protocole DHCP. Cependant, essayez d'aller le plus loin possible par vos propres moyens.

Tâche 1 : configurations de base des routeurs

Configurez les routeurs R1, R2 et FAI selon les instructions suivantes :

- Configurez le nom d'hôte des périphériques.
- Désactivez la recherche DNS.
- Configurez un mot de passe de mode d'exécution privilégié.
- Configurez une bannière du message du jour.
- Configurez un mot de passe pour les connexions de consoles.
- Configurez un mot de passe pour les connexions de terminaux virtuels (vty).
- Configurez des adresses IP sur tous les routeurs. Les PC reçoivent un adressage IP de DHCP plus tard dans l'exercice.
- Activez le protocole RIPv2 sur R1 et sur R2. N'annoncez pas le réseau 209.165.200.224/27.

Tâche 2 : configuration d'un serveur DHCP Cisco IOS

Configurez R1 comme serveur DHCP pour les deux réseaux locaux reliés directement.

Étape 1. Exclusion des adresses attribuées de manière statique

Excluez les trois premières adresses de chaque pool.

Étape 2. Configuration du pool DHCP

- Créez deux pools DHCP. Nommez l'un d'entre eux **R1_LAN10** pour le réseau 172.16.10.0/24, et l'autre **R1_LAN11** pour le réseau 172.16.11.0/24.
- Configurez chaque pool avec une passerelle par défaut et un DNS simulé sur 172.16.20.254.

Étape 3. Vérification de la configuration de DHCP

Tâche 3 : configuration du routage par défaut et statique

- Configurez FAI avec une route statique pour le réseau 209.165.201.0/27. Utilisez l'argument d'interface de sortie (exit interface).
- Configurez une route par défaut sur R2 et propagez la route dans le protocole OSPF. Utilisez l'argument d'adresse IP de saut suivant (next-hop IP address).

Tâche 4 : configuration de la fonction NAT statique

Étape 1. Mappage statique d'une adresse IP publique vers une adresse IP privée

Mappez statiquement l'adresse IP du serveur interne sur l'adresse publique 209.165.201.30.

Étape 2. Spécification des interfaces NAT internes et externes

Étape 3. Vérification de la configuration NAT statique

Tâche 5 : configuration d'une fonction NAT dynamique avec un pool d'adresses

Étape 1. Définition d'un pool d'adresses globales

Créez un pool nommé **NAT_POOL** pour les adresses IP 209.165.201.9 à 209.165.201.14 à l'aide d'un masque de sous-réseau /29.

Étape 2. Création d'une liste de contrôle d'accès nommée standard permettant d'identifier les adresses internes traduites

Utilisez le nom **NAT_ACL** et autorisez les hôtes reliés aux deux réseaux locaux sur R1.

Remarque : le réseau LAN **.10** doit être le premier configuré, puis le réseau LAN **.11**. Sinon, Packet Tracer n'évaluera pas correctement la liste de contrôle d'accès.

Étape 3. Mise en place d'une traduction de source dynamique

Reliez le pool NAT à la liste de contrôle d'accès et autorisez la surcharge NAT.

Étape 4. Spécification des interfaces NAT internes et externes

Vérifiez que les interfaces internes et externes sont toutes correctement spécifiées.

Étape 5. Vérification de la configuration NAT dynamique par commande ping de PC1 et PC2 vers FAI

Tâche 6 : documentation du réseau

Sur chaque routeur, exécutez la commande **show run** pour accéder aux configurations.

Exercice PT 7.4.3 : dépannage de DHCP et NAT

Diagramme de topologie

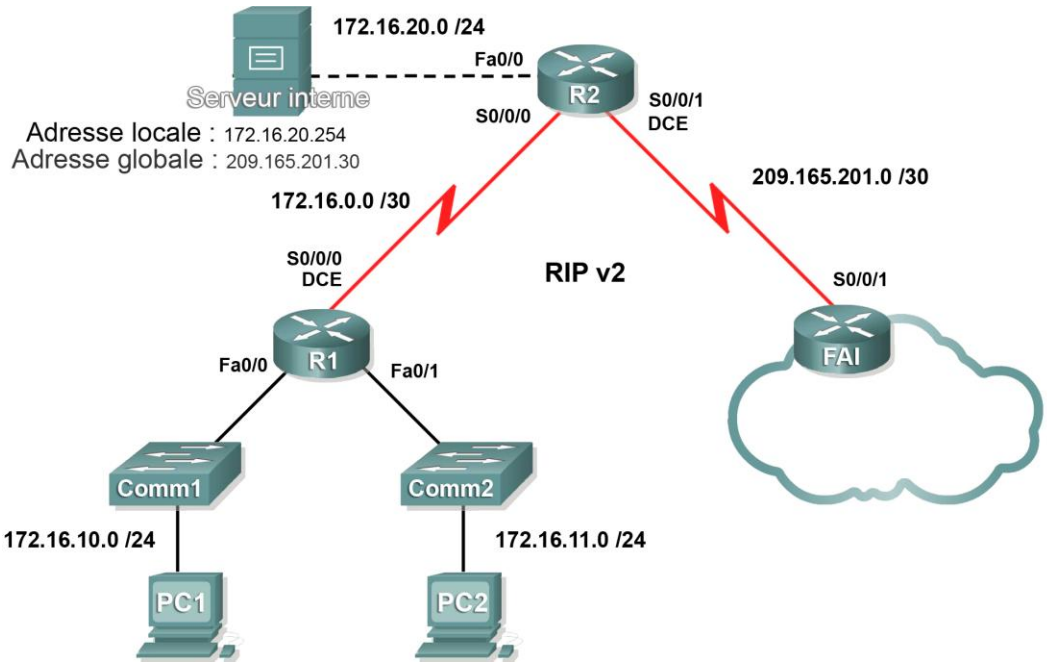


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	S0/0/0	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	S0/0/0	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
FAI	S0/0/1	209.165.201.2	255.255.255.252

Objectifs pédagogiques

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

- Trouver et corriger les erreurs de réseau
- Documenter le réseau corrigé

Scénario

Les routeurs de votre société ont été configurés par un ingénieur réseau sans expérience. De nombreuses erreurs de configuration ont entraîné des problèmes de connectivité. Votre supérieur vous a demandé de dépanner et de corriger les erreurs de configuration et de rapporter par écrit votre travail. En utilisant vos connaissances de DHCP, de NAT et des méthodes de test standard, trouvez et corrigez les erreurs. Assurez-vous que tous les clients disposent d'une connectivité totale.

Tâche 1 : recherche et correction des erreurs sur le réseau

Utilisez les commandes de dépannage pour détecter les erreurs et les corriger. Une fois toutes les erreurs corrigées, vous devez être en mesure d'envoyer une requête ping à partir de PC1 et de PC2 vers FAI. FAI doit être en mesure d'envoyer une requête ping au serveur Web interne à son adresse IP publique.

Tâche 2 : documentation du réseau corrigé

Sur chaque routeur, exécutez la commande **show run** pour accéder aux configurations.

Exercice PT 7.5.1 : exercice d'intégration des compétences Packet Tracer

Diagramme de topologie

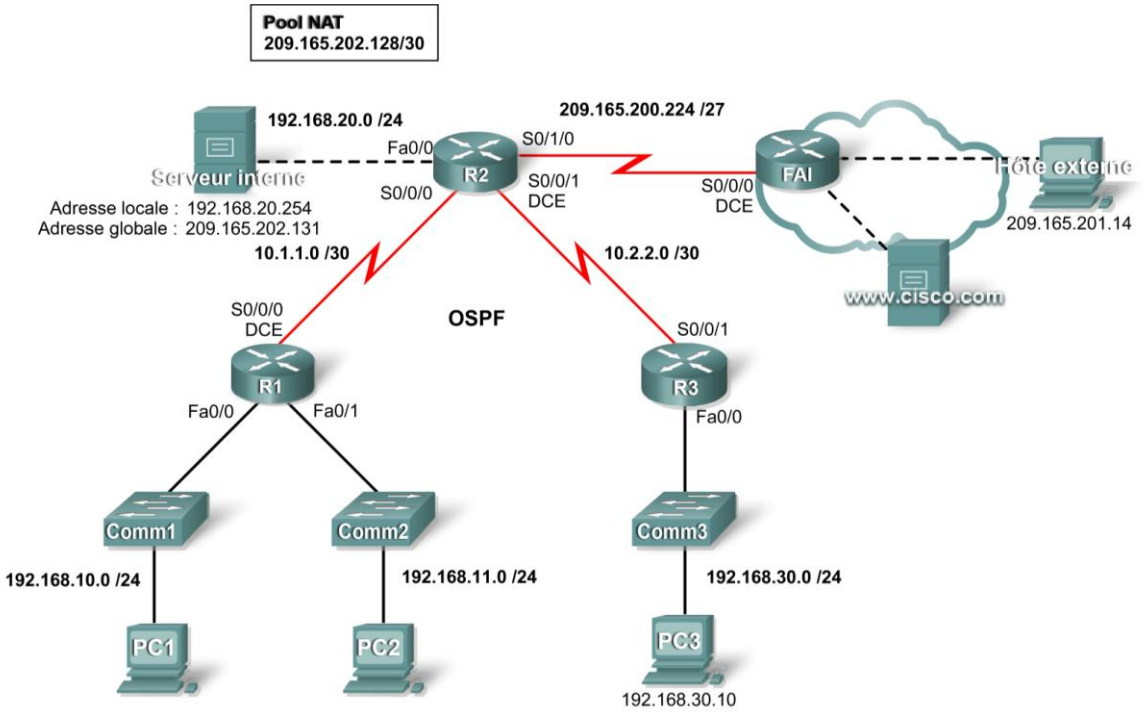


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**Fa0/0**	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**Fa0/0**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	225.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
Serveur interne	**Carte réseau**	Locale : 192.168.20.254	255.255.255.0
	Carte réseau	Globale : 209.165.202.131	255.255.255.252
Hôte externe	**Carte réseau**	209.165.201.14	255.255.255.240

Objectifs pédagogiques

- Appliquer des configurations de base
- Configurer l'encapsulation PPP avec CHAP
- Configurer un routage dynamique et un routage par défaut
- Configurer des routeurs avec Easy IP
- Vérifier que des PC sont automatiquement configurés avec des informations d'adressage
- Configurer un serveur DNS avec des valeurs DNS
- Configurer une liste de contrôle d'accès pour autoriser la fonction NAT
- Configurer une fonction NAT statique
- Configurer une fonction NAT dynamique avec surcharge
- Configurer le routeur FAI avec une route statique
- Tester la connectivité

Présentation

Au cours de cet exercice final, vous allez configurez les protocoles PPP, OSPF, DHCP, la fonction NAT et le routage par défaut vers FAI. Vous allez ensuite vérifier votre configuration.

Tâche 1 : application des configurations de base

Étape 1. Configuration de R1, R2 et R3 avec la configuration globale de base

- Nom d'hôte indiqué dans la table d'adressage
- Ligne de console pour un accès au réseau avec le mot de passe **cisco**
- Lignes vty 0-4 pour l'accès au réseau avec le mot de passe **cisco**
- Mot de passe secret **class**
- Bannière « ACCÈS AUTORISÉ UNIQUEMENT ! »

Seuls le nom d'hôte et la bannière sont notés.

Étape 2. Configuration des interfaces sur R1, R2 et R3

Consultez la table d'adressage pour déterminer les adresses des interfaces. Consultez le diagramme de topologie pour définir les interfaces qui sont des interfaces ETCD. Configurez les interfaces ETCD pour obtenir une fréquence d'horloge de 64000.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 38 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 2 : configuration de l'encapsulation PPP avec CHAP

Étape 1. Configuration de la liaison entre R1 et R2 pour utiliser l'encapsulation PPP avec l'authentification CHAP

Le mot de passe pour l'authentification CHAP est **cisco123.**

Étape 2. Configuration de la liaison entre R2 et R3 pour utiliser l'encapsulation PPP avec l'authentification CHAP

Le mot de passe pour l'authentification CHAP est **cisco123.**

Étape 3. Vérification du rétablissement de la connectivité entre les routeurs

R2 doit être en mesure d'envoyer une requête ping à R1 et à R3. Quelques minutes peuvent être nécessaires pour que les interfaces se rétablissent. Pour accélérer le processus, vous pouvez alterner entre les modes Realtime (temps réel) et Simulation. Une autre solution permettant de contourner ce comportement de Packet Tracer consiste à utiliser les commandes **shutdown** et **no shutdown** sur les interfaces.

Remarque : il est possible que les interfaces se désactivent de façon aléatoire pendant l'exercice à cause d'un bogue de Packet Tracer. En principe, l'interface se rétablit seule après quelques secondes d'attente.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 51 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 3 : configuration du routage dynamique et du routage par défaut

Étape 1. Configuration de R1, R2 et R3 pour utiliser le protocole de routage OSPF

- Utilisez l'ID de processus 1 lorsque vous configurez OSPF sur les routeurs.
- Annoncez tous les réseaux connectés à R1 et à R3 mais n'envoyez pas de mises à jour de routage aux interfaces du réseau local.
- Sur R2, n'annoncez pas le réseau 209.165.200.224 et n'envoyez pas de mises à jour de routage aux interfaces Fa0/0 ou Serial0/1/0.

Étape 2. Configuration d'une route par défaut sur R2

Configurez une route par défaut vers FAI, en indiquant l'interface sortante sur R2 comme adresse de saut suivant.

Étape 3. Configuration d'OSPF pour annoncer la route par défaut

Sur R2, entrez la commande pour annoncer la route par défaut vers R1 et R3, via OSPF.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 66 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : configuration de routeurs avec Easy IP

Étape 1. Configuration de R1 pour agir comme serveur DHCP pour les réseaux 192.168.10.0 et 192.68.11.0

- Nommez le pool DHCP pour le réseau 192.168.10.0 **R1LAN1**. Pour le réseau 192.168.11.0, donnez le nom **R1LAN2**.
- Excluez de l'attribution dynamique les neuf premières adresses de chaque réseau.
- En plus de l'adresse IP et du masque de sous-réseau, affectez les adresses de la passerelle par défaut et du serveur DNS.

Étape 2. Configuration de R3 pour agir comme serveur DHCP pour le réseau 192.168.30.0

- Nommez le pool DHCP pour le réseau 192.168.30.0 **R3LAN**.
- Excluez de l'attribution dynamique les neuf premières adresses de chaque réseau.
- En plus de l'adresse IP et du masque de sous-réseau, affectez les adresses de la passerelle par défaut et du serveur DNS.

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 75 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 5 : vérification de la configuration automatique des PC avec des informations d'adressage

Étape 1. Configuration de PC1, PC2 et PC3 pour la configuration IP automatique avec DHCP

Étape 2. Vérification d'attribution d'adresse à chaque PC par le pool DHCP qui convient

Étape 3. Vérification des résultats

Votre taux de réalisation doit être de 88 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 6 : configuration d'un serveur DNS avec des valeurs DNS

Étape 1. Configuration du serveur DNS

Pour configurer DNS sur le serveur interne, cliquez sur le bouton **DNS** dans l'onglet **Config**.

Vérifiez que le système DNS est sous tension puis saisissez la valeur DNS suivante :

- www.cisco.com 209.165.201.30

Étape 2. Vérification des résultats

Vous ne pouvez pas envoyer de commande ping au serveur **www.cisco.com** par nom de domaine tant que vous n'avez pas configuré la route statique à la tâche 10. Votre taux de réalisation doit être de 90 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 7 : configuration d'une liste de contrôle d'accès pour autoriser la fonction NAT

Étape 1. Création d'une liste de contrôle d'accès nommée standard

Créez la liste de contrôle d'accès nommée standard, **R2NAT**, qui autorise NAT à mapper tous les réseaux internes.

Remarque : pour que Packet Tracer note correctement cette tâche, vous devez saisir les réseaux autorisés dans l'ordre suivant :

- 192.168.10.0
- 192.168.20.0
- 192.168.30.0
- 192.168.11.0

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 91 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 8 : configuration de la fonction NAT statique

Étape 1. Configuration de la fonction NAT statique pour un serveur Web interne

Configurez la fonction NAT statique pour mapper l'adresse IP locale et les adresses IP globales pour le Serveur interne. Utilisez les adresses indiquées dans la table d'adressage.

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 92 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 9 : configuration de la fonction NAT dynamique avec surcharge

Étape 1. Configuration du pool NAT dynamique

Configurez un pool d'adresses NAT dynamique en utilisant le pool NAT indiqué dans le diagramme de topologie. Nommez le pool d'adresses **R2POOL**.

Étape 2. Configuration du mappage NAT dynamique

Mappez les adresses dans R2POOL sur les réseaux définis précédemment dans R2NAT.

Étape 3. Application de NAT aux interfaces internes et externes de R2

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 99 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 10 : configuration du routeur FAI avec une route statique

Étape 1. Configuration d'une route statique vers les adresses IP globales de R2

Il s'agit du réseau 209.165.202.128/27. Utilisez l'interface série de FAI comme adresse de saut suivant.

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 11 : test de connectivité

- Les hôtes internes doivent être capables d'envoyer une requête ping à l'hôte externe.
- Les hôtes internes doivent être capables d'envoyer une requête ping à www.cisco.com.
- L'hôte externe doit être capable d'envoyer une requête ping au Serveur interne par son adresse IP globale.

Exercice PT 8.1.2 : découverte et documentation du réseau

Diagramme de topologie

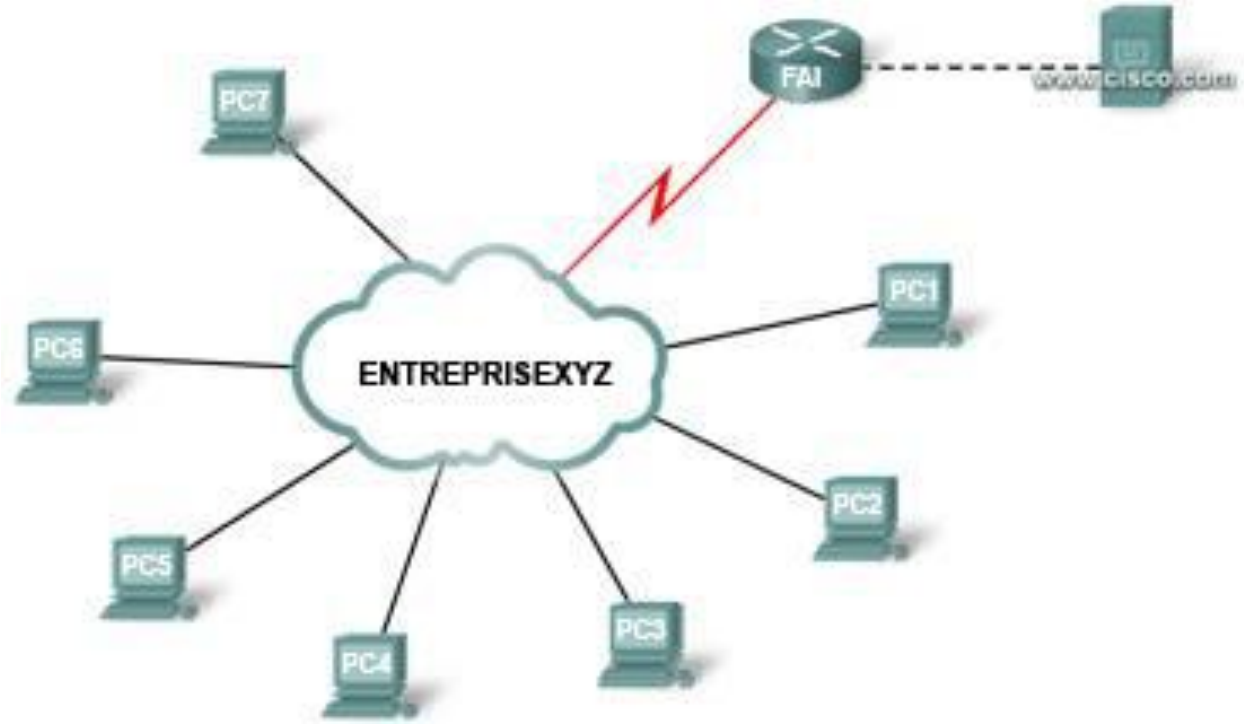


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC1	**Carte réseau**			
PC2	**Carte réseau**			
PC3	**Carte réseau**			
PC4	**Carte réseau**			
PC5	**Carte réseau**			
PC6	**Carte réseau**			
PC7	**Carte réseau**			

Objectifs pédagogiques

- Tester la connectivité
- Découvrir des informations de configuration du PC
- Découvrir les informations de configuration de la passerelle par défaut
- Découvrir les routes et voisins du réseau
- Établir la topologie du réseau

Présentation

Cet exercice couvre les étapes à suivre pour découvrir un réseau à l'aide, principalement, des commandes **telnet**, **show cdp neighbors detail** et **show ip route**. Il s'agit de la première partie d'un exercice en comptant deux.

La topologie que vous voyez lorsque vous ouvrez l'exercice Packet Tracer ne révèle pas tous les détails du réseau. Ils ont été cachés à l'aide de la fonction cluster de Packet Tracer. L'infrastructure du réseau a été réduite et la topologie du fichier ne montre que les périphériques d'extrémité. Votre tâche consiste à faire appel à vos connaissances des commandes de découverte et des réseaux pour découvrir l'ensemble de la topologie du réseau et la documenter.

Tâche 1 : test de connectivité

Étape 1. Convergence et test du réseau

Packet Tracer a besoin d'un peu d'aide pour la convergence du réseau. Envoyez des requêtes ping entre les PC et entre les PC et le serveur de www.cisco.com pour accélérer la convergence et tester le réseau. Chaque PC doit être en mesure d'envoyer des requêtes ping aux autres PC ainsi qu'au serveur. N'oubliez pas que plusieurs envois de requêtes ping peuvent être nécessaires avant d'aboutir.

Tâche 2 : découverte d'informations de configuration du PC

Étape 1. Accès à l'invite de commande de PC1

Cliquez sur **PC1**, sur l'onglet **Desktop** puis sur **Command Prompt**

Étape 2. Détermination des informations d'adressage pour PC1

Pour déterminer la configuration d'adressage IP actuelle, saisissez la commande **ipconfig /all**.

Remarque : dans Packet Tracer, vous devez saisir un espace entre **ipconfig** et **/all**.

Étape 3. Documentation des informations pour PC1 dans la table d'adressage

Étape 4. Procédure identique pour les autres PC

Répétez les étapes 1 à 3 pour les PC 2 à 7.

Tâche 3 : découverte des informations de configuration de la passerelle par défaut

Étape 1. Test de la connectivité entre PC1 et sa passerelle par défaut

À partir de PC1, envoyez une requête ping à la passerelle par défaut pour vérifier la connectivité.

Étape 2. Connexion Telnet à la passerelle par défaut

Utilisez la commande **telnet** *adresse-ip*. L'adresse IP est celle de la passerelle par défaut. Lorsque vous y êtes invité, entrez le mot de passe **cisco**.

Étape 3. Affichage des configurations d'interface actuelles

Utilisez les commandes **show ip interface brief** et **show protocols** pour déterminer les configurations d'interface actuelles.

Quelle est la différence entre ces deux commandes ?

_____

Étape 4. Documentation du nom d'hôte et de la configuration d'interface dans la table d'adressage

Utilisez l'espace suivant pour ébaucher une topologie.

Ébauche de topologie

Tâche 4 : découverte des routes et des voisins du réseau

Étape 1. Affichage de la table de routage sur le même routeur

Affichez la table de routage à l'aide de la commande **show ip route**. En principe, cinq routes connectées et six routes détectées par le protocole RIP doivent s'afficher, dont une est une route par défaut.

En plus des routes, quelles autres informations utiles la table de routage fournit-elle pour vous aider à découvrir et à documenter le réseau ?

_____

Étape 2. Découverte des périphériques Cisco connectés directement

Sur le même routeur, lancez la commande **show cdp neighbors detail** pour découvrir d'autres périphériques Cisco connectés directement.

Étape 3. Documentation des informations sur les voisins et test de connectivité

La commande **show cdp neighbors detail** fournit des informations sur un voisin, notamment son adresse IP. Documentez le nom d'hôte et l'adresse IP du voisin. Envoyez ensuite une requête ping à l'adresse IP pour tester la connectivité. Les deux ou trois premières requêtes ping échouent le temps que le protocole ARP résolve l'adresse MAC.

Étape 4. Connexion Telnet au voisin et découverte des périphériques Cisco connectés directement

Établissez une connexion Telnet avec le voisin et utilisez la commande **show cdp neighbors detail** pour découvrir d'autres périphériques Cisco connectés directement.

Cette fois, vous devez voir trois périphériques. Pourquoi le routeur est-il répertorié plusieurs fois ?

_____

Étape 5. Documentation des noms d'hôte et des adresses IP des voisins et test de connectivité

Documentez et envoyez une requête ping aux nouveaux voisins que vous avez découverts. N'oubliez pas que les deux ou trois premières requêtes ping échouent le temps que le protocole ARP résolve les adresses MAC.

Étape 6. Connexion Telnet à chaque voisin et recherche de périphériques Cisco supplémentaires

Établissez une connexion Telnet avec chacun des nouveaux voisins que vous avez découverts et utilisez la commande **show cdp neighbors detail** pour vérifier la présence de tout périphérique Cisco supplémentaire. Le mot de passe d'accès est **cisco**.

Étape 7. Poursuite de la découverte et de la documentation du réseau

Quittez les sessions Telnet pour revenir au routeur de passerelle par défaut pour PC1. à partir de ce routeur, établissez une connexion Telnet avec d'autres routeurs du réseau pour poursuivre la découverte et la documentation du réseau. N'oubliez pas d'utiliser les commandes **show ip route** et **show ip cdp neighbors** pour découvrir des adresses IP que vous pouvez utiliser pour Telnet.

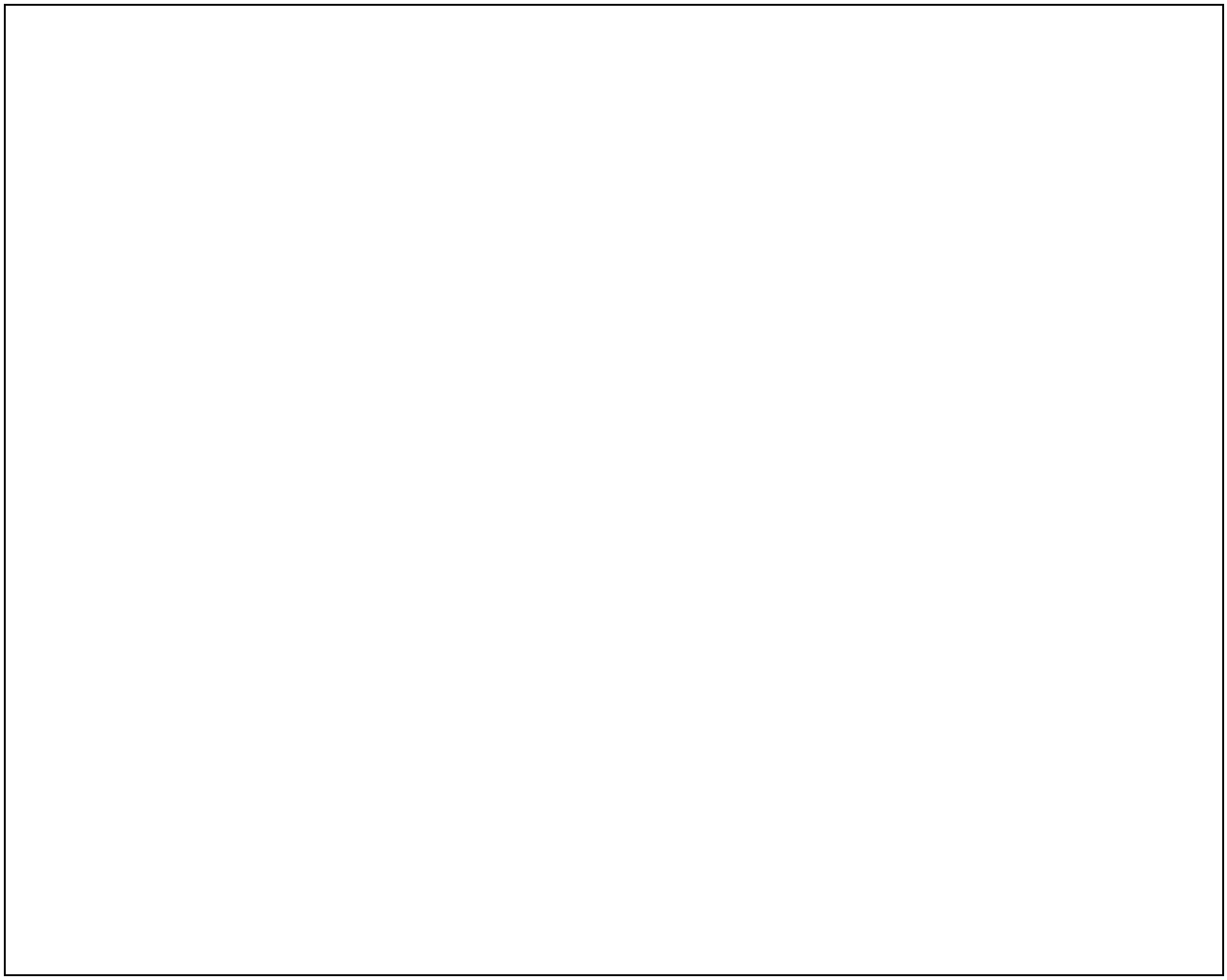
Tâche 5 : établissement de la topologie du réseau

Étape 1. Établissement d'une topologie

Maintenant que vous avez découvert tous les périphériques réseau et que vous avez documenté leurs adresses, utilisez la table d'adressage et votre ébauche de la topologie pour en établir une version définitive.

Indice : un nuage Frame Relay se trouve au milieu du réseau.

Diagramme de topologie finale

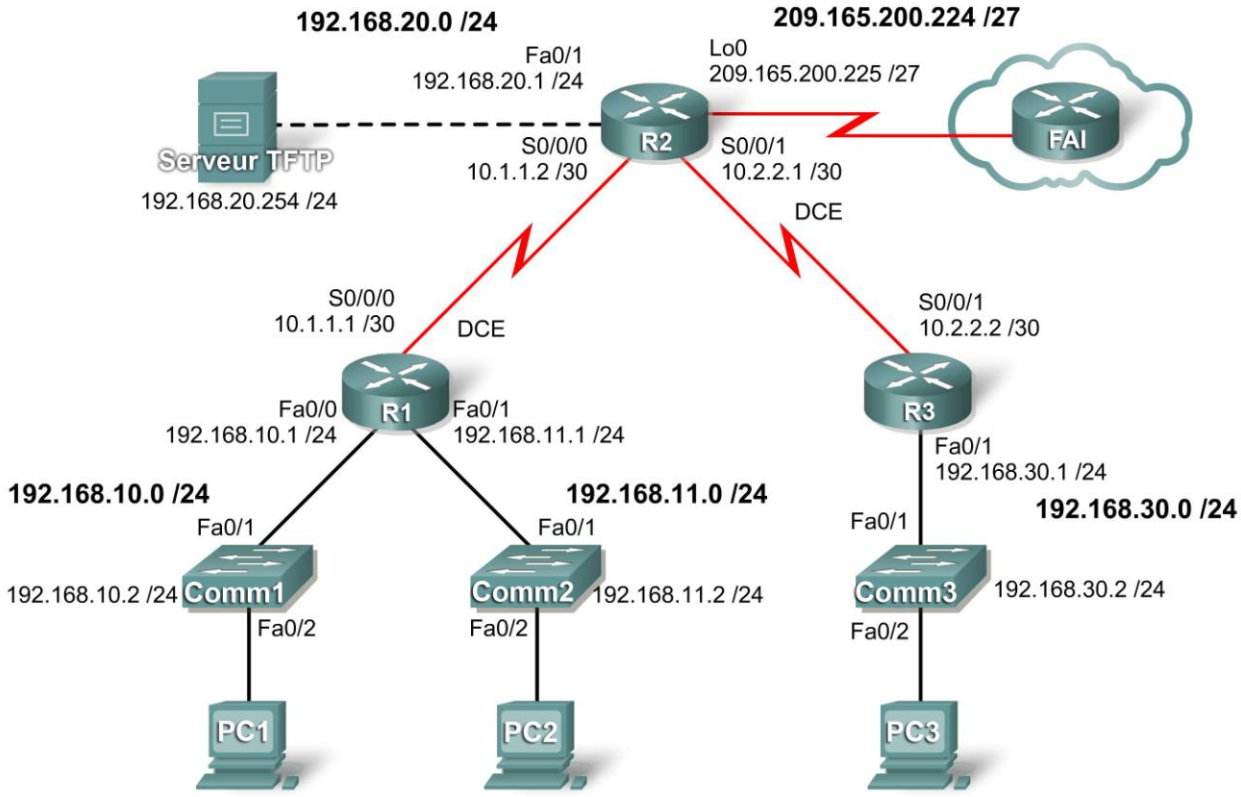


Étape 2. Conservation de cette documentation

Vous aurez besoin de votre diagramme de topologie et de la table d'adressage au prochain exercice, 8.4.6 Dépannage des problèmes réseau.

Exercice 8.3.7 : jeu de rôle de dépannage

Diagramme de topologie



Objectifs pédagogiques

- Construire un réseau
- Tester un réseau
- Interrompre un réseau
- Résoudre un problème
- Collecter des symptômes
- Corriger le problème
- Décrire le problème et la solution

Scénario

Au cours de cet exercice, vous et un autre participant allez construire le réseau représenté sur le diagramme de topologie. Vous allez configurer les fonctions NAT, DHCP et OSPF, puis vérifier la connectivité. Une fois le réseau totalement opérationnel, un des participants introduit plusieurs erreurs. L'autre participant fait alors appel à des compétences de dépannage pour identifier le problème et le résoudre. Dans un deuxième temps, les participants inversent leurs rôles et recommencent la procédure. Cet exercice peut être réalisé sur un équipement réel ou avec Packet Tracer.

Tâche 1 : construction du réseau

Étape 1 : câblage d'un réseau conformément au diagramme de topologie

Étape 2 : configuration des fonctions NAT, DHCP et OSPF

Tâche 2 : test du réseau

Étape 1 : contrôle de la connectivité de bout en bout

Étape 2 : vérification du bon fonctionnement de DHCP et NAT

Étape 3 : familiarisation avec chaque périphérique à l'aide des commandes show et debug

Tâche 3 : interruption du réseau

Un participant quitte la pièce, si nécessaire, pendant que l'autre participant casse la configuration. Un seul problème doit être introduit pour cela. L'idée est de s'aider mutuellement à développer des compétences de dépannage. La création de plusieurs problèmes élargit le champ du travail, ce qui n'est pas l'objectif de cet exercice de travaux pratiques. L'objectif est de vous aider à comprendre les diverses modifications apportées au réseau à cause d'un seul et unique problème.

Tâche 4 : dépannage du problème

Le participant revient et interroge l'autre participant sur les symptômes du problème. Commencez par des questions générales, puis tentez de rétrécir le champ du problème. Lorsque le participant interrogé pense avoir fourni suffisamment d'informations, interrompez le questionnement.

Tâche 5 : collecte des symptômes des équipements suspects

Commencez à rassembler des symptômes à l'aide des commandes **show** et **debug**. Utilisez la commande **show running-config** en tout dernier recours.

Tâche 6 : correction du problème

Corrigez la configuration et testez la solution.

Tâche 7 : description du problème et de la solution

Les deux participants notent le problème dans leur journal et décrivent la solution.

Tâche 8 : inversion des rôles et reprise de l'exercice

Les participants échangent maintenant leurs rôles et recommencent la procédure.

Tâche 9 : remise en état

Supprimez les configurations et rechargez les routeurs. Débranchez les câbles et stockez-les dans un endroit sécurisé. Reconnectez le câblage souhaité et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (réseau local de votre site ou Internet).

Exercice PT 8.4.6 : dépannage des problèmes de réseau

Objectifs pédagogiques

- Rassembler une documentation de réseau
- Tester la connectivité
- Recueillir des données et mettre en œuvre des solutions
- Tester la connectivité

Présentation

Au cours de cet exercice, vous allez dépanner les problèmes de connectivité entre des PC routés via ENTREPRISEXYZ. L'exercice est terminé lorsque vous atteignez 100 % et que chaque PC peut envoyer des requêtes ping aux autres PC et au serveur www.cisco.com. La solution proposée doit être conforme au diagramme de topologie.

Tâche 1 : recueil de la documentation du réseau

Pour réussir cet exercice, vous avez besoin de la documentation finale de l'exercice PT 8.1.2 : Documentation et découverte de réseau que vous avez réalisé en début de chapitre. Cette documentation doit contenir un diagramme de topologie et une table d'adressage précis. Si vous ne disposez pas de cette documentation, demandez à votre formateur des versions précises.

Tâche 2 : test de connectivité

À la fin de cet exercice, vous devez disposer d'une connectivité totale entre les PC ainsi qu'avec le serveur www.cisco.com. Pour commencer à dépanner les échecs de connectivité, envoyez les requêtes ping suivantes :

- des PC au serveur www.cisco.com ;
- de PC à PC ;
- d'un PC à la passerelle par défaut.

Est-ce qu'une requête ping a abouti ? Lesquelles ont échoué ?

_____

_____

_____

_____

_____

Tâche 3 : recueil de données et mise en œuvre de solutions

Étape 1. Choix d'un PC pour débuter le recueil des données

Choisissez un PC et commencez à recueillir des données en testant la connectivité avec la passerelle par défaut. Vous pouvez également utiliser **traceroute** pour voir l'endroit où échoue la connectivité.

Étape 2. Connexion Telnet avec la passerelle par défaut et poursuite du recueil des données

Si le PC que vous avez choisi n'a pas de connectivité avec sa passerelle par défaut, choisissez un autre PC pour appréhender le problème dans un autre sens.

Lorsque vous avez établi une connectivité à travers une passerelle par défaut, le mot de passe de connexion est **cisco**.

Étape 3. Utilisation des outils de dépannage pour vérifier la configuration

Au niveau du routeur de la passerelle par défaut, utilisez des outils de dépannage pour vérifier la configuration avec votre propre documentation. N'oubliez pas de vérifier les commutateurs en plus des routeurs. Assurez-vous de vérifier les éléments suivants :

- les informations d'adressage ;
- l'activation de l'interface ;
- l'encapsulation ;
- le routage ;
- la configuration du réseau local virtuel (VLAN) ;
- des défauts de concordance de vitesse ou du mode duplex ;
- le fonctionnement du protocole VTP.

Lorsque vous découvrez des symptômes du problème de connectivité du PC, documentez-les dans l'espace laissé libre à l'étape suivante.

Étape 4. Documentation des symptômes du réseau et solutions possibles

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Étape 5. Mise en œuvre des modifications selon vos solutions de l'étape précédente

Tâche 4 : test de connectivité

Étape 1. Test de la connectivité des PC

Tous les PC doivent être capables d'envoyer une requête ping aux autres PC et au serveur www.cisco.com. Si vous avez modifié des configurations du protocole IP, créez de nouveaux envois de requêtes ping car les envois précédents utilisent l'ancienne adresse IP.

Si des problèmes de connectivité existent toujours entre les PC ou entre un PC et le serveur, retournez à la tâche 3 afin de poursuivre le dépannage.

Étape 2. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Sinon, retournez à la tâche 3 et continuez le dépannage en appliquant les solutions que vous avez suggérées. Vous ne serez pas en mesure de cliquer sur **Check Results** et de voir les composants requis qui ne sont pas encore terminés.

Exercice PT 8.5.1 : dépannage des réseaux d'entreprise 1

Diagramme de topologie

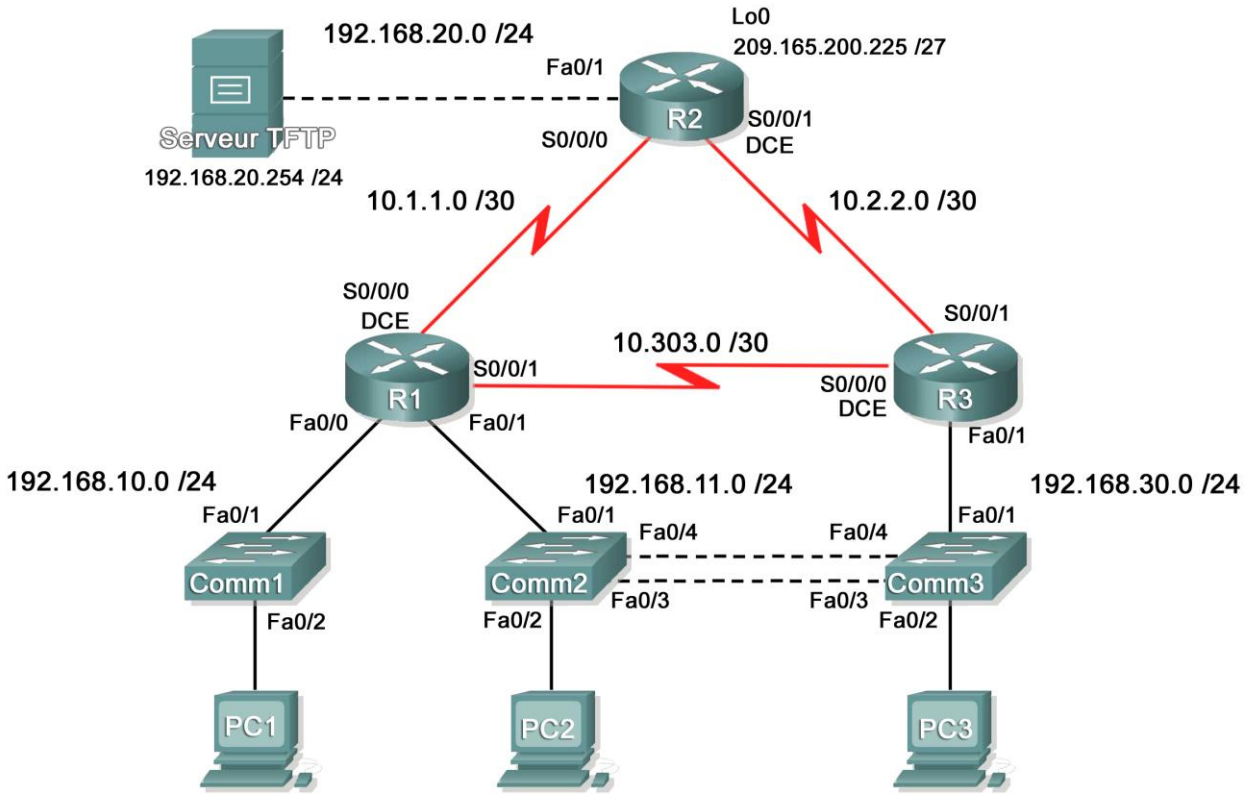


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/D
	Fa0/1	192.168.11.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
	S0/0/1	10.3.3.1	255.255.255.252	N/D
R2	**Fa0/1**	192.168.20.1	255.255.255.0	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226

Suite de la table d'adressage sur la page suivante

Table d'adressage (suite)

R3	**Fa0/1**	N/D	N/D	N/D
	Fa0/1.11	192.168.11.3	255.255.255.0	N/D
	Fa0/1.30	192.168.30.1	255.255.255.0	N/D
	S0/0/0	10.3.3.2	255.255.255.252	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
Comm1	**VLAN10**	DHCP	255.255.255.0	N/D
Comm2	**VLAN11**	192.168.11.2	255.255.255.0	N/D
Comm3	**VLAN30**	192.168.30.2	255.255.255.0	N/D
PC1	**Carte réseau**	DHCP	DHCP	DHCP
PC2	**Carte réseau**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**Carte réseau**	192.168.30.10	255.255.255.0	192.168.30.1
Serveur TFTP	**Carte réseau**	192.168.20.254	255.255.255.0	192.168.20.1

Objectifs pédagogiques

- Rechercher et corriger toutes les erreurs de réseau
- Vérifier que toutes les conditions requises sont remplies
- Documenter le réseau corrigé

Scénario

Il vous a été demandé de corriger des erreurs de configuration du réseau de l'entreprise. Pour cet exercice, n'utilisez aucune protection par mot de passe ou de connexion sur aucune ligne de console afin d'éviter un verrouillage accidentel. Pour tous les mots de passe de ce scénario, utilisez **ciscoccna**.

Remarque : il s'agit d'un exercice récapitulatif. Par conséquent, vous allez utiliser toutes vos connaissances et toutes les techniques de dépannage que vous avez acquises précédemment pour le mener à bien.

Conditions requises

- Comm2 est la racine Spanning Tree de VLAN 11, et Comm3 celle de VLAN 30.
- Comm3 est un serveur VTP avec Comm2 comme client.
- La liaison série entre R1 et R2 est le protocole Frame Relay.
- La liaison série entre R2 et R3 utilise l'encapsulation HDLC.
- La liaison série entre R1 et R3 utilise le protocole PPP.
- La liaison série entre R1 et R3 est authentifiée à l'aide de CHAP.
- R2 doit posséder des procédures de connexion sûres car il est le routeur de périphérie d'Internet.
- Toutes les lignes vty, à l'exception de celles appartenant à R2, autorisent uniquement des connexions à partir des sous-réseaux indiqués dans le diagramme de topologie, excluant l'adresse publique.
- L'usurpation de l'adresse IP d'origine doit être évitée sur toutes les liaisons qui ne se connectent pas à d'autres routeurs.
- R3 ne doit pas être en mesure d'établir une connexion Telnet avec R2 via la liaison série connectée directement.
- R3 a accès aux réseaux VLAN 11 et 30 via leur port Fast Ethernet 0/0.

- Le serveur TFTP ne doit recevoir aucun trafic dont l'adresse source est extérieure au sous-réseau. Tous les périphériques ont accès au serveur TFTP.
- Tous les périphériques sur le sous-réseau 192.168.10.0 doivent pouvoir obtenir leur adresse IP du protocole DHCP sur R1.
- Les périphériques doivent pouvoir accéder à toutes les adresses présentes dans le diagramme.

Tâche 1 : recherche et correction de toutes les erreurs de réseau

Tâche 2 : vérification du respect de toutes les conditions requises

Les contraintes de temps ne permettant pas de dépanner un problème dans chacun des sujets, seul un nombre limité de sujets présente des problèmes. Cependant, pour compléter et renforcer les connaissances en matière de dépannage, vous devez vérifier que chaque condition requise est remplie. Pour cela, présentez un exemple de chaque condition requise (par exemple, une commande **show** ou **debug**).

Tâche 3 : documentation du réseau corrigé

Exercice PT 8.5.2 : dépannage des réseaux d'entreprise 2

Diagramme de topologie

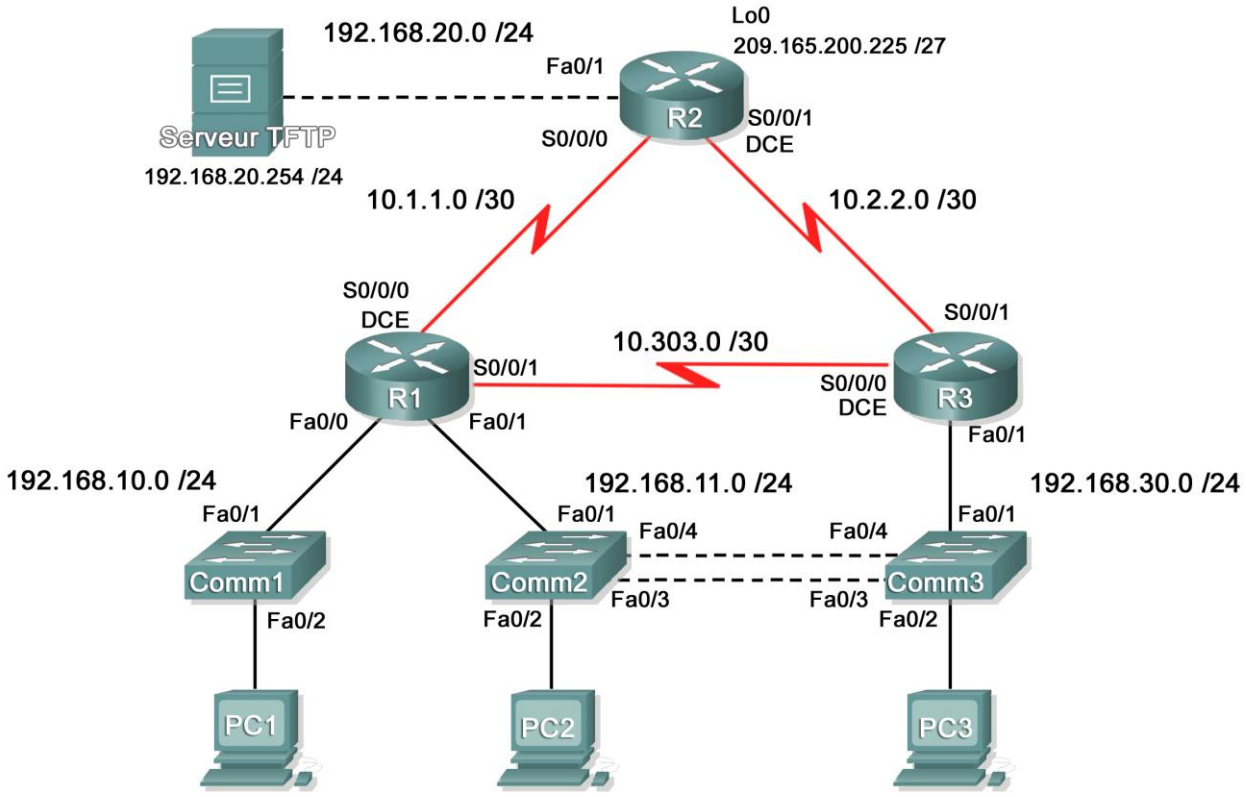


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/D
	Fa0/1	192.168.11.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
	S0/0/1	10.3.3.1	255.255.255.252	N/D
R2	**Fa0/1**	192.168.20.1	255.255.255.0	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226

Suite de la table d'adressage sur la page suivante

Table d'adressage (suite)

R3	**Fa0/1**	N/D	N/D	N/D
	Fa0/1.11	192.168.11.3	255.255.255.0	N/D
	Fa0/1.30	192.168.30.1	255.255.255.0	N/D
	S0/0/0	10.3.3.2	255.255.255.252	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
Comm1	**VLAN10**	DHCP	255.255.255.0	N/D
Comm2	**VLAN11**	192.168.11.2	255.255.255.0	N/D
Comm3	**VLAN30**	192.168.30.2	255.255.255.0	N/D
PC1	**Carte réseau**	DHCP	DHCP	DHCP
PC2	**Carte réseau**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**Carte réseau**	192.168.30.10	255.255.255.0	192.168.30.1
Serveur TFTP	**Carte réseau**	192.168.20.254	255.255.255.0	192.168.20.1

Objectifs pédagogiques

- Rechercher et corriger toutes les erreurs de réseau
- Vérifier que toutes les conditions requises sont remplies
- Documenter le réseau corrigé

Scénario

Pour cet exercice, n'utilisez aucune protection par mot de passe ou de connexion sur aucune ligne de console afin d'éviter un verrouillage accidentel. Pour tous les mots de passe de cet exercice, utilisez **ciscoccna**.

Remarque : il s'agit d'un exercice récapitulatif. Par conséquent, vous allez utiliser toutes vos connaissances et toutes les techniques de dépannage que vous avez acquises précédemment pour le mener à bien.

Conditions requises

- Comm2 est la racine Spanning Tree de VLAN 11, et Comm3 celle de VLAN 30.
- Comm3 est un serveur VTP avec Comm2 comme client.
- La liaison série entre R1 et R2 est le protocole Frame Relay.
- La liaison série entre R2 et R3 utilise l'encapsulation HDLC.
- La liaison série entre R1 et R3 est authentifiée à l'aide de CHAP.
- R2 doit posséder des procédures de connexion sûres car il est le routeur de périphérie d'Internet.
- Toutes les lignes vty, à l'exception de celles appartenant à R2, autorisent uniquement des connexions à partir des sous-réseaux indiqués dans le diagramme de topologie, excluant l'adresse publique.
- L'usurpation de l'adresse IP d'origine doit être évitée sur toutes les liaisons qui ne se connectent pas à d'autres routeurs.
- Vous devez utiliser les protocoles de routage de manière sécurisée. Ce scénario utilise le protocole EIGRP.
- R3 ne doit pas être en mesure d'établir une connexion Telnet avec R2 via la liaison série connectée directement.

- R3 a accès aux réseaux VLAN 11 et 30 via leur port Fast Ethernet 0/1.
- Le serveur TFTP ne doit recevoir aucun trafic dont l'adresse source est extérieure au sous-réseau. Tous les périphériques ont accès au serveur TFTP.
- Tous les périphériques sur le sous-réseau 192.168.10.0 doivent pouvoir obtenir leur adresse IP du protocole DHCP sur R1. Cela inclut Comm1.
- Les périphériques doivent pouvoir accéder à toutes les adresses présentes dans le diagramme.

Tâche 1 : recherche et correction de toutes les erreurs de réseau

Utilisez une fréquence d'horloge de **4 000 000** et une priorité du réseau LAN virtuel de **24 576**, le cas échéant.

Tâche 2 : vérification du respect de toutes les conditions requises

Les contraintes de temps ne permettant pas de dépanner un problème dans chacun des sujets, seul un nombre limité de sujets présente des problèmes. Cependant, pour compléter et renforcer les connaissances en matière de dépannage, vous devez vérifier que chaque condition requise est remplie. Pour cela, présentez un exemple de chaque condition requise (par exemple, une commande **show** ou **debug**).

Tâche 3 : documentation du réseau corrigé

Exercice PT 8.5.3 : dépannage des réseaux d'entreprise 3

Diagramme de topologie

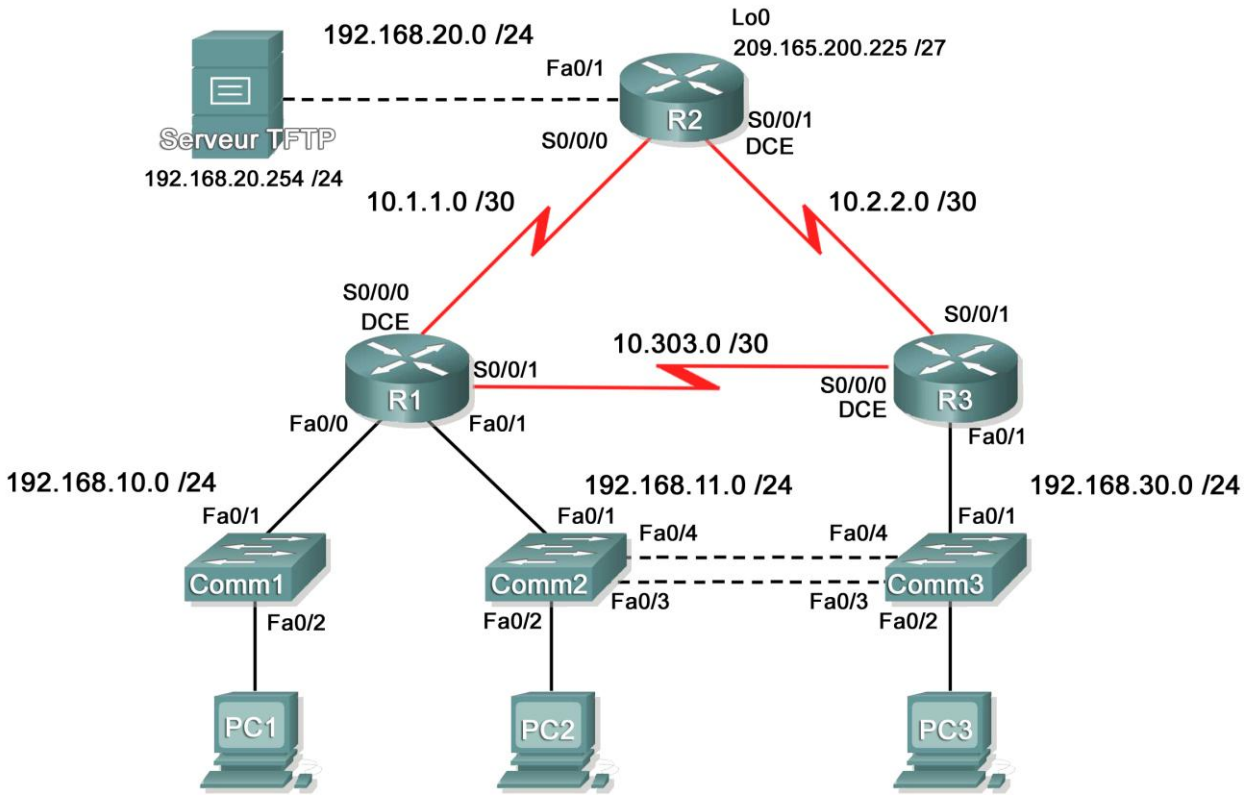


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/D
	Fa0/1	192.168.11.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
	S0/0/1	10.3.3.1	255.255.255.252	N/D
R2	**Fa0/1**	192.168.20.1	255.255.255.0	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226

Suite de la table d'adressage sur la page suivante

Table d'adressage (suite)

R3	**Fa0/1**	N/D	N/D	N/D
	Fa0/1.11	192.168.11.3	255.255.255.0	N/D
	Fa0/1.30	192.168.30.1	255.255.255.0	N/D
	S0/0/0	10.3.3.2	255.255.255.252	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
Comm1	**VLAN10**	DHCP	255.255.255.0	N/D
Comm2	**VLAN11**	192.168.11.2	255.255.255.0	N/D
Comm3	**VLAN30**	192.168.30.2	255.255.255.0	N/D
PC1	**Carte réseau**	DHCP	DHCP	DHCP
PC2	**Carte réseau**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**Carte réseau**	192.168.30.10	255.255.255.0	192.168.30.1
Serveur TFTP	**Carte réseau**	192.168.20.254	255.255.255.0	192.168.20.1

Objectifs pédagogiques

- Rechercher et corriger toutes les erreurs de réseau
- Vérifier que toutes les conditions requises sont remplies
- Documenter le réseau corrigé

Scénario

Pour cet exercice, n'utilisez aucune protection par mot de passe ou de connexion sur aucune ligne de console afin d'éviter un verrouillage accidentel. Pour tous les mots de passe de cet exercice, utilisez **ciscoccna**.

Remarque : il s'agit d'un exercice récapitulatif. Par conséquent, vous allez utiliser toutes vos connaissances et toutes les techniques de dépannage que vous avez acquises précédemment pour le mener à bien.

Conditions requises

- Comm2 est la racine Spanning Tree de VLAN 11, et Comm3 celle de VLAN 30.
- Comm3 est un serveur VTP avec Comm2 comme client.
- La liaison série entre R1 et R2 est le protocole Frame Relay.
- La liaison série entre R2 et R3 utilise l'encapsulation HDLC.
- La liaison série entre R1 et R3 est authentifiée à l'aide de CHAP.
- R2 doit posséder des procédures de connexion sûres car il est le routeur de périphérie d'Internet.
- Toutes les lignes vty, à l'exception de celles appartenant à R2, autorisent uniquement des connexions à partir des sous-réseaux indiqués dans le diagramme de topologie, excluant l'adresse publique.
- L'usurpation de l'adresse IP d'origine doit être évitée sur toutes les liaisons qui ne se connectent pas à d'autres routeurs.
- Vous devez utiliser les protocoles de routage de manière sécurisée. Ce scénario utilise le protocole OSPF.
- R3 ne doit pas être en mesure d'établir une connexion Telnet avec R2 via la liaison série connectée directement.

- R3 a accès aux réseaux VLAN 11 et 30 via leur port Fast Ethernet 0/1.
- Le serveur TFTP ne doit recevoir aucun trafic dont l'adresse source est extérieure au sous-réseau. Tous les périphériques ont accès au serveur TFTP.
- Tous les périphériques sur le sous-réseau 192.168.10.0 doivent pouvoir obtenir leur adresse IP du protocole DHCP sur R1. Cela inclut Comm1.
- Les périphériques doivent pouvoir accéder à toutes les adresses présentes dans le diagramme.

Tâche 1 : recherche et correction de toutes les erreurs de réseau

Utilisez une fréquence d'horloge de **4 000 000** et une priorité du réseau LAN virtuel de **24 576**, le cas échéant.

Tâche 2 : vérification du respect de toutes les conditions requises

Les contraintes de temps ne permettant pas de dépanner un problème dans chacun des sujets, seul un nombre limité de sujets présente des problèmes. Cependant, pour compléter et renforcer les connaissances en matière de dépannage, vous devez vérifier que chaque condition requise est remplie. Pour cela, présentez un exemple de chaque condition requise (par exemple, une commande **show** ou **debug**).

Tâche 3 : documentation du réseau corrigé

Exercice PT 8.6.1 : exercice d'intégration des compétences de CCNA

Diagramme de topologie

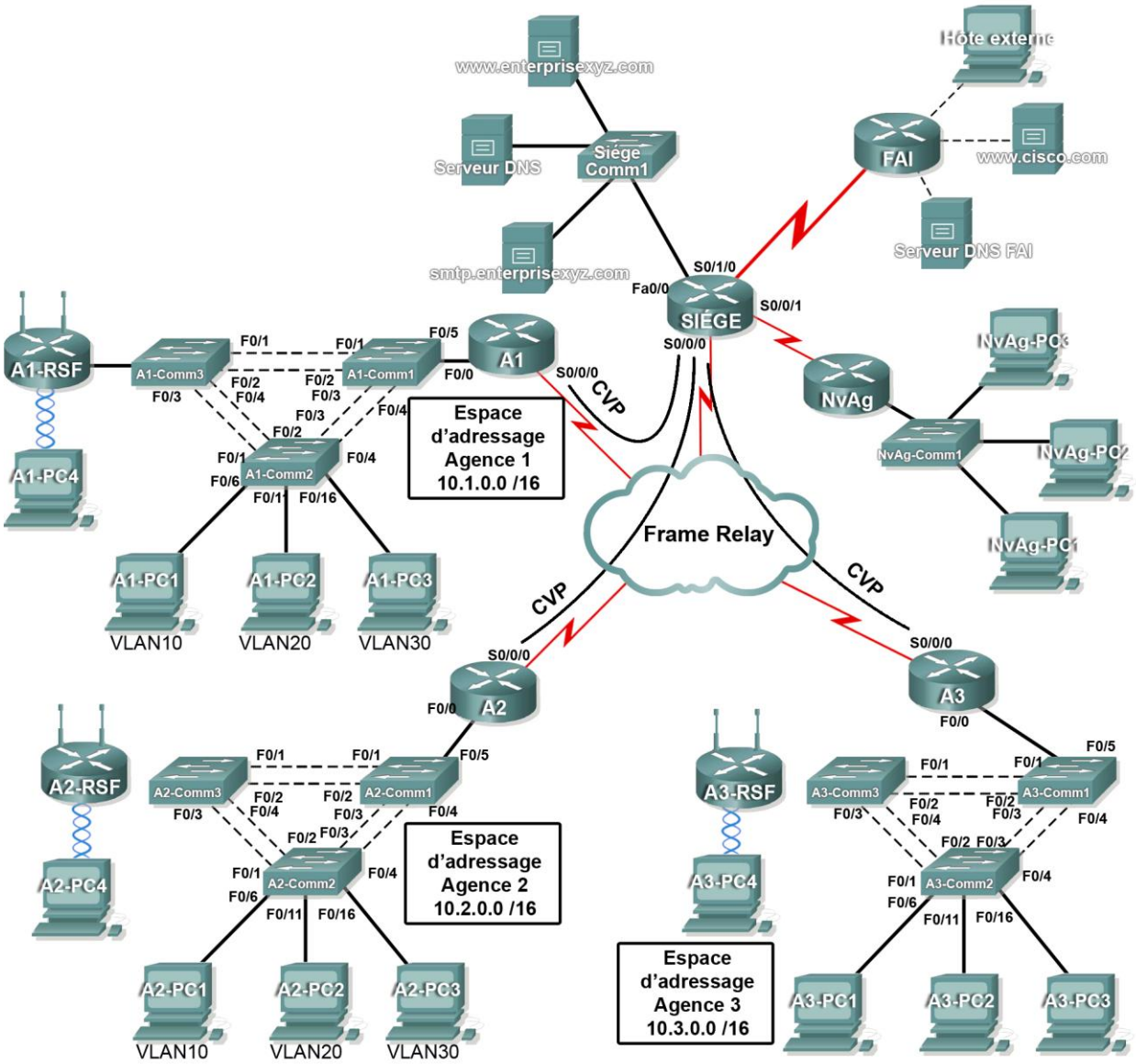


Table d'adressage de SIÈGE

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Mappages DLCI
SIÈGE	Fa0/0	10.0.1.1	255.255.255.0	N/D
	S0/0/0.41	10.255.255.1	255.255.255.252	DLCI 41 à A1
	S0/0/0.42	10.255.255.5	255.255.255.252	DLCI 42 à A2
	S0/0/0.43	10.255.255.9	255.255.255.252	DLCI 43 à A3
	S0/0/1	10.255.255.253	255.255.255.252	N/D
	S0/1/0	209.165.201.1	255.255.255.252	N/D

Table d'adressage des routeurs Agence

Périphérique	Interface	Adresse IP	Masque de sous-réseau
AX	Fa0/0.10	10.X.10.1	255.255.255.0
	Fa0/0.20	10.X.20.1	255.255.255.0
	Fa0/0.30	10.X.30.1	255.255.255.0
	Fa0/0.88	10.X.88.1	255.255.255.0
	Fa0/0.99	10.X.99.1	255.255.255.0
	S0/0/0	2^{e} adresse	255.255.255.252
AX-Comm1	VLAN 99	10.X.99.21	255.255.255.0
AX-Comm2	VLAN 99	10.X.99.22	255.255.255.0
AX-Comm3	VLAN 99	10.X.99.23	255.255.255.0
AX-RSF	VLAN 1	10.X.40.1	255.255.255.0

- Remplacez « X » par le numéro du routeur Agence (A1, A2 ou A3).
- Les circuits virtuels permanents point-à-point avec SIÈGE utilisent la seconde adresse du sous-réseau. SIÈGE utilise la première adresse.
- Les routeurs WRT300N obtiennent l'adresse Internet par le protocole DHCP auprès du routeur Agence.

Mappages de port et configuration des réseaux locaux virtuels

Numéro du VLAN	Adresse réseau	Nom du VLAN	Mappages de port
10	10.X.10.0/24	Admin	AX-Comm2, Fa0/6
20	10.X.20.0/24	Ventes	AX-Comm2, Fa0/11
30	10.X.30.0/24	Production	AX-Comm2, Fa0/16
88	10.X.88.0/24	SansFil	AX-Comm3, Fa0/7
99	10.X.99.0/24	Gestion&Natif	Toutes les agrégations

Objectifs pédagogiques

- Configurer le protocole Frame Relay dans une topologie en étoile « hub-and-spoke »
- Configurer le protocole PPP avec authentification PAP et CHAP
- Configurer la fonction NAT statique et dynamique
- Configurer le routage par défaut et statique

Présentation

Au cours de cet exercice faisant appel à vos compétences CCNA, la société XYZ utilise une combinaison des protocoles Frame Relay et PPP pour les connexions du réseau étendu. Le routeur SIÈGE fournit un accès à la ferme de serveurs et à Internet via la fonction NAT. SIÈGE utilise également une liste de contrôle d'accès pare-feu de base pour filtrer le trafic entrant. Chaque routeur Agence est configuré pour un routage entre réseaux locaux virtuels et pour le protocole DHCP. Le routage est possible par l'intermédiaire d'EIGRP et de routes par défaut et statiques. Les réseaux locaux virtuels, le protocole VTP et le STP sont configurés sur chacun des réseaux commutés. La sécurité de port est activée et un accès sans fil est fourni. Votre tâche consiste à mettre correctement en œuvre toutes ces technologies, en faisant appel à toutes les connaissances que vous avez acquises lors des quatre cours d'Exploration, résumées dans cet exercice.

Vous êtes responsable de la configuration du routeur SIÈGE et des routeurs A1, A2 et A3. Vous devez également configurer chaque périphérique qui est relié au réseau par un routeur Agence. Le routeur NvAg représente une nouvelle agence acquise après fusion avec une entreprise de plus petite taille. Vous n'avez pas accès au routeur NvAg. Vous allez cependant établir une liaison entre SIÈGE et NvAg pour fournir à cette nouvelle agence un accès au réseau interne et à Internet.

Les routeurs et les commutateurs sous votre administration ne sont pas configurés. Aucune des configurations de base, telles que nom d'hôte, mots de passe, bannières et autres commandes générales de maintenance, n'est évaluée par Packet Tracer. Elles n'entreront donc pas dans les spécifications des tâches. Cependant, vous êtes censé les configurer, et votre formateur peut décider de les noter.

Étant donné que cet exercice fait appel à un réseau très vaste avec près de 500 composants requis pour les éléments d'évaluation, vous ne verrez pas nécessairement votre taux de réalisation augmenter à chaque fois que vous saisirez une commande. D'autre part, il ne vous sera pas demandé d'atteindre un pourcentage précis à la fin de chaque tâche. En revanche, des tests de connectivité vous permettront de vérifier la configuration de chaque tâche. Il vous est cependant possible de cliquer à tout moment sur **Check Results** pour voir si un composant particulier est noté et si vous l'avez configuré correctement.

Puisque les routeurs Agence (A1, A2 et A3) et les commutateurs sont conçus de manière modulaire, vous pouvez réutiliser des scripts. Par exemple, vos configurations pour A1, A1-Comm1, A1-Comm2 et A1-Comm3 peuvent être directement appliquées aux périphériques A2 en n'apportant que quelques ajustements.

Remarque : cette vérification d'intégration des compétences CCNA est également disponible dans une version ouverte où vous pouvez choisir le schéma d'adressage et les technologies à mettre en œuvre. Vérifiez votre configuration en testant la connectivité de bout en bout.

Tâche 1 : configuration du protocole Frame Relay dans une topologie en étoile « hub-and-spoke »

Étape 1. Configuration du cœur de Frame Relay

Utilisez les tables d'adressage et les conditions requises ci-dessous.

SIÈGE est le routeur moyeu (hub). A1, A2 et A3 sont les rayons (spokes).

- SIÈGE utilise une sous-interface point-à-point pour chacun des routeurs Agence.
- A3 doit être configuré manuellement pour utiliser une encapsulation IETF.
- Le type LMI doit être configuré manuellement comme étant q933 pour SIÈGE, A1 et A2. A3 utilise ANSI.

Étape 2. Configuration de l'interface du réseau local sur SIÈGE

Étape 3. Vérification de la capacité d'envoi de requêtes ping de SIÈGE aux routeurs Agence

Tâche 2 : configuration du protocole PPP avec authentification PAP et CHAP

Étape 1. Configuration de la liaison WAN de SIÈGE vers FAI à l'aide de l'encapsulation PPP et de l'authentification CHAP

Le mot de passe CHAP est **ciscochap**.

Étape 2. Configuration de la liaison WAN de SIÈGE vers NvAg à l'aide de l'encapsulation PPP et de l'authentification PAP

Vous devez brancher un câble aux interfaces appropriées. SIÈGE est le côté DCE de la liaison. Vous choisissez la fréquence d'horloge. Le mot de passe PAP est **ciscopap**.

Étape 3. Vérification de la capacité d'envoi de requêtes ping de SIÈGE à FAI et à NvAg

Tâche 3 : configuration de la fonction NAT statique et dynamique sur SIÈGE

Étape 1. Configuration de la fonction NAT

Utilisez les conditions requises suivantes :

- Autorisez la traduction de toutes les adresses de l'espace d'adressage 10.0.0.0/8.
- La société XYZ possède l'espace d'adressage 209.165.200.240/29. Le pool, XYZCORP, utilise les adresses .241 à .245 avec un masque /29.
- Le site Web www.entreprisexyz.com sur 10.0.1.2 est enregistré avec le système DNS public à l'adresse IP 209.165.200.246.

Étape 2. Vérification du fonctionnement de NAT par une requête ping étendue

À partir de SIÈGE, envoyez une requête ping à l'interface série 0/0/0 sur FAI en utilisant l'interface du réseau local de SIÈGE comme adresse source. Cette requête ping doit aboutir.

Vérifiez que la fonction NAT a traduit la requête ping avec la commande **show ip nat translations**.

Tâche 4 : configuration du routage par défaut et statique

Étape 1. Configuration de SIÈGE avec une route par défaut vers FAI et une route statique vers le réseau local de NvAg

Utilisez l'argument d'interface de sortie (exit interface).

Étape 2. Configuration des routeurs Agence avec une route par défaut vers SIÈGE

Utilisez l'argument d'adresse IP de saut suivant (next-hop IP address).

Étape 3. Vérification de la connectivité au-delà de FAI

Les trois PC de NvAg et le PC NetAdmin doivent être capables d'envoyer une requête ping au serveur Web www.cisco.com.

Tâche 5 : configuration du routage entre réseaux locaux virtuels

Étape 1. Configuration de chaque routeur Agence pour le routage entre réseaux locaux virtuels

À l'aide de la table d'adressage pour les routeurs Agence, configurez et activez l'interface du réseau local pour le routage entre réseaux locaux virtuels. VLAN 99 est le réseau local virtuel natif.

Étape 2. Vérification des tables de routage

Chacun des routeurs Agence doit maintenant posséder six réseaux connectés directement et une route par défaut statique.

Tâche 6 : configuration et optimisation du routage EIGRP

Étape 1. Configuration de SIÈGE, A1, A2 et A3 avec EIGRP

- Utilisez AS 100.
- Désactivez les mises à jour EIGRP sur les interfaces adéquates.
- Résumez manuellement les routes EIGRP de telle sorte que chacun des routeurs Agence annonce uniquement l'espace d'adressage 10.X.0.0/16 à SIÈGE.

Remarque : Packet Tracer ne simule pas précisément l'avantage des routes résumées EIGRP. Les tables de routage indiquent encore tous les sous-réseaux, bien que vous ayez correctement configuré le résumé manuel.

Étape 2. Vérification des tables de routage et de la connectivité

SIÈGE et les routeurs Agence doivent maintenant posséder des tables de routage complètes.

Le PC NetAdmin doit maintenant pouvoir envoyer une requête ping à chaque sous-interface du réseau local virtuel sur chaque routeur Agence.

Tâche 7 : configuration de VTP, de l'agrégation, de l'interface des VLAN et des VLAN

Les conditions requises suivantes s'appliquent aux trois agences. Configurez un ensemble de trois commutateurs. Utilisez ensuite les scripts de ces commutateurs sur les deux autres ensembles de commutateurs.

Étape 1. Configuration des commutateurs Agence avec le protocole VTP

- AX-Comm1 est le serveur VTP. AX-Comm2 et AX-Comm3 sont des clients VTP.
- Le nom de domaine est **XYZCORP**.
- Le mot de passe est **xyzvtp**.

Étape 2. Configuration de l'agrégation sur AX-Comm1, AX-Comm2 et AX-Comm3

Configurez les interfaces appropriées en mode d'agrégation et affectez VLAN 99 comme le réseau local virtuel natif.

Étape 3. Configuration de l'interface de réseau local virtuel et de la passerelle par défaut sur AX-Comm1, AX-Comm2 et AX-Comm3

Étape 4. Création des réseaux locaux virtuels sur AX-Comm1

Créez et nommez les réseaux locaux virtuels répertoriés dans le tableau des mappages de port et de configuration des réseaux locaux virtuels uniquement sur AX-Comm1. Le protocole VTP annonce les nouveaux réseaux locaux virtuels à AX-Comm1 et AX-Comm2.

Étape 5. Vérification de l'envoi des réseaux locaux virtuels à AX-Comm2 et AX-Comm3

Utilisez les commandes adéquates pour vérifier que Comm2 et Comm3 possèdent désormais les réseaux locaux virtuels que vous avez créés sur Comm1. Packet Tracer peut avoir besoin de quelques minutes pour simuler les annonces VTP. Une façon rapide de forcer l'envoi d'annonces VTP consiste à faire passer l'un des commutateurs du client en mode transparent puis de le faire repasser en mode client.

Tâche 8 : affectation des réseaux locaux virtuels et configuration de la sécurité de port

Étape 1. Affectation des réseaux locaux virtuels aux ports d'accès

Utilisez le tableau des mappages de port et de configuration des réseaux locaux virtuels pour remplir les conditions requises suivantes :

- Configurez les ports d'accès.
- Affectez les réseaux locaux virtuels aux ports d'accès.

Étape 2. Configuration de la sécurité des ports

Utilisez la stratégie suivante pour établir la sécurité des ports sur les ports d'accès de AX-Comm2 :

- Autorisez une seule adresse MAC.
- Configurez la première adresse MAC apprise pour correspondre à la configuration.
- Configurez le port pour qu'il se désactive en cas de violation de la sécurité.

Étape 3. Vérification des affectations des réseaux locaux virtuels et de la sécurité de port

Utilisez les commandes appropriées pour vérifier que les réseaux locaux virtuels d'accès sont correctement affectés et que la stratégie de sécurité de port a été activée.

Tâche 9 : configuration du protocole STP

Étape 1. Configuration de AX-Comm1 comme pont racine

Paramétrez le niveau de priorité à 4096 sur AX-Comm1 afin que ces commutateurs soient toujours le pont racine de tous les réseaux locaux virtuels.

Étape 2. Configuration de AX-Comm3 comme pont racine de secours

Paramétrez le niveau de priorité à 8192 sur AX-Comm3 afin que ces commutateurs soient toujours le pont racine de secours de tous les réseaux locaux virtuels.

Étape 3. Vérification que AX-Comm1 est le pont racine

Tâche 10 : configuration du protocole DHCP

Étape 1. Configuration des pools DHCP pour chaque réseau local virtuel

Sur les routeurs Agence, configurez les pools DHCP pour chaque réseau local virtuel en fonction des conditions requises suivantes :

- Excluez les 10 premières adresses IP de chaque pool pour les réseaux locaux virtuels.
- Excluez les 24 premières adresses IP de chaque pool pour les réseaux locaux sans fil.
- Le nom de pool est **AX_VLAN##** où **X** est le numéro du routeur et ## est le numéro du réseau local virtuel.
- Incluez dans la configuration DHCP le serveur DNS relié à la ferme de serveurs de SIÈGE.

Étape 2. Configuration des PC pour utiliser DHCP

Actuellement, les PC sont configurés pour utiliser des adresses IP statiques. Modifiez cette configuration en DHCP.

Étape 3. Vérification de l'existence d'adresse IP pour les PC et les routeurs sans fil

Étape 4. Vérification de la connectivité

Tous les PC physiquement reliés au réseau doivent être capables d'envoyer une requête ping au serveur Web www.cisco.com.

Tâche 11 : configuration d'une liste de contrôle d'accès pare-feu

Étape 1. Vérification de la connectivité à partir de l'hôte externe

Le PC Hôte externe doit être capable d'envoyer une requête ping au serveur sur www.entreprisexyz.com.

Étape 2. Application d'une liste de contrôle d'accès pare-feu de base

FAI représentant la connectivité à Internet, configurez une liste de contrôle d'accès nommée appelée **FIREWALL** dans l'ordre suivant :

1. Autorisez les requêtes HTTP entrantes vers le serveur www.entreprisexyz.com.
2. Autorisez uniquement les sessions TCP établies à partir de FAI et de toute source au-delà de FAI.
3. Autorisez uniquement les réponses ping entrantes en provenance de FAI et de toute source au-delà de FAI.
4. Bloquez explicitement tout autre accès entrant à partir de FAI et de toute source au-delà de FAI.

Étape 3. Vérification de la connectivité à partir de l'hôte externe

Le PC Hôte externe ne doit pas être en mesure d'envoyer une requête ping au serveur sur www.xyzcorp. Toutefois, le PC Hôte externe doit pouvoir demander une page Web.

Tâche 12 : configuration de la connectivité sans fil

Étape 1. Vérification de la configuration de DHCP

Chaque routeur AX-RSF doit déjà posséder un adressage IP du protocole DHCP du routeur AX pour VLAN 88.

Étape 2. Configuration des paramètres de configuration réseau/réseau local

L'adresse « Router IP » (IP du routeur) à la page **Status** de l'onglet GUI doit être la première adresse IP du sous-réseau 10.X.40.0 /24. Conservez la valeur par défaut de tous les autres paramètres.

Étape 3. Configuration des paramètres du réseau sans fil

Les SSID des routeurs sont **AX-RSF_LAN** où **X** est le numéro du routeur Agence.

La clé WEP est **12345ABCDE**.

Étape 4. Configuration des routeurs sans fil pour un accès à distance

Configurez le mot de passe d'administration sur **cisco123** et activez la gestion à distance.

Étape 5. Configuration des PC de AX-PC4 pour l'accès au réseau sans fil avec DHCP

Étape 6. Vérification de la connectivité et de la capacité de gestion à distance

Chaque PC sans fil doit pouvoir accéder au serveur Web www.cisco.com.

Pour vérifier la capacité de gestion à distance, accédez au routeur sans fil via le navigateur Web.

Tâche 13 : dépannage du réseau

Étape 1. Coupure du réseau

Un participant quitte la salle, si nécessaire, pendant qu'un autre casse la configuration.

Étape 2. Détection du problème

Le participant revient et utilise les techniques de dépannage pour identifier le problème et le résoudre.

Étape 3. Nouvelle coupure du réseau

Les participants échangent les rôles et recommencent les étapes 1 et 2.