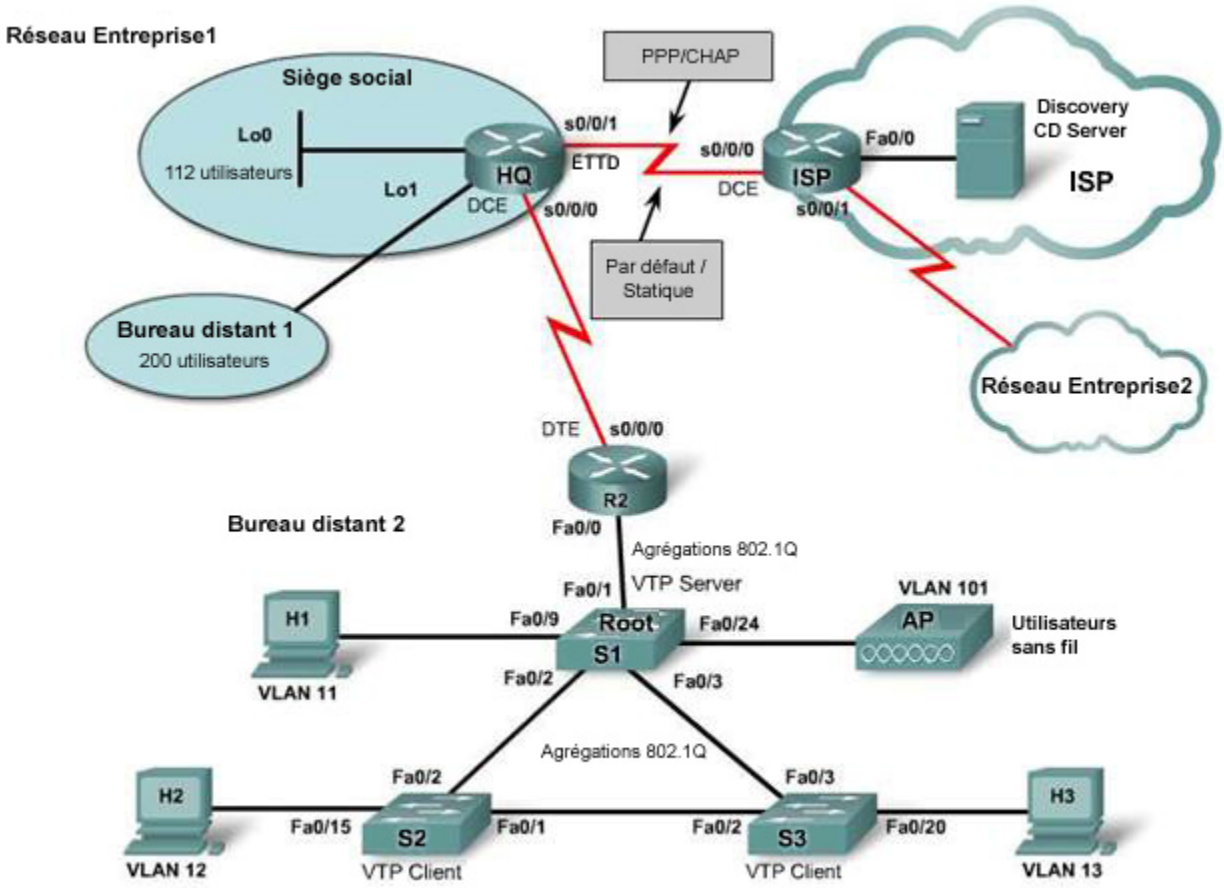
Résumé des travaux pratiques 10.0.1 : Mise en pratique



Objectifs

Partie A

- Analyser le bon de commande du client et concevoir le réseau proposé
- Créer un schéma d'adressage IP VLSM

Partie B

- Créer un réseau multicouche et établir une connexion à un fournisseur de services Internet simulé
- Configurer les paramètres de base sur des commutateurs gérant plusieurs réseaux locaux virtuels et le protocole VTP
- Configurer le pont racine STP
- Configurer les paramètres de base sur des routeurs et le routage entre réseaux locaux virtuels
- Vérifier la connectivité de base, la configuration des périphériques et les fonctionnalités

Partie C

- Configurer plusieurs routeurs utilisant le protocole OSPF, la traduction d'adresses de port (PAT) et une route par défaut
- Configurer une liaison de réseau étendu utilisant le protocole et l'authentification PPP
- Configurer plusieurs commutateurs avec la sécurité des ports
- Configurer des listes de contrôle d'accès pour contrôler l'accès au réseau et sécuriser les routeurs
- Vérifier la connectivité, la configuration des périphériques et les fonctionnalités

Contexte / Préparation

La société AnyCompany ouvre une nouvelle filiale (Remote Office 2) et vous a contacté pour étendre son réseau à son nouveau site. La direction de la société a également décidé qu'il s'agissait d'une excellente opportunité pour restructurer le réseau existant de façon à améliorer la sécurité et les performances.

Le réseau existant se compose du siège social, avec 112 employés, et d'un bureau commercial (Remote Office 1), avec 200 employés. Le nouveau bureau (Remote Office 2) accueillera quatre groupes d'employés, mais il s'étendra au fur et à mesure de la croissance de la société. Pour cette raison, vous mettrez en œuvre des réseaux locaux virtuels pour faciliter la gestion du trafic. Vous utiliserez également le protocole VTP qui simplifie la gestion des réseaux locaux virtuels. Un groupe du nouveau bureau, le personnel commercial, a besoin d'un accès sans fil au réseau de l'entreprise. Comme la sécurité est une préoccupation primordiale, le réseau sans fil doit se trouver sur un réseau local virtuel dédié.

Initialement, le réseau de Remote Office 2 sera composé de cinq réseaux locaux virtuels.

Ces travaux pratiques sont axés sur la configuration du routeur Cisco 1800 et du commutateur Cisco 2960, ou d'un matériel comparable, à l'aide de commandes Cisco IOS. Les informations de ces travaux pratiques s'appliquent à d'autres routeurs et commutateurs ; cependant, la syntaxe des commandes peut varier. Les interfaces peuvent être différentes en fonction du modèle de routeur. Par exemple, sur certains routeurs, Serial 0 peut être Serial 0/0 ou Serial 0/0/0 et Ethernet 0 peut être FastEthernet 0/0.

Il est recommandé de travailler en équipes de trois participants. Chaque participant peut être responsable d'un des trois commutateurs et de son PC hôte associé. L'équipe peut collaborer pour configurer les deux routeurs de la société.

Ressources requises :

- Un routeur ISP doté d'une interface série et d'une interface FastEthernet (préconfiguré par le formateur)
- Trois commutateurs Ethernet 2960 (ou comparables) pour le réseau local de Remote Office 2
- Deux routeurs 1841 (ou d'autres routeurs), dont un est doté d'une interface FastEthernet et l'autre de deux interfaces série
- Un point d'accès sans fil (facultatif)
- Un commutateur Ethernet 2960 pour connecter les PC filaires
- Trois PC sous Windows XP remplissant la fonction de clients filaires
- Un serveur Discovery CD Server préconfiguré par le formateur (facultatif si une interface de bouclage se trouve sur le routeur ISP)
- Câbles droits et croisés de catégorie 5
- Deux câbles série ETTD/DCE pour les liaisons de réseau étendu
- Bon de commande du fournisseur de services Internet (inclus dans ces travaux pratiques)

Partie A – Examen du bon de commande et développement du schéma de sous-réseau VLSM

Tâche 1 : examen du bon de commande du client et du réseau proposé

Vous avez reçu le bon de commande ci-dessous de votre responsable chez le fournisseur de services Internet. Examinez le bon de commande pour comprendre les grandes lignes de ce qui doit être réalisé pour le client.

ABC-XYZ-ISP Inc.

Bon de commande officiel

Client : AnyCompany1 ou AnyCompany2 **Date :** _____

(Entourez le nom du client que vous a affecté votre formateur)

Adresse : 1234 Fifth Street, Anytown

Contact client : Fred Pennypincher, Chief Financial Officer

Téléphone : 123-456-7890

Description du travail à effectuer

Examinez la topologie proposée pour le réseau au début des travaux pratiques. Le réseau existant comprend Headquarters (HQ) et Remote Office 1 (RO1). Vous devez configurer le routeur HQ, créer le réseau de Remote Office 2 (RO2) et le connecter au routeur HQ. Le matériel du réseau RO2 se compose d'un routeur 1841 supplémentaire, de trois nouveaux commutateurs 2960 et d'un point d'accès sans fil (PA). Le réseau RO2 utilise des réseaux locaux virtuels pour séparer les services, une batterie de serveurs et des utilisateurs sans fil. Le routeur RO2 relie les réseaux locaux virtuels et achemine le trafic au routeur HQ qui le transfère au routeur ISP. Le routeur HQ doit utiliser une adresse statique pour communiquer avec le routeur ISP. L'adresse IP de l'interface série du routeur ISP est :

_____

Si HQ est connecté à ISP en tant qu'AnyCompany1, l'adresse IP de l'interface Serial 0 du routeur ISP est 209.165.201.1/30.

Si HQ est connecté à ISP en tant qu'AnyCompany2, l'adresse IP de l'interface Serial 1 du routeur ISP est 209.165.202.129/30.

La liaison série vers le nouveau fournisseur de services Internet utilise l'encapsulation PPP avec l'authentification CHAP et des routes statiques. Le protocole de routage OSPF est utilisé entre les routeurs HQ et RO2 et l'encapsulation entre ces routeurs sur la liaison de réseau étendu est de type HDLC. Les routes provenant du réseau RO2 doivent être résumées et annoncées au routeur HQ.

Vous devez développer un schéma d'adressage VLSM qui englobe les réseaux existants HQ et RO1, ainsi que le nouveau réseau RO2.

Affecté à :

Guy Netwiz

Approuvé par :

Bill Broadband, ISP Manager

Tâche 2 : développement du schéma du réseau

REMARQUE : demandez au formateur de vérifier votre travail à chaque étape de cette tâche avant de passer à la Tâche 3.

Étape 1 : calcul de la taille du bloc d'adresses CIDR affecté

a. Une adresse réseau CIDR a été affectée au client : _____

Si le client est AnyCompany1, utilisez l'adresse 172.20.0.0/22.

Si le client est AnyCompany2, utilisez l'adresse 172.20.4.0/22.

b. Combien d'adresses IP d'hôtes ce bloc d'adresses représente-t-il au total ?

_____

En utilisant ce bloc d'adresses, vous allez développer un schéma d'adressage VLSM qui permet à AnyCompanyX de prendre en charge les réseaux existants HQ et RO1, ainsi que le nouveau réseau RO2.

Étape 2 : calcul de la taille de chaque bloc VLSM pour accueillir les utilisateurs

a. D'après l'adresse CIDR affectée par le fournisseur de services Internet et le nombre d'utilisateurs dans chaque zone ou dans chaque réseau local virtuel, optimisez le découpage en sous-réseaux de ce bloc d'adresses de façon à offrir suffisamment d'adresses pour tous les bureaux (HQ, RO1 et RO2) et les réseaux locaux virtuels.

b. Pour commencer, déterminez la taille du bloc d'adresses de sous-réseau nécessaire à une zone du réseau ou à un groupe d'utilisateurs. Remplissez le tableau à l'aide de ces informations. Examinez le nombre d'utilisateurs dans chaque zone ou sous-réseau et déterminez la plus petite puissance de 2 qui remplit cette condition. Par exemple, si 93 adresses sont indispensables, un bloc VLSM de 128 adresses (2^7) est nécessaire. L'autre puissance de 2 la plus proche est 64 (2^6) qui ne remplit pas la condition voulue. Un bloc de 128 adresses comporte des adresses inutilisées mais offre des adresses de réserve utilisables par la suite.

Zone réseau	**Nombre d'utilisateurs / Adresses IP**	**Taille du bloc d'adresses VLSM / Nb d'adresses (puissances de 2)**
Réseau HQ	112	
Réseau RO1	200	
Réseau RO2 / Réseaux locaux virtuels		
VLAN 1 (batterie de serveurs)	18 utilisateurs	
VLAN 2 (natif/gestion -IP)	9 utilisateurs	
VLAN 11 (Dept 1)	75 utilisateurs	
VLAN 12 (Dept 2)	112 utilisateurs	
VLAN 13 (Dept 3)	38 utilisateurs	
VLAN 101 (sans fil)	52 utilisateurs	
Liaison de réseau étendu (RO2 vers HQ)	2	
Nombre total d'utilisateurs et tailles des blocs pour RO2	306	
Taille du bloc RO2 à répartir	N/D	
Nombre total d'utilisateurs et tous les blocs VLSM	618	

c. Pour une affectation optimale des adresses provenant de l'adresse CIDR /22, commencez par trier les tailles des blocs de la plus grande à la plus petite. Pour ces travaux pratiques, ajoutez tous les blocs de petite taille pour chaque réseau local virtuel du réseau RO2 et affectez un seul bloc plus important qui englobe tous les petits blocs et remplit leurs conditions. Cela rassemble tous les petits sous-réseaux de RO2 et facilite le résumé du routage. Utilisez le tableau ci-dessous afin de trier les zones réseau par taille de bloc VLSM. Indiquez d'abord le gros bloc de l'ensemble du réseau RO2, puis les autres. Le bloc RO2 le plus important sera divisé par la suite en sous-réseaux plus petits.

Zone réseau / VLAN	**Taille du bloc VLSM en commençant par le plus important**
Taille totale du bloc RO2 (sera divisé en blocs de plus petite taille)	
Réseau RO1	
Réseau HQ	
RO2 - VLAN 11 (Dept 1)	
RO2 - VLAN 12 (Dept 2)	
RO2 - VLAN 13 (Dept 3)	
RO2 - VLAN 101 (sans fil)	
RO2 - VLAN 1 (batterie de serveurs)	
RO2 - VLAN 2 (natif/gestion -IP)	
RO2 - Liaison de réseau étendu HQ	

Étape 3 : définition des adresses de sous-réseau du bloc CIDR

a. Déterminez les blocs d'adresses CIDR à affecter à chaque zone du réseau ou du réseau local virtuel. Utilisez le tableau des sous-réseaux VLSM (Annexe A) pour entrer les informations sur les sous-réseaux pour chaque bloc CIDR.

b. Pour déterminer les adresses de sous-réseau du bloc CIDR 172.20.0.0/22 ou 172.20.4.0/22, utilisez l'outil de calcul du site Web Cisco Network Academy. Dans cet outil de calcul, entrez l'adresse de base du réseau (172.20.0.0 ou 172.20.4.0) et la valeur du masque 1 VLSM en notation décimale à point, en commençant à 255.255.252.0 (/22). Cliquez sur le bouton d'action **Calculate Subnetting using VLSM** (Calculer les sous-réseaux utilisant VLSM). Utilisez la même adresse de base et augmentez la longueur du masque d'une unité à chaque fois pour remplir le graphique.

REMARQUE : les entrées des numéros des sous-réseaux pour les masques /29 et /30 ne figurent pas dans le tableau. Répartissez un des masques /28 dans le masque /30 pour la liaison de réseau étendu.

Étape 4 : affectation de blocs d'adresses à chaque zone du réseau

a. Remplissez le tableau ci-dessous d'après les informations de sous-réseau du tableau des sous-réseaux CIDR/VLSM et le tableau trié des conditions minimales pour les adresses. Entourez chaque bloc du tableau d'adresses ci-dessus, ou coloriez-les, et repérez chacun en fonction de la zone réseau ou du réseau local virtuel auquel il est affecté.

Zone réseau / VLAN	Taille du bloc VLSM (nombre d'adresses)	Préfixe et adresse de sous-réseau	Plage d'adresses utilisable	Masque de sous-réseau
Taille totale du bloc RO2 (sera divisé en blocs de plus petite taille)				
RO2 – VLAN 11 (Dept 1)				
RO2 – VLAN 12 (Dept 2)				
RO2 – VLAN 13 (Dept 3)				
RO2 – VLAN 101 (sans fil)				
RO2 – VLAN 1 (batterie de serveurs)				
RO2 – VLAN 2 (natif/gestion – IP)				
RO2 – Liaison de réseau étendu				
Réseau RO1				
Réseau HQ				

b. Demandez au formateur de vérifier que votre modèle d'adressage est correct et qu'il affecte l'espace d'adressage de manière efficace. Aucun sous-réseau ne doit se chevaucher avec un autre ; les blocs d'adresses doivent être contigus et comporter des adresses de réserve utilisables au fur et à mesure de la croissance de la société.

Tâche 3 : définition des adresses IP à utiliser pour les interfaces des périphériques

Étape 1 : sélection des adresses IP à utiliser pour la configuration des périphériques

Sélectionnez des adresses dans le bloc affecté à une zone du réseau et indiquez l'adresse IP et le masque de sous-réseau à utiliser pour chaque périphérique/interface de la topologie. Ces adresses IP seront utilisées par la suite dans la Partie C lors de la configuration du matériel du réseau.

REMARQUE : lorsque vous avez terminé cette tâche, demandez au formateur de la vérifier avant de continuer.

Tableau d'interfaces / adresses IP de périphériques

Périphérique	Interface	Adresse IP	Masque de sous-réseau
HQ	Serial 0/0/0		
	Serial 0/0/1		
	Loopback0 (HQ)		
	Loopback1 (RO1)		
R2	Serial 0/0/0		
	FastEthernet 0/0		
	Sous-interface Fa0/0.1		
	Sous-interface Fa0/0.2		
	Sous-interface Fa0/0.11		
	Sous-interface Fa0/0.12		
	Sous-interface Fa0/0.13		
	Sous-interface Fa0/0.101		
ISP	Serial 0/0/0	209.165.201.1 (AnyCompany1) ou 209.165.202.129 (AnyCompany2)	255.255.255.252
S1 (RO2)	VLAN 2		
S2 (RO2)	VLAN 2		
S3 (RO2)	VLAN 2		
H1	Carte réseau		
H2	Carte réseau		
H3	Carte réseau		

Étape 2 : demandez au formateur de vérifier votre travail avant de passer à la Partie B.

Partie B – Élaboration physique du réseau et configuration de base des périphériques

Tâche 1 : construction physique du réseau et connexion des câbles aux interfaces et aux ports indiqués

Connectez le réseau du routeur du siège social de AnyCompanyX (HQ) au routeur ISP. Le routeur ISP et le serveur Discovery Server doivent être préconfigurés par le formateur. Si le routeur ISP est configuré avec une adresse de bouclage à la place du serveur Discovery CD Server, le serveur HTTP doit être activé dans le routeur. En cas de doute, demandez à votre formateur.

REMARQUE : assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration de démarrage. Les instructions d'effacement et de rechargement de la mémoire du commutateur et du routeur figurent dans la section Tools du site Academy Connection.

REMARQUE : Routeurs SDM – Si la configuration initiale (startup-config) est effacée dans un routeur SDM, le gestionnaire SDM ne s'affiche plus par défaut lorsque le routeur est redémarré. Il est alors nécessaire de définir une configuration de base de routeur à l'aide des commandes IOS. La procédure indiquée dans ces travaux pratiques utilise des commandes IOS et ne nécessite pas l'utilisation de SDM. Si vous voulez utiliser SDM, reportez-vous aux instructions du Manuel de travaux pratiques que vous pouvez télécharger depuis la section Tools du site Academy Connection. Consultez votre formateur si besoin.

Les adresses IP utilisées pour configurer les périphériques dans les tâches suivantes doivent être basées sur votre solution pour le schéma VLSM.

REMARQUE : Messages d'erreur de correspondance des réseaux locaux virtuels - Vous voudrez peut-être attendre que les commutateurs soient configurés pour connecter les liaisons des tronçons. Sinon, les messages d'erreur de correspondance des réseaux locaux virtuels natifs s'affichent tant que tous les commutateurs ne sont pas configurés.

Tâche 2 : configuration du routeur HQ

Étape 1 : configuration du nom de l'hôte HQ, des mots de passe, de l'absence de recherche de domaines et du message du jour

Étape 2 : configuration des interfaces série et de bouclage de HQ

La liaison WAN de HQ vers R2 utilise l'encapsulation HDLC Cisco par défaut.

La liaison WAN de HQ vers ISP utilise le protocole PPP avec authentification CHAP.

Étape 3 : création d'un ID utilisateur et d'un mot de passe CHAP

Définissez un nom d'utilisateur pour le routeur ISP sur le routeur HQ avec le mot de passe **cisco** à utiliser avec l'authentification CHAP.

Étape 4 : enregistrement de la configuration en cours du routeur (running-config) dans la configuration initiale (startup-config)

Étape 5 : copie et enregistrement de la configuration en cours (running-config) du routeur dans un éditeur de texte pour l'utiliser plus tard le cas échéant

a. Ouvrez un éditeur de texte tel que le Bloc-notes Windows.

b. Exécutez la commande **`show running-config`**.

c. Copiez le résultat et collez-le dans l'éditeur de texte.

d. Enregistrez le fichier sur le Bureau Windows sous le nom **HQ.txt**.

Tâche 3 : configuration du routeur R2 de Remote Office 2

Étape 1 : configuration du nom de l'hôte R2, des mots de passe, de l'absence de recherche de domaines et du message du jour

Étape 2 : configuration des sous-interfaces FastEthernet et des interfaces série de RO2

a. Il est plus facile de dépanner les sous-interfaces FastEthernet si les numéros correspondent aux numéros des réseaux locaux virtuels qu'elles représentent. Elles doivent également utiliser l'encapsulation 802.1Q.

b. Le réseau local virtuel VLAN 2 est le VLAN natif.

c. La liaison WAN de HQ vers R2 utilise l'encapsulation HDLC Cisco par défaut.

Étape 3 : enregistrement de la configuration en cours du routeur (running-config) dans la configuration initiale (startup-config)

Étape 4 : copie et enregistrement de la configuration en cours (running-config) du routeur dans un éditeur de texte pour l'utiliser plus tard le cas échéant

a. Ouvrez un éditeur de texte tel que le Bloc-notes Windows.

b. Exécutez la commande **`show running-config`**.

c. Copiez le résultat et collez-le dans l'éditeur de texte.

d. Enregistrez le fichier sur le Bureau Windows sous le nom **R2.txt**.

REMARQUE : si vous avez besoin de ce fichier par la suite, vous devrez le modifier pour le nettoyer et vérifier que la commande **`no shutdown`** est appliquée aux interfaces nécessaires.

Tâche 4 : configuration du commutateur S1 de Remote Office 2

REMARQUE : assurez-vous d'effacer startup-config, de supprimer le fichier vlan.dat et de recharger le commutateur avant de commencer la configuration.

Étape 1 : configuration du nom de l'hôte S1, des mots de passe, de l'absence de recherche de domaines et du message du jour

Étape 2 : configuration des réseaux locaux virtuels de Remote Office 2 sur S1 en utilisant les numéros et les noms figurant dans le tableau ci-dessous

Affectez des ports à chaque réseau local virtuel conformément aux indications. Utilisez le même tableau pour configurer les commutateurs S2 et S3 :

Numéro du réseau local virtuel RO2	Nom du VLAN	Ports affectés	Remarques
VLAN 1 (VLAN par défaut)	default	Ports 4-5	VLAN 1 ne peut pas être renommé
VLAN 2 (natif/gestion – IP)	Mgmnt	Port 23	
VLAN 11 (utilisateurs du service 1)	Dept1	Ports 6 à 11	
VLAN 12 (utilisateurs du service 2)	Dept2	Ports 12 à 17	
VLAN 13 (utilisateurs du service 3)	Dept3	Ports 18 à 22	
VLAN 101 (sans fil)	Wireless	Port 24	

Étape 3 : affectation d'une adresse IP au réseau local virtuel Management 2 sur S1

a. Affectez l'adresse du réseau local virtuel 2 d'après le Tableau Interfaces des périphériques / Adresses IP (Partie A, Tâche 3, Étape 1).

b. Configurez le commutateur avec une passerelle par défaut vers le routeur R2 pour VLAN 2.

Étape 4 : configuration des ports Fa0/1, Fa0/2 et Fa0/3 du commutateur S1 en tronçons 802.1Q

Les tronçons peuvent transmettre les informations des réseaux locaux virtuels. Configurez chaque tronçon pour utiliser le réseau local virtuel 2 (VLAN 2) comme réseau local natif.

Étape 5 : configuration de S1 comme commutateur racine pour le protocole STP

Modifiez la valeur par défaut 32769 de la priorité du réseau local virtuel 2 (VLAN 2) par la valeur 4096.

Étape 6 : configuration d'un domaine VTP

a. Définissez le nom de domaine AnyCompanyX (où X peut avoir la valeur 1 ou 2) sur S1 et le mot de passe **cisco**.

b. Configurez S1 comme le serveur VTP.

Étape 7 : enregistrement de la configuration en cours du commutateur (running-config) dans la configuration initiale (startup-config)

Étape 8 : copie et enregistrement de la configuration en cours (running-config) du commutateur dans un éditeur de texte pour l'utiliser plus tard le cas échéant

Tâche 5 : configuration du commutateur S2 de Remote Office 2

Étape 1 : configuration du nom de l'hôte S2, des mots de passe, de l'absence de recherche de domaines et du message du jour

Étape 2 : configuration du domaine VTP AnyCompanyX sur S2, S2 étant un client qui utilise le mot de passe cisco

Il n'est pas nécessaire de configurer les réseaux locaux virtuels sur S2. Du fait qu'il s'agit d'un client VTP, les informations proviennent du serveur VTP S1.

Vous devez néanmoins affecter les ports aux réseaux locaux virtuels d'après le tableau de la Partie B, Tâche 4, Étape 2.

Étape 3 : affectation d'une adresse IP au réseau local virtuel natif Management 2 sur S2

a. Utilisez l'adresse IP du Tableau Interfaces des périphériques / Adresses IP (Partie A, Tâche 3, Étape 1).

b. Configurez le commutateur avec une passerelle par défaut vers le routeur R2 pour VLAN 2.

Étape 4 : configuration des ports Fa0/1 et Fa0/2 du commutateur en tant que tronçons 802.1Q pour transmettre les informations VLAN

Étape 5 : enregistrement de la configuration en cours du commutateur (running-config) dans la configuration initiale (startup-config) et copie dans un éditeur de texte pour l'utiliser plus tard le cas échéant

Tâche 6 : configuration du commutateur S3 de Remote Office 2

Étape 1 : configuration du nom de l'hôte S3, des mots de passe, de l'absence de recherche de domaines et du message du jour

Étape 2 : configuration du domaine VTP AnyCompanyX sur S3 en mode client avec le mot de passe cisco

En mode client, il n'est pas nécessaire de configurer les réseaux locaux virtuels sur S3 car les informations proviennent du serveur VTP S1.

Vous devez néanmoins affecter les ports aux réseaux locaux virtuels d'après le tableau de la Partie B, Tâche 4, Étape 2.

Étape 3 : affectation d'une adresse IP au réseau local virtuel natif Management 2 sur S3

a. Utilisez l'adresse IP du Tableau Interfaces des périphériques / Adresses IP (Partie A, Tâche 3, Étape 1).

b. Configurez le commutateur avec une passerelle par défaut vers le routeur R2 pour VLAN 2.

Étape 4 : configuration des ports Fa0/2 et Fa0/3 du commutateur en tant que tronçons 802.1Q pour transmettre les informations VLAN

Étape 5 : enregistrement de la configuration en cours du commutateur (running-config) dans la configuration initiale (startup-config)

Étape 6 : copie et enregistrement de la configuration en cours (running-config) du commutateur dans un éditeur de texte pour l'utiliser plus tard le cas échéant

Tâche 7 : configuration des adresses IP hôtes

Étape 1 : configuration de chaque adresse IP hôte et du masque de sous-réseau

Utilisez les informations figurant dans le Tableau Interfaces des périphériques / Adresses IP (Partie A, Tâche 3, Étape 1).

Étape 2 : configuration de la passerelle par défaut

Utilisez les informations des réseaux locaux virtuels pour déterminer la passerelle par défaut pour chaque hôte. Il s'agit de l'adresse de la sous-interface de R2 figurant dans le Tableau Interfaces des périphériques / Adresses IP (Partie A, Tâche 3, Étape 1).

Tâche 8 : vérification des configurations des périphériques et de la connectivité de base

Étape 1 : avant de passer aux travaux pratiques de la Partie C, vérifiez que les périphériques sont correctement configurés

Vérifiez la connectivité de base entre les périphériques de AnyCompanyX. Vérifiez les points suivants et indiquez les commandes que vous avez utilisées :

Point à vérifier	Commande utilisée
Configuration de base de HQ (nom de l'hôte, mots de passe, etc.)	
Configuration de base de R2 (nom de l'hôte, mots de passe, etc.)	
Configuration de base de S1 (nom de l'hôte, mots de passe, etc.)	
Configuration de base de S2 (nom de l'hôte, mots de passe, etc.)	
Configuration de base de S3 (nom de l'hôte, mots de passe, etc.)	
Sous-interfaces créées sur Fa0/0 pour R2	
Encapsulation correcte sur les sous-interfaces de R2	
Réseaux locaux virtuels créés sur chaque commutateur	
Ports dans les réseaux locaux virtuels corrects sur chaque commutateur	
Le réseau local virtuel natif est VLAN 2	
Les ports corrects sont des tronçons 802.1Q sur chaque commutateur	
S1 est le commutateur racine	
S1 est le serveur VTP	
S2 est un client VTP	
S3 est un client VTP	
Envoi d'un requête ping à S1 à partir de H1, H2 et H3	
Envoi d'un requête ping à S2 à partir de H1, H2 et H3	
Envoi d'un requête ping à S3 à partir de H1, H2 et H3	
Envoi d'une requête ping à la passerelle par défaut R2 à partir de H1, H2 et H3	
Envoi d'une requête ping à la passerelle par défaut R2 à partir de S1, S2 et S3	
Envoi de requêtes ping à partir de H1 vers H2 et H3 (entre les réseaux locaux virtuels)	
Ping de HQ vers R2	

Partie C – Configuration de la sécurité du routage, des listes de contrôle d'accès et des commutateurs

Tâche 1 : configuration du routage pour HQ et R2

Étape 1 : configuration du processus OSPF 1 pour la zone 0 sur R2

Spécifiez le sous-réseau pour chaque interface R2 à l'aide du masque générique approprié.

Étape 2 : configuration du processus OSPF 1 pour la zone 0 sur HQ

Étape 3 : exécution de la commande `show ip route` sur HQ pour connaître la table de routage

Combien de routes OSPF ont-elles été signalées à partir de R2 ? _____

Étape 4 : configuration d'une route par défaut vers le fournisseur de services Internet et propagation vers R2 en utilisant le protocole OSPF

Étape 5 : vérification de l'apprentissage par R2 de la route par défaut configurée sur HQ

Exécutez la commande **`show ip route`** sur R2.

Quelle est la passerelle de dernier recours de R2 ? _____

Étape 6 : enregistrement de la configuration en cours du routeur (running-config) dans la configuration initiale (startup-config)

Tâche 2 : configuration d'une NAT surchargée (PAT) sur HQ

Étape 1 : configuration d'une NAT surchargée (PAT) sur HQ

a. Utilisez l'adresse IP sur le port série qui assure la connexion à ISP en tant qu'adresse surchargée.

b. Indiquez les interfaces NAT internes et externes.

Étape 2 : envoi d'une requête ping à l'adresse Serial 0/0/0 du routeur ISP (209.165.201.1 pour AnyCompany1 ou 209.165.201.129 pour AnyCompany2) à partir de l'invite de commandes du PC Hôte H1

La commande a-t-elle été exécutée correctement ? _____

Étape 3 : ouverture d'un navigateur sur l'hôte H1 et saisie de l'adresse IP de l'interface Serial 0/0/0 du routeur ISP (209.165.201.1)

Avez-vous pu accéder à l'interface HTTP au moyen du navigateur ? _____

Étape 4 : exécution de la commande `show ip nat translations` sur le routeur HQ

```
HQ#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.201.2:512 172.20.0.2:512     209.165.201.1:512  209.165.201.1:512
tcp 209.165.201.2:1072 172.20.0.2:1072    209.165.201.1:80   209.165.201.1:80
```

Pour la saisie du test ping (icmp), quelle est l'adresse locale interne et le numéro du port ?

_____

Pour la saisie du test ping (icmp), quelle est l'adresse globale interne et le numéro du port ?

_____

Pour la saisie de la connexion du navigateur (tcp), quelle est l'adresse locale interne et le numéro du port ?

_____

Pour la connexion du navigateur (tcp), quelle est l'adresse locale externe et le numéro du port ? _____

Étape 5 : enregistrement de la configuration du routeur dans la mémoire vive non volatile

Tâche 3 : configuration de la sécurité des ports pour les commutateurs

Étape 1 : affichage de l'entrée de Fa0/9 dans la table des adresses MAC

Il s'agit du port auquel H1 est connecté. Exécutez la commande **`show mac-address-table int f0/9`**. Vous devrez peut-être envoyer une requête ping du PC au commutateur ou à une autre destination pour actualiser l'entrée dans la table des adresses.

```
S1#show mac-address-table int f0/9
          Mac Address Table

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  11    000b.db04.a5cd    DYNAMIC     Fa0/9
Total Mac Addresses for this criterion: 1
```

Étape 2 : avant de configurer la sécurité d'un port, suppression de l'entrée de l'adresse MAC apprise dynamiquement à l'aide de la commande `clear mac-address-table dynamic interface command`

Étape 3 : avant de configurer la sécurité d'un port, désactivation du port et exécution des commandes de sécurité des ports

a. La commande **`switchport port-security mac-address sticky`** permet au commutateur d'apprendre l'adresse MAC actuellement associée au port. Cette adresse est intégrée à la configuration en cours. Si la configuration en cours (running-config) est enregistrée dans la configuration de démarrage (startup-config), l'adresse MAC est conservée lorsque le commutateur est rechargé.

b. La commande **`switchport port-security`** active la sécurité du port avec les paramètres par défaut suivants : 1 adresse MAC et **`shutdown`** comme action en cas de violation. Exécutez la commande **`no shutdown`** pour réactiver le port de façon qu'il apprenne l'adresse MAC du PC.

Étape 4 : envoi d'une requête ping de H1 à la passerelle par défaut VLAN 11

Laissez s'écouler quelque temps et exécutez la commande **`show running-config`** pour connaître l'adresse MAC que le commutateur a apprise.

Étape 5 : affichage de la sécurité du port Fa0/9 à l'aide de la commande `show port-security interface`

Quel est l'état du port ? _____

Quel est le nombre de violations de la sécurité ? _____

Quelle est l'adresse source:Vlan ? _____

```
S1#show port-security int fa0/9
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 000b.db04.a5cd:11
Security Violation Count   : 0
```

Étape 6 : retrait du câble du PC H1 du port Fa0/9 du commutateur et connexion du câble provenant du PC H2

a. Envoyez une requête ping de H2 à n'importe quelle adresse IP pour provoquer une violation de la sécurité sur le port Fa0/9. Vous devez recevoir des messages de violation de la sécurité.

b. Exécutez à nouveau la commande **`show port-security interface`** sur Fa0/9.

Quel est l'état du port ? _____

Quel est le nombre de violations de la sécurité ? _____

Quelle est l'adresse source:Vlan ? _____

Étape 7 : remise en place des câbles des PC sur leurs ports d'origine et restauration du port Fa0/9

a. Effacez l'entrée de l'adresse rémanente du port Fa0/9.

b. Pour rétablir l'interface de `error disable` à `administratively up`, entrez la commande **`shutdown`** suivie de la commande **`no shutdown`**.

Étape 8 : enregistrement de la configuration en cours du commutateur (running-config) dans la configuration initiale (startup-config)

Étape 9 : recommencez les étapes 1 à 6 pour configurer la sécurité des ports des deux autres commutateurs, S2 et S3, et enregistrez la configuration en cours (running-config) dans la configuration initiale (startup-config)

Tâche 4 : vérification de la connectivité globale du réseau avant d'appliquer les listes de contrôle d'accès

Étape 1 : avant de configurer les listes de contrôle d'accès, vérification du routage, de la traduction des adresses du réseau (NAT) et de la connectivité de base pour AnyCompanyX et le fournisseur de services Internet

Étape 2 : vérification des points suivants et indication des commandes utilisées

Point à vérifier	Commande utilisée
Configuration du routage de HQ (OSPF/statique)	
Configuration du routage de R2 (OSPF/statique/résumé)	
Surcharge NAT sur HQ	
Sécurité des ports des commutateurs S1, S2 et S3	
Test ping de H1, H2 et H3 vers HQ S0/0/0	
Test ping de H1, H2 et H3 vers HQ Lo0 (réseau local HQ)	
Test ping de H1, H2 et H3 vers HQ Lo1 (réseau local RO1)	
Test ping de H1, H2 et H3 vers ISP S0/0/0	
Test ping de H1, H2 et H3 vers ISP Discovery CD Server	
Navigateur Web de H1, H2 et H3 vers la boucle de routage ISP ou l'adresse Discovery CD Server	
Connexion Telnet de H1, H2 et H3 vers HQ et R2	

Tâche 5 : configuration de la sécurité ACL sur HQ et R2

REMARQUE : les commandes suivantes sont basées sur les plages d'adresses IP comme solution possible au schéma VLSM au cours des travaux pratiques. Remplacez les plages d'adresses par celles qui correspondent à celles que vous avez appliquées aux hôtes de Remote Office 2 et aux réseaux locaux virtuels.

Étape 1 : création et application de la liste de contrôle d'accès étendue au routeur de périphérie (HQ)

a. La liste de contrôle d'accès répond aux demandes des hôtes internes pour entrer dans le réseau. Autorisez les utilisateurs internes à envoyer des commandes **`ping`** ou **`trace`** vers n'importe quel emplacement sur Internet, mais n'autorisez pas l'accès par ces commandes aux personnes extérieures à l'entreprise.

b. Appliquez la liste de contrôle d'accès à l'interface NAT externe du routeur HQ de façon à protéger le réseau AnyCompanyX.

c. Testez la liste de contrôle d'accès : envoyez une requête ping de H1, H2 et H3 à l'adresse de bouclage du routeur ISP ou à l'adresse IP du serveur Discovery CD Server.

   La requête ping a-t-elle abouti ? _____

d. À l'aide d'un navigateur sur H1, H2 et H3, entrez l'adresse Loopback0 du routeur ISP ou l'adresse IP du serveur Discovery CD Server.

   Avez-vous pu accéder à l'interface Web sur le routeur ou à la page Web à partir du serveur ?

   _____

Étape 2 : création et application d'une liste de contrôle d'accès nommée étendue sur R2

a. La liste de contrôle d'accès autorise les requêtes sur le Web et les tests ping à quitter le réseau Remote Office 2 s'ils proviennent des réseaux locaux virtuels 1, 11, 12, 13 ou 101. Le trafic Telnet est autorisé s'il provient du réseau local virtuel 12 ; le trafic FTP est autorisé s'il provient du réseau local virtuel VLAN 13. Tout autre trafic est refusé.

b. Sur le routeur R2, appliquez la liste de contrôle d'accès à chaque sous-interface de Fa0/0 à l'exception de Fa0/0.2 qui est le réseau local virtuel natif.

c. Testez la liste de contrôle d'accès : envoyez une requête ping de H1, H2 et H3 à l'adresse de bouclage du routeur ISP ou à l'adresse IP du serveur Discovery CD Server.

   La requête ping a-t-elle abouti ? _____

d. À l'aide d'un navigateur sur H1, H2 et H3, entrez l'adresse Loopback0 du routeur ISP ou l'adresse IP du serveur Discovery CD Server.

   Avez-vous pu accéder à l'interface Web sur le routeur ou à la page Web à partir du serveur ?

   _____

e. Établissez une connexion Telnet de l'hôte H1 de VLAN 11 vers le routeur HQ en utilisant son adresse IP S0/0/0.

   Avez-vous pu vous ouvrir une connexion telnet vers le routeur ? _____

f. Établissez une connexion Telnet de l'hôte H2 de VLAN 12 vers le routeur HQ en utilisant son adresse IP S0/0/0.

   Avez-vous pu vous ouvrir une connexion Telnet vers le routeur ? _____

g. Utilisez la commande **`show access-lists`** pour vérifier que la liste de contrôle d'accès fonctionne.

Étape 3 : création et application d'une liste de contrôle d'accès standard pour contrôler l'accès VTY au routeur HQ

a. La liste de contrôle d'accès doit refuser les hôtes de tous les réseaux locaux virtuels de Remote Office 2 à l'exception de l'hôte H2 sur VLAN 12. Cela autorise toujours les autres hôtes sur VLAN 12 à accéder au routeur R2 par une connexion Telnet.

b. Appliquez la liste de contrôle d'accès aux lignes VTY de 0 à 4 sur le routeur R2.

c. Établissez une connexion Telnet de l'hôte H2 de VLAN 12 vers le routeur HQ en utilisant son adresse IP S0/0/0.

   Avez-vous pu vous ouvrir une connexion Telnet vers le routeur ? ___

d. Changez l'adresse IP de H2 et donnez-lui une autre valeur appartenant à VLAN 12 ; ouvrez à nouveau une connexion Telnet de l'hôte H2 de VLAN 12 vers le routeur HQ en utilisant son adresse IP S0/0/0.

   Avez-vous pu vous ouvrir une connexion Telnet vers le routeur ? ___

e. Utilisez la commande **`show access-lists`** pour vérifier le fonctionnement des listes de contrôle d'accès.

Étape 4 : enregistrement sur R2 et HQ de la configuration des routeurs dans la mémoire vive non volatile

Résumé des interfaces des routeurs				
Modèle du routeur	Interface Ethernet 1	Interface Ethernet 2	Interface série 1	Interface série 2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (Fa0)	FastEthernet 1 (Fa1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (Fa0/0)	FastEthernet 0/1 (Fa0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
REMARQUE : pour connaître la configuration exacte du routeur, consultez les interfaces. Vous pourrez ainsi identifier le type du routeur, ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. En revanche, le tableau fournit les identifiants des combinaisons d'interfaces possibles pour chaque périphérique. Ce tableau d'interfaces ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans une commande IOS.				

ANNEXE A

Tableau de sous-réseau CIDR / VLSM

Adresse de base : 172.20.0.0		Masque de sous-réseau : 255.255.252.0							
Masque CIDR	**/22**	**/23**	**/24**	**/25**	**/26**	**/27**	**/28**	**/29**	**/30**
Masque dot (octets 3&4)	**252.0**	**254.0**	**255.0**	**255.128**	**255.192**	**255.224**	**255.240**	**255.248**	**255.252**
Aucun hôte possible	**1,024**	**512**	**256**	**128**	**64**	**32**	**16**	**8**	**4**
N° de sous-réseau (octets 3 & 4)									

Adresse de base : 172.20.0.0		**Masque de sous-réseau : 255.255.252.0**							

