Version expérimentale
En cours de validation

TRAVAUX PRATIQUES – FILIÈRE SYSTÈMES ET RÉSEAUX

M201 – METTRE EN PLACE UNE INFRASTRUCTURE RÉSEAUX

72 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

CONSIGNES

1. Pour le formateur :

- Laisser à l'apprenant l'occasion de comprendre seul l'énoncé.
- S'assurer de la bonne compréhension du contexte avant de lui laisser le temps de réfléchir et répondre.
- Discuter les réponses des apprenants avant de donner la solution.

2. Pour l'apprenant :

- Lire et bien comprendre la question.
- Essayer de trouver par vous-même une réponse à cette question et la noter.
- Parcourir les réponses proposées.
- Pour chaque réponse : comparez-la à votre réponse et cochez-la si elle lui correspond ou bien est compatible.

3. Conditions de réalisation :

- Individuel ou par groupes (2 ou 3 maximum).
- Support de résumé théorique accompagnant.
- Stylo et feuille de papier.
- Ordinateur avec Packet Tracer installé
- Périphériques réseaux

PARTIE 1

Maîtriser les Concepts de commutation

Dans ce module, vous allez :

- Être en mesure de configurer les fonctionnalités avancées des routeurs et des commutateurs

12 heures

TP 1

Configurer les périphériques réseaux

Compétences visées :

- Configurer les périphériques réseaux

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

5 heures

TP 1

Configurer les périphériques réseaux

1. Configuration d’un commutateur
2. Configuration des paramètres de base d'un routeur

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer les périphériques réseaux?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

- **Objectifs**

- **Partie 1: Câbler le réseau et vérifier la configuration par défaut du commutateur**
- **Partie 2: Configurer les paramètres de base des périphériques réseau**
  - Configurez les paramètres de base du commutateur.
  - Configurez l'adresse IP du PC.
- **Partie 3: Vérifier et tester la connectivité réseau**
  - Affichez la configuration du périphérique.
  - Testez la connectivité de bout en bout avec ping.
  - Testez les fonctionnalités de gestion à distance avec Telnet.
- **Partie 4: Gérer la table d'adresses MAC**
  - Notez l'adresse MAC de l'hôte.
  - Déterminez les adresses MAC que le commutateur a apprises.
  - Répertoriez les options de la commande show mac address-table.
  - Définir une adresse MAC statique.

- **Contexte/scénario**

- Les commutateurs Cisco peuvent être configurés avec une adresse IP spéciale appelée interface virtuelle de commutateur (SVI). Le SVI, ou l'adresse de gestion, peut être utilisé pour un accès à distance au commutateur afin d'afficher ou de configurer des paramètres. Si le SVI du VLAN 1 est attribué à une adresse IP, tous les ports dans le VLAN 1 disposent d'un accès par défaut à l'adresse IP du SVI.

- Au cours de ces travaux pratiques, vous allez créer une topologie simple utilisant du câblage LAN Ethernet et accéder à un commutateur Cisco à l'aide de la console et de méthodes d'accès à distance. Vous allez examiner les configurations par défaut du commutateur avant de configurer les paramètres de base de celui-ci. Ces paramètres de base du commutateur comprennent le nom du périphérique, la description de l'interface, les mots de passe locaux, la bannière du message du jour (MOTD), l'adressage IP et l'adresse MAC statique. Vous pourrez également démontrer l'utilisation d'une adresse IP de gestion aux fins de gestion à distance du commutateur. La topologie se compose d'un commutateur et d'un hôte utilisant uniquement des ports Ethernet et de console.

- **Remarque:** Les commutateurs utilisés sont des modèles Cisco Catalyst 2960 équipés de Cisco IOS version 15.2(2) (image lanbasek9). D'autres commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent différer de ceux indiqués dans les travaux pratiques.

- **Remarque:** Assurez-vous que les commutateurs ont été réinitialisés et qu'ils ne présentent aucune configuration initiale. En cas de doute, contactez votre instructeur. Reportez-vous à l'Annexe A pour les procédures à suivre pour initialiser et recharger un commutateur.

- Le modèle **default bias**, utilisé par le gestionnaire de base de données de commutation (SDM), n'offre pas de fonctionnalités d'adresse IPv6. Vérifiez que SDM utilise le modèle **dual-ipv4-and-ipv6** ou **lanbase-routing**. Le nouveau modèle sera utilisé après redémarrage même si la configuration n'est pas enregistrée.
  - S1# **show sdm prefer**

Activité 1 : Configuration de base du commutateur – Lab

- Utilisez les commandes suivantes pour affecter le modèle **dual-ipv4-and-ipv6** comme modèle par défaut SDM.
  - S1# **configure terminal**
  - S1(config)# **sdm prefer dual-ipv4-and-ipv6 default**
  - S1(config)# **end**
  - S1# **reload**

Ressources requises

- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
- 1 ordinateur (Windows équipés d'un programme d'émulation de terminal tel que Tera Term)
- 1 câble console pour configurer le périphérique Cisco IOS via le port console
- 1 câble Ethernet, comme illustré dans la topologie

Topologie

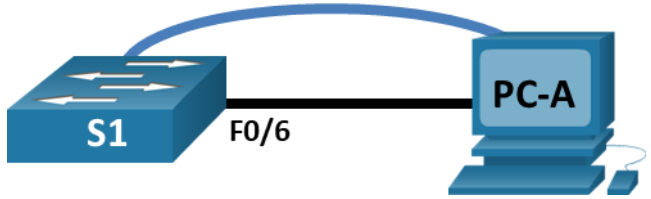


Table d'adressage

Appareil	Interface	Adresse IP / Préfixe
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad:1::2 /64
		fe80::2
PC-A	Carte réseau (NIC)	192.168.1.10 /24
		2001:db8:acad:1::10 /64

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

Partie 1: Câbler le réseau et vérifier la configuration par défaut du commutateur

Dans la Partie 1, vous allez configurer la topologie du réseau et vérifier les paramètres par défaut du commutateur.

Etape 1: Câblez le réseau conformément à la topologie indiquée

a. Connectez le câble de la console comme illustré dans la topologie. Ne connectez pas le câble Ethernet de PC-A à ce stade.

Remarque: Si vous utilisez Netlab, arrêtez l'interface F0/6 sur S1. Cela a le même effet que la non-connexion de PC-A à S1.

b. Connectez le commutateur à partir de PC-A en utilisant Tera Term ou un autre programme d'émulation du terminal.

Question:

- Pourquoi utiliser une connexion console pour la configuration initiale du commutateur? Pourquoi n'est-il pas possible de se connecter au commutateur par l'intermédiaire de Telnet ou de SSH?

Etape 2: Vérifiez la configuration par défaut du commutateur.

- Au cours de cette étape, vous allez examiner les paramètres par défaut du commutateur, tels que la configuration actuelle du commutateur, les informations IOS, les propriétés d'interface, les informations VLAN et la mémoire Flash.

- Au cours de ces travaux pratiques, vous allez créer une topologie simple Vous pouvez accéder à l'ensemble des commandes IOS du commutateur en mode d'exécution privilégié. L'accès au mode d'exécution privilégié doit être limité à l'aide de la protection par mot de passe afin d'empêcher toute utilisation non autorisée, car il offre un accès direct au mode de configuration globale ainsi qu'aux commandes utilisées pour configurer les paramètres d'exploitation. Vous définirez les mots de passe ultérieurement au cours de ces travaux pratiques.

- Parmi les commandes du mode d'exécution privilégié, on trouve celles du mode d'exécution utilisateur, ainsi que la commande **configure** qui donne accès aux autres modes de commande. Utilisez la commande **enable** pour passer en mode d'exécution privilégié.

a. En supposant que le commutateur ne possède pas de fichier de configuration stocké dans la mémoire vive non volatile (NVRAM), une connexion de console utilisant Tera Term ou un autre programme d'émulation de terminal vous mettra en mode d'exécution utilisateur sur le commutateur, avec une invite de Switch>. Utilisez la commande **enable** pour passer en mode d'exécution privilégié.

Ouvrez la fenêtre de configuration.

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

Vérifiez qu'il existe un fichier de configuration par défaut vierge sur le commutateur en exécutant la commande **show running-config** en mode d'exécution privilégié . Si un fichier de configuration a été précédemment enregistré, il doit être supprimé. Selon le modèle de commutateur et la version de l'IOS , votre configuration peut varier légèrement. Toutefois, elle ne doit pas comporter de mots de passe ni d'adresse IP configurés. Si votre commutateur ne possède pas de configuration par défaut, effacez et redémarrez-le.

Activité 1 : Configuration de base du commutateur – Lab

Remarque: L'Annexe A décrit les étapes à suivre pour initialiser et recharger un commutateur.

b. Examinez le fichier de configuration en cours d'exécution.

Questions:

- Combien d'interfaces FastEthernet un commutateur 2960 dispose-t-il?
- Combien d'interfaces Gigabit Ethernet un commutateur 2960 dispose-t-il?
- Quelle est la plage de valeurs affichée pour les lignes vty?

c. Examinez le fichier de configuration initiale dans la mémoire vive non volatile.

Question:

- Pourquoi ce message apparaît-il?

d. Examinez les caractéristiques de l'interface SVI du VLAN 1.

Questions:

- Est-ce qu'une adresse IP est attribuée au VLAN 1?
- Quelle est l'adresse MAC de cette interface SVI? Plusieurs réponses sont possibles.
- Cette interface est-elle opérationnelle ?

e. Examinez les propriétés IP de l'interface SVI du VLAN 1.

Question:

- Quel résultat voyez-vous?

f. Connectez un câble Ethernet entre le PC-A et le port 6 sur le commutateur, et examinez les propriétés IP du VLAN 1 de l'interface SVI. Attendez que le commutateur et le PC négocient les paramètres du mode bidirectionnel et de la vitesse.

Remarque: si vous utilisez Netlab, activez l'interface F0/6 sur S1.

Question:

- Quel résultat voyez-vous?

g. Examinez les informations relatives à la version de Cisco IOS du commutateur.

Questions:

- Quelle version de Cisco IOS le commutateur exécute-t-il?
- Quel est le nom de fichier de l'image système?
- Quelle est l'adresse MAC de base de ce commutateur?

h. Examinez les propriétés par défaut de l'interface FastEthernet utilisée par PC-A.

- Switch# **show interface f0/6**

Question:

- L'interface est-elle activée ou désactivée?
- Quel événement pourrait activer une interface?
- Quelle est l'adresse MAC de l'interface?
- Quels sont les paramètres de vitesse et de mode duplex de l'interface?

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

i. Examinez les paramètres VLAN par défaut du commutateur.

Question:

- Quel est le nom par défaut du VLAN 1?
- Quels sont les ports du VLAN 1 ?
- Le VLAN 1 est-il actif?
- Quel est le type de VLAN par défaut?

j. Observer la mémoire flash

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

- Switch# **show flash**
- Switch# **dir flash:**

Les fichiers ont une extension, telle que .bin, à la fin du nom de fichier. Les répertoires n'ont pas d'extension.

Question:

- Quel est le nom de fichier de l'image Cisco IOS?

Partie 2 : Configurer les paramètres de base des périphériques réseau

Dans la partie 2, vous configurerez les paramètres de base pour le commutateur et le PC.

Etape 1 : Configurez les paramètres de base du commutateur

a. Copiez la configuration de base suivante et copiez-la dans S1 en mode de configuration globale.

- ***no ip domain-lookup***
- ***hostname S1***
- ***service password-encryption***
- ***enable secret class***
- ***banner motd #*** *Unauthorized access is strictly prohibited.* ***#***

b. Définissez l'adresse IP de l'interface SVI du commutateur. Cette opération permet la gestion à distance du commutateur.

Avant de pouvoir gérer **S1** à distance à partir de **PC-A**, vous devez attribuer une adresse IP au commutateur. La configuration par défaut du commutateur consiste à s'assurer la gestion de commutateur par le biais du VLAN 1. Pour la configuration de base du commutateur, il est recommandé de modifier le VLAN de gestion à un autre VLAN que VLAN 1.

À des fins de gestion, utilisez VLAN 99. La sélection du VLAN 99 est arbitraire et n'implique nullement que vous deviez toujours utiliser ce VLAN particulier.

Commencez par créer le nouveau VLAN 99 sur le commutateur. Définissez ensuite l'adresse IP du commutateur à 192.168.1.2 et masque de sous-réseau 255.255.255.0 sur le VLAN 99 de l'interface virtuelle interne. Une adresse IPv6 peut également être configurée sur l'interface SVI. Utilisez les adresses IPv6 indiquées dans la **Table d'Adressage**.

Notez que l'interface VLAN 99 est désactivée, même après l'exécution de la commande ***no shutdown*** *. L'interface est actuellement désactivée, car aucun port de commutateur n'est attribué au VLAN 99.*

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

c. Attribuez tous les ports utilisateur au VLAN 99.

Pour établir la connectivité entre l'hôte et le commutateur, les ports utilisés par l'hôte doivent se trouver dans le même VLAN que le commutateur. Au bout de quelques secondes, le VLAN 99 apparaît, car au moins un port actif (F0/6 avec **PC-A** relié) est maintenant attribué au VLAN 99.

d. Exécutez la **commande show vlan brief** pour vérifier que tous les ports sont attribués au VLAN 99.

e. Configurez la passerelle par défaut pour **S1**. Si aucune passerelle par défaut n'est définie, le commutateur ne peut pas être géré à partir d'un réseau distant qui se trouve à plus d'un routeur de distance. Bien que cet exercice n'inclue pas de passerelle IP externe, considérez que vous connecterez le réseau local à un routeur pour un accès externe. En supposant que l'interface du réseau local soit 192.168.1.1 sur le routeur, définissez la passerelle par défaut pour le commutateur.

e. L'accès au port de console doit être également limité avec un mot de passe. Utilisez **cisco** comme mot de passe de connexion de la console dans cette activité. La configuration par défaut permet toutes les connexions console sans mot de passe requis. Afin d'empêcher les messages de console d'interrompre les commandes, utilisez l'option **logging synchronous**.

- S1(config)# **line con 0**
- S1(config-line)# **logging synchronous**

f. Configurez les lignes de terminal virtuel (vty) de telle sorte que le commutateur autorise l'accès à Telnet. Si vous ne configurez pas de mot de passe vty, vous ne pourrez pas établir de connexion Telnet pour accéder le commutateur.

Question:

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

Etape 2: Configurez une adresse IP sur PC-A

Attribuez l'adresse IP et le masque de sous-réseau au PC, comme indiqué dans la **Table d'Adressage**. Une version abrégée de la procédure est décrite ici. Aucune passerelle par défaut n'est requise pour cette topologie; toutefois, vous pouvez entrer **192.168.1.1** et **fe80::1** afin de simuler un routeur relié à **S1**.

1. Accédez au **Control Panel**(Panneau de configuration).
2. Dans l'affichage Catégorie, sélectionnez **View network status and tasks**(Afficher l'état du réseau et les tâches).
3. Cliquez sur **Change adapter settings** (Modifier les paramètres de la carte) dans le volet de gauche.
4. Cliquez avec le bouton droit sur une interface **Ethernet** , puis choisissez **Properties**(Propriétés).
5. Choisissez **Protocole Internet version 4 (TCP/IPv4)** et cliquez sur **Properties**.
6. Cliquez sur la case d'option **Use the following IP address** (Utiliser l'adresse IP suivante) et entrez l'adresse IP ainsi que le masque de sous-réseau et cliquez sur **OK**.
7. Sélectionnez **Protocole Internet version 6 (TCP/IPv6)** et cliquez sur **Properties**.
8. Cliquez sur la case d'option **Use the following IP address** (Utiliser l'adresse IP suivante) et entrez l'adresse IP et ainsi que le préfixe et cliquez sur **OK** pour continuer.
9. Cliquez sur **OK** pour quitter la fenêtre Properties.

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

○ Partie 3 : Vérifier et tester la connectivité réseau

Dans la Partie 3, vous allez vérifier et documenter la configuration du commutateur, tester la connectivité de bout en bout entre **PC-A** et **S1**, et tester la fonctionnalité de gestion à distance du commutateur.

Etape 1: Affichez la configuration du commutateur

Utilisez la connexion de console sur **PC-A** pour afficher et vérifier la configuration du commutateur. La commande **show run** affiche la totalité de la configuration en cours, une page à la fois. Utilisez la barre d'espace pour passer d'une page à l'autre.

a. Un exemple de configuration est présenté ici. Les paramètres que vous avez configurés sont représentés en jaune. Les autres paramètres de configuration sont les paramètres par défaut d'IOS.

- S1# **show run**

```
Building configuration...
Current configuration : 2206 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$mtvC$6NC.1VKr3p6bj7YGE.jNg0
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<output omitted>
!
interface FastEthernet0/24
 switchport access vlan 99
!
interface GigabitEthernet0/1
 switchport access vlan 99
!
interface GigabitEthernet0/2
 switchport access vlan 99
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD::2/64
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password 7 00071A150754
 logging synchronous
 login
line vty 0 4
 password 7 121A0C041104
 login
line vty 5 15
 password 7 121A0C041104
 login
!
end
```

b. Vérifiez les paramètres du VLAN 99 de gestion.

- S1# **show interface vlan 99**

Question:

- Quelle est la bande passante définie sur cette
- Quel est l'état du VLAN
- Quel est l'état du protocole de ligne?

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

- **Partie 3 : Vérifier et tester la connectivité réseau**

Etape 2: Testez la connectivité de bout en bout avec ping

Vérifiez que PC-A peut envoyer une requête ping à l'adresses IPv4 et IPv6 de S1.

C:\> **ping 192.168.1.2**

C : \ > **ping 2001:db8:acad:1:: 2**

Étant donné que **PC-A** doit résoudre l'adresse MAC de **S1** par l'intermédiaire du protocole ARP, il se peut que le premier paquet arrive à expiration. Si les résultats des requêtes ping continuent à échouer, dépannez les configurations de base des périphériques. Vérifiez à la fois le câblage physique et l'adressage logique.

Etape 3: Testez et vérifiez la gestion à distance de S1

Vous allez maintenant utiliser Telnet pour accéder à distance au commutateur. Au cours de cette activité, **PC-A** et **S1** sont situés côte à côte. Dans un réseau de production, il se peut que le commutateur soit placé dans une armoire de répartition située au dernier étage du bâtiment tandis que votre PC de gestion se trouve au rez-de-chaussée. Au cours de cette étape, vous allez utiliser Telnet pour accéder à distance au commutateur **S1** en utilisant l'adresse de gestion de son interface SVI. Telnet n'est pas un protocole sécurisé; cependant, vous l'utiliserez pour tester l'accès à distance. Avec Telnet, toutes les informations, y compris les mots de passe et les commandes, sont transmis en texte clair. Lors des activités suivantes, vous utiliserez SSH pour accéder à distance aux périphériques réseau.

a. Open Tera Term ou autre programme d'émulation de terminal avec la capacité Telnet.

b. Sélectionnez le serveur Telnet et indiquez l'adresse de gestion SVI pour vous connecter à S1. Le mot de passe est **cisco**.

c. Après la saisie du mot de passe **cisco**, vous accéderez à l'invite du mode d'exécution utilisateur. Accédez au mode d'exécution privilégié en utilisant la commande **enable** et le mot de passe **class**.

d. Enregistrez la configuration.

e. Tapez **exit** pour terminer la session Telnet.

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

- **Partie 4: Gérer la table d'adresses MAC**

Dans la partie 4, vous déterminerez les adresses MAC acquises par le commutateur, configurerez une adresse MAC statique sur une interface du commutateur, puis supprimerez l'adresse MAC statique depuis cette interface.

Etape 1: Notez l'adresse MAC de l'hôte

Ouvrez une invite de commande sur PC-A et exécutez la commande **ipconfig /all** pour déterminer et enregistrer les adresses (physiques) de la couche 2 de la carte réseau.

Etape 2: Déterminez les adresses MAC que le commutateur a apprises.

Ouvrez la fenêtre de configuration.

Affichez les adresses MAC à l'aide de la commande **show mac address-table**.

- S1# **show mac address-table**

Questions:

- Combien y a-t-il d'adresses dynamiques?
- Combien y a-t-il d'adresses MAC au total?
- Est-ce que l'adresse MAC dynamique correspond à l'adresse MAC de PC-A?

a. Répertoriez les options de la commande show mac address-table.

Affichez les options de la table d'adresses MAC.

- S1# **show mac address-table**

Question:

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

b. Exécutez la commande show mac address-table dynamic pour n'afficher que les adresses MAC acquises de façon dynamique.

- S1# **show mac address-table dynamic**

Question:

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

c. Affichez la saisie de l'adresse MAC pour PC-A. Le formatage d'adresse MAC pour la commande est xxxx.xxxx.xxxx.

- S1# **show mac address-table address <PC-A MAC here>**

Etape 3: Définir une adresse MAC statique.

a. Effacez la table d'adressage MAC.

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

- S1# **clear mac address-table dynamic**

b. Vérifiez que la table d'adressage MAC a bien été effacée.

- S1# **show mac address-table**

Question:

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

Activité 1 : Configuration de base du commutateur – Lab

c. Nouvel examen de la table MAC

Il est fort probable qu'une application exécutée sur votre PC a déjà envoyé une trame à partir de la carte réseau vers S1. Observez à nouveau la table des adresses MAC en mode d'exécution privilégié pour voir si S1 a réappris l'adresse MAC de PC-A.

- S1# **show mac address-table**

Questions:

- Combien y a-t-il d'adresses dynamiques?
- Pourquoi cela est-il différent du dernier affichage ?

Si S1 n'a pas encore réacquis l'adresse MAC de PC-A, envoyez une requête ping à l'adresse IP du VLAN 99 du commutateur à partir de PC-A, puis réexécutez la commande **show mac address-table**.

d. Définir une adresse MAC statique.

Pour spécifier à quels ports un hôte peut se connecter, une option consiste à créer un mappage statique de l'adresse MAC hôte vers un port.

Définissez une adresse MAC statique sur F0/6 en utilisant l'adresse qui a été enregistrée pour PC-A lors de l'étape 1 de la Partie 4. L'adresse MAC 0050.56BE.6C89 est utilisée exclusivement en guise d'exemple. Vous devez utiliser l'adresse MAC de PC-A, qui est différente de celle présentée ici comme un exemple.

- S1(config)# **mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6**

e. Vérifiez les entrées de la table d'adressage MAC.

- S1# **show mac address-table**

Questions:

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

f. Supprimez l'entrée MAC statique. Passez en mode de configuration globale et supprimez la commande en insérant **no** au début de la chaîne de commande.

Remarque: l'adresse MAC 0050.56BE.6C89 est utilisée exclusivement dans l'exemple. Utilisez l'adresse MAC pour PC-A.

- S1(config)# **no mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6**

g. Vérifiez que l'adresse MAC statique a été supprimée.

- S1# **show mac address-table**

Question:

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

Questions de réflexion

1. Pourquoi devriez-vous configurer le mot de passe vty pour le commutateur?
2. Pourquoi modifier le VLAN 1 par défaut à un autre numéro de VLAN?
3. Comment empêcher l'envoi des mots de passe en texte clair?
4. Pourquoi configurer une adresse MAC statique sur une interface de port?

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

- **Annexe A: Initialiser et redémarrer un commutateur**

a. Accédez au commutateur par la console et passez en mode d'exécution privilégié.

Ouvrez la fenêtre de configuration.

- Switch> **enable**
- Switch#

b. Utilisez la commande show flash pour déterminer si des réseaux locaux virtuels ont été créés sur le commutateur.

- Switch# **show flash**

```
Directory of flash:/

2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text

    3 -rwx 1632 Mar 1 1993 00:06:33 +00:00 config.text

    4 -rwx 13336 Mar 1 1993 00:06:33 +00:00 multiple-fs

    5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-
mz.150-2.SE.bin

    6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat

32514048 bytes total (20886528 bytes free)
```

c. Si vous avez trouvé le fichier vlan.dat dans la mémoire Flash, supprimez-le.

- Switch# **delete vlan.dat**

```
Delete filename [vlan.dat]?
```

d. Vous êtes invité à vérifier le nom du fichier. Si vous avez saisi le nom correctement, appuyez sur Enter (Entrée); sinon, vous pouvez modifier le nom du fichier.

Vous êtes invité à confirmer la suppression du fichier. Appuez sur Enter (Entrée) pour confirmer.

```
Delete flash:/vlan.dat? [confirm]
```

- Switch#

e. Utilisez la commande **erase startup-config** pour supprimer le fichier de configuration initiale de la mémoire vive non volatile. Vous êtes invité à supprimer le fichier de configuration. Appuyez sur Entrée pour confirmer.

e. Switch# **erase startup-config**

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

[OK]

Erase of nvram: complete
```

- Switch#

f. Redémarrez le commutateur pour supprimer toutes les anciennes informations de configuration de la mémoire. Vous serez invité à confirmer le rechargement du commutateur. Appuyez sur Entrée pour confirmer.

- Switch# reload

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

Remarque: Vous serez peut-être invité à enregistrer la configuration en cours avant de redémarrer le commutateur. Répondre en tapant **no** et appuyez sur Enter (Entrée).

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

f. Après le redémarrage du commutateur, vous êtes invité à ouvrir la boîte de dialogue de configuration initiale. Répondre en tapant no à l'invite et appuyez Enter (Entrée).

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

- Switch>

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

Réponses

- **Partie 1 / Etape 1:**

b: Aucun paramètre d'adressage IP n'est encore configuré. Un commutateur Cisco 2960 mis en service pour la première fois n'a pas de mise en réseau configurée.

Partie 1 / Etape 2:

a: `Switch> enable`

`Switch#`

b: – `Switch# show running-config`

- 24

- 2

- 0-4 et 5-15 ou 0-15

c: `Switch# show startup-config`

`startup-config is not present`

- Aucune configuration n'a été enregistrée dans la NVRAM.

d: `Switch# show interface vlan1`

- Non

- 0CD9:96E2:3D40 dans ce cas.

- Les commutateurs Cisco ont la commande **no shutdown** configurée par défaut sur le VLAN 1, mais le VLAN 1 n'atteindra pas l'état up/up jusqu'à ce qu'un port lui soit attribué et que ce port soit également up. S'il n'y a pas de port à l'état actif dans le VLAN 1, l'interface VLAN 1 sera active, protocole de ligne inactif. Par défaut, tous les ports sont affectés initialement au VLAN 1.

e: - `Switch# show ip interface vlan1`

- Vlan1 est actif, le protocole de ligne est inactif / Traitement du protocole Internet désactivé

f: - `Switch# show ip interface vlan1`

- Vlan1 est en place, le protocole de ligne est en place / Traitement du protocole Internet désactivé

g: - `Switch# show version`

- Les réponses peuvent varier…

h: - `Switch# show interface f0/6`

- Il devrait être allumé à moins qu'il n'y ait un problème de câblage.

- Connexion d'un hôte ou d'un autre périphérique

- Les réponses peuvent varier

- Full-duplex, 100Mb/s

PARTIE 1

PARTIE 1

Activité 1 : Configuration de base du commutateur – Lab

Réponses

i:- `Switch# show vlan`

- default

- Tous les ports; F0/1 – F0/24; G0/1, G0/2

- Oui

- enet (Ethernet)

j: Les réponses peuvent varier

- **Partie 2 / Etape 1:**

b:
```
S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# ipv6 address 2001:db8:acad::2/64
S1(config-if)# ipv6 address fe80::2 link-local
S1(config-if)# no shutdown
S1(config-if)# exit
```

c:
```
S1(config)# interface range f0/1 – 24,g0/1 – 2
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

d: `S1# show vlan brief`

e: `S1(config)# ip default-gateway 192.168.1.1`

f:
```
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
```

g:
```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
```

- Sans la commande de connexion, le commutateur ne demandera pas de mot de passe.

Activité 1 : Configuration de base du commutateur – Lab

Réponses

- **Partie 3 / Etape 1:**

b: - 1000000 Kb/s (1 Gb/sec) - up - up

- **Partie 3 / Etape 3:**

d: `S1# copy running-config startup-config`

- **Partie 4 / Etape 1:**

- Les réponses peuvent varier

- **Partie 4 / Etape 2:**

- 1 (peut varier) - 24(peut varier) - Oui

- **Partie 4 / Etape 3:**

a: 12 (peut varier)

b: 1 (peut varier)

- **Partie 4 / Etape 4:**

b: - au moins 20 (d'autres entrées statiques peuvent avoir été créées manuellement)

- 0 (peut être 1, selon la rapidité avec laquelle les adresses sont réacquises par le commutateur)

c: - 1

- Le commutateur a réacquis dynamiquement l'adresse MAC du PC.

e: - 22 (varies)

- Il y a 22 adresses statiques. Le nombre total d'adresses MAC et d'adresses statiques doit être le même car aucun autre périphérique n'est actuellement connecté à S1.

g: 21 (varies)

Questions de réflexion

- Si vous ne configurez pas de mot de passe vty, vous ne pourrez pas vous connecter par telnet au commutateur.
- Pour une meilleure sécurité.
- Issue the service password-encryption command.
- Pour spécifier les ports auxquels un hôte peut se connecter.

PARTIE 1

TP 1

Configurer les périphériques réseaux

1. Configuration d’un commutateur
2. Configuration des paramètres de base d'un routeur

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer les périphériques réseaux?
- Réponses correctes pour au moins 70 % des questions.

Activité 2 : Configurer les paramètres de base du routeur– Lab

- **Objectifs**

- **Partie 1 : Configuration de la topologie et initialisation des appareils**
- Câblez l'équipement pour qu'il corresponde à la topologie du réseau.
- Initialisez et redémarrez le routeur et le commutateur.
- **Partie 2 : Configuration des périphériques et vérification de la connectivité**
- Attribuer des informations IPv4 et IPv6 statiques aux interface des PC.
- Configurez les paramètres de base du routeur.
- Configurez le routeur pour SSH.
- Vérifiez la connectivité du réseau.
- **Partie 3 : afficher les informations du routeur**
- Récupérez des informations sur le matériel et les logiciels à partir du routeur.
- Interprétez le résultat à partir de la configuration initiale.
- Interprétez le résultat à partir de la table de routage.
- Vérifiez l'état des interfaces.

- **Contexte/scénario**

Ces travaux pratiques passent en revue les commandes de routeur IOS vues précédemment. Dans les Parties 1 et 2, vous allez câbler le matériel et définir des configurations de base ainsi que des paramètres d'interface sur le routeur.

Dans la Partie 3, vous allez utiliser SSH pour vous connecter à distance au routeur et utiliser des commandes IOS pour récupérer des informations à partir du périphérique afin de répondre à des questions sur le routeur.

Pour des besoins de révision, ces travaux pratiques contiennent les commandes nécessaires aux configurations spécifiques du routeur.

Remarque: Les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs Cisco 4221 équipés de Cisco IOS version 16.9.4 (universalk9 image). Les commutateurs utilisés dans les laboratoires sont des Cisco Catalyst 2960s avec Cisco IOS Release 15.2(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif des interfaces du routeur à la fin de ce TP pour obtenir les identifiants d'interface corrects.

Remarque : Assurez-vous que le routeur et le commutateur ont été réinitialisés et ne possèdent aucune configuration initiale. Consultez votre instructeur pour connaître la procédure d'initialisation et de redémarrage d'un routeur et d'un commutateur.

PARTIE 1

PARTIE 1

Activité 2 : Configurer les paramètres de base du routeur– Lab

Ressources requises

- 1 Routeur (Cisco 4221 équipé de l'image universelle Cisco IOS version 16.9.4 ou similaire)
- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.2(2) image lanbasek9 ou similaire)
- 2 PC (Windows, équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet comme indiqué dans la topologie

Remarque: les interfaces Gigabit Ethernet des routeurs Cisco 4221 sont à détection automatique et un câble Ethernet droit peut être utilisé entre le routeur et le PC-B. Si vous utilisez un autre modèle de routeur Cisco, il peut être nécessaire d'utiliser un câble croisé Ethernet.

Topologie

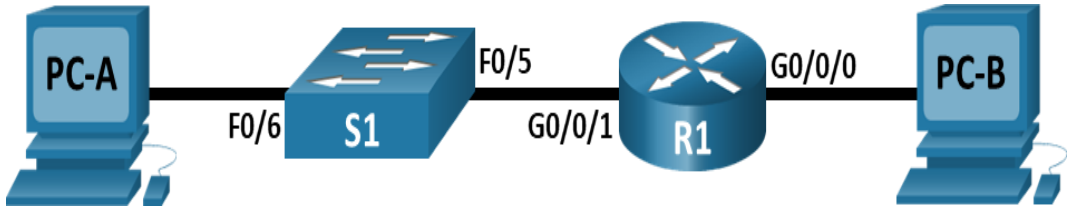


Table d'adressage

Appareil	Interface	Adresse IP / Préfixe	Passerelle par défaut
R1	G0/0/0	192.168.0.1 /24	S/O
		2001:db8:acad::1 /64	
		fe80::1	
	G0/0/1	192.168.1.1 /24	
		2001:db8:acad:1 /64	
		fe80::1	
	Loopback0	10.0.0.1 /24	
		2001:db8:acad:2::1 /64	
		fe80::1	
PC-A	Carte réseau (NIC)	192.168.1.10 /24	192.168.1.1
		2001:db8:acad:1::10 /64	fe80::1
PC-B	Carte réseau (NIC)	192.168.0.10 /24	192.168.0.1
		2001:db8:acad:: 10 /64	fe80::1

Instructions

Partie 1 : Configuration de la topologie et initialisation des appareils

Etape 1: Câblez le réseau conformément à la topologie indiquée

a. Connectez les équipements représentés dans le schéma de topologie et effectuez le câblage nécessaire.

b. Mettez sous tension tous les périphériques de la topologie.

PARTIE 1

Activité 2 : Configurer les paramètres de base du routeur– Lab

Etape 2: Initialisez et redémarrez le routeur et le commutateur

- **Partie 2 : Configuration des périphériques et vérification de la connectivité**

Etape 1: Configurer les interfaces des ordinateurs

a. Configurez l'adresse IP, le masque de sous-réseau et la passerelle par défaut sur le PC-A.

b. Configurez l'adresse IP, le masque de sous-réseau et la passerelle par défaut sur le PC-B

Etape 2: Configurez le routeur

a. Accédez au routeur par la console et activez le mode d'exécution privilégié.

b. Passez en mode de configuration.

c. Attribuez un nom de l'appareil au routeur.

d. Définissez le nom de domaine du routeur ccna-lab.com.

e. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

f. Cryptez les mots de passe en texte clair.

g. Configurez le système pour qu'il nécessite un mot de passe de 12 caractères minimum.

h. Configurez le nom d'utilisateur **SshAdmin** avec un mot de passe crypté de **55Hadm!n2020**

i. Générer un ensemble de clés de crypto avec un module de 1024 bits.

j. Définissez le mot de passe EXEC privilégié sur **$cisco!PRIV***

k. Attribuez **$cisco!!CON*** comme mot de passe de la console, configurez les sessions pour qu'elles se déconnectent après quatre minutes d'inactivité et activez la connexion.

l. Attribuez **$cisco!!VTY*** comme mot de passe vty, configurez les lignes vty pour accepter uniquement les connexions SSH, configurez les sessions pour qu'elles se déconnectent après quarte minutes d'inactivité et activez la connexion à l'aide de la base de données locale.

m. Créez une bannière qui avertit quiconque d'accéder à l'appareil que tout accès non autorisé est interdit.

n. Activation du routage IPv6

o. Configurez les trois interfaces du routeur avec les informations d'adressage IPv4 et IPv6 de la table d'adressage ci-dessus. Configurez les trois interfaces avec des descriptions. Activez les trois interfaces.

p. Le routeur ne doit pas autoriser les connexions vty pendant deux minutes si trois tentatives de connexion échouées se produisent dans 60 secondes.

q. Réglez l'horloge sur le routeur.

r. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Question :

- Quel serait le résultat du redémarrage du routeur avant l'exécution de la commande **copy running-config startup-config** ?

PARTIE 1

Activité 2 : Configurer les paramètres de base du routeur– Lab

Etape 3: Vérifiez la connectivité du réseau

a. À l'aide de la ligne de commande de PC-A, envoyez une requête ping aux adresses IPv4 et IPv6 pour PC-B.

Remarque: il peut être nécessaire de désactiver le pare-feu des PC.

Question:

- Les requêtes ping ont-elles abouti?

b. Accédez à distance à R1 à partir de PC-A à l'aide du client SSH de Tera Term.

À l'aide de Tera Term sur PC-A, ouvrez une session SSH sur l'adresse IPv4 de l'interface de bouclage R1. Assurez-vous que la case d'option **SSH** est sélectionnée et cliquez sur **OK** pour vous connecter au routeur. Connectez-vous en tant que **SSHadmin** avec le mot de passe **55Hadm!n2020**.

Question:

- L'accès distant a-t-il abouti?

À l'aide de Tera Term sur PC-A, ouvrez une session SSH sur l'adresse IPv6 de l'interface boucle avec retour R1. Assurez-vous que la case d'option **SSH** est sélectionnée et cliquez sur **OK** pour vous connecter au routeur. Connectez-vous en tant que **SSHadmin** avec le mot de passe **55Hadm!n2020**.

Remarque: L'adresse IPv6 doit être entourée de crochets, c'est-à-dire [*IPv6 address*]

Questions :

- L'accès distant a-t-il abouti?
- Pourquoi le protocole Telnet est-il considéré comme un risque de sécurité ?

Partie 3: Afficher les informations du routeur

Dans la Partie 3, vous allez utiliser des commandes **show** à partir d'une session SSH en vue de récupérer des informations du routeur.

Etape 1: Établissez une session SSH vers R1

En utilisant le client Telnet/SSH sur **PC-A**, ouvrez une session SSH à l'adresse IPv6 de l'interface de bouclage **R1** et connectez-vous en tant que **SShadmin** avec le mot de passe **55Hadm! n2020**.

Etape 2: Récupérez les informations matérielles et logicielles importantes.

a. Utilisez la commande show version pour répondre aux questions sur le routeur.

Questions:

- Quel est le nom de l'image IOS exécutée par le routeur?
- Quelle quantité de mémoire vive non volatile (NVRAM) le routeur possède-t-il?
- Quelle quantité de mémoire Flash le routeur possède-t-il?

Activité 2 : Configurer les paramètres de base du routeur– Lab

b. Les commandes **show** fournissent souvent plusieurs écrans de résultats. Le filtrage de la sortie vous permet d'afficher certaines sections de la sortie. Pour activer la commande de filtrage, entrez un caractère de barre verticale (|) après une commande **show**, suivi d'un paramètre et d'une expression de filtrage. Vous pouvez faire correspondre le résultat avec l'instruction de filtrage à l'aide du mot-clé **include** afin d'afficher toutes les lignes du résultat qui contiennent l'expression de filtrage. Filtrez la commande **show version** en utilisant **show version | include register** pour répondre à la question ci-dessous.

Question:

- Quel est le processus de démarrage du routeur lors du prochain redémarrage?

Etape 3: Affichez la configuration initiale

a. Utilisez la commande **show startup-config** sur le routeur pour répondre aux questions ci-dessous.

Questions :

- Comment les mots de passe sont-ils présentés dans les résultats?

b. Use the **show running-config | section vty** command.

Question:

- Quel est le résultat de l'exécution de cette commande?

Etape 4: Affichez la table de routage sur le routeur

Utilisez la commande **show ip route** sur le routeur pour répondre aux questions ci-dessous.

Questions :

- Quel code est utilisé dans la table de routage pour indiquer un réseau connecté directement?
- Combien d'entrées de route sont codées avec un code C dans la table de routage?

Etape 5: Affichez la liste récapitulative des interfaces sur le routeur.

a. Utilisez la commande **show ip interface brief** sur le routeur pour répondre à la question ci-dessous.

Question :

- Quelle commande a modifié l'état des ports Gigabit Ethernet depuis administratively "down" à "up"?

b. Exécutez la commande **show ipv6 int brief** afin de vérifier les paramètres IPv6 sur R1.

Question :

- Que nous révèlent les résultats [up/up]?

PARTIE 1

Activité 2 : Configurer les paramètres de base du routeur– Lab

c. Sur PC-B, modifiez sa configuration afin qu'il n'ait plus d'adresse IPv6 statique. Vous devrez peut-être redémarrer l'ordinateur. Exécutez la commande ipconfig sur PC-B afin d'examiner la configuration IPv6.

Questions :

- Quelle est l'adresse IPv6 attribuée à PC-B ?
- Quelle est la passerelle par défaut attribuée à PC-B ?
- Envoyez une requête ping à partir de PC-B à l'adresse link-local de la passerelle par défaut de R1. A-t-elle abouti?
- Envoyez une requête ping à partir de PC-B à l'adresse de monodiffusion IPv6 2001:db8:acad::1 de R1. A-t-elle abouti?

Questions de réflexion

- Lors de la recherche d'un problème de connectivité réseau, un technicien suspecte qu'une interface n'a pas été activée. Quelle commande **show** le technicien pourrait-il utiliser pour dépanner ce problème ?

Activité 2 : Configurer les paramètres de base du routeur– Lab

Réponses

- **Partie 2 / Etape 2:**

a:
```
router> enable
```

b:
```
router# config terminal
```

c:
```
router(config)# hostname R1
```

d:
```
R1(config)# ip domain name ccna-lab.com
```

e:
```
R1(config)# no ip domain lookup
```

f:
```
R1(config)# service password-encryption
```

g:
```
R1(config)# security passwords min-length 12
```

h:
```
R1(config)# username SSHadmin secret 55Hadm!n2020
```

i:
```
R1(config)# crypto key generate rsa modulus 1024
```

j:
```
R1(config)# enable secret $cisco!PRIV*
```

k:
```
R1(config)# line console 0
R1(config-line)# password $cisco!!CON*
R1(config-line)# exec-timeout 4 0
R1(config-line)# login
```

l:
```
R1(config)# line vty 0 4
R1(config-line)# password $cisco!!VTY*
R1(config-line)# exec-timeout 4 0
R1(config-line)# transport input ssh
R1(config-line)# login local
```

m:
```
R1(config)# ipv6 unicast-routing
```

n:
```
R1(config)# interface g0/0/0
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad::1/64
R1(config-if)# description Connection to PC-B
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# description Connection to S1
```

PARTIE 1

Activité 2 : Configurer les paramètres de base du routeur– Lab

Réponses

```
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface loopback0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# description loopback adapter
R1(config-if)# no shutdown
R1(config-if)# exit
```

o: `R1(config)# login block-for 120 attempts 3 within 60`
`R1(config)# exit`

p: `R1# clock set 15:20:00 5 Sept 2019`

q: `R1# copy running-config startup-config`

- Le contenu de la configuration en cours d'exécution dans la RAM serait effacé lors du rechargement. Par conséquent, le routeur démarrerait sans configuration de démarrage et il serait demandé à l'utilisateur s'il souhaite entrer dans la boîte de dialogue de configuration initiale.

- **Partie 2 / Etape 3:**

a: Oui

b: - Oui - Oui

- Une session Telnet peut être vue en clair. Il n'est pas crypté. Les mots de passe peuvent facilement être vus à l'aide d'un renifleur de paquets.

- **Partie 3 / Etape 2:**

a: - `R1# show version`

- La version de l'image peut varier, mais dans cet atelier, il s'agit de isr4200-universalk9_ias.16.09.04.SPA.bin.

- Les réponses peuvent varier, mais dans ce laboratoire, il s'agit de 32 768 octets de NVRAM.

- Les réponses peuvent varier, mais dans cet atelier, il dispose de 6 598 655 Koctets de mémoire flash.

b: - `R1# show version | include register`

- Les réponses peuvent varier. Dans la plupart des cas (0x2102), le routeur subira un démarrage normal, chargera l'IOS à partir de la mémoire Flash et chargera la configuration de démarrage à partir de la NVRAM si elle est présente. Si le registre de configuration est 0x2142, le routeur contournera la configuration de démarrage et commencera à l'invite de commande en mode utilisateur. Si le démarrage initial échoue, le routeur passe en mode ROMMON.

Activité 2 : Configurer les paramètres de base du routeur– Lab

Réponses

- **Partie 3 / Etape 3:**

- `R1# show start`

- Les mots de passe sont chiffrés grâce à la commande service password-encryption.

- Un utilisateur reçoit la sortie de configuration de démarrage en commençant par la ligne qui inclut la première instance de l'expression de filtrage.

- **Partie 3 / Etape 4:**

- `R1# show ip route`

- Le C désigne un sous-réseau directement connecté. Un L désigne une interface locale. Les deux réponses sont correctes.

- 3

- **Partie 3 / Etape 5:**

a: - `R1# show ip interface brief`

- no shutdown

b: - `R1# show ipv6 interface brief`

- L'état [up/up] reflète l'état des couches 1 et 2 de l'interface et ne repose pas sur l'état de la couche 3.

c: Les réponses varieront. Adresse IPv6 de 2001 :db8:acad:a:d428:7de2:997c:b05a

- fe80::1

- Oui - Oui

Questions de réflexion

- Les réponses peuvent varier. Cependant, show ip interface brief ou show interfaces ou show startup-config fournirait les informations.

PARTIE 1

TP 2

Appliquer les Concepts de commutation

Compétences visées :

- Comprendre les concepts de commutation

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

1 heures

TP 2

Appliquer les Concepts de commutation

1. Concepts de commutation

Critères de réussite :

- Le stagiaire est-il capable de :
  - Comprendre les concepts de commutation?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 1

Activité 1 : qui entend la diffusion?– Packet Tracer

- **Objectifs**

- **Partie 1: Observer le trafic de diffusion dans une implémentation VLAN**
- **Partie 2: Répondre aux questions de révision**

- **Scénario**

Dans cet exercice, un commutateur Catalyst 2960 24 ports est entièrement rempli. Tous les ports sont utilisés. Vous allez observer le trafic de diffusion lors d'une implémentation de VLAN et répondre à quelques questions de réflexion.

- **Instructions**

Etape 1: Utilisez la commande ping pour générer du trafic

a. Cliquez sur **PC0** , puis sur l'onglet **Desktop** > **Command Prompt**.

b. Saisissez la commande **ping 192.168.1.8** . La requête ping doit réussir.

Contrairement à un LAN, un VLAN est un domaine de diffusion créé par des commutateurs. Dans le mode **Simulation** de Packet Tracer, envoyez une requête ping aux périphériques finaux sur leur propre VLAN. En vous basant sur vos observations, répondez aux questions de l'Étape 2.

Etape 2: Générez et examinez le trafic de diffusion dans une implémentation VLAN

a. Basculez en mode **Simulation**.

b. Cliquez sur **Edit Filters** dans le panneau de simulation. Désactivez la case à cocher **Show All/None**. Cochez la case **ICMP**.

c. Cliquez sur l'outil **Add Complex PDU** ; il s'agit de l'icône en forme d'enveloppe ouverte dans la barre d'outils de droite.

d. Amenez le pointeur de la souris au-dessus de la topologie. Il prend alors la forme d'une enveloppe avec un signe plus (+).

e. Cliquez sur **PC0** pour qu'il serve de source à ce message test, et la boîte de dialogue **Create Complex PDU** apparaît. Entrez les valeurs suivantes:

- Destination IP Address: 255.255.255.255 (adresse de diffusion)
- Sequence Number (numéro de séquence): 1
- One Shot Time: 0

Dans les paramètres PDU, la valeur par défaut de **Select Application (sélectionner l'application)** est PING.

Question:

- Indiquez au moins trois autres applications disponibles.

f. Cliquez sur **Create PDU** (créer une PDU). Ce paquet de diffusion test apparaît désormais dans la section **Simulation Panel Event List.** Il apparaît également dans la fenêtre PDU List (liste des PDU). Il s'agit de la première unité de données de protocole pour le Scénario 0.

g. Cliquez à deux reprises sur **Capture/Forward** (capture/avance).

Question:

- Qu'est-il arrivé au paquet?

h. Répétez cette procédure pour **PC8** et **PC16**.

Activité 1 : qui entend la diffusion?– Packet Tracer

Questions de réflexion

- Si un PC du VLAN 10 envoie un message de diffusion, quels périphériques le reçoivent?
- Si un PC du VLAN 20 envoie un message de diffusion, quels périphériques le reçoivent?
- Si un PC du VLAN 30 envoie un message de diffusion, quels périphériques le reçoivent?
- Qu'arrive-t-il à une trame envoyée depuis un PC du VLAN 10 vers un PC du VLAN 30?
- Quels ports du commutateur s'allument si un PC connecté au port 11 envoie un message de monodiffusion à un PC connecté au port 13?
- Quels ports du commutateur s'allument si un PC connecté au port 2 envoie un message de monodiffusion à un PC connecté au port 23?
- En termes de ports, quels sont les domaines de collision sur le commutateur?
- En termes de ports, quels sont les domaines de diffusion sur le commutateur?

Activité 1 : qui entend la diffusion?– Packet Tracer

Réponses

- **Etape 2:**

e: DNS, FINGER, FTP, HTTP, HTTPS, IMAP, NETBIOS, PING, POP3, SFTP, SMTP, SNMP, SSH, TELNET, TFTP and OTHER

g: Le paquet est envoyé au commutateur puis diffusé à tous les PC qui appartiennent au même VLAN et dans ce cas, VLAN 10.

Questions de réflexion

- Tous les terminaux sur VLAN 10
- Tous les terminaux sur VLAN 20
- Tous les terminaux sur VLAN 30
- Il sera abandonné car ils ne sont pas sur le même VLAN.
- Les ports 11 et 13 s'allumeront.
- Le paquet sera abandonné.
- Chaque port est son propre domaine de collision.
- Chaque VLAN est son propre domaine de diffusion.

TP 3

Mettre en œuvre des VLAN

Compétences visées :

- Configurer les VLAN
- Configurer le routage inter-VLAN

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

6 heures

TP 3

Mettre en œuvre des VLAN

1. Configuration des VLAN
2. Configuration du protocole DTP
3. Configuration du routage inter-VLAN

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer les VLANs?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 1

Activité 1 : Configurer les VLAN et le trunking – Lab

- **Objectifs**

- **Partie 1: Créer le réseau et configurer les paramètres de base des périphériques**
- **Partie 2: Créer les VLAN et attribuer les ports de commutateur**
- **Partie 3: Mettre à jour les attributions des ports VLAN et la base de données VLAN**
- **Partie 4: Configurer un trunk 802.1Q entre les commutateurs**
- **Partie 5: Supprimer la base de données VLAN**

- **Contexte/scénario**

Les commutateurs modernes utilisent des VLAN pour améliorer les performances réseau en divisant les vastes domaines de diffusion de couche 2 en domaines plus petits. Ces VLAN peuvent également être utilisés comme mesure de sécurité en contrôlant quels hôtes peuvent communiquer. D'une manière générale, les VLAN permettent d'adapter un réseau aux objectifs de l'entreprise.

Les trunks de VLAN sont utilisés pour étendre des VLAN sur plusieurs périphériques. Les trunks permettent au trafic issu de plusieurs VLAN de circuler sur une liaison unique, tout en maintenant intactes l'identification et la segmentation des VLAN.

Au cours de ces travaux pratiques, vous allez créer des VLAN sur les deux commutateurs présents dans la topologie, attribuer les VLAN aux ports d'accès des commutateurs, vérifier que les VLAN fonctionnent comme prévu, puis créer un trunk de VLAN entre les deux commutateurs afin de permettre aux hôtes inclus dans un même VLAN de communiquer par le biais du trunk, quel que soit le commutateur auquel l'hôte est réellement connecté.

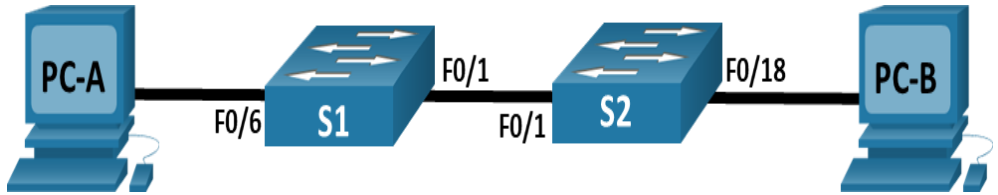
Remarque: les commutateurs utilisés lors des travaux pratiques CCNA sont des commutateurs Cisco Catalyst 2960 équipés de Cisco IOS version 15.0(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque: Assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre formateur.

- **Ressources requises**

- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.2.2 image lanbasek9 ou similaires)
- 2 PC (Windows, équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

- **Topologie**



Activité 1 : Configurer les VLAN et le trunking – Lab

- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	Carte réseau	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	Carte réseau	192.168.10.4	255.255.255.0	192.168.10.1

- **Instructions**

- **Partie 1: Créer le réseau et configurer les paramètres de base des périphériques**

Dans la Partie 1, vous allez configurer la topologie du réseau et les paramètres de base sur les hôtes de PC et les commutateurs.

Etape 1: Câblez le réseau conformément à la topologie indiquée

Connectez les équipements représentés dans le schéma de topologie et effectuez le câblage nécessaire.

Etape 2: Configurez les paramètres de base pour chaque commutateur

a. Accédez au commutateur par la console et activez le mode d'exécution privilégié.

Ouvrez la fenêtre de configuration.

a. Passez en mode de configuration.

b. Attribuez un nom de périphérique au commutateur.

c. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes incorrectement saisies comme s'il s'agissait de noms d'hôtes.

d. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

e. Attribuez **cisco** comme mot de passe de console et activez la connexion.

f. Définissez **cisco** comme mot de passe vty et activez la connexion.

g. Cryptez les mots de passe en texte clair.

h. Créez une bannière qui avertit quiconque d'accéder à l'appareil que tout accès non autorisé est interdit.

i. Configurez l'adresse IP listée dans la table d'adressage pour VLAN 1 sur le commutateur.

j. Arrêtez toutes les interfaces qui ne seront pas utilisées.

k. Réglez l'horloge sur le commutateur.

l. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Etape 3: Configurez les PC hôtes

Reportez-vous à la table d'adressage pour les informations d'adresses d'hôte de PC.

PARTIE 1

Activité 1 : Configurer les VLAN et le trunking – Lab

Etape 4: Testez la connectivité

Vérifiez que les hôtes de PC peuvent s'envoyer mutuellement des requêtes ping.

Remarque: Il peut être nécessaire de désactiver le pare-feu des PC pour pouvoir envoyer une requête ping entre les PC.

Questions :

- PC-A peut-il envoyer une requête ping à PC-B?
- PC-A peut-il envoyer une requête ping à S1?
- PC-B peut-il envoyer une requête ping à S2?

Ouvrez la fenêtre de configuration.

- S1 peut-il envoyer une requête ping à S2?
- Si vous avez répondu "Non" à l'une de ces questions, pourquoi les requêtes ping n'ont-elles pas abouti?

Partie 2: Créer les VLAN et attribuer les ports de commutateur

Dans Partie 2, vous allez créer des VLAN de gestion, d'exploitation, de parking_Lot et natifs sur les deux commutateurs. Vous attribuerez ensuite ces VLAN aux interfaces appropriées. La commande **show vlan** est utilisée pour vérifier vos paramètres de configuration.

Etape 1: Créez les VLAN sur les commutateurs

a. création des réseaux locaux virtuels sur S1

- S1(config)# **vlan 10**
- S1 (config-vlan) # **name Operations**
- S1(config-vlan)# **vlan 20**
- S1 (config-vlan) # **nom Parking_Lot**
- S1(config-vlan)# **vlan 99**
- S1(config-vlan)# **name Management**
- S1 (config-vlan) # **vlan 1000**
- S1(config-vlan)# **name Native**
- S1(config-vlan)# **end**

b. Créez les mêmes VLAN sur S2.

c. Exécutez la commande **show vlan brief** pour afficher la liste des VLAN sur S1.

- S1# **show vlan brief**

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
```

PARTIE 1

PARTIE 1

Activité 1 : Configurer les VLAN et le trunking – Lab

```
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gi0/1, Gi0/2
10 Operations active
20 Parking_Lot active
99 Management active
1000 Native active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
```

Questions:

- Quel est le VLAN par défaut?
- Quels ports sont attribués au VLAN par défaut?

Etape 2: Attribuez les VLAN aux interfaces de commutateur correctes

a. Attribuez les VLAN aux interfaces sur S1.

1. Attribuez PC-A au VLAN d'opération.
   - S1(config)# **interface f0/6**
   - S1(config-if)# **switchport mode access**
   - S1(config-if)# **switchport access vlan 10**
2. Déplacez l'adresse IP de commutateur vers le VLAN 99.
   - S1(config)# **interface vlan 1**
   - S1(config-if)# **no ip address**
   - S1(config-if)# **interface vlan 99**
   - S1(config-if)# **ip address 192.168.1.11 255.255.255.0**
   - S1(config-if)# **end**

b. Exécutez la commande **show vlan brief** et vérifiez que les VLAN sont attribués aux interfaces correctes

c. Exécutez la commande **show ip interface brief**.

Question:

- Quel est l'état du VLAN 99? Expliquez votre réponse.

d. Attribuez PC-B au VLAN d'opérations sur S2.

e. Supprimez l'adresse IP du VLAN 1 sur S2.

f. Configurez une adresse IP pour le VLAN 99 sur S2, conformément à la table d'adressage.

g. Exécutez la commande **show vlan brief** pour vérifier que les VLAN sont attribués aux interfaces correctes.

Questions:

- S1 peut-il envoyer une requête ping vers S2? Expliquez votre réponse.

Activité 1 : Configurer les VLAN et le trunking – Lab

- PC-A peut-il envoyer une requête ping à PC-B? Expliquez votre réponse.

Partie 3: Mettre à jour les attributions des ports VLAN et la base de données VLAN

Dans la Partie 3, vous allez modifier les attributions des ports VLAN et supprimer des VLAN de la base de données VLAN.

Etape 1: Attribuez un VLAN à plusieurs interfaces

a. Sur S1, attribuez les interfaces F0/11 – 24 au VLAN99.
- S1(config)# **interface range f0/11-24**
- S1(config-if-range)# **switchport mode access**
- S1(config-if-range)# **switchport access vlan 99**
- S1(config-if-range)# **end**

b. Exécutez la commande **show vlan brief** pour vérifier les attributions de VLAN.

c. Réattribuez les interfaces F0/11 et F0/21 au VLAN 10.

d. Vérifiez que les attributions de VLAN sont correctes.

Etape 2: Supprimez une attribution de VLAN de l'interface

a. Exécutez la commande **no switchport access vlan** pour supprimer l'attribution du VLAN 99 à l'interface F0/24.
- S1(config)# **interface f0/24**
- S1(config-if)# **no switchport access vlan**
- S1(config-if)# **end**

b. Assurez-vous que la modification de VLAN a été effectuée.

Question:

- À quel VLAN le port F0/24 est-il maintenant associé?

Etape 3: Supprimez un ID VLAN de la base de données VLAN

a. Ajoutez le VLAN 30 à l'interface F0/24 sans exécuter la commande globale VLAN.
- S1(config)# **interface f0/24**
- S1(config-if)# **switchport access vlan 30**

```
% Access VLAN does not exist. Creating vlan 30
```

Remarque: La technologie actuelle des commutateurs ne nécessite plus l'exécution de la commande **vlan** pour l'ajout d'un VLAN à la base de données. En attribuant un VLAN inconnu à un port, le VLAN sera créé et ajouté à la base de données VLAN.

b. Vérifiez que le nouveau VLAN s'affiche dans la table VLAN.

Question:

- Quel est le nom par défaut du VLAN 30?

c. Exécutez la commande **no vlan 30** pour supprimer le VLAN 30 de la base de données VLAN.
- S1(config)# **no vlan 30**
- S1(config)# **end**

PARTIE 1

Activité 1 : Configurer les VLAN et le trunking – Lab

d. Exécutez la commande show vlan brief. L'interface F0/24 a été attribuée au VLAN 30.

Question:

- Après la suppression du VLAN 30 de base de données VLAN, à quel VLAN le port F0/24 est-il attribué? Que devient-il du trafic destiné à l'hôte connecté à F0/24?

e. Exécutez la commande **no switchport access vlan** sur l'interface F0/24.

f. Exécutez la commande **show vlan brief** pour déterminer l'attribution de VLAN de F0/24.

Questions:

- À quel VLAN le port F0/24 est-il attribué?

Remarque: Avant de supprimer un VLAN de la base de données, il est recommandé de réattribuer tous les ports qui ont été attribués à ce VLAN.

- Pourquoi devez-vous réattribuer un port à un autre VLAN avant de supprimer le VLAN de la base de données VLAN?

○ Partie 4: Configurer un trunk 802.1Q entre les commutateurs

Dans la Partie 4, vous allez configurer l'interface F0/1 pour utiliser le protocole DTP (Dynamic Trunking Protocol) afin de lui permettre de négocier le mode trunk. Une fois cette opération réalisée et vérifiée, vous allez désactiver le protocole DTP sur l'interface F0/1 et configurer celle-ci manuellement en tant que trunk.

Etape 1: Utilisez le protocole DTP pour initier le trunking sur F0/1.

Le mode DTP par défaut d'un port de commutateur 2960 est le mode automatique dynamique (dynamic auto). Cela permet à l'interface de convertir la liaison en trunk si l'interface voisine est configurée pour le mode trunk ou le mode dynamique souhaitable.

Ouvrez la fenêtre de configuration.

a. Configurez F0/1 sur S1 pour négocier le mode trunk.

- S1(config)# **interface f0/1**
- S1(config-if)# **switchport mode dynamic desirable**

```
Sep 19 02:51:47.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up

Sep 19 02:51:47.291: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan99, changed state to up
```

Vous devriez également recevoir des messages d'état du lien sur le commutateur S2.

- S2#

```
Sep 19 02:42:19.424: %LINK-3-UPDOWN: Interface FastEthernet0/1,
changed state to up

Sep 19 02:42:21.454: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan99, changed state to up

Sep 19 02:42:22.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```

PARTIE 1

Activité 1 : Configurer les VLAN et le trunking – Lab

b. Exécutez la commande **show vlan brief** sur S1 et S2. L'interface F0/1 n'est plus attribuée au VLAN 1. Les interfaces en mode trunk ne sont pas répertoriées dans la table VLAN.

c. Exécutez la commande **show interfaces trunk** pour afficher les interfaces en mode trunk. Notez que le mode sur S1 est souhaitable (desirable) et sur S2 est automatique (auto).

- S1# **show interfaces trunk**
- S2# **show interfaces trunk**

Remarque: Par défaut, tous les VLAN sont autorisés sur un trunk. La commande **switchport trunk** permet de contrôler quels VLAN ont accès au trunk. Pour ces travaux pratiques, conservez les paramètres par défaut permettant à tous les VLAN de traverser F0/1.

Fermez la fenêtre de configuration.

d. Assurez-vous que le trafic VLAN circule sur l'interface trunk F0/1.

Questions:

- S1 peut-il envoyer une requête ping à S2?
- PC-A peut-il envoyer une requête ping à PC-B?
- PC-A peut-il envoyer une requête ping à S1?
- PC-B peut-il envoyer une requête ping à S2?

Si vous avez répondu "Non" à l'une de ces questions, expliquez pourquoi ci-dessous.

Etape 2: Configurez manuellement l'interface trunk F0/1.

La commande **switchport mode trunk** est utilisée pour configurer manuellement un port en tant que trunk. Cette commande doit être exécutée sur les deux extrémités de la liaison.

a. Modifiez le mode de port de commutateur (switchport) sur l'interface F0/1 de manière à imposer le trunking. Veillez à effectuer cette opération sur les deux commutateurs.

Ouvrez la fenêtre de configuration.

- S1(config)# **interface f0/1**
- S1(config-if)# **switchport mode trunk**

b. Exécutez la commande **show interfaces trunk** pour afficher le mode trunk. Notez que le mode est passé de **desirable** à **on**.

- S2# **show interfaces trunk**

c. Modifiez la configuration du trunk sur les deux commutateurs en changeant le VLAN natif de VLAN 1 à VLAN 1000.

- S1(config)# **interface f0/1**
- S1(config-if)# **switchport trunk native vlan 1000**

d. Exécutez la commande show interfaces trunk pour afficher le mode trunk. Notez que les informations du VLAN natif sont mises à jour.

- S2# **show interfaces trunk**

Questions:

- Pourquoi voudriez-vous configurer manuellement une interface en mode trunk au lieu d'utiliser le protocole DTP?
- Pourquoi souhaitez-vous modifier le VLAN natif sur un trunk?

PARTIE 1

Activité 1 : Configurer les VLAN et le trunking – Lab

○ Partie 5: Suppression de la base de données VLAN

Dans la Partie 5, vous allez supprimer la base de données VLAN du commutateur. Il est nécessaire d'effectuer cette opération lors de la réinitialisation d'un commutateur à ses paramètres par défaut.

Etape 5: Déterminez si la base de données VLAN existe

Exécutez la commande **show flash** afin de déterminer si un fichier **vlan.dat** existe dans la mémoire Flash.

- S1# **show flash:**

Remarque: Si un fichier **vlan.dat** est présent en mémoire Flash, la base de données VLAN ne contient pas ses paramètres par défaut.

Etape 2: Supprimez la base de données VLAN

a. Exécutez la commande **delete vlan.dat** pour supprimer le fichier vlan.dat de la mémoire Flash et réinitialiser la base de données VLAN à ses paramètres par défaut. Vous serez invité à confirmer deux fois que vous souhaitez supprimer le fichier vlan.dat. Appuyez deux fois sur Entrée.

- S1# **delete vlan.dat**

```
Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]
```

b. Exécutez la commande **show flash** pour vérifier que le fichier vlan.dat a bien été supprimé.

- S1# **show flash:**

Question:

- Quelles autres commandes sont nécessaires pour réinitialiser un commutateur à ses paramètres par défaut?

Questions de réflexion

- Qu'est-ce qui est nécessaire pour permettre aux hôtes présentés dans le VLAN 10 de communiquer avec ceux du VLAN 99?
- Quels sont les principaux avantages dont une entreprise peut bénéficier grâce à une utilisation efficace des VLAN?

PARTIE 1

Activité 1 : Configurer les VLAN et le trunking – Lab

Réponses

- **Partie 1 / Etape 2 :**

a:
```
switch> enable
```

b:
```
switch# config terminal
```

c:
```
switch(config)# hostname S1
switch(config)# hostname S2
```

d:
```
S1(config)# no ip domain-lookup
S2(config)# no ip domain-lookup
```

e:
```
S1(config)# enable secret class
S2(config)# enable secret class
```

f:
```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S2(config)# line console 0
S2(config-line)# password cisco
S2(config-line)# login
```

g:
```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S2(config)# line vty 0 4
S2(config-line)# password cisco
S2(config-line)# login
```

h:
```
S1(config)# service password-encryption
S2(config)# service password-encryption
```

i:
```
S1(config)# banner motd $ Authorized Users Only! $
S2(config)# banner motd $ Authorized Users Only! $
```

j:
```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S2(config)# interface vlan 1
S2(config-if)# ip address 192.168.1.12 255.255.255.0
S2(config-if)# no shutdown
S2(config-if)# exit
```

PARTIE 1

PARTIE 1

Activité 1 : Configurer les VLAN et le trunking – Lab

Réponses

k:
```
S1# clock set 15:30:00 19 September 2019
S2# clock set 15:30:00 19 September 2019
```

l:
```
S1# copy running-config startup-config
S2# copy running-config startup-config
```

- **Partie 1 / Etape 4 :**

- Oui - Non -Oui -Non

- Les pings ont échoué lors de la tentative de ping d'un appareil sur un sous-réseau différent. Pour que ces pings réussissent, une passerelle par défaut doit exister pour acheminer le trafic d'un sous-réseau à un autre.

- **Partie 2 / Etape 1 :**

c: - VLAN 1

- Tous les ports du commutateur sont attribués au VLAN 1 par défaut.

- **Partie 2 / Etape 2 :**

b:
```
S1# show vlan brief
10OperationsactiveFa0/6
```

c:
```
S1# show ip interface brief
Vlan99192.168.1.11YES manual updown
```

- L'état du VLAN 99 est up/down, up car le VLAN existe dans la base de données mais down car le VLAN n'a pas encore été affecté à un port actif.

d:
```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10
```

e:
```
S2(config)# interface vlan 1
S2(config-if)# no ip address
```

f:
```
S2(config-if)# interface vlan 99
S2(config-if)# ip address 192.168.1.12 255.255.255.0
```

g:
```
S2# show vlan brief
10OperationsactiveFa0/18
```

- Non. Les adresses IP des commutateurs résident désormais dans le VLAN 99. Le trafic VLAN 99 ne sera pas envoyé via l'interface F0/1.
- Non. L'interface F0/1 n'est pas affectée au VLAN 10, donc le trafic VLAN 10 ne sera pas envoyé dessus.
- **Partie 3 / Etape 1 :**

b:
```
S1# show vlan brief
```

PARTIE 1

Activité 1 : Configurer les VLAN et le trunking – Lab

Réponses

c:
```
S1(config)# interface range f0/11, f0/21
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```

d: `S1# show vlan brief` Fa0/11, Fa0/21

- **Partie 3 / Etape 2 :**

b: - VLAN 1, the default VLAN.

- `S1# show vlan brief` Fa0/24

- **Partie 3 / Etape 3:**

b: `S1# show vlan brief` 30VLAN0030activeFa0/24

- VLAN0030

d: Lorsque vous supprimez un VLAN, tous les ports attribués à ce VLAN deviennent inactifs. Ainsi, le port F0/24 est toujours associé au VLAN 30. Cependant, le VLAN 30 est désormais inactif car il n'existe pas dans la base de données VLAN. De plus, le port ne transférera aucun trafic.

- `S1# show vlan brief`

e:
```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

f: - The default VLAN, VLAN 1

- `S1# show vlan brief` Fa0/24

- Les interfaces affectées à un VLAN qui est supprimé de la base de données VLAN deviennent inactives et ne peuvent pas être utilisées jusqu'à ce qu'elles soient réaffectées à un autre VLAN. Cela peut être difficile à résoudre car les interfaces à ressources partagées n'apparaissent pas non plus dans la liste des ports (la partie 4 contient plus d'informations sur les interfaces à ressources partagées).

- **Partie 4 / Etape 1:**

b: `S1# show vlan brief`

d: - Oui - Oui - Non - Non

- Les commutateurs sont en VLAN 99 et les PC sont en VLAN 10 ; par conséquent, les pings entre les VLAN ont échoué.

- **Partie 4 / Etape 2:**

a:
```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

c:
```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 1000
```

Activité 1 : Configurer les VLAN et le trunking – Lab

Réponses

d: - Tous les équipements n'utilisent pas le DTP. L'utilisation de la commande switchport mode trunk garantit que le port deviendra un trunk, quel que soit le type d'équipement connecté à l'autre extrémité de la liaison.

- L'utilisation du VLAN 1, le VLAN par défaut, car le VLAN natif représente un risque pour la sécurité. Tous les différents protocoles de contrôle qui sont échangés entre les commutateurs sont échangés via le VLAN 1 natif non balisé, et ces informations pourraient être exposées si les paramètres par défaut sont utilisés sur les ports auxquels les utilisateurs se connectent.

Partie 5 / Etape 2:

b: Pour rétablir les paramètres par défaut d'un commutateur, les commandes **erase startup-config** et **reload** doivent être émises après la commande **delete vlan.dat**.

Questions de réflexion

- Les réponses varient, mais pour permettre le routage inter-VLAN, un périphérique de couche 3 est nécessaire pour acheminer le trafic entre les VLAN.
- Les réponses varieront, mais les avantages du VLAN incluent : une meilleure sécurité, des économies de coûts (utilisation efficace de la bande passante et des liaisons montantes), des performances supérieures (domaines de diffusion plus petits), une atténuation des tempêtes de diffusion, une meilleure efficacité du personnel informatique, une gestion plus simple des projets et des applications.

TP 3

Mettre en œuvre des VLAN

1. Configuration des VLAN
2. Configuration du protocole DTP
3. Configuration du routage inter-VLAN

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer les VLANs?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 1

Activité 2 : Configurer DTP– Packet Tracer

- **Objectifs**

- **Configurer le trunking statique**
- **Configuration et vérification du protocole DTP**

- **Contexte/scénario**

À mesure que le nombre de commutateurs augmente sur un réseau, la gestion des VLANs et des trunks peut devenir complexe. Pour faciliter certaines configurations de VLAN et de trunking, la négociation de trunk entre les périphériques réseau est gérée par le protocole DTP (Dynamic Trunking Protocol), et est automatiquement activée sur les commutateurs Catalyst 2960 et Catalyst 3650.

Dans cet exercice, vous configurerez des trunks entre les commutateurs. Vous attribuerez des ports aux VLANs et vérifierez la connectivité de bout en bout entre les hôtes d'un même VLAN. Vous configurerez les trunks entre les commutateurs, et vous configurerez le VLAN 999 comme le VLAN natif.

- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau
PC1	Carte réseau	192.168.10.1	255.255.255.0
PC2	Carte réseau	192.168.20.1	255.255.255.0
PC3	Carte réseau	192.168.30.1	255.255.255.0
PC4	Carte réseau	192.168.30.2	255.255.255.0
PC5	Carte réseau	192.168.20.2	255.255.255.0
PC6	Carte réseau	192.168.10.2	255.255.255.0
S1	VLAN 99	192.168.99.1	255.255.255.0
S2	VLAN 99	192.168.99.2	255.255.255.0
S3	VLAN 99	192.168.99.3	255.255.255.0

- **Instructions**

  - **Partie 1: Vérifiez la configuration VLAN**

Vérifiez les VLANs configurés sur les commutateurs.

a. Sur S1, accédez au mode EXEC privilégié et entrez la commande **show vlan brief** pour vérifier les VLANs présents.

Ouvrez la fenêtre de configuration.

- S1# **show vlan brief**

```
VLAN Name Status Ports
---- -------------------------------- --------- ---------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
```

Activité 2 : Configurer DTP– Packet Tracer

```
                                    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gig0/1, Gig0/2
     99 Management active
     999 Native active
     1002 fddi-default active
     1003 token-ring-default active
     1004 fddinet-default active
     1005 trnet-default active
```

b. Répétez l'étape 1a sur S2 et S3.

Question :

- Quels VLANs sont configurés sur les commutateurs ?

c. Sur S2, créez un VLAN 10 et nommez-le Red.

- S2(config)# **vlan 10**
- S2(config-vlan)# **name Red**

d. Créez les VLANs 20 et 30 conformément au tableau ci-dessous.

Numéro de VLAN	Nom du VLAN
10	Red
20	Blue
30	Yellow

e. Vérifiez que les nouveaux VLANs ont bien été ajoutés. Exécutez la commande **show vlan brief** en mode d'exécution privilégié.

Question :

- **En** plus des VLANs par défaut, quels VLANs sont configurés sur S2 ?

f. Répétez les étapes précédentes pour créer les VLANs supplémentaires sur S3.

Partie 2: Attribution de VLAN aux ports.

Exécutez la commande **switchport mode access** pour définir le mode d'accès des liaisons d'accès. Utilisez la commande **switchport access vlan** *vlan-id* pour attribuer un VLAN à un port d'accès.

Ports	Contrôles	Réseau
S2 F0/1 – 8 S3 F0/1 – 8	VLAN 10 (Red)	192.168.10.0 /24
S2 F0/9 – 16 S3 F0/9 – 16	VLAN 20 (Blue)	192.168.20.0 /24
S2 F0/17 – 24 S3 F0/17 – 24	VLAN 30 (Yellow)	192.168.30.0 /24

PARTIE 1

Activité 2 : Configurer DTP– Packet Tracer

a. Attribuez des VLANs aux ports sur S2 en utilisant les attributions du tableau ci-dessus.

- S2(config-if)# **interface range f0/1 - 8**
- S2(config-if-range)# **switchport mode access**
- S2(config-if-range)# **switchport access vlan 10**
- S2 (config-if-range) # **interface range f0/9 -16**
- S2(config-if-range)# **switchport mode access**
- S2(config-if-range)# **switchport access vlan 20**
- S2(config-if-range)# **interface range f0/17 - 24**
- S2(config-if-range)# **switchport mode access**
- S2(config-if-range)# **switchport access vlan 30**

b. Attribuez des VLANs aux ports sur S3 en utilisant les attributions du tableau ci-dessus.

Maintenant que vous avez les ports attribués aux VLAN, essayez de faire un ping de **PC1** à **PC6** .

Question :

- La requête ping a-t-elle abouti ? Expliquez votre réponse.

○ Partie 3: Configuration de trunks sur S1, S2 et S3.

Le protocole DTP (Dynamic Trunking Protocol) gère les trunks entre les commutateurs Cisco. Actuellement, tous les switchports sont en mode "trunking" par défaut, c'est-à-dire en mode automatique dynamique. À cette étape, vous modifierez le mode de trunking sur dynamic desirable pour la liaison entre les commutateurs S1 et S2. La liaison entre les commutateurs S1 et S3 sera définie en tant que trunk statique. Utilisez le VLAN 999 en tant que VLAN natif dans cette topologie.

a. Sur le commutateur S1, configurez la liaison de trunk en dynamique désirable sur l'interface GigabitEthernet 0/1. La configuration de S1 est affichée ci-dessous.

- S1(config)# **interface g0/1**
- S1(config-if)# **switchport mode dynamic desirable**

Question :

- Quel sera le résultat de la négociation de trunk entre S1 et S2 ?

b. Sur le commutateur S2, vérifiez que le trunk a été négocié en entrant la commande **show interfaces trunk** . L'interface GigabiteEthernet 0/1 doit apparaître dans la sortie.

Question :

- Quels sont le mode et l'état de ce port ?

c. Pour la liaison trunk entre S1 et S3, configurez l'interface GigabitEthernet 0/2 comme une liaison trunk statique sur S1. De plus, désactivez la négociation DTP sur l'interface G0/2 sur S1.

- S1(config)# **interface g0/2**
- S1(config-if)# **switchport mode trunk**
- S1(config-if)# **switchport nonegotiate**

c. Utilisez la commande show dtp pour vérifier l'état de **DTP**.

- S1# **show dtp**

PARTIE 1

Activité 2 : Configurer DTP– Packet Tracer

```
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    1 interfaces using DTP
```

e. Vérifiez que le trunking est activé sur tous les commutateurs à l'aide de la commande **show interfaces trunk**.

- S1# **show interfaces trunk**

```
Port Mode Encapsulation Status Native vlan
Gig0/1 desirable n-802.1q trunking 1
Gig0/2 on 802.1q trunking 1

Port Vlans allowed on trunk
Gig0/1 1-1005
Gig0/2 1-1005

Port Vlans allowed and active in management domain
Gig0/1 1,99,999
Gig0/2 1,99,999

Port Vlans in spanning tree forwarding state and not pruned
Gig0/1 1,99,999
Gig0/2 1,99,999
```

Question :

- Quel est actuellement le VLAN natif pour ces trunks ?

f. Configurez le VLAN 999 en tant que VLAN natif pour les trunks sur S1.

- S1(config)# **interface range g0/1 - 2**
- S1(config-if-range)# **switchport trunk native vlan 999**

Question :

- Quels messages avez-vous reçus sur S1 ? Quelles corrections apporteriez-vous ?

g. Sur S2 et S3, configurez le VLAN 999 en tant que VLAN natif.

h. Vérifiez que le trunking est bien configuré sur tous les commutateurs. Vous devriez pouvoir envoyer une requête ping d'un commutateur à un autre dans la topologie en utilisant les adresses IP configurées dans l'interface SVI.

i. Tentative de ping de PC1 à PC6.

Question :

- Pourquoi le ping a-t-il échoué ? (Conseil : regardez la sortie '**show vlan brief**' des trois commutateurs. Comparez les sorties du '**show interface trunk**' sur tous les commutateurs.)

j. Corrigez la configuration si nécessaire.

PARTIE 1

Activité 2 : Configurer DTP– Packet Tracer

- **Partie 4: Reconfigurez le trunk sur S3.**

a. Lancer la commande ‘show interface trunk’ sur S3.

Question :

- Quel est le mode et l'encapsulation sur G0/2 ?

b. Configurez G0/2 pour qu'il corresponde à G0/2 sur S1 .

Question :

- Quel est le mode et l'encapsulation sur G0/2 après le changement ?

c. Saisissez Émettez la commande **'show interface G0/2 switchport**' sur le commutateur S3.

Question :

- Quel est l'état '**Négociation de la trunking**' affiché ?

Fermez la fenêtre de configuration.

- **Partie 5: Vérification de la connectivité de bout en bout.**

a. De PC1 ping PC6.

b. De PC2 ping PC5.

c. De PC3 ping PC4.

PARTIE 1

Activité 2 : Configurer DTP– Packet Tracer

Réponses

- **Partie 1**

b: Les VLAN 99 et 999 sont configurés sur tous les commutateurs.

- **Partie 2**

c: VLANs 1, 10, 20, 30, 99, et 999.

- **Partie 3**

b: Non, les pings n'ont pas abouti. En effet, les ports qui connectent les commutateurs ne sont pas configurés en tant que trunks pour transporter le trafic de plusieurs VLAN. Selon la sortie brève de show vlan, les ports G0/1 et G0/2 sont toujours des membres de port d'accès de VLAN1.

- **Partie 4**

a: La jonction sera négociée avec succès car le port sur S2 est en mode automatique dynamique par défaut.

b: Le switchport est en mode automatique, qui est la valeur par défaut. Le port est en mode trunking.

e: VLAN 1

f:

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (999), with S3 GigabitEthernet0/2 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (999), with S2 GigabitEthernet0/1 (1).

- Pour corriger la non-concordance du VLAN natif, configurez le VLAN 999 en tant que VLAN natif sur S2 et S3.

i: Les pings ont échoué car les VLAN 10, 20 et 30 n'étaient pas configurés sur S1. Pour résoudre le problème, les vlans doivent être configurés sur S1 pour correspondre à ce qui est configuré sur S2 et S3.

- **Partie 5**

a: La liaison n'a pas été négociée car S1 G0/2 est défini sur non négocié. L'interface G0/2 sur S3 est toujours en mode d'accès.

b: Le mode est activé et l'encapsulation est 801.2q.

c: off

Activité 2 : Configurer DTP– Packet Tracer

Réponses

Configuration :

Switch S1 :

```
enable
config t
vlan 10
 name Red
vlan 20
 name Blue
vlan 30
 name Yellow
interface g0/1
 switchport mode dynamic desirable
 switchport trunk native vlan 999
interface g0/2
 switchport mode trunk
 switchport trunk native vlan 999
 switchport nonegotiate
end
```

Switch S2:

```
enable
config t
vlan 10
 name Red
vlan 20
 name Blue
vlan 30
 name Yellow
interface range f0/1 - 8
 switchport mode access
 switchport access vlan 10
interface range f0/9 - 16
 switchport mode access
 switchport access vlan 20
interface range f0/17 - 24
 switchport mode access
 switchport access vlan 30
interface GigabitEthernet0/1
 switchport mode dynamic auto
 switchport trunk native vlan 999
end
```

Switch S3

```
enable
config t
vlan 10
 name Red
vlan 20
 name Blue
vlan 30
 name Yellow
interface range f0/1 - 8
 switchport mode access
 switchport access vlan 10
interface range f0/9 - 16
 switchport mode access
 switchport access vlan 20
interface range f0/17 - 24
 switchport mode access
 switchport access vlan 30
interface GigabitEthernet0/2
 switchport trunk
native vlan 999
 switchport mode trunk
 switchport nonegotiate
end
```

TP 3

Mettre en œuvre des VLAN

1. Configuration des VLAN
2. Configuration du protocole DTP
3. Configuration du routage inter-VLAN

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer les VLANs?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 1

Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

- **Objectifs**

- **Partie 1: Création du réseau et configuration des paramètres de base des périphériques**
- **Partie 2: Créer les VLAN et attribuer les ports de commutateur**
- **Partie 3 : Configurer un trunk 802.1Q entre les commutateurs**
- **Partie 4: Configurer du routage inter-VLAN sur le routeur**
- **Partie 5: Vérifier que le routage inter-VLAN fonctionne**

- **Contexte/scénario**

Les commutateurs modernes utilisent des réseaux locaux virtuels (VLAN) pour fournir des services de segmentation traditionnellement fournis par les routeurs dans les configurations du LAN. Les VLAN traitent de l'évolutivité, de la sécurité et de la gestion du réseau. D'une manière générale, les VLAN permettent d'adapter un réseau aux objectifs de l'entreprise. La communication entre les VLAN nécessite un périphérique fonctionnant au niveau de la couche 3 du modèle OSI. Les routeurs des topologies VLAN offrent une sécurité et une gestion des flux de trafic supplémentaires.

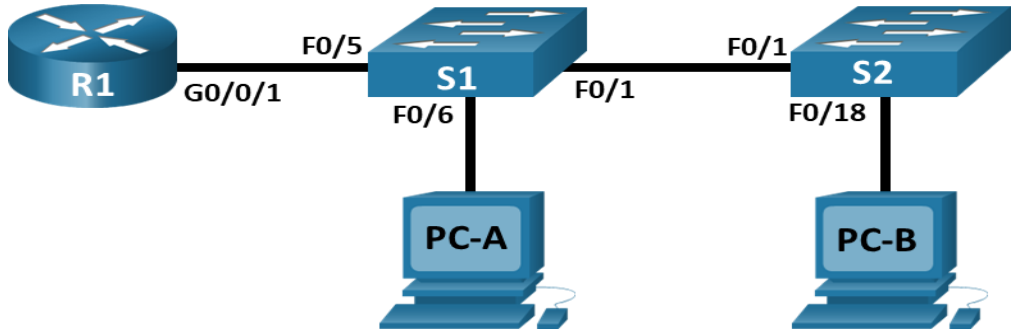
Les trunks de VLAN sont utilisés pour étendre des VLAN sur plusieurs périphériques. Les trunks permettent au trafic de plusieurs VLAN de circuler sur une liaison unique, tout en maintenant intactes l'identification et la segmentation des VLAN. Un type particulier de routage inter-VLAN, appelé «Router-On-A-Stick», utilise un trunk entre le routeur et le commutateur pour permettre à tous les VLAN de passer au routeur.

Au cours de ces travaux pratiques, vous allez créer des VLAN sur les deux commutateurs présents dans la topologie, vérifier que les VLAN fonctionnent comme prévu, puis créer un trunk de VLAN entre les deux commutateurs et entre S1 et R1, et configurer le routage inter-vlan sur R1 afin de permettre aux hôtes dans des VLAN différents de communiquer quel que soit le commutateur auquel l'hôte est réellement connecté.

Remarque: Les routeurs utilisés dans les travaux pratiques CCNA sont Cisco 4221 équipé de version 16.9.4 de Cisco IOS XE (image universalk9). Les commutateurs utilisés dans les travaux pratiques sont des modèles Cisco Catalyst 2960s équipé de version 15.2.2 de Cisco IOS (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque: Assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur.

- **Topologie**



Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0/1.3	192.168.3.1	255.255.255.0	N/A
	G0/0/1.4	192.168.4.1	255.255.255.0	N/A
	G0/0/1.8	S/O	S/O	S/O
S1	VLAN 3	192.168.3.11	255.255.255.0	192.168.3.1
S2	VLAN 3	192.168.3.12	255.255.255.0	192.168.3.1
PC-A	Carte réseau	192.168.3.3	255.255.255.0	192.168.3.1
PC-B	Carte réseau	192.168.4.3	255.255.255.0	192.168.4.1

Table de VLAN

VLAN	Nom	Interface attribuée
3	Gestion	S1: VLAN 3 S2: VLAN 3 S1: F0/6
4	Opérations	S2: F0/18
7	ParkingLot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-17, F0/19-24, G0/1-2
8	Natif	N/A

Ressources requises

- 1 Routeur (Cisco 4221 équipé de Cisco IOS XE version 16.9.4, image universelle ou similaire)
- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.2(2) image lanbasek9 ou similaires)
- 2 PC (Windows, équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

Instructions

Partie 1: Création du réseau et configuration des paramètres de base des périphériques

Dans la Partie 1, vous allez configurer la topologie du réseau et les paramètres de base sur les hôtes de PC et les commutateurs.

Etape 1: Câblez le réseau conformément à la topologie indiquée

Connectez les équipements représentés dans le schéma de topologie et effectuez le câblage nécessaire.

Etape 2: Configurez les paramètres de base du routeur

PARTIE 1

PARTIE 1

Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

a. Accédez au routeur par la console et activez le mode d'exécution privilégié.

b. Passez en mode de configuration.

c. Attribuez un nom de l'appareil au routeur.

d. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

e. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

f. Attribuez **cisco** comme mot de passe de console et activez la connexion.

g. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

h. Cryptez les mots de passe en texte clair.

i. Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

j. Enregistrez la configuration en cours dans le fichier de configuration initiale.

k. Réglez l'horloge sur le routeur.

Remarque: utilisez le point d'interrogation (**?**) pour obtenir de l'aide et connaître la séquence de paramètres requise pour exécuter cette commande.

Etape 3: Configurez les paramètres de base pour chaque commutateur

- Accédez au commutateur par la console et activez le mode d'exécution privilégié.
- Passez en mode de configuration.

a. Attribuez un nom de périphérique au commutateur.

b. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

c. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

d. Attribuez **cisco** comme mot de passe de console et activez la connexion.

e. Attribuez **cisco** comme mot de passe vty et activez la connexion.

f. Cryptez les mots de passe en texte clair.

g. Créez une bannière qui avertit quiconque accède à l'appareil que tout accès non autorisé est interdit.

h. Réglez l'horloge sur le commutateur.

Remarque: utilisez le point d'interrogation (**?**) pour obtenir et connaître la séquence de paramètres requise pour exécuter cette commande.

i. Copiez la configuration en cours en tant que configuration de démarrage.

Etape 4: Configurez les PC hôtes

Reportez-vous à la table d'adressage pour les informations d'adresses d'hôte de PC.

○ Partie 2: Création du VLAN et attribution des ports de commutateur

Dans la partie 2, vous allez créer des VLAN, comme spécifié dans le tableau ci-dessus, sur les deux commutateurs. Vous attribuerez ensuite ces VLAN aux interfaces appropriées.

PARTIE 1

Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

La commande **show vlan** est utilisée pour vérifier vos paramètres de configuration. Effectuez les tâches suivantes sur chaque commutateur.

Etape 1: Créez les VLAN sur les commutateurs

a. Créez et nommez les VLAN requis sur chaque commutateur à partir du tableau ci-dessus.

b. Configurez et activez l'interface de gestion et la passerelle par defaut sur chaque commutateur en utilisant les informations relatives à l'adresse IP dans le tableau d'adressage.

c. Attribuez tous les ports inutilisés des deux commutateurs au VLAN ParkingLot, configurez-les pour le mode d'accès statique et désactivez-les administrativement.

Remarque: La commande Interface range est utile pour accomplir cette tâche avec autant de commandes que nécessaire.

Etape 2: Attribuez les VLAN aux interfaces de commutateur correctes

- Attribuez les ports utilisés au VLAN approprié (spécifié dans la table VLAN ci-dessus) et configurez-les pour le mode d'accès statique. Assurez-vous de le faire sur les deux commutateurs
- Exécutez la commande **show vlan brief** et vérifiez que les VLAN sont attribués aux interfaces correctes

○ Partie 3: Configuration d'un trunk 802.1Q entre les commutateurs

Dans la partie 3, vous allez configurer manuellement l'interface F0/1 en tant que trunk.

Etape 1: Configurez manuellement l'interface trunk F0/1

- Modifiez le mode de port de commutateur (switchport) sur l'interface F0/1 de manière à imposer le trunking. Veillez à effectuer cette opération sur les deux commutateurs.
- Dans le cadre de la configuration du trunk, définissez le VLAN natif à 8 sur les deux commutateurs. Vous pouvez voir des messages d'erreur temporairement pendant que les deux interfaces sont configurées pour différents VLAN natifs.
- Comme autre partie de la configuration du trunk, spécifiez que les VLAN 3, 4 et 8 sont uniquement autorisés à traverser le trunk.
- Exécutez la commande **show interfaces trunk** pour vérifier les ports de trunk, le VLAN natif et les VLAN autorisés sur le trunk.

Etape 2: Configurer manuellement l'interface F0/5 du Trunk S1

a. Enregistrez la configuration en cours dans le fichier de configuration initiale sur S1 et S2.

b. Exécutez la commande **show interfaces trunk** pour vérifier le trunk.

Question:

- Pourquoi F0/5 n'apparaît-il pas dans la liste des trunk?

○ Partie 4: Configurer le routage inter-VLAN sur le routeur

a. Activez l'interface G0/0/1 sur le routeur.

Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

a. Configurez les sous-interfaces pour chaque VLAN comme spécifié dans la table d'adressage IP. Toutes les sous-interfaces utilisent l'encapsulation 802.1Q. Assurez-vous que la sous-interface du VLAN natif n'a pas d'adresse IP attribuée. Inclure une description pour chaque sous-interface.

b. Utilisez la commande show ip interface brief pour vérifier que la configuration de la sous-interface est opérationnelle

- **Partie 5: Vérifier que le routage inter-VLAN fonctionne**

Etape 1: Effectuez les tests suivants à partir de PC-A. Tout devrait réussir

Remarque: Vous devrez peut-être désactiver le pare-feu du PC pour que les requêtes ping puissent aboutir.

a. Envoyez une requête ping à partir de PC-A vers la passerelle par défaut.

b. Envoyez une requête ping de PC-A vers PC-B.

c. Envoyez une requête ping de PC-A vers S2.

Etape 2: Effectuer le test suivant à partir de PC-B

À partir de l'invite de commande sur PC-B, exécutez la commande tracert à l'adresse de PC-A.

Question:

- Quelles sont les adresses IP intermédiaires affichées dans les résultats?

Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

Réponses

- **Partie 1 /Etape 2:**

a:
```
router> enable
```

b:
```
router# config terminal
```

c:
```
router(config)# hostname R1
```

d:
```
R1(config)# no ip domain-lookup
```

e:
```
R1(config)# enable secret class
```

f:
```
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
```

g:
```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

h:
```
R1(config)# service password-encryption
```

i:
```
R1(config)# banner motd $ Authorized Users Only! $
```

j:
```
R1(config)# exit
R1# copy running-config startup-config
```

K:
```
R1# clock set 15:30:00 19 September 2019
```

- **Partie 1 /Etape 3 :**

a:
```
switch> enable
```

b:
```
switch# config terminal
```

c:
```
switch(config)# hostname S1
switch(config)# hostname S2
```

d:
```
S1(config)# no ip domain-lookup
S2(config)# no ip domain-lookup
```

e:
```
S1(config)# enable secret class
S2(config)# enable secret class
```

f:
```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S2(config)# line console 0
S2(config-line)# password cisco
S2(config-line)# login
```

PARTIE 1

Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

Réponses

g:
```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S2(config)# line vty 0 15
S2(config-line)# password cisco
S2(config-line)# login
```

h:
```
S1(config)# service password-encryption
S2(config)# service password-encryption
```

i:
```
S1(config)# banner motd $ Authorized Users Only! $
S2(config)# banner motd $ Authorized Users Only! $
```

j:
```
S1# clock set 15:30:00 19 September 2019
S2# clock set 15:30:00 19 September 2019
```

k:
```
S1# copy running-config startup-config
S2# copy running-config startup-config
```

- **Partie 2/ Etape 1 :**

a:
```
S1(config)# vlan 3
S1(config-vlan)# name Management
S1(config-vlan)# vlan 4
S1(config-vlan)# name Operations
S1(config-vlan)# vlan 7
S1(config-vlan)# name ParkingLot
S1(config-vlan)# vlan 8
S1(config-vlan)# name Native
```

```
S2(config)# vlan 3
S2(config-vlan)# name Management
S2(config-vlan)# vlan 4
S2(config-vlan)# name Operations
S2(config-vlan)# vlan 7
S2(config-vlan)# name ParkingLot
S1(config-vlan)# vlan 8
S1(config-vlan)# name Native
```

b:
```
S1(config)# interface vlan 3
S1(config-if)# ip address 192.168.3.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.3.1
```

```
S2(config)# interface vlan 3
S2(config-if)# ip address 192.168.3.12 255.255.255.0
S2(config-if)# no shutdown
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.3.1
```

PARTIE 1

PARTIE 1

Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

Réponses

c:
```
S1(config)# interface range f0/2 – 4 , f0/7 – 24 , g0/1 – 2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 7
S1(config-if-range)# shutdown
```

```
S2(config)# interface range f0/2 – 17, f0/19 – 24 , g0/1 – 2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 7
S2(config-if-range)# shutdown
```

Partie 2/ Etape 2 :

a:
```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 3
```

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 4
```

b: `S1# show vlan brief`

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/5
3	Management	active	Fa0/6
4	Operations	active	
7	Parking	Lotactive	Fa0/2, Fa0/3, Fa0/4, Fa0/7
			Fa0/8, Fa0/9, Fa0/10, Fa0/11
			Fa0/12, Fa0/13, Fa0/14, Fa0/15
			Fa0/16, Fa0/17, Fa0/18, Fa0/19
			Fa0/20, Fa0/21, Fa0/22, Fa0/23
			Fa0/24, Gi0/1, Gi0/2
8	Native	active	
<output omitted>			

`S2# show vlan brief`

VLAN	Name	Status	Ports
1	default	active	Fa0/1
3	Management	active	
4	Operations	active	Fa0/18
7	Parking	Lotactive	Fa0/2, Fa0/3, Fa0/4, Fa0/5
			Fa0/6, Fa0/7, Fa0/8, Fa0/9
			Fa0/10, Fa0/11, Fa0/12, Fa0/13
			Fa0/14, Fa0/15, Fa0/16, Fa0/17
			Fa0/19, Fa0/20, Fa0/21, Fa0/22
			Fa0/23, Fa0/24, Gi0/1, Gi0/2
8	Native	active	
<output omitted>			

Partie 3/ Etape 1 :

a:
```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

Réponses

b:
```
S1(config-if)# switchport trunk native vlan 8
S2(config-if)# switchport trunk native vlan 8
```

c:
```
S1(config-if)# switchport trunk allowed vlan 3,4,8
S2(config-if)# switchport trunk allowed vlan 3,4,8
```

d:
```
S1# show interfaces trunk
PortModeEncapsulationStatusNative vlan
Fa0/3on802.1qtrunking8
PortVlans allowed on trunk
Fa0/33-4,8
PortVlans allowed and active in management domain
Fa0/33-4,8
PortVlans in spanning tree forwarding state and not pruned
Fa0/33-4,8
S2#show interfaces trunk
PortModeEncapsulationStatusNative vlan
Fa0/1on802.1qtrunking8
PortVlans allowed on trunk
Fa0/13-4,8
PortVlans allowed and active in management domain
Fa0/13-4,8
PortVlans in spanning tree forwarding state and not pruned
Fa0/13-4,8
```

Partie 3/ Etape 2 :

a:
```
S1(config)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 8
S1(config-if)# switchport trunk allowed vlan 3,4,8
```

b:
```
S1# copy running-config startup-config
S2# copy running-config startup-config
```

c: Le port S1 5 ne s'affichera pas car l'état de l'interface GigabitEthernet 0/0/1 sur le routeur est administrativement arrêté.

Partie 4 :

a:
```
R1(config)# interface g0/0/1
R1(config-if)# no shutdown
R1(config-if)# exit
```

PARTIE 1

Activité 1 : Configuration du routage inter-VLAN avec la méthode router-on-a-stick– Lab

Réponses

b:
```
R1(config)# interface g0/0/1.3
R1(config-subif)# description Management Network
R1(config-subif)# encapsulation dot1q 3
R1(config-subif)# ip address 192.168.3.1 255.255.255.0
R1(config-subif)# interface g0/0/1.4
R1(config-subif)# description Operations Network
R1(config-subif)# encapsulation dot1q 4
R1(config-subif)# ip address 192.168.4.1 255.255.255.0
R1(config-subif)# interface g0/0/1.8
R1(config-subif)# description Native VLAN
R1(config-subif)# encapsulation dot1q 8 native
```

c:
```
R1# show ip interface brief
InterfaceIP-AddressOK? Method StatusProtocol
GigabitEthernet0/0/0unassignedYES unsetupup
GigabitEthernet0/0/1unassignedYES unsetupup
GigabitEthernet0/0/1.3 192.168.3.1YES manual upup
GigabitEthernet0/0/1.4 192.168.4.1YES manual upup
GigabitEthernet0/0/1.8 unassignedYES unsetupup
<output omitted>
```

Partie 5/ Etape 2:

- La sortie tracert affiche deux entrées dans les résultats. Le premier saut est G0/0/1.4 sur l'adresse d'interface R1, qui est l'adresse de passerelle pour PC-B. Le deuxième saut est l'adresse de PC-A.

PARTIE 1

Activité 2 : Configuration de la commutation de couche 3 et du routage inter-VLAN– Packet Tracer

- **Objectifs**

- **Partie 1: Configurer la commutation de couche 3**
- **Partie 2: Configurer le routage inter-VLAN**
- **Partie 3: Configurer le routage inter-VLAN IPv6**

- **Contexte/scénario**

Un commutateur multicouche comme le Cisco Catalyst 3650 est capable d'assurer à la fois la commutation de la couche 2 et le routage de la couche 3. Cette double fonctionnalité est l'un des bénéfices des commutateurs multicouches. Un avantage pour une petite ou moyenne entreprise serait la possibilité d'acheter un seul commutateur multicouche au lieu de périphérique de réseau de commutation et de routage séparés. Les capacités d'un commutateur multicouche comprennent la possibilité de passer d'un VLAN à un autre en utilisant plusieurs interfaces virtuelles commutées (SVI), ainsi que la possibilité de convertir un port de commutation de couche 2 en une interface de couche 3.

- **Table d'adressage**

Appareil	Interface	Adresse IP / Préfixe
MLS	VLAN 10	192.168.10.254 /24
		2001:db8:acad:10::1/64
	VLAN 20	192.168.20.254 /24
		2001:db8:acad:20:: 1/64
	VLAN 30	192.168.30.254/24
		2001:db8:acad:30:: 1/64
	VLAN 99	192.168.99.254/24
	G0/2	209.165.200.225
		2001:db8:acad:a::1/64
PC0	Carte réseau	192.168.10.1
PC1	Carte réseau	192.168.20.1
PC2	Carte réseau	192.168.30.1
PC3	Carte réseau	192.168.10.2/24
PC3		2001:db8:acad:10::2/64
PC4	Carte réseau	192.168.20.2/24
PC4		2001:db8:acad:20::2/64
PC5	Carte réseau	192.168.30.2
PC5		2001:db8:acad:10::2/64
S1	VLAN 99	192.168.99.1
S2	VLAN 99	192.168.99.2
S3	VLAN 99	192.168.99.3

PARTIE 1

PARTIE 1

Activité 2 : Configuration de la commutation de couche 3 et du routage inter-VLAN– Packet Tracer

- **Instructions**
  - **Partie 1: Configurer la commutation de couche 3**

Dans la Partie 1, vous allez configurer le port Gigabit Ethernet 0/2 sur le commutateur MLS multicouche en tant que port routé et vérifier que vous pouvez envoyer une requête ping sur une autre adresse de couche 3.

a. Sur le commutateur multicouche (MLS), configurez G0/2 en tant que port routé et attribuez une adresse IP en fonction de la table d'adressage.
   - MLS(config)# **interface g0/2**
   - MLS(config-if)# **no switchport**
   - MLS(config-if)# **ip address 209.165.200.225 255.255.255.252**

b. Vérifiez la connectivité dans le **cloud** en envoyant une requête ping à 209.165.200.226.
   - MLS# **ping 209.165.200.226**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

- **Partie 2: Configurer le routage inter-VLAN**

Etape 1: Ajoutez de réseaux VLAN

Ajoutez des réseaux VLAN au MLS en vous reportant au tableau ci-dessous. La notation Packet Tracer est sensible à la casse, alors tapez les noms exactement comme indiqué.

Numéro de VLAN	Nom du VLAN
10	Personnel
20	Élève
30	faculté

Etape 2: Configurez l'interface SVI sur le MLS

Configurez et activez l'interface SVI sur les réseaux VLAN 10, 20, 30 et 99 conformément à la table d'adressage. La configuration du réseau VLAN 10 est indiquée ci-dessous.

- MLS(config)# **interface vlan 10**
- MLS(config-if)# **ip address 192.168.10.254 255.255.255.0**

Etape 3: Configurez le trunking sur MLS

La configuration du trunk diffère légèrement sur un commutateur de la couche 3. Sur le commutateur de la couche 3, l'interface de trunk doit être encapsulée avec le protocole dot1q, mais il n'est pas nécessaire de spécifier les numéros de VLAN comme c'est le cas lorsqu'on travaille avec un routeur et des sous-interfaces.

a. Sur MLS, configurez l'interface **g0/1**.

b. Configurez l'interface comme un port de trunk statique.
   - MLS(config-if)# **switchport mode trunk**

Activité 2 : Configuration de la commutation de couche 3 et du routage inter-VLAN– Packet Tracer

c. Spécifiez le VLAN natif comme 99.

- MLS(config-if)# **switchport trunk native vlan 99**

d. Encapsulez le lien avec le protocole dot1q.

- MLS(config-if)# **switchport trunk encapsulation dot1q**

Remarque: Packet Tracer peut ne pas marquer l'encapsulation du trunk.

Etape 4: Configurez le trunking sur S1

a. Configurez l'interface **g0/1** de S1 en tant que trunk statique.

b. Configurez le VLAN natif sur le trunk.

Etape 5: Activez le routage

a. Utilisez la commande **show ip route**. Existe-t-il des routes actives?

b. Saisissez la commande **ip routing** pour activer le routage en mode de configuration globale.

- MLS(config)# **ip routing**

c. Utilisez la commande **show ip route** pour vérifier que le routage est activé.

- MLS# **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
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.10.0/24 is directly connected, Vlan10
C 192.168.20.0/24 is directly connected, Vlan20
C 192.168.30.0/24 is directly connected, Vlan30
C 192.168.99.0/24 is directly connected, Vlan99
     209.165.200.0/30 is subnetted, 1 subnets
C 209.165.200.224 is directly connected, GigabitEthernet0/2
```

Etape 6: Vérifiez la connectivité de bout en bout

a. Envoyez une requête ping à PC3 ou MLS depuis PC0 pour vérifier la connectivité au sein du réseau VLAN 10.

b. Envoyez une requête ping à PC4 ou MLS depuis PC1 pour vérifier la connectivité au sein du réseau VLAN 20.

PARTIE 1

Activité 2 : Configuration de la commutation de couche 3 et du routage inter-VLAN– Packet Tracer

c. Envoyez une requête ping à PC5 ou MLS depuis PC2 pour vérifier la connectivité au sein du réseau VLAN 30.

d. Envoyez une requête ping à S2, S3 ou MLS depuis S1 pour vérifier la connectivité au sein du réseau VLAN 99.

e. Pour vérifier le routage inter-VLAN, envoyez une requête ping aux périphériques en dehors du réseau VLAN de l'expéditeur.

f. À partir de n'importe quel périphérique, envoyez une requête ping à l'adresse suivante au sein du **cloud**: 209.165.200.226

Le commutateur de la couche 3 assure désormais le routage entre les VLAN et fournit une connectivité routée vers le cloud.

○ Partie 3: Configurer le routage inter-VLAN IPv6

Les commutateurs de couche 3 routent également entre les réseaux IPv6.

Etape 1: Activez le routage IPv6

Entrez la commande **ipv6 unicast-routing** pour activer le routage IPv6 en mode de configuration globale.

- MLS(config)# **ipv6 unicast-routing**

Etape 2: Configurez le SVI pour IPv6 sur MLS

Configurez l'adressage IPv6 sur SVI pour les VLAN 10, 20 et 30 selon la table d'adressage. La configuration du réseau VLAN 10 est indiquée ci-dessous.

- MLS(config)# **interface vlan 10**
- MLS (config-if) # **ipv6 address 2001:db8:acad:10::1/64**

Etape 3: Configurez G0/2 avec IPv6 sur MLS

a. Configurez l'adressage IPv6 sur G0/2.
- MLS (config) # **interface G0/2**
- MLS (config-if) # **ipv6 address 2001:db8:acad:a::1/64**

b. Utilisez la commande **show ipv6 route** pour vérifier les réseaux connectés IPv6.
- MLS# **show ipv6 route**

```
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S ::/0 [1/0]
via 2001:DB8:ACAD:A::2, GigabitEthernet0/2
C 2001:DB8:ACAD:A::/64 [0/0]
```

PARTIE 1

Activité 2 : Configuration de la commutation de couche 3 et du routage inter-VLAN– Packet Tracer

```
via ::, GigabitEthernet0/2
L 2001:DB8:ACAD:A::1/128 [0/0]
     via ::, GigabitEthernet0/2
C 2001:DB8:ACAD:10::/64 [0/0]
     via ::, Vlan10
L 2001:DB8:ACAD:10::1/128 [0/0]
     via ::, Vlan10
C 2001:DB8:ACAD:20::/64 [0/0]
     via ::, Vlan20
L 2001:DB8:ACAD:20::1/128 [0/0]
     via ::, Vlan20
C 2001:DB8:ACAD:30::/64 [0/0]
     via ::, Vlan30
L 2001:DB8:ACAD:30::1/128 [0/0]
     via ::, Vlan30
L FF00::/8 [0/0]
     via ::, Null0
```

Les périphériques PC3, PC4 et PC5 ont été configurés avec des adresses IPv6. Vérifiez le routage inter-VLAN IPv6 et la connectivité vers **le Cloud**.

a. Depuis PC3, ping MLS pour vérifier la connectivité au sein du VLAN 10.

b. Depuis PC4, ping MLS pour vérifier la connectivité au sein du VLAN 20.

c. Depuis PC5, ping MLS pour vérifier la connectivité au sein du VLAN 30.

d. Pour vérifier le routage inter-VLAN ping entre les périphériques PC3, PC4 et PC5.

e. Depuis PC3 ping l'adresse dans le **Cloud**, 2001:db8:acad:a::2.

Activité 2 : Configuration de la commutation de couche 3 et du routage inter-VLAN– Packet Tracer

Réponses

Configuration :

Switch S1 :

```
enable
conf t
int g0/1
switchport mode trunk
switchport trunk native vlan 99
end
```

MLS :

```
enable
config t
ip routing
ipv6 unicast-routing
interface GigabitEthernet0/1
 switchport trunk native vlan 99
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface GigabitEthernet0/2
 no switchport
 ip address 209.165.200.225 255.255.255.252
 ipv6 address 2001:DB8:ACAD:A::1/64vlan 10
 name Staff
vlan 20
 name Student
vlan 30
 name Faculty
interface Vlan10
 ip address 192.168.10.254 255.255.255.0
 ipv6 address 2001:DB8:ACAD:10::1/64
 no shutdown
interface Vlan20
 ip address 192.168.20.254 255.255.255.0
 ipv6 address 2001:DB8:ACAD:20::1/64
 no shutdown
interface Vlan30
 ip address 192.168.30.254 255.255.255.0
 ipv6 address 2001:DB8:ACAD:30::1/64
 no shutdown
interface Vlan99
 ip address 192.168.99.254 255.255.255.0
 no shutdown
end
```

PARTIE 1

Activité 3 : Dépannage du routage inter-VLAN– Packet Tracer

Objectifs

- **Partie 1 : détection des problèmes du réseau**
- **Partie 2 : implémentation de la solution**
- **Partie 3 : vérification de la connectivité réseau**

Scénario

Dans cet exercice, vous allez résoudre des problèmes de connectivité provoqués par des configurations incorrectes de VLAN et de routage inter-VLAN.

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut	VLAN
R1	G0/1,10	172.17.10.1	255.255.255.0	N/A	VLAN 10
R1	G0/1,30	172.17.30.1	255.255.255.0	N/A	VLAN 30
PC1	Carte réseau	172.17.10.10	255.255.255.0	172.17.10.1	VLAN 10
PC3	Carte réseau	172.17.30.10	255.255.255.0	172.17.30.1	VLAN 30

Instructions

Partie 1: Détection des problèmes du réseau

Examinez le réseau et localisez la source des problèmes de connectivité.

Ouvrez la fenêtre de configuration.

Les commandes que vous pouvez trouver utiles incluent :

- R1# **show ip interface brief**
- R1# **show interface g0/1.10**
- R1# **show interface g0/1.30**
- S1# **show interface trunk**

- Testez la connectivité et utilisez les commandes **show** nécessaires pour vérifier les configurations.
- Vérifiez que tous les paramètres configurés correspondent aux exigences indiquées dans le tableau d'adressage.
- Dressez la liste de tous les problèmes et des solutions possibles dans le **tableau de documentation**.

Tableau de documentation

Problèmes	Solutions

Partie 2 : implémentation de la solution

Mettez en œuvre les solutions recommandées.

Partie 3: Vérifiez la connectivité réseau

Vérifiez que les PC peuvent envoyer des requêtes ping aux autres PC et à R1. Si ce n'est pas le cas, continuez le dépannage jusqu'à ce que les requêtes ping aboutissent.

Activité 3 : Dépannage du routage inter-VLAN– Packet Tracer

Réponses

- **Partie 1:**

Problèmes	Solutions
L'interface physique G0/1 est active mais la sous-interface G0/1.10 est administrativement inactive.	Implémentez la commande no shutdown pour activer la sous-interface G0/1.10.
PC3 est configuré avec la mauvaise adresse de passerelle par défaut.	Changez la passerelle par défaut sur PC3 de 172.17.10.1 à 172.17.30.1
L'interface G0/1 sur S1 est configurée comme port d'accès au lieu de port de jonction.	Utilisez la commande **switchport mode trunk** pour faire passer l'interface du mode d'accès au mode trunk.
Les affectations VLAN de sous-interface sont commutées sur R1. Les affectations configurées ne correspondent pas à celles indiquées dans la table d'adressage.	Exécutez la commande **no encapsulation dot1q** pour supprimer la configuration incorrecte. Configurez ensuite les sous-interfaces avec la commande d'encapsulation correcte dot1q <vlan>. Entrez à nouveau les informations d'adresse IP correctes.

PARTIE 1

PARTIE 2

Etablir un réseau d'entreprise évolutif

Dans ce module, vous allez :

- Être en mesure de concevoir un réseau évolutif
- Etre en mesure de comprendre et configurer le protocole STP
- Etre capable de configurer l'agrégation des liaisons avec l'EtherChannel
- Etre en mesure de comprendre le fonctionnement du FHRP

8 heures

TP 1

Etudier l’évolutivité du réseau

Compétences visées :

- Comparer les périphériques de couche 2 et 3 du réseau

Recommandations clés:

- Lire attentivement l’énoncé et les questions
- Se référer au cours

1 heures

TP 1

Etablir un réseau d'entreprise évolutif

1. Sélection des périphériques réseau

Critères de réussite :

- Le stagiaire est-il capable de :
  - Comprendre la différence entre les périphériques de couche 2 et de couche 3?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 2

Activité 1 : Comparer les périphériques de couche 2 et de couche 3– Packet Tracer

- **Objectif**

- **Partie 1: Comparer les commutateurs de couche 2 et de couche 3**
- **Partie 2: Comparer un commutateur de couche 3 et un routeur**

- **Contexte**

Dans cet exercice, vous allez utiliser diverses commandes pour examiner trois topologies différentes de commutation et pour comparer les similitudes et les différences entre les commutateurs 2960 et 3650. Vous allez également comparer la table de routage d'un routeur 4321 et celle d'un commutateur 3560.

Remarque: Recherchez sur l'internet pour plus de détails sur le *commutateur WS-C3650-24PS-L de couche 3* et le routeur *ISR 4321/K9* .

- **Instructions**

Etape 1: Comparer les commutateurs de couche 2 et de couche 3

a. Examinez les aspects physiques des commutateurs **D1** et **ASw-1**.

Questions:

- Combien de switchports physiques chaque switch a-t-il ?
- Combien de ports de commutateur Fast Ethernet et Gigabit Ethernet chaque commutateur possède-t-il ?
- Indiquez la vitesse de transmission des ports de commutateur Fast Ethernet et Gigabit Ethernet sur chaque commutateur.
- L'un des deux commutateurs présente-t-il une conception modulaire?

b. Les ports d'un commutateur 3650 peuvent être configurés comme des interfaces de couche 3 en entrant la commande **no switchport** en mode de configuration de l'interface. Cela permet aux techniciens d'attribuer une adresse IP et un masque de sous-réseau au port de commutateurs de la même manière que lors de leur configuration sur l'interface d'un routeur.

Questions:

- Quelle est la différence entre un commutateur de couche 2 et un commutateur de couche 3?
- Quelle est la différence entre l'interface physique d'un commutateur et l'interface VLAN?
- Sur quelles couches les commutateurs 2960 et 3560 fonctionnent-ils?
- Exécutez la commande **show run** pour examiner les configurations des commutateurs **D1** et **ASw-1**. Remarquez-vous des différences entre les deux configurations?
- Essayez d'afficher la table de routage sur D1 et ASw-1 en utilisant la commande **show ip route** . D'après vous, pourquoi la commande fonctionne-t-elle sur le commutateur D1 mais pas sur le commutateur ASW-1?

Etape 2: Comparer un commutateur de couche 3 et un routeur

Dans le passé, les commutateurs et les routeurs étaient des appareils séparés et distincts. Le terme "switch" a été réservé aux dispositifs matériels qui fonctionnent au niveau de la couche 2. Les routeurs sont des périphériques qui prennent des décisions de réacheminement basées sur des informations de couche 3. Ils utilisent des protocoles de routage pour partager les informations de routage et communiquer entre eux. Les commutateurs de couche 3, tels que le 3650, peuvent être configurés de manière à transférer des paquets de couche 3.

PARTIE 2

Activité 1 : Comparer les périphériques de couche 2 et de couche 3– Packet Tracer

L'exécution de la commande **ip routing** en mode de configuration globale permet de configurer des commutateurs de couche 3 à l'aide de protocoles de routage, leur conférant ainsi certaines des fonctionnalités d'un routeur. Malgré quelques similitudes, les commutateurs de la couche 3 sont différents des routeurs à de nombreux autres aspects.

a. Ouvrez l'onglet Physical sur D1 et R1.

Questions:

- Remarquez-vous des similitudes entre les deux périphériques? Remarquez-vous des différences entre les deux périphériques?
- Exécutez la commande **show run** et examinez les configurations de R1 et de D1. Quelles différences remarquez-vous entre les deux?
- Quelle commande permet la configuration de D1 avec une adresse IP sur l'une de ses interfaces physiques?
- Exécutez la commande **show ip route** sur les deux périphériques. Voyez-vous des similitudes ou des différences entre les deux tables?
- Analysez maintenant la table de routage de R2 et de D2. Qu'est-ce qui est présent maintenant qui n'était pas présent dans la configuration de R1 et D1?
- Quel réseau se trouve dans la table de routage de D2 qui a été appris de R2?

b. Assurez-vous que chaque topologie dispose d'une connectivité de bout en bout en procédant aux tests suivants:

- Envoyez une requête ping de **PC1** vers **PC2**
- Envoyez une requête ping de **PC3** vers **PC4**
- Envoyez une requête ping de **PC5** vers **PC6** et **PC7**

Dans les trois exemples, chaque PC se trouve sur un réseau différent.

Questions:

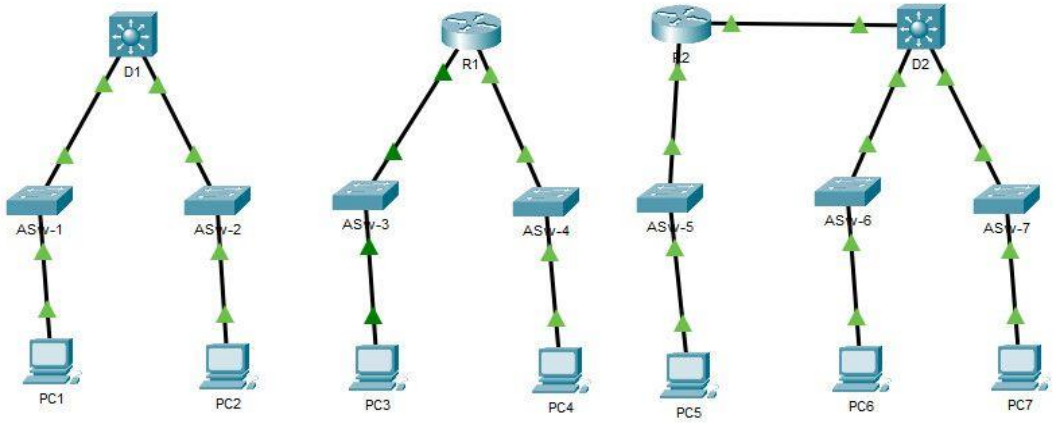
- Quel périphérique sert à établir la communication entre les réseaux?
- Pourquoi pouvions-nous envoyer des requêtes ping sur des réseaux sans la présence d'un routeur?
- **Question bonus:** Nous disons que les routeurs sont des appareils de couche 3 et que les commutateurs conventionnels (non-couche 3) sont des appareils de couche 2. Cependant, nous pouvons attribuer une adresse IP à une interface de gestion (SVI) d'un commutateur de couche 2. Comment est-ce possible si les commutateurs sont des périphériques de couche 2?

PARTIE 2

Activité 1 : Comparer les périphériques de couche 2 et de couche 3– Packet Tracer

Réponses

Topologie



- **Etape 1:**

a:

- Le 2960 dispose de 26 ports. Le 3650 dispose de 24 ports fixes et de quatre ports modulaires qui acceptent les modules SFP.
- Le 2960 dispose de 24 ports de commutation Fast Ethernet et de 2 ports Gigabit Ethernet. Le 3650 dispose de 24 ports Gigabit Ethernet fixes et de 4 ports modulaires.
- Les ports de commutation Fast Ethernet prennent en charge des vitesses de 10/100 Mo/s, et les ports de commutation Gigabit Ethernet prennent en charge des vitesses allant jusqu'à 1 000 Mo/s.
- Oui, le 3650.

b:

- Un commutateur de couche 2 prend des décisions de transfert basées sur les adresses L2 (MAC). Les ports de commutation sur les commutateurs de couche 3 peuvent être configurés en tant qu'interfaces avec des adresses IP. Les commutateurs peuvent également être configurés avec des protocoles de routage comme un routeur.
- L'interface physique d'un commutateur est utilisée pour connecter physiquement les périphériques finaux au réseau. Une interface virtuelle commutée (SVI ou VLAN) est utilisée pour configurer le commutateur avec une adresse IP afin qu'il puisse être géré à distance.
- Le 2960 fonctionne sur la couche 2 et le 3650 sur les couches 2 et 3.
- Oui, les ports du D1 sont tous Gigabit Ethernet, tandis que le 2960 possède principalement des ports Fast Ethernet et deux ports Gigabit Ethernet destinés aux liaisons montantes entre les commutateurs. De plus, le D1 a différentes désignations pour ses ports. Le D1 utilise le format stack-module-port. D1 a des ports de commutateur qui sont configurés avec la commande no switchport et affichent une adresse IP et un masque configurés sur les ports G1/1/1 et G1/1/2. De plus, D1 a le routage IP activé avec la commande de routage ip.

PARTIE 2

Activité 1 : Comparer les périphériques de couche 2 et de couche 3– Packet Tracer

Réponses

- Il fonctionne sur D1 car il fonctionne sur les couches 2 et 3, ce qui lui permet de fonctionner comme un commutateur de couche 2 mais en même temps, lui permet d'acheminer les paquets et de prendre des décisions de transfert basées sur les informations de couche 3 (adresses IP) que les commutateurs conventionnels ne peux pas. ASw-1 est un commutateur de couche 2 et n'a donc pas de table de routage.

▪ **Etape 2:**

a:

- Ils ont tous deux un port console, des ports USB et des interfaces Gigabit Ethernet. R1 et D1 sont tous deux modulaires, ce qui signifie que différentes interfaces peuvent être ajoutées. R1 a des interfaces série et asynchrones tandis que D1 n'a que des interfaces Ethernet. D1 peut utiliser Ethernet en cuivre ou en fibre selon les modules présents et R1 peut utiliser différents types de connexion également en fonction des modules utilisés. D1 a beaucoup plus de ports Gigabit Ethernet que R1.
- R1 et D1 ont les mêmes adresses IP configurées sur eux mais sur des interfaces différentes.
- La commande **no switchport**.
- Les codes sont les mêmes sauf que le routeur a un code L pour local. Il s'agit d'un lien configuré sur l'interface physique de R1. La table de routage du commutateur n'a pas ce code. Les deux appareils affichent les mêmes réseaux dans leurs tables de routage.
- Ils ont tous deux configuré OSPF et apprennent les réseaux l'un de l'autre.
- Le réseau 1.1.1.0/24 a été appris à partir de R2.

b:

- Routeur ou commutateur multicouche.
- Un commutateur multicouche peut router entre les réseaux tant qu'il est configuré avec une adresse IP et que le routage IP est activé. Le routage IP doit également être activé si vous prévoyez d'exécuter des protocoles de routage tels que OSPF sur le commutateur. La commande **no switchport** doit être activée sur l'interface afin d'attribuer une adresse IP et un masque de sous-réseau sur l'interface physique du commutateur.
- Les commutateurs gérés de couche 2, tels que Cisco Catalyst 2960, disposent d'un serveur intégré accessible via la couche 3. Le serveur permet l'accès Telnet, SSH ou HTTP au commutateur à partir du réseau afin que le commutateur puisse être géré à distance et configuré. Il est utile de considérer cette fonctionnalité comme distincte de la fonction de transfert de données du commutateur, qui existe au niveau de la couche 2.

TP 2

Implémenter la redondance dans les réseaux commutés sans boucle

Compétences visées :

- Comprendre le fonctionnement du protocole STP
- Configurer le protocole PVST+

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

2 heures

TP 2

Implémenter la redondance dans les réseaux commutés sans boucle

1. Le protocole Spanning Tree (STP)
2. Configuration PVST+

Critères de réussite :

- Le stagiaire est-il capable de :
  - Comprendre et configurer le protocole STP ?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 2

Activité 1 : Investiguer la prévention des boucles de STP– Packet Tracer

- **Objectifs**

Dans ce TP, vous observerez les états du port spanning-tree et observerez le processus de convergence spanning-tree.

- **Décrire le fonctionnement du protocole STP.**
- **Expliquez comment le protocole Spanning Tree empêche les boucles de commutation tout en permettant la redondance dans les réseaux commutés.**

- **Contexte/Scénario**

Dans cette activité, vous allez utiliser Packet Tracer pour observer le fonctionnement du protocole Spanning Tree dans un réseau commuté simple qui a des chemins redondants.

○ Partie 1: Observer une instance de spanning-tree convergée

Etape 1: Vérifier la connectivité

Ping de PC1 à PC2 pour vérifier la connectivité entre les hôtes. La requête ping devrait aboutir.

Etape 2: Afficher l'état de la spanning-tree sur chaque commutateur.

Utilisez la commande **show spanning-tree vlan 1** pour collecter des informations sur l'état de spanning tree de chaque commutateur. Complétez le tableau. Pour les besoins de l'activité, considérez uniquement les informations sur les ports de trunk Gigabit. Les ports Fast Ethernet sont des ports d'accès qui ont des périphériques finaux connectés et ne font pas partie du spanning tree basée sur les trunks inter-commutateurs.

Commutateur	Port	État (FWD, BLK...)	Pont racine?
S1	G0/1		
	G0/2		
S2	G0/1		
	G0/2		
S3	G0/1		
	G0/2		

Packet Tracer utilise un voyant de liaison différent sur l'une des connexions entre les commutateurs.

Questions :

- Que pensez-vous que cette lumière de lien signifie ?
- Quel chemin les trames prendront de PC1 à PC2 ?
- Pourquoi les trames ne passent-elles pas par S3 ?
- Pourquoi spanning tree a-t-il placé un port en état de blocage ?

○ Partie 2: Observer la convergence de spanning-tree

Etape 1: Retirer la connexion entre S1 et S2

a. Ouvrez une fenêtre CLI sur le commutateur S3 et exécutez la commande **show spanning-tree vlan 1**. Laissez la fenêtre CLI ouverte.

Ouvrez la fenêtre de configuration.

Activité 1 : Investiguer la prévention des boucles de STP– Packet Tracer

b. Sélectionnez l'outil de suppression dans la barre de menus et cliquez sur le câble qui relie S1 et S2.

Etape 2: Observer la convergence de spanning-tree

a. Revenez rapidement à l'invite CLI sur le commutateur S3 et exécutez la commande **show spanning-tree vlan 1** .

b. Utilisez la touche flèche vers le haut pour rappeler la commande **show spanning-tree vlan 1** et émettez-la à plusieurs reprises jusqu'à ce que le voyant orange du câble devienne vert. Observez l'état du port G0/2.

Question :

- Que pensez-vous qu'il deviendra le statut du port G0/2 au cours de ce processus ?
- Vous avez observé la transition de l'état du port qui se produit au fur et à mesure qu'un port spanning-tree passe de l'état de blocage à l'état de transfert.

c. Vérifiez la connectivité en pingant de PC1 vers PC2. Votre ping doit être réussi.

Question :

- Y a-t-il des ports affichant un voyant de liaison orange indiquant que le port est dans un état spanning-tree autre que le transfert ? Les stagiaires doivent justifier la réponse.

Activité 1 : Investiguer la prévention des boucles de STP– Packet Tracer

Réponses

- **Partie 1 / Etape 2:**

Commutateur	Port	État (FWD, BLK...)	Pont racine?
S1	G0/1	FWD	No
	G0/2	FWD	No
S2	G0/1	FWD	Yes
	G0/2	FWD	Yes
S3	G0/1	FWD	No
	G0/2	BLK	No

- Il indique que le port ne transfère pas de trames car il est dans un état spanning-tree, dans ce cas l'état bloquant.

- Ils passeront de S1 à S2.

- La raison principale est que le spanning tree a placé le port G0/2 sur S3 en mode bloquant. Aucune trame n'est envoyée ou reçue sur ce port.

- Si tous les ports pouvaient transmettre des trames, une boucle de commutation existerait dans le réseau. Les boucles de commutation peuvent dégrader les performances du réseau et même entraîner la défaillance d'un réseau.

- **Partie 2 / Etape 2:**

b: D'abord c'était BLK, il est ensuite devenu LSN (écoute), puis LRN (apprentissage), et enfin FWD pour la transmission.

c: Aucun voyant de liaison orange n'est affiché car il ne s'agit plus de chemins redondants dans le réseau.

PARTIE 2

TP 2

Implémenter la redondance dans les réseaux commutés sans boucle

1. Le protocole Spanning Tree (STP)
2. Configuration de PVST+

Critères de réussite :

- Le stagiaire est-il capable de :
  - Comprendre et configurer le protocole STP ?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 2

Activité 1 : configuration du protocole Rapid PVST+– Packet Tracer

- **Objectifs**

- **Partie 1 : configuration des VLAN**
- **Partie 2 : configuration du protocole RSTP PVST+ et de l'équilibrage de la charge**
- **Partie 3 : configuration de PortFast et de la protection BPDU**

- **Contexte/Scénario**

Au cours de cet exercice, vous allez configurer les VLAN et les trunks, le protocole Rapid Spanning Tree PVST+ et les ponts racines principaux et secondaires, puis examiner les résultats de la configuration. Vous optimiserez également le réseau en configurant PortFast et la protection BPDU sur les ports de périphérie.

- **Topologie**

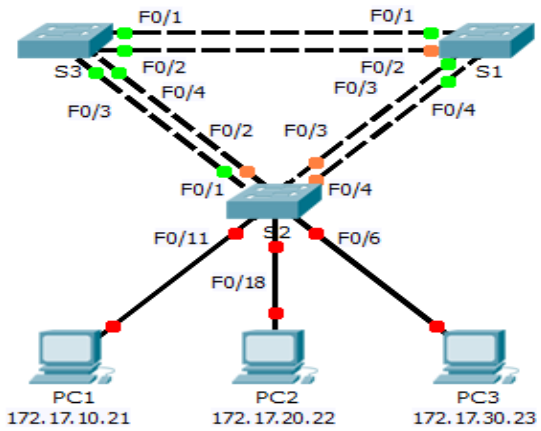


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	Carte réseau	172.17.10.21	255.255.255.0	172.17.10.254
PC2	Carte réseau	172.17.20.22	255.255.255.0	172.17.20.254
PC3	Carte réseau	172.17.30.23	255.255.255.0	172.17.30.254

Caractéristiques d'attribution des ports de commutation

Ports	Affectations	Réseau
S2 F0/6	VLAN 30	172.17.30.0/24
S2 F0/18	VLAN 20	172.17.20.0/24
S2 F0/11	VLAN 10	172.17.10.0/24

- **Partie 1: configuration des VLAN**

Etape 1: Activez les ports utilisateur sur S2 en mode d'accès.

Reportez-vous au schéma de topologie pour déterminer quels ports de commutation sur **S2** sont activés pour l'accès aux périphériques de l'utilisateur final. Ces trois ports seront configurés pour le mode d'accès et activés avec la commande **no shutdown**.

Questions :

Activité 1 : configuration du protocole Rapid PVST+– Packet Tracer

```
S2(config)# interface range f0/6,f0/11,f0/18
S2(config-if-range)# switchport mode access
S2(config-fi-range)# no shutdown
```

Etape 2: Créez des VLAN.

À l'aide de la commande appropriée, créez les VLAN 10, 20, 30, 40, 50, 60, 70, 80 et 99 sur l'ensemble des commutateurs.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 20
S1(config-vlan)# vlan 30
S1(config-vlan)# vlan 40
S1(config-vlan)# vlan 50
S1(config-vlan)# vlan 60
S1(config-vlan)# vlan 70
S1(config-vlan)# vlan 80
S1(config-vlan)# vlan 99
```

```
S2(config)# vlan 10
S2(config-vlan)# vlan 20
S2(config-vlan)# vlan 30
S2(config-vlan)# vlan 40
S2(config-vlan)# vlan 50
S2(config-vlan)# vlan 60
S2(config-vlan)# vlan 70
S2(config-vlan)# vlan 80
S2(config-vlan)# vlan 99
```

```
S3(config)# vlan 10
S3(config-vlan)# vlan 20
S3(config-vlan)# vlan 30
S3(config-vlan)# vlan 40
S3(config-vlan)# vlan 50
S3(config-vlan)# vlan 60
S3(config-vlan)# vlan 70
S3(config-vlan)# vlan 80
S3(config-vlan)# vlan 99
```

PARTIE 2

Activité 1 : configuration du protocole Rapid PVST+– Packet Tracer

Etape 2: Attribuez des VLAN aux ports de commutation.

Les affectations de ports sont indiquées dans la table au début de cet exercice. Enregistrez vos configurations après l'attribution des ports de commutation aux VLAN.

```
S2(config)# interface f0/6
S2(config-if)# switchport access vlan 30
S2(config-if)# interface f0/11
S2(config-if)# switchport access vlan 10
S2(config-if)# interface f0/18
S2(config-if)# switchport access vlan 20
```

Etape 3: Vérifiez les VLAN.

Utilisez la commande **show vlan brief** sur tous les commutateurs afin de vérifier que tous les réseaux VLAN sont inscrits dans la table VLAN.

Etape 4: Attribuez les trunks au VLAN 99 natif.

Utilisez la commande appropriée pour configurer les ports F0/1 à F0/4 sur chaque commutateur en tant que ports trunk, et attribuez ces ports trunk au VLAN 99 natif.

```
S1(config)# interface range f0/1-4
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99
S2(config)# interface range f0/1-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S3(config)# interface range f0/1-4
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
```

Etape 5: Configurez l'interface de gestion sur les trois commutateurs munis d'une adresse.

```
S1(config)# interface vlan99
S1(config-if)# ip address 172.17.99.11 255.255.255.0
S2(config)# interface vlan99
S2(config-if)# ip address 172.17.99.12 255.255.255.0
S3(config)# interface vlan99
S3(config-if)# ip address 172.17.99.13 255.255.255.0
```

Vérifiez que les commutateurs sont configurés correctement en envoyant des requêtes ping entre eux.

PARTIE 2

Activité 1 : configuration du protocole Rapid PVST+– Packet Tracer

- **Partie 2: Configuration du protocole RSTP PVST+ et de l'équilibrage de la charge**

Faute d'être révolutionnaire, le protocole RSTP (Rapid Spanning Tree Protocol, IEEE 802.1w) est une évolution de la norme 802.1D. Grosso modo, la terminologie 802.1D reste la même. La plupart des paramètres ont été conservés de façon à ce que les utilisateurs déjà familiarisés avec la norme 802.1D puissent rapidement configurer le nouveau protocole. Dans la plupart des cas, le protocole RSTP fonctionne mieux que les extensions propriétaires de Cisco sans aucune configuration supplémentaire. Il est également possible de revenir à la norme 802.1D à partir de la norme 802.1w de façon à interagir avec les anciens ponts en fonction de chaque port.

Etape 1: Configurez le mode STP.

Utilisez la commande **spanning-tree mode** pour configurer les commutateurs de telle sorte qu'ils utilisent Rapid PVST en tant que mode STP.

Etape 2: Configurez RSTP PVST+ et l'équilibrage de la charge.

Configurez **S1** en tant que pont racine principal pour les VLAN 1, 10, 30, 50 et 70. Configurez **S3** en tant que pont racine principal pour les VLAN 20, 40, 60, 80 et 99. Configurez **S2** en tant que racine secondaire pour tous les VLAN.

Vérifiez vos configurations à l'aide de la commande **show spanning-tree**.

- **Partie 3: Configuration de PortFast et de la protection BPDU**

Etape 1: Configurez PortFast sur S2.

PortFast permet à un port de passer presque immédiatement en état de transmission, diminuant ainsi considérablement la durée des états d'écoute et d'apprentissage. PortFast minimise le temps nécessaire à la mise en ligne du serveur ou de la station de travail. Configurez PortFast sur les interfaces **S2** connectées aux PC.

Etape 2: Configurez la protection BPDU sur S2.

L'amélioration de la protection des unités BPDU du protocole STP PortFast permet aux concepteurs de réseau d'appliquer les frontières de domaine STP et de conserver la topologie active prévisible. Les périphériques situés derrière les ports et dont le mode PortFast du protocole STP est activé ne peuvent pas influencer la topologie STP. Lors de la réception des BPDU, le fonctionnement de la protection BPDU désactive le port sur lequel le mode PortFast a été configuré. La protection BPDU fait passer le port à l'état err-disable et un message s'affiche sur la console. Configurez la protection BPDU sur les interfaces **S2** connectées aux PC.

Etape 3: Vérifiez votre configuration.

Utilisez la commande **show run** pour vérifier votre configuration.

PARTIE 2

Activité 1 : configuration du protocole Rapid PVST+– Packet Tracer

Réponses

Partie 2 / Etape 1 :

```
S1(config)# spanning-tree mode rapid-pvst

S2(config)# spanning-tree mode rapid-pvst

S3(config)# spanning-tree mode rapid-pvst
```

Partie 2 / Etape 2 :

```
S1(config)# spanning-tree vlan 1,10,30,50,70 root primary

S2(config)# spanning-tree vlan 1,10,20,30,40,50,60,70,80,99
root secondary

S3(config)# spanning-tree vlan 20,40,60,80,99 root primary
```

Partie 3 / Etape 1 :

```
S2(config)# interface range f0/6 , f0/11 , f0/18
S2(config-if-range)# spanning-tree portfast
```

Partie 3 / Etape 2 :

```
S2(config)# interface range f0/6 , f0/11 , f0/18
S2(config-if-range)# spanning-tree bpduguard enable
```

TP 3

Configurer l'agrégation des liaisons

Compétences visées :

- Configurer l'agrégation des liaisons avec ETHERCHANNEL

Recommandations clés:

- Lire attentivement l’énoncé et les questions
- Se référer au cours

3 heures

TP 3

Configurer l'agrégation des liaisons

1. Configuration d’ EtherChannel

Critères de réussite :

- Le stagiaire est-il capable de :
  - Comprendre configurer la technologie EtherChannel?
- Réponses correctes pour au moins 70 % des questions.

03 -Configurer l'agrégation des liaisons

Configuration d' EtherChannel

PARTIE 2

Activité 1 : Configurer EtherChannel– Packet Tracer

- **Objectifs**

- **Partie 1 : configuration des paramètres de base du commutateur**
- **Partie 2 : configuration d'un réseau EtherChannel avec Cisco PAgP**
- **Partie 3 : configuration d'un réseau EtherChannel LACP 802.3ad**
- **Partie 4 : configuration d'une liaison EtherChannel redondante**

- **Contexte**

Trois commutateurs viennent d'être installés. Il existe des liaisons ascendantes redondantes entre les commutateurs. Tel que configuré, un seul de ces liens peut être utilisé ; sinon, une boucle de bridging pourrait se produire. Toutefois, l'utilisation d'une seule liaison consomme uniquement la moitié de la bande passante disponible. EtherChannel permet de grouper jusqu'à huit liaisons redondantes au sein d'une seule liaison logique. Au cours de ces travaux pratiques, vous allez configurer le protocole d'agrégation de ports (PAgP), un protocole Cisco EtherChannel et le protocole LACP (Link Aggregation Control Protocol), une version ouverte de la norme IEEE 802.3ad d'EtherChannel.

Avant de commencer la configuration, consultez les directives et restrictions de configuration EtherChannel énumérées à la fin de cette activité.

- **Tableau de Port-Channel**

Groupe de canaux	Ports	Protocole
1	S1 F0/21. F0/22 S3 F0/21, F0/22	PAgP
2	S1 G0/1, G0/2 S2 G0/1, G0/2	LACP
3	S2 F0/23, F0/24 S3 F0/23, F0/24	LACP négocié

- **Instructions**

- **Partie 1: Configuration des paramètres de base du commutateur**

a. Attribuez à chaque commutateur un nom d'hôte selon le diagramme de topologie.

b. Avant de commencer l'agrégation de liens entre les commutateurs, vérifiez la configuration existante des ports qui connectent les commutateurs pour vous assurer que les ports rejoignent correctement les EtherChannels. Les commandes qui fournissent des informations sur l'état des ports de commutateur sont les suivantes:

   - S1# **show interfaces | include Ethernet**
   - S1# **show interface status**
   - S1# **show interfaces trunk**

c. Configurez tous les ports requis pour les EtherChannels en tant que ports de trunk statiques.

Remarque: si les ports sont configurés en mode automatique dynamique DTP, et que vous ne réglez pas le mode des ports sur trunk, les liens ne forment pas de trunks et restent des ports d'accès. Le mode par défaut sur un commutateur 2960 est l'activation du DTP et le réglage sur l'auto dynamique. La fonction DTP peut être désactivée sur les interfaces avec la commande **switchport nonegotiate**.

Activité 1 : Configurer EtherChannel– Packet Tracer

- **Partie 2: Configuration d'un réseau EtherChannel avec Cisco PAgP**

Remarque: lors de la configuration des EtherChannels, il est recommandé de fermer les ports physiques regroupés sur les deux appareils avant de les configurer en groupes de canaux. Sinon, EtherChannel Misconfig Guard peut placer ces ports dans un état de désactivation par erreur. Les ports et les canaux de port peuvent être de nouveau activés après la configuration d'EtherChannel.

Etape 1: Configuration du port-channel 1

a. Le premier EtherChannel qui est créé pour cette activité regroupe les ports F0/21 et F0/22 entre **S1** et **S3**. Configurez les ports des deux commutateurs comme des ports de trunk statiques.

Ouvrez la fenêtre de configuration.

b. Utilisez la commande **show interfaces trunk** pour vous assurer que vous avez un lien trunk actif pour ces deux liens, et que le VLAN natif sur les deux liens est le même.

- S1# **show interfaces trunk**

```
Port Mode Encapsulation Status Native vlan
F0/21 on 802.1q trunking 1
F0/22 on 802.1q trunking 1
G0/1 on 802.1q trunking 1
G0/2 on 802.1q trunking 1

<output omitted>
```

c. Sur S1 et S3, ajoutez les ports F0/21 et F0/22 au canal de port 1 avec la commande **channel-group 1 mode desirable** . L'option **mode desirable** permet au commutateur d'activer la négociation active en vue de former une liaison PAgP.

Remarque: Les interfaces doivent être **shutdown** avant de les ajouter au groupe de canaux.

- S1(config)# **interface range f0/21 – 22**
- S1(config-if-range)# **shutdown**
- S1(config-if-range)# **channel-group 1 mode desirable**
- S1(config-if-range)# **no shutdown**

- S3(config)# **interface range f0/21 - 22**
- S3(config-if-range)# **shutdown**
- S3(config-if-range)# **channel-group 1 mode desirable**
- S3(config-if-range)# **no shutdown**

Le message “Creating a port-channel interface Port-channel 1” doit apparaître sur les deux commutateurs lorsque le groupe de canaux est configuré. Cette désignation d'interface apparaîtra sous la forme Po1 dans la sortie de commande.

d. Configurez l'interface logique pour qu'elle devienne un trunk en entrant d'abord la commande **interface port-channel** *number*, puis la commande **switchport mode trunk** . Ajoutez cette configuration aux deux commutateurs.

- S1(config)# **interface port-channel 1**
- S1(config-if)# **switchport mode trunk**

- S3(config)# **interface port-channel 1**
- S3(config-if)# **switchport mode trunk**

PARTIE 2

PARTIE 2

Activité 1 : Configurer EtherChannel– Packet Tracer

Etape 2: Vérification de l'état du port-channel 1

a. Lancer la commande **show etherchannel summary** sur S1 et S3 pour vérifier que EtherChannel fonctionne sur les deux commutateurs. Cette commande affiche le type d'EtherChannel, les ports utilisés et les états des ports. La sortie de commande est affichée pour S1.

- S1# **show etherchannel summary**

```
Flags: D - down P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3 S - Layer2
        U - in use f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------
1 Po1(SU) PAgP F0/21(P) F0/22(P)
```

b. Si EtherChannel ne s'affiche pas, arrêtez les interfaces physiques aux deux extrémités d'EtherChannel, puis activez-les de nouveau. Les commandes show interfaces trunk et show spanning-tree doivent montrer le canal du port comme un lien logique.

○ Partie 3: Configuration d'un réseau EtherChannel LACP 802.3ad

Etape 1: Configuration du port-channel 2

a. En 2000, l'IEEE a publié la version 802.3ad, qui est une version standard ouverte d'EtherChannel. Il est communément appelé LACP. En utilisant les commandes précédentes, configurez le lien entre **S1** et **S2,**, en utilisant les ports G0/1 et G0/2, comme un EtherChannel LACP. Vous devez utiliser un numéro de canal de port sur **S1** différent de 1, car vous l'avez déjà utilisé à l'étape précédente. Pour configurer le canal 2 du port en tant que LACP, utilisez la commande de configuration de l'interface mode **channel-group** *2* **mode active** . Le mode actif indique que le commutateur tente activement de négocier ce lien comme LACP, par opposition à PAgP. La configuration de S1 est affichée ci-dessous.

- S1(config)# **interface range g0/1 - 2**
- S1(config-if-range)# **shutdown**
- S1(config-if-range)# **channel-group 2 mode active**
- S1(config-if-range)# **no shutdown**
- S1(config-if-range)# **interface port-channel 2**
- S1(config-if)# **switchport mode trunk**

Etape 2: Vérification de l'état du port-channel 2

Utilisez la commande **show** de la Partie 1 Étape 2 pour vérifier l'état du port-channel 2. Identifiez le protocole utilisé par chaque port.

Activité 1 : Configurer EtherChannel– Packet Tracer

- **Partie 3: Configuration d'une liaison EtherChannel redondante**

Etape 1: Configuration du port-channel 3

Il existe différentes options pour la commande **channel-group** *number* **mode** :

- S2(config)# **interface range f0/23 - 24**
- S2(config-if-range)# **channel-group 3 mode ?**

```
active Enable LACP unconditionally
  auto Enable PAgP only if a PAgP device is detected
  desirable Enable PAgP unconditionally
  on Enable Etherchannel only
  passive Enable LACP only if a LACP device is detected
```

a. Sur le commutateur **S2**, ajoutez les ports F0/23 et F0/24 au port-channel 3 avec la commande **channel-group 3 mode passive**. L'option **passive** indique que vous souhaitez que le commutateur utilise LACP uniquement si un autre périphérique LACP est détecté. Configurez le port-channel 3 de manière statique en tant qu'interface trunk.

- S2(config)# **interface range f0/23 - 24**
- S2(config-if-range)# **shutdown**
- S2(config-if-range)# **channel-group 3 mode passive**
- S2(config-if-range)# **no shutdown**
- S2(config-if-range)# **interface port-channel 3**
- S2(config-if)# **switchport mode trunk**

b. Sur **S3**, ajoutez les ports F0/23 et F0/24 au port Canal 3 avec la commande **channel-group 3 mode active** . L'option **active** indique que vous souhaitez que le commutateur utilise LACP sans condition. Configurez le port-channel 3 de manière statique en tant qu'interface trunk.

Etape 2: Vérification de l'état du canal de port 3

a. Utilisez la commande **show** de la Partie 1 Étape 2 pour vérifier l'état du port-channel 3. Identifiez le protocole utilisé par chaque port.

b. La création de liens EtherChannel n'empêche pas Spanning Tree de détecter les boucles de commutation. Affichez l'état de l'arborescence des ports actifs sur **S1**.

- S1# **show spanning-tree active**

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID Priority 32769
            Address 0001.436E.8494
            Cost 9
            Port 27(Port-channel1)
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
            Address 000A.F313.2395
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 20
```

PARTIE 2

Activité 1 : Configurer EtherChannel– Packet Tracer

```
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- --------
Po1 Root FWD 9 128.27 Shr
Po2 Altn BLK 3 128.28 Shr
```

Le port Channel 2 n'est pas opérationnel car le protocole Spanning Tree a placé certains ports en mode de blocage. Malheureusement, ces ports étaient les ports Gigabit. Dans cette topologie, vous pouvez restaurer ces ports en configurant **S1** comme racine **principale** pour VLAN 1. Vous pouvez également définir la priorité sur **24576**.

- S1(config)# **spanning-tree vlan 1 root primary**

ou

- S1(config)# **spanning-tree vlan 1 priority 24576**

Vous devrez peut-être attendre que STP recalcule la topologie de tree. Appuyez sur l'avance rapide si nécessaire. Utilisez la commande **show spanning-tree active** pour vérifier que les ports Gigabit sont maintenant en état de transfert.

- **Instructions et restrictions de configuration d'EtherChannel**

EtherChannel a quelques directives spécifiques qui doivent être suivies afin d'éviter les problèmes de configuration.

1. Toutes les interfaces Ethernet prennent en charge EtherChannel jusqu'à un maximum de huit interfaces sans exiger que les interfaces soient sur le même module d'interface.
2. Toutes les interfaces d'un EtherChannel doivent fonctionner à la même vitesse et au même duplex.
3. Les liaisons EtherChannel peuvent fonctionner comme des ports d'accès VLAN uniques ou comme des liaisons de trunk entre les commutateurs.
4. Toutes les interfaces d'un EtherChannel de couche 2 doivent être membres du même VLAN ou être configurées en tant que trunks.
5. Si configuré en tant que liaisons de trunk, EtherChannel de couche 2 doit avoir le même VLAN natif et avoir les mêmes VLAN autorisés sur les deux commutateurs connectés au trunk.
6. Lors de la configuration des liaisons EtherChannel, toutes les interfaces doivent être arrêtées avant de commencer la configuration EtherChannel. Une fois la configuration terminée, les liens peuvent être réactivés.
7. Après avoir configuré l'EtherChannel, vérifiez que toutes les interfaces sont dans l'état up/up.
8. Il est possible de configurer un EtherChannel comme statique, ou d'utiliser PAGP ou LACP pour négocier la connexion EtherChannel. La détermination de la configuration d'un EtherChannel est la valeur de la commande de **channel-group** *number* **mode**. Les valeurs valides sont les suivantes :

PARTIE 2

Activité 1 : Configurer EtherChannel– Packet Tracer

Active LACP est activé sans condition

passive Le LACP n'est activé que si un autre appareil compatible LACP est connecté.

Desirable PAgP est activé sans condition

Auto PAgP n'est activé que si un autre appareil compatible avec le PAgP est connecté.

sur EtherChannel est activé, mais sans LACP ni PAGP.

9. Les ports LAN peuvent former un EtherChannel à l'aide de PAgP si les modes sont compatibles. Les modes PAgP compatibles sont :
   - **desirable => desirable**
   - **desirable => auto**

   Si les deux interfaces sont en mode **automatique** , un Etherchannel ne peut pas se former.

10. Les ports LAN peuvent former un EtherChannel à l'aide de LACP si les modes sont compatibles. Les modes LACP compatibles sont :
    - **active => active**
    - **active => passive**

    Si les deux interfaces sont en mode **passive** , un EtherChannel ne peut pas se former à l'aide de LACP.

11. Les numéros de groupe de canaux sont locaux au commutateur individuel. Bien que cette activité utilise le même numéro de groupe de canaux à chaque extrémité de la connexion EtherChannel, elle n'est pas obligatoire. Le groupe de canaux 1 (interface po1) sur un commutateur peut former un EtherChannel avec le groupe de canaux 5 (interface po5) sur un autre commutateur.

PARTIE 2

Activité 1 : Configurer EtherChannel– Packet Tracer

Réponses

- **Partie 3 / Etape 1:**

a:

```
S2(config)# interface range g0/1 – 2
S2(config-if-range)# shutdown
S2(config-if-range)# channel-group 2 mode active
S2(config-if-range)# no shutdown
S2(config-if-range)# interface port-channel 2
S2(config-if)# switchport mode trunk
```

- **Partie 3 / Etape 2:**

```
S1# show etherchannel summary
```

- **Partie 4 / Etape 2:**

```
S2# show etherchannel summary
```

Configuration

Switch S3

```
enable
config terminal
hostname S3
interface range f0/21 – 22
 switchport mode trunk
 shutdown
 channel-group 1 mode desirable
 no shutdown
interface port-channel 1
 switchport mode trunk
interface range f0/23 – 24
 switchport mode trunk
 shutdown
 channel-group 3 mode active
 no shutdown
interface port-channel 3
 switchport mode trunk
end
```

Switch S2

```
enable
config terminal
hostname S2
interface range g0/1 – 2
 switchport mode trunk
 shutdown
 channel-group 2 mode active
 no shutdown
interface port-channel 2
 switchport mode trunk
interface range f0/23 – 24
 switchport mode trunk
 shutdown
 channel-group 3 mode passive
 no shutdown
interface port-channel 3
 switchport mode trunk
 end
```

Switch S1

```
enable
config terminal
hostname S1
interface range f0/21 – 22
 switchport mode trunk
 shutdown
 channel-group 1 mode desirable
 no shutdown
interface port-channel 1
 switchport mode trunk
interface range g0/1 – 2
 switchport mode trunk
 shutdown
 channel-group 2 mode active
 no shutdown
interface port-channel 2
 switchport mode trunk
spanning-tree vlan 1 root primary
end
```

Activité 2 : Dépannage d'EtherChannel – Packet Tracer

- **Objectifs**

- **Partie 1: Examen de la couche physique et résolution des problèmes de mode de port de commutateur**
- **Partie 2: Identification et correction des erreurs d'attribution de port-channel**
- **Partie 3: Identification et correction des erreurs de protocole de port-channel**

- **Contexte**

Quatre commutateurs ont été récemment configurés par un technicien junior. Les utilisateurs se plaignent de la lenteur du réseau et ils aimeraient que vous meniez une enquête.

- **Tableau de Port-Channel**

Groupe de canaux	Ports	Protocole
1	S1: G0/1, G0/2 S2: G0/1, G0/2	LACP actif
2	S2: G0/1, G0/2 S4: G0/1, G0/2	LACP actif
3	S1: F0/23, F0/24 S2: F0/23, F0/24	LACP actif
4	S3: F0/23, F0/24 S4: F0/23, F0/24	LACP actif
5	S1: F0/21, F0/22 S4: F0/21, F0/22	LACP actif
6	S2: F0/21, F0/22 S3: F0/21, F0/22	LACP actif

- **Tableau de Périphérique**

Périphérique	Groupe	Ports
S1	1	G0/1, G0/2
S1	3	F0/23, F0/24
S1	5	F0/21, F0/22
S2	2	G0/1, G0/2
S2	3	F0/23, F0/24
S2	6	F0/21, F0/22
S3	1	G0/1, G0/2
S3	4	F0/23, F0/24
S3	6	F0/21, F0/22
S4	2	G0/1, G0/2
S4	4	F0/23, F0/24
S4	5	F0/21, F0/22

PARTIE 2

Activité 2 : Dépannage d'EtherChannel – Packet Tracer

- **Instructions**

  - **Partie 1: Examen de la couche physique et résolution des problèmes de mode de port de commutateur**

Etape 1: Recherchez des ports d'accès

Examinez les commutateurs. Lorsque deux liaisons redondantes ou plus connectent les mêmes commutateurs, le protocole Spanning Tree ne met qu'un port en mode de transfert pour empêcher les boucles de commutation. Vous pouvez le voir dans Packet Tracer. Lorsque des ports physiques sont attribués à un port EtherChannel, ils se comportent comme un port logique unique. Chaque paire sera opérationnelle ou désactivée.

Etape 2: Vérifiez que les ports sont en mode de trunk

a. Vérifiez que tous les ports physiques de la topologie sont configurés comme des trunks. Corrigez ceux qui sont en mode d'accès.

b. Corrigez les ports EtherChannel qui ne sont pas configurés comme des trunks.

Partie 2: Identification et correction des erreurs d'attribution de port-channel

Etape 1: Examinez les attributions de port-channel

La topologie Packet Tracer et les tableaux de port-channel et de périphérique fournissent des détails sur les ports physiques et leurs attributions EtherChannel. Utilisez la commande **show etherchannel summary** pour savoir comment les liaisons Etherchannel sont configurés. Vérifiez que les commutateurs sont configurés comme indiqué dans la documentation.

Etape 2: Corrigez les attributions de port-channel

Corrigez les ports qui ne sont pas attribués au port EtherChannel approprié.

- **Partie 3: Identification et correction des erreurs de protocole de port-channel**

Etape 1: Identifiez les problèmes de protocole

En 2000, l'IEEE a publié la version 802.3ad (LACP), qui est une version standard ouverte d'EtherChannel. Pour des raisons de compatibilité, l'équipe de conception réseau a choisi d'utiliser le protocole LACP sur le réseau. L'équipe de conception a exigé que tous les ports participant à EtherChannel négocient activement la liaison en tant que LACP. Vérifiez que les ports physiques sont configurés conformément à la topologie et le tableau de port-channel.

Etape 2: Corrigez les problèmes de protocole

a. Corrigez les ports de commutateur qui ne négocient pas à l'aide du protocole LACP.

b. Ré-exécutez la commande **show etherchannel summary** pour vérifier que toutes les liaisons EtherChannel sont désormais correctement configurées.

Activité 2 : Dépannage d'EtherChannel – Packet Tracer

Réponses

- **Partie 1 / Etape 1:**

a:
```
S2(config)# interface range f0/21 – 24, g0/1-2
S2(config-if-range)# switchport mode trunk
```

b: -
```
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
```

-
```
S2(config)# interface port-channel 2
S2(config-if)# switchport mode trunk
S2(config-if)# interface port-channel 3
S2(config-if)# switchport mode trunk
S2(config-if)# interface Port-channel 6
S2(config-if)# switchport mode trunk
```

- **Partie 2 / Etape 1 :**

```
S1# show etherchannel summary
S2# show etherchannel summary
S3# show etherchannel summary
S4# show etherchannel summary
```

Partie 2 / Etape 2:

```
S4(config)# interface range f0/21 – 22
S4(config-if-range)# channel-group 5 mode active
```

Partie 3 / Etape 1:

```
S3# show etherchannel summary
```

Partie 3 / Etape 2:

a:
```
S3(config)# interface range g0/1 – 2
S3(config-if-range)# no channel-group
S3(config-if-range)# channel-group 1 mode active
S3(config-if-range)# interface range f0/21 – 22
S3(config-if-range)# no channel-group
S3(config-if-range)# channel-group 6 mode active
S3(config-if-range)# interface range f0/23 – 24
S3(config-if-range)# no channel-group
S3(config-if-range)# channel-group 4 mode active
```

PARTIE 2

TP 4

Comprendre le concept du FHRP

Compétences visées :

- Configurer le protocole HSRP

Recommandations clés:

- Lire attentivement l’énoncé et les questions
- Se référer au cours

2 heures

TP 4

Comprendre le concept du FHRP

1. Configuration du protocole HSRP

Critères de réussite :

- Le stagiaire est-il capable de :
  - Comprendre configurer la technologie HSRP?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 2

Activité 1 : Guide de configuration HSRP– Packet Tracer

Objectifs

Dans cette activité Packet Tracer, vous apprendrez comment configurer Hot Standby Router Protocol (HSRP) pour fournir des périphériques de passerelle par défaut redondants aux hôtes des réseaux locaux. Après avoir configuré HSRP, vous testez la configuration pour vérifier que les hôtes peuvent utiliser la passerelle par défaut redondante si le périphérique de passerelle actuel devient indisponible.

- **Configurez un routeur actif HSRP.**
- **Configurez un routeur de secours HSRP.**
- **Vérifiez le fonctionnement du protocole HSRP.**

Contexte/scénario

Le protocole Spanning Tree assure une redondance sans boucle entre les commutateurs d'un réseau local. Cependant, il ne fournit pas de passerelles redondantes par défaut pour les appareils des utilisateurs finaux au sein du réseau si un routeur de passerelle tombe en panne. Les FHRP (First Hop Redundancy Protocols) fournissent des passerelles redondantes par défaut pour les dispositifs finaux sans qu'aucune configuration supplémentaire de l'utilisateur final ne soit nécessaire. En utilisant un FHRP, deux ou plusieurs routeurs peuvent partager la même adresse IP virtuelle et la même adresse MAC et peuvent agir comme un seul routeur virtuel. Les hôtes du réseau sont configurés avec une adresse IP partagée comme passerelle par défaut. Dans cette activité Packet Tracer, vous allez configurer le protocole HSRP (Hot Standby Router Protocol) de Cisco, qui est un FHRP.

Vous allez configurer HSRP sur les routeurs R1 et R3, qui servent de passerelles par défaut pour les hôtes sur LAN 1 et LAN 2. Lorsque vous configurez HSRP, vous allez créer une passerelle virtuelle qui utilise la même adresse de passerelle par défaut pour les hôtes des deux réseaux locaux.

Si un routeur de passerelle devient indisponible, le second routeur prend le relais en utilisant la même adresse de passerelle par défaut que celle utilisée par le premier routeur. Étant donné que les hôtes sur les réseaux locaux sont configurés avec l'adresse IP de la passerelle virtuelle comme passerelle par défaut, les hôtes retrouvent la connectivité aux réseaux distants une fois que HSRP active le routeur restant.

Table d'adressage

Appareil	Interface	Adresse IP	Passerelle par défaut
R1	G0/0	10.1.1.1/30	N/A
	G0/1	192.168.1.1/24	N/A
	G0/2	10.1.1.9/30	N/A
R2	G0/0	10.1.1.2/30	N/A
	G0/1	10.1.1.5/30	N/A
	G0/2	10.100.100.1/30	N/A
R3	G0/0	192.168.1.3/24	N/A
	G0/1	10.1.1.6/30	N/A
	G0/2	10.1.1.10/30	N/A
I-Net	G0/1	10.100.100.2/30	N/A
Passerelle virtuelle HSRP	Virtuel	192.168.1.254/24	N/A
S1	VLAN 1	192.168.1.11/24	192.168.1.1
S3	VLAN 1	192.168.1.13/24	192.168.1.3
PC-A	Carte réseau	192.168.1.101/24	192.168.1.1
PC-B	Carte réseau	192.168.1.103/24	192.168.1.3
Serveur web	Carte réseau	209.165.200.226/27	209.165.100.225

Remarque: Le routeur I-Net est présent dans le cloud Internet et n'est pas accessible dans cette activité.

PARTIE 2

Activité 1 : Guide de configuration HSRP– Packet Tracer

- **Instructions**

Partie 1: Vérification de la connectivité

Etape 1: Tracez le chemin d'accès au serveur Web depuis le PC-A

a. Accédez au bureau de PC-A et ouvrez une invite de commandes.

b. Suivez le chemin d'accès depuis PC-A vers le serveur Web en exécutant la commande **tracert 209.165.200.226** .

Quels périphériques se trouvent sur le chemin d'accès de PC-A au serveur Web ? Utilisez la table d'adressage pour déterminer les noms de périphériques.

Etape 2: Tracez le chemin d'accès au serveur Web depuis le PC-B

Répétez le processus à l'étape 1 de PC-B.

Question :

- Quels périphériques se trouvent sur le chemin d'accès de PC-B au serveur Web ?

Etape 3: Observez le comportement du réseau lorsque R3 devient indisponible

a. Sélectionnez l'outil de suppression dans la barre d'outils Packet Tracer et supprimez le lien entre **R3** et **S3** .

b. Ouvrez une invite de commandes sur PC-B. Exécutez la commande **tracert** avec le serveur Web comme destination.

c. Comparez la sortie actuelle avec la sortie de la commande de l'étape 2.

Question :

- Quels sont les résultats ?

d. Cliquez sur l'icône **Connexions** située dans le coin inférieur gauche de la fenêtre Packet Tracer. Recherchez et sélectionnez l'icône **Copper Strait-Through** dans la palette des types de connexion.

e. Cliquez sur **S3** et sélectionnez le port **Gigbitethernet0/2** . Cliquez sur **R3** et sélectionnez le port **Gigabitethernet0/0** .

f. Une fois que les voyants de liaison sur la connexion sont tous les deux verts, testez la connexion en ping sur le serveur Web. La requête ping devrait aboutir.

Partie 2: Configurer les routeurs actifs et de secours HSRP

Etape 1: Configurez HSRP sur R1

a. Configurez HSRP sur l'interface LAN G0/1 de R1.

- R1(config)# **interface g0/1**

b. Spécifiez le numéro de version du protocole HSRP. La version la plus récente est la version **2**.

Remarque : La version de secours 1 ne prend en charge que l'adressage IPv4.

- R1(config-if)# **standby version 2**

c. Configurez l'adresse IP de la passerelle virtuelle par défaut. Cette adresse doit être configurée sur tous les hôtes qui nécessitent les services de la passerelle par défaut. Il remplace l'adresse de l'interface physique du routeur qui a été précédemment configuré sur les hôtes.

Activité 1 : Guide de configuration HSRP– Packet Tracer

Plusieurs instances de HSRP peuvent être configurées sur un routeur. Vous devez spécifier le numéro de groupe HSRP pour identifier l'interface virtuelle entre les routeurs d'un groupe HSRP. Ce nombre doit être cohérent entre les routeurs du groupe. Le numéro de groupe pour cette configuration est 1.

- R1(config-if)# **standby 1 ip 192.168.1.254**

d. Désignez le routeur actif pour le groupe HSRP. C'est le routeur qui sera utilisé comme périphérique de passerelle à moins qu'il ne tombe en panne ou que le chemin d'accès ne devienne inactif ou inutilisable. Spécifiez la priorité de l'interface du routeur. La valeur par défaut est 100. Une valeur plus élevée déterminera quel routeur est le routeur actif. Si les priorités des routeurs dans le groupe HSRP sont les mêmes, le routeur avec l'adresse IP configurée la plus élevée deviendra le routeur actif.

- R1(config-if)# **standby 1 priority 150**

R1 fonctionnera en tant que routeur actif et le trafic des deux réseaux locaux l'utilisera comme passerelle par défaut.

e. S'il est souhaitable que le routeur actif reprenne ce rôle lorsqu'il est à nouveau disponible, configurez-le pour préemption du service du routeur de secours. Le routeur actif prend en charge le rôle de passerelle lorsqu'il redevient opérationnel.

- R1(config-if)# **standby 1 preempt**

Question :

- Quelle sera la priorité du HSRP de R3 lorsqu'il sera ajouté au groupe 1 du HSRP ?

Etape 2: Configurez HSRP sur R3

Configurez R3 comme routeur de secours.

a. Configurez l'interface R3 connectée au LAN 2.
b. Répétez uniquement les étapes 1b et 1c ci-dessus.

Etape 3: Vérifiez la configuration HSRP

Vérifiez HSRP en exécutant la commande **show standby** sur le R1 et le R3. Vérifiez les valeurs du rôle HSRP, du groupe, de l'adresse IP virtuelle de la passerelle, de la préemption et de la priorité. Notez que HSRP identifie également les adresses IP du routeur actif et de secours pour le groupe.

- R1# **show standby**

```
GigabitEthernet0/1 - Group 1 (version 2)
  State is Active
    4 state changes, last state change 00:00:30
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.696 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.3
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)
```

PARTIE 2

PARTIE 2

Activité 1 : Guide de configuration HSRP– Packet Tracer

- R3# **show standby**

```
GigabitEthernet0/0 - Group 1 (version 2)
  State is Standby
    4 state changes, last state change 00:02:29
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.720 secs
  Preemption disabled
  Active router is 192.168.1.1
    MAC address is d48c.b5ce.a0c1
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Gi0/0-1" (default)
```

À l'aide du résultat ci-dessus, répondez aux questions suivantes :

Questions :

- Quel est le routeur actif ?
- Quelle est l'adresse MAC pour l'adresse IP virtuelle ?
- Quelle est l'adresse IP et la priorité du routeur de secours ?

b. Utilisez la commande **show standby brief** sur le R1 et le R3 pour afficher un résumé de l'état HSRP. Voici un exemple de résultat.

- R1# **show standby brief**

```
P indicates configured to preempt.
                     |
Interface Grp Pri P State Active Standby Virtual IP
Gi0/1 1 150 P Active local 192.168.1.3 192.168.1.254
```

- R3# **show standby brief**

```
P indicates configured to preempt.

Interface Grp Pri P State Active Standby Virtual IP
Gi0/0 1 100 Standby 192.168.1.1 local 192.168.1.254
```

c. Modifiez l'adresse de la passerelle par défaut du PC-A, du PC-C, du S1 et du S3.

Questions :

- Quelle adresse devez-vous utiliser ?
- Vérifiez les nouveaux paramètres. Émettez un ping depuis PC-A et PC-C vers le serveur Web. Les requêtes ping ont-elles abouti ?

Activité 1 : Guide de configuration HSRP– Packet Tracer

- **Partie 3: Observez l'opération HSRP**

Etape 1: Rendre le routeur actif indisponible

Ouvrez une invite de commandes sur **PC-B** et entrez la commande **tracert 209.165.200.226** .

Question :

- Le chemin est-il différent du chemin utilisé avant la configuration de HSRP ?

Etape 1: Brisez le lien vers R1

a. Sélectionnez l'outil Supprimer dans la barre d'outils Packet Tracer et supprimez le câble qui relie R1 à S1.

b. Revenez immédiatement sur PC-B et exécutez à nouveau la commande **tracert 209.165.200.226** . Observez la sortie de la commande jusqu'à ce que la commande termine son exécution. Vous devrez peut-être répéter la trace pour voir le chemin complet.

Question :

- En quoi cette trace était-elle différente de la trace précédente ?

HSRP subit un processus pour déterminer quel routeur doit prendre le relais lorsque le routeur actif devient indisponible. Ce processus prend du temps. Une fois le processus est terminé, le routeur de secours R3 devient actif et est utilisé comme passerelle par défaut pour les hôtes sur LAN 1 et LAN 2.

Etape 3: Restaurer le lien vers R1

a. Reconnectez R1 à S1 à l'aide d'un câble direct en cuivre.

b. Exécutez une trace du PC-B vers le serveur Web. Vous devrez peut-être répéter la trace pour voir le chemin complet.

Questions :

- Quel chemin est utilisé pour accéder au serveur Web ?
- Si la commande preempt n'a pas été configurée pour le groupe HSRP sur R1, les résultats auraient-ils été les mêmes ?

Activité 1 : Guide de configuration HSRP– Packet Tracer

Réponses

- **Partie 1 / Etape 1 :**

b: R1, R2 and I-Net

- **Partie 1 / Etape 2 :** R3, R2 and I-Net

- **Partie 1 / Etape 3 :**

c: La commande tracert ne peut pas déterminer le chemin d'accès au serveur Web car le chemin a été rompu.

- **Partie 2 / Etape 1 :**

e: 100, qui est la valeur par défaut.

- **Partie 2 / Etape 3 :**

a: - R1 - 0000.0C9F.F001 - L'adresse IP est 192.168.1.3 et la priorité est 100.

c: - 192.168.1.254 - Oui

- **Partie 3 / Etape 1 :**

a: Oui. Le chemin passe maintenant par R1 au lieu de R3.

- **Partie 3 / Etape 2 :**

b: Au début, la trace a expiré. Finalement, la trace est passée par R3, R2 et I-Net. R3 a été utilisé comme première passerelle de saut dans cette trace au lieu de R1.

- **Partie 3 / Etape 2 :**

b:

- Au début, la trace échoue. Finalement, il recommence à utiliser R1 comme passerelle.

- Non, R1 ne redeviendrait pas la passerelle. Le chemin passant par R3 continuerait d'être utilisé.

PARTIE 3

Mettre en œuvre les protocoles de configuration dynamique

Dans ce module, vous allez :

- Être capable de configurer les services d'attribution automatique des adresses IPv4 et IPv6

5 heures

TP 1

Mettre en œuvre les protocoles de configuration dynamique

Compétences visées :

- Configurer le DHCPv4
- Configurer le DHCPv6

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

5 heures

TP 1

Mettre en œuvre les protocoles de configuration dynamique

1. Configuration DHCPv4
2. Configuration DHCPv6

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer le service DHCPv4?
- Réponses correctes pour au moins 70 % des questions.

Activité 1 : Implémentation de DHCPv4– Lab

- **Objectifs**

- **Partie 1: création d'un réseau et configuration des paramètres de base des périphériques**
- **Partie 2: Configurer et vérifier deux serveurs DHCPv4 sur R1**
- **Partie 3: Configurer et vérifier un relais DHCP sur R2**

- **Scenario**

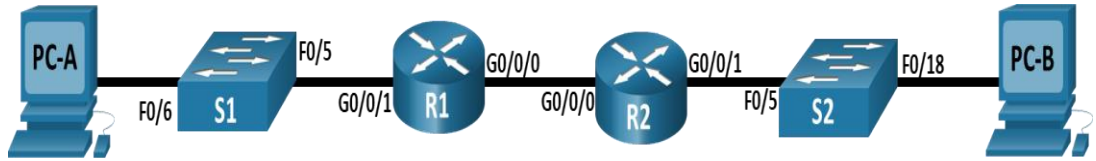
Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau permettant aux administrateurs réseau de gérer et d'automatiser l'attribution des adresses IP. Sans le protocole DHCP de IPv4, l'administrateur réseau doit attribuer et configurer manuellement les adresses IP, les serveurs DNS préférés et les passerelles par défaut. À mesure que le réseau se développe, cela devient un problème administratif lorsque les périphériques sont transférés d'un réseau interne à l'autre.

Dans ce scénario, la taille de l'entreprise s'est développée, et les administrateurs réseau ne peuvent plus attribuer d'adresses IP aux périphériques manuellement. Votre travail consiste à configurer le routeur R1 en vue d'attribuer des adresses IPv4 dans deux sous-réseaux différents.

Remarque: les routeurs utilisés dans les travaux pratiques CCNA sont Cisco 4221 équipé de version 16.9.4 de Cisco IOS XE (image universalk9). Les commutateurs utilisés dans les travaux pratiques sont des modèles Cisco Catalyst 2960s équipé de version 15.2.2 de Cisco IOS (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque: Assurez-vous que les routeurs et les commutateurs ont été effacés et n'ont aucune configuration de démarrage. En cas de doute, contactez votre formateur.

- **Topologie**



- **Ressources requises**

- 2 Routeurs (Cisco 4221 équipé de Cisco IOS version 16.9.4, image universelle ou similaire)
- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.2(2) image lanbasek9 ou similaires)
- 2 PC (Windows, équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

PARTIE 3

PARTIE 3

Activité 1 : Implémentation de DHCPv4– Lab

- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0/0	10.0.0.1	255.255.255.252	N/A
	G0/0/1	S/O	S/O	S/O
	G0/0/1.100			N/A
	G0/0/1.200			N/A
	G0/0/1.1000	S/O	S/O	S/O
R2	G0/0/0	10.0.0.2	255.255.255.252	N/A
	G0/0/1			N/A
S1	VLAN 200			
S2	VLAN 1			
PC-A	Carte réseau	le protocole DHCP	le protocole DHCP	le protocole DHCP
PC-B	Carte réseau	le protocole DHCP	le protocole DHCP	le protocole DHCP

- **Table de VLAN**

VLAN	Nom	Interface attribuée
1	N/A	S2: F0/18
100	Clients	S1: F0/6
200	Gestion	S1: VLAN 200
999	Parking_Lot	S1: F0/1-4, F0/7-24, G0/1-2
1000	Natif	N/A

- **Instructions**

  - **Partie 1: Création du réseau et configuration des paramètres de base des périphériques**

Dans la Partie 1, vous allez configurer la topologie du réseau et les paramètres de base sur les hôtes de PC et les commutateurs.

Etape 1: Établir un schéma d'adressage

Segmenter le réseau 192.168.1.0/24 pour répondre aux exigences suivantes:

a. Un sous-réseau, «Sous-réseau A», prenant en charge 58 hôtes (le VLAN client à R1).

- Sous-réseau A :

  Enregistrez la première adresse IP dans le tableau d'adressage pour R1 G0/0/1.100. Enregistrez la deuxième adresse IP dans la table d'adresses pour S1 VLAN 200 et entrez la passerelle par défaut associée.

b. Un sous-réseau, «Sous-réseau B», prenant en charge 28 hôtes (le VLAN de gestion à R1).

- Sous-réseau B:

Activité 1 : Implémentation de DHCPv4– Lab

Enregistrez la première adresse IP dans la table d'adressage pour R1 G0/0/1.200. Enregistrez la deuxième adresse IP dans la table d'adresses pour S1 VLAN 1 et entrez la passerelle par défaut associée.

c. Un sous-réseau, «Sous-réseau C», supportant 12 hôtes (le réseau client à R2).

- Sous-réseau C:

Enregistrez la première adresse IP dans le tableau d'adressage pour R2 G0/0/1.

Etape 2: Câblez le réseau conformément à la topologie indiquée

Connectez les équipements représentés dans le schéma de topologie et effectuez le câblage nécessaire.

Etape 3: Configurez les paramètres de base pour chaque routeur

a. Attribuez un nom de l'appareil au routeur.

Ouvrez la fenêtre de configuration.

b. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

c. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

d. Attribuez **cisco** comme mot de passe de console et activez la connexion.

e. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

f. Cryptez les mots de passe en texte clair.

g. Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.

h. Enregistrez la configuration en cours dans le fichier de configuration initiale.

i. Réglez l'horloge sur le routeur à l'heure et à la date d'aujourd'hui.

Remarque: utilisez le point d'interrogation (**?**) pour obtenir de l'aide et connaître la séquence de paramètres requise pour exécuter cette commande.

Etape 1: Configurer le routage inter-VLAN sur R1

a. Activez l'interface G0/0/1 sur le routeur.

b. Configurez les sous-interfaces pour chaque VLAN selon les besoins de la table d'adressage IP. Toutes les sous-interfaces utilisent l'encapsulation 802.1Q et se voient attribuer la première adresse utilisable à partir du pool d'adresses IP que vous avez calculé. Assurez-vous que la sous-interface du VLAN natif n'a pas d'adresse IP attribuée. Inclure une description pour chaque sous-interface.

c. Vérifiez que les sous-interfaces sont opérationnelles.

Etape 2: Configurer G0/0/1 sur R2, puis G0/0/0 et le routage statique pour les deux routeurs

a. Configurez G0/0/1 sur R2 avec la première adresse IP du sous-réseau C que vous avez calculée précédemment.

b. Configurez l'interface G0/0/0 pour chaque routeur en fonction du tableau d'adressage IP ci-dessus.

Activité 1 : Implémentation de DHCPv4– Lab

a. Configurez une route par défaut sur chaque routeur pointant vers l'adresse IP de G0/0/0 sur l'autre routeur.

b. Vérifiez que le routage statique fonctionne en faisant appel à l'adresse G0/0/1 de R2 à partir de R1.

c. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Etape 6: Configurez les paramètres de base pour chaque commutateur

a. Attribuez un nom de périphérique au commutateur.

Ouvrez la fenêtre de configuration.

b. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

c. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

d. Attribuez **cisco** comme mot de passe de console et activez la connexion.

e. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

f. Cryptez les mots de passe en texte clair.

g. Créez une bannière qui avertit quiconque accède à l'appareil que tout accès non autorisé est interdit.

h. Enregistrez la configuration en cours dans le fichier de configuration initiale.

i. Réglez l'horloge sur le commutateur à l'heure et à la date d'aujourd'hui.

Remarque: utilisez le point d'interrogation (**?**) pour obtenir et connaître la séquence de paramètres requise pour exécuter cette commande.

j. Copiez la configuration en cours en tant que configuration de démarrage.

Etape 7: création des réseaux locaux virtuels sur S1

Remarque: S2 n'est configuré qu'avec des paramètres de base.

a. Créez et nommez les VLAN requis sur le commutateur 1 à partir du tableau ci-dessus.

b. Configurez et activez l'interface de gestion sur S1 (VLAN 200) à l'aide de la deuxième adresse IP du sous-réseau calculée précédemment. En outre, définissez la passerelle par défaut sur S1.

c. Configurez et activez l'interface de gestion sur S2 (VLAN 1) à l'aide de la deuxième adresse IP du sous-réseau calculée précédemment. En outre, définissez la passerelle par défaut sur S2

d. Attribuez tous les ports inutilisés sur S1 au VLAN Parking_Lot, configurez-les pour le mode d'accès statique et désactivez-les administrativement. Sur S2, désactivez administrativement tous les ports non utilisés.

Remarque: La commande Interface range est utile pour accomplir cette tâche avec autant de commandes que nécessaire.

Etape 8: Attribuez les VLAN aux interfaces de commutateur correctes

Activité 1 : Implémentation de DHCPv4– Lab

a. Attribuez les ports utilisés au VLAN approprié (spécifié dans la table de VLAN ci-dessus) et configurez-les pour le mode d'accès statique.

Ouvrez la fenêtre de configuration.

a. Vérifiez que les VLAN sont attribués aux interfaces correctes.

Question:

- Pourquoi l'interface F0/5 est-elle répertoriée sous VLAN 1?

Etape 9: Configurez manuellement l'interface F0/5 de S1 en tant que trunk 802.1Q

a. Changez le mode switchport sur l'interface pour forcer le trunking.

b. Dans le cadre de la configuration du trunk, définissez le VLAN natif sur 1000.

c. Comme autre partie de la configuration du trunk, spécifiez que les VLAN 100, 200 et 1000 sont autorisés à traverser le trunk.

d. Enregistrez la configuration en cours dans le fichier de configuration initiale.

e. Vérifiez l'état de la trunking.

Question:

- À ce stade, quelle serait l'adresse IP des PC s'ils étaient connectés au réseau par DHCP ?

Partie 2: Configurer et vérifier deux serveurs DHCPv4 sur R1

Dans la partie 2, vous allez configurer et vérifier un serveur DHCPv4 sur R1. Le serveur DHCPv4 desservira deux sous-réseaux, le sous-réseau A et le sous-réseau C.

Etape 2: Configurez R1 avec des pools DHCPv4 pour les deux sous-réseaux pris en charge. Seul le pool DHCP pour le sous-réseau A est donné ci-dessous

a. Excluez les cinq premières adresses utilisables de chaque pool d'adresses.

Ouvrez la fenêtre de configuration.

b. Créez le pool DHCP (utilisez un nom unique pour chaque pool).

c. Spécifiez le réseau que ce serveur DHCP prend en charge.

d. Configurer le nom de domaine comme ccna-lab.com

e. Configurez la passerelle par défaut appropriée pour chaque pool DHCP.

f. Configurez la durée de bail pour 2 jours 12 heures et 30 minutes.

g. Ensuite, configurez le deuxième pool DHCPv4 en utilisant le nom de pool R2_Client_LAN et le réseau calculé, routeur par défaut et utilisez le même nom de domaine et le même temps de location que le pool DHCP précédent.

Activité 1 : Implémentation de DHCPv4– Lab

Etape 2: Save your configuration

Enregistrez la configuration en cours dans le fichier de configuration initiale.

Etape 3: Vérifier la configuration du serveur DHCPv4

a. Exécutez la commande **show ip dhcp pool** pour examiner les détails du pool.

b. Exécutez la commande **show ip dhcp liaisons** pour examiner les affectations d'adresses DHCP établies.

c. Exécutez la commande **show ip dhcp server statistics** pour examiner les messages DHCP.

Etape 4: Tentative d'acquisition d'une adresse IP à partir de DHCP sur PC-A

a. À partir d'une invite de commande sur PC-A, exécutez la commande **ipconfig /renew**.

b. Une fois le processus de renouvellement est terminé, exécutez la commande **ipconfig** pour afficher les nouvelles informations IP.

c. Testez la connectivité en envoyant une requête ping à l'adresse IP de l'interface G0/0/1 de R1.

- **Partie 3: Configurer et vérifier un relais DHCP sur R2**

Etape 1: Configurer R2 en tant qu'agent de relais DHCP pour le LAN sur G0/0/1

a. Configurez la commande **ip helper-address** sur G0/0/1 en spécifiant l'adresse IP G0/0/0 de R1.

Ouvrez la fenêtre de configuration.

b. Enregistrement de votre configuration.

Etape 2: Tentative d'acquisition d'une adresse IP à partir de DHCP sur PC-B

a. Ouvrez une fenêtre d'invite de commandes sur PC-B et exécutez la commande **ipconfig /renew**.

b. Une fois le processus de renouvellement est terminé, exécutez la commande **ipconfig** pour afficher les nouvelles informations IP.

c. Testez la connectivité en envoyant une requête ping à l'adresse IP de l'interface G0/0/1 de R1.

d. Exécutez la commande **show ip dhcp binding** sur R1 pour vérifier les liaisons DHCP.

e. Exécutez la commande **show ip dhcp server statistics** sur R1 et R2 pour vérifier les messages DHCP.

Activité 1 : Implémentation de DHCPv4– Lab

Réponses

- **Partie 1 / Etape 1 :**

a: 192.168.1.0/26 (.1 -.63)

b: 192.168.1.64/27 (.65-.95)

c: 192.168.1.96/28 (.97-.111)

- **Partie 1 / Etape 3 :**

a:
```
router(config)# hostname R1
```

b:
```
R1(config)# no ip domain lookup
```

c:
```
R1(config)# enable secret class
```

d:
```
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
```

e:
```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

f:
```
R1(config)# service password-encryption
```

g:
```
R1(config)# banner motd " $ Authorized Users Only! $
```

h:
```
R1# copy running-config startup-config
```

i:
```
R1# clock set 15:30:00 27 Aug 2019
```

- **Partie 1 / Etape 4 :**

a:
```
R1(config)# interface g0/0/1
R1(config-if)# no shutdown
R1(config-if)# exit
```

b:
```
R1(config)# interface g0/0/1.100
R1(config-subif)# description Client Network
R1(config-subif)# encapsulation dot1q 100
R1(config-subif)# ip address 192.168.1.1 255.255.255.192
R1(config-subif)# interface g0/0/1.200
R1(config-subif)# encapsulation dot1q 200
R1(config-subif)# description Management Network
R1(config-subif)# ip address 192.168.1.65 255.255.255.224
R1(config-subif)# interface g0/0/1.1000
R1(config-subif)# encapsulation dot1q 1000 native
R1(config-subif)# description Native VLAN
```

c:
```
R1# show ip interface brief
```

PARTIE 3

Activité 1 : Implémentation de DHCPv4– Lab

Réponses

- **Partie 1 / Etape 5 :**

a:
```
R2(config)# interface g0/0/1
R2(config-if)# ip address 192.168.1.97 255.255.255.240
R2(config-if)# no shutdown
R2(config-if)# exit
```

b:
```
R1(config)# interface g0/0/0
R1(config-if)# ip address 10.0.0.1 255.255.255.252
R1(config-if)# no shutdown
R2(config)# interface g0/0/0
R2(config-if)# ip address 10.0.0.2 255.255.255.252
R2(config-if)# no shutdown
```

c:
```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2
R2(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1
```

d:
```
R1# ping 192.168.1.97
```

e:
```
R1# copy running-config startup-config
```

- **Partie 1 / Etape 6:**

a:
```
switch(config)# hostname S1
```

b:
```
S1(config)# no ip domain-lookup
```

c:
```
S1(config)# enable secret class
```

d:
```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
```

e:
```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
```

f:
```
S1(config)# service password-encryption
```

g:
```
S1(config)# banner motd $ Authorized Users Only! $
```

h:
```
S1(config)# exit
S1# copy running-config startup-config
```

i:
```
S1# clock set 15:30:00 27 Aug 2019
```

- **Partie 1 / Etape 7 :**

a:
```
S1(config)# vlan 100
S1(config-vlan)# name Clients
S1(config-vlan)# vlan 200
S1(config-vlan)# name Management
S1(config-vlan)# vlan 999
S1(config-vlan)# name Parking_Lot
S1(config-vlan)# vlan 1000
S1(config-vlan)# name Native
S1(config-vlan)# exit
```

PARTIE 3

Activité 1 : Implémentation de DHCPv4– Lab

Réponses

b:
```
S1(config)# interface vlan 200
S1(config-if)# ip address 192.168.1.66 255.255.255.224
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.1.65
```

c:
```
S2(config)# interface vlan 1
S2(config-if)# ip address 192.168.1.98 255.255.255.240
S2(config-if)# no shutdown
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.1.97
```

d:
```
S1(config)# interface range f0/1 – 4, f0/7 – 24, g0/1 – 2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S2(config)# interface range f0/1 – 4,f0/6 – 17,f0/19 – 24,g0/1 – 2
S2(config-if-range)# switchport mode access
S2(config-if-range)# shutdown
S2(config-if-range)# exit
```

Partie 1 / Etape 8 :

a:
```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 100
```

b:
```
S1# show vlan brief
```

- Le port 5 se trouve dans le VLAN par défaut et n'a pas été configuré en tant que trunk 802.1Q.

- **Partie 1 / Etape 9 :**

a:
```
S1(config)# interface f0/5
S1(config-if)# switchport mode trunk
```

b:
```
S1(config-if-range)# switchport trunk native vlan 1000
```

c:
```
S1(config-if-range)# switchport trunk allowed vlan 100,200,1000
```

d:
```
S1(config)# exit
S1# copy running-config startup-config
```

e:
```
S1# show interfaces trunk
```

- Ils se configureraient eux-mêmes avec une adresse IP privée automatique (APIPA) dans la plage 169.254.x.x.

PARTIE 3

Activité 1 : Implémentation de DHCPv4– Lab

Réponses

- **Partie 2 / Etape 1 :**

a:
```
R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.5
```

b:
```
R1(config)# ip dhcp pool R1_Client_LAN
```

c:
```
R1(dhcp-config)# network 192.168.1.0 255.255.255.192
```

d:
```
R1(dhcp-config)# domain-name ccna-lab.com
```

e:
```
R1(dhcp-config)# default-router 192.168.1.1
```

f:
```
R1(dhcp-config)# lease 2 12 30
```

g:
```
R1(config)# ip dhcp excluded-address 192.168.1.97 192.168.1.101
R1(config)# ip dhcp pool R2_Client_LAN
R1(dhcp-config)# network 192.168.1.96 255.255.255.240
R1(dhcp-config)# default-router 192.168.1.97
R1(dhcp-config)# domain-name ccna-lab.com
R1(dhcp-config)# lease 2 12 30
```

Partie 2 / Etape 2 :

```
R1# copy running-config startup-config
```

Partie 3 / Etape 1 :

a:
```
R2(config)# interface g0/0/1
R2(config-if)# ip helper-address 10.0.0.1
```

b:
```
R2(config-if)# exit
R2# copy running-configuration startup-configuration
```

PARTIE 3

TP 1

Mettre en œuvre les protocoles de configuration dynamique

1. Configuration DHCPv4
2. Configuration DHCPv6

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer le service DHCPv6?
- Réponses correctes pour au moins 70 % des questions.

Activité 1 : Configurer DHCPv6– Lab

- **Objectifs**

- **Partie 1: Créer un réseau et configurer les paramètres de base des périphériques**
- **Partie 2: Vérifier l'attribution d'adresse SLAAC via R1**
- **Partie 3: Configurer et vérifier un serveur DHCPv6 sans état sur R1**
- **Partie 4: Configurer et vérifier un serveur DHCPv6 avec état sur R1**
- **Partie 5: Configurer et vérifier un relais DHCPv6 sur R2**

- **Contexte/scénario**

L'attribution dynamique des adresses de monodiffusion globale IPv6 (GUA) peut être configurée de trois manières:

- SLAAC (Configuration Automatique des Adresses Sans État)
- Protocole DHCPv6 (Protocole de configuration d'hôte dynamique sans état pour IPv6)
- DHCPv6 avec état
- Lors de l'utilisation de SLAAC pour attribuer des adresses IPv6 à des hôtes, un serveur DHCPv6 n'est pas utilisé. Étant donné qu'un serveur DHCPv6 n'est pas utilisé lors de la mise en œuvre de SLACC, les hôtes ne peuvent pas recevoir d'informations réseau critiques supplémentaires, notamment une adresse de serveur de noms de domaine (DNS) ainsi qu'un nom de domaine.

Lors de l'utilisation de DHCPv6 sans état pour attribuer des adresses IPv6 à l'hôte, un serveur DHCPv6 est utilisé pour attribuer les informations réseau critiques supplémentaires, mais l'adresse IPv6 est attribuée à l'aide de SLAAC.

Lors de la mise en œuvre de DHCPv6 avec état, un serveur DHCPv6 attribue toutes les informations du réseau, y compris l'adresse IPv6.

La détermination de la manière dont les hôtes obtiennent leur adressage IPv6 dynamique dépend du paramètre d'indicateur contenu dans les messages d'annonces du routeur (RA).

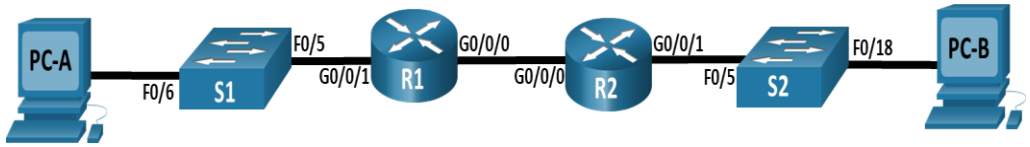
Dans ce scénario, la taille de l'entreprise s'est développée, et les administrateurs réseau ne peuvent plus attribuer d'adresses IP aux périphériques manuellement. Votre travail consiste à configurer le routeur R2 en vue d'attribuer des adresses IPv6 dans deux sous-réseaux différents connectés au routeur R1.

Remarque: les routeurs utilisés dans les travaux pratiques CCNA sont Cisco 4221 équipé de version 16.9.4 de Cisco IOS XE (image universalk9). Les commutateurs utilisés dans les travaux pratiques sont des modèles Cisco Catalyst 2960s équipé de version 15.2.2 de Cisco IOS (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque: Assurez-vous que les routeurs et les commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre formateur.

Activité 1 : Configurer DHCPv6– Lab

- **Topologie**



- **Ressources requises**

- 2 Routeurs (Cisco 4221 équipé de Cisco IOS version 16.9.4, image universelle ou similaire)
- 2 Commutateurs (Cisco 2960 équipés de Cisco IOS version 15.2.2 image lanbasek9 ou similaires) - **Facultatif**
- 2 PC (Windows, équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

- **Table d'adressage**

Appareil	Interface	Adresse IPv6
R1	G0/0/0	2001:db8:acad:2::1 /64
		fe80::1
	G0/0/1	2001:db8:acad:1::1/64
		fe80::1
R2	G0/0/0	2001:db8:acad:2:: 2/64
		fe80::2
	G0/0/1	2001:db8:acad:3::1 /64
		fe80::1
PC-A	Carte réseau	le protocole DHCP
PC-B	Carte réseau	le protocole DHCP

- **Instructions**

- **Partie 1: Créer un réseau et configurer des paramètres de base des périphériques**

Dans la Partie 1, vous allez configurer la topologie du réseau et les paramètres de base sur les hôtes de PC et les commutateurs.

Etape 1: Câblez le réseau conformément à la topologie indiquée

Connectez les équipements représentés dans le schéma de topologie et effectuez le câblage nécessaire.

PARTIE 3

Activité 1 : Configurer DHCPv6– Lab

Etape 2: Configurez les paramètres de base pour chaque commutateur. (Facultatif)

a. Attribuez un nom de périphérique au commutateur.

b. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

c. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

d. Attribuez **cisco** comme mot de passe de console et activez la connexion.

e. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

f. Cryptez les mots de passe en texte clair.

g. Créez une bannière qui avertit quiconque accède à l'appareil que tout accès non autorisé est interdit.

h. Arrêtez tous les ports inutilisés

i. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Fermez la fenêtre de configuration.

Etape 3: Configurez les paramètres de base pour chaque routeur

a. Attribuez un nom de l'appareil au routeur.

b. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

c. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

d. Attribuez **cisco** comme mot de passe de console et activez la connexion.

e. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

f. Cryptez les mots de passe en texte clair.

g. Créez une bannière qui avertit quiconque accède à l'appareil que tout accès non autorisé est interdit.

h. Activation du routage IPv6

i. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Etape 4: Configurez les interfaces et le routage pour les deux routeurs

a. Configurez les interfaces G0/0/0 et G0/0/1 sur R1 et R2 avec les adresses IPv6 spécifiées dans le tableau ci-dessus.

b. Configurez une route par défaut sur chaque routeur pointé vers l'adresse IP de G0/0/0 sur l'autre routeur.

c. Vérifiez que le routage fonctionne en envoyant une requête ping à l'adresse G0/0/1 de R2 via R1

d. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Fermez la fenêtre de configuration.

PARTIE 3

Activité 1 : Configurer DHCPv6– Lab

○ Etape 2: Vérifier l'attribution d'adresse SLAAC via R1

a. Dans la partie 2, vous vérifierez que l'hôte PC-A reçoit une adresse IPv6 à l'aide de la méthode SLAAC.

b. Mettez le PC-A sous tension et assurez-vous que la carte réseau est configurée pour la configuration automatique IPv6.

c. Après quelques instants, les résultats de la commande **ipconfig** devraient montrer que PC-A s'est attribué une adresse du réseau 2001:db 8:1::/64.

```
C:\Users\Student> ipconfig /all

Windows IP Configuration

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:5c43:ee7c:2959:da68
   Temporary IPv6 Address. . . . . . : 2001:db8:acad:1:3c64:e4f9:46e1:1f23
   Link-local IPv6 Address . . . . . : fe80::5c43:ee7c:2959:da68%6
   IPv4 Address. . . . . . . . . . . : 169.254.218.104
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%6
```

D'où vient la partie host-id de l'adresse?

○ Partie 3: Configurer et vérifier un serveur DHCPv6 sur R1

Dans la partie 3, vous allez configurer et vérifier un serveur DHCP sans état sur R1. L'objectif est de fournir à PC-A des informations sur le serveur DNS et le domaine.

Etape 1: Examinez la configuration de PC-A plus en détail

a. Exécutez la commande **ipconfig /all** sur PC-A et jetez un œil à la sortie.

- C:\Users\Student> **ipconfig /all**

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-3FR7RKA
   Primary Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) 852574L Gigabit Network
Connection
Physical Address. . . . . . . . . : 00-50-56-83-63-6D
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:5c43:ee7c:2959:da68
(Preferred)
```

Activité 1 : Configurer DHCPv6– Lab

```
Temporary IPv6 Address. . . . . : 2001:db8:acad:1:3c64:e4f9:46e1:1f23
(Preferred)

   Link-local IPv6 Address . . . . . :
fe80::5c43:ee7c:2959:da68%6(Preferred)

   IPv4 Address. . . . . . . . . . . : 169.254.218.104 (Preferred)

   Subnet Mask . . . . . . . . . . . : 255.255.0.0

   Default Gateway . . . . . . . . . : fe80::1%6

   DHCPv6 IAID . . . . . . . . . . . : 50334761

   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F5-CE-A2-00-50-56-B3-
63-6D

   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1

                                       fec0:0:0:ffff::2%1

                                       fec0:0:0:ffff::3%1

   NetBIOS over Tcpip. . . . . . . . : Enabled
```

b. Notez qu'il n'y a pas de suffixe DNS principal. Notez également que les adresses de serveur DNS fournies sont des adresses "site local anycast", et non des adresses monodiffusion, comme prévu.

Etape 2: Configurez R1 pour fournir DHCPv6 sans état pour PC-A

a. Créez un pool DHCP IPv6 sur R1 nommé R1-STATELESS. Dans le cadre de ce pool, attribuez l'adresse du serveur DNS comme 2001:db8:acad::1 et le nom de domaine comme stateless.com.

- R1 (config) # **ipv6 dhcp pool R1-STATELESS**
- R1 (config-dhcp) # **dns-server 2001:db8:acad::254**
- R1 (config-dhcp) # **domaine name Stateless.com**

b. Configurez l'interface G0/0/1 sur R1 pour fournir l'indicateur de configuration Other au LAN R1, et spécifiez le pool DHCP que vous venez de créer en tant que ressource DHCP pour cette interface.

- R1(config)# **interface g0/0/1**
- R1(config-if)# **ipv6 nd other-config-flag**
- R1 (config-if) # **serveur dhcp ipv6 R1-STATELESS**

c. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Fermez la fenêtre de configuration.

d. Redémarrez PC-A.

e. Examinez la sortie de **ipconfig /all** et notez les modifications.

- C:\Users\Student> **ipconfig /all**

PARTIE 3

Activité 1 : Configurer DHCPv6– Lab

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-3FR7RKA
   Primary Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : STATELESS.com

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix . : STATELESS.com
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network
Connection
   Physical Address. . . . . . . . . : 00-50-56-83-63-6D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:5c43:ee7c:2959:da68
(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:db8:acad:1:3c64:e4f9:46e1:1f23
(Preferred)
   Link-local IPv6 Address . . . . . : fe80::5c43:ee7c:2959:da68%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 169.254.218.104 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%6
   DHCPv6 IAID . . . . . . . . . . . : 50334761
   DUID de client DHCPv6. . . . . . . : 00-01-00-01-24-F5-CE-A2-00-50-56-
B3-63-6D
   DNS Servers . . . . . . . . . . . : 2001:db8:acad::254
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix . : STATELESS.com
```

f. Testez la connectivité en envoyant une requête ping à l'adresse IP de l'interface G0/0/1 de R2.

○ Partie 4: Configurer un serveur DHCPv6 avec état sur R1

Dans la partie 4, vous allez configurer R1 pour répondre aux demandes DHCPv6 du LAN sur R2.

a. Créez un pool DHCPv6 sur R1 pour le réseau 2001:db8:acad:3:aaaa::/80. Cela fournira des adresses au réseau local connecté à l'interface G0/0/1 sur R2. Dans le cadre du pool, définissez le serveur DNS sur 2001:db8:acad::254 et définissez le nom de domaine sur Stateful.com.

- R1 (config) # **ipv6 dhcp pool R2-STATEFUL**
- R1 (config-dhcp) # **address prefix 2001:db8:acad:3:aaa::/80**

PARTIE 3

Activité 1 : Configurer DHCPv6– Lab

- R1 (config-dhcp) # **dns-server 2001:db8:acad::254**
- R1 (config-dhcp) # **domaine-name Stateful.com**

b. Attribuez le pool DHCPv6 que vous venez de créer à l'interface g0/0/0 sur R1.

- R1 (config) # **interface g0/0/1**
- R1 (config-if) # **serveur dhcp ipv6 R2-STATEFUL**

○ Partie 5: Configurer et vérifier un relais DHCPv6 sur R2

Dans la partie 5, vous allez configurer et vérifier le relais DHCPv6 sur R2, permettant à PC-B de recevoir une adresse IPv6.

Etape 1: Mettez le PC-B sous tension et examinez l'adresse SLAAC qu'il génère

- C:\Users\Student> **ipconfig /all**

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-3FR7RKA
   Primary Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : Non

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network
Connection
   Physical Address. . . . . . . . . : 00-50-56-B3-7B-06
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:3:a0f 3:3 d39:f9fb:a020
(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:db8:acad:3:d4f 3:7 b16:eee:b2b5
(Preferred)
   Link-local IPv6 Address . . . . .: fe80::a0f3:3d39:f9fb:a 020% 6
(Preferred)
   IPv4 Address. . . . . . . . . . . : 169.254.160.32 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%6
   DHCPv6 IAID . . . . . . . . . . . : 50334761
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F2-08-38-00-50-56-B3-
7B-06
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Notez dans la sortie que le préfixe utilisé est 2001:db8:acad:3::

PARTIE 3

Activité 1 : Configurer DHCPv6– Lab

Etape 2: Configurez R2 en tant qu'agent de relais DHCP pour le LAN sur G0/0/1

a. Configurez la commande **ipv6 dhcp relay** sur l'interface R2 G0/0/1, en spécifiant l'adresse de destination de l'interface G0/0/0 sur R1. Configurez également la commande **managed-config-flag** .

Ouvrez la fenêtre de configuration.

- R2(config)# **interface g0/0/1**
- R2(config-if)# **ipv6 nd managed-config-flag**
- R2 (config-if) #**ipv6 dhcp relay destination 2001:db8:cafe:1::6 g0/0/0**

b. Save your configuration.

Etape 3: Essayez d'acquérir une adresse IPv6 à partir de DHCPv6 sur PC-B

a. Redémarrez PC-B.

b. Ouvrez une invite de commande sur PC-B et exécutez la commande **ipconfig /all** et examinez la sortie pour voir les résultats de l'opération de relais DHCPv6.

- C:\Users\Student> **ipconfig /all**

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-3FR7RKA
   Primary Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : STATEFUL.com

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix . : STATEFUL.com
   Description . . . . . . . . . . . : Intel(R) 852574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B3-7B-06
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad3:aaaa:7104:8b7d:5402 (Preferred)
   Lease Obtained. . . . . . . . . . : Sunday, October 6, 2019 3:27:13 PM
   Lease Expires . . . . . . . . . . : Tuesday, October 8, 2019 3:27:13 PM
   Link-local IPv6 Address . . . . .: fe80::a0f3:3d39:f9fb:a 020% 6 (Preferred)
   IPv4 Address. . . . . . . . . . . : 169.254.160.32 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::2%6
   DHCPv6 IAID . . . . . . . . . . . : 50334761
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-F2-08-38-00-50-56-B3-7B-06
   DNS Servers . . . . . . . . . . . : 2001:db8:acad::254
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix . : STATELESS.com
```

Testez la connectivité en envoyant une requête ping à l'adresse IP de l'interface G0/0/1 de R1.

PARTIE 3

Activité 1 : Configurer DHCPv6– Lab

Réponses

- **Partie 1 / Etape 2:**

a:
```
switch(config)# hostname S1
switch(config)# hostname S2
```

b:
```
S1(config)# no ip domain-lookup
S2(config)# no ip domain-lookup
```

c:
```
S1(config)# enable secret class
S2(config)# enable secret class
```

d:
```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S2(config)# line console 0
S2(config-line)# password cisco
S2(config-line)# login
```

e:
```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S2(config)# line vty 0 4
S2(config-line)# password cisco
S2(config-line)# login
```

f:
```
S1(config)# service password-encryption
S2(config)# service password-encryption
```

g:
```
S1(config)# banner motd $ Authorized Users Only! $
S2(config)# banner motd $ Authorized Users Only! $
```

h:
```
S1(config)# interface range f0/1-4, f0/7-24, g0/1-2
S1(config-if-range)# shutdown
S2(config)# interface range f0/1-4,f0/7-17,f0/19-24,g0/1-2
S2(config-if-range)# shutdown
```

i:
```
S1# copy running-config startup-config
S2# copy running-config startup-config
```

- **Partie 1 / Etape 3:**

a:
```
router(config)# hostname R1
router(config)# hostname R2
```

b:
```
R1(config)# no ip domain lookup
R2(config)# no ip domain lookup
```

c:
```
R1(config)# enable secret class
R2(config)# enable secret class
```

d:
```
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R2(config)# line console 0
R2(config-line)# password cisco
R2(config-line)# login
```

e:
```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R2(config)# line vty 0 4
R2(config-line)# password cisco
R2(config-line)# login
```

PARTIE 3

PARTIE 3

Activité 1 : Configurer DHCPv6– Lab

Réponses

f:
```
R1(config)# service password-encryption
R2(config)# service password-encryption
```
g:
```
R1(config)# banner motd $ Authorized Users Only! $
R2(config)# banner motd $ Authorized Users Only! $
```
e:
```
R1(config)# ipv6 unicast-routing
R2(config)# ipv6 unicast-routing
```
h:
```
R1(config)# exit
R1# copy running-config startup-config
R2(config)# exit
R2# copy running-config startup-config
```

Partie 1 / Etape 4:

a:
```
R1(config)# interface g0/0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config)# interface g0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R2(config)# interface g0/0/1
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# ipv6 address 2001:db8:acad:3::1/64
R2(config-if)# no shutdown
R2(config)# interface g0/0/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# ipv6 address 2001:db8:acad:2::2/64
R2(config-if)# no shutdown
```
b:
```
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2
R2(config)# ipv6 route ::/0 2001:db8:acad:2::1
```
c:
```
R1#(config)# exit
```
d:
```
R1# ping 2001:db8:acad:1::1
R1# copy running-config startup-config
```

- **Partie 2 :**

La réponse dépendra de la configuration du système d'exploitation. Soit l'hôte génère une adresse EUI-64 basée sur l'interface MAC, soit l'hôte génère une adresse 64 bits aléatoire.

- **Partie 3 / Etape 2:**

c: `R1# copy running-config startup-config`

- **Partie 5 / Etape 2 :** b : `R2# copy running-configuration startup-configuration`

PARTIE 4

Sécuriser un réseau local

Dans ce module, vous allez :

- Être en mesure d’assurer la sécurité de réseau LAN
- Être capable de concevoir et sécuriser un réseau sans fil (WLAN)

8 heures

TP 1

Sécuriser un réseau local

Compétences visées :

- Sécuriser la couche 2 du réseau LAN

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

3 heures

TP 1

Sécuriser un réseau local

1. Configuration de la sécurité du commutateur

Critères de réussite :

- Le stagiaire est-il capable de :
  - Etablir et configurer la sécurité LAN?
- Réponses correctes pour au moins 70 % des questions.

Activité 1 : Configuration de la sécurité du commutateur- Lab

Objectifs

- **Partie 1: Configurer les périphériques réseau.**
  - Câblage du réseau.
  - Configurer R1.
  - Configurer et vérifier les paramètres de base du commutateur.
- **Partie 2: Configurer les VLAN sur Les Commutateures.**
  - Configurer VLAN 10.
  - Configurer le SVI pour VLAN 10.
  - Configurer VLAN 333 avec le nom natif sur S1 et S2.
  - Configurer VLAN 999 avec le nom ParkingLot sur S1 et S2.
- **Partie 3: Configurer la Sécurité du Commutateur.**
  - Mettre en œuvre le trunc 802.1Q
  - Configurer les ports d'accès.
  - Sécuriser et désactiver les ports de commutateures inutilisés.
  - Documenter et mettre en œuvre les fonctions de sécurité des ports.
  - Mettre en œuvre la sécurité d'espionnage DHCP.
  - Mettre en œuvre PortFast et la protection BPDU.
  - Vérifier la connectivité de bout en bout.

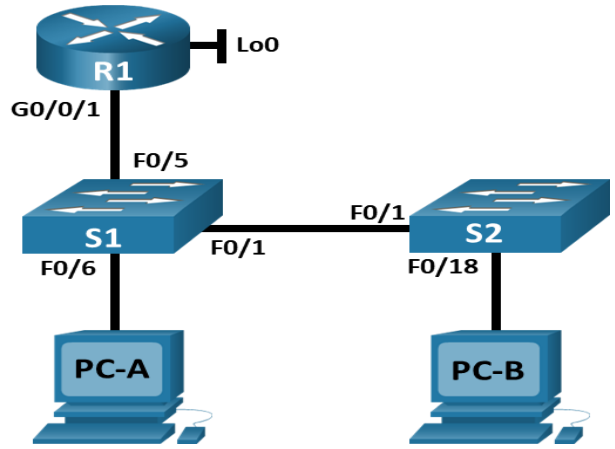
Contexte/scénario

Ces travaux pratiques passent en revue les fonctionnalités de sécurité de couche 2 précédemment apprises.

Remarque: les routeurs utilisés dans les travaux pratiques CCNA sont Cisco 4221 version 16.9.3 de Cisco IOS XE (image universalk9). Les commutateurs utilisés dans les travaux pratiques sont des modèles Cisco Catalyst 2960s version 15.0(2) de Cisco IOS (image lanbasek9). D'autres routeurs, commutateurs et d'autres versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque: vérifiez que les paramètres des commutateurs ont été effacés et qu'ils ne présentent aucune configuration initiale. En cas de doute, contactez votre instructeur.

Topologie



PARTIE 4

Activité 1 : Configuration de la sécurité du commutateur- Lab

- **Ressources requises**

- 1 routeur (Cisco 4221 avec la version 16.9.3 de Cisco IOS XE universelle ou similaire).
- 2 commutateurs (Cisco 2960 avec la version 15.0(2) de Cisco IOS image lanbasek9 ou similaire).
- 2 PC (Windows équipé d'un programme d'émulation de terminal tel que Tera Term).
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console.
- Câbles Ethernet comme la topologie indique.

- **Table d'adressage**

Périphérique	Interface /Vlan	Adresse IP	Masque de sous-réseau
R1	G0/0/1	192.168.10.1	255.255.255.0
R1	Bouclage 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC – A	Carte réseau (NIC)	DHCP	255.255.255.0
PC – B	Carte réseau (NIC)	DHCP	255.255.255.0

- **Instructions**

- **Partie 1: Configurer les périphériques réseau**

Etape 1: Câblage du réseau

a. Chargez le script de configuration suivant sur R1.

```
Enable
configure terminal
hostname R1
no ip domain lookup
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.201 192.168.10.202
!
ip dhcp pool Students
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 domain-name CCNA2.Lab-11.6.1
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
 Description de Liaison porte 5 à S1
 ip dhcp relay information trusted
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 exec-timeout 0 0
```

PARTIE 4

Activité 1 : Configuration de la sécurité du commutateur- Lab

b. Vérifiez la configuration d'exécution sur R1 à l'aide de la commande suivante:

- R1# **show ip interface brief**

c. Vérifiez que l'adressage IP et les interfaces sont dans l'état up/ up (dépannez si nécessaire).

Etape 2: Configurer et vérifier les paramètres de base du commutateur

a. Configurez le nom d'hôte pour les commutateurs S1 et S2.

Ouvrez la fenêtre de configuration.

b. Empêchez les recherches DNS indésirables sur les deux commutateures

c. Configurez les descriptions d'interface des ports utilisés sur S1 et S2.

d. Déterminé la passerelle par défaut pour le VLAN de gestion d'être 192.168.10.1 sur les deux commutateurs.

○ Partie 2:Configurer les VLAN sur les commutateures

Etape 1: Configurer VLAN 10

Ajoutez VLAN 10 à S1 et S2 et nommez le VLAN **Management.**

Etape 2: Configurer le SVI pour VLAN 10

Configurez l'adresse IP selon la table d'adressage de SVI pour VLAN 10 sur S1 et S2. Activez les interfaces SVI et fournissez une description de l'interface.

Etape 3: Configurer VLAN 333 avec le nom natif sur S1 et S2

Etape 4: Configurer VLAN 999 avec le nom ParkingLot sur S1 et S2.

○ Partie 3: Configurer la Sécurité du Commutateur

Etape 1: Mettre en œuvre le trunk 802.1Q

a. Sur les deux commutateurs, configurez le trunk sur F0/1 pour utiliser le VLAN 333 comme VLAN natif.

b. Vérifiez que le trunk est configuré sur les deux commutateurs.

- S1# **show interface trunk**

```
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 333

Port Vlans allowed on trunk
Fa0/1 1-4094

Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999
```

- S2# **show interface trunk**

```
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 333
```

PARTIE 4

Activité 1 : Configuration de la sécurité du commutateur- Lab

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

Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999
```

c. Désactivez la négociation DTP sur F0/1 sur S1 et S2.

d. Vérifiez en utilisant la commande **show interfaces** .

- S2# **show interfaces f0/1 switchport | include Negotiation**

```
Negotiation of Trunking: Off
```

- S2# **show interfaces f0/1 switchport | include Negotiation**

```
Negotiation of Trunking: Off
```

Etape 2: Configurer les ports d'accès

a. Sur S1, configurez F0/5 et F0/6 comme des ports d'accès associés au VLAN 10.

b. Sur S2, configurez F0/18 comme un port d'accès associé au VLAN 10.

Etape 3: Sécuriser et désactiver les ports de commutateures inutilisés

a. Sur S1 et S2, déplacez les ports inutilisés de VLAN 1 à VLAN 999 et désactivez les ports inutilisés.

b. Vérifiez que les ports inutilisés sont désactivés et associés au VLAN 999 en exécutant la commande **show**.

- S1# **show interfaces status**

```
Port Name Status Vlan Duplex Speed Type
Fa0/1 Link to S2 connected trunk a-full a-100 10/100BaseTX
Fa0/2 disabled 999 auto auto 10/100BaseTX
Fa0/3 disabled 999 auto auto 10/100BaseTX
Fa0/4 disabled 999 auto auto 10/100BaseTX
Fa0/5 Link to R1 connected 10 a-full a-100 10/100BaseTX
Fa0/6 Link to PC-A connected 10 a-full a-100 10/100BaseTX
Fa0/7 disabled 999 auto auto 10/100BaseTX
Fa0/8 disabled 999 auto auto 10/100BaseTX
Fa0/9 disabled 999 auto auto 10/100BaseTX
Fa0/10 disabled 999 auto auto 10/100BaseTX
<output omitted>
```

- S2# **show interfaces status**

Activité 1 : Configuration de la sécurité du commutateur- Lab

```
Port Name Status Vlan Duplex Speed Type
Fa0/1 Link to S1 connected trunk a-full a-100 10/100BaseTX
Fa0/2 disabled 999 auto auto 10/100BaseTX
Fa0/3 disabled 999 auto auto 10/100BaseTX
<output omitted>
Fa0/14 disabled 999 auto auto 10/100BaseTX
Fa0/15 disabled 999 auto auto 10/100BaseTX
Fa0/16 disabled 999 auto auto 10/100BaseTX
Fa0/17 disabled 999 auto auto 10/100BaseTX
Fa0/18 Link to PC-B connected 10 a-full a-100 10/100BaseTX
Fa0/19 disabled 999 auto auto 10/100BaseTX
Fa0/20 disabled 999 auto auto 10/100BaseTX
Fa0/21 disabled 999 auto auto 10/100BaseTX
Fa0/22 disabled 999 auto auto 10/100BaseTX
Fa0/23 disabled 999 auto auto 10/100BaseTX
Fa0/24 disabled 999 auto auto 10/100BaseTX
Gi0/1 disabled 999 auto auto 10/100/1000BaseTX
Gi0/2 disabled 999 auto auto 10/100/1000BaseTX
```

Etape 4: Documenter et mettre en œuvre les fonctions de sécurité des ports

Les interfaces F0/6 sur S1 et F0/18 sur S2 sont configurées comme ports d'accès. Dans cette étape, vous allez aussi configurer la sécurité des ports sur ces deux ports d'accès.

a. Sur S1, exécutez la commande **show port-security interface f0/6** pour afficher les paramètres de sécurité de port par défaut de l'interface F0/6. Notez vos réponses dans le tableau ci-dessous.

Configuration de la sécurité des ports par défaut	
Caractéristique	Paramètre par défaut
Sécurité des ports	
Nombre maximal des adresses MAC	
Mode de violation	
Délai d'expiration	
Type d'obsolescence	
Obsolescence d'adresse statique sécurisé	
Adresses MAC rémanentes	

b. Sur S1, activez la sécurité des ports sur F0/6 avec les paramètres suivants:

- Nombre maximal d'entrées d'adresse : **3**
- Mode de violation : **Restrict**
- Temps d'obsolescence : **60 min**
- Type d'obsolescence : **Inactivité**

PARTIE 4

Activité 1 : Configuration de la sécurité du commutateur- Lab

c. Vérifiez la sécurité de port sur S1 F0/6

- S1# **show port-security interface f0/6**

```
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Restrict
Aging Time : 60 mins
Aging Type : Inactivity
SecureStatic Address Aging : Disabled
Adresses MAC maximales (Maximum MAC Adresses) : 3
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0022.5646.3411:10
Security Violation Count : 0
```

- S1# **show port-security address**

```
Secure Mac Address Table
------------------------------------------------------------
Vlan Mac Address Type Ports Remaining Age
                                                    (mins)
---- ----------- ---- ----- -------------
  10 0022.5646.3411 SecureDynamic Fa0/6 60 (I)
------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

d. Activez la sécurité des ports pour F0/18 sur S2. Configurez le port pour ajouter automatiquement les adresses MAC apprissent sur le port à la configuration courante.

e. Configurez les paramètres de sécurité de port suivant sur S2 F/18:

- Nombre maximal d'entrées d'adresse: **2**
- Mode de Violation : **Protect**
- Temps d'obsolescence : **60 min**

f. Vérifiez la sécurité de port sur S2 F0/18

- S2# **show port-security interface f0/18**

```
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 60 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Adresses MAC maximales (Maximum MAC Adresses) : 2
Total MAC Addresses : 1
```

Activité 1 : Configuration de la sécurité du commutateur- Lab

```
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0022.5646.3413:10
Security Violation Count : 0
```

- S2# **show port-security address**

```
Secure Mac Address Table
------------------------------------------------------------
Vlan Mac Address Type Ports Remaining Age
                                                    (mins)
---- ----------- ---- ----- -------------
  10 0022.5646.3413 SecureSticky Fa0/18 -
------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

Etape 5: Mettre en œuvre la sécurité d'espionnage DHCP

a. Sur S2, activez et configurez l'espionnage DHCP sur le VLAN 10.

b. Configurez le port trunc sur S2 comme un port approuvé.

c. Limitez les ports non approuvés, F18 sur S2 à cinq paquets DHCP par seconde.

d. Vérifiez l'espionnage DHCP sur S2.

- S2# **show ip dhcp snooping**

```
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface Trusted Allow option Rate limit (pps)
----------------------- ------- ------------ ----------------
FastEthernet0/1 yes yes unlimited
  Custom circuit-ids:
FastEthernet0/18 no no 5
  Custom circuit-ids:
```

PARTIE 4

Activité 1 : Configuration de la sécurité du commutateur- Lab

e. À partir de l'invite de commande sur PC-B, libérez puis renouvelez l'adresse IP.

- C:\Users\Student> **ipconfig /release**
- C:\Users\Student> **ipconfig /renew**

b. Vérifiez la liaison de l'espionnage DHCP en utilisant la commande **show ip dhcp snooping binding** .

- S2# **show ip dhcp snooping**

```
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- -------------------------
00:50:56:90:D0:8E 192.168.10.11 86213 dhcp-snooping 10 FastEthernet0/18
Total number of bindings: 1
```

Etape 6: Mettre en œuvre PortFast et la protection BPDU

a. Configurez PortFast sur tous les ports d'accès qui sont utilisés sur les deux commutateures.

b. Activez la protection BPDU sur les ports d'accès S1 et S2 VLAN 10 connectés aux PC-A et PC-B.

c. Vérifiez que la protection BPDU et PortFast sont activés sur les ports appropriés.

- S1# **show spanning-tree interface f0/6 detail**

```
Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.6.
   <output omitted for brevity>
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 128, received 0
```

Etape 7: Vérifier la connectivité de bout en bout

Vérifiez la connectivité PING entre tous les périphériques de la table d'adressage IP. Si les pings échouent, vous devrez peut-être désactiver le pare-feu sur les hôtes PC.

Questions de réflexion

- En référence à la sécurité des ports sur S2, pourquoi n'y a-t-il pas un valeur de minuterie pour l'obsolescence restant en minutes lorsque l'apprentissage rémanente a été configurée?
- En référence à la sécurité des ports sur S2, si vous chargez le script running-config sur S2, pourquoi PC-B sur le port 18 n'obtiendra-t-il jamais d'adresse IP via DHCP?
- En ce qui concerne la sécurité des ports, quelle est la différence entre le type d'obsolescence absolu et le type d'obsolescence inactif ?

Activité 1 : Configuration de la sécurité du commutateur- Lab

Réponses

- **Partie 1 / Etape 2 :**

a:

```
Switch# config t                    Switch# config t
Switch(config)# hostname S1         Switch(config)# hostname S1
```

b:

```
S1(config)# no ip domain-lookup
S2(config)# no ip domain-lookup
```

c:

```
S1(config)# interface f0/1
S1(config-if)# description Link to S2
S1(config-if)# interface f0/5
S1(config-if)# description Link to R1
S1(config-if)# interface f0/6
S1(config-if)# description Link to PC-A
S2(config)# interface f0/1
S2(config-if)# description Link to S1
S2(config-if)# interface f0/18
S2(config-if)# description Link to PC-B
```

d:

```
S1(config)# ip default-gateway 192.168.10.1
S2(config)# ip default-gateway 192.168.10.1
```

- **Partie 2 / Etape 1 :**

```
S1(config)# vlan 10
S1(config-vlan)# name Management
S2(config)# vlan 10
S2(config-vlan)# name Management
```

- **Partie 2 / Etape 2:**

```
S1(config)# interface vlan 10
S1(config-if)# ip address 192.168.10.201 255.255.255.0
S1(config-if)# description Management SVI
S1(config-if)# no shutdown
S2(config)# interface vlan 10
S2(config-if)# ip address 192.168.10.202 255.255.255.0
2S1(config-if)# description Management SVI
S2(config-if)# no shutdown
```

Partie 2 / Etape 3:

```
S1(config)# vlan 333
S1(config-vlan)# name Native
S2(config)# vlan 333
S2(config-vlan)# name Native
```

Activité 1 : Configuration de la sécurité du commutateur- Lab

Réponses

- **Partie 2 / Etape 4 :**

```
S1(config-vlan)# vlan 999
S1(config-vlan)# name ParkingLot
S2(config-vlan)# vlan 999
S2(config-vlan)# name ParkingLot
```

- **Partie 3 / Etape 1 :**

a:

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 333
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 333
```

c:

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

- **Partie 3 / Etape 2 :**

a:

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10
```

b:

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10
```

- **Partie 3 / Etape 3:**

a:

```
S1(config)# interface range f0/2-4 , f0/7-24, g0/1-2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown
S2(config)# interface range f0/2-17 , f0/19-24, g0/1-2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown
```

- **Partie 3 / Etape 4:**

a:

Configuration de la sécurité des ports par défaut	
Caractéristique	Paramètre par défaut
Sécurité des ports	**Disabled**
Nombre maximal des adresses MAC	1
Mode de violation	**Shutdown**
Délai d'expiration	0 mins
Type d'obsolescence	**Absolute**
Obsolescence d'adresse statique sécurisé	**Disabled**
Adresses MAC rémanentes	0

PARTIE 4

Activité 1 : Configuration de la sécurité du commutateur- Lab

Réponses

- **Partie 3 / Etape 4 :**

a:
```
S1(config)# interface f0/6
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation restrict
S1(config-if)# switchport port-security aging time 60
S1(config-if)# switchport port-security aging type inactivity
```

d:
```
S2(config)# interface f0/18
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security mac-address sticky
```

e:
```
S2(config)# interface f0/18
S2(config-if)# switchport port-security aging time 60
S2(config-if)# switchport port-security maximum 2
S2(config-if)# switchport port-security violation protect
```

- **Partie 3 / Etape 5 :**

a:
```
S2(config)# ip dhcp snooping
S2(config)# ip dhcp snooping vlan 10
```

b:
```
S2(config)# interface f0/1
S2(config-if)# ip dhcp snooping trust
```

c:
```
S2(config)# interface f0/18
S2(config-if)# ip dhcp snooping limit rate 5
```

- **Partie 3 / Etape 6 :**

a:
```
S1(config)# interface range f0/5 – 6
S1(config-if)# spanning-tree portfast
S2(config)# interface f0/18
S2(config-if)# spanning-tree portfast
```

b:
```
S1(config)# interface f0/6
S1(config-if)# spanning-tree bpduguard enable
S2(config)# interface f0/18
S2(config-if)# spanning-tree bpduguard enable
```

Questions de réflexion

a: Ce commutateur ne prend pas en charge le vieillissement de la sécurité des ports des adresses sécurisées permanentes.

b: La sécurité du port est définie pour seulement deux adresses MAC et le port 18 a deux adresses MAC "collantes" liées au port. De plus, la violation est protégée, qui n'enverra jamais de message console/syslog ni n'incrémentera le compteur de violation.

c: Si le type d'inactivité est défini, les adresses sécurisées sur le port seront supprimées uniquement s'il n'y a pas de trafic de données provenant des adresses source sécurisées pendant la période spécifiée. Si le type absolu est défini, toutes les adresses sécurisées sur ce port expirent exactement après la fin de la durée spécifiée.

TP 2

Concevoir et sécuriser un réseau WLAN

Compétences visées :

- Configurer et dépanner les réseaux WLAN

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

5 heures

TP 2

Concevoir et sécuriser un réseau WLAN

1. Configuration de réseau WLAN

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer un réseau WLAN?
- Réponses correctes pour au moins 70 % des questions.

Activité 1 : Configuration de réseau sans fil- Packet Tracer

- **Objectifs**

- **Connecter à un routeur sans fil**
- **Configurer le routeur sans fil**
- **Connecter un périphérique câblé au routeur sans fil**
- **Connecter un périphérique sans fil au routeur sans fil**
- **Ajouter un point d'accès au réseau pour étendre la couverture sans fil**
- **Mettre à jour les paramètres du routeur par défaut**

- **Introduction**

Dans cet exercice, vous allez configurer un routeur sans fil et un point d'accès pour qu'ils acceptent les clients sans fil et acheminent les paquets IP. En plus, vous allez mettre à jour certains paramètres par défaut.

- **Instructions**

  - **Partie 1: Connecter à un routeur sans fil**

Etape 1: Connecter l'administrateur au routeur sans fil

a. Connectez **l'administrateur** au **routeur sans fil (WR)** à l'aide d'un câble Ethernet droit via les ports Ethernet. Sélectionnez l'option **Connexions**(Connections), représentée avec un boulon lumineux, en bas à gauche de Packet Tracer. Cliquez sur **Cuivre droit**(Copper Straight-Through), représenté avec une ligne noire solide.

b. Lorsque le curseur change au mode de connexion, cliquez sur **Admin** et choisissez **FastEthernet0**. Cliquez sur **WR** (routeur sans fil) et choisissez le port Ethernet disponible pour connecter l'autre extrémité du câble.

WR (wireless router) agira en tant que commutateur pour les périphériques connectés au LAN et comme un routeur pour l'internet. **L'administrateur** est maintenant connecté au LAN (**GigabitEthernet 1**). Quand Packet Tracer affiche des triangles verts de chaque côté de la connexion entre l' **administrateur** et le **WR (routeur sans fil)**, continuez à l'étape suivante.

Remarque: si le triangle vert n'apparait pas, assurez-vous d'activer **Show Link lights** sous **Options > Préférences (Prefrences)**. Vous pouvez également cliquer sur **Avance rapide** (Fast Forward Time) juste sur le boîte de sélection **Connexions (Connections)**dans la barre jaune.

Etape 2: Configurer l'administrateur pour utiliser DHCP

Pour accéder à la page de gestion du **routeur sans fil** , **l'administrateur** doit communiquer sur le réseau. Un routeur sans fil inclut généralement un serveur DHCP qui est toujours activé par défaut sur le LAN **L'administrateur** recevra des informations d'adresses IP du serveur DHCP sur **le routeur sans fil**.

a. Cliquez sur **Admin**, puis sélectionnez l'onglet **Bureau (Desktop)**.

b. Cliquez sur **Configuration IP** et sélectionnez **DHCP**.

Questions :

- Quelle est l'adresse IP de l'ordinateur ?
- Quel est le masque de sous-réseau de l'ordinateur ?
- Quelle est la passerelle par défaut de l'ordinateur ?

Activité 1 : Configuration de réseau sans fil- Packet Tracer

c. Fermez la fenêtre **IP Configuration**.

Remarque: les valeurs peuvent varier dans la gamme du réseau en raison d'un fonctionnement normal du DHCP.

Etape 3: Se connecter à l'interface web du routeur sans fil

a. Dans l'onglet **Bureau (Desktop)** de **Admin**, choisissez **Navigateur web (Web Browser)**.

b. Tapez **192.168.0.1** dans le champ de l'URL pour ouvrir la page de configuration web du routeur sans fil.

c. Utilisez **admin** comme nom d'utilisateur et mot de passe.

d. Sous le titre configuration réseau (Network Setup), à la page **Configuration de Base** (Basic Setup), observez la gamme d'adresses IP du serveur DHCP.

Question :

- est ce que L'adresse IP de **l'administrateur** est dans cette gamme ? Est-ce normal? Expliquez votre réponse.

Etape 4: Configurer Le Port Internet du routeur sans fil (WR)

Dans cette étape, **le routeur sans fil** est configuré pour diriger les paquets des clients sans fil à Internet. Vous allez configurer le port **Internet** sur le **routeur sans fil** pour vous connecter à Internet.

a. Dans **la Configuration Internet** ,en haut de la page **Configuration de base** , changez la méthode d'adressage IP de l'internet **Configuration automatique – DHCP** à **IP statique**.

b. Tapez l'adresse IP pour être attribuée à l'interface Internet comme suit :

- **Adresse IP Internet**: 209.165.200.225
- **Masque de sous-réseau**: 255.255.255.252
- **Passerelle par défaut**: 209.165.200.226
- **Serveur DNS**: 209.165.201.1

c. Défilez la page vers le bas, puis cliquez sur **Enregistrer les Paramètres**(Save Settings).

Remarque: si vous recevez le message **Expiration de la requête** , fermez la fenêtre Admin et attendez que les voyants oranges se transforment en triangles verts. Cliquez sur le bouton d'avance rapide pour accélérer ce processus. Ensuite, reconnectez-vous au **routeur sans fil** du navigateur de **l'administrateur** en utilisant le processus expliqué dans l'étape 3.

d. Pour vérifier la connectivité, ouvrez un nouveau navigateur web et naviguez au serveur **www.cisco.pka**

Remarque : il peut prendre quelques secondes avant que le réseau converge. Cliquez sur **Temps d'Avance Rapide** (Fast Forward Time) ou sur **Alt+D** pour accélérer le processus.

Partie 2: Configurer les paramètres sans fil

Dans cet exercice, vous allez seulement configurer les paramètres sans fil pour 2,4 GHz.

Etape 1: Configurer le SSID du routeur sans fil

a. Naviguez à une interface utilisateur graphique (GUI) du **routeur sans fil** à l'adresse **192.168.0.1** dans un navigateur web sur **Admin**.

Activité 1 : Configuration de réseau sans fil- Packet Tracer

b. Naviguez à **sans fil (Wireless) > paramètres sans fil de base**(Basic Wireless Settings).

c. Remplacez le **Nom du réseau (SSID)** par **aCompany** , seulement pour la fréquence 2,4 GHz. Notez que Les SSID sont sensibles à la casse.

d. Remplacez le **Canal standard** par **6 – 2,437 GHz**.

e. Dans cet exercice, désactivez les deux fréquences de 5 GHz. Laissez les autres paramètres tels quels.

f. Défiler la fenêtre jusqu'en bas et cliquez sur **Enregistrer les Paramètres**(Save Settings).

Etape 2: Configurer les paramètres de sécurité sans fil

Dans cette étape, vous configurez les paramètres de sécurité sans fil en utilisant le mode de sécurité WPA2 avec chiffrement et phrase secrète.

a. Naviguez à Sans fil (Wireless)> Sécurité sans fil (Wireless security).

b. Sous l'en-tête 2,4 GHz, sélectionnez WPA2 Personal pour un mode de sécurité.

c. Dans le champ Chiffrement, conservez le paramètre par défaut AES.

d. Dans le champ Phrase secrète, saisissez Cisco123! comme un phrase secrète.

e. Cliquez sur le bouton Enregistrer les paramètres (Save Settings).

f. Vérifiez que les paramètres des pages Paramètres sans fil de base (Basic Wireless Settings) et Sécurité sans fil (Wireless Security) sont corrects et enregistrés.

Etape 3: Connecter les clients sans fil

a. Ouvrez **Laptop1**. Cliquez sur l'onglet **Bureau**. Cliquez sur **PC sans fil**(PC Wireless).

b. Cliquez sur l'onglet **Connexion (Connect)**. Cliquez sur **Rafraîchir (Refresh)** si nécessaire. Sélectionnez le nom du réseau sans fil **aCompany**.

c. Saisissez la phrase secrète configurée à l'étape précédente. Saisissez **Cisco123!** Dans le champ Clé prépartagée et cliquez sur **Connexion**. Fermez la fenêtre Ordinateur sans fil.

d. Ouvrez un navigateur web et vérifiez que vous pouvez naviguez au serveur **www.cisco.pka**.

e. Répétez les étapes ci-dessus pour connecter **Laptop2** au réseau sans fil.

Partie 3: Connecter les clients sans fil à un point d'accès

Un point d'accès est un périphérique qui étend le réseau local sans fil. Un point d'accès est connecté à un routeur filaire à l'aide d'un câble Ethernet pour projeter le signal à l'emplacement souhaité.

Etape 1: Configurer le point d'accès

a. Connectez le **port 0** du **point d'accès** à un port Ethernet disponible du **routeur sans fil** à l'aide d'un câble Ethernet droit.

b. Cliquez sur **Point d'accès**. Sélectionnez l'onglet **Config**.

c. Sous le titre INTERFACE, sélectionnez **Port 1**.

d. Dans le champ SSID, saisissez **aCompany**.

Activité 1 : Configuration de réseau sans fil- Packet Tracer

e. Sélectionnez **WPA2-PSK**. Saisissez la phrase secrète **Cisco123!** Dans le champ Phrase secrète.

f. Conservez **AES** comme type de chiffrement par défaut.

Etape 1: Connecter les clients sans fil

a. Ouvrez **Laptop3**. Cliquez sur l'onglet **Bureau**. Cliquez sur **PC sans fil** (PC Wireless).

b. Cliquez sur l'onglet **Connexion**. Cliquez sur **Rafraîchir** si nécessaire. Sélectionnez le nom du réseau sans fil **aCompany** avec le signal le plus puissant (Canal 1) et cliquez sur **Connecter**.

c. Ouvrez un navigateur web et vérifiez que vous pouvez accéder au serveur **www.cisco.pka**.

Partie 4: Autres tâches administratives

Etape 1: Changer le mot de passe d'accès au routeur sans fil

a. Sur **Admin**, naviguez à l'interface utilisateur graphique GUI du routeur sans fil à l'adresse **192.168.0.1**.

b. Naviguez à **Administration > Gestion (Management)** et remplacez le **mot de passe du routeur** par **cisco**.

c. Défiler la fenêtre jusqu'en bas et cliquez sur **Enregistrez les Paramètres** (Save Settings).

d. Utilisez le nom d'utilisateur **admin** et le mot de passe **cisco** pour vous connecter au routeur sans fil. Cliquez sur **OK** pour continuer.

e. Cliquez sur **Continue** et passez à l'étape suivante.

Etape 2: Modifier la gamme d'adresses DHCP du routeur sans fil

Dans cette étape, vous allez remplacer l'adresse du réseau interne 192.168.0.0/24 par l'adresse 192.168.50.0/24. lorsque l'adresse du réseau LAN est modifiée, les adresses IP des périphériques du LAN et du sans fil doivent être renouvelées pour recevoir les nouvelles adresses IP avant l'expiration du bail.

a. Naviguez à la page **Configuration (Setup) > Configuration de Base** (Basic Setup).

b. Défilez la page vers le bas pour accéder à **Configuration Réseau** (Network Setup).

c. L'adresse IP attribuée à **Adresse IP du routeur** est 192.168.0.1. Remplacez-le par 192.168.50.1. Vérifiez que l'adresse IP commence toujours à .100 et que 50 adresses IP sont disponibles dans le pool DHCP.

d. Ajoutez **209.165.201.1** comme un serveur DNS avec les paramètres DHCP.

e. Défiler la fenêtre jusqu'en bas et cliquez sur **Enregistrez les Paramètres** (Save Settings).

f. Notez que la gamme d'adresses DHCP a été automatiquement mettre à jour pour refléter le changement d'adresse IP de l'interface. Le navigateur web affichera **Expiration du Requête** (Request Timeout) après un court instant.

Activité 1 : Configuration de réseau sans fil- Packet Tracer

Question :

- Pourquoi ?

g. Dans l'onglet **Bureau Admin**, cliquez sur **Invite de commandes**.

h. Tapez **ipconfig /renew** pour forcer **l'administrateur** à acquérir ses informations IP via DHCP.

Question :

- Quelles sont les nouvelles informations d'adresse IP de **l'administrateur**?

i. Vérifiez que vous pouvez toujours naviguer au serveur **www.cisco.pka** .

j. Renouvelez l'adresse IP sur les autres ordinateurs portables pour vérifier que vous pouvez toujours naviguer au serveur **www.cisco.pka**.

k. Notez que **Laptop1** est connecté au **point d'accès** au lieu de **WR**.

Question :

- Pourquoi ?

Activité 1 : Configuration de réseau sans fil- Packet Tracer

Réponses

- **Partie 1/ Etape 2 :**

b:

- 192.168.0.100
- 255.255.255.0
- 192.168.0.1

- **Partie 1/ Etape 3 :**

d: Oui. L'administrateur a 192.168.0.100/24 qui appartient à 192.168.0.0/24 et dans la plage de 192.168.0.100 à 192.168.0.149. Il est attendu car l'administrateur a acquis ses informations IP auprès de WR via DHCP.

- **Partie 4 / Etape 2:**

f: Parce que l'adresse IP de l'administrateur n'est plus dans le même réseau que le routeur. L'adresse IP d'Admin est en dehors de la nouvelle plage du serveur DHCP.

h: Votre réponse peut varier. L'adresse IP de l'administrateur est comprise entre 192.168.50.100 et 149.

IP Address: 192.168.50.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.50.1

DNS Server: 209.165.201.1

k: L'AP avait un meilleur signal pour Laptop1.

PARTIE 4

Activité 2 : Configuration de WLAN de base sur le WLC - Packet Tracer

Objectifs

Dans ce travail pratique, vous allez explorer certaines des fonctionnalités d'un contrôleur LAN sans fil. Vous allez créer un nouveau WLAN sur le contrôleur et implémenter la sécurité sur ce LAN. Ensuite, vous allez configurer un hôte sans fil pour se connecter au nouveau WLAN via un point d'accès qui est sous le contrôle du WLC. Enfin, vous vérifierez la connectivité.

- **Connectez-vous à une interface graphique (GUI) de contrôleur LAN sans fil.**
- **Expliquez certaines des informations disponibles sur l'écran du moniteur WLC.**
- **Configurez un WLAN sur un contrôleur LAN sans fil.**
- **Implémentez la sécurité sur un WLAN.**
- **Configurez un hôte sans fil pour se connecter à un LAN sans fil.**

Contexte / Scénario

Une organisation centralise le contrôle de son LAN sans fil en remplaçant ses points d'accès autonomes par des points d'accès légers (LAP) et un contrôleur LAN sans fil (WLC). Vous dirigerez ce projet et vous souhaitez vous familiariser avec le WLC et tout défi potentiel pouvant survenir pendant le projet. Vous allez configurer un WLC en ajoutant un nouveau réseau sans fil et en le sécurisant avec la sécurité WPA-2 PSK. Pour tester la configuration, vous connecterez un ordinateur portable au réseau local sans fil et exécuterez une commande ping sur le réseau.

Table d'adressage

Périphérique	Interface	Adresse IP
R-1	G/0/0	172.31.1.1/24
	G0/0/1.5	192.168.5.1/24
	G0/0/1.200	192.168.200.1/24
SW-1	VLAN 200	192.168.200.100/24
LAP-1	G0	DHCP
WLC-1	Gestion	192.168.200.254/24
Serveur	Carte réseau (NIC)	172.31.1.254/24
Ordinateur de l'utilisateur admin	Carte réseau (NIC)	192.168.200.200/24
Hôte sans fil	Carte réseau sans fil (NIC)	DHCP

Instructions

Partie 1: Surveiller le WLC

Attendez que STP ait convergé sur le réseau. Vous pouvez cliquer sur le bouton Packet Tracer Avance Rapide pour accélérer le processus. Continuez lorsque tous les voyants de liaison sont verts.

a. Allez sur le bureau **d'Admin PC** et ouvrez un navigateur. Entrez l'adresse IP de gestion de **WLC-1** de la table d'adressage dans la barre d'adresse. Vous devez spécifier le protocole **HTTPS** .

b. Cliquez sur **login** et entrez ces informations d'identification: Nom d'utilisateur: **admin**, Mot de passe: **Cisco123**. Après un court délai, vous verrez l'écran Résumé du moniteur WLC.

Activité 2 : Configuration de WLAN de base sur le WLC – Packet Tracer

Remarque: Packet Tracer ne prend pas en charge le tableau de bord initial présenté dans ce module.

c. Faites défiler l'écran Résumé du moniteur.

Question :

- Que peut-on apprendre de cet écran?
- Le WLC est-il connecté à un AP?

d. Cliquez sur Détails à côté de l'entrée Tous les points d'accès dans la section Résumé du point d'accès de la page. Quelles informations pouvez-vous trouver sur les points d'accès sur l'écran Tous les points d'accès?

Vous allez maintenant créer un nouveau LAN sans fil sur le WLC. Vous allez configurer les paramètres requis pour que les hôtes rejoignent le WLAN.

Partie 2: Créer un réseau WLAN

Etape 1: Créer et activer le WLAN

a. Cliquez sur **WLAN** dans la barre de menus WLC. Recherchez la liste déroulante dans le coin supérieur droit de l'écran WLAN. Il dira **Créer nouveau**. Cliquez sur **Allez** pour créer un nouveau WLAN.

b. Saisissez le **nom de profil** du nouveau WLAN. Utilisez le nom du profil **Floor 2 Employees.** Attribuez un SSID de **SSID-5** au WLAN. Les hôtes devront utiliser ce SSID pour rejoindre le réseau.

c. Sélectionnez **l'ID** du WLAN. Cette valeur est une étiquette qui sera utilisée pour identifier le WLAN dans d'autres affichages. Sélectionnez une valeur de **5** pour la garder cohérente avec le numéro de VLAN et le SSID. Ce n'est pas une exigence mais cela aide à comprendre la topologie.

a. Cliquez sur **Appliquer** pour que les paramètres prennent effet.

b. Maintenant que le WLAN a été créé, vous pouvez configurer les fonctionnalités du réseau. Cliquez sur **Activé** pour rendre le WLAN fonctionnel. C'est une erreur courante de sauter accidentellement cette étape.

c. Choisissez l'interface VLAN qui sera utilisée pour le WLAN. Le WLC utilisera cette interface pour le trafic utilisateur sur le réseau. Cliquez sur la liste déroulante pour Interface/Groupe d'interfaces (G). Sélectionnez l'interface **WLAN-5** . Cette interface a été précédemment configurée sur le WLC pour cette activité.

d. Cliquez sur l'onglet **Avancé** .

e. Faites défiler jusqu'à la partie Flex Connect de la page. Cliquez pour activer **la commutation locale FlexConnect** et **l'authentification locale FlexConnect**.

f. Cliquez sur **Appliquer** pour activer le nouveau WLAN. Si vous oubliez de le faire, le WLAN ne fonctionnera pas.

Etape 2: Sécuriser le WLAN

Le nouveau WLAN n'a actuellement aucune sécurité en place. Ce WLAN utilisera initialement la sécurité WPA2-PSK. Dans une autre activité, vous allez configurer le WLAN pour utiliser WPA2-Enterprise, une bien meilleure solution pour les grands réseaux sans fil.

g. Dans l'écran d'édition des WLAN pour le WLAN des employés de l'étage 2, cliquez sur l'onglet **Sécurité** . Sous l'onglet **Couche 2** , sélectionnez **WPA + WPA2** dans la liste déroulante **Sécurité de couche 2** . Cela révélera les paramètres WPA.

h. Cochez la case à côté de **Stratégie WPA2**. Cela révèlera des paramètres de sécurité supplémentaires. Sous **Gestion des clés d'authentification**, activez **PSK**.

Activité 2 : Configuration de WLAN de base sur le WLC - Packet Tracer

a. Vous pouvez maintenant entrer la clé pré-partagée qui sera utilisée par les hôtes pour rejoindre le WLAN. Utilisez **Cisco123** comme mot de passe.

b. Cliquez sur **Appliquer** pour enregistrer ces paramètres.

Remarque: il n'est pas recommandé de réutiliser les mots de passe lors de la configuration de la sécurité. Nous avons réutilisé les mots de passe dans cette activité pour simplifier la configuration.

Etape 3: Vérifier les paramètres

a. Après avoir appliqué la configuration, cliquez sur **Retour**. Cela vous ramènera à l'écran des WLAN.

Question:

- Quelles informations sur le nouveau WLAN sont disponibles sur cet écran?

b. Si vous cliquez sur l'ID WLAN, vous serez redirigé vers l'écran d'édition des WLAN. Utilisez-le pour vérifier et modifier les détails des paramètres.

Partie 2: Connecter un hôte au WLAN

Etape 1: Connectez-vous au réseau et vérifiez la connectivité

a. Accédez au bureau de **Wireless Host** et cliquez sur la vignette **PC Wireless** .

b. Cliquez sur l'onglet **Connect** (Connexion). Après un bref délai, vous devriez voir le SSID du WLAN apparaître dans le tableau des noms de réseau sans fil. Sélectionnez le réseau **SSID-5** et cliquez sur le bouton **Connecter** .

c. Entrez la clé pré-partagée que vous avez configurée pour le WLAN et cliquez sur **Connecter**.

d. Cliquez sur l'onglet **Informations sur le lien** . Vous devriez voir un message confirmant que vous vous êtes correctement connecté au point d'accès. Vous devriez également voir une onde sans fil dans la topologie montrant la connexion au LAP-1.

e. Cliquez sur le bouton **Plus d'informations** pour voir les détails de la connexion.

f. Fermez l'application PC Wireless et ouvrez l'application de configuration IP. Vérifiez que l'hôte sans fil a reçu une adresse IP non-APIPA via DHCP. Sinon, cliquez plusieurs fois sur le bouton Fast Forward Time.

g. À partir de l'hôte sans fil, envoyez une requête ping à la passerelle par défaut WLAN et au serveur pour vérifier que l'ordinateur portable dispose d'une connectivité complète.

Activité 2 : Configuration de WLAN de base sur le WLC - Packet Tracer

Réponses

- **Partie 1 / Etape 1 :**

c :

- Les réponses varieront. De nombreuses informations précieuses peuvent être trouvées ici, y compris des informations de fonctionnement sur le WLC, des informations sur les points d'accès connus et les clients connectés, ainsi que sur les points d'accès et les clients indésirables qui ont été détectés sur le réseau.
- Oui, le WLC est connecté à un point d'accès. Ceci est affiché dans la section Résumé des points d'accès de la page.

d: Les informations affichées sur le WLC incluent le nom de l'AP, l'adresse IP de l'AP, le modèle de périphérique, le MAC, la version du logiciel, l'état opérationnel, la source d'alimentation, etc.

- **Partie 2 / Etape 3 :**

a: Le nom du WLAN, le SSID, la politique de sécurité et l'état de l'administrateur sont disponibles ici. La valeur Admin Status indique si le WLAN est opérationnel ou non.

PARTIE 4

Activité 3 : Configuration de réseau sans fil WPA2 Entreprise sur le WLC – Packet Tracer

Objectifs

Dans cette activité, vous allez configurer un nouveau WLAN sur un contrôleur LAN sans fil (WLC), y compris l'interface VLAN qu'il utilisera. Vous allez configurer le WLAN pour utiliser un serveur RADIUS et WPA2-Enterprise pour authentifier les utilisateurs. Vous allez aussi configurer le WLC pour utiliser un serveur SNMP.

- **Configurer une nouvelle interfaces VLAN sur un WLC.**
- **Configurer un nouvel WLAN sur un WLC.**
- **Configurer une nouvelle étendue sur le WLC interne de serveur DHCP.**
- **Configurer le WLC avec les paramètres SNMP.**
- **Configurer le WLC pour l'utilisateur de serveur RADIUS pour authentifier les utilisateurs WLAN.**
- **Sécuriser un WLAN avec WPA2-Enterprise.**
- **Connecter les hôtes au nouvel WLC.**

Contexte/scénario

Vous avez déjà configuré et testé le WLC avec un WLAN existant. Vous avez configuré WPA2-PSK pour ce WLAN car il devait être utilisé dans une petite entreprise. Vous avez été demander de configurer et de tester une topologie WLC qui sera utilisée dans une grande entreprise. Vous savez que WPA2-PSK ne s'adapte pas bien et n'est pas approprié pour l'utiliser dans un réseau d'entreprise. cette nouvelle topologie va utiliser un serveur RADIUS et WPA2-Enterprise pour authentifier les utilisateurs de réseau sans fil WLAN.

Cela permet l'administration des comptes d'utilisateurs à partir d'un emplacement central d'offrir une sécurité et une transparence améliorées car chaque compte a son propre nom d'utilisateur et mot de passe. En plus, l'activité de l'utilisateur est enregistrée sur le serveur.

Dans ce travaux pratiques, vous allez créer une nouvelle interface VLAN, utilisez cette interface pour créer un nouveau WLAN et sécuriser ce WLAN avec WPA2-Enterprise. Vous allez configurer également le WLC pour utiliser le serveur RADIUS d'entreprise pour authentifier les utilisateurs. En plus, vous allez configurer le WLC pour utiliser un serveur SNMP.

Table d'adressage

Appareil	Interface	Adresse IP
R1	G0/0/0.5	192.168.5.1/24
	G0/0/0.200	192.168.200.1/24
	G0/0/1	172.31.1.1/24
Commutateur 1 (SW1)	VLAN 200	192.168.200.100/24
LAP-1	G0	DHCP
WLC-1	Gestion	192.168.200.254/24
Serveur RADIUS/SNMP	Carte réseau (NIC)	172.31.1.254/24
Ordinateur de l'utilisateur admin	Carte réseau (NIC)	192.168.200.200/24

Activité 3 : Configuration de réseau sans fil WPA2 Entreprise sur le WLC – Packet Tracer

- **Instructions**
  - **Partie 1: Créer un nouveau WLAN**

Etape 1: Créer une nouvelle interface de VLAN

Chaque WLAN nécessite une interface virtuelle sur le WLC. Ces interfaces sont appelées interfaces dynamiques. L'interface virtuelle est attribuée à un ID VLAN et le trafic qui utilise l'interface sera étiqueté comme trafic VLAN. C'est pourquoi les connexions entre les points d'accès, le WLC et le routeur existent via des ports truncs. Pour que le trafic provenant de plusieurs WLAN soit transporté via le réseau, le trafic des WLAN VLAN doit être agrégé.

a. Ouvrez le navigateur du bureau d'Admin PC. Connectez-vous à l'adresse IP du WLC via HTTPS.

b. Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **Cisco123**.

c. Cliquez le menu **Contrôleur** et puis cliquez **Interfaces** dans le menu de gauche. Vous verrez l'interface virtuelle par défaut et l'interface de gestion à laquelle vous êtes connecté.

d. Cliquez sur le bouton **Nouveau** (New) dans le coin supérieur droit de la page. Vous devrez peut-être défiler la page vers la droite pour le voir.

e. Saisissez le nom du nouvelle interface. Nous l'appellerons **WLAN-5**. Configurez l'ID VLAN comme **5**. Il s'agit du VLAN qui acheminera le trafic pour le WLAN que nous créerons plus tard. Cliquez sur **Appliquer** (Apply). Cela conduit à un écran de configuration pour l'interface VLAN.

f. D'abord, configurez l'interface pour utiliser le port physique numéro **1**. Plusieurs interfaces VLAN peuvent utiliser le même port physique car les interfaces physiques sont comme des ports de trunc dévoués

g. Adressez les interface comme suivants :

- Adresse IP de l'interface : **192.168.5.254**
- Masque réseau: **255.255.255.0**
- Passerelle: **192.168.5.1**
- Serveur DHCP primaire: **192.168.5.1**

Le trafic d'utilisateur pour le WLAN qui utilise cette interface VLAN sera sur le réseau 192.168.5.0/24. La passerelle par défaut est l'adresse d'une interface sur le routeur R-1. Un pool DHCP a été configuré sur le routeur. L'adresse que nous configurons ici pour DHCP indique au WLC de transmettre toutes les requêtes DHCP qu'il reçoit des hôtes sur le WLAN au serveur DHCP sur le routeur.

h. Assurez-vous de cliquer sur **Appliquer** pour appliquer vos modifications et sur **OK** pour répondre au message d'avertissement. Cliquez sur **Enregistrer la Configuration** pour que votre configuration soit effectué quand le WLC recommence.

Etape 2: Configurer le WLC pour utiliser un serveur RADIUS

WPA2-Enterprise utilise un serveur RADIUS externe pour authentifier les utilisateurs WLAN. Des comptes d'utilisateurs individuels avec des noms d'utilisateur et des mots de passe uniques peuvent être configurés sur le serveur RADIUS. Avant que le WLC puisse utiliser les services du serveur RADIUS, le WLC doit être configuré avec l'adresse du serveur.

Activité 3 : Configuration de réseau sans fil WPA2 Entreprise sur le WLC - Packet Tracer

a. Cliquez sur le menu **Sécurité** sur le WLC.

b. Cliquez sur le button **Nouveau** et entrez l'adresse IP du serveur RADIUS dans le champ Adresse IP du serveur.

c. Le serveur RADIUS authentifiera le WLC avant de lui permettre d'accéder aux informations de compte d'utilisateur qui se trouvent sur le serveur. Cela nécessite une valeur secrète partagée. Utilisez **Cisco123**. Confirmez le secret partagé et cliquez sur **Appliquer**.

Remarque: Il n'est pas recommandé de réutiliser les mots de passe. Cette activité réutilise les mots de passe seulement pour vous permettre de la terminer et de la réviser plus facilement.

Etape 3: Créer un nouveau WLAN

Créez un nouveau WLAN. Utilisez la nouvelle interface VLAN créée pour le nouveau WLAN.

a. Cliquez sur l'entrée **WLAN** dans la barre de menus. Recherchez la liste déroulante dans le coin supérieur droit de l'écran WLAN. Il dira **Créer nouveau**. Cliquez sur **Allez** pour créer un nouveau WLAN.

b. Saisissez le **Nom de Profil** du nouveau WLAN. Utilisez le nom du profil **Floor 2 Employees.** Attribuez un SSID de **SSID-5** au WLAN. Modifiez le menu déroulant ID à **5**. Les hôtes devront utiliser ce SSID pour rejoindre le réseau. Lorsque vous terminerez, cliquez sur **Appliquer** pour accepter vos paramètres.

Remarque: L'ID est une valeur arbitraire qui est utilisée comme étiquette pour le WLAN. Dans ce cas, nous l'avons configuré sur 5 pour être cohérent avec le VLAN pour le WLAN. Il peut s'agir de n'importe quelle valeur disponible.

a. Cliquez sur **Appliquer** pour que les paramètres prennent effet.

b. Maintenant que le WLAN a été créé, vous pouvez configurer les fonctionnalités du réseau. Cliquez sur **Activé** pour rendre le WLAN fonctionnel. C'est une erreur courante de sauter accidentellement cette étape.

c. Choisissez l'interface VLAN qui sera utilisée pour le nouveau WLAN. Le WLC utilisera cette interface pour le trafic utilisateur sur le réseau. Cliquez sur la liste déroulante pour Interface/Groupe d'interfaces (G). Sélectionnez l'interface que nous avons créée à l'étape 1.

d. Cliquez sur l'onglet Avancé . Défiler jusqu'à la section **FlexConnect** de l'interface.

e. Cliquez pour activer **la commutation locale FlexConnect** et **l'authentification locale FlexConnect**.

f. Cliquez sur **Appliquer** pour activer le nouveau WLAN. Si vous oubliez de le faire, le WLAN ne fonctionnera pas.

Etape 4: Configurez La Sécurité WLAN

Au lieu de WPA2-PSK, nous allons configurer le nouveau WLAN pour utiliser WPA2-Enterprise.

a. Cliquez sur l'ID WLAN du WLAN nouvellement créé pour continuer à le configurer, si nécessaire.

b. Cliquez sur l'onglet Sécurité. Sous l'onglet Couche 2 , sélectionnez **WPA + WPA2** dans la boîte déroulante.

Activité 3 : Configuration de réseau sans fil WPA2 Entreprise sur le WLC – Packet Tracer

c. Sous les paramètres WPA + WPA2, activez **la stratégie WPA2**. Cliquez **802.1X** sous Gestion des clés d'authentification. Ceci indique au WLC d'utiliser le protocole 802.1X pour authentifier les utilisateurs en externe.

d. Cliquez sur l'onglet **Serveur AAA** . Ouvrez la liste déroulante à côté de Serveur 1 dans la colonne Serveurs d'authentification et sélectionnez le serveur que nous avons configuré à l'étape 2.

e. Cliquez sur **Appliquez** pour terminer cette configuration. Vous avez maintenant configuré le WLC pour utiliser le serveur RADIUS pour authentifier les utilisateurs qui tentent de se connecter au WLAN.

Partie 2: Configurer une portée DHCP et SNMP

Etape 1: Configurez une portée DHCP

Le WLC propose son propre serveur DHCP interne. Cisco recommande de ne pas utiliser le serveur DHCP WLAN pour les services DHCP à haut volume, tels que ceux requis par plusieurs utilisateurs de WLAN. Cependant, dans les petits réseaux, le serveur DHCP peut être utilisé pour fournir des adresses IP aux LAP qui sont connectés au réseau de gestion câblé. Dans cette étape, nous allons configurer une portée DHCP sur le WLC et l'utiliser pour adresser LAP-1.

a. Vous devez connecté à l'interface graphique GUI de WLC à partir du PC d'administration.

b. Cliquez le menu **Contrôleur** et puis cliquez **Interfaces**.

Question :

- Quelles interfaces sont présentes?

c. Cliquez la **gestion** d'interface. Enregistrez ses informations d'adressage ici.

- Adresse IP :
- Masque réseau :
- Passerelle :
- Serveur DHCP principal:

d. Nous voulons que le WLC utilise son propre serveur DHCP pour fournir l'adressage aux périphériques sur le réseau de gestion sans fil, tels que les points d'accès légers. Pour cette raison, entrez l'adresse IP de l'interface de gestion WLC comme adresse de serveur DHCP principale. Cliquez sur **Apply** (Appliquer). Cliquez sur **OK** pour accuser la réception des messages d'avertissement qui s'affichent.

e. Dans le menu de gauche, développez la section **Serveur DHCP interne** . Cliquez sur **DHCP Scope**.

f. Pour créer une portée DHCP, cliquez sur le bouton **Nouveau...**

g. Nommez la portée **Gestion câblé**. Vous allez configurer cette portée DHCP pour fournir des adresses au réseau d'infrastructure filaire qui connecte le PC Admin, WLC-1 et LAP-1.

h. Cliquez sur **Appliquez** pour créer le VLAN.

i. Cliquez sur la nouvelle portée dans la table des portées DHCP pour configurer les informations d'adressage pour la portée. Saisissez les informations suivantes :

- Adresse de début du pool: **192.168.200.240**
- Adresse de fin du pool: **192.168.200.249**
- Statut : **Activé**

Activité 3 : Configuration de réseau sans fil WPA2 Entreprise sur le WLC - Packet Tracer

Fournissez les valeurs du **Réseau**, du **Masque de Réseau** et **des Routeurs par Défaut** à partir des informations que vous avez collectées à l'étape 1c.

j. Cliquez sur **Appliquer** pour activer les configurations. Cliquez sur **Enregistrer la configuration** dans le coin supérieur droit de l'interface WLC pour enregistrer votre travail afin qu'il soit disponible lorsque le WLC redémarrer.

Le serveur DHCP interne fournira une adresse à LAP-1 après un bref délai. Lorsque LAP-1 aura son adresse IP, le tunnel CAPWAP sera établi et LAP-1 pourra fournir l'accès au WLAN des Floor 2 Employees (SSID-5). Si vous déplacez la souris sur LAP-1 dans la topologie, vous devriez voir son adresse IP, l'état du tunnel CAPWAP et le WLAN auquel LAP-1 fournit l'accès.

Etape 2: Configurer le SNMP:

a. Cliquez sur le menu de **Gestion** dans l'interface graphique WLC et développez l'entrée pour **SNMP** dans le menu de gauche.

b. Cliquez sur **Trap Receivers** puis sur **New…**

c. Entrez la chaîne de communauté comme **WLAN_SNMP** et l'adresse IP du serveur à **172.31.1.254**.

d. Cliquez sur **Appliquez** pour terminer la configuration.

- **Partie 3: Connecter les hôtes au réseau**

Etape 1: Configurer un hôte pour se connecter au réseau d'entreprise

Dans l'application client Packet Tracer PC Wireless, vous devez configurer un profil WLAN pour se connecter à un WLAN WPA2-Enterprise.

a. Cliquez sur Hôte sans fil et accédez à l'application **PC Wireless** .

b. Cliquez sur l'onglet **Profils** , puis sur **Nouveau** pour créer un nouveau profil. Nommez le profil **WLC NET**.

c. Mettez en surbrillance le nom du réseau sans fil pour le WLAN que nous avons créé précédemment et cliquez sur **Configuration Avancée**.

d. Vérifiez que le SSID du LAN sans fil est présent, puis cliquez sur **Suivant**. L'hôte sans fil devrait voir SSID-5. Si ce n'est pas le cas, déplacez la souris sur LAP-1 pour vérifier qu'il communique avec le WLC. La boîte de dialogue devrait indiquer que LAP-1 connaît le SSID-5. Si ce n'est pas le cas, vérifiez la configuration WLC. Vous pouvez également saisir manuellement le SSID.

e. Vérifiez que le paramètre de réseau DHCP est sélectionné et cliquez sur **Suivant**.

f. Dans la liste déroulante Sécurité, sélectionnez **WPA2-Enterprise**. Cliquez sur **Next (Suivant)**.

g. Entrez le nom de connexion **user1** et le mot de passe **User1Pass** et cliquez sur **Suivant**.

h. Vérifiez les paramètres de profil et cliquez sur **Enregistrer**.

i. Sélectionnez le profil **WLC NET** et cliquez sur le bouton **Connecter au réseau** . Après un bref délai, vous devriez voir l'hôte sans fil se connecter au LAP-1. Vous pouvez cliquer sur le bouton Fast Forward Time pour accélérer le processus s'il prend trop de temps.

Activité 3 : Configuration de réseau sans fil WPA2 Entreprise sur le WLC - Packet Tracer

j. Confirmez que l'hôte sans fil s'est connecté au WLAN. L'hôte sans fil doit recevoir une adresse IP du serveur DHCP configuré pour les hôtes sur R1. L'adresse sera dans le réseau 192.168.5.0/24. Vous devrez peut-être cliquer sur le bouton Fast Forward Time pour accélérer le processus.

Etape 2: vérification de la connectivité

a. Fermez l'application PC Wireless.

b. Ouvrez une invite de commande et vérifiez que l'ordinateur portable qui est l'hôte sans fil a obtenu une adresse IP à partir du réseau WLAN.

Question :

- Dans quel réseau l'adresse doit-elle se trouver? Expliquez votre réponse.

c. Envoyez une requête ping à la passerelle par défaut, au SW1 et au serveur RADIUS. Le succès indique une connectivité complète dans cette topologie.

Questions de réflexion

a. Le serveur RADIUS utilise un mécanisme double d'authentification . Quelles sont les deux éléments authentifiées par le serveur RADIUS? Pourquoi pensez-vous que c'est nécessaire?

b. Quels sont les avantages de WPA2-Enterprise par rapport à WPA2-PSK?

Activité 3 : Configuration de réseau sans fil WPA2 Entreprise sur le WLC – Packet Tracer

Réponses

- **Partie 2 / Etape 1 :**

b : WLAN-5, management, and virtual.

c:

- IP address: 192.168.200.254
- Netmask: 255.255.255.0
- Gateway: 192.168.200.1
- Primary DHCP server: none specified

- **Partie 2 / Etape 1 :**

b : L'adresse doit être dans le réseau 192.168.5.0/24. L'interface a été configurée pour obtenir son adresse IP à partir de 192.168.5.1. Il s'agit de l'adresse de la sous-interface du routeur pour le VLAN 5. DHCP s'exécute sur le routeur pour fournir des adresses aux hôtes sans fil.

Questions de réflexion

a: Le serveur RADIUS authentifie à la fois le WLC et l'hôte sans fil. Le WLC effectue la demande d'authentification au nom de l'hôte sans fil. Il est nécessaire d'authentifier le WLC car il est important de protéger les tables de noms d'utilisateurs et de mots de passe du serveur RADIUS contre les intrusions par des périphériques non autorisés. C'est pourquoi un secret partagé est requis lors de la configuration du WLC pour utiliser le serveur RADIUS.

b: WPA2-PSK exige que tous les hôtes utilisent le même mot de passe. De plus, un nom d'utilisateur n'est pas requis. Cela signifie qu'il est plus difficile de surveiller le moment où les utilisateurs se connectent et se déconnectent du réseau. De plus, étant donné que de nombreux hôtes utilisent le même mot de passe, il est plus facile pour un pirate de voler le mot de passe et d'accéder au réseau. Enfin, si le mot de passe PSK doit être changé, tous les utilisateurs doivent être informés du nouveau mot de passe. Cela crée également une probabilité plus élevée que le mot de passe soit volé. WPA2-Enterprise utilisant RADIUS permet la création et l'administration de plusieurs comptes d'utilisateurs uniques. Le comportement des utilisateurs peut facilement être audité à partir des journaux conservés par le serveur RADIUS. De plus, les utilisateurs peuvent facilement être supprimés ou ajoutés au fur et à mesure que le personnel change dans l'entreprise.

Activité 4 : Résolution des problèmes de WLAN- Packet Tracer

- **Objectifs**

Dans cette activité, vous allez résoudre des différents problèmes liés aux réseaux sans fil domestiques et aux réseaux sans fil d'entreprise.

- **Résoudre les problèmes de connectivité LAN sans fil dans un réseau domestique.**
- **Résoudre les problèmes de connectivité LAN sans fil dans un réseau d'entreprise.**

- **Contexte/scénario**

Maintenant que vous avez appris à configurer le sans fil dans les réseaux domestiques et d'entreprise, vous devez apprendre à dépanner les deux dans les environnements sans fil. Votre objectif est d'activer la connectivité entre les hôtes des réseaux et le serveur Web par l'adresse IP et l'URL. La connectivité entre les réseaux domestique et d'entreprise n'est pas requise.

Pour accéder Le Routeur domestique sans fil, le mot d'utilisateur et le mot de passe est **admin**.

Le nom d'utilisateur de l'interface de gestion WLC est **admin** et le mot de passe est **Cisco123**

- **Table d'adressage**

Appareil	Interface	Adresse IP
Routeur sans fil domestique	Internet	DHCP
	Réseau local (LAN)	192.168.0.1
R1	G0/0/0.10	192.168.10.1/24
	G0/0/0.20	192.168.20.1/24
	G0/0/0.200	192.168.200.1/24
	G0/0/1	172.31.1.1/24
Commutateur 1 (SW1)	le VLAN 200	192.168.200.100/24
LAP-1	G0	DHCP
WLC-1	Gestion	192.168.200.254/24
Serveur RADIUS	Carte réseau (NIC)	172.31.1.254/24
PC administratif	Carte réseau (NIC)	192.168.200.200/24
Serveur web	Carte réseau	203.0.113.78/24
Serveur DNS	Carte réseau (NIC)	10.100.100.254
L'Administrateur domestique	Carte réseau (NIC)	DHCP
Ordinateur portable	Carte réseau (NIC)	DHCP
Ordinateur portable1	Sans Fil 0	DHCP
Ordinateur Portable 2	Sans Fil 0	DHCP
Tablette PC	Sans fil 0	DHCP
Smartphone	Sans Fil 0	DHCP

Activité 4 : Résolution des problèmes de WLAN- Packet Tracer

- **L'information de réseau sans fil (WLAN)**

WLAN	SSID	Authentification	Nom d'utilisateur	Mot de passe
Réseau domestique	SSID domestique	WPA2-Personal	S/O	Cisco123
VLAN10 de Réseau sans fil (WLAN)	SSID-10	WPA-2 PSK/Personal	S/O	Cisco123
VLAN 20 de réseau sans fil (WLAN)	SSID-20	WPA-2 802.1x/Enterprise	user2	user2pass

- **Instructions**

  - **Partie 1: Résoudre les problèmes du réseau**

Remarque: Vous ne dépannerez que le routeur sans fil domestique, le WLC et les périphériques hôtes sans fil dans cette activité.

Etape 1: Tester la connectivité

a. Testez la connectivité entre les hôtes sans fil et le serveur Web par utiliser l'adresse IP et le URL. **www.netacad.pt**.

b. Enregistrez les hôtes qui ne peuvent pas accéder au serveur Web dans la table de l'étape 2.

Etape 2: Chercher les problèmes et enregistrer les résultats

a. Cherchez les problèmes de connectivité avec chaque hôte. Les problèmes peuvent être à la configuration de l'hôte ou d'autres composants de réseau sans fil.

b. Complétez la table.

Appareil	Réseau Domestique/Entreprise	Problème	Solution

  - **Partie 2: Résoudre les problèmes**

Modifiez les configurations de périphérique pour que les hôtes puissent atteindre la connectivité avec le réseau. Testez pour vous assurer que tous les hôtes peuvent atteindre l'objectif de communication de se connecter au serveur Web par l'adresse IP et l'URL.

PARTIE 4

Activité 4 : Résolution des problèmes de WLAN- Packet Tracer

Réponses

- **Partie 1 /Etape 2 :**

b)

Appareil	Réseau Domestique/Entreprise	Problème	Solution
Smartphone, Tablet PC, Laptop	Home	Impossible d'accéder à l'URL du serveur par son nom. L'adresse du serveur DNS est mal configurée sur le serveur DHCP du routeur sans fil domestique.	Remplacez l'adresse statique du serveur DHCP du routeur sans fil domestique par 10.100.100.254
Tablet PC	Home	Client défini sur l'adressage statique	Doit être défini sur DHCP.
Wireless router	Home	L'interface Internet est définie sur statique.	Définir l'interface Internet sur DHCP
WLC	Enterprise	WLAN Wireless VLAN 20 n'est pas activé.	Activez le WLAN et appliquez.
Laptop 2	Enterprise	L'ordinateur portable 2 ne se connecte pas au VLAN sans fil 20. Nom d'utilisateur incorrect dans le profil client.	Remplacez le nom d'utilisateur par user2.
WLC	Enterprise	L'ordinateur portable 1 ne peut pas se connecter au WLAN. Sur le WLC, WLAN-Wireless VLAN 10 a la gestion des clés d'authentification définie sur 802.1x plutôt que PSK, qui est la configuration requise pour la sécurité WPA2 PSK.	Modifiez la gestion des clés d'authentification sur PSK, entrez la valeur PSK à partir du tableau WLAN.

PARTIE 5

Mettre en œuvre le routage d'un réseau d'entreprise

Dans ce module, vous allez :

- Etre en mesure de comprendre les mécanismes du routage
- Etre en mesure de comprendre les concepts des protocoles de routage
- Etre capable de configurer les protocoles de routage OSPF et BGP

17 heures

TP 1

Implémenter les routes statique et par défaut

Compétences visées :

- Configurer les routes statiques et par défaut

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

5 heures

TP 1

Implémenter les routes statique et par défaut

1. Configuration des routes statiques et par défaut

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer et Dépanner les routes statique et par défaut?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 5

Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

- **Objectifs**

- **Partie 1: création d'un réseau et configuration des paramètres de base des périphériques**
- **Partie 2: configurer et vérifier l'adressage IPv4 et IPv6 sur R1 et R2**
- **Partie 3: configurer et vérifier le routage statique et par défaut IPv4 sur R1 et R2**
- **Partie 4: configurer et vérifier le routage statique et par défaut IPv6 sur R1 et R2**

- **Contexte/scénario**

Le routage statique et le routage par défaut sont les formes les plus simples de routage réseau et configurées manuellement. Ils sont fixes, ce qui signifie qu'ils ne changent pas dynamiquement pour répondre aux conditions changeantes du réseau. Elles sont valides et mises à la disposition de la table de routage ou non valides et non mises à la disposition de la table de routage. Les routes statiques ont une distance administrative par défaut de 1. Toutefois, les routes statiques et par défaut peuvent être configurées avec une distance administrative définie par l'administrateur. Cette fonctionnalité permet à l'administrateur de mettre la route statique ou par défaut en réserve et de le rendre disponible à la table de routage uniquement lorsque les routes dont les distances administratives sont inférieures (généralement générées par des protocoles de routage dynamiques) ne sont plus valides.

Remarque : Dans ces Travaux Pratiques, vous allez configurer des routes statiques, par défaut et flottantes IPv4 et IPv6, ce qui peut ne pas refléter les meilleures pratiques de mise en réseau.

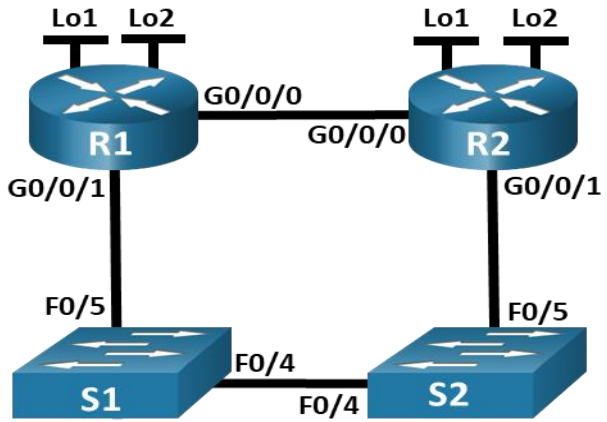
Remarque: Les routeurs utilisés dans les travaux pratiques CCNA sont Cisco 4221 équipé de version 16.9.4 de Cisco IOS XE (image universalk9). Les commutateurs utilisés dans les travaux pratiques sont des modèles Cisco Catalyst 2960s équipé de version 15.2.2 de Cisco IOS (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques.

Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque: Assurez-vous que les routeurs et les commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre formateur.

Remarque : Dans ces Travaux Pratiques, vous allez configurer des routes statiques, par défaut et flottantes IPv4 et IPv6, ce qui peut ne pas refléter les meilleures pratiques de mise en réseau.

- **Topologie**



Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

- **Table d'adressage**

Appareil	Interface	Adresse IP / Préfixe
R1	G0/0/0	172.16.1.1 /24
		2001:db8:acad:2::1 /64
		fe80::1
	G0/0/1	192.168.1.1 /24
		2001:db8:acad:1 /64
		fe80::1
	Loopback1	10.1.0.1 /24
		2001:db8:acad:10::1 /64
		fe80::1
	Loopback2	209.165.200.225 /27
		2001:db8:acad:209:: 1 /64
		fe80::1
R2	G0/0/0	172.16.1.2 /24
		2001:db8:acad:2::2 /64
		fe80::2
	G0/0/1	192.168.1.2 /24
		2001:db8:acad:1::2 /64
		fe80::2
	Loopback1	10.2.0.1 /24
		2001:db8:acad:11::2 /64
		fe80::2
	Loopback2	209.165.200.193 /27
		2001:db8:acad:210:: 1 /64
		fe80::2

- **Ressources requises**

- 2 Routeurs (Cisco 4221 équipé de Cisco IOS version 16.9.4, image universelle ou similaire)
- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.2(2) image lanbasek9 ou similaires)
- 1 ordinateur (Windows équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

- **Instructions**

- **Partie 1: Création du réseau et configuration des paramètres de base des périphériques**

Dans la Partie 1, vous allez configurer la topologie du réseau et les paramètres de base sur les hôtes de PC et les commutateurs.

Etape 1: Câblez le réseau conformément à la topologie indiquée

Connectez les équipements représentés dans le schéma de topologie et effectuez le câblage nécessaire.

Etape 2: configuration des paramètres de base pour chaque routeur

PARTIE 5

PARTIE 5

Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

a. Attribuez un nom de l'appareil au routeur.

Ouvrez la fenêtre de configuration.

b. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

c. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

d. Attribuez **cisco** comme mot de passe de console et activez la connexion.

e. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

f. Cryptez les mots de passe en texte clair.

g. Créez une bannière qui avertit quiconque accède à l'appareil que tout accès non autorisé est interdit.

h. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Etape 3: Configurez les paramètres de base pour chaque commutateur

a. Attribuez un nom de périphérique au commutateur.

b. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.

c. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.

d. Attribuez cisco comme mot de passe de console et activez la connexion.

e. Attribuez **cisco** comme mot de passe VTY et activez la connexion.

f. Cryptez les mots de passe en texte brut.

g. Créez une bannière qui avertit quiconque accède à l'appareil que tout accès non autorisé est interdit.

h. Désactivez toutes les interfaces qui ne seront pas utilisées.

i. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Question:

- L'exécution de la commande **show cdp neighbors** à ce stade sur R1 ou R2 entraîne une liste vide. Expliquez votre réponse.

« Parce que les interfaces du routeur sont fermées par défaut. »

Partie 2: Configurer et vérifier l'adressage IPv4 et IPv6 sur R1 et R2

Dans la partie 2, vous allez configurer et vérifier les adresses IPv4 et IPv6 sur R1 et R2. Utilisez le tableau ci-dessus pour obtenir les informations nécessaires pour compléter cette partie.

Etape 1: Configurez les adresses IP pour les deux routeurs

a. Activez le routage de monodiffusion IPv6 sur les deux routeurs.

b. Configurez les adresses IP d'interfaces conformément à la table d'adressage.

Etape 2: Vérifiez l'adressage

Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

a. Exécutez la commande pour vérifier les attributions d'IPv4 aux interfaces.

b. Exécutez la commande pour vérifier les attributions d'IPv6 aux interfaces.

Etape 3: Enregistrez votre configuration

Enregistrez la configuration en cours dans le fichier de configuration initiale sur les deux routeurs.

Fermez la fenêtre de configuration.

- ***Partie 3:*** **Configurer et vérifier le routage statique et par défaut IPv4 sur R1 et R2**

Dans la partie 3, vous allez configurer le routage statique et par défaut sur R1 et R2 pour activer la connectivité complète entre les routeurs à l'aide d'IPv4. Encore une fois, le routage statique utilisé ici n'est pas destiné à représenter les meilleures pratiques, mais à évaluer votre capacité à compléter les configurations requises.

Etape 1: Sur R1, configurez une route statique vers le réseau Loopback1 de R2, en utilisant l'adresse G0/0/1 de R2 comme tronçon suivant

Ouvrez la fenêtre de configuration.

a. Utilisez la commande **ping** pour vous assurer que l'interface G0/0/1 de R2 est accessible.

b. Configurez une route statique pour le réseau Loopback1 de R2 via l'adresse G0/0/1 de R2.

Etape 2: Sur R1, configurez une route statique par défaut via l'adresse G0/0/0 de R2

a. Utilisez la commande **ping** pour vous assurer que l'interface G0/0/0 est accessible.

b. Configurez une route statique par défaut via l'adresse G0/0/0 de R2.

Etape 3: Sur R1, configurez une route statique flottante par défaut via l'adresse G0/0/1 de R2.

Configurez une route statique flottante par défaut avec un AD de 80 via l'adresse G0/0/1 de R2.

Etape 4: Sur R2, configurez une route statique par défaut via l'adresse G0/0/0 de R1

a. Utilisez la commande **ping** pour vous assurer que l'interface G0/0/0 de R1 est accessible.

b. Configurez une route statique par défaut via l'adresse G0/0/0 de R1.

Etape 5: Vérifiez que les routes sont opérationnels

a. Utilisez la commande **show ip route** pour vous assurer que la table de routage de R1 affiche les routes statiques et par défaut.

b. Sur R1, exécutez la commande **traceroute 10.2.0.1**. La sortie devrait montrer que le saut suivant est 192.168.1.2.

c. Sur R1, exécutez la commande **traceroute 209.165.200.193**. La sortie devrait montrer que le saut suivant est 172.16.1.2.

Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

d. Exécutez la commande **shutdown** sur R1 G0/0/0.

e. Démontrer que la route statique flottante fonctionne. D'abord, Exécutez la commande **show ip route static** . Vous devriez voir deux routes statiques. Route statique par défaut avec un AD de 80 et une route statique vers le réseau 10.2.0.0/24 avec un AD de 1.

f. Démontrez que la route statique flottante fonctionne en exécutant la commande **traceroute 209.165.200.193** . Le traceroute montrera le tronçon suivant comme 192.168.1.2.

g. Exécutez la commande **no shutdown** sur R1 G0/0/0.

Fermez la fenêtre de configuration.

- ***Partie 4: Configurer et vérifier le routage statique et par défaut IPv6 sur R1 et R2***

Dans la partie 4, vous allez configurer le routage statique et par défaut sur R1 et R2 pour activer la connectivité complète entre les routeurs en utilisant IPv6. Encore une fois, le routage statique utilisé ici n'est pas destiné à représenter les meilleures pratiques, mais à évaluer votre capacité à compléter les configurations requises.

Etape 1: Sur R2, configurez une route statique vers le réseau Loopback1 de R1, en utilisant l'adresse G0/0/1 de R1 comme tronçon suivant

a. Utilisez la commande **ping** pour vous assurer que l'interface G0/0/1 de R1 est accessible.

b. Configurez une route statique pour le réseau Loopback1 de R1 via l'adresse G0/0/1 de R1.

Etape 2: Sur R2, configurez une route statique par défaut via l'adresse G0/0/0 de R1

Utilisez la commande **ping** pour vous assurer que l'interface G0/0/0 de R1 est accessible.

Configurez une route statique par défaut via l'adresse G0/0/0 de R1.

Etape 3: Sur R2, configurez une route statique flottante par défaut via l'adresse G0/0/1 de R1

Configurez une route statique flottante par défaut avec un AD de 80 via l'adresse G0/0/1 de R2.

Etape 4: Sur R1, configurez une route statique par défaut via l'adresse G0/0/0 de R1

a. Utilisez la commande **ping** pour vous assurer que l'interface G0/0/0 est accessible.

b. Configurez une route statique par défaut via l'adresse G0/0/0 de R2.

Etape 5: Vérifiez que les routes sont opérationnels

a. Utilisez la commande **show ipv6 route** pour vous assurer que la table de routage de R2 affiche les routes statiques et par défaut.

b. Sur R2, exécutez la commande **traceroute 2001:db8:acad:10::1**. La sortie devrait montrer que le tronçon suivant est 2001:db8:acad:1::1.

c. Sur R2, exécutez la commande **traceroute 2001:db8:acad:209::1**. La sortie devrait montrer que le saut suivant est 2001:db8:acad:2 : :1.

Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

d. Exécutez la commande **shutdown** sur R2 G0/0/0.

e. Démontrez que la route statique flottante fonctionne. D'abord, Exécutez la commande **show ipv6 route static** . Vous devriez voir deux routes statiques. Route statique par défaut avec un AD de 80 et une route statique vers le réseau 2001:db8:acad:10::/64 avec un AD de 1.

f. Enfin, démontrez que la route statique flottante fonctionne en exécutant la commande **traceroute 2001:db8:acad:209::1** . Le traceroute montrera le tronçon suivant comme 2001:db8:acad:1::1.

PARTIE 5

Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

Réponses

Configuration

Routeur R1 :

```
R1# show run
Building configuration…
Current configuration : 1877 bytes
!
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$RYDJ$t/c7oO27si0aj8ubUL4Zm0
!
no aaa new-model
!
no ip domain lookup
!
login on-success log
!
subscriber templating
!
ipv6 unicast-routing
multilink bundle-name authenticated
!
spanning-tree extend system-id
!
redundancy
mode none
!
interface Loopback1
ip address 10.1.0.1 255.255.255.0
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:10::1/64
!
interface Loopback2
ip address 209.165.200.225 255.255.255.224
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:209::1/64
!
interface GigabitEthernet0/0/0
ip address 172.16.1.1 255.255.255.0
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:2::1/64
negotiation auto
!
interface GigabitEthernet0/0/1
ip address 192.168.1.1 255.255.255.0
negotiation auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:1::1/64
!
interface Serial0/1/0
no ip address
!
interface Serial0/1/1
no ip address
!
ip forward-protocol nd
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.1.2
ip route 0.0.0.0 0.0.0.0 192.168.1.2 80
ip route 10.2.0.0 255.255.255.0 192.168.1.2
!
ipv6 route ::/0 2001:DB8:ACAD:2::2
!
control-plane
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
password 7 02050D480809
login
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
password 7 0822455D0A16
login
!
end
```

PARTIE 5

Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

Réponses

Configuration

Routeur R2 :

```
R2# show run
Building configuration…
Current configuration : 1881 bytes
!
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$UiZY$inHX.hTsQ1oHjw81NXiLb/
!
no aaa new-model
!
no ip domain lookup
!
login on-success log
!
subscriber templating
!
ipv6 unicast-routing
multilink bundle-name authenticated
!
spanning-tree extend system-id
!
redundancy
mode none
!
interface Loopback1
ip address 10.2.0.1 255.255.255.0
ipv6 address FE80::2 link-local
ipv6 address 2001:DB8:ACAD:11::2/64
!
interface Loopback2
ip address 209.165.200.193 255.255.255.224
ipv6 address FE80::2 link-local
ipv6 address 2001:DB8:ACAD:210::1/64
!
interface GigabitEthernet0/0/0
ip address 172.16.1.2 255.255.255.0
shutdown
ipv6 address FE80::2 link-local
ipv6 address 2001:DB8:ACAD:2::2/64
!
interface GigabitEthernet0/0/1
ip address 192.168.1.2 255.255.255.0
negotiation auto
ipv6 address FE80::2 link-local
ipv6 address 2001:DB8:ACAD:1::2/64
!
interface Serial0/1/0
no ip address
!
interface Serial0/1/1
no ip address
!
ip forward-protocol nd
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
ipv6 route 2001:DB8:ACAD:10::/64
2001:DB8:ACAD:1::1
ipv6 route ::/0 2001:DB8:ACAD:1::1 80
ipv6 route ::/0 2001:DB8:ACAD:2::1
!
!
control-plane
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
password 7 045802150C2E
login
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
password 7 14141B180F0B
login
!
end
```

PARTIE 5

Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

Réponses

Configuration

Switch S1 :

```
S1# show run
Building configuration…
Current configuration : 1707 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.IEP$MS5z.mITakTYTwLWyXHxI0
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
!
ip http server
ip http secure-server
!
banner motd ^C Authorized
Users Only! ^C
!
line con 0
password 7 121A0C041104
login
line vty 0 4
password 7 121A0C041104
login
line vty 5 15
login
!
end
```

PARTIE 5

Activité 1 : Configuration des routes statiques et par défaut IPv4 et IPv6 - Lab

Réponses

Configuration

Switch S2 :

```
S2# show run
Building configuration…
Current configuration : 1707 bytes
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$IYmC$UST.4nznlABNG3REPrLc7/
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
!
ip http server
ip http secure-server
!
banner motd ^C Authorized
Users Only! ^C
!
line con 0
password 7 00071A150754
login
line vty 0 4
password 7 00071A150754
login
line vty 5 15
login
!
end
```

Activité 2 : Dépannage des routes statiques et par défaut IPv4 et IPv6 - Lab

- **Objectifs**

- **Partie 1: Évaluer le fonctionnement du réseau**
- **Partie 2: Recueillir de l'information, élaborer un plan d'action et mettre en œuvre des corrections**

- **Contexte/scénario**

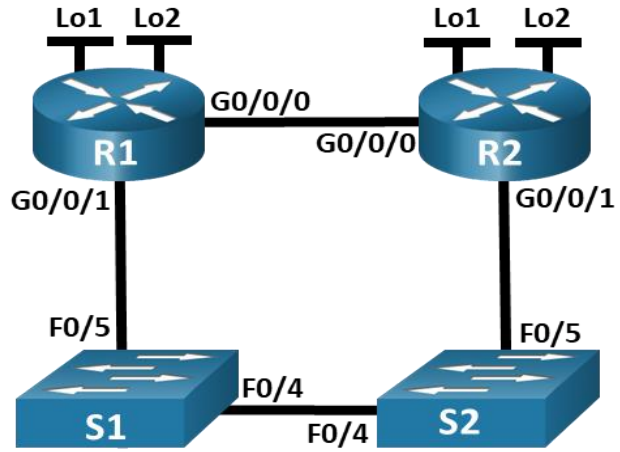
Votre instructeur a préconfiguré tout l'équipement réseau et a inclus des erreurs intentionnelles qui empêchaient les itinéraires configurés de fonctionner. Votre tâche consiste à évaluer le réseau, identifier et corriger les erreurs de configuration pour restaurer la connectivité complète. Vous pouvez trouver des erreurs avec les instructions d'itinéraire ou avec d'autres configurations qui ont une incidence sur la précision des instructions d'itinéraire.

Remarque: L'approche de routage statique utilisée dans ce TP est utilisée pour évaluer votre capacité à configurer différents types d'itinéraires statiques uniquement. Cette approche peut ne pas refléter les meilleures pratiques de réseautage.

Remarque: les routeurs utilisés dans les travaux pratiques CCNA sont Cisco 4221 équipé de version 16.9.4 de Cisco IOS XE (image universalk9). Les commutateurs utilisés dans les travaux pratiques sont des modèles Cisco Catalyst 2960s équipé de version 15.2.2 de Cisco IOS (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque: Assurez-vous que les routeurs et les commutateurs ont été effacés et n'ont aucune configuration de démarrage. En cas de doute, contactez votre instructeur.

- **Topologie**



- **Ressources requises**

- 2 Routeurs (Cisco 4221 équipé de Cisco IOS version 16.9.4, image universelle ou similaire)
- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.2(2) image lanbasek9 ou similaires)
- 1 ordinateur (Windows équipés d'un programme d'émulation de terminal tel que Tera Term)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

PARTIE 5

Activité 2 : Dépannage des routes statiques et par défaut IPv4 et IPv6- Lab

- **Table d'adressage**

Appareil	Interface	Adresse IP / Préfixe
R1	G0/0/0	172.16.1.1 /24
		2001:db8:acad:2::1 /64
		fe80::1
	G0/0/1	192.168.1.1 /24
		2001:db8:acad:1 /64
		fe80::1
	Loopback1	10.1.0.1 /24
		2001:db8:acad:10::1 /64
		fe80::1
	Loopback2	209.165.200.225 /27
		2001:db8:acad:209:: 1 /64
		fe80::1
R2	G0/0/0	172.16.1.2 /24
		2001:db8:acad:2::2 /64
		fe80::2
	G0/0/1	192.168.1.2 /24
		2001:db8:acad:1::2 /64
		fe80::2
	Loopback1	10.2.0.1 /24
		2001:db8:acad:11::2 /64
		fe80::2
	Loopback2	209.165.200.193 /27
		2001:db8:acad:210:: 1 /64
		fe80::2

- **Instructions**

  - **Partie 1: Évaluer le fonctionnement du réseau**

Utilisez Ping et/ou Traceroute à partir de la console du routeur pour tester les critères suivants et enregistrer les résultats.

a. Le trafic de R1 à l'adresse 172.16.2.1 de R2 utilise le saut suivant 192.168.0.14.

b. Le trafic de R1 à l'adresse 209.165.200.129 de R2 utilise le saut suivant 192.168.0.30.

c. Lorsque l'interface G0/0/0 de R1 est arrêtée, le trafic de R1 à 172.16.2.1 de R2 utilise le saut suivant 192.168.0.30.

d. Trafic de R2 à l'adresse de R1 2001:db8:acad:171::1 utilisez le saut suivant 2001:db8:acad::1.

e. Trafic de R2 à l'adresse de R1 2001:db8:acad:209::1 utilisez le saut suivant 2001:db8:acad:16::1.

f. Lorsque l'interface G0/0/0 de R2 est arrêtée, le trafic de R2 vers R1 2001:db8:acad:171::1 utilise le saut suivant 2001:db8:acad:16::1.

  - **Partie 2: Recueillir des informations, créer un plan d'action et mettre en œuvre des corrections**

a. Pour chaque critère qui n'est pas satisfait, recueillir des informations en examinant les tables de configuration et de routage en cours d'exécution et élaborer une hypothèse sur ce qui est à l'origine du dysfonctionnement.

Activité 2 : Dépannage des routes statiques et par défaut IPv4 et IPv6 - Lab

b. Créez un plan d'action qui, selon vous, permettra de résoudre le problème. Développez une liste de toutes les commandes que vous avez l'intention d'émettre pour résoudre le problème, ainsi qu'une liste de toutes les commandes dont vous avez besoin pour rétablir la configuration, si votre plan d'action ne parvient pas à corriger le problème.

c. Exécutez vos plans d'action un à la fois pour chaque critère qui échoue et enregistrez les actions de correction.

Activité 2 : Dépannage des routes statiques et par défaut IPv4 et IPv6 - Lab

Réponses

Configuration

Routeur R1 :

```
enable
config terminal
hostname R1
ipv6 unicast-routing
interface g0/0/1
ip address 192.168.0.17 255.255.255.240
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad:16::1/64
no shutdown
interface g0/0/0
ip address 192.168.0.1 255.255.255.240
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad::1/64
no shutdown
interface loopback 1
ip address 172.16.1.1 255.255.255.0
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad:171::1/64
interface loopback 2
ip address 209.165.200.1 255.255.255.128
ipv6 address fe80::1 link-local
ipv6 address 2001:db8:acad:209::1/64
ip route 209.165.200.128 255.255.255.128 192.168.0.30
ip route 0.0.0.0 0.0.0.0 192.168.0.14
ip route 0.0.0.0 0.0.0.0 192.168.0.30 80
ipv6 route ::/0 2001:db8:acad:16::2
```

Routeur R2 :

```
enable
config terminalenable
config terminal
hostname R2
no ip domain lookup
ipv6 unicast-routing
interface g0/0/0
ip address 192.168.0.14 255.255.255.240
ipv6 address fe80::2 link-local
ipv6 address 2001:db8:acad::14/64
no shutdown
interface g0/0/1
ip address 192.168.0.30 255.255.255.240
ipv6 address fe80::2 link-local
ipv6 address 2001:db8:acad:16::2/64
no shutdown
interface loopback 1
ip address 172.16.2.1 255.255.255.0
ipv6 address fe80::2 link-local
ipv6 address 2001:db8:acad:172::1/64
interface loopback 2
ip address 209.165.200.129 255.255.255.128
ipv6 address fe80::2 link-local
ipv6 address 2001:db8:acad:210::1/64
ipv6 route 2001:db8:acad:209::/64 2001:db8:acad:16::1
ipv6 route ::/0 2001:db8:acad::1
ipv6 route ::/0 2001:db8:acad:16::1 80
ip route 0.0.0.0 0.0.0.0192.168.0.17
end
```

Switch S1 :

```
enable
config terminal
hostname S1
interface range f0/1-3,
f0/6-24, g0/1-2
shutdown
end
```

Switch S2

```
enable
config terminal
hostname S2
interface range f0/1-3,
f0/6-24, g0/1-2
shutdown
end
```

TP 2

Implémenter le protocole OSPF

Compétences visées :

- Configurer le protocole OSPF

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

10 heures

TP 2

Implémenter le protocole OSPF

1. Configuration OSPFv2 à zone unique
2. Configuration OSPFv3 à zone unique
3. Configuration OSPF à zone multiple

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer l' OSPFv2 à zone unique?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 5

Activité 1 : Configuration OSPFv2 point à point à zone unique - Packet Tracer

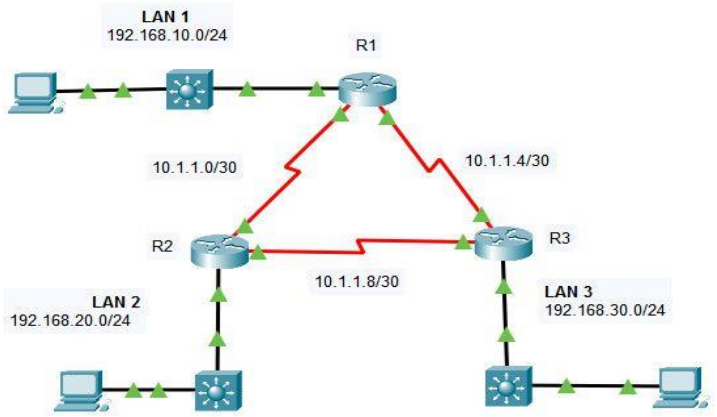
- **Objectifs**

- **Partie 1 : Configurer les ID du routeur.**
- **Partie 2 : Configurer les réseaux pour le routage OSPF.**
- **Partie 3 : Configuration des interfaces passives.**
- **Partie 4 : Vérifier la configuration OSPF.**

- **Contexte**

Dans cette activité, vous allez activer le routage OSPF à l'aide d'instructions réseau et de masques génériques, configurer le routage OSPF sur les interfaces et utiliser les masques quad-zéro des instructions réseau. En outre, vous allez configurer des ID de routeur explicites et des interfaces passives.

- **Topologie**



- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau
R1	G0/0/0	192.168.10.1	/24
	S0/1/0	10.1.1.1	/30
	S0/1/1	10.1.1.5	/30
R2	G0/0/0	192.168.20.1	/24
	S0/1/0	10.1.1.2	/30
	S0/1/1	10.1.1.9	/30
R3	G0/0/0	192.168.30.1	/24
	S0/1/0	10.1.1.10	/30
	S0/1/1	10.1.1.6	/30
PC1	Carte réseau	192.168.10.10	/24
PC2	Carte réseau	192.168.20.10	/24
PC3	Carte réseau	192.168.30.10	/24

- **Instructions**

- **Partie 1: Configurer un ID de routeur**

a. Démarrez le processus de routage OSPF sur les trois routeurs. Utilisez le processus ID **10**.

Ouvrez la fenêtre de configuration.

- Router(config)# **router ospf** *process-id*

b. Utilisez la commande router-id pour définir les ID OSPF des trois routeurs comme suit

Activité 1 : Configuration OSPFv2 point à point à zone unique - Packet Tracer

- R1: **1.1.1.1**
- R2: **2.2.2.2**
- R3: **3.3.3.3**

Utilisez la commande suivante :

- Router(config-router)# **router-id** *rid*

Partie 2: Configurer les réseaux pour le routage OSPF

Etape 1: Configurer les réseaux pour le routage OSPF en utilisant des commandes réseau et des masques de joker

Question :

- Combien d'instructions sont nécessaires pour configurer OSPF pour router tous les réseaux connectés au routeur R1 ?
- Le réseau local connecté au routeur R1 a un masque /24. Quel est l'équivalent de ce masque dans la représentation décimale pointillée ?
- Soustrayez le masque de sous-réseau décimal en pointillé de 255.255.255.255. Quel est le résultat ?
- Quel est l'équivalent décimal en pointillés du masque de sous-réseau /30 ?
- Soustrayez la représentation décimale pointillée du masque /30 de 255.255.255.255. Quel est le résultat ?

a. Configurez le processus de routage sur R1 avec les instructions réseau et les masques génériques nécessaires pour activer le routage OSPF pour tous les réseaux connectés. Les valeurs d'instruction réseau doivent être les adresses réseau ou sous-réseau des réseaux configurés.

Ouvrez la fenêtre de configuration.

- Router(config-router)# **network** network-address wildcard-mask **area** area-id

b. Vérifiez que OSPF a été configuré correctement en affichant la configuration en cours d'exécution. Si vous trouvez une erreur, supprimez l'instruction réseau à l'aide de la commande **no** et reconfigurez-la.

Etape 2: Configurez les réseaux pour le routage OSPF à l'aide d'adresses IP d'interface et de masques quad-zéro

Sur le routeur R2, configurez OSPF à l'aide de commandes réseau avec les adresses IP des interfaces et les masques quad-zéro. La syntaxe de la commande network est la même que celle utilisée ci-dessus.

Etape 3: Configurer le routage OSPF sur les interfaces de routeur

Sur le routeur R3, configurez les interfaces requises avec OSPF.

Question :

- Quelles interfaces sur R3 doivent être configurées avec OSPF ?

Configurez chaque interface à l'aide de la syntaxe de commande ci-dessous :

- Router(config-if)# **ip ospf** *process-id* **area** *area-id*

Fermez la fenêtre de configuration.

PARTIE 5

Activité 1 : Configuration OSPFv2 point à point à zone unique - Packet Tracer

Partie 3: Configurer des interfaces passives

OSPF enverra son trafic de protocole à partir de toutes les interfaces qui participent au processus OSPF. Sur les liens qui ne sont pas configurés vers d'autres réseaux, tels que les réseaux locaux, ce trafic inutile consomme des ressources. La commande passive-interface empêchera le processus OSPF d'envoyer un trafic de protocole de routage inutile sur les interfaces LAN.

Question :

- Quelles interfaces sur R1, R2 et R3 sont des interfaces LAN ?

Configurez le processus OSPF sur chacun des trois routeurs à l'aide de la commande **passive interface**.

Ouvrez la fenêtre de configuration.

- Router(config-router)# **passive-interface** *interface*

Partie 4: Vérifier la configuration OSPF

- Utilisez les commandes **show** pour vérifier la configuration réseau et de l'interface passive du processus OSPF sur chaque routeur.

```
R1#show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/1/0
L       10.1.1.1/32 is directly connected, Serial0/1/0
C       10.1.1.4/30 is directly connected, Serial0/1/1
L       10.1.1.5/32 is directly connected, Serial0/1/1
O       10.1.1.8/30 [110/128] via 10.1.1.2, 00:14:19, Serial0/1/0
                    [110/128] via 10.1.1.6, 00:14:19, Serial0/1/1
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
O    192.168.20.0/24 [110/65] via 10.1.1.2, 00:31:45, Serial0/1/0
O    192.168.30.0/24 [110/65] via 10.1.1.6, 00:14:19, Serial0/1/1
```

```
R2#show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/1/0
L       10.1.1.2/32 is directly connected, Serial0/1/0
O       10.1.1.4/30 [110/128] via 10.1.1.1, 00:20:11, Serial0/1/0
                    [110/128] via 10.1.1.10, 00:20:11, Serial0/1/1
C       10.1.1.8/30 is directly connected, Serial0/1/1
L       10.1.1.9/32 is directly connected, Serial0/1/1
O    192.168.10.0/24 [110/65] via 10.1.1.1, 00:37:37, Serial0/1/0
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0/0
O    192.168.30.0/24 [110/65] via 10.1.1.10, 00:20:11, Serial0/1/1
```

```
R3#show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O       10.1.1.0/30 [110/128] via 10.1.1.9, 00:21:54, Serial0/1/0
                    [110/128] via 10.1.1.5, 00:21:54, Serial0/1/1
C       10.1.1.4/30 is directly connected, Serial0/1/1
L       10.1.1.6/32 is directly connected, Serial0/1/1
C       10.1.1.8/30 is directly connected, Serial0/1/0
L       10.1.1.10/32 is directly connected, Serial0/1/0
O    192.168.10.0/24 [110/65] via 10.1.1.5, 00:21:54, Serial0/1/1
O    192.168.20.0/24 [110/65] via 10.1.1.9, 00:21:54, Serial0/1/0
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.30.1/32 is directly connected, GigabitEthernet0/0/0

R3#
```

```
R1#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.0 0.0.0.255 area 0
    10.1.1.0 0.0.0.3 area 0
    10.1.1.4 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:08:38
    2.2.2.2              110      00:08:45
    3.3.3.3              110      00:08:38
  Distance: (default is 110)
```

PARTIE 5

PARTIE 5

Activité 1 : Configuration OSPFv2 point à point à zone unique - Packet Tracer

Réponses

- **Partie 2 / Etape 1 :**

- 3
- 255.255.255.0
- 0.0.0.255
- 255.255.255.252
- 0.0.0.3

- **Partie 2 / Etape 3:**

- G0/0/0, S0/1/0, S0/1/1

- **Partie 3 :**

- G0/0/0 sur les trois routeurs.

- **Configuration :**

R1 :

```
enable
configure terminal
router ospf 10
  router-id 1.1.1.1
  network 192.168.10.0 0.0.0.255 area 0
  network 10.1.1.0 0.0.0.3 area 0
  network 10.1.1.4 0.0.0.3 area 0
  passive-interface g0/0/0
end
```

R2:

```
enable
configure terminal
router ospf 10
  router-id 2.2.2.2
  network 192.168.20.1 0.0.0.0 area 0
  network 10.1.1.2 0.0.0.0 area 0
  network 10.1.1.9 0.0.0.0 area 0
  passive-interface g0/0/0
end
```

R3:

```
enable
configure terminal
router ospf 10
  router-id 3.3.3.3
interface GigabitEthernet0/0/0
  ip ospf 10 area 0
interface Serial0/1/0
  ip ospf 10 area 0
interface Serial0/1/1
  ip ospf 10 area 0
router ospf 10
  passive-interface g0/0/0
end
```

PARTIE 5

Activité 2 : Modifier la zone unique OSPFv2- Packet Tracer

- **Objectifs**

- **Partie 1 : Modification des paramètres OSPF par défaut**
- **Partie 2 : Vérification de la connectivité**

- **Scénario**

Dans cet exercice, le protocole OSPF est déjà configuré et tous les périphériques finaux disposent d'une connectivité complète. Vous allez modifier les configurations du routage OSPF par défaut en modifiant les minuteurs hello et dead, et en ajustant la bande passante d'une liaison. Vous vérifierez ensuite que la connectivité complète a été restaurée pour l'ensemble des périphériques finaux.

- **Topologie**

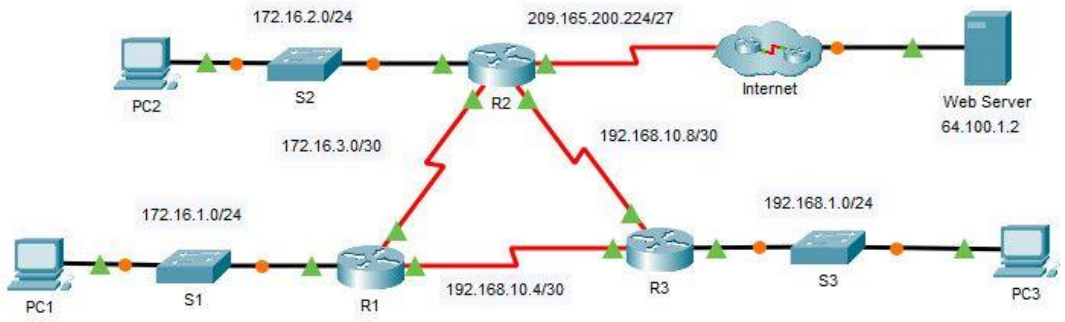


Table d'adressage

Appareil	Interface	Adresse IPv4	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
	S0/1/0	209.165.200.225	255.255.255.224	N/A
R3	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	Carte réseau	172.16.1.2	255.255.255.0	172.16.1.1
PC2	Carte réseau	172.16.2.2	255.255.255.0	172.16.2.1
PC3	Carte réseau	192.168.1.2	255.255.255.0	192.168.1.1
Serveur web	Carte réseau	64.100.1.2	255.255.255.0	64.100.1.1

- **Instructions**

  - **Partie 1: Modification des paramètres OSPF par défaut**

Etape 1: Testez la connectivité entre tous les périphériques finaux

Avant de modifier les paramètres OSPF, vérifiez que tous les PC peuvent envoyer une requête ping au serveur web ainsi qu'aux autres PC.

Activité 2 : Modifier la zone unique OSPFv2- Packet Tracer

Etape 2: Ajustez les minuteurs Hello et Dead entre R1 et R2

a. Exécutez les commandes suivantes sur **R1**.

Ouvrez la fenêtre de configuration.

- R1(config)# **interface s0/0/0**
- R1(config-if)# **ip ospf hello-interval 15**
- R1(config-if)# **ip ospf dead-interval 60**

b. Après une courte période de temps, la connexion OSPF avec **R2** échouera, comme le montre la sortie du routeur.

```
00:02:40: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired


00:02:40: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
```

Les deux côtés de la connexion doivent posséder les mêmes minuteurs pour que la contiguïté soit maintenue. Identifiez l'interface sur R2 qui est connectée à R1. Réglez les minuteries de l'interface R2 pour qu'elles correspondent aux paramètres de **R1**.

Après une brève période de temps, vous devriez voir un message d'état indiquant que la contiguïté OSPF a été rétablie.

```
00:21:52: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on
Serial0/0/0 from LOADING to FULL, Loading Done
```

Etape 3: Ajustez le paramètre de bande passante sur R1

Suivez le chemin entre **PC1** et le serveur web situé à l'adresse 64.100.1.2. Notez que le chemin entre **PC1** et l'adresse 64.100.1.2 passe par **R2**. Le protocole OSPF utilise de préférence le chemin de moindre coût.

- C:\> **tracert 64.100.1.2**

```
Tracing route to 64.100.1.2 over a maximum of 30 hops:

1 1 ms 0 ms 8 ms 172.16.1.1

2 0 ms 1 ms 0 ms 172.16.3.2

3 1 ms 9 ms 2 ms 209.165.200.226

4 * 1 ms 0 ms 64.100.1.2

Trace complete.
```

a. Sur l'interface série 0/0/0 de **R1**, définissez la bande passante sur 64 Kbit/s. Ceci ne modifie pas le débit de port réel, mais uniquement la métrique que le processus OSPF utilisera sur **R1** pour calculer les meilleures routes.

- R1(config-if)# **bandwidth 64**

b. Suivez le chemin entre **PC1** et le serveur web situé à l'adresse 64.100.1.2. Notez que le chemin entre **PC1** et l'adresse 64.100.1.2 est redirigé via **R3**. Le protocole OSPF utilise de préférence le chemin de moindre coût.

- C:\> **tracert 64.100.1.2**

PARTIE 5

Activité 2 : Modifier la zone unique OSPFv2- Packet Tracer

```
Tracing route to 64.100.1.2 over a maximum of 30 hops:

1  1 ms  0 ms  3 ms  172.16.1.1
2  8 ms  1 ms  1 ms  192.168.10.6
3  2 ms  0 ms  2 ms  172.16.3.2
4  2 ms  3 ms  1 ms  209.165.200.226
5  2 ms  11 ms  64.100.1.2

Trace complete.
```

- **Partie 2: Vérification de la connectivité**

Vérifiez que tous les PC peuvent envoyer des pings au serveur web et entre eux.

Réponses

Configuration

R1 :

```
interface s0/0/0
 ip ospf hello-interval 15
 ip ospf dead-interval 60
 bandwidth 64
```

R2:

```
interface s0/0/0
 ip ospf hello-interval 15
 ip ospf dead-interval 60
```

PARTIE 5

PARTIE 5

Activité 3 : Vérifier la zone unique OSPFv2- Packet Tracer

Objectifs

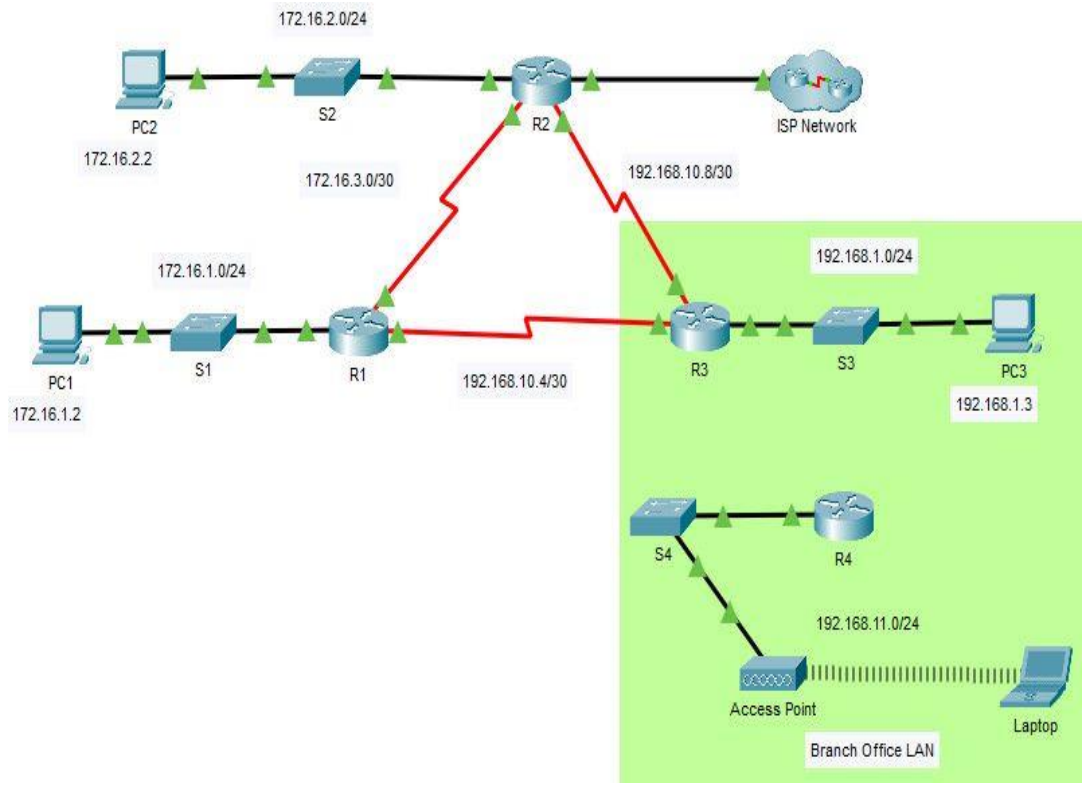
Dans ce Travaux Pratiques, vous allez utiliser les commandes CLI pour vérifier le fonctionnement d'un réseau OSPFv2 existant. Dans la partie 2, vous allez ajouter un nouveau réseau local à la configuration et vérifier la connectivité.

- **Identifier et vérifier l'état des voisins OSPF.**
- **Déterminez comment les routes sont appris dans le réseau.**
- **Expliquez comment l'état voisin est déterminé.**
- **Examinez les paramètres de l'ID de processus OSPF.**
- **Ajoutez un nouveau réseau local dans un réseau OSPF existant et vérifiez la connectivité.**

Contexte/scénario

Vous êtes l'administrateur réseau d'une filiale d'une organisation plus grande. Votre filiale ajoute un nouveau réseau sans fil dans un réseau local existant de filiale. Le réseau existant est configuré pour échanger des routes à l'aide d'OSPFv2 dans une configuration à zone unique. Votre tâche consiste à vérifier le fonctionnement du réseau OSPFv2 existant, avant d'ajouter dans le nouveau réseau local. Lorsque vous êtes sûr que le réseau local OSPFv2 actuel fonctionne correctement, vous allez connecter le nouveau réseau local et vérifier que les routes OSPF sont propagées pour le nouveau réseau local. En tant qu'administrateur réseau de filiale, vous avez un accès complet à l'IOS sur les routeurs R3 et R4. Vous n'avez qu'un accès en lecture aux routeurs LAN d'entreprise R1 et R2, en utilisant le nom d'utilisateur **BranchAdmin** et le mot de passe **Branch1234**.

Topologie



Activité 3 : Vérifier la zone unique OSPFv2- Packet Tracer

- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	G0/1	64.100.54.6	255.255.255.252	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
R3	G0/0	192.168.1.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
R4	G0/0/0	192.168.1.2	255.255.255.0	N/A
	G0/0/1	192.168.11.1	255.255.255.0	N/A
Routeur FAI	Carte réseau	64.100.54.5	255.255.255.252	N/A
PC1	Carte réseau	172.16.1.2	255.255.255.0	172.16.1.1
	Carte réseau	172.16.2.2	255.255.255.0	172.16.2.1
PC3	Carte réseau	192.168.1.2	255.255.255.0	192.168.1.1
Ordinateur portable	Carte réseau	le protocole DHCP	le protocole DHCP	le protocole DHCP

- **Instructions**

  - **Partie 1: Vérifiez l'opération réseau OSPFv2 existante**

Les commandes suivantes vous aideront à trouver les informations nécessaires pour répondre aux questions:

- **show ip interface brief**
- **show ip route**
- **show ip route ospf**
- **show ip ospf neighbor**
- **show ip protocols**
- **show ip ospf**
- **show ip ospf interface**

Etape 1: Vérifiez l'opération OSPFv2

Attendez que STP ait convergé sur le réseau. Vous pouvez cliquer sur le bouton Packet Tracer Fast Forward pour accélérer le processus. Continuez uniquement lorsque tous les voyants de liaison sont verts.

a. Connectez-vous au routeur **R1** en utilisant le nom d'utilisateur **BranchAdmin** et le mot de passe **Branch1234** . Exécutez la commande **show ip route** .

Ouvrez la fenêtre de configuration.

- R1# **show ip route**

PARTIE 5

Activité 3 : Vérifier la zone unique OSPFv2- Packet Tracer

```
--- output omitted ----

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C 172.16.1.0/24 is directly connected, GigabitEthernet0/0
L 172.16.1.1/32 is directly connected, GigabitEthernet0/0
O 172.16.2.0/24 [110/65] via 172.16.3.2, 00:02:18, Serial0/0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0
L 172.16.3.1/32 is directly connected, Serial0/0/0
O 192.168.1.0/24 [110/65] via 192.168.10.6, 00:02:18, Serial0/0/1
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.10.4/30 is directly connected, Serial0/0/1
L 192.168.10.5/32 is directly connected, Serial0/0/1
O 192.168.10.8/30 [110/128] via 172.16.3.2, 00:02:18, Serial0/0/0
                  [110/128] via 192.168.10.6, 00:02:18, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.16.3.2, 00:02:18, Serial0/0/0
```

Questions:

- Comment le routeur **R1** a-t-il reçu la route par défaut?
- De quel routeur **R1** a-t-il reçu la route par défaut?
- Comment pouvez-vous filtrer la sortie de **show ip route** pour afficher uniquement les routes apprises par OSPF?

b. Exécutez la commande **show ip ospf neighbor** sur **R1**.

- **Questions:**
  - Quels routeurs ont formé des adjacences avec le routeur **R1**?
  - Quels sont les ID du routeur et l'état des routeurs affichés dans la sortie de commande?
  - Tous les routeurs adjacents sont-ils affichés dans la sortie?

c. À l'aide de l'invite de commande sur **PC1**, ping l'adresse du **routeur ISP** indiqué dans le tableau d'adresses. Est-elle aboutit? Sinon, effectuez une commande **clear ospf process** sur les routeurs et répétez la commande ping.

Etape 2: Vérifiez l'opération OSPFv2 sur R2

a. Connectez-vous au routeur **R2** en utilisant le nom d'utilisateur **BranchAdmin** et le mot de passe **Branch1234** . Exécutez la commande **show ip route** . Vérifiez que les routes vers tous les réseaux de la topologie sont affichées dans la table de routage.

Question:

- Comment le routeur R2 a-t-il appris la route par défaut vers le FAI?

b. Entrez la commande **interface show ip ospf g0/0** sur le routeur **R2**.

Questions:

- Quel type de réseau OSPF est connecté à cette interface?
- Est-ce que les paquets OSPF hello sont envoyés sur cette interface? Expliquez votre réponse.

c. À l'aide de l'invite de commande sur **PC2**, ping l'adresse S0/0/1 sur le routeur **R3**.

Activité 3 : Vérifier la zone unique OSPFv2- Packet Tracer

Question:

- Est-elle aboutit?

Etape 3: Vérifiez l'opération OSPFv2 sur R3

a. Exécutez la commande **show ip protocols** sur le routeur R3.

Question:

- Le routeur R3 achemine pour quels réseaux?

b. Exécutez la commande **show ip ospf neighbor detail** sur le routeur **R3** .

Question:

- Quelle est la priorité voisine affichée pour les routeurs voisins OSPF? Cette valeur est la valeur par défaut.

c. À l'aide de l'invite de commande sur **PC3**, ping l'adresse du **routeur FAI** indiqué dans le tableau d'adresses.

Question:

- Est-elle aboutit?

Partie 2: Ajoutez le nouveau réseau local des filiales au réseau OSPFv2

Vous allez maintenant ajouter le LAN de Branch Office préconfiguré au réseau OSPFv2.

Etape 1: Vérifiez la configuration OSPFv2 sur le routeur R4

Exécutez une commande **show run | begin router ospf** sur le routeur **R4** . Vérifiez que les instructions réseau sont présentes pour les réseaux configurés sur le routeur.

Question:

- Quelle interface est configurée pour ne pas envoyer de paquets de mise à jour OSPF ?

Etape 2: Connectez le routeur de filiale R4 au réseau OSPFv2

a. À l'aide du câble Ethernet approprié, connectez l'interface G0/0/0 sur le routeur **R4** à l'interface G0/1 sur le commutateur **S3** . Utilisez la commande **show ip ospf neighbor** pour vérifier que le routeur **R4** est maintenant adjacent au **R3.**

Question:

- Quel état est affiché pour le routeur **R3**?

b. À l'aide de la commande **show ip ospf neighbor** sur **R3** , déterminez l'état du routeur **R4** . Il se peut qu'il y ait un délai pendant que l'OSPF converge.

Question:

- Pourquoi l'état du routeur R4 est-il différent de l'état de R1 et R2?

c. En utilisant l'invite de commande sur l'ordinateur portable, ping l'adresse du PC2.

Question:

- Est-elle aboutit?

PARTIE 5

Activité 3 : Vérifier la zone unique OSPFv2- Packet Tracer

Réponses

- **Partie 1 / Etape 1 :**

a) - La route par défaut a été apprise via OSPF.

- Router 2

- Utilisez soit **show ip route ospf** soit **show ip route | inclure O**

b) - R2 et R3

- 2.2.2.2 – Full/- and 3.3.3.3 – Full/-

- Oui

- **Partie 1 / Etape 2 :**

a) - Il a été configuré statiquement par l'administrateur.

b) - BROADCAST

- Non. L'interface est configurée en tant qu'interface passive dans OSPF.

c) - Oui.

- **Partie 1 / Etape 3 :**

a) - 192.168.1.0/24, 192.168.10.4/30, and 192.168.10.8/30.

b) - 0.

c) - Oui.

- **Partie 2 / Etape 1 :**

- Interface GigabitEtherenet0/0/1

Partie 2 / Etape 2 :

a) - FULL/DR

b) - Étant donné que le type de réseau OSPF entre R1 et R2 est point à point, il n'y a pas d'élection OSPF. R4 est sur le même segment de réseau Ethernet que le routeur R3, donc le type de réseau OSPF est Diffusion et il y a une élection OSPF. Lorsque plusieurs routeurs se trouvent sur un segment de réseau à accès multiple, un seul routeur, le DR, envoie les mises à jour OSPFv2. Un deuxième routeur, dans ce cas R4, devient le routeur désigné de secours et peut prendre le relais en cas de défaillance du routeur DR.

c) - Oui.

PARTIE 5

Activité 4 : Propager une route par défaut dans OSPFv2 - Packet Tracer

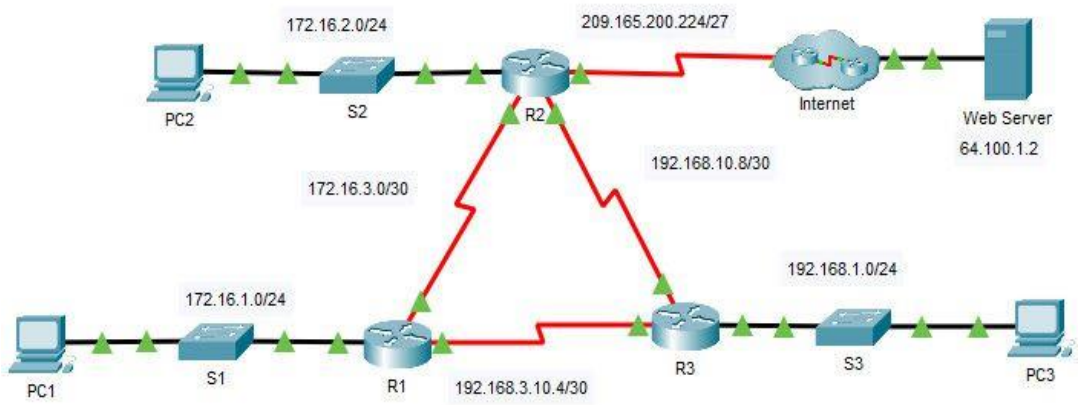
- **Objectifs**

- **Partie 1: Propager une route par défaut**
- **Partie 2: Vérifier la connectivité**

- **Contexte/scénario**

Au cours de cet exercice, vous allez configurer une route par défaut IPv4 sur Internet et propager cette route par défaut aux autres routeurs OSPF. Vous vérifierez ensuite que la route par défaut est présente dans les tables de routage en aval et que les hôtes peuvent désormais accéder à un serveur web sur Internet.

- **Topologie**



- **Table d'adressage**

Appareil	Interface	Adresse IPv4	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
R2	G0/0	172.16.2.1	255.255.255.0	N/A
	S0/0/0	172.16.3.2	255.255.255.252	N/A
	S0/0/1	192.168.10.9	255.255.255.252	N/A
	S0/1/0	209.165.200.225	255.255.255.224	N/A
R3	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.10.6	255.255.255.252	N/A
	S0/0/1	192.168.10.10	255.255.255.252	N/A
PC1	Carte réseau	172.16.1.2	255.255.255.0	172.16.1.1
PC2	Carte réseau	172.16.2.2	255.255.255.0	172.16.2.1
PC3	Carte réseau	192.168.1.2	255.255.255.0	192.168.1.1
Serveur web	Carte réseau	64.100.1.2	255.255.255.0	64.100.1.1

- **Instructions**

- **Partie 1: Propager une route par défaut**

Etape 1: Testez la connectivité au serveur web

PARTIE 5

Activité 4 : Propager une route par défaut dans OSPFv2 - Packet Tracer

a. À partir de PC1, PC2 et PC3, essayez d'effectuer un ping sur l'adresse IP du serveur Web, 64.100.1.2.

Questions:

- Certains des pings ont-ils réussi ?
- Quel message avez-vous reçu et quel appareil a émis le message?

b. Examinez les tables de routage sur les routeurs R1, R2 et R3.

Ouvrez la fenêtre de configuration.

Question:

- Quelle instruction est présenté dans les tables de routage qui indique que les pings vers le serveur Web échoueront?

Etape 2: Configurez une route par défaut sur R2

- Configurez **R2** avec une route par défaut connectée directement à l'internet.
  - R2(config)# **ip route 0.0.0.0 0.0.0.0 Serial0/1/0**

Remarque: Le routeur avertit que si cette interface n'est pas une connexion point à point, elle peut avoir un impact sur les performances. Vous pouvez ignorer cet avertissement car il s'agit d'une connexion point à point.

Etape 3: Propagez la route dans OSPF

Configurez OSPF de manière à propager la route par défaut dans les mises à jour du routage OSPF.

- R2(config)# **router ospf 1**
- R2(config-router)# **default-information originate**

Etape 4: Examinez les tables de routage sur R1 et R3

Examinez les tables de routage de **R1** et de **R3** afin de vérifier que la route a été propagée.

- R1> **show ip route**

```
<output omitted>

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

<output omitted>

O*E2 0.0.0.0/0 [110/1] via 172.16.3.2, 00:00:08, Serial0/0/0

!--------------------
```

```
R3> show ip route

<output omitted>

Gateway of last resort is 192.168.10.9 to network 0.0.0.0

<output omitted>

O*E2 0.0.0.0/0 [110/1] via 192.168.10.9, 00:08:15, Serial0/0/1
```

Partie 2: Vérification de la connectivité

Vérifiez que **PC1**, **PC2**, et **PC3** peuvent envoyer des requêtes ping au serveur web.

Activité 4 : Propager une route par défaut dans OSPFv2 - Packet Tracer

Réponses

- **Partie 1 / Etape 1 :**

a) - Non

- Destination inaccessible depuis R2.

b) - La passerelle de dernier recours n'est pas définie

Configuration

R2 :

```
enable
config terminal
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
router ospf 1
default-information originate
```

TP 2

Implémenter le protocole OSPF

1. Configuration OSPFv2 à zone unique
2. Configuration OSPFv3 à zone unique
3. Configuration OSPF à zone multiple

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer l' OSPFv3 à zone unique?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 5

Activité 1 : Modifier la zone unique OSPFv2- Packet Tracer

- **Objectifs**

- **Partie 1 : configuration du routage OSPFv3**
- **Partie 2 : vérification de la connectivité**

- **Scénario**

Dans cet exercice, l'adressage IPv6 est déjà configuré. Vous êtes chargé de configurer la topologie à trois routeurs avec l'OSPFv3 à zone unique de base, puis de vérifier la connectivité entre les périphériques finaux.

- **Topologie**

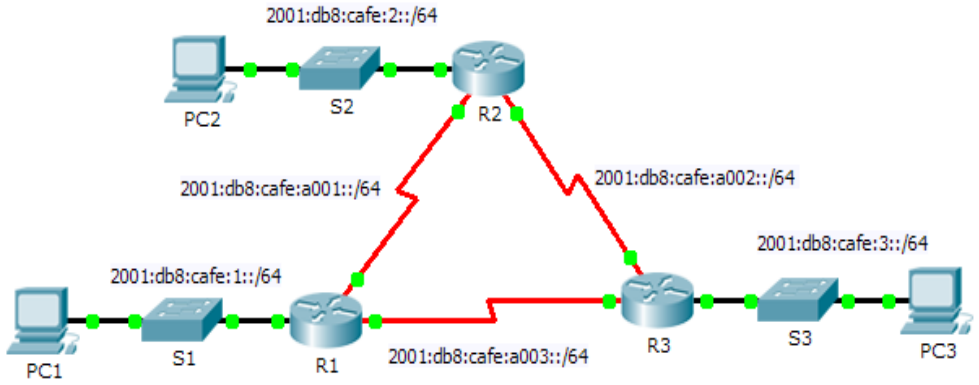


Table d'adressage

Périphérique	Interface	Préfixe/adresse IPv6	Passerelle par défaut
R1	G0/0	2001:db8:cafe:1::1/64	N/A
	S0/0/0	2001:db8:cafe:a001::1/64	N/A
	S0/0/1	2001:db8:cafe:a003::1/64	N/A
R2	G0/0	2001:db8:cafe:2::1/64	N/A
	S0/0/0	2001:db8:cafe:a001::2/64	N/A
	S0/0/1	2001:db8:cafe:a002::1/64	N/A
R3	G0/0	2001:db8:cafe:3::1/64	N/A
	S0/0/0	2001:db8:cafe:a003::264	N/A
	S0/0/1	2001:db8:cafe:a002::2/64	N/A
PC1	Carte réseau	2001:db8:cafe:1::10/64	fe80::1
PC2	Carte réseau	2001:db8:cafe:2::10/64	fe80::2
PC3	Carte réseau	2001:db8:cafe:3::10/64	fe80::3

- **Instructions**

- **Partie 1: configuration du routage OSPFv3**

Etape 1: Configurez OSPFv3 sur R1, R2 et R3.

Activité 1 : Modifier la zone unique OSPFv2- Packet Tracer

- Respectez les conditions requises suivantes pour configurer le routage OSPF sur les trois routeurs :
  - Activation du routage IPv6
  - ID de processus 10
  - ID de chaque routeur : R1 = 1.1.1.1 ; R2 = 2.2.2.2 ; R3 = 3.3.3.3
  - Activation d'OSPFv3 sur chaque interface

Remarque : Packet Tracer 6.0.1 ne prend pas en charge la commande **auto-cost reference-bandwidth**. Par conséquent, vous ne pourrez pas ajuter les coûts de bande passante dans cet exercice.

Etape 2: Vérifiez que le routage OSPF est opérationnel.

Vérifiez que chaque routeur a établi une contiguïté avec les deux autres routeurs. Vérifiez que la table de routage dispose d'une route vers chaque réseau de la topologie.

- **Partie 2 : vérification de la connectivité**

- Chaque PC doit être en mesure d'envoyer une requête ping aux deux autres PC. Si ce n'est pas le cas, vérifiez vos configurations.

PARTIE 5

Activité 1 : Modifier la zone unique OSPFv2- Packet Tracer

Réponse

Partie 1 /Etape 1 :

R1

```
enable
conf t
!
ipv6 unicast-routing
!
ipv6 router ospf 10
router-id 1.1.1.1
end
clear ipv6 ospf process
y
conf t
!
interface GigabitEthernet 0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/1
 ipv6 ospf 10 area 0
!
end
```

R2

```
enable
conf t
!
ipv6 unicast-routing
!
ipv6 router ospf 10
router-id 2.2.2.2
end
clear ipv6 ospf process
y
conf t
!
interface GigabitEthernet 0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/1
 ipv6 ospf 10 area 0
!
end
```

R3

```
ena
conf t
!
ipv6 unicast-routing
!
ipv6 router ospf 10
router-id 3.3.3.3
end
clear ipv6 ospf process
y
conf t
!
interface GigabitEthernet 0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/0
 ipv6 ospf 10 area 0
!
interface Serial0/0/1
 ipv6 ospf 10 area 0
!
end
```

TP 2

Implémenter le protocole OSPF

1. Configuration OSPFv2 à zone unique
2. Configuration OSPFv3 à zone unique
3. Configuration OSPF à zone multiple

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer l' OSPF à zone multiple?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 5

Activité 1 : Configurer OSPFv2 multizone- Packet Tracer

- **Objectifs**

- **Partie 1 : Configurer OSPFv2 multizone**
- **Partie 2 : Vérifier et examiner l'OSPFv2 multizone**

- **Scénario**

Dans cet exercice, vous allez configurer OSPFv2 multizone. Le réseau est déjà connecté et les interfaces sont configurées avec l'adressage IPv4. Votre travail consiste à activer l'OSPFv2 multizone, à vérifier la connectivité et à examiner le fonctionnement de l'OSPFv2 multizone.

Table d'adressage

Device	Interface	IP Address	Subnet Mask	OSPFv2 Area
R1	G0/0	10.1.1.1	255.255.255.0	1
	G0/1	10.1.2.1	255.255.255.0	1
	S0/0/0	192.168.10.2	255.255.255.252	0
R2	G0/0	10.2.1.1	255.255.255.0	0
	S0/0/0	192.168.10.1	255.255.255.252	0
	S0/0/1	192.168.10.5	255.255.255.252	0
R3	G0/0	192.168.2.1	255.255.255.0	2
	G0/1	192.168.1.1	255.255.255.0	2
	S0/0/1	192.168.10.6	255.255.255.252	0

- **Instructions**

  - **Partie 1: Configurer OSPFv2 multizone**

Etape 1: Configurez OSPFv2 sur R1

Configure OSPFv2 on R1 with a process ID of 1 and a router ID of 1.1.1.1.

Etape 2: Annoncez chaque réseau directement connecté dans OSPFv2 sur R1.

Configurez chaque réseau dans OSPFv2 en attribuant des zones en fonction de la table d'adressage.

Etape 2: Configure OSPFv2 on R2 and R3.

Répétez les étapes ci-dessus pour R2 et R3 en utilisant un ID de routeur de 2.2.2.2 et 3.3.3.3, respectivement.

  - **Partie 2 : Vérifier et examiner l'OSPFv2 multizone**

Etape 1: Vérifiez la connectivité à chacune des zones OSPFv2.

À partir de R1, envoyez une requête ping à chacun des périphériques distants suivants dans la zone 0 et la zone 2 : 192.168.1.2, 192.168.2.2 et 10.2.1.2.

Etape 2: Utilisez les commandes show pour examiner les opérations OSPFv2 en cours.

Utilisez les commandes suivantes pour collecter des informations sur votre implémentation multizone OSPFv2.

Activité 1 : Configurer OSPFv2 multizone- Packet Tracer

- **show ip protocols**
- **show ip route**
- **show ip ospf database**
- **show ip ospf interface**
- **show ip ospf neighbor**

Questions de réflexion

a. Quels routeurs sont des routeurs internes ?

b. Quels routeurs sont des routeurs frontaliers de zone ?

c. Quels routeurs sont des routeurs système autonomes ?

d. Quels routeurs génèrent des LSA de type 1 ?

e. Quels routeurs génèrent des LSA de type 2 ?

f. Quels routeurs génèrent des LSA de type 3 ?

g. Quels routeurs génèrent des LSA de type 4 et 5 ?

h. Combien de routes interzone chaque routeur possède-t-il ?

i. Pourquoi y aurait-il généralement un ASBR dans ce type de réseau ?

PARTIE 5

Activité 1 : Configurer OSPFv2 multizone- Packet Tracer

Réponse

Partie 1 /Etape 1 :

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
```

Partie 1 /Etape 2 :

```
R1(config-router)# network 10.1.1.0 0.0.0.255 area 1
R1(config-router)# network 10.1.2.0 0.0.0.255 area 1
R1(config-router)# network 192.168.10.0 0.0.0.3 area 0
```

Partie 1 /Etape 3 :

```
R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 10.2.1.0 0.0.0.255 area 0
R2(config-router)# network 192.168.10.0 0.0.0.3 area 0
R2(config-router)# network 192.168.10.4 0.0.0.3 area 0
!
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 192.168.2.0 0.0.0.255 area 2
R3(config-router)# network 192.168.1.0 0.0.0.255 area 2
R3(config-router)# network 192.168.10.4 0.0.0.3 area 0
```

Question de reflexion

a. R2

b. R1, R2 et R3 sont tous des routeurs backboon.

c. R1 et R3

d. Aucune, toutes les interfaces actives sur les trois routeurs se connectent à une zone OSPF.

e. Tous les routeurs OSPF génèrent des LSA de type 1.

f. Les routeurs cachés dans chacune des zones qui sont des DR sont. ID de routeur 4.4.4.4, 5.5.5.5, 6.6.6.6, 9.9.9.9

g. R1 et R3 parce que chacun est un ABR et a besoin d'inonder les informations de zone d'une zone à l'autre.

h. Aucun, car il n'y a pas d'ASBR dans le réseau.

i. ASBR est utilisé pour connecter des domaines de routage externes.

j. R1 et R3 ont deux IA et R2 a 4 IA.

Activité 2 : Configurer OSPFv3 multizone- Packet Tracer

- **Objectifs**

- **Partie 1 : Configurer OSPFv3**
- **Partie 2 : Vérifier les opérations OSPFv3 multizones**

- **Scénario**

Dans cet exercice, vous allez configurer OSPFv3 multizone. Le réseau est déjà connecté et les interfaces sont configurées avec l'adressage IPv6. Votre travail consiste à activer l'OSPFv3 multizone, à vérifier la connectivité et à examiner le fonctionnement de l'OSPFv3 multizone.

Table d'adressage

Device	Interface	IPv6 Address	OSPF Area
RA	G0/0	2001:db8:1:a1::1/64	1
	G0/1	2001:db8:1:a2::1/64	1
	S0/0/0	2001:db8:1:ab::2/64	0
	Link-Local	fe80::a	N/A
RB	G0/0	2001:db8:1:b1::1/64	0
	S0/0/0	2001:db8:1:ab::1/64	0
	S0/0/1	2001:db8:1:bc::1/64	0
	Link-Local	fe80::b	N/A
RC	G0/0	2001:db8:1:c1::1/64	2
	G0/1	2001:db8:1:d2::1/64	2
	S0/0/1	2001:db8:1:bc::2/64	0
	Link-Local	fe80::c	N/A

- **Instructions**

- **Partie 1: Configurer OSPFv3**

Etape 1: Activez le routage IPv6 et configurez OSPFv3 sur RA.

a. Activez le routage IPv6.

b. Configurez OSPFv3 sur RA avec un ID de processus de 1 et un ID de routeur de 1.1.1.1.

Etape 2: Annoncez chaque réseau directement connecté dans OSPFv3 sur RA.

Configurez chaque interface IPv6 active avec OSPFv3 en attribuant chacune à la zone répertoriée dans la table d'adressage.

Etape 3: Configurez OSPFv3 sur RB et RC.

Répétez les étapes 1 et 2 pour RB et RC. L'ID de routeur pour RB doit être 2.2.2.2 et l'ID de routeur pour RC doit être 3.3.3.3.

- **Partie 1: Vérifier les opérations OSPFv3 multizones**

Etape 1: Vérifiez la connectivité à chacune des zones OSPFv3.

- À partir de RA, envoyez une requête ping à chacun des appareils distants dans la zone 0 et la zone 2 :
  - 2001:db8:1:b1::2
  - 2001:db8:1:a1::2
  - 2001:db8:1:a2::2
  - 2001:db8:1:c1::2
  - 2001:db8:1:c2::2

PARTIE 5

Activité 2 : Configurer OSPFv3 multizone- Packet Tracer

Etape 2: Utilisez les commandes show pour examiner le fonctionnement d'OSPFv3.

Utilisez les commandes suivantes pour collecter des informations sur votre implémentation multizone OSPFv3.

- **show ipv6 ospf**
- **show ipv6 route**
- **show ipv6 ospf database**
- **show ipv6 ospf interface**
- **show ipv6 ospf neighbor**

Remarque : la sortie de Packet Tracer pour les protocoles show ipv6 n'est actuellement pas alignée sur la sortie IOS 15. Reportez-vous aux laboratoires d'équipement physique pour obtenir la sortie correcte de la commande show.

PARTIE 5

Activité 2 : Configurer OSPFv3 multizone- Packet Tracer

Réponse

Partie 1 /Etape 1 :

a-
```
RA(config)# ipv6 unicast-routing
```

b-
```
RA(config)# ipv6 router ospf 1
RA(config-rtr)# router-id 1.1.1.1
```

Partie 1 /Etape 2 :

```
RA(config)# interface GigabitEthernet0/0
RA(config-if)# ipv6 ospf 1 area 1
RA(config-if)# interface GigabitEthernet0/1
RA(config-if)# ipv6 ospf 1 area 1
RA(config-if)# interface Serial 0/0/0
RA(config-if)# ipv6 ospf 1 area 0
```

Partie 1 /Etape 3 :

```
RB(config)# ipv6 unicast-routing
RB(config)# ipv6 router ospf 1
RB(config-rtr)# router-id 2.2.2.2
RB(config-rtr)# interface GigabitEthernet0/0
RB(config-if)# ipv6 ospf 1 area 0
RB(config-if)# interface Serial0/0/0
RB(config-if)# ipv6 ospf 1 area 0
RB(config-if)# interface Serial0/0/1
RB(config-if)# ipv6 ospf 1 area 0
RC(config)# ipv6 unicast-routing
RC(config)# ipv6 router ospf 1
RC(config-rtr)# router-id 3.3.3.3
RC(config-rtr)# interface GigabitEthernet0/0
RC(config-if)# ipv6 ospf 1 area 2
RC(config-if)# interface GigabitEthernet0/1
RC(config-if)# ipv6 ospf 1 area 2
RC(config-if)# interface Serial 0/0/1
RC(config-if)# ipv6 ospf 1 area 0
```

TP 3

Implémenter le protocole BGP

Compétences visées :

- Configurer le protocole BGP

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

2 heures

TP 3

Implémenter le protocole BGP

1. Configuration BGP

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer l’ OSPF à zone multiple?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 5

Activité 1 : configuration et vérification du routage eBGP- Packet Tracer

- **Objectifs**

- **Partie 1 : création d'un réseau et configuration des paramètres de base des périphériques**
- **Partie 2 : configuration du protocole eBGP sur R1**
- **Partie 3 : vérification de la configuration eBGP**

- **Scénario**

Dans ces travaux pratiques, vous configurerez eBGP pour votre entreprise. Le FAI fournira la route par défaut vers Internet. Au terme de la configuration, vous exécuterez diverses commandes **show** pour vérifier que la configuration d'eBGP fonctionne comme prévu.

- **Topologie**

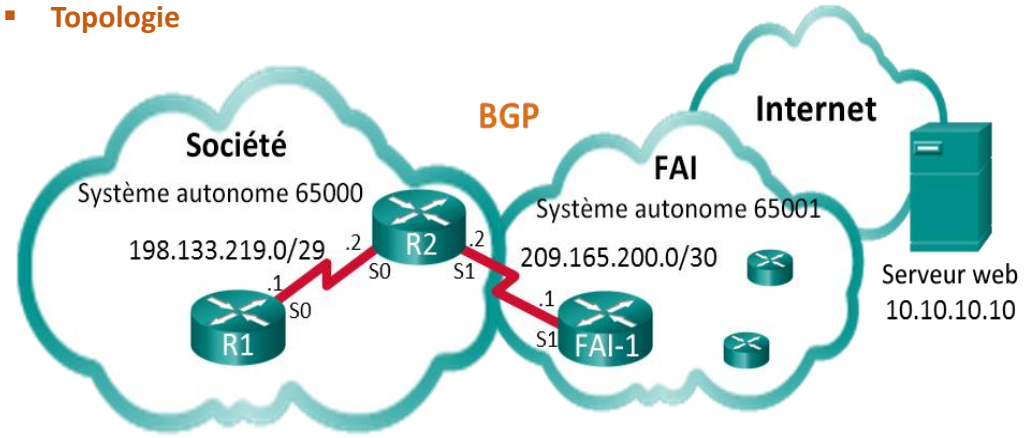


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau
R1	S0/0/0 (DCE)	198.133.219.1	255.255.255.248
R2	S0/0/0	198.133.219.2	255.255.255.248
	S0/0/1 (DCE)	209.165.200.2	255.255.255.252
FAI-1	S0/0/1	209.165.200.1	255.255.255.252
Serveur web		10.10.10.10	255.255.255.255

- **Ressources requises**

- 3 routeurs (Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles série conformément à la topologie

- **Instructions**

- **Partie 1: Création d'un réseau et configuration des paramètres de base des périphériques**

Etape 1: câblage du réseau conformément à la topologie indiquée.

Etape 2: initialisation et rechargement des appareils réseau, le cas échéant.

Etape 3: configuration des paramètres de base sur R1 et R2.

Activité 1 : configuration et vérification du routage eBGP- Packet Tracer

- Désactivez la recherche DNS pour empêcher les routeurs d'essayer de traduire de manière incorrecte les commandes saisies comme s'il s'agissait de noms d'hôtes.
- Configurez les noms d'hôtes conformément à la topologie.
- Configurez les interfaces conformément à la table d'adressage.
- Enregistrez la configuration en cours dans le fichier de configuration initiale.

Etape 4: copie de la configuration sur ISP1.

Copiez et collez la configuration suivante sur ISP1.

```
hostname ISP-1
no ip domain-lookup
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
interface Serial0/0/1
 ip address 209.165.200.1 255.255.255.252
 no shut
ip route 0.0.0.0 0.0.0.0 lo0
router bgp 65001
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 209.165.200.2 remote-as 65000
end
```

○ Partie 2: configuration d'eBGP sur R2

Configurez R2 pour qu'il devienne un homologue eBGP avec ISP-1. Consultez la topologie pour connaître le numéro de système autonome BGP.

Etape 1: activation de BGP et identification du numéro de système autonome de l'entreprise.

Etape 2: utilisation de la commande neighbor pour identifier ISP1 comme homologue BGP.

Etape 3: ajout du réseau de l'entreprise à la table BGP pour l'annoncer à ISP1.

○ Partie 3: vérification de la configuration eBGP

Dans la Partie 3, utilisez les commandes de vérification BGP pour contrôler que la configuration BGP fonctionne comme prévu.

Etape 1: affichage de la table de routage IPv4 sur R2.

Etape 2: affichage de la table BGP sur R2.

Etape 3: affichage de l'état de connexion BGP sur R2.

Etape 4: affichage de la table de routage IPv4 sur ISP-1.

Vérifiez que le réseau 198.133.218.0/29 est annoncé au routeur ISP1.

Activité 1 : configuration et vérification du routage eBGP- Packet Tracer

Envoyez une requête ping au serveur web depuis R1. Les requêtes ping ont-elles abouti ? (**Remarque :** pour que les requêtes ping aboutissent, une route statique par défaut doit être configurée sur R1 à l'aide de l'interface de série 0/0/0 en tant qu'interface de sortie.)

Question de réflexion

La topologie utilisée dans ces travaux pratiques a été créée pour expliquer comment configurer le protocole de routage BGP. Cependant, le protocole BGP ne serait normalement pas configuré pour une topologie comme celle-ci dans le monde réel. Expliquez votre réponse.

PARTIE 5

Activité 1 : configuration et vérification du routage eBGP- Packet Tracer

Réponse

- **Partie 2/ Etape 1**

```
R2(config)# router bgp 65000
```

- **Partie 2/ Etape 2**

```
R2(config-router)# neighbor 209.165.200.1 remote-as 65001
```

- **Partie 2/ Etape 3**

```
R2(config-router)# network 198.133.219.0 mask 255.255.255.248
```

- **Partie 3/ Etape 1**

```
R2# show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.1 to network 0.0.0.0
 B*    0.0.0.0/0 [20/0] via 209.165.200.1, 00:00:07
      198.133.219.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.133.219.0/29 is directly connected, Serial0/0/0
L        198.133.219.2/32 is directly connected, Serial0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/30 is directly connected, Serial0/0/1
L        209.165.200.2/32 is directly connected, Serial0/0/1
```

Partie 3/ Etape 2

```
R2# show ip bgp
BGP table version is 4, local router ID is 209.165.200.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  0.0.0.0          209.165.200.1            0             0 65001 i
 *>  198.133.219.0/29 0.0.0.0                  0         32768 i
```

PARTIE 5

Activité 1 : configuration et vérification du routage eBGP- Packet Tracer

Réponse

- **Partie 3/ Etape 3**

```
R2# show ip bgp summary
BGP router identifier 209.165.200.2, local AS number 65000
BGP table version is 4, main routing table version 4
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 320 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 792 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
209.165.200.1   4        65001      12      11        4    0    0 00:06:56        1
```

- **Partie 3/ Etape 4**

```
ISP-1# show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Loopback0
      10.0.0.0/32 is subnetted, 1 subnets
C        10.10.10.10 is directly connected, Loopback0
      198.133.219.0/29 is subnetted, 1 subnets
B        198.133.219.0 [20/0] via 209.165.200.2, 00:00:25
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/30 is directly connected, Serial0/0/1
L        209.165.200.1/32 is directly connected, Serial0/0/1
```

Question de réflexion

- Oui, les requêtes ping ont normalement dû aboutir.

Les réponses peuvent varier. En règle générale, le protocole BGP n'est pas nécessaire pour un réseau à résidence unique. Le FAI fournit une plage d'adresses IP de sous-réseau IP que l'entreprise utilise pour l'accès Internet. Le FAI est chargé de router le trafic de l'entreprise vers le routeur R2. Par conséquent, le protocole BGP ne doit être configuré que pour le FAI.

PARTIE 6

Gérer la connectivité des réseaux d'entreprise

Dans ce module, vous allez :

- Etre en mesure de comprendre les technologies de réseau WAN
- Etre capable de sécuriser l'accès au réseau informatique
- Etre en mesure de mettre en place un système de gestion, de surveillance et de dépannage des réseaux informatiques

17 heures

TP 1

Étudier les réseaux étendus

Compétences visées :

- Étudier les différents technologies des réseaux étendus

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

3 heures

TP 1

Étudier les réseaux étendus

1. Concepts WAN
2. Configuration PPPoE

Critères de réussite :

- Le stagiaire est-il capable de :
  - Comprendre les concepts WAN?
- Réponses correctes pour au moins 70 % des questions.

Activité 1 : Concepts WAN - Packet Tracer

Objectifs

Dans cette activité, vous étudierez différents types de WAN en explorant une topologie qui utilise diverses technologies de connectivité.

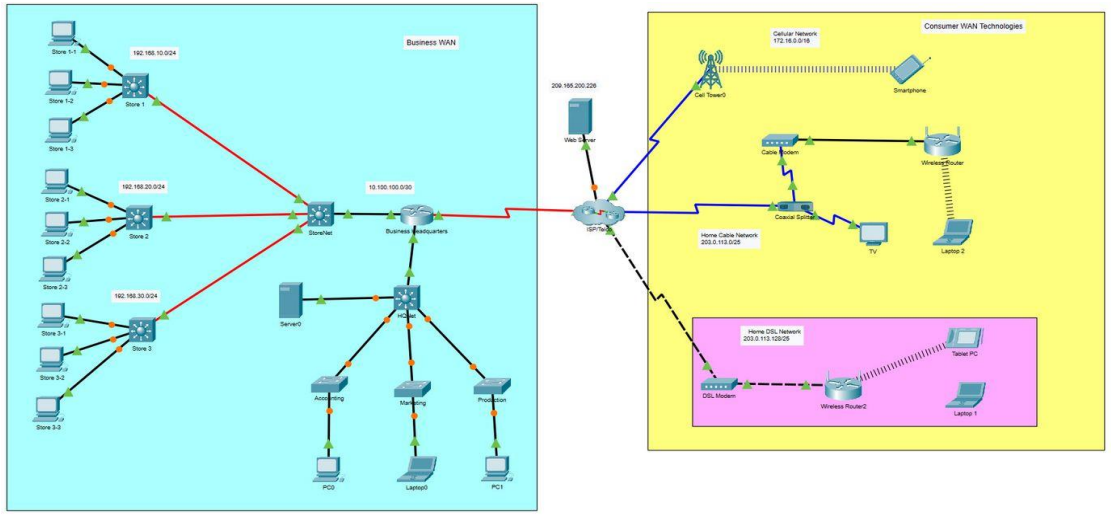
- **Décrivez les différentes options de connectivité WAN.**

Contexte/scénario

Vous explorerez les technologies WAN utilisées pour connecter les utilisateurs professionnels et domestiques aux services de données.

Remarque: Il n'y a pas de notation dans cette activité.

Topologie



Instructions

Partie 1: Recherche sur les technologies WAN des consommateurs pour les appareils domestiques et mobiles

Etape 1: Explorez les technologies WAN des consommateurs

Dans cette étape, vous explorerez trois technologies WAN des consommateurs et les réseaux domestiques.

a. Regardez les deux réseaux domestiques.

Question:

- Quelles sont les technologies WAN utilisées?

b. Examinez les connexions utilisées dans la topologie réseau en sélectionnant l'icône Connexions (le foudre orange) dans le menu Périphériques de Packet Tracer. Passez la souris sur les icônes du média pour afficher leurs noms dans la zone blanche située en bas de la fenêtre du Packet Tracer.

Question:

- Quels médias sont utilisés pour connecter les deux réseaux domestiques au FAI? Quels appareils dans les réseaux domestiques sont directement connectés au FAI?

c. Cliquez sur le modem DSL et ouvrez l'onglet Physique.

Activité 1 : Concepts WAN - Packet Tracer

Questions:

- Quels sont les ports disponibles sur l'appareil et qu'est-ce qui y est connecté ?
- Quel est l'objectif du modem DSL ?
- Quel est le type de connexion entre le réseau de l'ISP/Telco/Cable d'entreprise et le réseau câblé domestique ? Pourquoi le séparateur est-il nécessaire?

d. Regardez les ports du modem câble.

Questions:

- A quoi sert le modem-câble ? Quels sont ses connexions ?
- À quel port le câble du modem câble se connecte-t-il sur le routeur sans fil domestique? D'où vient l'adresse IP de l'interface?

e. Regardez le Smartphone.

Question:

- Quelle est son adresse IP? D'où vient l'adresse IP?
- Quel service de données le téléphone cellulaire utilise-t-il actuellement (données cellulaires ou Wi-Fi)?

Etape 2: Explorez le réseau WAN d'entreprise

Dans cette étape, vous allez explorer le WAN d'entreprise. L'entreprise est un magasin de vente de pneus au détail. Il a un siège social local où la plupart des fonctions commerciales se produisent, et trois magasins qui sont connectés au réseau étendu de l'entreprise.

a. Regardez le menu Connexions.

Question:

- Quels types de connexions voyez-vous en cours d'utilisation dans le réseau Business?

b. Ouvrez la vue physique du commutateur StoreNet.

Question :

- Quels types d'interfaces sont présents ? Vous devrez peut-être zoomer et faire défiler la vue pour voir.
- Quelles sont les interfaces et les supports utilisés pour connecter les réseaux de magasins au réseau du siège de l'entreprise ? Pourquoi?
- Quel type de service WAN est utilisé pour connecter le routeur du siège social au FAI ?

Partie 2: Explorer la connectivité

Envoyez une requête ping aux appareils sur les réseaux WAN d'entreprise et WAN de consommateurs. Envoyez une requête ping également entre les réseaux et entre les réseaux et le serveur Web. Tous les hôtes peuvent-ils ping les uns les autres et le serveur Web?

Est-ce une bonne situation?

Activité 1 : Concepts WAN - Packet Tracer

Réponses

- **Partie 1 / Etape 1:**

a) - Les réseaux domestiques utilisent les technologies câble et DSL WAN.

b) - Le réseau câblé utilise un support coaxial pour connecter le réseau câblé domestique au FAI. Le support coaxial se connecte au dispositif séparateur coaxial. Le câble téléphonique relie le réseau DSL au FAI. Le câble téléphonique se connecte au modem DSL.

c) - Le modem DSL a deux ports. L'un est connecté à la ligne téléphonique du Telco. L'autre port est connecté au LAN domestique via Ethernet.

- Il convertit les signaux du réseau de données téléphoniques en Ethernet pour le réseau domestique.

- La connexion à la maison se fait avec un câble coaxial. Le séparateur est nécessaire car le câble transporte à la fois des données numériques et des signaux vidéo. Le répartiteur divise le média afin que le signal de données puisse être envoyé au modem câble et le signal vidéo au téléviseur.

d) - Le modem câble convertit les signaux de données du câble en signaux Ethernet. Il est connecté au câble coaxial du répartiteur et au câble UTP de l'interface Ethernet.

- Il se connecte à l'interface internet. L'adresse IP provenait du réseau ISP via DHCP.

e) - L'adresse IP est 198.51.100.100. L'adresse doit provenir du réseau Telco via DHCP.

- Le téléphone utilise actuellement les données cellulaires du réseau 3G/4G.

Partie 1 / Etape 2:

a) - Ethernet sur cuivre et fibre et également série.

b) - Le commutateur est doté de ports média en cuivre Gigabit Ethernet et de quatre ports modulaires. Trois modules SFP (Small Form-Factor Pluggable) à fibre optique GLC-LH-SMD sont insérés dans les ports modulaires. Ces modules permettent au switch de se connecter aux réseaux Ethernet fibre optique.

- Les magasins sont connectés au commutateur StoreNet avec Ethernet via des câbles à fibres optiques. Cela a été fait en raison de la distance nécessaire pour atteindre les magasins. En réalité, un autre fournisseur fournirait ce service de fibre optique, mais cela a été simplifié pour les besoins de cette activité.

- Le routeur utilise une connexion WAN série pour se connecter au FAI.

- **Partie 2**

- Les hôtes des deux réseaux peuvent cingler le serveur Web, mais les hôtes des réseaux WAN professionnels ne peuvent pas cingler les hôtes des réseaux WAN grand public et vice versa.

- Oui, ces réseaux ne doivent pas être directement accessibles de l'extérieur pour des raisons de sécurité.

TP 1

Étudier les réseaux étendus

1. Concepts WAN
2. Configuration PPPoE

Critères de réussite :

- Le stagiaire est-il capable de :
  - Comprendre les concepts WAN?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 6

Activité 1 : Configuration d'un routeur en tant que client PPPoE pour la connectivité DSL Lab

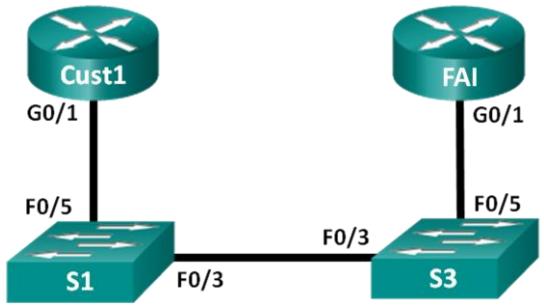
- **Objectifs**

- **Partie 1 : création du réseau**
- **Partie 2 : configuration du routeur du fournisseur d'accès à Internet (FAI)**
- **Partie 3 : configuration du routeur Cust1**

- **Contexte/scénario**

- Les FAI utilisent souvent le protocole point à point sur Ethernet (PPPoE) dans le cas des liaisons DSL avec leurs clients. Le protocole PPP prend en charge l'attribution d'une adresse IP à un appareil au niveau de l'extrémité distante d'une liaison PPP. Plus important encore, le protocole PPP prend en charge l'authentification CHAP. Les FAI peuvent contrôler les dossiers comptables afin de voir si la facture d'un client a été payée avant de l'autoriser à se connecter à Internet.
- Au cours de ces travaux pratiques, vous allez configurer à la fois le côté client et le côté FAI de la connexion lors de la configuration du protocole PPPoE. D'une manière générale, vous ne devrez configurer que le côté client.

- **Topologie**



- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Cust1	G0/1	Apprentissage par le biais du protocole PPP	Apprentissage par le biais du protocole PPP	Apprentissage par le biais du protocole PPP
FAI	G0/1	N/A	N/A	N/A

- **Ressources requises**

- 2 routeurs (Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 2 commutateurs (Cisco 2960 équipé de Cisco IOS version 15.0(2), image lanbasek9 ou similaire)
- Câbles de console pour configurer les appareils Cisco IOS via les ports de console
- Câbles Ethernet conformément à la topologie

- **Instructions**

  - **Partie 1: Création du réseau**

Etape 1: Câblez le réseau conformément à la topologie indiquée.

Etape 2: Initialisez et redémarrez les routeurs et les commutateurs.

Activité 1 : Configuration d'un routeur en tant que client PPPoE pour la connectivité DSL Lab

Etape 3: Configurez les paramètres de base pour chaque routeur.

a. Désactivez la commande de recherche DNS.

b. Configurez le nom du périphérique conformément à la topologie.

c. Cryptez les mots de passe en texte brut.

d. Créez une bannière MOTD (message du jour) pour informer les utilisateurs que tout accès non autorisé est interdit.

e. Attribuez le mot de passe du mode d'exécution privilégié crypté **class**.

f. Attribuez le mot de passe **cisco** à la console et au vty, puis activez la connexion.

g. Définissez la connexion à la console sur le mode synchronisé.

h. Enregistrez votre configuration.

- **Partie 2: configuration du routeur FAI**

- Dans la Partie 2, vous allez configurer le routeur FAI à l'aide de paramètres PPPoE pour la connexion à partir du routeur Cust1.

Remarque : de nombreuses commandes de configuration PPPoE du routeur FAI sortent du cadre de ce cours ; toutefois, elles sont nécessaires à la réalisation de ces travaux pratiques. Vous pouvez les copier et les coller dans le routeur FAI au niveau de l'invite du mode de configuration globale.

a. Créez le nom d'utilisateur de base de données locale **Cust1** avec le mot de passe **ciscopppoe**.

```
ISP(config)# username Cust1 password ciscopppoe
```

b. Créez un pool d'adresses qui seront attribuées aux clients.

```
ISP(config)# ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
```

c. Créez le modèle virtuel et associez-lui l'adresse IP de l'interface G0/1. Associez le modèle virtuel au pool d'adresses. Configurez le protocole CHAP afin d'authentifier les clients.

```
ISP(config)# interface virtual-template 1
ISP(config-if)# ip address 10.0.0.254 255.255.255.0
ISP(config-if)# mtu 1492
ISP(config-if)# peer default ip address pool PPPoEPOOL
ISP(config-if)# ppp authentication chap callin
ISP(config-if)# exit
```

d. Attribuez le modèle au groupe PPPoE.

```
ISP(config)# bba-group pppoe global
ISP(config-bba-group)# virtual-template 1
ISP(config-bba-group)# exit
```

PARTIE 6

Activité 1 : Configuration d'un routeur en tant que client PPPoE pour la connectivité DSL Lab

e. Associez le groupe bba à l'interface physique G0/1.

```
ISP(config)# interface g0/1
ISP(config-if# pppoe enable group global
ISP(config-if)# no shutdown
```

- **Partie 3: Configuration du routeur Cust1**

Dans la Partie 3, vous allez configurer le routeur Cust1 à l'aide de paramètres PPPoE.

a. Configurez l'interface G0/1 pour la connectivité PPPoE.

```
Cust1(config)# interface g0/1
Cust1(config-if)# pppoe enable
Cust1(config-if)# pppoe-client dial-pool-number 1
Cust1(config-if)# exit
```

b. Associez l'interface G0/1 à une interface de numérotation. Utilisez le nom d'utilisateur **Cust1** et le mot de passe **ciscopppoe** configurés à la Partie 2.

```
Cust1(config)# interface dialer 1
Cust1(config-if)# mtu 1492
Cust1(config-if)# ip address negotiated
Cust1(config-if)# encapsulation ppp
Cust1(config-if)# dialer pool 1
Cust1(config-if)# ppp authentication chap callin
Cust1(config-if)# ppp chap hostname Cust1
Cust1(config-if)# ppp chap password ciscopppoe
Cust1(config-if)# exit
```

c. Configurez une route statique par défaut pointant vers l'interface de numérotation.

```
Cust1(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
```

d. Configurez le débogage sur le routeur Cust1 de manière à afficher la négociation PPP et PPPoE.

```
Cust1# debug ppp authentication
Cust1# debug pppoe events
```

e. Activez l'interface G0/1 sur le routeur Cust1 et observez le résultat du débogage lors de l'établissement de la session de numérotation PPPoE et de l'authentification CHAP.

```
Cust1(config)# interface g0/1
Cust1(config-if)# no shutdown
```

PARTIE 6

Activité 1 : Configuration d'un routeur en tant que client PPPoE pour la connectivité DSL Lab

```
*Jul 30 19:28:42.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
*Jul 30 19:28:46.175: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Jul 30 19:28:47.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
*Jul 30 19:29:03.839:  padi timer expired
*Jul 30 19:29:03.839:  Sending PADI: Interface = GigabitEthernet0/1
*Jul 30 19:29:03.839: PPPoE 0: I PADO  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.887:  PPPOE: we've got our pado and the pado timer went off
*Jul 30 19:29:05.887: OUT PADR from PPPoE Session
*Jul 30 19:29:05.895: PPPoE 1: I PADS  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.895: IN PADS from PPPoE Session
*Jul 30 19:29:05.899: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jul 30 19:29:05.899: PPPoE: Virtual Access interface obtained.
*Jul 30 19:29:05.899: PPPoE : encap string prepared
*Jul 30 19:29:05.899: [0]PPPoE 1: data path set to PPPoE Client
*Jul 30 19:29:05.903: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Jul 30 19:29:05.911: Vi2 PPP: Using dialer call direction
*Jul 30 19:29:05.911: Vi2 PPP: Treating connection as a callout
*Jul 30 19:29:05.911: Vi2 PPP: Session handle[C6000001] Session id[1]
*Jul 30 19:29:05.919: Vi2 PPP: No authorization without authentication
*Jul 30 19:29:05.939: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Jul 30 19:29:05.939: Vi2 PPP: Sent CHAP SENDAUTH Request
*Jul 30 19:29:05.939: Vi2 PPP: Received SENDAUTH Response FAIL
*Jul 30 19:29:05.939: Vi2 CHAP: Using hostname from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: Using password from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"
*Jul 30 19:29:05.955: Vi2 CHAP: I SUCCESS id 1 len 4
*Jul 30 19:29:05.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access2, changed state to up
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
```

f. Exécutez une commande **show ip interface brief** sur le routeur Cust1 de manière à afficher l'adresse IP attribuée par le routeur FAI. Voici un exemple de résultat. À l'aide de quelle méthode l'adresse IP a-t-elle été obtenue ?

```
Cust1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
Dialer1                    10.0.0.1        YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  up                    up
```

PARTIE 6

Activité 1 : Configuration d'un routeur en tant que client PPPoE pour la connectivité DSL Lab

g. Exécutez une commande **show ip route** sur le routeur Cust1. Voici un exemple de résultat.

```
Cust1# show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Dialer1
      10.0.0.0/32 is subnetted, 2 subnets
C        10.0.0.1 is directly connected, Dialer1
C        10.0.0.254 is directly connected, Dialer1
```

h. Exécutez une commande **show pppoe session** sur le routeur Cust1. Voici un exemple de résultat.

```
Cust1# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                VT  VA         State
           SID  LocMAC                              VA-st      Type
    N/A      1  30f7.0da3.0b01  Gi0/1               Di1 Vi2        UP
                30f7.0da3.0bc1                          UP
```

i. Exécutez une requête ping vers 10.0.0.254 à partir du routeur Cust1. La requête ping devrait aboutir. Si ce n'est pas le cas, dépannez le scénario jusqu'à ce que la connectivité soit établie.

```
Cust1# ping 10.0.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Question de réflexion

Pourquoi les FAI qui utilisent la technologie DSL utilisent-ils également principalement le protocole PPPoE avec leurs clients ?

PARTIE 6

Activité 1 : Configuration d'un routeur en tant que client PPPoE pour la connectivité DSL Lab

Réponses

Partie 3

f : PPP

Question de réflexion

Le protocole PPP prend en charge l'authentification sur une liaison Ethernet. Les FAI peuvent authentifier les clients et introduire une adresse IP.

Configuration :

Routeur Cust1

```
Cust1# show run
Building configuration...
Current configuration : 1433 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Cust1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 1
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Dialer1
 mtu 1492
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ppp authentication chap callin
 ppp chap hostname Cust1
 ppp chap password 0 ciscopppoe
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Dialer1
!
control-plane
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
```

PARTIE 6

Activité 1 : Configuration d'un routeur en tant que client PPPoE pour la connectivité DSL Lab

Réponses

```
line con 0
 password 7 14141B180F0B
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin
lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 05080F1C2243
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Routeur FAI

```
ISP# show run
Building configuration...

Current configuration : 1485 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
username Cust1 password 0 ciscopppoe
!
```

```
bba-group pppoe global
 virtual-template 1
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable group global
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
```

Activité 1 : Configuration d'un routeur en tant que client PPPoE pour la connectivité DSL Lab

Réponses

```
!
interface Virtual-Template1
 ip address 10.0.0.254
255.255.255.0
 mtu 1492
 peer default ip address pool
PPPoEPOOL
 ppp authentication chap callin
!
ip local pool PPPoEPOOL 10.0.0.1
10.0.0.10
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C
Unauthorized Access Prohibited.
^C
!
```

```
line con 0
 password 7 14141B180F0B
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120
ssh
 stopbits 1
line vty 0 4
 password 7 05080F1C2243
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

TP 2

Sécuriser l’accès aux réseaux

Compétences visées :

- Sécuriser l’accès aux réseaux avec les ACLs
- Configurer l’accès au réseau public avec NAT pour IPv4

Recommandations clés:

- Lire attentivement l’énoncé et les questions
- Se référer au cours

7 heures

TP 2

Sécuriser l’accès aux réseaux

1. Configuration des ACLs
2. Configuration de la NAT pour IPv4
3. Configuration de IPSec VPN

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer les ACLs?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 6

Activité 1 : Configurer des listes ACL IPv4 standard numérotées - Packet Tracer

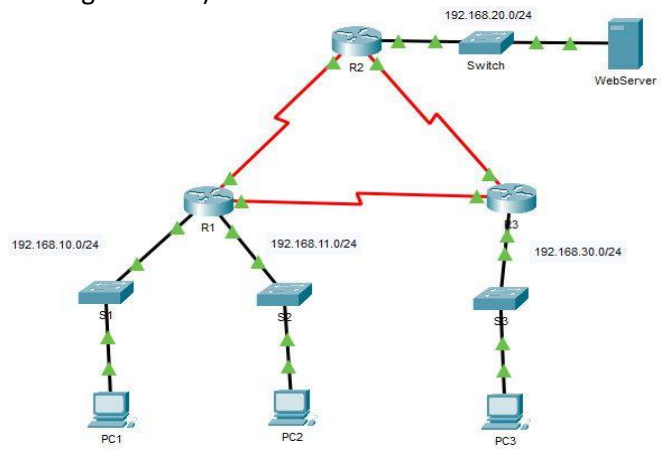
- **Objectifs**

- **Partie 1: Planifier la mise en œuvre d'une liste de contrôle d'accès**
- **Partie 2: Configurer, appliquer et vérifier une liste de contrôle d'accès standard**

- **Contexte**

Les listes de contrôle d'accès standard sont des scripts de configuration de routeur déterminant l'autorisation ou le rejet de paquets en fonction de leur adresse source. Cet exercice porte sur la définition de critères de filtrage, sur la configuration de listes de contrôle d'accès standard, sur l'application de listes de contrôle d'accès aux interfaces des routeurs et sur la vérification et le test de la mise en œuvre de listes de contrôle d'accès. Les routeurs sont déjà configurés, y compris le routage d'adresses IP et de protocole EIGRP (Enhanced Interior Gateway Routing Protocol).

- **Topologie**



- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	G0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
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
ServeurWeb	Carte réseau	192.168.20.254	255.255.255.0	192168.20.1

- **Instructions**

  - **Partie 1: Planifier la mise en œuvre d'une liste de contrôle d'accès**

Etape 1: Étudiez la configuration réseau actuelle

Avant d'appliquer une liste de contrôle d'accès à un réseau, il convient de vérifier que vous disposez d'une connectivité complète. Vérifiez la connectivité complète du réseau en choisissant un PC et en envoyant une requête ping à d'autres périphériques sur le réseau. Chaque requête ping doit aboutir.

Activité 1 : Configurer des listes ACL IPv4 standard numérotées Packet Tracer

Etape 2: Évaluez deux stratégies réseau et planifiez les implémentations de liste de contrôle d'accès

a. Les stratégies réseau suivantes sont implémentées sur **R2**:

- Le réseau 192.168.11.0/24 n'est pas autorisé à accéder au **ServeurWeb** situé sur le réseau 192.168.20.0/24.
- Tous les autres accès sont autorisés.

Pour limiter l'accès du réseau 192.168.11.0/24 vers **ServeurWeb** sur 192.168.20.254 sans perturber le reste du trafic, il faut créer une liste de contrôle d'accès sur **R2**. Cette liste d'accès doit être placée sur l'interface de sortie vers **ServeurWeb**. Une deuxième règle doit être créée sur **R2** pour autoriser tous les autres types de trafic.

b. Les stratégies réseau suivantes sont implémentées sur R3:

- Le réseau 192.168.10.0/24 n'est pas autorisé à communiquer avec le réseau 192.168.30.0/24.
- Tous les autres accès sont autorisés.

Une liste d'accès doit être créée sur le routeur **R3** afin de limiter l'accès du réseau 192.168.10.0/24 au réseau 192.168.30/24 sans perturber les autres trafics. Il faut placer la liste ACL sur l'interface sortante vers **PC3**. Une deuxième règle doit être créée sur **R3** pour autoriser tous les autres types de trafic.

- **Partie 2: Configurer, appliquer et vérifier une liste de contrôle d'accès standard**

Etape 1: Configurez et appliquez une liste de contrôle d'accès standard numérotée sur R2

a. Créez une liste de contrôle d'accès en utilisant le numéro **1** sur **R2** avec une instruction refusant l'accès vers le réseau 192.168.20.0/24 à partir du réseau 192.168.11.0/24.

Ouvrez la fenêtre de configuration.

- R2(config)# **access-list 1 deny 192.168.11.0 0.0.0.255**

b. Par défaut, une liste d'accès refuse tout trafic non conforme aux règles. Pour autoriser tout autre trafic, configurez l'instruction suivante:

- R2(config)# **access-list 1 permit any**

c. Avant d'appliquer une liste d'accès à une interface pour filtrer le trafic, il est recommandé d'examiner le contenu de la liste d'accès afin de vérifier qu'elle filtrera le trafic comme prévu.

- R2# **show access-lists**

```
Standard IP access list 1
        10 deny 192.168.11.0 0.0.0.255
        20 permit any
```

d. Pour que la liste de contrôle d'accès filtre réellement le trafic, elle doit être appliquée au routeur. Appliquez la liste de contrôle d'accès en la plaçant pour le trafic sortant sur l'interface Gigabit Ethernet 0/0.

Remarque: Dans un réseau opérationnel réel, il n'est pas recommandé d'appliquer une liste d'accès non testée à une interface active.

- R2(config)# **interface GigabitEthernet0/0**
- R2(config-if)# **ip access-group 1 out**

Activité 1 : Configurer des listes ACL IPv4 standard numérotées Packet Tracer

Etape 2: Configurez et appliquez une liste de contrôle d'accès standard numérotée sur R3

a. Créez une liste de contrôle d'accès en utilisant le numéro **1** sur **R3** avec une instruction refusant l'accès au réseau 192.168.30.0/24 à partir du réseau du **PC1** (192.168.10.0/24).

- R3(config)# **access-list 1 deny 192.168.10.0 0.0.0.255**

b. Par défaut, une liste ACL refuse tout trafic non conforme aux règles. Pour autoriser tout autre trafic, créez une deuxième règle pour la liste de contrôle d'accès ACL1.

- R3(config)# **access-list 1 permit any**

c. Vérifiez que la liste d'accès est correctement configurée.

- R3# **show access-lists**

```
Standard IP access list 1
        10 deny 192.168.10.0 0.0.0.255
        20 permit any
```

d. Appliquez la liste de contrôle d'accès en la plaçant pour le trafic sortant sur l'interface Gigabit Ethernet 0/0.

- R3(config)# **interface GigabitEthernet0/0**
- R3(config-if)# **ip access-group 1 out**

Etape 3: Vérifiez la configuration et le fonctionnement des listes de contrôle d'accès

a. Utilisez la commande **show run** ou **show ip interface gigabitethernet 0/0** pour vérifier que les listes de contrôle d'accès sont placées correctement.

b. Avec les deux listes de contrôle d'accès en place, le trafic réseau est limité en fonction des stratégies détaillées dans la Partie 1. Utilisez les tests suivants pour vérifier les implémentations de liste de contrôle d'accès :

- Une requête ping de 192.168.10.10 vers 192.168.11.10 aboutit.
- Une requête ping de 192.168.10.10 vers 192.168.20.254 aboutit.
- Une requête ping de 192.168.11.10 vers 192.168.20.254 échoue.
- Une requête ping de 192.168.10.10 vers 192.168.30.10 échoue.
- Une requête ping de 192.168.11.10 vers 192.168.30.10 aboutit.
- Une requête ping de 192.168.30.10 vers 192.168.20.254 aboutit.

c. Exécutez à nouveau la commande **show access-lists** sur les routeurs **R2** et **R3** . Vous devriez voir une sortie qui indique le nombre de paquets qui correspondent à chaque ligne de la liste d'accès.

Remarque: Le nombre de correspondances affichées pour vos routeurs peut être différent, en raison du nombre de pings envoyés et reçus.

- R2# **show access-lists**

```
Standard IP access list 1
        10 deny 192.168.11.0 0.0.255 (4 match (s))
        20 deny any (8 match (s))
```

- R3# **show access-lists**

```
Standard IP access list 1
        10 deny 192.168.10.0 0.0.0.255 (4 match(es))
        20 permit any (8 match(es))
```

PARTIE 6

Activité 1 : Configurer des listes ACL IPv4 standard numérotées - Packet Tracer

Réponses

Configuration :

R1 :

```
enable
configure terminal
interface GigabitEthernet0/0
  ip access-group 1 out
access-list 1 deny 192.168.11.0 0.0.0.255
access-list 1 permit any
end
```

- **R2 :**

```
enable
configure terminal
interface GigabitEthernet0/0
  ip access-group 1 out
access-list 1 deny 192.168.10.0 0.0.0.255
access-list 1 permit any
end
```

PARTIE 6

Activité 1 : Configurer les ACLs IPv4 standard nommées - Packet Tracer

- **Objectifs**

- **Partie 1 : configuration et application d'une liste de contrôle d'accès standard nommée**

- **Partie 2 : vérification de l'implémentation de la liste de contrôle d'accès**

- **Contexte**

L'administrateur réseau principal vous a chargé de créer une liste ACL standard nommée afin d'empêcher l'accès au serveur de fichiers. Le serveur de fichiers contient la base de données des applications Web. Seules la station de travail Web Manager PC1 et le serveur Web doivent accéder au serveur de fichiers. Tout autre trafic vers le serveur de fichiers doit être refusé.

- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192168.20,1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
Serveur de fichiers	Carte réseau	192.168.200.100	255.255.255.0	192.168.200.1
Serveur Web	Carte réseau	192.168.100.100	255.255.255.0	192.168.100.1
PC0	Carte réseau	192.168.20.3	255.255.255.0	192168.20,1
PC1	Carte réseau	192.168.20.4	255.255.255.0	192168.20,1
PC2	Carte réseau	192.168.10.3	255.255.255.0	192.168.10.1

- **Instructions**

  - **Partie 1: Configuration et application d'une liste de contrôle d'accès standard nommée**

Etape 1: Vérifiez la connectivité avant de configurer et d'appliquer la liste de contrôle d'accès

Les trois postes de travail devraient être capables de faire un ping à la fois sur le **serveur Web** et sur le **serveur de fichiers**.

Etape 2: Configurez une liste de contrôle d'accès standard nommée

a. Configurez la liste de contrôle d'accès nommée suivante sur **R1**.

- R1(config)# **ip access-list standard File_Server_Restrictions**
- R1(config-std-nacl)# **permit host 192.168.20.4**
- R1(config-std-nacl)# **permit host 192.168.100.100**
- R1(config-std-nacl)# **deny any**

Remarque: À des fins de notation, le nom ACL respecte la casse et les instructions doivent être dans le même ordre que celui indiqué.

b. Utilisez la commande **show access-lists** pour vérifier le contenu de la liste d'accès avant de l'appliquer à une interface. Assurez-vous que vous n'avez pas mal tapé les adresses IP et que les instructions sont dans le bon ordre.

- R1# **show access-lists**

Activité 2 : Configurer les ACLs IPv4 standard nommées - Packet Tracer

```
Standard IP access list File_Server_Restrictions
10 permit host 192.168.20.4
20 permit host 192.168.100.100
30 deny any
```

Etape 3: Appliquez la liste de contrôle d'accès nommée

a. Appliquez l'ACL en sortie sur l'interface Fast Ethernet 0/1.

Remarque : Dans un réseau opérationnel réel, l'application d'une liste d'accès à une interface active n'est pas une bonne pratique et devrait être évitée si possible.

- R1(config-if)# **ip access-group File_Server_Restrictions out**

b. Enregistrer la configuration.

- **Partie 2: Vérification de l'implémentation de la liste de contrôle d'accès**

Etape 1: Vérifiez la configuration de la liste de contrôle d'accès et son application à l'interface

Utilisez la commande **show access-lists** pour vérifier la configuration de la liste de contrôle d'accès. Utilisez la commande **show run** ou **show ip interface fastethernet 0/1** pour vérifier que la liste de contrôle d'accès est appliquée correctement à l'interface.

Etape 2: Vérifiez que la liste de contrôle d'accès fonctionne convenablement

Les trois postes de travail devraient pouvoir envoyer un ping au **serveur Web**, mais seuls le **PC1** et le **serveur Web** devraient pouvoir envoyer un ping au **serveur de fichiers**. Répétez la commande **show access-lists** pour voir le nombre de paquets correspondant à chaque instruction.

Réponses

Configuration :

R1 :

```
enable
configure terminal
ip access-list standard File_Server_Restrictions
  permit host 192.168.20.4
  permit host 192.168.100.100 deny any interface
f0/1 ip access-group File_Server_Restrictions out
```

PARTIE 6

PARTIE 6

Activité 3 : Configurer les ACLs étendues - Scénario 1- Packet Tracer

- **Objectifs**

- **Partie 1: Configurer, appliquer et vérifier une liste de contrôle d'accès numérotée étendue**
- **Partie 2: Configurer, appliquer et vérifier une liste de contrôle d'accès nommée étendue**

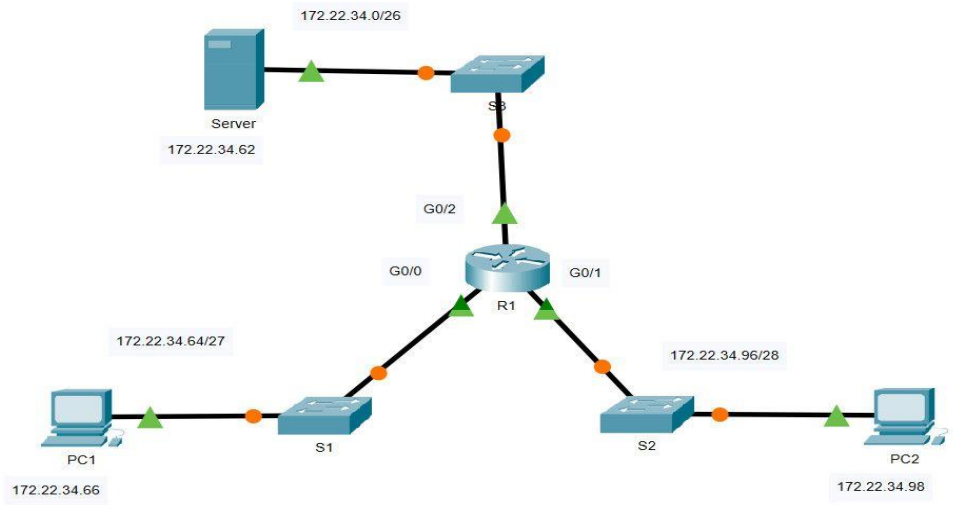
- **Contexte**

Deux employés ont besoin d'accéder aux services fournis par le serveur. **PC1** a uniquement besoin d'un accès FTP tandis que **PC2** a uniquement besoin d'un accès web. Les deux ordinateurs peuvent envoyer une requête ping au serveur, mais pas entre eux.

- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Serveur	Carte réseau	172.22.34.62	255.255.255.192	172.22.34.1
PC1	Carte réseau	172.22.34.66	255.255.255.224	172.22.34.65
PC2	Carte réseau	172.22.34.98	255.255.255.240	172.22.34.97

- **Topologie**



- **Instructions**

- **Partie 1: Configurer, appliquer et vérifier une liste de contrôle d'accès numérotée étendue**

Etape 1: Configurez un ACL pour autoriser le FTP et l'ICMP à partir du LAN du PC1

a. En mode de configuration globale sur **R1**, entrez la commande suivante pour déterminer le premier numéro valide d'une liste de contrôle d'accès étendue.

Activité 3 : Configurer les ACLs étendues - Scénario 1- Packet Tracer

Ouvrez la fenêtre de configuration.

- R1(config)# **access-list ?**

```
<1-99> IP standard access list
  <100-199> IP extended access list
```

b. Ajoutez **100** à la commande et faites suivre d'un point d'interrogation.

- R1(config)# **access-list 100 ?**

```
deny Specify packets to reject
  permit Specify packets to forward
remark Access list entry comment
```

c. Pour autoriser le trafic FTP, tapez **permit,** suivi d'un point d'interrogation.

- R1(config)# **access-list 100 permit ?**

```
  ahp Authentication Header Protocol
    eigrp Cisco's EIGRP routing protocol
    esp Encapsulation Security Payload
    gre Cisco's GRE tunneling
    icmp Internet Control Message Protocol
    ip Any Internet Protocol
    ospf OSPF routing protocol
    tcp Transmission Control Protocol
    udp User Datagram Protocol
```

d. Lorsqu'elle est configurée et appliquée, cette ACL devrait permettre le FTP et l'ICMP. ICMP est indiqué ci-dessus, mais FTP non. En effet, FTP est un protocole de couche d'application qui utilise TCP au niveau de la couche de transport. Entrez TCP pour affiner l'aide ACL.

- R1(config)# **access-list 100 permit tcp ?**

```
A.B.C.D Source address
  any Any source host
  host A single source host
```

e. L'adresse source peut représenter un seul périphérique, tel que PC1, à l'aide du mot-clé **host** , puis de l'adresse IP de PC1. L'utilisation du mot-clé **any** permet n'importe quel hôte sur n'importe quel réseau. Le filtrage peut également être effectué par une adresse réseau. Dans ce cas, il s'agit de tout hôte qui possède une adresse appartenant au réseau 172.22.34.64/27. Saisissez cette adresse de réseau, suivie d'un point d'interrogation.

- R1(config)# **access-list 100 permit tcp 172.22.34.64 ?**

```
A.B.C.D Source wildcard bits
```

f. Calculate the wildcard mask by determining the binary opposite of the /27 subnet mask.

11111111.11111111.11111111.11100000 = 255.255.255.224

00000000.00000000.00000000.000**11111** = 0.0.0.31

g. Tapez le masque générique suivi d'un point d'interrogation.

- R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?**

PARTIE 6

Activité 3 : Configurer les ACLs étendues - Scénario 1- Packet Tracer

```
A.B.C.D Destination address
  any Any destination host
  eq Match only packets on a given port number
  gt Match only packets with a greater port number
  host A single destination host
  lt Match only packets with a lower port number
  neq Match only packets not on a given port number
  range Match only packets in the range of port numbers
```

h. Configurez l'adresse de destination. Dans ce scénario, nous filtrons le trafic pour une seule destination, qui est le serveur. Saisissez le mot clé host suivi de l'adresse IP du serveur.

- R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?**

```
dscp Match packets with given dscp value
  eq Match only packets on a given port number
  established established
  gt Match only packets with a greater port number
  lt Match only packets with a lower port number
  neq Match only packets not on a given port number
  precedence Match packets with given precedence value
  range Match only packets in the range of port numbers
  <cr>
```

i. Notez que l'une des options est **<cr>** (retour chariot). Autrement dit, vous pouvez appuyer sur **Entrée** et l'instruction autoriserait tout le trafic TCP. Néanmoins, nous n'autorisons que le trafic FTP; en conséquence, saisissez le mot clé **eq** suivi d'un point d'interrogation pour afficher les options possibles. Ensuite, saisissez **ftp** et appuyez sur **Enter**.

- R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?**

```
<0-65535> Port number
  ftp File Transfer Protocol (21)
  pop3 Post Office Protocol v3 (110)
  smtp Simple Mail Transport Protocol (25)
  telnet Telnet (23)
  www World Wide Web (HTTP, 80)
```

- R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp**

j. Créez une deuxième instruction de liste d'accès pour autoriser le trafic ICMP (ping, etc.) entre PC1 et le serveur. Notez que le numéro de la liste d'accès reste le même et qu'il n'est pas nécessaire d'indiquer un type de trafic ICMP spécifique.

- R1(config)# **access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62**

k. Par défaut, tout autre trafic est refusé.

l. Exécutez la commande **show access-list** et vérifiez que la liste d'accès 100 contient les instructions correctes. Notez que la déclaration **deny any any** n'apparaît pas à la fin de la liste d'accès. L'exécution par défaut d'une liste d'accès est que si un paquet ne correspond pas à une instruction dans la liste d'accès, il n'est pas autorisé via l'interface.

Activité 3 : Configurer les ACLs étendues - Scénario 1- Packet Tracer

- R1# **show** access-lists

```
Extended IP access list 100
    10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
    20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

Etape 2: Appliquez la liste de contrôle d'accès sur l'interface appropriée pour filtrer le trafic

Du point de vue de **R1**, le trafic auquel s'applique la liste de contrôle d'accès 100 est entrant depuis le réseau connecté à l'interface Gigabit Ethernet 0/0. Passez en mode de configuration d'interface et appliquez la liste de contrôle d'accès.

Remarque: Sur un réseau opérationnel réel, il n'est pas recommandé d'appliquer une liste d'accès non testée à une interface active.

- R1(config)# **interface gigabitEthernet 0/0**
- R1(config-if)# **ip access-group 100 in**

Etape 1: Vérifiez l'implémentation de la liste de contrôle d'accès

a. Envoyez une requête ping de PC1 au serveur. Si les requêtes ping n'aboutissent pas, vérifiez les adresses IP avant de continuer.

b. Établissez une connexion FTP entre PC1 et le serveur. Le nom d'utilisateur et le mot de passe sont **cisco** dans les deux cas.

- PC> **ftp 172.22.34.62**

c. Quittez le service FTP.

- ftp> **quit**

Fermez la fenêtre de configuration.

d. Envoyez une requête ping de PC1 vers PC2. L'hôte de destination doit être injoignable,car la ACL n'a pas explicitement autorisé le trafic.

Partie 2: Configurer, appliquer et vérifier une liste de contrôle d'accès nommée étendue

Etape 1: Configurez une liste de contrôle d'accès pour autoriser l'accès HTTP et ICMP à partir du LAN du PC2

a. Les listes de contrôle d'accès nommées commencent par le mot-clé **ip**. En mode de configuration globale sur **R1**, entrez la commande suivante suivie d'un point d'interrogation.

Ouvrez la fenêtre de configuration.

- R1(config)# **ip access-list ?**

```
extended Extended Access List
standard Standard Access List
```

b. Vous pouvez configurer des listes de contrôle d'accès étendues et nommées standard. Cette liste d'accès filtre les adresses IP source et de destination; par conséquent, elle doit être étendue. Saisissez **HTTP_ONLY** comme nom. (Pour la notation Packet Tracer, le nom est sensible à la casse et les instructions de liste d'accès doivent être dans l'ordre correct.)

- R1(config)# **ip access-list extended HTTP_ONLY**

PARTIE 6

Activité 3 : Configurer les ACLs étendues - Scénario 1- Packet Tracer

c. L'invite change. Vous êtes maintenant en mode de configuration de liste de contrôle d'accès nommée étendue. Tous les appareils sur le réseau LAN de **PC2** ont besoin d'un accès TCP. Saisissez l'adresse du réseau, suivie d'un point d'interrogation.

- R1(config-ext-nacl)# **permit tcp 172.22.34.96 ?**

```
A.B.C.D Source wildcard bits
```

d. Une autre manière de calculer un masque générique est de soustraire le masque de sous-réseau de 255.255.255.255.

```
255.255.255.255 - 255.255.255.240 = 0.  0.  0. 15
```

- R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15**

e. Terminez l'instruction en spécifiant l'adresse du serveur comme vous l'avez fait dans la Partie 1 et en filtrant le trafic **www**.

- R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www**

f. Créez une deuxième instruction de liste d'accès pour autoriser le trafic ICMP (ping, etc.) entre **PC2** et **Serveur**. Remarque: L'invite reste identique et un type de trafic ICMP spécifique n'a pas besoin d'être spécifié.

- R1(config-ext-nacl)# **permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62**

g. Par défaut, tout autre trafic est refusé. Quittez le mode de configuration de liste de contrôle d'accès étendue nommée.

h. Exécutez la commande **show access-list** et vérifiez que la liste d'accès **HTTP_ONLY** contient les instructions correctes.

- R1# **show access-lists**

```
Extended IP access list 100
10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
Extended IP access list HTTP_ONLY
10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

Etape 2: Appliquez la liste de contrôle d'accès sur l'interface appropriée pour filtrer le trafic

Du point de vue de **R1**, le trafic auquel s'applique la liste de contrôle d'accès **HTTP_ONLY** est entrant depuis le réseau connecté à l'interface Gigabit Ethernet 0/1. Passez en mode de configuration d'interface et appliquez la liste de contrôle d'accès.

Remarque: Sur un réseau opérationnel réel, il n'est pas recommandé d'appliquer une liste d'accès non testée à une interface active. Il devrait être évité si possible.

- R1(config)# **interface gigabitEthernet 0/1**
- R1(config-if)# **ip access-group HTTP_ONLY in**

Etape 3: Vérifiez l'implémentation de la liste de contrôle d'accès

- Envoyez une requête ping de **PC2** au **Server**. Si les requêtes ping n'aboutissent pas, vérifiez les adresses IP avant de continuer.
- Depuis le PC2, ouvrez un navigateur web et entrez l'adresse IP du serveur. La page Web du serveur doit être affichée.
- Établissez une connexion FTP entre **PC2** et **Serveur**. La connexion devrait échouer. Si ce n'est pas le cas, résolvez les instructions de liste d'accès et les configurations de groupe d'accès sur les interfaces.

Activité 3 : Configurer les ACLs étendues - Scénario 1- Packet Tracer

Réponses

▪ ,,,

Configuration

R1 :

```
enable
configure terminal
access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
interface gigabitEthernet 0/0
  ip access-group 100 in
ip access-list extended HTTP_ONLY
  permit tcp 172.22.34.96 0.0.0.15
  permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
  permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
interface gigabitEthernet 0/1
ip access-group HTTP_ONLY in
```

Activité 4 : Configurer les listes de contrôle d'accès étendues - Scénario 2 Packet Tracer

- **Objectifs**

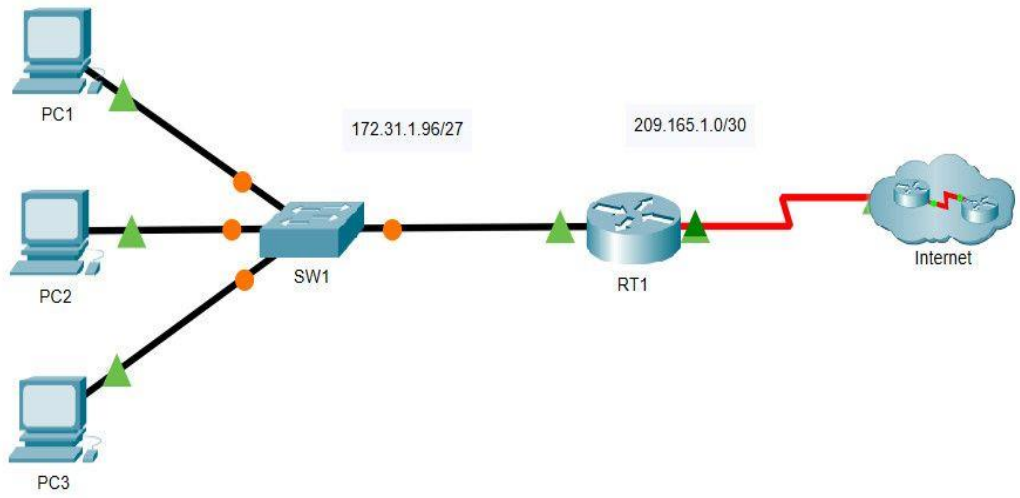
- **Partie 1: Configurer une liste de contrôle d'accès ACL étendue nommée**
- **Partie 2: Appliquer et vérifier la liste de contrôle d'accès ACL étendue**
- **Contexte**

Dans ce scénario, certains appareils du LAN sont autorisés à accéder à différents services sur des serveurs sur Internet.

- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
RT1	G0/0	172.31.1.126	255.255.255.224	N/A
RT1	S0/0/0	209.165.1.2	255.255.255.252	N/A
PC1	Carte réseau	172.31.1.101	255.255.255.224	172.31.1.126
PC2	Carte réseau	172.31.1.102	255.255.255.224	172.31.1.126
PC3	Carte réseau	172.31.1.103	255.255.255.224	172.31.1.126
Serveur 1	Carte réseau	64.101.255.254		
Serveur 2	Carte réseau	64.103.255.254		

- **Topologie :**



- **Instructions**

- **Partie 1: Configurer une liste de contrôle d'accès ACL étendue nommée**

Configurez une liste de contrôle d'accès nommée pour implémenter la stratégie suivante:

PARTIE 6

Activité 4 : Configurer les listes de contrôle d'accès étendues - Scénario 2 Packet Tracer

- Bloquer les accès HTTP et HTTPS de **PC1** au **Serveur 1** et **Serveur 2.** Les serveurs sont dans le cloud et vous êtes la seule personne qui connaît leur adresse IP.
- Bloquer l'accès FTP de **PC2** au **Serveur 1** et **Serveur 2**.
- Bloquez l'accès ICMP de **PC3** au **Serveur 1** et **Serveur 2**.

Remarque: À des fins d'évaluation, vous devez configurer les instructions dans l'ordre indiqué dans les étapes suivantes.

Etape 1: Refusez à PC1 l'accès aux services HTTP et HTTPS sur Serveur1 et Serveur2

a. Créez une liste de contrôle d'accès IP nommée qui empêchera **PC1** d'accéder aux services HTTP et HTTPS de **Serveur 1** et **Serveur 2**. Quatre instructions de contrôle d'accès sont requises.

Question:

- Quelle est la commande pour commencer la configuration d'une liste d'accès étendue avec le nom **ACL**?

Ouvrez la fenêtre de configuration.

b. Commencez la configuration d'ACL avec une déclaration qui refuse l'accès de **PC1** au **Serveur 1**, uniquement pour HTTP (port 80). Consultez le tableau d'adressage pour l'adresse IP de **PC1** et **Serveur 1**.

- RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.101.255.254 eq 80**

c. Ensuite, saisissez la déclaration qui refuse l'accès du **PC1** au **Serveur 1**, uniquement pour HTTPS (port 443).

- RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.101.255.254 eq 443**

d. Saisissez la déclaration qui refuse l'accès du **PC1** au **Serveur 2**, uniquement pour HTTP. Consultez la table d'adressage pour l'adresse IP de **Serveur 2.**

- RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.103.255.254 eq 80**

e. Saisissez la déclaration qui refuse l'accès du **PC1** au **Serveur 2**, uniquement pour HTTP.

- RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.103.255.254 eq 443**

Etape 2: Refusez à PC2 l'accès aux services FTP sur Serveur 1 et Serveur 2

Consultez la table d'adressage pour l'adresse IP de **PC2**.

a. Saisissez la déclaration qui refuse l'accès du **PC2** au **Serveur 1**, uniquement pour FTP (port 21 seulement).

- RT1(config-ext-nacl)# **deny tcp host 172.31.1.102 host 64.101.255.254 eq 21**

b. Saisissez la déclaration qui refuse l'accès du **PC2** au **Serveur 2**, uniquement pour FTP (port 21 seulement).

- RT1(config-ext-nacl)# **deny tcp host 172.31.1.102 host 64.103.255.254 eq 21**

Etape 3: Empêchez PC3 d'envoyer une requête ping à Serveur 1 et Serveur 2

Consultez la table d'adressage pour l'adresse IP de **PC3.**

Activité 4 : Configurer les listes de contrôle d'accès étendues - Scénario 2 Packet Tracer

a. Saisissiez la déclaration qui refuse l'accès ICMP de **PC3** vers **Serveur 1**.

- RT1(config-ext-nacl)# **deny icmp host 172.31.1.103 host 64.101.255.254**

b. Saisissiez la déclaration qui refuse l'accès ICMP de **PC3** vers **Serveur 2 .**

- RT1(config-ext-nacl)# **deny icmp host 172.31.1.103 host 64.103.255.254**

Etape 4: Autorisez tout autre trafic IP

Par défaut, une liste d'accès refuse tout trafic qui ne correspond à aucune règle de la liste. Saisissiez la commande qui autorise tout le trafic qui ne correspond à aucune des instructions de liste d'accès configurées.

Etape 5: Vérifiez la configuration de la liste d'accès avant de l'appliquer à une interface

Avant d'appliquer une liste d'accès, la configuration doit être vérifiée pour s'assurer qu'il n'y a pas d'erreurs typographiques et que les déclarations sont dans le bon ordre. Pour afficher la configuration actuelle de la liste d'accès, utilisez la commande **show access-lists** ou **show running-config** .

- RT1# **show access-lists**

```
Extended IP access list ACL
        10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
        20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
        30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
        40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
        50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
        60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
        70 deny icmp host 172.31.1.103 host 64.101.255.254
        80 deny icmp host 172.31.1.103 host 64.103.255.254
        90 permit ip any any
```

- RT1# **show running-config | begin access-list**

```
ip access-list extended ACL
        deny tcp host 172.31.1.101 host 64.101.255.254 eq www
        deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
        deny tcp host 172.31.1.101 host 64.103.255.254 eq www
        deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
        deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
        deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
        deny icmp host 172.31.1.103 host 64.101.255.254
        deny icmp host 172.31.1.103 host 64.103.255.254
        permit ip any any
```

Remarque: La différence entre la sortie de la commande **show access-lists** et la sortie de la commande **show running-config** est que la commande **show access-lists** inclut les numéros de séquence attribués à la commande instructions de configuration. Ces numéros de séquence permettent la modification, la suppression et l'insertion de lignes uniques dans la configuration de la liste d'accès. Les numéros de séquence définissent également l'ordre de traitement des instructions de contrôle d'accès individuelles, en commençant par le numéro de séquence le plus bas.

Activité 4 : Configurer les listes de contrôle d'accès étendues - Scénario 2 Packet Tracer

- **Partie 2: Appliquer et vérifier la liste de contrôle d'accès étendue**

Le trafic à filtrer provient du réseau 172.31.1.96/27 et est à destination des réseaux distants. L'emplacement approprié de la liste de contrôle d'accès dépend également de la relation du trafic par rapport à **RT1**. En général, les listes d'accès étendues doivent être placées sur l'interface la plus proche de la source du trafic.

Etape 1: Appliquez la liste de contrôle d'accès à l'interface appropriée dans la bonne direction

Remarque: Dans un réseau opérationnel réel, une ACL non testée ne doit jamais être appliquée à une interface active. Ce n'est pas une bonne pratique et peut perturber le fonctionnement du réseau.

Question:

- Sur quelle interface l'ACL nommée doit-elle être appliquée et dans quelle direction?

Ouvrez la fenêtre de configuration.

Passez en mode de configuration de commandes pour appliquer la liste de contrôle d'accès à l'interface.

Etape 2: Testez l'accès pour chaque PC

a. Accédez aux sites web de **Serveur 1** et **Serveur 2** en utilisant le navigateur web de **PC1.** Utilisez les protocoles HTTP et HTTPS. Utilisez la commande **show access-lists** pour afficher l'instruction liste d'accès autorisée ou refusée au trafic. La sortie de la commande **show access-lists** affiche le nombre de paquets correspondant à chaque instruction depuis la dernière fois que les compteurs ont été effacés ou que le routeur a redémarré.

Remarque: Pour effacer les compteurs d'une liste d'accès, utilisez la commande **clear access-list counters** .

- RT1#**show ip access-lists**

```
Extended IP access list ACL
10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (12 match(es))
20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))
30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
70 deny icmp host 172.31.1.103 host 64.101.255.254
80 deny icmp host 172.31.1.103 host 64.103.255.254
90 permit ip any any
```

b. Accédez aux services FTP de **Serveur 1** et **Serveur 2** en utilisant **PC1**. Le nom d'utilisateur et le mot de passe sont **cisco**.

c. Envoyez une requête ping à **Serveur 1** et **Serveur 2** depuis **PC1**.

d. Répétez les étapes 2a à 2c avec **PC2** et **PC3** pour vérifier le bon fonctionnement de la liste d'accès.

Activité 4 : Configurer les listes de contrôle d'accès étendues - Scénario 2 Packet Tracer

Réponses

- **Partie 1 / Etape 1 :**

a- ip access-list extended ACL

- **Partie 2/ Etape 1 :**

- Interface Gigabit Ethernet 0/0, in.

Configuration :

R1 :

```
enable
configure terminal
ip access-list extended ACL
  deny tcp host 172.31.1.101 host 64.101.255.254 eq www
  deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
  deny tcp host 172.31.1.101 host 64.103.255.254 eq www
  deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
  deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
  deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
  deny icmp host 172.31.1.103 host 64.101.255.254 deny
  icmp host 172.31.1.103 host 64.103.255.254
  permit ip any any
interface GigabitEthernet0/0
  ip access-group ACL in
end
```

TP 2

Sécuriser l’accès aux réseaux

1. Configuration des ACLs
2. Configuration de la NAT pour IPv4
3. Configuration de IPSec VPN

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer le service NAT?
- Réponses correctes pour au moins 70 % des questions.

Activité 1 : Étude du fonctionnement de la NAT Packet Tracer

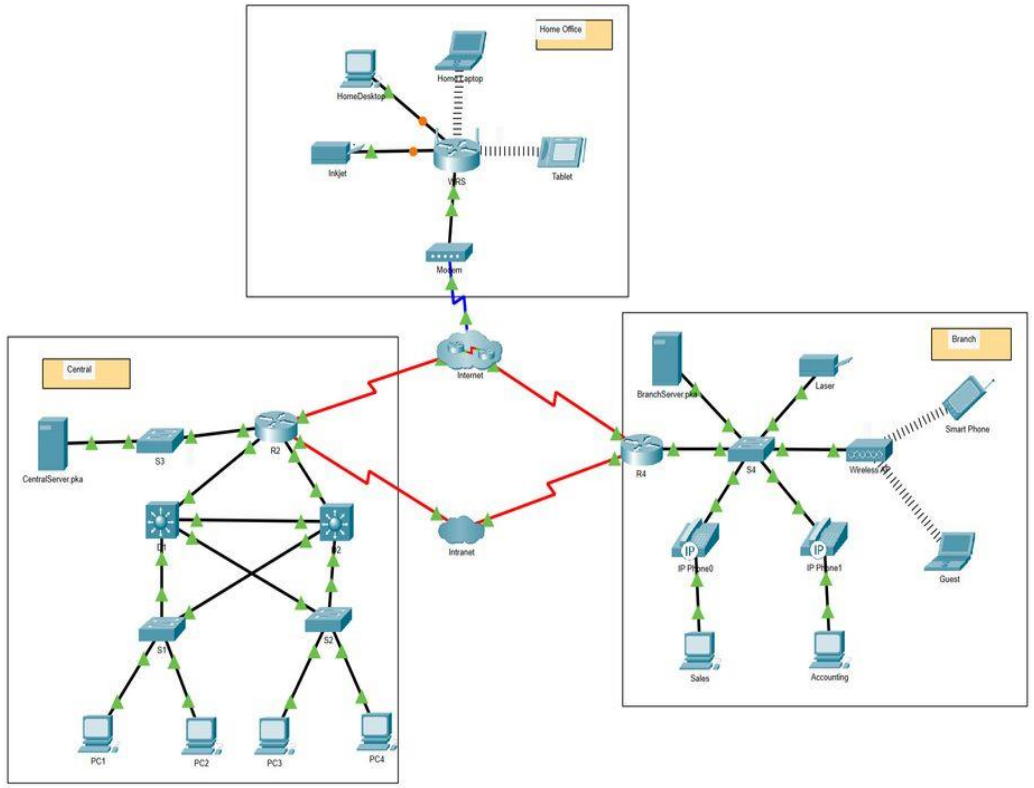
- **Objectifs**

- **Partie 1: Étude du fonctionnement de la NAT sur l'intranet**
- **Partie 2: Étude du fonctionnement de la NAT sur Internet**
- **Partie 3: Approfondissement de l'étude**

- **Scénario**

À mesure qu'une trame circule sur un réseau, les adresses MAC peuvent changer. Les adresses IP peuvent également changer lorsqu'un paquet est transféré via un périphérique configuré avec la fonction NAT. Dans cet exercice, nous étudierons ce qui arrive aux adresses IP pendant le processus NAT.

- **Topologie**



- **Table d'adressage**

Le tableau suivant fournit l'adressage pour les interfaces de périphériques réseau uniquement.

PARTIE 6

PARTIE 6

Activité 1 : Étude du fonctionnement de la NAT Packet Tracer

Appareil	Interface	Adresse IP / Préfixe
R2	G0/0	10.255.255.245/30
	G0/1	10.255.255.249/30
	G0/2	10.10.10.1/24
	S0/0/0	64.100.100.2/27
	S0/0/1.1	64.100.200.2/30
R4	G0/0	172.16.0.1/24
	S0/0/0	64.100.150.1/30
	S0/0/1.1	64.100.200.1/30
WRS	Réseau local (LAN)	192.168.0.1/24
	Internet	64.104.223.2/30

- **Instructions**
  - **Partie 1: Étude du fonctionnement de la NAT sur l'intranet**

Etape 1: Attendez que le réseau converge

La convergence des différents éléments du réseau peut prendre quelques minutes. Vous pouvez accélérer le processus en cliquant sur Fast Forward Time.

Etape 2: Générez une requête HTTP à partir de n'importe quel PC appartenant au domaine Central

a. Passez en mode **Simulation** et modifiez les filtres pour afficher uniquement les requêtes HTTP.

b. Ouvrez le navigateur Web d'un PC appartenant au domaine **Central** et tapez l'URL **http://branchserver.pka** puis cliquez **Go**. Réduisez la fenêtre du navigateur.

c. Cliquez sur **Capture / Forward** jusqu'à ce que la PDU soit sur **D1** ou **D2**. Cliquez sur la PDU la plus récente dans la liste des événements. Enregistrez les adresses IP source et de destination.

Question:

- À quels périphériques ces adresses appartiennent-elles?

d. Cliquez sur **Capture / Forward** jusqu'à ce que la PDU soit sur **R2**. Enregistrez les adresses IP source de destination dans le paquet sortant.

Question:

- À quels périphériques ces adresses appartiennent-elles?

e. Connectez-vous à R2 à partir de l'interface de ligne de commande en utilisant le mot de passe **classe** pour entrer EXEC privilégié et exécutez la commande suivante:

Ouvrez la fenêtre de configuration.

- R2# **show run | include pool**

```
ip nat pool R2Pool 64.100.100.3 64.100.100.31 netmask 255.255.255.224

ip nat inside source list 1 pool R2Pool
```

L'adresse provient du pool NAT **R2Pool**.

f. Cliquez sur **Capture / Forward** jusqu'à ce que la PDU soit sur **R4**. Enregistrez les adresses IP source de destination dans le paquet sortant.

Question:

- À quels périphériques ces adresses appartiennent-elles?

g. Cliquez sur **Capture / Forward** jusqu'à ce que la PDU soit sur **Branchserver.pka**. Enregistrez les adresses de port TCP source et de destination dans le segment sortant.

Activité 1 : Étude du fonctionnement de la NAT Packet Tracer

h. Sur les deux routeurs **R2** et **R4**, exécutez la commande suivante et associez les adresses IP et les ports enregistrés plus haut à la ligne de sortie correspondante:

- R2# **show ip nat translations**
- R4# **show ip nat translations**

Question:

- Quels sont les éléments communs aux adresses IP locales internes?
- Des adresses privées ont-elles croisé l'intranet?

Fermez la fenêtre de configuration.

i. Cliquez sur le bouton Réinitialiser la simulation et restez dans Modèle de simulation.

Partie 2: Étude du fonctionnement de la NAT sur Internet

Etape 1: Générez une requête HTTP à partir de n'importe quel PC appartenant à Home Office

a. Ouvrez le navigateur Web de n'importe quel PC du domaine **Home Office** , tapez l'URL **http://centralserver.pka** et cliquez sur **OK** .

b. Cliquez sur Capture/Forward jusqu'à ce que la PDU soit sur WRS. Enregistrez les adresses IP source et de destination entrantes et sortantes.

Question:

- À quels périphériques ces adresses appartiennent-elles?

c. Cliquez sur Capture / Forward jusqu'à ce que la PDU soit sur R2. Enregistrez les adresses IP source de destination dans le paquet sortant.

Question:

- À quels périphériques ces adresses appartiennent-elles?

d. Sur **R2**, exécutez la commande suivante et associez les adresses IP et les ports enregistrés plus haut à la ligne de sortie correspondante:

Ouvrez la fenêtre de configuration.

- R2# **show ip nat translations**

Fermez la fenêtre de configuration.

e. Passez en mode temps réel (Realtime).

Question:

- Les pages Web se sont-elles toutes affichées dans les navigateurs?

Partie 3 : Approfondissement de l'étude

Essayez avec plus de paquets, HTTP et HTTPS puis répondez aux questions suivantes:

Questions:

- Les tables de traduction NAT augmentent-elles?
- WRS dispose-t-il d'un pool d'adresses?
- Les ordinateurs de la salle de classe se connectent-ils à l'internet de cette manière?
- Pourquoi la NAT utilise-t-elle quatre colonnes d'adresses et de ports?
- Où sont les réseaux à l'intérieur global et local?
- Sur quels appareils les services NAT fonctionnent-ils? Qu'est-ce qu'ils ont en commun?

Activité 1 : Étude du fonctionnement de la NAT Packet Tracer

Réponses

Part 1 / Etape 1:

c) 10.X.X.X and 64.100.200.1 The PC and R4

d) 64.100.100.X et 64.100.200.1 La première adresse n'est pas affectée à une interface. R4 est la deuxième adresse

f) 64.100.100.X et 172.16.0.3. La première adresse provient de R2Pool sur R2. Branchserver.pka est la deuxième adresse.

g) source 80, destination 102x

h) - Ils sont réservés à un usage privé.

- Non

Part 2 / Etape 1:

b) Entrant : 192.168.0.X et 64.100.100.2. Sortant : 64.104.223.2 et 64.100.100.2. L'ordinateur et R2 ; WRS et R2.

c) 64.104.223.2 et 10.10.10.2, qui est WRS et centralserver.pka.

e) Oui.

Part 3

- Oui. Il y a des entrées supplémentaires lorsque de nouvelles conversations sont lancées.
- Non, il utilise la même adresse IP pour tous les appareils.
- Cela dépend de l'infrastructure du campus. Un moyen simple de vérifier consiste à utiliser quelque chose comme https://www.whatsmyip.org pour déterminer si toutes les machines de la classe utilisent la même adresse.
- Les colonnes répertorient les adresses globales internes, locales internes, locales externes et globales externes.
- Les adresses locales internes se trouvent sur les réseaux locaux de chaque domaine. Les adresses globales externes proviennent des liaisons WAN vers Internet et l'intranet.
- WRS, R2 et R4. Ils connectent tous des réseaux locaux internes à des réseaux extérieurs nécessitant des adresses IP routables.

PARTIE 6

Activité 2 : Configuration de la NAT statique Packet Tracer

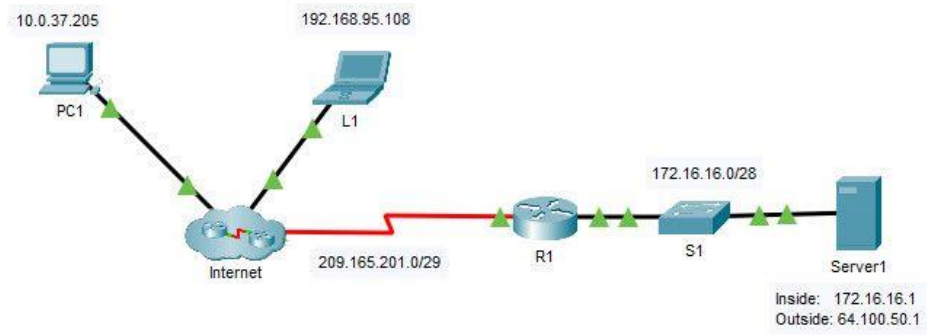
- **Objectifs**

- **Partie 1 : Test d'accès sans la NAT**
- **Partie 2 : Configuration de la NAT statique**
- **Partie 3 : Test d'accès avec la NAT**

- **Scénario**

Dans les réseaux configurés IPv4, les clients et les serveurs utilisent l'adressage privé. Avant que les paquets avec l'adressage privé puissent traverser l'internet, ils doivent être traduits en adressage public. En général, une adresse IP statique publique et privée est attribuée aux serveurs qui sont accessibles depuis l'extérieur de l'entreprise. Dans cet exercice, vous allez configurer la NAT statique pour que les périphériques externes puissent accéder au serveur interne sur son adresse publique.

- **Topologie**



- **Instructions**

  - **Partie 1: Test d'accès sans la NAT**

Etape 1: Essayez de vous connecter à Serveur1 en mode Simulation

a. Passage en mode de simulation.

b. Depuis **PC1** ou **L1**, utilisez le navigateur Web pour tenter de vous connecter à la page Web du **serveur 1** au 172.16.16.1. Continuez à cliquer sur le bouton **Capture Forward** , notez que les paquets ne quittent jamais le cloud Internet. Les tentatives doivent échouer.

c. Sortie du mode **Simulation**.

d. À partir de **PC1**, ping l'interface **R1**S0/0/0 (209.165.201.2). La requête ping doit réussir.

Etape 2: Affichez la table de routage de R1 et la configuration en cours

a. Affichez la configuration en cours sur **R1**. Notez qu'aucune commande ne fait référence à la NAT. Un moyen simple de confirmer cela est d'émettre la commande suivante:

Ouvrez la fenêtre de configuration.

- R1# **show run | include nat**

Activité 2 : Configuration de la NAT statique Packet Tracer

b. Vérifiez que la table de routage ne contient pas d'entrées faisant référence aux adresses de réseau IP pour **PC1** et **L1**.

c. Vérifiez que la fonction NAT n'est pas utilisée par **R1**.

- R1# **show ip nat translations**

Partie 2: Configuration de la NAT statique

Etape 1: Configurez les instructions de la NAT statique

a. Consultez la topologie. Créez une traduction NAT statique pour mapper l'adresse locale interne de **Server1** à son adresse externe.

- R1(config)# **ip nat inside source static 172.16.16.1 64.100.50.1**

tape 2: Configurez les interfaces.

a. Configurez l'interface **G0/0** en tant qu'interface interne.

- R1(config)# **interface g0/0**
- R1(config-if)# **ip nat inside**

b. Configurez l'interface publique s0/0/0 en tant qu'interface externe.

Partie 3: Tentative d'accès avec la NAT

Etape 1: Vérifiez la connectivité avec la page Web de Serveur1

a. Ouvrez l'invite de commande sur **PC1** ou **L1**, essayez d'envoyer une requête ping à l'adresse publique de **Server1**. Les requêtes ping doivent aboutir.

b. Vérifiez que **PC1** et **L1** peuvent désormais accéder à la page Web de **Server1**.

Etape 2: Affichez les traductions NAT

Utilisez les commandes suivantes pour vérifier la configuration statique du NAT sur **R1**:

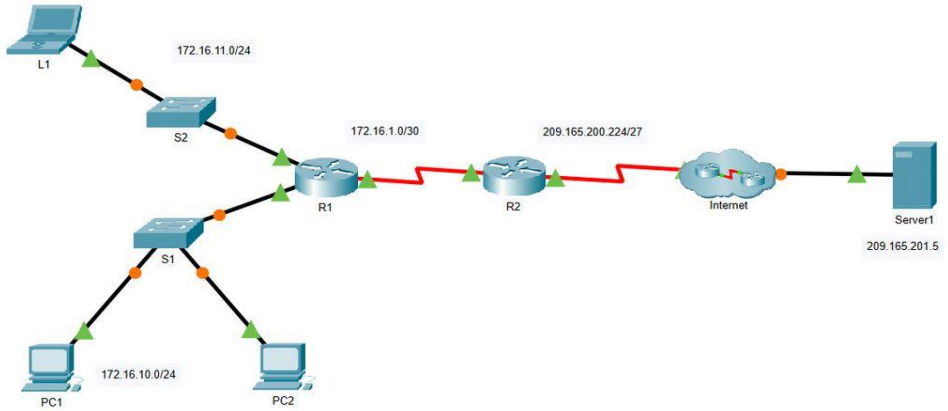
Ouvrez la fenêtre de configuration.

- **show running-config**
- **show ip nat translations**
- **show ip nat statistics**

PARTIE 6

Activité 3 : Configurer la NAT dynamique- Packet Tracer

- **Objectifs**
- **Partie 1: Configurer la NAT dynamique**
- **Partie 2: Vérifier l'implémentation de la NAT**
- **Topologie**



- **Instructions**

- **Partie 1: Configurer la NAT dynamique**

Etape 1: Configurer le trafic qui sera autorisé

Sur **R2**, configurer une instruction pour ACL 1 afin d'autoriser toutes les adresses appartenant à 172.16.0.0/16.

Etape 2: Configurez un pool d'adresses pour la NAT

a. Configurez **R2** avec un pool NAT qui utilise les deux adresses dans l'espace d'adresses 209.165.200.232/30.

b. Remarquez dans la topologie qu'il y a 3 adresses de réseau qui seront traduites sur la base de l'ACL créée.

Question:

- Que se passera-t-il si plus de deux appareils tentent d'accéder à l'internet ?

Etape 3: Associez ACL1 au pool NAT

Entrez la commande associant ACL 1 au pool NAT que vous venez de créer.

Etape 4: Configurez les interfaces NAT

Configurez les interfaces **R2** avec les commandes NAT internes et externes appropriées.

- **Partie 2: Vérifier l'implémentation de la NAT**

Etape 1: Accédez aux services sur l'internet

Dans le navigateur Web de **L1**, **PC1** ou **PC2**, accédez à la page Web de **Server1**.

Etape 2: Affichez les traductions NAT

Affichez les traductions NAT sur **R2**. Identifiez l'adresse source interne du PC et l'adresse traduite à partir du pool NAT dans la sortie de commande.

Ouvrez la fenêtre de configuration.

- R2# **show ip nat translations**

Activité 3 : Configurer la NAT dynamique- Packet Tracer

...

Réponses

Partie 1/ Etape 1:

- Les appareils supplémentaires se verraient refuser l'accès jusqu'à ce que l'une des traductions précédentes expire, libérant une adresse à utiliser.

Configuration :

R2 :

```
enable
configure terminal
access-list 1 permit 172.16.0.0 0.0.255.255
ip nat pool ANY_POOL_NAME 209.165.200.229
209.165.200.230 netmask 255.255.255.252
ip nat inside source list 1 pool ANY_POOL_NAME
interface s0/0/0
  ip nat outside
interface s0/0/1
  ip nat inside end
```

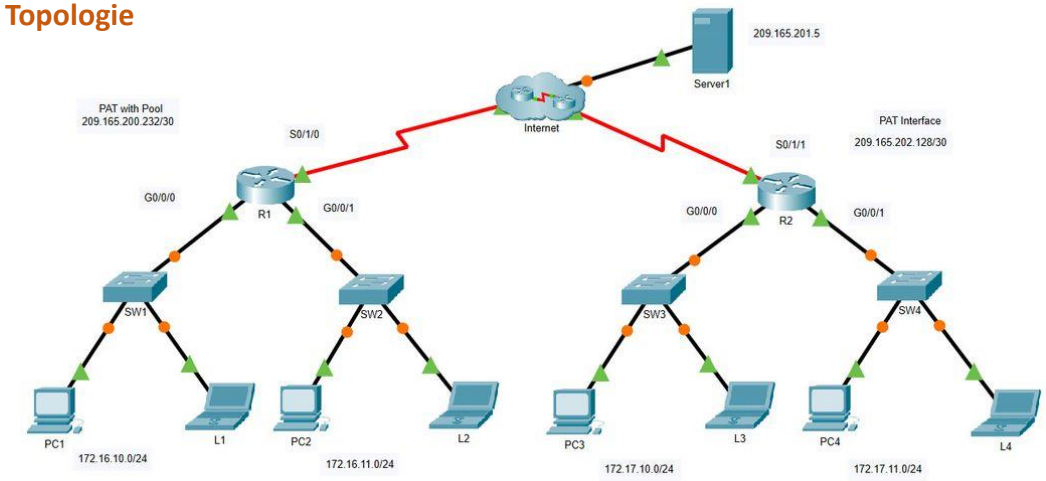
PARTIE 6

Activité 4 : Configurer la PAT- Packet Tracer

- **Objectifs**

- **Partie 1 : Configurer la NAT dynamique avec surcharge**
- **Partie 2 : Vérification de la NAT dynamique avec mise en œuvre de la surcharge**
- **Partie 3 : Configurer le PAT à l'aide d'une interface**
- **Partie 4 : Vérification de la mise en œuvre de l'interface PAT**

- **Topologie**



- **Instructions**

- **Partie 1: Configurer la NAT dynamique avec surcharge**

Etape 1: Configurez le trafic qui sera autorisé

Sur **R1**, configurez une déclaration pour ACL 1 afin d'autoriser toute adresse appartenant à 172.16.0.0/16.

- R1(config)# **access-list 1 permit 172.16.0.0 0.0.255.255**

Etape 2: Configurez un pool d'adresses pour la NAT

Configurez **R1** avec un pool NAT qui utilise les deux adresses utilisables dans l'espace d'adresses 209.165.200.232/30.

- R1(config)# **ip nat pool ANY_POOL_NAME 209.165.200.233 209.165.200.234 netmask 255.255.255.252**

Etape 3: Associez ACL 1 au pool NAT et autorisez la réutilisation des adresses

- R1(config)# **ip nat inside source list 1 pool ANY_POOL_NAMEoverload**

Etape 4: Configurez les interfaces NAT

Configurez les interfaces **R1** avec les commandes NAT internes et externes appropriées.

- R1(config)# **interface s0/1/0**
- R1(config-if)# **ip nat outside**
- R1(config-if)# **interface g0/0/0**
- R1(config-if)# **ip nat inside**
- R1 (config-if) # **interface g0/0/1**
- R1(config-if)# **ip nat inside**

Activité 4 : Configurer la PAT- Packet Tracer

Partie 2: Vérifier la NAT dynamique avec mise en œuvre de la surcharge

Etape 1: Accédez aux services sur l'internet

Depuis le navigateur Web de chacun des PC qui utilisent **R1** comme passerelle (**PC1, L1** , **PC2 et L2**), accédez à la page Web du **Server1** .

Question :

- Toutes les connexions ont-elles été fructueuses ?

Etape 2: Affichez les traductions NAT

Affichez les traductions NAT sur **R1**.

- R1# **show ip nat translations**

Notez que les quatre appareils ont été en mesure de communiquer, et qu'ils utilisent une seule adresse hors du pool. PAT continuera d'utiliser la même adresse jusqu'à épuisement des numéros de port à associer à la traduction. Une fois que cela se produit, l'adresse suivante dans le pool sera utilisée. Alors que la limite théorique serait de 65 536 puisque le champ numéro de port est un nombre de 16 bits, le périphérique serait probablement à court de mémoire avant que cette limite ne soit atteinte.

Partie 3: Configurer PAT à l'aide d'une interface

Etape 1: Configurez le trafic qui sera autorisé

Sur **R2**, configurez une déclaration pour ACL 2 afin d'autoriser toute adresse appartenant à 172.17.0.0/16.

Etape 2: Associez ACL 2 à l'interface NAT et autorisez la réutilisation des adresses

Entrez l'instruction NAT **R2** pour utiliser l'interface connectée à Internet et fournir des traductions pour tous les périphériques internes.

- R2(config)# **ip nat inside source list 2 interface s0/1/1 overload**

Etape 3: Configurez les interfaces NAT

Configurez les interfaces **R2** avec les commandes NAT internes et externes appropriées.

Partie 4: Vérifier l'implémentation de l'interface PAT

Etape 1: Accédez aux services sur l'internet

Depuis le navigateur Web de chacun des PC qui utilisent **R2** comme passerelle (**PC3, L3** , **PC4 et L4**), accédez à la page Web du **Server1** .

Question :

- Toutes les connexions ont-elles été fructueuses ?

Etape 2: Affichez les traductions NAT

fenêtre de configuration.

Affichez les traductions NAT sur **R2**.

Etape 3: Comparez les statistiques NAT sur R1 et R2

Comparez les statistiques NAT sur les deux périphériques.

Question :

- Pourquoi **R2** ne liste-t-il pas les mappages dynamiques ?

Activité 4 : Configurer la PAT- Packet Tracer

Réponses

- **Partie 2 / Etape 1:**

- Oui

- **Partie 4 / Etape 1 :**

- Oui

- **Partie 4 / Etape 2 :**

- R1 répertorie les mappages dynamiques pour le pool d'adresses qui a été configuré. R2 utilise uniquement l'interface externe comme adresse pour traduire les adresses internes afin qu'il n'y ait pas de mappage dynamique.

Configuration :

R1:

```
enable
configure terminal
interface GigabitEthernet0/0/0
  ip nat inside
interface GigabitEthernet0/0/1
  ip nat inside
interface Serial0/1/0
  ip nat outside
ip nat pool DYNAMIC 209.165.200.233 209.165.200.234 netmask 255.255.255.252
ip nat inside source list 1 pool DYNAMIC overload
access-list 1 permit 172.16.0.0 0.0.255.255
end
```

R2 :

```
enable
configure terminal
interface GigabitEthernet0/0/0
  ip nat inside interface
GigabitEthernet0/0/1
  ip nat inside
interface Serial0/1/1
  ip nat outside
ip nat inside source list 2 interface Serial0/1/1 overload
access-list 2 permit 172.17.0.0 0.0.255.255
end
```

TP 2

Sécuriser l’accès aux réseaux

1. Configuration des ACLs
2. Configuration de la NAT pour IPv4
3. Configuration de IPSec VPN

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer le service NAT?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 6

Activité 1 : Configurer et vérifier un VPN IPsec de site à site Packet Tracer

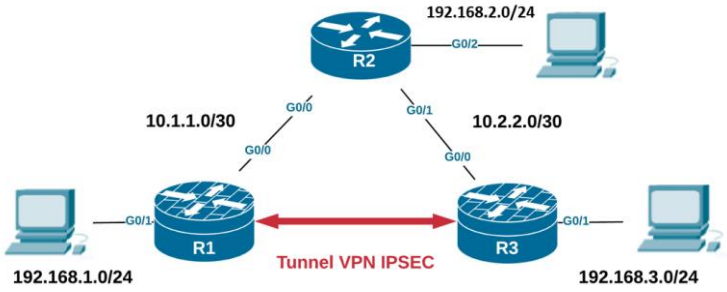
- **Objectifs**

- **Partie 1: Vérifiez la connectivité sur l'ensemble du réseau.**
- **Partie 2: Configurez R1 pour prendre en charge un VPN IPsec de site à site avec R3.**

- **Scénario**

La topologie du réseau montre trois routeurs. Votre tâche consiste à configurer R1 et R3 pour prendre en charge un VPN IPsec de site à site lorsque le trafic circule entre leurs réseaux locaux respectifs. Le tunnel VPN IPsec va de R1 à R3 via R2. R2 agit comme un intermédiaire et n'a aucune connaissance du VPN. IPsec assure la transmission sécurisée d'informations sensibles sur des réseaux non protégés, tels qu'Internet. IPsec fonctionne au niveau de la couche réseau et protège et authentifie les paquets IP entre les périphériques IPsec participants (homologues), tels que les routeurs Cisco.

- **Topologie**



- **Table d'adressage**

Le tableau suivant fournit l'adressage pour les interfaces de périphériques réseau uniquement.

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252		N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252		N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252		N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252		N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

- **Paramètres de la stratégie ISAKMP Phase 1**

Parameters	Parameter Options and Defaults	R1	R3
Key Distribution Method	Manual or **ISAKMP**	**ISAKMP**	**ISAKMP**
Encryption Algorithm	**DES**, 3DES, or AES	AES 256	AES 256
Hash Algorithm	MD5 or **SHA-1**	**SHA-1**	**SHA-1**
Authentication Method	Pre-shared keys or **RSA**	pre-share	pre-share
Key Exchange	DH Group 1, 2, or 5	DH 5	DH 5
IKE SA Lifetime	86400 seconds or less	**86400**	**86400**
ISAKMP Key	Provided by user.	vpnpa55	vpnpa55

Remarque : Les paramètres en gras sont les valeurs par défaut. Seuls les paramètres non gras doivent être explicitement configurés.

Activité 1 : Configurer et vérifier un VPN IPsec de site à site Packet Tracer

- **Paramètres de stratégie IPsec Phase 2**

Parameters	R1	R3
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	10.2.2.2	10.1.1.2
Traffic to be Encrypted	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Les routeurs ont été préconfigurés avec les éléments suivants :

Mot de passe pour la ligne de console : **ciscoconpa55**

Mot de passe pour les lignes vty : **ciscovtypa55**

Activer le mot de passe : **ciscoenpa55**

Nom d'utilisateur et mot de passe SSH : **SSHadmin / ciscosshpa55 OSPF 101**

- **Partie 1 :Configurer les paramètres IPsec sur R1**

Etape 1 : Tester la connectivité.

Ping de PC-A à PC-C.

Étape 2 : Activez le package de technologie de sécurité.

a. Activez le package de technologie de sécurité à l'aide de la commande suivante pour activer le package.

R1(config)# **license boot module c1900 technology-package securityk9**

b. Acceptez le contrat de licence utilisateur final.

c. Enregistrez la configuration en cours et rechargez le routeur pour activer la licence de sécurité.

d. Vérifiez que le package Security Technology a été activé à l'aide de la commande **show version**.

Étape 3 : Identifiez le trafic intéressant sur R1.

Configurez l'ACL 110 pour identifier le trafic du LAN sur R1 vers le LAN sur R3 comme intéressant. Ce trafic intéressant déclenchera la mise en œuvre du VPN IPsec lorsqu'il y a du trafic entre les LAN R1 à R3. Tout autre trafic provenant des réseaux locaux ne sera pas chiffré. En raison de l'implicite **deny all**, il n'est pas nécessaire de configurer une instruction **deny ip any any**.

R1(config)# **access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**

Étape 4 : configurez la stratégie ISAKMP IKE Phase 1 sur R1.

Configurez les propriétés de la stratégie **crypto ISAKMP 10** sur R1 avec la clé de chiffrement partagée **vpnpa55**. Reportez-vous au tableau ISAKMP Phase 1 pour les paramètres spécifiques à configurer. Les valeurs par défaut ne doivent pas être configurées. Par conséquent, seules la méthode de chiffrement, la méthode d'échange de clés et la méthode DH doivent être configurées.

Activité 1 : Configurer et vérifier un VPN IPsec de site à site Packet Tracer

Remarque : le groupe DH le plus élevé actuellement pris en charge par Packet Tracer est le groupe 5. Dans un réseau de production, vous devez configurer au moins DH 14.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

Étape 5 : configurez la stratégie IPsec IKE Phase 2 sur R1.

a. Créez le transform-set VPN-SET pour utiliser **esp-aes** et **esp-sha-hmac**.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

b. Créez la Crypto map VPN-MAP qui lie tous les paramètres de la phase 2 ensemble. Utilisez le numéro de séquence 10 et identifiez-le comme une map ipsec-isakmp.

```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Étape 6 : Configurez la carte de chiffrement sur l'interface sortante.

Liez la crypto map **VPN-MAP** à l'interface série 0/0/0 sortante.

```
R1(config)# interface s0/0/0
R1(config-if)# crypto map VPN-MAP
```

- **Partie 2 : Configurer les paramètres IPsec sur R3**

Étape 1 : activez le package de technologie de sécurité.

a. Sur R3, émettez la commande **show version** pour vérifier que les informations de licence du package Security Technology ont été activées.

b. Si le package de technologie de sécurité n'a pas été activé, activez le package et rechargez R3.

PARTIE 6

Activité 1 : Configurer et vérifier un VPN IPsec de site à site Packet Tracer

Étape 2 : configurez le routeur R3 pour prendre en charge un VPN de site à site avec R1.

Configurez les paramètres alternatifs sur R3. Configurez l'ACL 110 pour identifier le trafic du LAN sur R3 vers le LAN sur R1 comme intéressant.

R3(config)# **access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255**

Étape 3 : Configurez les propriétés ISAKMP IKE Phase 1 sur R3.

Configurez les propriétés de la stratégie crypto ISAKMP 10 sur R3 avec la clé de chiffrement partagée vpnpa55.

R3(config)# **crypto isakmp policy 10**

R3(config-isakmp)# **encryption aes 256**

R3(config-isakmp)# **authentication pre-share**

R3(config-isakmp)# **group 5**

R3(config-isakmp)# **exit**

R3(config)# **crypto isakmp key vpnpa55 address 10.1.1.2**

Étape 4 : configurez la stratégie IPsec IKE Phase 2 sur R3.

a. Créez le transform-set VPN-SET pour utiliser **esp-aes** et **esp-sha-hmac**.

R3(config)# **crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**

b. Créez la transform-set VPN-MAP pour lier tous les paramètres de la phase 2 ensemble. Utilisez le numéro de séquence 10 et identifiez-le comme une map ipsec-isakmp.

R3(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R3(config-crypto-map)# **description VPN connection to R1**

R3(config-crypto-map)# **set peer 10.1.1.2**

R3(config-crypto-map)# **set transform-set VPN-SET**

R3(config-crypto-map)# **match address 110**

R3(config-crypto-map)# **exit**

Étape 5 :Configurez la carte de chiffrement sur l'interface sortante.

Liez la crypto map VPN-MAP à l'interface série 0/0/1 sortante.

R3(config)# **interface s0/0/1**

R3(config-if)# **crypto map VPN-MAP**

- **Partie 3 :Vérifier le VPN IPsec**

Étape 1 :Vérifiez le tunnel avant tout trafic intéressant.

Exécutez la commande show crypto ipsec sa sur R1. Notez que le nombre de paquets encapsulés, chiffrés, désencapsulés et déchiffrés est tous défini sur 0.

PARTIE 6

Activité 1 : Configurer et vérifier un VPN IPsec de site à site Packet Tracer

Étape 2 : Créer un trafic intéressant.

Envoyez une requête ping à PC-C depuis PC-A.

Étape 3 : Vérifiez le tunnel après un trafic intéressant.

Sur R1, relancez la commande **show crypto ipsec sa**. Notez que le nombre de paquets est supérieur à 0, ce qui indique que le tunnel VPN IPsec fonctionne.

Étape 4 :Créez un trafic inintéressant.

Envoyez une requête ping à PC-B à partir de PC-A.

Remarque : L'émission d'un ping du routeur R1 vers PC-C ou R3 vers PC-A n'est pas un trafic intéressant.

Étape 5 :Vérifiez le tunnel.

Sur R1, relancez la commande **show crypto ipsec sa**. Notez que le nombre de paquets n'a pas changé, ce qui vérifie que le trafic inintéressant n'est pas chiffré.

Activité 1 : Configurer et vérifier un VPN IPsec de site à site Packet Tracer

Réponses

Configuration :

Routeur R1

```
enable
config t
license boot module c1900 technology-package securityk9
yes
end
copy running-config startup-config
reload
config t
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key vpnpa55 address 10.2.2.2
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to R3
set peer 10.2.2.2
set transform-set VPN-SET
match address 110
exit
interface S0/0/0
crypto map VPN-MAP
```

Routeur R3

```
enable
config t
access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key vpnpa55 address 10.1.1.2
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to R1
set peer 10.1.1.2
set transform-set VPN-SET
match address 110
exit
interface S0/0/1
crypto map VPN-MAP
```

TP 3

Mettre en place un système de gestion et de supervision des réseaux

Compétences visées :

- Adopter des techniques d'Optimisation, surveillance et dépannage des réseaux informatiques

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

7 heures

TP 3

Mettre en place un système de gestion et de supervision des réseaux

1. Gestion réseau : CDP, LLDP, NTP
2. Supervision réseau
3. Dépannage réseau (Network Troubleshooting)

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer les protocoles CDP, LLDP. Et NTP?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 6

Activité 1 : Utiliser le CDP pour cartographier un réseau- Packet Tracer

- **Objectifs**

- **Mappez un réseau en utilisant le protocole CDP et l'accès SSH à distance.**

- **Contexte/scénario**

Un administrateur réseau principal vous demande de mapper le réseau distant d'une filiale et de déterminer le nom d'un commutateur récemment installé nécessitant une adresse IP pour être configuré. Votre tâche consiste à créer une carte du réseau de bureaux de la succursale. Vous devez enregistrer tous les noms de périphériques réseau, toutes les adresses IP, tous les masques de sous-réseau et toutes les interfaces physiques interconnectées avec les périphériques réseau, ainsi que le nom du commutateur qui ne possède pas d'adresse IP.

Pour mapper le réseau, vous devrez utiliser SSH pour l'accès à distance et le protocole CDP (Cisco Discovery Protocol) pour rechercher des informations sur les périphériques réseau voisins, comme des routeurs et des commutateurs. Du fait que le protocole CDP est un protocole de couche 2, il peut être utilisé pour découvrir des informations concernant les périphériques ne possédant aucune adresse IP. Vous allez enregistrer les informations collectées pour compléter la table d'adressage et fournir une base de données topologique du réseau distant de la filiale.

Les noms d'utilisateur et les mots de passe administratifs locaux et à distance sont :

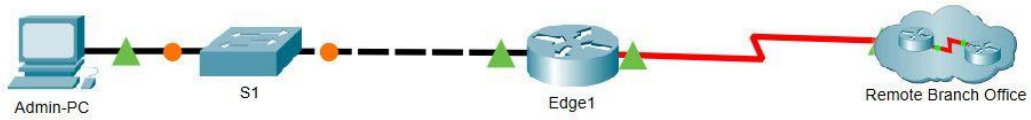
Réseau local

- Nom d'utilisateur : **admin01**
- Mot de passe : **S3cre7P@55**

Réseau de la filiale

- Nom d'utilisateur : **branchadmin**
- Mot de passe : **S3cre7P@55**

- **Topologie**



- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau	Interface locale et voisin connecté
Edge1	G0/0	192.168.1.1	255.255.255.0	G0/1 - S1
	S0/0/0			S0/0/0 - ISP
	S0/0/1	209.165.200.10		S0/0/1 - ISP

- **Instructions**

Etape 1: Utiliser le protocole SSH pour accéder à distance aux périphériques réseau

Activité 1 : Utiliser le CDP pour cartographier un réseau- Packet Tracer

Dans la partie 1, vous utiliserez Admin-PC pour accéder à distance au routeur de passerelle Edge1. Ensuite, à partir du routeur Edge1, vous accèderez à la filiale distante par SSH.

a. Ouvrez une invite de commande sur Admin-PC.

b. Accédez par SSH au routeur de passerelle à l'adresse 192.168.1.1 en utilisant le nom d'utilisateur **admin01** et le mot de passe **S3cre7P@55**.

- PC> **ssh –l admin01 192.168.1.1**

```
Open
Password:
```

- `Edge1#`

Remarque: notez que vous êtes directement mis en mode d'exécution privilégié. Cela est dû au fait que le compte utilisateur admin01 est défini sur le niveau de privilège 15.

c. Utilisez les commandes **show ip interface brief** et **show interfaces** pour documenter les interfaces physiques, les adresses IP et les masques de sous-réseau du routeur Edge1 dans la table d'adressage.

d. Depuis Edge1, utilisez SSH pour accéder à la succursale distante au 209.165.200.10 avec le nom d'utilisateur **branchadmin** et le même mot de passe que ci-dessus :

- Edge1# **ssh –l branchadmin 209.165.200.10**

```
Open
Password:
```

- `Branch-Edge#`

Une fois connecté à la filiale distante à l'adresse 209.165.200.10, quelle information précédemment manquante peut désormais être ajoutée à la table d'adressage ci-dessus ?

Partie 2: Utiliser le protocole CDP pour détecter les périphériques voisins

Vous êtes maintenant connecté à distance au routeur Branch-Edge. En utilisant le protocole CDP, commencez à chercher des périphériques réseau connectés.

a. Lancez les commandes **show ip interface brief** et **show interfaces** pour documenter les interfaces réseau, les adresses IP et les masques de sous-réseau du routeur Branch-Edge. Ajoutez les informations manquantes à la table d'adressage afin de mapper le réseau :

- Branch-Edge# **show ip interface brief**
- Branch-Edge# **show interfaces**

b. Les meilleures pratiques en matière de sécurité ne recommandent l'utilisation du protocole CDP qu'en cas de besoin, il faudrait donc peut-être l'activer. Utilisez une commande **show cdp** pour vérifier son statut.

- Branch-Edge# **show cdp**

```
% CDP is not enabled
```

c. Vous devez activer le protocole CDP, mais il est judicieux de diffuser les informations du CDP uniquement vers les périphériques réseau internes et non vers les réseaux externes. Pour ce faire, activez le protocole CDP, puis désactivez le CDP sur l'interface S0/0/1.

Activité 1 : Utiliser le CDP pour cartographier un réseau- Packet Tracer

- Branch-Edge# **configure terminal**
- Branch-Edge(config)# **cdp run**
- Branch-Edge(config)# **interface s0/0/1**
- Branch-Edge(config-if)# **no cdp enable**
- Branch-Edge(config-if)# **exit**

d. Lancez une commande **show cdp neighbors** pour détecter les périphériques réseau voisins.

Remarque: le CDP n'affichera que les appareils Cisco connectés qui exécutent également le CDP.

- Branch-Edge# **show cdp neighbors**

Un périphérique réseau voisin a-t-il été détecté ? De quel type de périphérique s'agit-il ? Quel est son nom ? Sur quelle interface est-il connecté ? L'adresse IP du périphérique est-elle listée ? Enregistrez les informations dans la table d'adressage.

Remarque: La réception des mises à jour CDP peut prendre un certain temps. Si vous ne voyez aucune sortie de la commande, appuyez plusieurs fois sur le bouton Temps d'avance rapide.

e. Pour obtenir l'adresse IP du périphérique voisin, utilisez la commande **show cdp neighbors detail** et enregistrez l'adresse IP :

- Branch-Edge# **show cdp neighbors detail**

Question :

- Outre l'adresse IP du périphérique voisin, quelle information potentiellement sensible est indiquée ?

f. Maintenant que vous connaissez l'adresse IP de l'appareil voisin, connectez-vous à celui-ci avec SSH afin de découvrir d'autres appareils qui pourraient être ses voisins.

Remarque: Pour établir une connexion SSH, utilisez les mêmes nom d'utilisateur et mot de passe de filiale distante.

- Branch-Edge# **ssh –l branchadmin** *<the ip address of the neighbor device>*

Question :

- Après avoir établi une connexion SSH, quelles sont les informations affichées par l'invite de commande ?

g. Vous êtes connecté à distance au voisin suivant. Utilisez la commande **show cdp neighbors** et la commande **show cdp neighbors detail** pour détecter d'autres périphériques voisins connectés.

Question :

- Quels types de périphériques réseau avoisinent ce périphérique ? Enregistrez tous les périphériques détectés dans la table d'adressage. Incluez leurs noms d'hôte, leurs interfaces et leurs adresses IP.

h. Poursuivez la détection de nouveaux périphériques réseau en utilisant le protocole SSH et les commandes show CDP. Vous finirez par atteindre les limites du réseau et il n'y aura plus de périphériques à détecter.

Question :

- Quel est le nom du commutateur qui ne dispose pas d'adresse IP sur le réseau ?

i. Dessinez une topologie du réseau distant de la filiale en utilisant les informations que vous avez rassemblées en utilisant le protocole CDP.

Activité 1 : Utiliser le CDP pour cartographier un réseau- Packet Tracer

Réponses

,,,

- **Partie 1 :**

c) - Le nom d'hôte du routeur Branch-Edge

- **Partie 2 :**

d) - C'est un routeur. Son nom est Branch-Firewall et il est connecté sur l'interface G0/0. L'adresse IP de l'appareil n'est pas répertoriée.

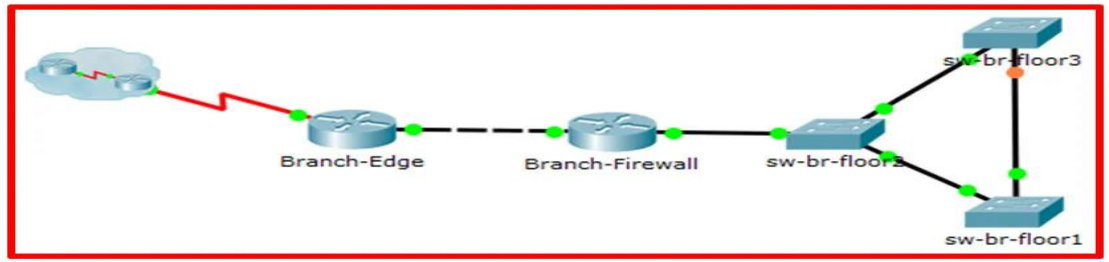
e) - La version du logiciel IOS de l'appareil voisin. Il peut s'agir d'une faille de sécurité potentielle si elle est connue d'un acteur malveillant.

f) - Branch-Firewall#

g) - Un routeur (Branch-Edge) et un switch (sw-br-floor2). Le commutateur sw-br-floor2 est un périphérique nouvellement découvert situé à 192.168.4.132 sur l'interface G0/1.

h) - sw-br-floor1

i) - Remarque : les réponses varieront. Toutes les réponses doivent montrer les mêmes connexions physiques entre les appareils.



PARTIE 6

Activité 2 : Utiliser LLDP pour mapper un réseau- Packet Tracer

Objectifs

Cartographier un réseau en utilisant l'accès à distance LLDP et SSH.

Contexte/scénario

Un administrateur réseau principal vous demande de mapper le réseau des succursales distantes et de découvrir des informations sur tous les périphériques du réseau. Vous devez enregistrer tous les noms de périphériques réseau, les adresses IP et les masques de sous-réseau, ainsi que les interfaces physiques qui interconnectent les périphériques réseau.

Pour cartographier le réseau, vous utiliserez SSH pour l'accès à distance et le Link Layer Discovery Protocol (LLDP) pour découvrir des informations sur les périphériques réseau voisins. Comme le LLDP est un protocole de couche 2, il peut être utilisé pour découvrir des informations sur des appareils qui n'ont pas de connectivité de couche 3. Vous noterez les informations que vous recueillez pour remplir le tableau d'adressage et fournir un diagramme de la topologie du réseau de bureaux distants.

Vous aurez besoin de l'adresse IP de la filiale distante. Cette adresse est 209.165.200.10. Les noms d'utilisateur et les mots de passe administratifs locaux et à distance sont :

Réseau local

- Nom d'utilisateur : **admin01**
- Mot de passe : **S3cre7P@55**

Réseau de bureaux distants

Nom d'utilisateur : **RBOadmin**

Topologie

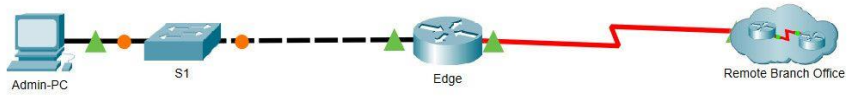


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Interface locale et voisin connecté
Points d'accès	G0/0	192.168.1.1	255.255.255.0	
	S0/0/0			S0/0/0 - ISP
	SVI	192.168.1.2		blank
	G0/0	209.165.200.10		G0/0 - ISP

Instructions

Partie 1: Utiliser le protocole SSH pour accéder à distance aux périphériques réseau

Dans la partie 1, vous utiliserez l'Admin-PC pour accéder à distance au routeur de la passerelle Edge. Ensuite, à partir du routeur Edge, vous ferez du SSH dans le bureau RBO distant.

a. Ouvrez une invite de commande sur Admin-PC.

b. Accédez par SSH au routeur de passerelle à l'adresse 192.168.1.1 en utilisant le nom d'utilisateur **admin01** et le mot de passe **S3cre7P@55**.

- PC> **ssh –l admin01 192.168.1.1**

```
Open

Password:
```

- Edge#

PARTIE 6

Activité 2 : Utiliser LLDP pour mapper un réseau- Packet Tracer

Remarque: notez que vous êtes directement mis en mode d'exécution privilégié. Cela est dû au fait que le compte utilisateur admin01 est défini sur le niveau de privilège 15.

c. Le routeur **Edge** était précédemment configuré pour utiliser CDP. Le commutateur **S1** a déjà été configuré pour utiliser LLDP. Émettez la commande **show cdp** pour vérifier que CDP est actuellement actif. Désactivez CDP en exécutant la commande suivante :

- Edge(config)# **no cdp run**

d. **LLDP** peut être configuré pour transmettre et recevoir sur une interface spécifique. Configurez **Edge** de sorte qu'il reçoive des messages LLDP de **S1** mais n'envoie pas de messages à **S1** pour des raisons de sécurité Activer **LLDP**.

- Edge(config)# **lldp run**
- Edge(config)# **int g0/0**
- Edge(config-if)# **no lldp transmit**
- Edge(config-if)# **exit**

e. Utilisez la commande **show lldp neighbors** pour vérifier que **Edge** reçoit des messages de **S1** .

f. Connectez-vous à **S1** avec SSH à partir du routeur **Edge** à l'aide des informations d'identification **admin01** . Lancez la commande **show lldp neighbors**. Notez que **S1** n'a pas reçu d'informations d' **Edge** .

- Edge# **ssh –l admin01 192.168.1.2**

  `Password:`
- S1> **show lldp neighbors**
- S1> **exit**

g. Quittez de la connexion avec S1 pour revenir à l'interface de ligne de commande du routeur Edge. Utilisez les commandes **show ip interface brief** et **show interfaces** pour documenter les interfaces physiques, les adresses IP et les masques de sous-réseau du routeur Edge1 dans la table d'adressage.

- Edge# **show ip interface brief**
- Edge# **show interfaces**

h. À partir de votre session avec le routeur Edge, connectez-vous avec SSH au Bureau RBO distant à 209.165.200.10 avec le nom d'utilisateur **RBOAdmin** et le même mot de passe utilisé pour admin01.

- Edge# **ssh –l RBOadmin 209.165.200.10**

  `Password:`
- RBO-Edge#

Après s'être connecté au bureau RBO distant au 209.165.200.10, quelle information précédemment manquante peut maintenant être ajoutée au tableau d'adressage ci-dessus ?

○ Partie 2: Utiliser LLDP pour découvrir les périphériques voisins

Vous êtes maintenant connecté à distance au routeur RBO-Edge. En utilisant LLDP, commencez à chercher des périphériques réseau connectés.

a. Lancez les commandes **show ip interface brief** et **show interfaces** pour documenter les interfaces réseau, les adresses IP et les masques de sous-réseau du routeur RBO-Edge. Ajoutez les informations manquantes à la table d'adressage afin de mapper le réseau :

PARTIE 6

Activité 2 : Utiliser LLDP pour mapper un réseau- Packet Tracer

b. Les meilleures pratiques en matière de sécurité recommandent de n'exécuter le LLDP qu'en cas de besoin, de sorte qu'il peut être nécessaire de l'activer. Utilisez une commande **show lldp** pour vérifier son statut.

- RBO-Edge# **show lldp**

```
% LLDP is not enabled
```

c. Vous devez activer le LLDP, mais c'est une bonne idée de n'envoyer les informations du LLDP qu'aux appareils du réseau interne et non aux réseaux externes. Découvrez quelle interface est connectée à Internet en émettant la commande **show ip interface brief**. Activez le protocole LLDP et désactivez complètement LLDP sur l'interface connectée à Internet.

- RBO-Edge# **configure terminal**
- RBO-Edge(config)# **lldp run**
- RBO-Edge(config)# **interface g0/0**
- RBO-Edge(config-if)# **no lldp transmit**
- RBO-Edge(config-if)# **no lldp receive**
- RBO-Edge(config-if)# **exit**

d. Lancez une commande **show cdp neighbors** pour détecter les périphériques réseau voisins.

Remarque : LLDP affichera uniquement les périphériques connectés qui exécutent également LLDP.

- RBO-Edge# **show lldp neighbors**

Question :

- Un périphérique réseau voisin a-t-il été détecté ? De quel type de périphérique s'agit-il ? Quel est son nom ? Sur quelle interface est-il connecté ? L'adresse IP du périphérique est-elle listée ? Enregistrez les informations dans la table d'adressage.

e. Utilisez la commande **show ip route** pour déterminer l'adresse du périphérique que vous avez trouvé avec la commande **show lldp neighbors** . En fonction des informations fournies sur l'adresse locale dans la table de routage et la longueur du préfixe du réseau, utilisez ces informations pour déterminer l'adresse du voisin.

f. Pour trouver des informations supplémentaires sur le périphérique voisin, utilisez la commande **show lldp neighbors detail** :

- RBO-Edge# **show lldp neighbors detail**

Question :

- Quels autres éléments d'information potentiellement sensibles sont répertoriés ?

Remarque : La version actuelle de Packet Tracer ne fournit pas l'adresse de gestion du périphérique voisin. Dans cette activité, plusieurs adresses de périphériques voisins ont été fournies dans le tableau d'adressage.

g. Connectez-vous au périphérique voisin avec SSH pour découvrir d'autres périphériques qui peuvent être ses voisins.

Remarque : Pour vous connecter à SSH, utilisez le même nom d'utilisateur et le même mot de passe que ceux du Remote RBO Office.

- RBO-Edge# **ssh –l RBOadmin** *<the ip address of the neighbor device>*

Activité 2 : Utiliser LLDP pour mapper un réseau- Packet Tracer

Question :

- Après avoir établi une connexion SSH, quelles sont les informations affichées par l'invite de commande ?

h. Vous êtes connecté à distance au voisin suivant. Utilisez la commande **show lldp neighbors** et la commande **show lldp neighbors detail** pour détecter d'autres périphériques voisins connectés.

Question :

- Quels types de périphériques réseau avoisinent ce périphérique ? Enregistrez tous les périphériques détectés dans la table d'adressage. Incluez leurs noms d'hôte, leurs interfaces et leurs adresses IP.

Ajoutez le nom de périphérique récemment découvert à côté de l'entrée SVI pour l'adresse 192.168.4.131.

i. Connectez-vous au SVI pour l'adresse 192.168.4.131 en utilisant SSH et les informations d'identification utilisées précédemment. Si vous êtes invité à entrer un mot de passe secret d'activation, utilisez le même mot de passe que celui utilisé pour **RboAdmin**. Utilisez la commande **show lldp neighbors** et la commande **show lldp neighbors detail** pour détecter d'autres périphériques voisins connectés.

Question :

- Quels types de périphériques réseau avoisinent ce périphérique ? Enregistrez tous les périphériques détectés dans la table d'adressage. Incluez leurs noms d'hôte, leurs interfaces et leurs adresses IP.

Placez le nom de périphérique nouvellement découvert à côté de l'entrée SVI pour l'adresse 192.168.4.132.

j. Connectez-vous au SVI pour l'adresse 192.168.4.133 en utilisant SSH et les informations d'identification utilisées précédemment. Émettez la commande **show lldp**, vous devriez recevoir un message :

```
% LLDP is not enabled
```

Activer lldp globalement comme à l'étape C. Il n'est pas nécessaire de configurer les options de transmission ou de réception car elles sont activées par défaut. Utilisez la commande **show lldp neighbors** et la commande **show lldp neighbors detail** pour détecter d'autres périphériques voisins connectés.

Question :

- Quels types de périphériques réseau avoisinent ce périphérique ? Enregistrez tous les périphériques détectés dans la table d'adressage. Incluez leurs noms d'hôte, leurs interfaces et leurs adresses IP. Il peut être utile de se reconnecter aux périphériques précédemment découverts pour afficher les voisins une fois de plus pour compléter la table d'adressage entière maintenant que tous les périphériques sont configurés pour LLDP.

k. Dessinez une topologie du réseau de bureaux de RBO à distance en utilisant les informations que vous avez recueillies avec le LLDP.

Activité 2 : Utiliser LLDP pour mapper un réseau- Packet Tracer

Réponses

- **Partie :**

h) - The RBO-Edge router hostname

- **Partie 2**

d)- C'est un routeur. Son nom est RBO-Firewall et il est connecté sur l'interface G0/0. L'adresse IP de l'appareil n'est pas répertoriée.

f) - La version du logiciel IOS de l'appareil voisin.

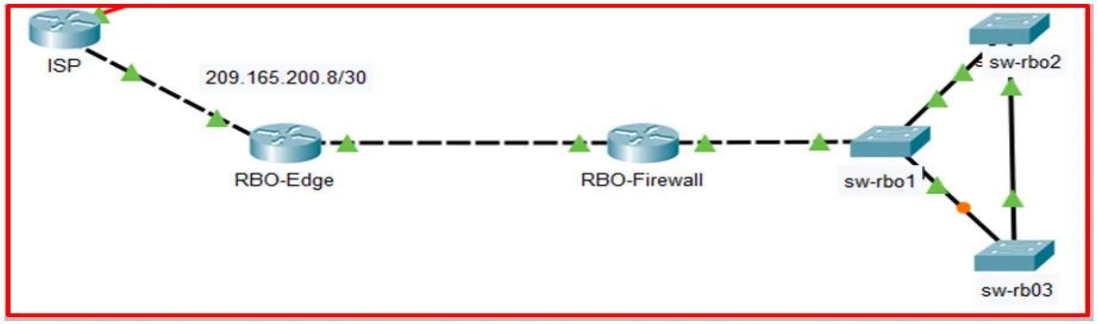
g) - RBO-Firewall#

h)- Un routeur (RBO-Edge) et un switch (sw-rbo1). Le commutateur sw-rbo1 est un périphérique nouvellement découvert sur l'interface G0/1.

i)- Un routeur (RBO-Firewall), un switch (sw-rbo2). Le commutateur sw-rbo2 est un périphérique nouvellement découvert sur l'interface G0/2.

j) - Un interrupteur (sw-rbo1) connecté à Fa0/24, un interrupteur (sw-rbo2) connecté à G0/1.

k)-



PARTIE 6

PARTIE 6

Activité 3 : Configurer et vérifier le protocole NTP - Packet Tracer

- **Objectifs**

- **Configurer et vérifier le protocole NTP**

- **Contexte/scénario**

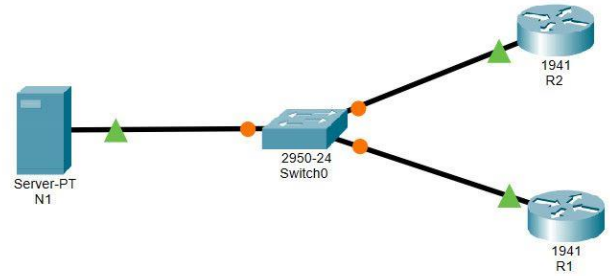
Le protocole NTP (Network Time Protocol) synchronise l'heure sur un ensemble de serveurs et de clients temporels distribués. La synchronisation temporelle est requise par un certain nombre d'applications. Cependant, dans le cadre de ces travaux pratiques, nous nous concentrerons uniquement sur la corrélation entre les événements listés dans le journal système et d'autres événements temporels issus de plusieurs périphériques réseau. NTP utilise le protocole UDP comme protocole de transport. Toutes les communications NTP utilisent le temps universel coordonné (UTC).

Un serveur NTP reçoit généralement son heure d'une source de temps autorisée, telle qu'une horloge atomique reliée à un serveur de temps. Le serveur NTP distribue ensuite cette heure à l'ensemble du réseau. NTP est extrêmement efficace. Un paquet par minute suffit pour synchroniser deux appareils avec une précision de l'ordre de la milliseconde.

- **Table d'adressage**

Appareil	Interface	Adresse IP	Masque de sous-réseau
N1	Carte réseau	209.165.200.225	255.255.255.0
R1	G0/0	209.165.200.226	255.255.255.0
R2	G0/0	209.165.200.227	255.255.255.0

- **Topologie**



- **Instructions**

- **Partie 1: Serveur NTP**

a. Le serveur N1 est déjà configuré comme serveur NTP pour cette topologie. Vérifiez sa configuration sous **Services** > **NTP**.

Ouvrez la fenêtre de configuration.

b. À partir de R1, envoyez une requête ping à N1 (209.165.200.225) afin de vérifier la connectivité. La requête ping devrait aboutir.

c. Répétez la requête ping vers N1 à partir de R2 pour vérifier la connectivité à N1.

- **Etape 1: Configurez les clients NTP**

Les périphériques Cisco peuvent être configurés pour se référer à un serveur NTP pour utiliser la synchronisation de leurs horloges. Il est important de garder une heure synchronisée entre tous les périphériques. Configurez R1 et R2 comme des clients NTP, de sorte que leurs horloges soient synchronisées. R1 et R2 utilisent tous deux le serveur N1 comme serveur NTP.

a. Vérifiez les paramètres actuels du NTP et de l'horloge comme indiqué ci-dessous:

Activité 3 : Configurer et vérifier le protocole NTP - Packet Tracer

- R1# **show ntp status**

```
%NTP is not enabled.
```

- R1# **show clock detail**

```
* 0:1:53 .745 UTC lun. mars 1 1993

Time source is hardware calendar
```

b. Configurez R1 et R2 en tant que client NTP. Utilisez la commande **ntp server** pour spécifier un serveur NTP, comme indiqué ci-dessous:

- R1# **conf t**
- R1(config)# **ntp server 209.165.200.225**

c. Répétez cette configuration sur **R2**.

Etape 3: Vérifier les paramètres NTP

a. Vérifiez l'horloge sur les routeurs R1 et R2 pour vous assurer qu'ils sont synchronisés:

- R1# **show clock detail**

```
12:7:18 .451 UTC sam. 12 oct. 2019

Time source is NTP
```

Remarque: Lorsque vous utilisez des routeurs physiques, patientez quelque minutes pour que les horloges de R1 et R2 soient synchronisées. Avec Packet Tracer, vous pouvez utiliser le bouton Fast Forward Time pour accélérer la synchronisation.

Exécutez la même commande sur R2.

Question:

- Les horloges sont-elles synchronisées?

b. Vérifiez l'état NTP et les associations NTP à l'aide des commandes suivantes pour vérifier le fonctionnement et la configuration NTP.

- R1# **show ntp status**

```
Clock is synchronized, stratum 2, reference is 209.165.200.225

<Output omitted>
```

- R1# **show ntp associations**

```
address ref clock st when poll reach delay offset disp

*~209.165.200.225127.127.1.1 1 11 32 377 9.00 4.00 0.24

 * sys.peer, # selected, + candidate, - outlyer, x
falseticker, ~ configured
```

Réponses

- **Etape 3 :**

a) - Oui. R1 et R2 ont la même heure que N1.

PARTIE 6

PARTIE 6

Activité 4 : Sauvegarder les fichiers de configuration- Packet Tracer

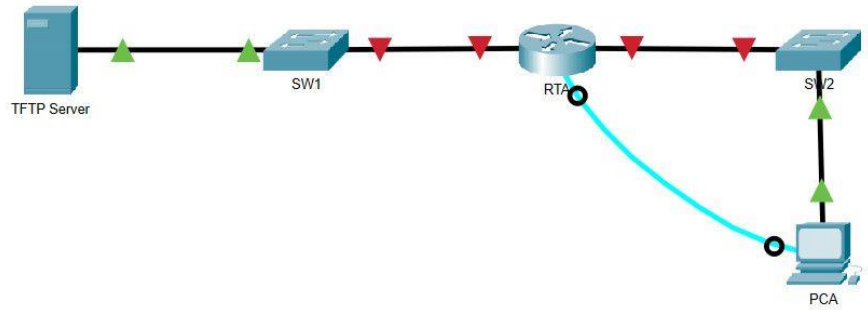
- **Objectifs**

- **Partie 1 : Établissement de la connectivité avec le serveur TFTP**
- **Partie 2 : Transfert du fichier de configuration à partir du serveur TFTP**
- **Partie 3 : Sauvegarde de la configuration et de l'IOS sur le serveur TFTP**

- **Contexte/scénario**

Dans Cet exercice vous allez restaurer une configuration à partir d'une sauvegarde, puis effectuer une nouvelle sauvegarde. En raison d'une défaillance matérielle, un nouveau routeur a été installé. Heureusement, des fichiers de sauvegarde de configuration ont été enregistrés sur un serveur TFTP. Vous devez restaurer ces fichiers à partir du serveur TFTP pour reconnecter le routeur en minimisant le temps d'arrêt.

- **Topologie**



- **Instructions**

Partie 1: Établissement de la connectivité avec le serveur TFTP

Remarque: Étant donné qu'il s'agit d'un nouveau routeur, la configuration initiale sera effectuée à l'aide d'une connexion de console avec le routeur.

a. Cliquez sur **PCA**, puis sur l'onglet **Desktop** et enfin sur **Terminal** pour accéder à la ligne de commande **RTA**.

b. Configurez et activez l'interface **Gigabit Ethernet 0/0**. L'adresse IP doit correspondre à celle de la passerelle par défaut du **serveur TFTP**.

c. Testez la connectivité avec le **serveur TFTP**. Résolvez les éventuels problèmes.

Partie 2: Transférer le fichier de configuration du serveur TFTP

a. Entrez la commande suivante à partir du mode d'exécution privilégié :

- Router# **copy tftp running-config**

```
Address or name of remote host []? 172.16.1.2
Source filename []? RTA-confg
Destination filename [running-config]? <cr>
```

Activité 4 : Sauvegarder les fichiers de configuration- Packet Tracer

Le routeur doit renvoyer ceci :

```
Accessing tftp://172.16.1.2/RTA-confg...
Loading RTA-confg from 172.16.1.2: !
[OK - 785 bytes]
785 bytes copied in 0.001 secs
```

- RTA#

b. Exécutez la commande pour afficher la configuration actuelle.

Question :

- Quelles modifications ont été apportées ?

c. Exécutez la commande **show** appropriée pour afficher l'état de l'interface.

Question :

- Toutes les interfaces sont-elles actives ?

d. Corriger tout problème lié à l'interface et tester la connectivité entre le PCA et le serveur TFTP.

Partie 3: Sauvegarde de la configuration et de l'IOS vers le serveur TFTP

a. Remplacez le nom d'hôte **RTA** par **RTA-1**.

b. Enregistrez la configuration en mémoire NVRAM.

c. Copiez la configuration sur le **serveur TFTP** à l'aide de la commande **copy** :

- RTA-1# **copy running-config tftp:**

```
Address or name of remote host []? 172.16.1.2
Destination filename [RTA-1-confg]? <cr>
```

d. Exécutez la commande pour afficher les fichiers présents dans la mémoire Flash.

e. Sauvegardez l'IOS en flash sur le **serveur TFTP** en utilisant la commande suivante :

- RTA-1# **copy flash tftp:**

```
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.16.1.2
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? <cr>
```

Quel caractère spécial s'affiche à plusieurs reprises indiquant que le fichier IOS est copié sur le serveur TFTP avec succès ?

f. Ouvrez le serveur TFTP et cliquez sur l'onglet Services, sélectionnez TFTP et faites défiler la liste des fichiers IOS.

Question :

- Le fichier IOS **C1900-UniversalK9-mz.spa.151-4.m4.bin** a-t-il été copié sur le serveur TFTP ?

g. Ouvrez le serveur TFTP et cliquez sur l'onglet Services, sélectionnez TFTP et faites défiler la liste des fichiers IOS.

Question :

- Le fichier IOS **C1900-UniversalK9-mz.spa.151-4.m4.bin** a-t-il été copié sur le serveur TFTP ?

Activité 4 : Sauvegarder les fichiers de configuration- Packet Tracer

Réponses

,,,

- **Partie 2**

b) - La configuration stockée sur le serveur TFTP a été chargée dans le routeur et le nom d'hôte du routeur a été remplacé par RTA.

c) - Non, G0/1 est en panne administrativement.

- **Partie 3 :**

e) - The exclamation point !.

f)- Oui, le fichier c1900-universalk9-mz.SPA.151-4.M4.bin est répertorié dans les fichiers sur le serveur TFP.

PARTIE 6

Activité 5 : Utiliser un serveur TFTP pour mettre à niveau une image IOS Cisco - Packet Tracer

Objectifs

- **Partie 1: Mettre à niveau d'une image IOS sur un périphérique Cisco**
- **Partie 2: Sauvegarder une image IOS sur un serveur TFTP**

Scénario

Un serveur TFTP permet de gérer le stockage des images IOS et des révisions de ces images. Quel que soit le réseau, il est recommandé de conserver une copie de sauvegarde de l'image du logiciel Cisco IOS au cas où l'image du système dans le routeur serait corrompue ou accidentellement effacée. Un serveur TFTP peut également être utilisé pour stocker de nouvelles mises à niveau vers l'IOS et être ensuite déployé sur l'ensemble du réseau là où cela s'avère nécessaire. Au cours de cet exercice, vous allez mettre à niveau des images IOS sur des périphériques Cisco à l'aide d'un serveur TFTP. Vous allez également sauvegarder une image IOS en utilisant un serveur TFTP.

Topologie

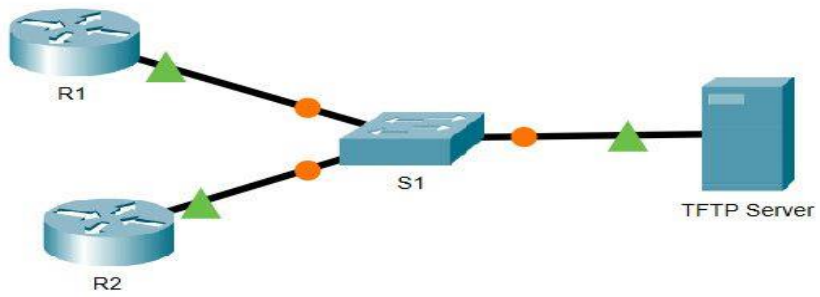


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0/0	192.168.2.1	255.255.255.0	N/A
R2	G0/0	192.168.2.2	255.255.255.0	N/A
S1	VLAN 1	192.168.2.3	255.255.255.0	192.168.2.1
Serveur TFTP	Carte réseau	192.168.2.254	255.255.255.0	192.168.2.1

Instructions

Partie 1: Mettez à niveau d'une image IOS sur un périphérique Cisco

Etape 1: Mettez à niveau une image IOS sur un routeur

a. Accédez au serveur TFTP et activez le service TFTP.

b. Notez les fichiers d'images IOS qui sont disponibles sur le serveur TFTP.

Question:

- Quelles images IOS stockées sur le serveur sont compatibles avec un routeur de 1941 ?

Ouvrez la fenêtre de configuration.

c. À partir de **R2**, exécutez la commande **show flash:** et notez la mémoire Flash disponible.

d. Copy the CISCO1941/K9 IOS version 15.5 image for the 1941 router from the TFTP Server to R2.

Activité 5 : Utiliser un serveur TFTP pour mettre à niveau une image IOS Cisco- Packet Tracer

Remarque: Dans un réseau réel, s'il y a plus d'une interface active sur le routeur, vous devrez peut-être entrer la commande **ip tftp source interface** pour spécifier quelle interface doit être utilisée pour contacter le serveur TFTP. Cette commande n'est pas prise en charge dans PT 7.2 et les versions anciennes et n'est pas nécessaire pour effectuer cette activité.

R2# **copy tftp: flash:**

```
Address or name of remote host []? 192.168.2.254
Source filename []? C1900-UniversalK9-MZ.SPA.155-3.M4A.bin
Destination filename [c1900-universalk9-mz.SPA.155-3.M4a.bin]?

Accessing tftp://192.168.2.254/c1900-universalk9-mz.SPA.155-3.M4a.bin....
Loading c1900-universalk9-mz.SPA.155-3.M4a.bin from 192.168.2.254:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 4.099 secs (860453 bytes/sec)
```

e. Assurez-vous que l'image IOS a été copiée dans la mémoire Flash.

Question:

- Combien la mémoire Flash contient-elle d'images IOS?

f. Utilisez la commande **boot system** pour charger l'image IPBase version 15.5 lors du prochain redémarrage.

- R2 (config) # **boot system flash c1900-universalk9-mz.SPA.155-3.M4a.bin**

g. Enregistrez la configuration et redémarrez le routeur **R2**.

h. Utilisez la commande **show version** pour verifier que la mise à niveau a été chargée après le redémarrage de **R2** .

- R2# **show version**

```
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.5(3)M4a, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Thu 06-Oct-16 13:56 by mnguyen

ROM: System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)

R2 uptime is 21 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.155-3.M4a.bin"
---- output omitted -----
```

PARTIE 6

Activité 5 : Utiliser un serveur TFTP pour mettre à niveau une image IOS Cisco- Packet Tracer

Etape 2: Mettez à niveau une image IOS sur un commutateur

a. Accédez au serveur TFTP et copiez l'image **c2960-lanbasek9-mz.150-2.SE4.bin** sur S1.
   - S1# **copy tftp: flash:**

b. Utilisez la commande **boot system** pour configurer le commutateur pour charger la nouvelle image IOS au démarrage.

c. Redémarrez S1 et vérifiez que la nouvelle image a été chargée dans la mémoire.

d. Fermez la fenêtre de Configuration TFTP si elle est toujours ouverte.

Partie 2: Sauvegarder une image IOS sur un serveur TFTP

a. Sur **R1**, affichez le contenu de la mémoire Flash et enregistrez l'image IOS.
   - R1# **show flash**:

b. Utilisez la commande **copy** pour sauvegarder l'image IOS dans la mémoire Flash de **R1** sur un serveur TFTP. **Remarque**: l'image isr4300 est considérablement plus grande que l'image c1900. Il faudra plus de temps pour le transmettre au serveur TFTP.
   - R1# **copy flash: tftp:**

```
Source filename []? ISR4300-UniversalK9.03.16.05.S.155-3.S5-Ext.Spa.bin

Address or name of remote host []? 192.168.2.254

Destination filename [isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin]?

Writing isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!! --- output omitted ----

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - 486899872 bytes]

486899872 bytes copied in 18.815 secs (83367 bytes/sec)
```

c. Accédez au serveur TFTP et vérifiez que l'image IOS a été copiée sur le serveur TFTP.

Remarque: Vous devrez peut-être démarrer et arrêter le service TFTP sur le serveur afin que le fichier apparaisse dans la liste des fichiers.

PARTIE 6

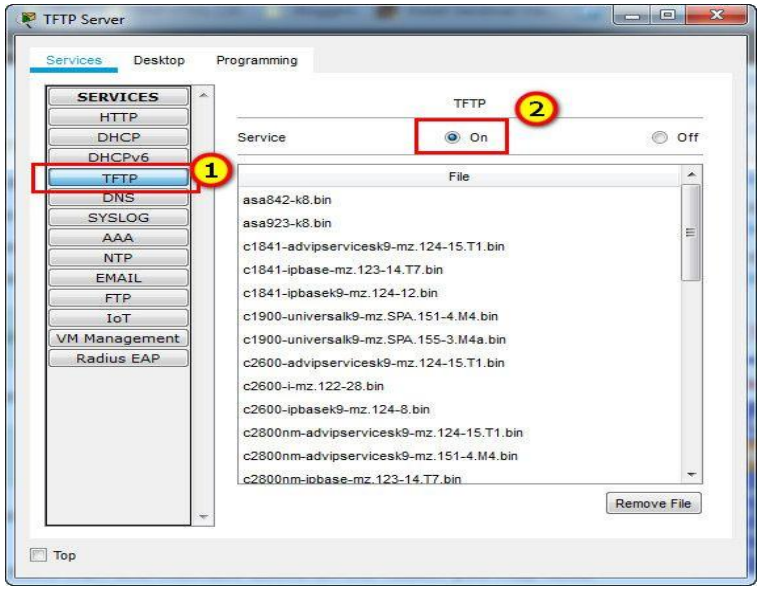
PARTIE 6

Activité 5 : Utiliser un serveur TFTP pour mettre à niveau une image IOS Cisco- Packet Tracer

Réponses

- **Partie 1 / Etape 1 :**

a)- Go to **TFTP Server** –> tab **Services** –> **TFTP** –> tick **On**



b) - c1900-universalk9-mz.SPA.151-4.M4.bin and c1900-universalk9-mz.SPA.155-3.M4a.bin

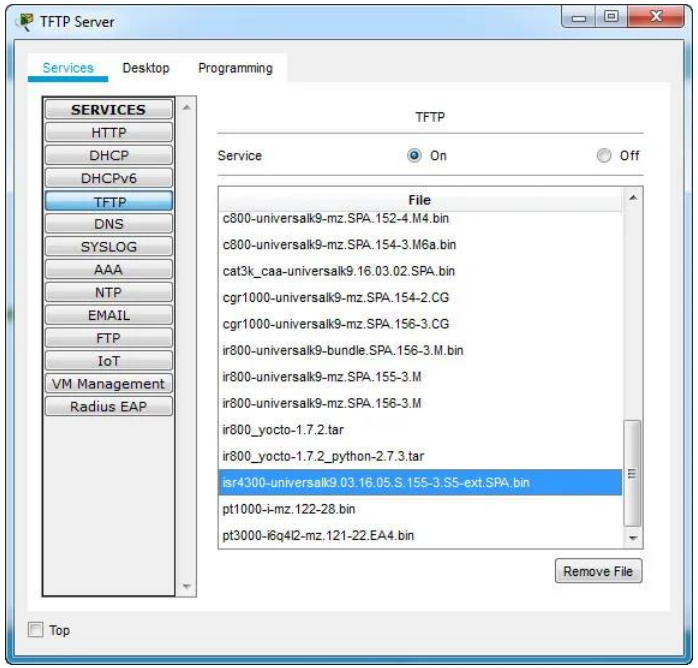
c) - 221896413

e) - 2

- **Partie 2**

a) - isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin

c) –



TP 3

Mettre en place un système de gestion et de supervision des réseaux

1. Gestion réseau : CDP, LLDP, NTP
2. Supervision réseau
3. Dépannage réseau (Network Troubleshooting)

PARTIE 6

Activité 1 : Rechercher un Logiciel de surveillance du réseau - Lab

- **Objectifs**

- **Partie 1 : Sondez votre compréhension de la surveillance du réseau**
- **Partie 2 : Recherchez des Outils de surveillance du réseau**
- **Partie 3 : Sélectionnez un outil de surveillance du réseau**

- **Contexte/Scénario**

La surveillance du réseau est nécessaire pour tout réseau de taille. La surveillance proactive de l'infrastructure réseau peut aider les administrateurs réseau dans leurs tâches quotidiennes. La grande variété d'outils de mise en réseau disponibles varie en coût, en fonction des fonctionnalités, du nombre d'emplacements réseau et du nombre de nœuds pris en charge. Dans cet atelier, vous effectuerez des recherches sur les logiciels de surveillance de réseau disponibles. Vous recueillerez des informations sur les produits logiciels et les fonctionnalités de ces produits. Vous étudierez un produit plus en détail et énumérerez certaines des fonctionnalités clés disponibles.

- **Required Resources**

- PC with internet access

- **Instructions**

- **Partie 1 : Sondez votre compréhension de la surveillance du réseau**

Décrivez la surveillance du réseau telle que vous la comprenez. Donnez un exemple de la façon dont il pourrait être utilisé dans un réseau de production.

- **Partie 2 : Recherchez des Outils de surveillance du réseau**

Étape 1 : Recherchez et trouvez trois outils de surveillance du réseau

Énumérez les trois outils que vous avez trouvés.

Étape 2 : Remplissez le formulaire suivant pour les outils de surveillance du réseau sélectionnés.

Vendor	Product Name	Features

- **Partie 3 : Sélectionnez un outil de surveillance du réseau**

Étape 1 : Sélectionnez un ou plusieurs outils de surveillance à partir de votre recherche

À partir de vos recherches, identifiez un ou plusieurs outils que vous choisiriez pour surveiller votre réseau. Énumérez les outils et expliquez les raisons pour lesquelles vous les avez choisis, y compris les caractéristiques spécifiques que vous considérez comme importantes.

Étape 2 : Étudiez l'outil de surveillance du réseau PRTG

Recherchez sur Internet les termes **Paessler** et **PRTG** et recherchez une liste de fonctionnalités. Donnez des exemples de certaines des fonctionnalités que vous avez trouvées pour PRTG dans l'espace prévu ci-dessous.

Questions de réflexion

- Sur la base de vos recherches, à quelles conclusions êtes-vous parvenu concernant les logiciels de surveillance de réseau ?

PARTIE 6

Activité 1 : Rechercher un Logiciel de surveillance du réseau - Lab

Réponses

- **Partie 1:**

- La surveillance du réseau est effectuée à l'aide d'un logiciel, généralement un outil ou un ensemble d'outils qui aident les administrateurs réseau à dépanner, surveiller et modifier les périphériques au sein de leur réseau. Des rapports, des graphiques de performances, la gestion de l'inventaire matériel, la gestion de l'inventaire logiciel, la cartographie réseau des topologies, la génération d'alertes par e-mail et/ou des SMS à un administrateur réseau peuvent faire partie de l'outil logiciel. Un administrateur réseau peut décider de configurer une alerte par e-mail lorsque la perte de paquets sur un routeur dépasse une certaine limite.

- **Partie 3 / Etape 1:**

- les réponses varieront considérablement. De nombreux outils commerciaux proposent des essais gratuits de 30 jours. PRTG est gratuit jusqu'à 100 capteurs réseau. La facilité d'utilisation du produit peut être un facteur important lors de la sélection des outils. Le support multi-fournisseurs est également important.

- **Partie 3 / Etape 2:**

- les réponses varieront. PRTG dispose d'une surveillance réseau complète avec prise en charge de plus de 170 types de capteurs. Il dispose également d'alertes flexibles, notamment : e-mail, syslog, pager, fichiers sonores d'alarme et alertes de condition multiples. La surveillance du réseau à distance, les cartes du réseau et les interfaces Web personnalisables sont également disponibles.

- **Partie 2 / Etape 1:**

- Les réponses varieront. **Solar Winds**, **PRTG, Nagios**, **Cacti et OpManager** sont quelques exemples.

Vendor	Product Name	Features
Solar Winds: www.solarwinds.com	Network Performance Monitor	Performance monitoring, automated network device discovery, network alerting, multi-vendor device support
Paessler: www.paessler.com	PRTG	Logging, bandwidth monitoring, packet sniffing, support for NetFlow Offers both a free version which is limited to 100 monitored interfaces and a paid version which is sold in increments of 500 monitored
Nagios: www.nagios.org	Nagios XI	Real-time event monitoring, performance and capacity planning, configuration wizards, user-specific notification preferences
Cacti: www.cacti.net	Cacti	Open Source product that maintains many of the same features and adds a database to store the logs as opposed to the text logs used by the popular predecessor, MRTG.
ManageEngine: https://www.manageengine.com/network-monitoring/	OpManager	Paid product based on the number of sensors. OpManage touts the ability to monitor both physical and virtual environments including VMWare, Xen, Hyper-V among others.

- **Questions de réflexion**

- Les réponses varieront. Compte tenu du nombre de produits disponibles, le choix du bon produit est crucial. Les versions d'essai de 30 jours peuvent être intéressantes car elles permettent à l'administrateur réseau de travailler avec un produit avant de l'acheter. Il y aura une courbe d'apprentissage à l'utilisation du produit, avec celui qui est choisi.

TP 2

Mettre en place un système de gestion et de supervision des réseaux

1. Gestion réseau: CDP, LLDP, NTP
2. Supervision réseau
3. Dépannage réseau (Network Troubleshooting)

Critères de réussite :

- Le stagiaire est-il capable de :
  - Dépanner les réseaux d'entreprise ?
- Réponses correctes pour au moins 70 % des questions.

PARTIE 6

Activité 1 : Dépanner les réseaux d'entreprise_Packet Tracer

- **Objectifs**

- **Partie 1: Vérifier les technologies de commutation**
- **Partie 2: Vérifier DHCP**
- **Partie 3: Vérifier le routage**
- **Partie 4 : Vérifier les technologies WAN**
- **Partie 5: Vérifier la connectivité**

- **Scénario**

Cette activité utilise une variété de technologies que vous avez rencontrées au cours de vos études CCNA, y compris le routage IPv4, le routage IPv6, la sécurité des ports, EtherChannel, DHCP et NAT. Votre tâche consiste à examiner les spécifications, à isoler et résoudre tous les problèmes, et à documenter les étapes suivies en vue de vérifier ces spécifications.

La société a remplacé les routeurs R1 et R3 pour permettre une connexion fibre optique entre les emplacements. Les configurations des routeurs précédents avec des connexions série ont été modifiées et appliquées comme configuration de démarrage. IPv6 est testé sur une petite partie du réseau et doit être vérifié.

Remarque: les mots de passe ont été supprimés pour faciliter le dépannage dans cet exercice. Les protections par mot de passe habituelles doivent être réappliquées; toutefois, l'activité ne classe pas ces éléments.

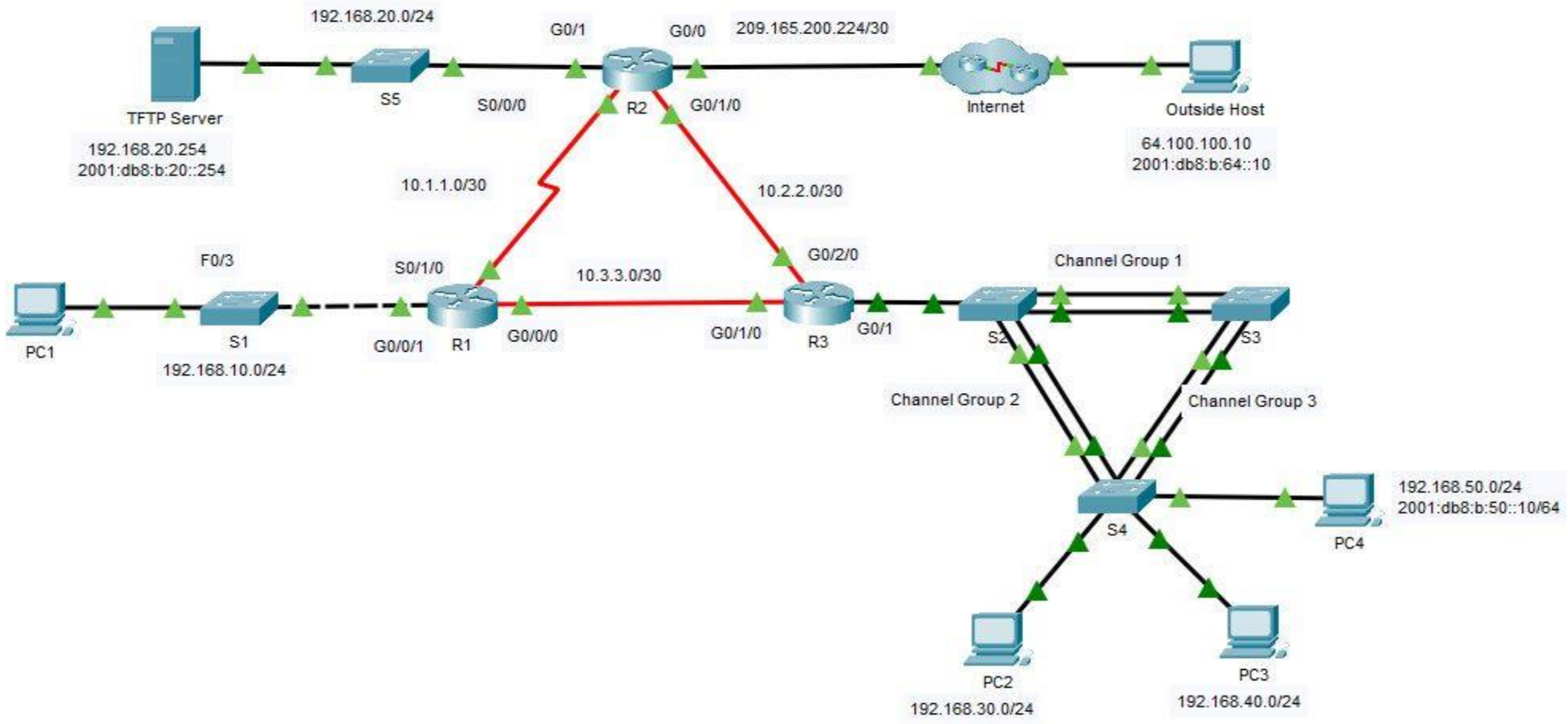
- **Table d'adressage**

Appareil	Interface	Adresse IP <préfixe>	Passerelle par défaut
R1	G0/0/1	192.168.10.1 /24	S/O
	S0/1/0	10.1.1.1 /30	S/O
	G0/0/0	10.3.3.1 /30	S/O
R2	G0/0	209.165.200.225 /27	S/O
	G0/0	2001:db8:b:209::1/64	S/O
	G0/1	192.168.20.1 /30	S/O
	G0/1	2001:db8:b:20::1/64	S/O
	S0/0/0	10.1.1.2 /30	S/O
	G0/1/0	10.2.2.1 /30	S/O
	G0/1/0	2001:db8:b:10:2::1/64	S/O
R3	G0/1.30	192.168.30.1 /24	S/O
	G0/1.40	192.168.40.1 /24	S/O
	G0/1.50	192.168.50.1 /24	S/O
	G0/1.50	2001:db8:b:50::1/64	S/O
	G0/1.99	S/O	S/O
	G0/1/0	10.3.3.2 /30	S/O
	G0/2/0	10.2.2.2 /30	S/O
	G0/2/0	2001:db8:b:10:2::2/64	S/O
S1	VLAN10	192.168.10.2 /24	192.168.10.1
S2	VLAN11	192.168.99.2 /24	S/O
S3	VLAN30	192.168.99.3 /24	S/O
S4	VLAN30	192.168.99.4 /24	S/O
PC1	Carte réseau	IPv4 attribué par DHCP	IPv4 attribué par DHCP
PC2	Carte réseau	IPv4 attribué par DHCP	IPv4 attribué par DHCP
PC3	Carte réseau	IPv4 attribué par DHCP	IPv4 attribué par DHCP
PC4	Carte réseau	IPv4 attribué par DHCP	IPv4 attribué par DHCP
	Carte réseau	2001:db8:b:50::10/64	fe80::3
Serveur TFTP	Carte réseau	192.168.20.254 /24	192.168.20.1
	Carte réseau	2001:db8:b:20::254/64	fe80::2

PARTIE 6

Activité 1 : Dépanner les réseaux d'entreprise Packet Tracer

- **Topologie**



Activité 1 : Dépanner les réseaux d'entreprise- Packet Tracer

- **Instructions**

  - **Partie 1: Vérifier les technologies de commutation**

a. La sécurité des ports est configurée de telle sorte que seul **PC1** peut accéder à l'interface F0/3 de **S1**. Toutes les violations doivent désactiver l'interface.

Exécutez la commande sur S1 pour afficher l'état actuel de sécurité du port.

- S1# **show port-security**

b. Entrez en mode de configuration de l'interface pour l'interface F0/3 et configurez la sécurité des ports.

- S1(config-if)# **switchport port-security**
- S1(config-if)# **switchport port-security mac-address sticky**

c. Les périphériques du réseau local sur S1 doivent être dans VLAN 10. Affichez l'état actuel de la configuration du VLAN.

Question:

- Quels ports sont actuellement attribués au VLAN 10?

d. PC1 devrait recevoir une adresse IP du routeur R1.

Question:

- Une adresse IP est-elle actuellement attribuée au PC?

e. Notez que l'interface G0/1 sur R1 n'est pas dans le même VLAN que PC1. Modifiez l'interface G0/1 pour qu'elle soit membre de VLAN 10 et définissez portfast sur l'interface.

- S1 (config-if) # **int G0/1**
- S1(config-if)# **switchport access vlan 10**
- S1(config-if)# **spanning-tree portfast**

f. Réinitialisez l'adresse de l'interface sur PC1 à partir de l'interface graphique ou à l'aide de l'invite de commande et de la commande **ipconfig /renew** . Est-ce que PC1 a une adresse? Si ce n'est pas le cas, vérifiez à nouveau vos étapes. Testez la connectivité avec le serveur TFTP. La requête ping devrait aboutir.

g. Un commutateur supplémentaire a été ajouté au réseau local connecté à R3. L'agrégation de liaisons à l'aide d'EtherChannel est configurée sur **S2**, **S3** et **S4**. Les liens EtherChannel doivent être définis sur trunk. Les liens EtherChannel doivent être définis pour former un canal sans utiliser un protocole de négociation. Exécutez la commande sur chaque commutateur pour déterminer si le canal fonctionne correctement.

- S2# **show etherchannel summary**

```
<output omitted>

1 Po1 (SU) - Fa0/1 (P) Fa0/2 (P)

2 Po2 (SU) - Fa0/3 (P) Fa0/4 (P)
```

Question:

- Y a-t-il eu des problèmes avec EtherChannel?

h. Modifiez S3 pour inclure les ports F0/1 et F0/2 comme port channel 1.

- S3(config)# **interface range f0/1-2**
- S3(config-if-range)# **channel-group 1 mode on**

PARTIE 6

Activité 1 : Dépanner les réseaux d'entreprise- Packet Tracer

Vérifiez l'état de l'EtherChannel sur S3. Il devrait être stable maintenant. Si ce n'est pas le cas, vérifiez les étapes précédentes.

i. Vérifiez l'état du trunk sur tous les commutateurs.

- S3# **show int trunk**

Question:

- Y a-t-il des problèmes avec le trunking?

j. Corrigez les problèmes de trunk sur S2.

- S2 (config) # **int g0/1**
- S2(config-if)# **switchport trunk native vlan 99**

k. STP doit être défini sur PVST+ sur **S2**, **S3**et **S4**. **S2** doit être configuré pour être le pont racine pour tous les VLAN. Exécutez la commande pour afficher l'état spanning-tree sur S2.

- S2# **show spanning-tree summary totals**

```
Switch is in pvst mode

Root bridge for:
```

l. La sortie de la commande indique que S2 n'est pas le pont racine pour les VLAN. Corrigez l'état de spanning-tree sur S2.

- S2(config)# **spanning-tree vlan 1-1005 root primary**

m. Vérifiez l'état de spanning-tree sur S2 pour vérifier les modifications.

- S2# **show spanning-tree summary totals**

```
Switch is in pvst mode

Root bridge for: default V30 V40 V50 Native
```

Partie 2: Vérifier DHCP

- R1 est le serveur DHCP du LAN R1.
- R3 est le serveur DHCP pour les 3 réseaux locaux connectés à R3.

a. Vérifiez l'adressage des PC.

Question:

- Est-ce qu'ils ont tous une adresse correcte?

b. Vérifiez les paramètres DHCP sur R3. Filtrez la sortie de la commande **show run** pour démarrer avec la configuration DHCP.

Ouvrez la fenêtre de configuration.

- R3# **sh run | begin dhcp**

```
ip dhcp excluded-address 192.168.30.1 192.168.30.9

ip dhcp excluded-address 192.168.40.1 192.168.40.9

ip dhcp excluded-address 192.168.50.1 192.168.50.9

!

ip dhcp pool LAN30

 network 192.168.30.0 255.255.255.0

 default-router 192.168.30.1
```

PARTIE 6

Activité 1 : Dépanner les réseaux d'entreprise- Packet Tracer

```
ip dhcp pool LAN40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.30.1
ip dhcp pool LAN50
 network 192.168.50.0 255.255.255.0
 default-router 192.168.30.1
```

Question:

- Y a-t-il des problèmes avec les configurations DHCP?

c. Effectuez les corrections nécessaires et réinitialisez les adresses IP sur les PC. Vérifiez la connectivité à tous les appareils.

Question:

- Avez-vous pu ping toutes les adresses IPv4?

Partie 3: Vérifier le routage

Vérifiez que les exigences suivantes ont été respectées. Si non, complétez les configurations.

- Tous les routeurs sont configurés avec l'ID de processus OSPF 1 et aucune mise à jour de routage ne doit être envoyée vers les interfaces qui ne disposent pas de routeurs connectés.
- Le routeur R2 est configuré avec une route par défaut IPv4 pointant vers le FAI et il redistribue cette route par défaut dans le domaine d'OSPFv2.
- Le routeur R2 est configuré avec une route par défaut entièrement qualifié IPv6 pointant vers le FAI et il redistribue cette route par défaut dans le domaine d'OSPFv3.
- La fonction NAT est configurée sur le routeur R2 et aucune adresse non traduite n'est autorisée à transiter sur l'internet.

a. Vérifiez les tables de routage sur tous les routeurs.

Ouvrez la fenêtre de configuration.

- R3# **show ip route ospf**

```
<output omitted>
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O 10.1.1.0 [110/649] via 10.2.2.1, 01:15:53, GigabiteThernet0/2/0
O 192.168.10.0 [110/649] via 10.3.3.1, 01:15:53, GigabiteThernet0/1/0
192.168.20.0 [110/2] via 10.2.2.1, 01:15:53, GigabiteThernet0/2/0
<output omitted>
```

Question:

- Tous les réseaux apparaissent-ils sur tous les routeurs?

b. Ping sur l'hôte externe à partir de R2.

Question:

- La requête ping a-t-elle abouti?

PARTIE 6

Activité 1 : Dépanner les réseaux d'entreprise- Packet Tracer

c. Corriger la propagation d'une route par défaut
   - R2(config)# **router ospf 1**
   - R2(config-router)# **default-information originate**

d. Vérifiez les tables de routage sur R1 et R3 pour vous assurer que la route par défaut est présent.

e. Testez la connectivité IPv6 de R2 à l'hôte externe et au serveur TFTP. En principe, cette requête ping doit aboutir. Dépanner s'ils ne le sont pas.

f. Testez la connectivité IPv6 de R2 à PC4. Si le ping échoue, assurez-vous de vérifier que l'adressage IPv6 correspond à la table d'adressage.

g. Testez la connectivité IPv6 de R3 à l'hôte externe. Si le ping échoue, vérifiez les routes IPv6 sur R3. Assurez-vous de valider la route par défaut provenant de R2. Si la route n'apparaît pas, modifiez la configuration IPv6 OSPF sur R2.
   - R2(config)# **ipv6 router ospf 1**
   - R2(config-rtr)# **default-information originate**

h. Vérifiez la connectivité entre R2 et l'hôte externe. La requête ping devrait aboutir.

Partie 4: Vérifier les technologies WAN

- La liaison série entre R1 et R2 est utilisée comme liaison de sauvegarde en cas de panne et ne doit transporter du trafic que si la liaison fibre n'est pas disponible.
- La liaison Ethernet entre R2 et R3 est une connexion à fibre optique.
- La liaison Ethernet entre R1 et R3 est une connexion fibre et doit être utilisée pour transférer le trafic depuis R1.

a. Regardez de près la table de routage sur R1.

Question:

- Y a-t-il des routes utilisant le lien série?

Utilisez la commande traceroute pour vérifier les chemins suspects.

- R1# **traceroute 192.168.20.254**

```
Type escape sequence to abort.

Tracing the route to 192.168.20.254

  1 10.1.1.2 1 msec 1 msec 1 msec

  2 192.168.20.254 1 msec 9 msec 0 msec
```

Notez que le trafic est envoyé via l'interface S0/1/0 par opposition à l'interface G0/0/0.

b. Les configurations d'origine provenant des connexions WAN série précédentes ont été transférées aux nouveaux périphériques. Comparez les paramètres de l'interface G0/0/0 et Serial0/1/0. Notez qu'ils ont tous deux une valeur de coût OSPF définie. Supprimez le paramètre de coût OSPF de l'interface G0/0/0. Il sera également nécessaire de supprimer le paramètre sur le lien sur R3 qui se connecte à R1.
   - R1 (config) # **int g0/0/0**
   - R1(config-if)# **no ip ospf cost 648**
   - R3 (config) # **int g0/1/0**
   - R3 (config-if) # **no ip ospf cost 648**

PARTIE 6

Activité 1 : Dépanner les réseaux d'entreprise- Packet Tracer

c. Réexécuttez la commande traceroute à partir de R1 pour vérifier que le chemin a changé.

d. La modification a été apportée pour diriger le trafic sur la liaison plus rapide, mais la route de sauvegarde doit être testée. Arrêtez l'interface G0/2/0 sur R3 et testez la connectivité au serveur TFTP et à l'hôte externe.

Question:

- Les requêtes ping ont-elles abouti?

e. R2 est requis pour effectuer NAT pour tous les réseaux internes. Consultez les traductions NAT sur R2.

- R2# **show ip nat translations**

f. Notez que la liste est vide si vous avez seulement tenté de ping à partir de R1. Essayez d'envoyer une requête ping de R3 vers l'hôte externe et vérifiez à nouveau les traductions NAT sur R2. Exécutez la commande pour afficher les statistiques NAT actuelles qui fourniront également les interfaces impliquées dans NAT.

- R2# **show ip nat statistics**

```
<output will vary>

Total translations: 0 (0 static, 0 dynamic, 0 extended)

Outside Interfaces: GigabitEthernet0/0

Inside Interfaces: GigabitEthernet0/1 , GigabitEthernet0/1/0

Hits: 17 Misses: 27

Expired translations: 17

Dynamic mappings:
```

g. Définissez l'interface Serial 0/0/0 comme interface interne pour traduire les adresses.

- R2(config)# **int s0/0/0**
- R2(config-if)# **ip nat inside**

h. Testez la connectivité à l'hôte externe à partir de R1. La requête ping devrait aboutir. Réactivez l'interface G0/2/0 sur R3.

Partie 5: Vérifier la connectivité

- Les périphériques doivent être configurés conformément à la table d'adressage.
- Chaque périphérique doit être capable d'envoyer une requête ping à n'importe quel autre périphérique interne. Les PC internes doivent pouvoir envoyer une requête ping sur l'hôte externe.
- PC4 doit pouvoir envoyer une requête ping sur le serveur TFTP et l'hôte externe à l'aide d'IPv6.

Activité 1 : Dépanner les réseaux d'entreprise_Packet Tracer

Réponses

- **Partie 1:**

C) - F0/3, F0/4

d) – Non, il n'a qu'une adresse APIPA

f) - S3 shows Po1 as down (SD)

h) - S2 utilise le VLAN 1 comme VLAN natif sur l'interface de liaison G0/1.

- **Partie 2 :**

a) **-** Non, PC3 et PC4 ont des passerelles incorrectes

b) - Le paramètre de routeur par défaut est incorrect sur LAN40 et LAN50.

c) - Réinitialisez l'adresse de l'interface sur PC3, PC4 à partir de l'interface graphique ou en utilisant l'invite de commande et la commande **ipconfig /renew**.

- PC1, PC2, PC3 et PC4 doivent avoir une connectivité complète pour IPv4 en interne. Les hôtes ne peuvent pas envoyer de ping à l'extérieur. Ce problème sera traité dans la partie 3.

- **Partie 3**

a) - Tous les réseaux sont dans les tables de routage. Cependant, la route par défaut ne se propage pas vers R1 et R3, il n'y a donc qu'une connectivité vers l'extérieur à partir de R2.

b) - R2 devrait pouvoir envoyer un ping à l'hôte extérieur

- **Partie 4**

a)- Oui. Le trafic pour le réseau 192.168.20.0 et la route par défaut utilisent S0/1/0 au lieu de G0/0/0.

d)- Le serveur TFTP est accessible ; cependant, l'hôte extérieur ne peut pas être atteint. Les élèves doivent réfléchir aux autres causes du manque de connectivité. Dans ce cas, il s'agit d'un problème de NAT non défini comme interne sur l'interface série sur R2**.**

Configuration :

S1:

```
enable
config terminal
interface f0/3
switchport port-security
switchport port-security mac-address sticky
interface g0/1
switchport access vlan 10
spanning-tree portfast
```

PARTIE 6

PARTIE 6

Activité 1 : Dépanner les réseaux d'entreprise_Packet Tracer

Réponses

Configuration :

S2:

```
enable
config terminal
int g0/1
switchport trunk native vlan 99 spanning-
tree vlan 1-1005 root primary
```

S3:

```
enable
config terminal
interface range f0/1-2
channel-group 1 mode on
```

R1:

```
enable
config terminal
int g0/0/0
no ip ospf cost 648
```

R2 :

```
enable
config terminal
router ospf 1
default-information originate
ipv6 router ospf 1
default-information originate
int s0/0/0
ip nat inside
```

R3

```
enable
config terminal
router ospf 1
passive-interface g0/1.30
passive-interface g0/1.40
passive-interface g0/1.50
ip dhcp pool LAN40
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
ip dhcp pool LAN50
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1 int g0/1/0
no ip ospf cost 648
```

PARTIE 6

Activité 2 : Défi du dépannage - Documenter le réseau Packet Tracer

- **Objectifs**

Dans ce TP, vous allez documenter un réseau qui vous est inconnu.

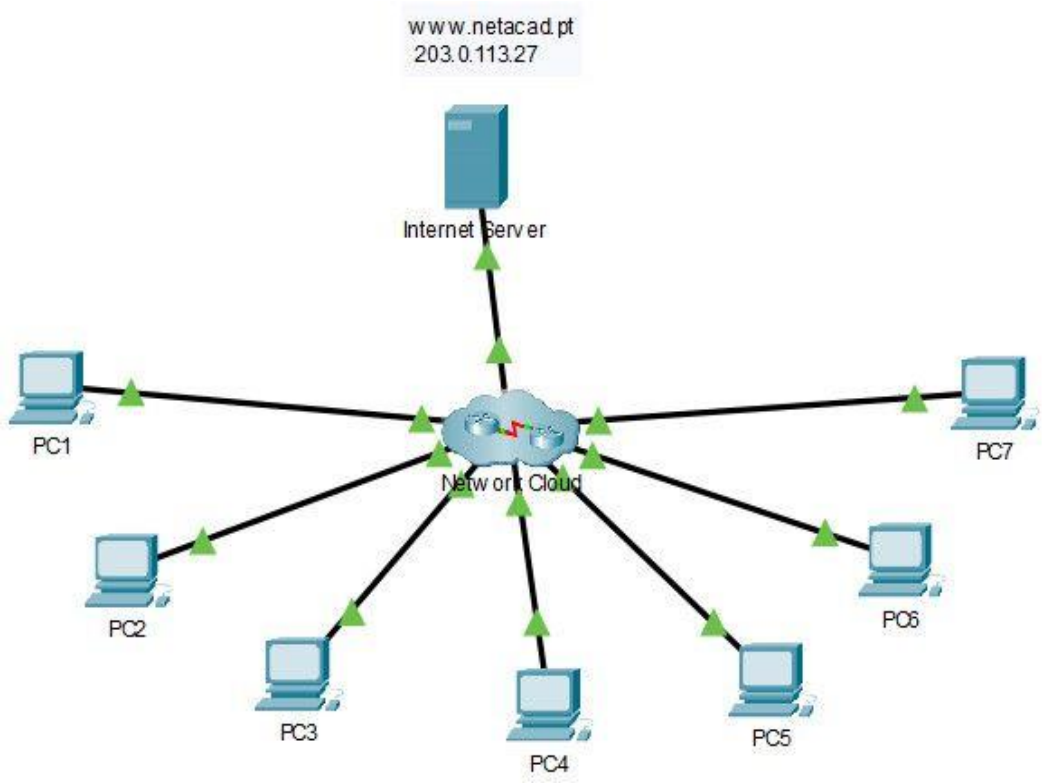
- **Test de la connectivité réseau**
- **Compiler les informations d'adressage de l'hôte.**
- **Accédez à distance aux périphériques de passerelle par défaut.**
- **Documentez les configurations de périphériques de passerelle par défaut.**
- **Découvrez les périphériques sur le réseau.**
- **Dessinez la topologie du réseau.**

- **Contexte/scénario**

Votre employeur a été embauché pour prendre en charge l'administration d'un réseau d'entreprise parce que l'ancien administrateur du réseau a quitté l'entreprise. La documentation réseau est manquante et doit être recréée. Vous travaillez à documenter les hôtes et les périphériques réseau, y compris tous les adressages de périphérique et les interconnexions logiques. Vous accéderez à distance aux périphériques réseau et utiliserez la découverte de réseau pour compléter une table de périphériques et dessiner la topologie du réseau.

Cet exercice constitue la première partie d'une activité de deux exercices. Vous utiliserez la documentation que vous créez dans cette activité pour vous guider lors du dépannage du réseau dans la partie II, **Packet Tracer - Défi de dépannage - Utiliser la documentation pour résoudre les problèmes**.

- **Contexte/scénario**



PARTIE 6

Activité 2 : Défi du dépannage - Documenter le réseau Packet Tracer

Lorsque vous étudiez et documentez la topologie du réseau, notez les problèmes que vous découvrez qui ne respectent pas les pratiques enseignées dans le programme d'études du CCNA.

- **Table d'adressage**

Appareil	Interface	Type de périphérique (routeur, commutateur, hôte)	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC1	Carte réseau	Hôte			
PC2					
PC3					
PC4					
PC5					
PC6					
PC7					

- **Instructions**

Partie 1: Tester la connectivité

Ping entre les PC et le serveur Internet pour tester le réseau. Tous les PC sont censés pouvoir envoyer des requêtes ping vers les autres PC et vers le serveur internet.

Partie 2: Détection des informations de configuration des PC

Accédez à l'invite de commande de chaque PC et affichez les paramètres IP. Inscrivez ces informations dans le tableau de documentation.

Partie 3: Découvrir les informations sur les périphériques de passerelle par défaut

Connectez-vous à chaque périphérique de passerelle par défaut à l'aide du protocole Telnet et enregistrez des informations sur les interfaces utilisées dans la table. Le mot de passe VTY est **cisco** et le mot de passe privilégié EXEC est **class**.

- C:\> **telnet *IP_address***

Partie 4: Reconstruire la topologie du réseau

Dans cette partie de l'activité, vous continuerez à enregistrer des informations sur les périphériques du réseau dans le tableau d'adressage. En outre, vous commencerez à diagrammer la topologie du réseau en fonction de ce que vous pouvez découvrir sur les interconnexions de périphériques.

Etape 1: Accédez aux tables de routage sur chaque périphérique de passerelle

- Utilisez les tables de routage de chaque routeur pour en savoir plus sur le réseau. Prenez note de vos conclusions.

Etape 2: Découvrez les périphériques autres que la passerelle

Utilisez un protocole de découverte réseau pour documenter les périphériques voisins. Enregistrez vos constatations dans le tableau d'adressage. À ce stade, vous devriez également être en mesure de commencer à documenter les interconnexions de périphériques.

Activité 2 : Défi du dépannage - Documenter le réseau Packet Tracer

- **Partie 5: Explorer davantage les configurations et les interconnexions des périphériques**

Etape 1: Limiter l'accès aux configurations d'un périphérique

Connectez-vous aux autres appareils du réseau. Recueillir des informations sur les configurations de périphériques.

Etape 2: Afficher les informations sur les voisins

Utilisez les protocoles de découverte pour améliorer vos connaissances sur les périphériques réseau et les topologies.

Etape 3: Se connecter à d'autres appareils

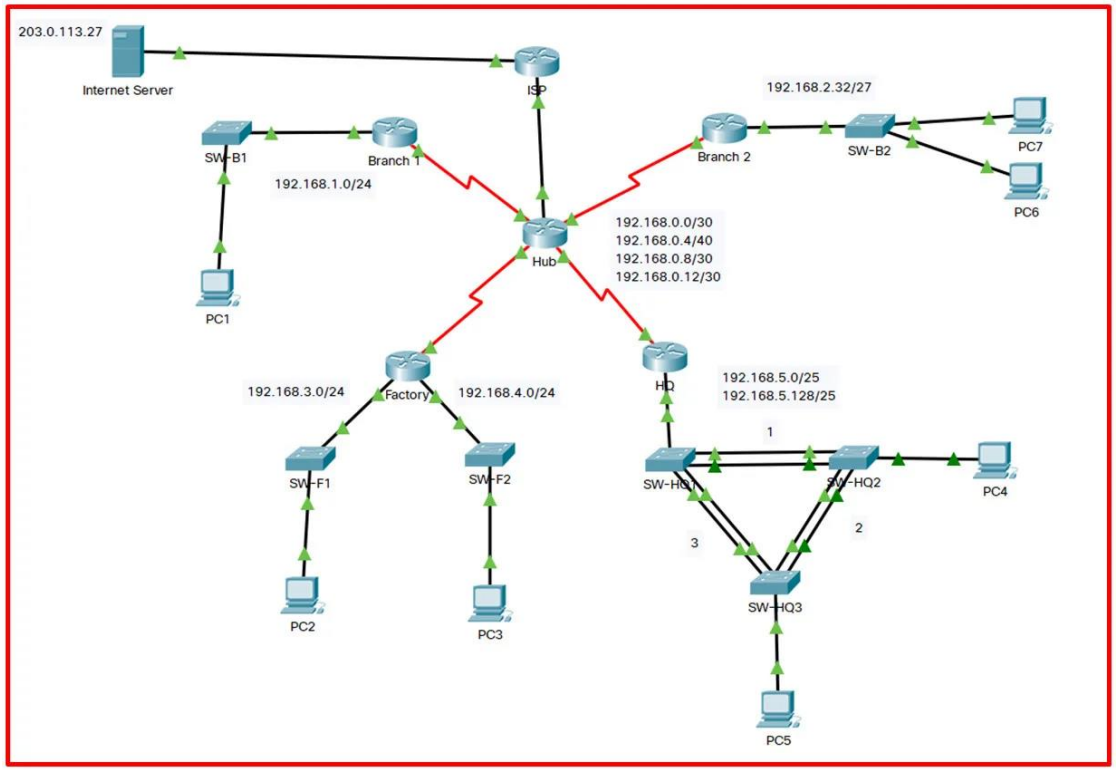
- Afficher les informations de configuration des autres périphériques du réseau. Enregistrez vos résultats dans la table des périphériques.
- Maintenant, vous devriez connaître tous les périphériques et configurations d'interface dans le réseau. Toutes les lignes de la table doivent contenir des informations sur le périphérique. Utilisez vos informations pour reconstruire autant de la topologie réseau que possible.

Question de reflexion

Vous avez peut-être remarqué que certaines des pratiques utilisées pour configurer les périphériques réseau sont obsolètes, inefficaces ou non sécurisées. Faites une liste d'autant de recommandations que vous avez sur la façon de reconfigurer les appareils pour suivre les pratiques que vous avez apprises dans le programme d'études du CCNA.

la topologie du réseau

les dessins des stagiaires auront une mise en page différente ; cependant, les interconnexions des appareils doivent être cohérentes. La topologie cachée est illustrée ci-dessous.



Activité 2 : Défi du dépannage - Documenter le réseau Packet Tracer

Réponses

Device	Interface	Device Type (router, switch, host)	IP Address	Subnet Mask	Default Gateway
PC1	NIC	Host	192.168.1.153	255.255.255.0	192.168.1.1
PC2	NIC	Host	192.168.3.50	255.255.255.0	192.168.3.1
PC3	NIC	Host	192.168.4.115	255.255.255.0	192.168.4.1
PC4	NIC	Host	192.168.5.83	255.255.255.128	192.168.5.1
PC5	NIC	Host	192.168.5.227	255.255.255.128	192.168.5.129
PC6	NIC	Host	192.168.2.48	255.255.255.224	192.168.2.33
PC7	NIC	Host	192.168.2.67	255.255.255.224	192.168.2.65
Hub	G0/0/0	router	192.0.2.1	255.255.255.252	N/A
Hub	S0/1/0	router	192.168.0.1	255.255.255.252	N/A
Hub	S0/1/1	router	192.168.0.5	255.255.255.252	N/A
Hub	S0/2/0	router	192.168.0.9	255.255.255.252	N/A
Hub	S0/2/1	router	192.168.0.13	255.255.255.252	N/A
Branch-1	G0/0/0	router	192.168.1.1	255.255.255.0	N/A
Branch-1	S0/1/0	router	192.168.0.2	255.255.255.252	N/A
Branch-2	G0/0/0	router	192.168.2.33	255.255.255.224	N/A
Branch-2	S0/1/0	router	192.168.0.6	255.255.255.252	N/A
Factory	G0/0/0	router	192.168.3.1	255.255.255.0	N/A
Factory	G0/0/1	router	192.168.4.1	255.255.255.0	N/A
Factory	S0/1/0	router	192.168.0.14	255.255.255.252	N/A
HQ	G0/0/0.1	router	192.168.6.1	255.255.255.0	N/A
HQ	G0/0/0.5	router	192.168.5.1	255.255.255.128	N/A
HQ	G0/0/0.10	router	192.168.5.128	255.255.255.128	N/A
HQ	S0/1/0	router	192.168.0.10	255.255.255.252	N/A
SW-B1	VLAN 1	switch	192.168.1.252	255.255.255.0	192.168.1.1
SW-B2	VLAN 1	switch	192.168.2.62	255.255.255.0	192.168.2.1
SW-F1	VLAN 1	switch	192.168.3.252	255.255.255.0	192.168.3.1
SW-F2	VLAN 1	switch	192.168.4.252	255.255.255.0	192.168.4.1
SW-HQ1	VLAN 1	switch	192.168.6.252	255.255.255.0	192.168.6.1
SW-HQ2	VLAN 1	switch	192.168.6.253	255.255.255.0	192.168.6.1
SW-HQ3	VLAN 1	switch	192.168.6.254	255.255.255.0	192.168.6.1

- **Partie 1 :**

- C:\> telnet IP_address

- **Question de réflexion**

La liste est longue. Cette question vous donne l'occasion d'examiner bon nombre des meilleures pratiques qui ont été abordées dans le programme CCNA. Utiliser les discussions des élèves pour s'assurer qu'autant de questions que possible ont été discutées. Certains problèmes sont :

- Tous les appareils utilisent les mêmes mots de passe simples et bien connus. Ceux-ci doivent être modifiés, doivent varier d'un appareil à l'autre et doivent être plus solides.
- Les commutateurs utilisent tous le SVI et le VLAN de gestion par défaut. Cela devrait être changé.
- La plupart des ports de commutation se trouvent dans le VLAN 1. Ils doivent être déplacés vers différents VLAN.

PARTIE 6

Activité 2 : Défi du dépannage - Documenter le réseau Packet Tracer

Réponses

- Tous les ports de commutation inutilisés se trouvent dans le VLAN 1 et sont actifs.
- Les ports de commutation inutilisés doivent être arrêtés et déplacés vers un VLAN inutilisé.
- La sécurité du port n'est pas utilisée.
- OSPF est actif sur les interfaces LAN. Les interfaces passives réduiront le trafic réseau inutile.
- La négociation DTP est active sur les ports de jonction. C'est un risque pour la sécurité.
- SSH n'est pas utilisé sur le réseau.
- L'accès de gestion à tous les appareils n'est pas limité à l'aide d'ACL ou d'AAA.
- 802.1x n'est pas implémenté.
- IP Source Guard n'est pas implémenté
- CDP est activé par défaut et doit être désactivé ou limité.
- DTP est actif sur tous les ports de SW-B1, SW-F1, SW-F2, SW-HQ1, SW-HQ2 et SW-HQ3, à l'exception des ports connectés à PC-4 et PC-5.
- L'ancien protocole STP est utilisé sur tous les commutateurs et doit être remplacé par RSTP (802.1w).
- Le VLAN natif 1 est utilisé sur les liaisons de jonction et doit être modifié.
- Le VLAN 99 est créé uniquement sur SW-B2 uniquement. Il n'est pas utilisé et n'a pas de nom et doit être supprimé.
- Le routeur concentrateur a le jeu de commandes ip default-gateway et l'adresse IP est à lui-même.

Activité 3 : Épreuve de dépannage - Utilisation de la documentation pour résoudre des problèmes_Packet Tracer

- **Objectifs**

Dans ce laboratoire, vous utilisez la documentation réseau pour identifier et résoudre les problèmes de communication réseau.

- **Utiliser diverses techniques et outils pour identifier les problèmes de connectivité.**
- **Utilisez la documentation pour guider les efforts de dépannage.**
- **Identifier les problèmes spécifiques au réseau.**
- **Mettre en œuvre des solutions aux problèmes de communication en réseau.**
- **Vérifier le fonctionnement du réseau.**

- **Contexte/scénario**

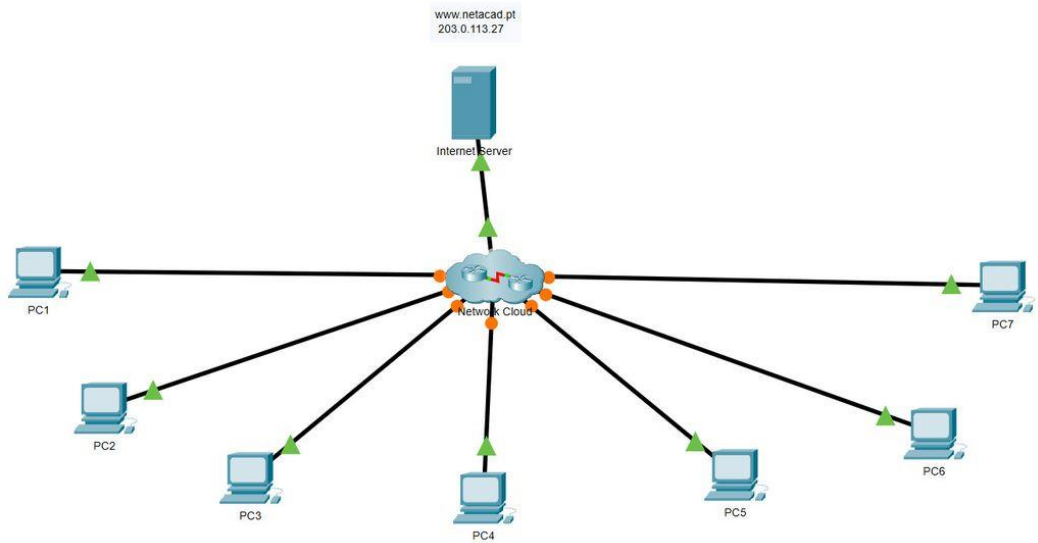
Dans cette activité, vous utiliserez la documentation que vous avez créée dans le **Packet Tracer - Épreuve de dépannage - Documentez l'activité réseau** pour guider les efforts de dépannage réseau.

Il a été découvert que le réseau avec lequel vous avez travaillé dans l'activité PT précédente a développé des problèmes de communication. Certains hôtes ne peuvent pas effectuer de ping sur d'autres hôtes et le serveur Internet. Il est de votre travail de déterminer quels sont les problèmes et de les localiser et de les réparer.

Des problèmes de réseau peuvent exister dans n'importe quel périphérique. Assurez-vous de vérifier les erreurs complètes:

- Configurations d'adressage
- Activation d'interface
- Routage
- NAT

- **Topologie**



PARTIE 6

Activité 3 : Épreuve de dépannage - Utilisation de la documentation pour résoudre des problèmes Packet Tracer

Table d'adressage

Appareil	Interface	Type de périphérique (routeur, commutateur, hôte)	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC1					
PC2					
PC3					
PC4					
PC5					
PC6					
PC7					

Instructions

Les mots de passe pour tous les appareils sont VTY: **cisco**, Enable secret: **class**

Partie 1: Évaluer la connectivité

Tous les hôtes devraient être en mesure de ping les uns les autres et le serveur Internet. Déterminez si cette exigence est respectée. Si ce n'est pas le cas, déterminez quels hôtes et réseaux devraient faire l'objet d'une étude plus approfondie.

Partie 2: Appareils d'accès réseau

À partir des hôtes qui ont des problèmes de communication, utilisez les outils ICMP pour déterminer où ces problèmes peuvent se trouver dans le réseau. À partir des ordinateurs hôtes, accédez aux périphériques du réseau et affichez les configurations et l'état opérationnel.

Partie 3: Dépanner le réseau

Après avoir localisé les problèmes, reconfigurez les périphériques pour résoudre le problème de connectivité. Utilisez la documentation de l'activité précédente pour vous aider.

Partie 4: Documenter les problèmes

Enregistrez vos problèmes dans le tableau ci-dessous.

Appareil	Problème	Action

PARTIE 6

Activité 3 : Épreuve de dépannage - Utilisation de la documentation pour résoudre des problèmes Packet Tracer

Réponses

- **Table d'adressage**

Device	Interface	Device Type (router, switch, host)	IP Address	Subnet Mask	Default Gateway
PC1	NIC	host	192.168.1.153	255.255.255.0	192.168.1.1
PC2	NIC	host	192.168.3.50	255.255.255.0	192.168.3.1
PC3	NIC	host	192.168.4.115	255.255.255.0	192.168.4.1
PC4	NIC	host	192.168.5.83	255.255.255.128	192.168.5.1
PC5	NIC	host	192.168.5.227	255.255.255.128	192.168.5.129
PC6	NIC	host	192.168.2.48	255.255.255.224	192.168.2.33
PC7	NIC	host	192.168.2.67	255.255.255.224	192.168.2.65
Hub	G0/0/0	router	192.0.2.1	255.255.255.252	N/A
Hub	S0/1/0	router	192.168.0.1	255.255.255.252	N/A
Hub	S0/1/1	router	192.168.0.5	255.255.255.252	N/A
Hub	S0/2/0	router	192.168.0.9	255.255.255.252	N/A
Hub	S0/2/1	router	192.168.0.13	255.255.255.252	N/A
Branch-1	G0/0/0	router	192.168.1.1	255.255.255.0	N/A
Branch-1	S0/1/0	router	192.168.0.2	255.255.255.252	N/A
Branch-2	G0/0/0	router	192.168.2.33	255.255.255.224	N/A
Branch-2	S0/1/0	router	192.168.0.6	255.255.255.252	N/A
Factory	G0/0/0	router	192.168.3.1	255.255.255.0	N/A
Factory	G0/0/1	router	192.168.4.1	255.255.255.0	N/A
Factory	S0/1/0	router	192.168.0.14	255.255.255.252	N/A
HQ	G0/0/0.1	router	192.168.6.1	255.255.255.0	N/A
SW-HQ3	VLAN 1	switch	192.168.6.254	255.255.255.0	192.168.6.1
HQ	G0/0/0.5	router	192.168.5.1	255.255.255.128	N/A
HQ	G0/0/0.10	router	192.168.5.129	255.255.255.128	N/A
HQ	S0/1/0	router	192.168.0.10	255.255.255.252	N/A
SW-B1	VLAN 1	switch	192.168.1.252	255.255.255.0	192.168.1.1
SW-B2	VLAN 1	switch	192.168.2.62	255.255.255.0	192.168.2.1
SW-F1	VLAN 1	switch	192.168.3.252	255.255.255.0	192.168.3.1
SW-F2	VLAN 1	switch	192.168.4.252	255.255.255.0	192.168.4.1
SW-HQ1	VLAN 1	switch	192.168.6.252	255.255.255.0	192.168.6.1
SW-HQ2	VLAN 1	switch	192.168.6.253	255.255.255.0	192.168.6.1

- **Remarque :**

Il y a cinq problèmes dans le réseau. Les étudiants doivent commencer par les hôtes, envoyer un ping à la passerelle par défaut, puis utiliser la trace ICMP pour déterminer où se trouve l'interruption du chemin de communication. Ils doivent ensuite utiliser Telnet, leur documentation et CDP pour accéder à divers périphériques sur le chemin. Ils doivent utiliser les commandes show appropriées pour afficher la configuration et le fonctionnement des périphériques sur le chemin afin de localiser les problèmes.

- **Problème 1 :**

PC1 peut envoyer un ping à sa passerelle par défaut et à certains autres périphériques du réseau, mais il ne peut pas envoyer de ping au serveur Internet. Des tests supplémentaires révèlent que certains autres PC peuvent atteindre le serveur. Cela indique que le problème est probablement lié au chemin emprunté par PC1 pour accéder à Internet. Une trace indique que les paquets n'atteignent que le routeur Hub.

- **Solution 1 :**

PARTIE 6

Activité 3 : Épreuve de dépannage - Utilisation de la documentation pour résoudre des problèmes Packet Tracer

Réponses

Les étudiants doivent Telnet à l'interface la plus proche du routeur Hub et inspecter sa configuration. Là, l'étudiant découvrira que l'instruction de configuration ip nat inside est absente de l'interface qui connecte le routeur Hub au routeur Branch-1. Cette instruction doit être ajoutée à la configuration et PC1 doit maintenant pouvoir accéder au serveur Internet.

Sur PC1, accédez à l'invite de commande, entrez : telnet 192.168.1.1, mot de passe cisco

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
User Access Verification
Password:
Branch-1>en Password:
Branch-1#telnet 192.168.0.1
Trying 192.168.0.1 ...Open
User Access Verification
Password:
Hub>en
Password:
Hub#config ter
Hub(config)#interface s0/1/0
Hub(config-if)#ip nat inside
```

- **Problème 2 :**

PC3 ne peut pas envoyer de ping au serveur Internet. De plus, on constate qu'il ne peut pas cingler sa passerelle ou d'autres appareils sur le réseau.

Solution 2 :

Ces tests indiquent que le problème vient soit de la passerelle, soit du PC lui-même. L'examen de l'adressage IP du PC3 montre que l'adressage est correct. De plus, un voyant de liaison vert s'allume sur le PC, de sorte que la liaison entre le PC et le commutateur LAN est active. Les étudiants doivent savoir, d'après leur documentation, que le PC 2 est connecté au routeur d'usine, tout comme le PC3. Étant donné que PC3 ne peut pas envoyer de ping à sa passerelle, l'étudiant doit établir une connexion Telnet entre PC2 et le routeur pour inspecter sa configuration. On constatera que l'interface Gigabit Ethernet 0/0/1 du routeur d'usine est arrêtée. L'activation de l'interface doit permettre à PC3 de n'envoyer un ping qu'aux hôtes directement connectés.

Sur PC2, telnet au routeur d'usine via la passerelle par défaut :

```
C:\>telnet 192.168.3.1
Trying 192.168.3.1 ...Open
User Access Verification
Password: cisco
Factory>enable
Password: class
Factory#show ip int brief
Interface              IP-Address    OK?   Method                    Status     Protocol
GigabitEthernet0/0/0   192.168.3.1   YES   manual                      up         up
GigabitEthernet0/0/1   192.168.4.1   YES   manual  administratively    down       down
Serial0/1/0            192.168.0.14  YES   manual                      up         up
Serial0/1/1            unassigned    YES   unset administratively      down       down
Vlan1                  unassigned    YES   unset administratively      down       down
Factory#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Factory(config)#interface g0/0/1 Factory(config-if)#no shutdown
```

Activité 3 : Épreuve de dépannage - Utilisation de la documentation pour résoudre des problèmes Packet Tracer

Réponses

Problème 3 :

Même après l'activation de l'interface LAN pour PC3, aucun périphérique ne peut envoyer de ping à PC3, à l'exception de PC2, qui est directement connecté au routeur d'usine. De même, PC3 ne peut envoyer de ping à aucun périphérique sur d'autres réseaux.

Solution 3 :

L'inspection de la configuration du routeur d'usine indique que la déclaration de réseau OSPF pour le réseau local PC3, 192.168.4.0/24, est manquante. L'ajout de cette instruction réseau restaure la connectivité vers et depuis le réseau local.

```
Factory(config)#router ospf 10
Factory(config-router)#network 192.168.4.0 0.0.0.255 area 0
```

Problème 4 :

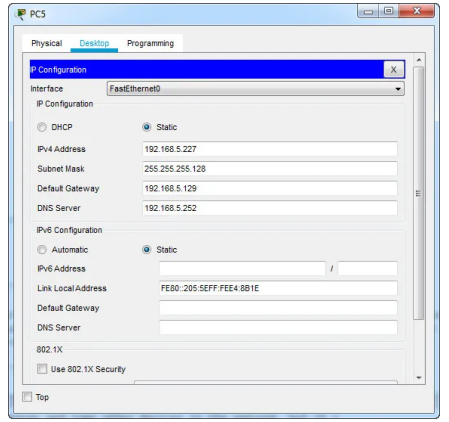
Il s'avère que le PC5 ne peut pas cingler sa passerelle. Cependant, il ne peut pas cingler d'autres PC sur le réseau ou le serveur Internet.

Solution 4 :

Alors qu'il est tentant d'aller directement au routeur passerelle pour rechercher le problème. l'inspection de l'adressage du PC5 montre qu'il lui manque son adresse de passerelle par défaut. L'ajout de cette adresse résout le problème. L'adresse doit être disponible dans la documentation du réseau ou en accédant au routeur HQ à partir d'un autre PC disposant d'une connectivité.

Sur PC4, telnet au routeur HQ via la passerelle par défaut :

```
C:\>telnet 192.168.5.1
Trying 192.168.5.1 ...Open
User Access Verification
Password:
HQ>enable
Password:
HQ#show ip int brief
Interface                  IP-Address      OK?     Method                 Status     Protocol
GigabitEthernet0/0/0       unassigned      YES      unset                   up         up
GigabitEthernet0/0/0.1     192.168.6.1     YES      manual                  up         up
GigabitEthernet0/0/0.5     192.168.5.1     YES      manual                  up         up
GigabitEthernet0/0/0.10    192.168.5.129   YES      manual                 up         up
GigabitEthernet0/0/1       unassigned      YES    unset administratively    down       down
Serial0/1/0                192.168.0.10    YES      manual                  up         up
Serial0/1/1                unassigned      YES      unset administratively   down       down
Vlan1                     unassigned      YES      unset                   up         down
```



PARTIE 6

Activité 3 : Épreuve de dépannage - Utilisation de la documentation pour résoudre des problèmes Packet Tracer

Réponses

Problème 5 :

PC6 et PC7 peuvent envoyer un ping à leurs adresses de passerelle par défaut et entre eux, mais ne peuvent pas envoyer de ping au serveur Internet. En fait, le routeur de passerelle par défaut renvoie un message d'inaccessibilité de l'hôte de destination, ce qui signifie généralement qu'une route vers le réseau de destination n'est pas connue du routeur de passerelle.

Solution 3 :

Le résultat du ping indique que le routeur de passerelle par défaut, Branch-2, n'a probablement pas de route pour atteindre le serveur Internet. Les étudiants ont peut-être remarqué après avoir affiché des tables de routage sur d'autres routeurs qu'une route par défaut est distribuée via OSPF. L'étudiant doit accéder au routeur de passerelle par défaut et afficher la table de routage. Les étudiants doivent voir qu'aucune route n'a été reçue via OSPF, y compris la route par défaut. Après avoir inspecté la configuration de l'appareil, il apparaît que l'OSPF est correctement configuré. Par conséquent, le problème doit être lié au lien sur lequel le routeur aurait dû recevoir les mises à jour OSPF. L'inspection indique que l'adresse IP de l'interface S0/1/0 est mal configurée. L'adresse doit être changée en 192.168.0.6/30. Cela restaurera la connectivité de la couche 3 avec le routeur concentrateur et permettra la réception des mises à jour OSPF.

On **PC6**, telnet to **Branch-2** Router through Default gateway:

```
C:\>telnet 192.168.2.33
Trying 192.168.2.33 ...Open
User Access Verification
Password:
Branch-2>en
Password:
Branch-2#conf t
Branch-2(config)#int s0/1/0
Branch-2(config-if)#ip address 192.168.0.6 255.255.255.252
```

PARTIE 6

PARTIE 6

Mettre en place une solution VOIP

Dans ce module, vous allez :

- Etre capable de Configurer et mettre en œuvre d'une solution VOIP

5heures

TP 1

Implémenter la solution de communication unifiée Cisco

Compétences visées :

- Virtualiser les réseaux
- Automatiser les réseaux

Recommandations clés:

- Lire attentivement l'énoncé et les questions
- Se référer au cours

5 heures

TP 1

Implémenter la solution de communication unifiée Cisco

1. Configuration de Call Manager Express

Critères de réussite :

- Le stagiaire est-il capable de :
  - Configurer le CME ?
- Réponses correctes pour au moins 70 % des questions.

Activité 1 Mettre en œuvre une infrastructure TOIP - Packet Tracer

- **Objectifs**

- **Partie 1: Préparer le réseau pour la prise en charge de la voix**
- **Partie 2: Configuration du Call Manager Express sur le routeur**
- **Partie 3: Vérifier et Expérimenter le bon fonctionnement.**

- **Contexte/scénario**

Nous allons configurer un réseau simple embarquant le VoIP (Voice over Internet Protocol). Le réseau comportera également un serveur DHCP qui servira a distribué une IP à chaque terminal du réseau.

- **Ressources requises**

Nous aurons donc besoin d'une typologie simple avec :

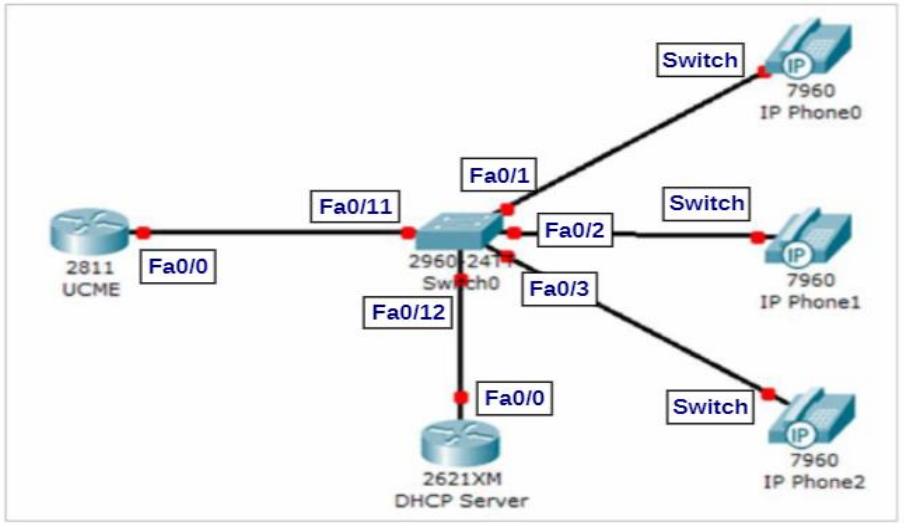
Trois téléphones IP (dans la catégorie « End Devices », choisir l'équipement « IPPhone ») : il s'agit d'une simulation des modèles 7960.

Un commutateur 2960, sur lequel on connectera le port « commutateur » de chaque téléphone : il s'agit d'une simulation du modèle 2960-24TT

Un routeur 2811 qui jouera le rôle d'UCME

Un routeur 2621XM qui jouera le rôle de serveur DHCP pour les téléphones IP

- **Topologie**



- **Instructions**

Partie 1: Préparer le réseau pour la prise en charge de la voix

data center (DC) existants.

Etape 1: Configuration de DHCP

Configuration de l'interface FastEthernet 0/0 du Router et création du serveur DHCP.

PARTIE 7

Activité 1 Mettre en œuvre une infrastructure TOIP - Packet Tracer

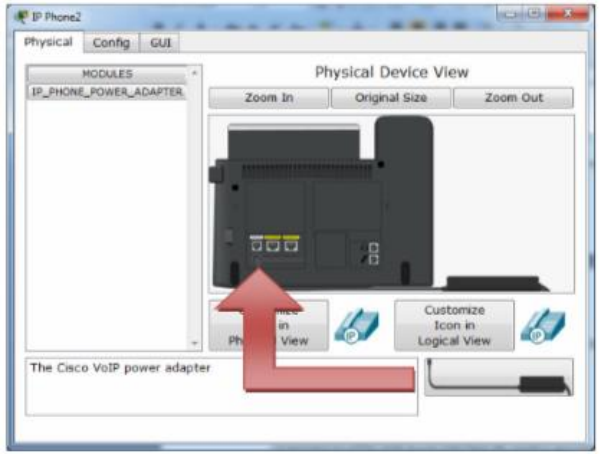
a. Configuration de l'interface Fa 0/0, avec l'adresse 172.16.5.2/24

b. Configuration du serveur DHCP

Puis nous créons et configurons le serveur DHCP utilisé pour distribué une adresse IP à chaque terminal IP du réseau.

- Exclure les adresses .1 à .5 (du réseau 192.168.2.0 /24) de la distribution DHCP

Ensuite nous allons démarrer les IP Phones, en cliquant dessus nous allons brancher l'adaptateur secteur afin de l'alimenter



Etape 2: Configuration de VLAN Voice sur le switch

Nous allons configurer les interfaces du Switch afin de séparer les données (transferts de fichiers par exemple) et les communications.

a. Déclarer les Vlan sur le switch

b. Configurer les ports sur lesquels sont connectés les téléphones IP

c. Configurer le port 12 sur lequel est connecté le serveur DHCP pour les téléphones

d. Configurer le port 11 sur lequel est connecté le routeur UCME

Partie 2: Configuration du Call Manager Express sur le routeur

Etape 1 : Activer le service de la téléphonie

Nous allons donc configurer Call Manager Express afin d'activer le support VoIP sur notre réseau.

Max-dn: max number of phone lines

Max-ephone: max number of telephones

Auto assign: enregistrer automatiquement les téléphones 1 a 5

Etape 2 : Configurer les téléphones sur CME

Les téléphones sont connectés et le réseau configuré, seulement il faut ajouter une configuration supplémentaire afin de leur permettre de communiquer. Il faut donc leur assigner un numéro de téléphone afin de les mettre en relation.

a. Déclarer les numéros de téléphone

Activité 1 Mettre en œuvre une infrastructure TOIP - Packet Tracer

b. Associer les numéros de téléphone aux téléphones IP

NB : Notre version de Packet Tracer ne permet pas d'associer plusieurs boutons ; la dernière commande, qui aurait pour vocation de définir une 2 ème ligne, échoue donc :

Partie 3: Vérifier et Expérimenter le bon fonctionnement.

Etape 1: Vérification de la configuration

a: Vérifier la configuration des téléphones

b: vérifier la configuration sur l'UCME

Etape 2: Expérimenter le bon fonctionnement

Maintenant que votre réseau basique est configuré, nous allons nous assurer que le tout fonctionne correctement. Commençons par passer un appel depuis l'IP-phone1 vers le l'IP-phone2.

a: Sur l'IP-phone1, on tape le n° à 4 chiffres : 5003, associé dans notre cas à l'IP-phone2, puis entrée

b: Décrocher sur l'IP-Phone2 et tenter d'appeler un n° de téléphone depuis l'IP-Phone0

Activité 1 Mettre en œuvre une infrastructure TOIP - Packet Tracer

Réponses

Partie 1 / Etape 1 :

a:

```
Router> enable
Router# conf t
Router(config)# int fa0/0
Router(config-if)# ip addr 172.16.5.2 255.255.255.0
Router(config-if)# no shut
Router(config-if)# exit
```

b:

```
Router(config)# ip dhcp excluded-address 172.16.5.1 172.16.5.5
Router(config)# ip dhcp pool PHONES
Router(dhcp-config)# network 172.16.2.0 255.255.255.0
Router(dhcp-config)# default-router 172.16.5.1
Router(dhcp-config)# option 150 ip 172.16.5.1
```

Partie 1 / Etape 2 :

a:

```
Switch> enable Switch# conf t
Switch(config)# vlan 5
Switch(config-vlan)# name PHONES
Switch(config-vlan)# vlan 10
Switch(config-vlan)# name DATA
Switch(config-vlan)# exit
Switch(config)#
```

b:

```
Switch(config)# int range fa 0/1-3
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# switchport voice vlan 5 // pour les flux VOIX
Switch(config-if-range)# exit
Switch(config)#
```

c:

```
Switch(config)# int fa 0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 5
```

d:

```
Switch(config)# int fa 0/11
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)#
```

PARTIE 7

Activité 1 Mettre en œuvre une infrastructure TOIP - Packet Tracer

Réponses

Partie 2 / Etape 1 :

Router(config)# **telephony-service**
Router(config-telephony)# **max-dn 10**
// Nombre d'entrées maximum dans l'annuaire (1 à 144)
Router(config-telephony)# **max-ephones 5**
// Nombre maximum de téléphones IP (1 à 42)
Router(config-telephony)# **ip source-address 172.16.5.1 port 2000**
// Définit l'adresse IP du serveur de téléphonie (UCME)
// et le port utilisés par les téléphones
Router(config-telephony)# **exit**

Partie 2 / Etape 2 :

a:

Router(config)# **ephone-dn 1**
Router(config-ephone-dn)# **number 5001**
Router(config)# **ephone-dn 2**
Router(config-ephone-dn)# **number 5002**
Router(config)# **ephone-dn 3**
Router(config-ephone-dn)# **number 5003**
Router(config)# **ephone-dn 4**
Router(config-ephone-dn)# **number 5004**
Router(config-ephone-dn)# **exit**

b:

Router(config)# **ephone 1**
Router(config-ephone)# **button 1:1**
Router(config)# **ephone 2**
Router(config-ephone)# **button 1:2**
Router(config)# **ephone 3**
Router(config-ephone)# **button 1:3**
Router(config-ephone)# **button 2:4**
Router(config-ephone)# **exit**

Partie 3 / Etape 1 :

a: Router**# show ephone**

```
Router#sh ephone

ephone-1 Mac:0050.0FCC.10CE TCP socket:[1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0    keepalive 43 max_line 2
 button 1: dn  CH1   DOWN

ephone-2 Mac:00D0.BC39.33DE TCP socket:[1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0    keepalive 43 max_line 2
 button 1: dn  CH1   DOWN

ephone-3 Mac:00E0.B024.857B TCP socket:[1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0    keepalive 43 max_line 2
 button 1: dn  CH1   DOWN
Router#
```

On a bien 3 téléphones qui ont cherché leur configuration, mais ne l'ont pas trouvé. Ils sont donc déclarés **UNREGISTERED**

Activité 1 Mettre en œuvre une infrastructure TOIP - Packet Tracer

Réponses

b: Router# **show ephone**

```
Router#sh ephone

ephone-1 Mac:0050.0FCC.10CE TCP socket:[1] activeLine:0 REGISTERED in SCCP ver 1
2 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging
IP:172.16.5.6 1431 7960   keepalive 43 max_line 2
 button 1: dn 1  number 5001 CH1   IDLE

ephone-2 Mac:00D0.BC39.33DE TCP socket:[1] activeLine:0 REGISTERED in SCCP ver 1
2 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:172.16.5.8 1476 7960   keepalive 43 max_line 2
 button 1: dn 2  number 5002 CH1   IDLE

ephone-3 Mac:00E0.B024.857B TCP socket:[1] activeLine:0 REGISTERED in SCCP ver 1
2 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:172.16.5.7 1426 7960   keepalive 43 max_line 2
 button 1: dn 3  number 5003 CH1   IDLE
Router#
```

Chaque téléphone a bien le statut **REGISTERED**

Le bouton 1 est bien associé à une entrée de l'annuaire (ici dn = 3) et un numéro d'extension ou ligne (ici 5003)

L'adresse IP de l'IP-phone est également mémorisée par le manager.

a:

*Le téléphone appelant se décroche et une indication de sonnerie (**Ring Out**) apparaît sur l'écran.*

*Sur le téléphone cible, la lumière clignote et le n° de l'appelant s'inscrit (**From : 5001**).*

b:

*Lorsque l'on décroche, on passe à l'état connecté : **Connected** s'inscrit sur l'écran.*

*Si on tente d'appele un des deux autres postes depuis IP-Phone0, ça « sonne » occupé : **Busy** s'incrit sur l'écran.*

- **Partie 3 / Etape 2 :**

PARTIE 7