Exercice PT 8.6.1 : exercice d'intégration des compétences de CCNA

Diagramme de topologie

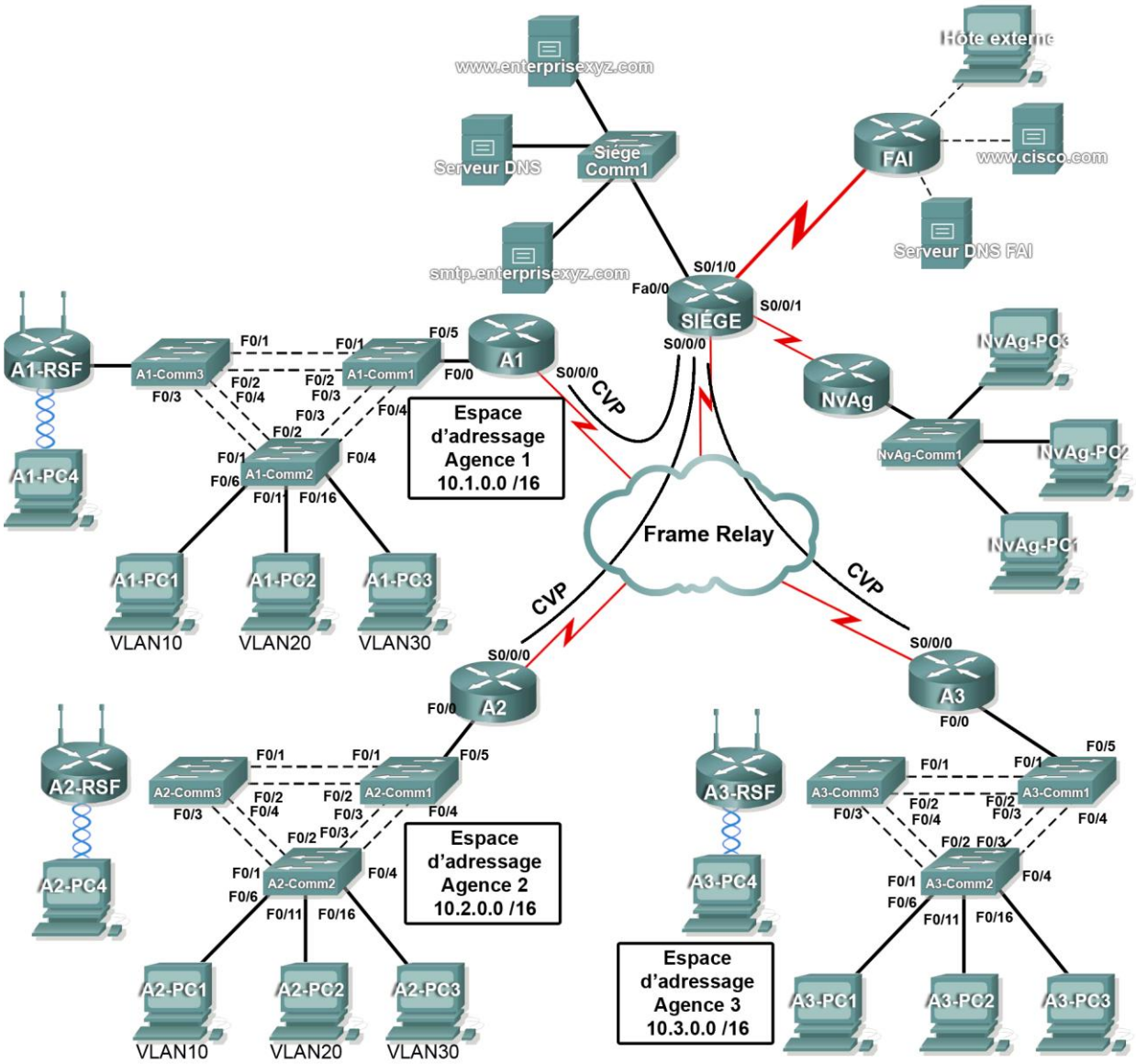

Table d'adressage de SIÈGE

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Mappages DLCI
SIÈGE	Fa0/0	10.0.1.1	255.255.255.0	N/D
	S0/0/0.41	10.255.255.1	255.255.255.252	DLCI 41 à A1
	S0/0/0.42	10.255.255.5	255.255.255.252	DLCI 42 à A2
	S0/0/0.43	10.255.255.9	255.255.255.252	DLCI 43 à A3
	S0/0/1	10.255.255.253	255.255.255.252	N/D
	S0/1/0	209.165.201.1	255.255.255.252	N/D

Table d'adressage des routeurs Agence

Périphérique	Interface	Adresse IP	Masque de sous-réseau
AX	Fa0/0.10	10.X.10.1	255.255.255.0
	Fa0/0.20	10.X.20.1	255.255.255.0
	Fa0/0.30	10.X.30.1	255.255.255.0
	Fa0/0.88	10.X.88.1	255.255.255.0
	Fa0/0.99	10.X.99.1	255.255.255.0
	S0/0/0	2^{e} adresse	255.255.255.252
AX-Comm1	VLAN 99	10.X.99.21	255.255.255.0
AX-Comm2	VLAN 99	10.X.99.22	255.255.255.0
AX-Comm3	VLAN 99	10.X.99.23	255.255.255.0
AX-RSF	VLAN 1	10.X.40.1	255.255.255.0

- Remplacez « X » par le numéro du routeur Agence (A1, A2 ou A3).
- Les circuits virtuels permanents point-à-point avec SIÈGE utilisent la seconde adresse du sous-réseau. SIÈGE utilise la première adresse.
- Les routeurs WRT300N obtiennent l'adresse Internet par le protocole DHCP auprès du routeur Agence.

Mappages de port et configuration des réseaux locaux virtuels

Numéro du VLAN	Adresse réseau	Nom du VLAN	Mappages de port
10	10.X.10.0/24	Admin	AX-Comm2, Fa0/6
20	10.X.20.0/24	Ventes	AX-Comm2, Fa0/11
30	10.X.30.0/24	Production	AX-Comm2, Fa0/16
88	10.X.88.0/24	SansFil	AX-Comm3, Fa0/7
99	10.X.99.0/24	Gestion&Natif	Toutes les agrégations

Objectifs pédagogiques

- Configurer le protocole Frame Relay dans une topologie en étoile « hub-and-spoke »
- Configurer le protocole PPP avec authentification PAP et CHAP
- Configurer la fonction NAT statique et dynamique
- Configurer le routage par défaut et statique

Présentation

Au cours de cet exercice faisant appel à vos compétences CCNA, la société XYZ utilise une combinaison des protocoles Frame Relay et PPP pour les connexions du réseau étendu. Le routeur SIÈGE fournit un accès à la ferme de serveurs et à Internet via la fonction NAT. SIÈGE utilise également une liste de contrôle d'accès pare-feu de base pour filtrer le trafic entrant. Chaque routeur Agence est configuré pour un routage entre réseaux locaux virtuels et pour le protocole DHCP. Le routage est possible par l'intermédiaire d'EIGRP et de routes par défaut et statiques. Les réseaux locaux virtuels, le protocole VTP et le STP sont configurés sur chacun des réseaux commutés. La sécurité de port est activée et un accès sans fil est fourni. Votre tâche consiste à mettre correctement en œuvre toutes ces technologies, en faisant appel à toutes les connaissances que vous avez acquises lors des quatre cours d'Exploration, résumées dans cet exercice.

Vous êtes responsable de la configuration du routeur SIÈGE et des routeurs A1, A2 et A3. Vous devez également configurer chaque périphérique qui est relié au réseau par un routeur Agence. Le routeur NvAg représente une nouvelle agence acquise après fusion avec une entreprise de plus petite taille. Vous n'avez pas accès au routeur NvAg. Vous allez cependant établir une liaison entre SIÈGE et NvAg pour fournir à cette nouvelle agence un accès au réseau interne et à Internet.

Les routeurs et les commutateurs sous votre administration ne sont pas configurés. Aucune des configurations de base, telles que nom d'hôte, mots de passe, bannières et autres commandes générales de maintenance, n'est évaluée par Packet Tracer. Elles n'entreront donc pas dans les spécifications des tâches. Cependant, vous êtes censé les configurer, et votre formateur peut décider de les noter.

Étant donné que cet exercice fait appel à un réseau très vaste avec près de 500 composants requis pour les éléments d'évaluation, vous ne verrez pas nécessairement votre taux de réalisation augmenter à chaque fois que vous saisirez une commande. D'autre part, il ne vous sera pas demandé d'atteindre un pourcentage précis à la fin de chaque tâche. En revanche, des tests de connectivité vous permettront de vérifier la configuration de chaque tâche. Il vous est cependant possible de cliquer à tout moment sur **Check Results** pour voir si un composant particulier est noté et si vous l'avez configuré correctement.

Puisque les routeurs Agence (A1, A2 et A3) et les commutateurs sont conçus de manière modulaire, vous pouvez réutiliser des scripts. Par exemple, vos configurations pour A1, A1-Comm1, A1-Comm2 et A1-Comm3 peuvent être directement appliquées aux périphériques A2 en n'apportant que quelques ajustements.

Remarque : cette vérification d'intégration des compétences CCNA est également disponible dans une version ouverte où vous pouvez choisir le schéma d'adressage et les technologies à mettre en œuvre. Vérifiez votre configuration en testant la connectivité de bout en bout.

Tâche 1 : configuration du protocole Frame Relay dans une topologie en étoile « hub-and-spoke »

Étape 1. Configuration du cœur de Frame Relay

Utilisez les tables d'adressage et les conditions requises ci-dessous.

SIÈGE est le routeur moyeu (hub). A1, A2 et A3 sont les rayons (spokes).

- SIÈGE utilise une sous-interface point-à-point pour chacun des routeurs Agence.
- A3 doit être configuré manuellement pour utiliser une encapsulation IETF.
- Le type LMI doit être configuré manuellement comme étant q933 pour SIÈGE, A1 et A2. A3 utilise ANSI.

Étape 2. Configuration de l'interface du réseau local sur SIÈGE

Étape 3. Vérification de la capacité d'envoi de requêtes ping de SIÈGE aux routeurs Agence

Tâche 2 : configuration du protocole PPP avec authentification PAP et CHAP

Étape 1. Configuration de la liaison WAN de SIÈGE vers FAI à l'aide de l'encapsulation PPP et de l'authentification CHAP

Le mot de passe CHAP est **ciscochap**.

Étape 2. Configuration de la liaison WAN de SIÈGE vers NvAg à l'aide de l'encapsulation PPP et de l'authentification PAP

Vous devez brancher un câble aux interfaces appropriées. SIÈGE est le côté DCE de la liaison. Vous choisissez la fréquence d'horloge. Le mot de passe PAP est **ciscopap**.

Étape 3. Vérification de la capacité d'envoi de requêtes ping de SIÈGE à FAI et à NvAg

Tâche 3 : configuration de la fonction NAT statique et dynamique sur SIÈGE

Étape 1. Configuration de la fonction NAT

Utilisez les conditions requises suivantes :

- Autorisez la traduction de toutes les adresses de l'espace d'adressage 10.0.0.0/8.
- La société XYZ possède l'espace d'adressage 209.165.200.240/29. Le pool, XYZCORP, utilise les adresses .241 à .245 avec un masque /29.
- Le site Web www.entreprisexyz.com sur 10.0.1.2 est enregistré avec le système DNS public à l'adresse IP 209.165.200.246.

Étape 2. Vérification du fonctionnement de NAT par une requête ping étendue

À partir de SIÈGE, envoyez une requête ping à l'interface série 0/0/0 sur FAI en utilisant l'interface du réseau local de SIÈGE comme adresse source. Cette requête ping doit aboutir.

Vérifiez que la fonction NAT a traduit la requête ping avec la commande **show ip nat translations**.

Tâche 4 : configuration du routage par défaut et statique

Étape 1. Configuration de SIÈGE avec une route par défaut vers FAI et une route statique vers le réseau local de NvAg

Utilisez l'argument d'interface de sortie (exit interface).

Étape 2. Configuration des routeurs Agence avec une route par défaut vers SIÈGE

Utilisez l'argument d'adresse IP de saut suivant (next-hop IP address).

Étape 3. Vérification de la connectivité au-delà de FAI

Les trois PC de NvAg et le PC NetAdmin doivent être capables d'envoyer une requête ping au serveur Web www.cisco.com.

Tâche 5 : configuration du routage entre réseaux locaux virtuels

Étape 1. Configuration de chaque routeur Agence pour le routage entre réseaux locaux virtuels

À l'aide de la table d'adressage pour les routeurs Agence, configurez et activez l'interface du réseau local pour le routage entre réseaux locaux virtuels. VLAN 99 est le réseau local virtuel natif.

Étape 2. Vérification des tables de routage

Chacun des routeurs Agence doit maintenant posséder six réseaux connectés directement et une route par défaut statique.

Tâche 6 : configuration et optimisation du routage EIGRP

Étape 1. Configuration de SIÈGE, A1, A2 et A3 avec EIGRP

- Utilisez AS 100.
- Désactivez les mises à jour EIGRP sur les interfaces adéquates.
- Résumez manuellement les routes EIGRP de telle sorte que chacun des routeurs Agence annonce uniquement l'espace d'adressage 10.X.0.0/16 à SIÈGE.

Remarque : Packet Tracer ne simule pas précisément l'avantage des routes résumées EIGRP. Les tables de routage indiquent encore tous les sous-réseaux, bien que vous ayez correctement configuré le résumé manuel.

Étape 2. Vérification des tables de routage et de la connectivité

SIÈGE et les routeurs Agence doivent maintenant posséder des tables de routage complètes.

Le PC NetAdmin doit maintenant pouvoir envoyer une requête ping à chaque sous-interface du réseau local virtuel sur chaque routeur Agence.

Tâche 7 : configuration de VTP, de l'agrégation, de l'interface des VLAN et des VLAN

Les conditions requises suivantes s'appliquent aux trois agences. Configurez un ensemble de trois commutateurs. Utilisez ensuite les scripts de ces commutateurs sur les deux autres ensembles de commutateurs.

Étape 1. Configuration des commutateurs Agence avec le protocole VTP

- AX-Comm1 est le serveur VTP. AX-Comm2 et AX-Comm3 sont des clients VTP.
- Le nom de domaine est **XYZCORP**.
- Le mot de passe est **xyzvtp**.

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

Configurez les interfaces appropriées en mode d'agrégation et affectez VLAN 99 comme le réseau local virtuel natif.

Étape 3. Configuration de l'interface de réseau local virtuel et de la passerelle par défaut sur AX-Comm1, AX-Comm2 et AX-Comm3

Étape 4. Création des réseaux locaux virtuels sur AX-Comm1

Créez et nommez les réseaux locaux virtuels répertoriés dans le tableau des mappages de port et de configuration des réseaux locaux virtuels uniquement sur AX-Comm1. Le protocole VTP annonce les nouveaux réseaux locaux virtuels à AX-Comm1 et AX-Comm2.

Étape 5. Vérification de l'envoi des réseaux locaux virtuels à AX-Comm2 et AX-Comm3

Utilisez les commandes adéquates pour vérifier que Comm2 et Comm3 possèdent désormais les réseaux locaux virtuels que vous avez créés sur Comm1. Packet Tracer peut avoir besoin de quelques minutes pour simuler les annonces VTP. Une façon rapide de forcer l'envoi d'annonces VTP consiste à faire passer l'un des commutateurs du client en mode transparent puis de le faire repasser en mode client.

Tâche 8 : affectation des réseaux locaux virtuels et configuration de la sécurité de port

Étape 1. Affectation des réseaux locaux virtuels aux ports d'accès

Utilisez le tableau des mappages de port et de configuration des réseaux locaux virtuels pour remplir les conditions requises suivantes :

- Configurez les ports d'accès.
- Affectez les réseaux locaux virtuels aux ports d'accès.

Étape 2. Configuration de la sécurité des ports

Utilisez la stratégie suivante pour établir la sécurité des ports sur les ports d'accès de AX-Comm2 :

- Autorisez une seule adresse MAC.
- Configurez la première adresse MAC apprise pour correspondre à la configuration.
- Configurez le port pour qu'il se désactive en cas de violation de la sécurité.

Étape 3. Vérification des affectations des réseaux locaux virtuels et de la sécurité de port

Utilisez les commandes appropriées pour vérifier que les réseaux locaux virtuels d'accès sont correctement affectés et que la stratégie de sécurité de port a été activée.

Tâche 9 : configuration du protocole STP

Étape 1. Configuration de AX-Comm1 comme pont racine

Paramétrez le niveau de priorité à 4096 sur AX-Comm1 afin que ces commutateurs soient toujours le pont racine de tous les réseaux locaux virtuels.

Étape 2. Configuration de AX-Comm3 comme pont racine de secours

Paramétrez le niveau de priorité à 8192 sur AX-Comm3 afin que ces commutateurs soient toujours le pont racine de secours de tous les réseaux locaux virtuels.

Étape 3. Vérification que AX-Comm1 est le pont racine

Tâche 10 : configuration du protocole DHCP

Étape 1. Configuration des pools DHCP pour chaque réseau local virtuel

Sur les routeurs Agence, configurez les pools DHCP pour chaque réseau local virtuel en fonction des conditions requises suivantes :

- Excluez les 10 premières adresses IP de chaque pool pour les réseaux locaux virtuels.
- Excluez les 24 premières adresses IP de chaque pool pour les réseaux locaux sans fil.
- Le nom de pool est **AX_VLAN##** où **X** est le numéro du routeur et ## est le numéro du réseau local virtuel.
- Incluez dans la configuration DHCP le serveur DNS relié à la ferme de serveurs de SIÈGE.

Étape 2. Configuration des PC pour utiliser DHCP

Actuellement, les PC sont configurés pour utiliser des adresses IP statiques. Modifiez cette configuration en DHCP.

Étape 3. Vérification de l'existence d'adresse IP pour les PC et les routeurs sans fil

Étape 4. Vérification de la connectivité

Tous les PC physiquement reliés au réseau doivent être capables d'envoyer une requête ping au serveur Web www.cisco.com.

Tâche 11 : configuration d'une liste de contrôle d'accès pare-feu

Étape 1. Vérification de la connectivité à partir de l'hôte externe

Le PC Hôte externe doit être capable d'envoyer une requête ping au serveur sur www.entreprisexyz.com.

Étape 2. Application d'une liste de contrôle d'accès pare-feu de base

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

1. Autorisez les requêtes HTTP entrantes vers le serveur www.entreprisexyz.com.
2. Autorisez uniquement les sessions TCP établies à partir de FAI et de toute source au-delà de FAI.
3. Autorisez uniquement les réponses ping entrantes en provenance de FAI et de toute source au-delà de FAI.
4. Bloquez explicitement tout autre accès entrant à partir de FAI et de toute source au-delà de FAI.

Étape 3. Vérification de la connectivité à partir de l'hôte externe

Le PC Hôte externe ne doit pas être en mesure d'envoyer une requête ping au serveur sur www.xyzcorp. Toutefois, le PC Hôte externe doit pouvoir demander une page Web.

Tâche 12 : configuration de la connectivité sans fil

Étape 1. Vérification de la configuration de DHCP

Chaque routeur AX-RSF doit déjà posséder un adressage IP du protocole DHCP du routeur AX pour VLAN 88.

Étape 2. Configuration des paramètres de configuration réseau/réseau local

L'adresse « Router IP » (IP du routeur) à la page **Status** de l'onglet GUI doit être la première adresse IP du sous-réseau 10.X.40.0 /24. Conservez la valeur par défaut de tous les autres paramètres.

Étape 3. Configuration des paramètres du réseau sans fil

Les SSID des routeurs sont **AX-RSF_LAN** où **X** est le numéro du routeur Agence.

La clé WEP est **12345ABCDE**.

Étape 4. Configuration des routeurs sans fil pour un accès à distance

Configurez le mot de passe d'administration sur **cisco123** et activez la gestion à distance.

Étape 5. Configuration des PC de AX-PC4 pour l'accès au réseau sans fil avec DHCP

Étape 6. Vérification de la connectivité et de la capacité de gestion à distance

Chaque PC sans fil doit pouvoir accéder au serveur Web www.cisco.com.

Pour vérifier la capacité de gestion à distance, accédez au routeur sans fil via le navigateur Web.

Tâche 13 : dépannage du réseau

Étape 1. Coupure du réseau

Un participant quitte la salle, si nécessaire, pendant qu'un autre casse la configuration.

Étape 2. Détection du problème

Le participant revient et utilise les techniques de dépannage pour identifier le problème et le résoudre.

Étape 3. Nouvelle coupure du réseau

Les participants échangent les rôles et recommencent les étapes 1 et 2.