Packet Tracer : exercice d'intégration des compétences CCNA

Topologie

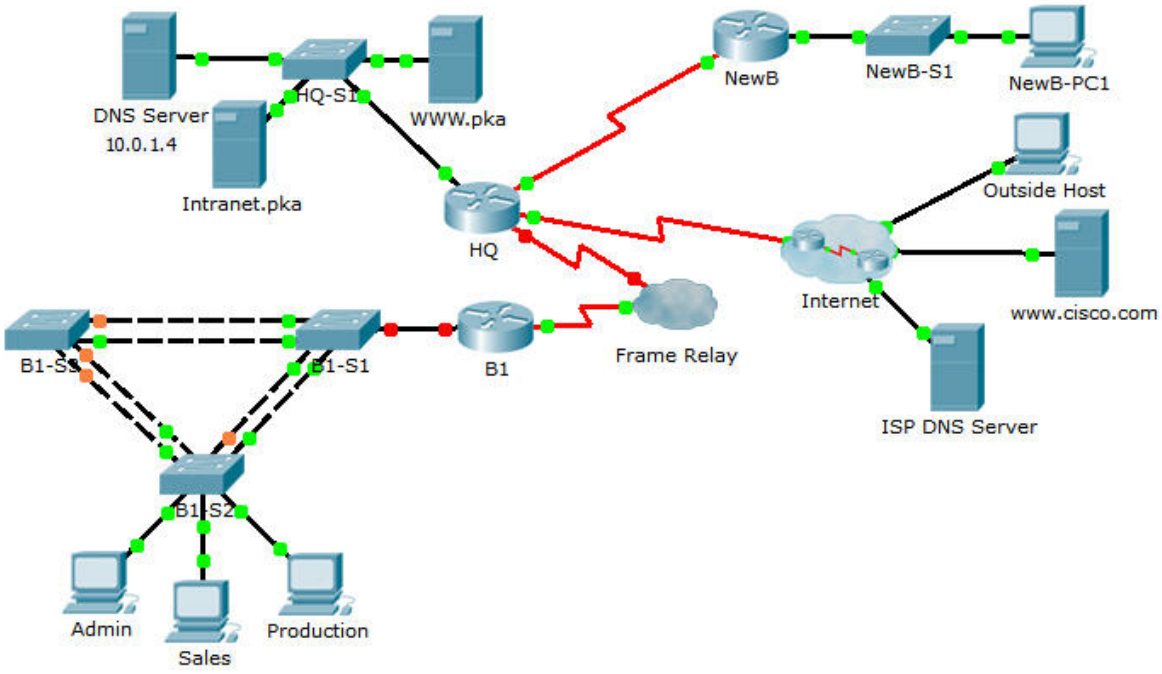

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut Mappage DLCI
HQ	G0/0	10.0.1.1	255.255.255.0	N/A
	S0/0/0.41	10.255.255.1	255.255.255.252	DLCI 41 to B1
	S0/0/1	10.255.255.253	255.255.255.252	N/A
	S0/1/0	209.165.201.1	255.255.255.252	N/A
B1	G0/0.10	10.1.10.1	255.255.255.0	N/A
	G0/0.20	10.1.20.1	255.255.255.0	N/A
	G0/0.30	10.1.30.1	255.255.255.0	N/A
	G0/0.99	10.1.99.1	255.255.255.0	N/A
	S0/0/0	10.255.255.2	255.255.255.252	N/A
B1-S2	VLAN 99	10.1.99.22	255.255.255.0	10.1.99.1

Configurations de VLAN et mappages de ports

Numéro de VLAN	Adresse réseau	Nom du VLAN	Mappages de ports
10	10.1.10.0/24	Admin	Fa0/6
20	10.1.20.0/24	Ventes	Fa0/11
30	10.1.30.0/24	Production	Fa0/16
99	10.1.99.0/24	Gestion & Natif	Fa0/1-4
999	N/A	BlackHole	Ports inutilisés

Scénario

Dans le cadre de cet exercice complet d'intégration des compétences CCNA, la société XYZ Corporation utilise les protocoles Frame Relay et PPP pour les connexions WAN. Les autres technologies incluent la fonction NAT, le protocole DHCP, le routage statique et le routage par défaut, le protocole EIGRP pour IPv4, le routage inter-VLAN et les configurations de VLAN. Les configurations de sécurité incluent SSH, la sécurité des ports, la sécurité de commutateur et les listes de contrôle d'accès.

Conditions requises

Remarque : le mot de passe du mode d'exécution utilisateur est **cisco** et le mot de passe du mode d'exécution privilégié est **class**.

SSH

- Configurez **HQ** de manière à utiliser SSH pour l'accès à distance.
  - Définissez la valeur du module à **2048**. Le nom de domaine est **CCNASkills.com**.
  - Le nom d'utilisateur est **admin** et le mot de passe est **adminonly**.
  - Seul SSH doit être autorisé sur les lignes VTY.
  - Modifiez les valeurs par défaut de SSH : version 2 ; délai d'expiration égal à 60 secondes ; deux nouvelles tentatives.

Frame Relay

- Configurez le protocole Frame Relay entre **HQ** et **B1**.
  - Référez-vous à la table d'adressage pour l'adresse IP, le masque de sous-réseau et le DLCI.
  - **HQ** utilise une sous-interface point à point et le DLCI 41 pour se connecter à **B1**.
  - Le type de LMI doit être configuré manuellement en tant que **q933a** pour **HQ** et **B1**.

PPP

- Configurez la liaison WAN depuis **HQ** vers Internet en utilisant l'encapsulation PPP et l'authentification CHAP.
  - Créez un utilisateur **ISP** avec le mot de passe **cisco**.
- Configurez la liaison WAN depuis **HQ** vers **NewB** en utilisant l'encapsulation PPP et l'authentification PAP.
  - **HQ** représente le côté DCE de la liaison. Choisissez la fréquence d'horloge.
  - Créez un utilisateur **NewB** avec le mot de passe **cisco**.

NAT

- Configurez les fonctions NAT statique et dynamique sur HQ.
  - Autorisez toutes les adresses de l'espace d'adressage 10.0.0.0/8 à traduire, en utilisant une liste d'accès standard nommée **NAT**.
  - La société XYZ est propriétaire de l'espace d'adressage 209.165.200.240/29. Le pool **HQ** utilise les adresses .241 à .245 avec un masque /29.
  - Le site Web **WWW.pka** à l'adresse 10.0.1.2 est enregistré avec le système DNS public à l'adresse IP 209.165.200.246 et doit être accessible à partir de l'**hôte externe**.

DHCP

- Sur **B1**, configurez un pool DHCP pour Sales VLAN 20 avec les spécifications suivantes :
  - Excluez les 10 premières adresses IP dans la plage.
  - Le nom de pool sensible à la casse est **VLAN20**.
  - Incluez le serveur DNS relié au LAN **HQ** comme faisant partie de la configuration DHCP.
- Configurez **Sales** PC de manière à utiliser DHCP.

Routage statique et par défaut

- Configurez **HQ** avec une route par défaut vers **Internet** et une route statique vers le LAN **NewB**. Utilisez l'argument exit interface.

Routage EIGRP

- Configurez et optimisez **HQ** et **B1** avec le routage EIGRP.
  - Utilisez le système autonome 100 et désactivez la récapitulation automatique.
  - **HQ** doit annoncer le routeur statique et par défaut à **B1**.
  - Désactivez les mises à jour EIGRP sur les interfaces adéquates.
  - Récapitulez manuellement les routes EIGRP de telle sorte que le routeur **B1** n'annonce que l'espace d'adressage 10.1.0.0/16 à **HQ**.

Routage inter-VLAN

- Configurez **B1** pour le routage inter-VLAN.
  - À l'aide de l'espace d'adressage des routeurs de filiale, configurez et activez l'interface LAN pour le routage inter-VLAN. Le réseau local virtuel VLAN 99 est le réseau local virtuel natif.

Configurations de VLAN et de trunking

- Configurez le trunking et les VLAN sur **B1-S2**.
  - Créez et nommez les VLAN énumérés dans la table **Configuration VLAN et mappages de ports** sur **B1-S2** uniquement.
  - Configurez l'interface VLAN 99 ainsi que la passerelle par défaut.
  - Attribuez des VLAN aux ports d'accès appropriés.
  - Définissez le mode de trunking à la valeur « on » pour Fa0/1 - Fa0/4.
  - Désactivez tous les ports inutilisés et attribuez le VLAN **BlackHole**.

Sécurité des ports

- Utilisez la stratégie suivante pour établir la sécurité des ports sur les ports d'accès **B1-S2** :
  - Autorisez une adresse MAC à apprendre sur le port.

- Configurez la première adresse MAC apprise afin de se conformer à la configuration.
- Configurez le port pour qu'il se désactive en cas de violation de la sécurité.

Stratégie de liste d'accès

- Étant donné que HQ est connecté à Internet, configurez une liste de contrôle d'accès nommée **HQINBOUND** en respectant l'ordre suivant :
  - Autorisez les requêtes HTTP entrantes adressées au serveur **WWW.pka**.
  - Autorisez uniquement les sessions TCP établies à partir d'Internet.
  - Autorisez uniquement les réponses ping entrantes à partir d'Internet.
  - Bloquez explicitement tous les autres accès entrants à partir d'Internet.

Connectivité

- Vérifiez la connectivité complète à partir de chaque PC vers **WWW.pka** et **www.cisco.pka.**