Cas ESN

Consciente de l'importance de modifier nos habitudes nutritionnelles et de protéger notre environnement, la société ESN a développé l'enseigne Espace Santé Nature qui offre une large gamme de produits issus de l'agriculture biologique, labellisés et contrôlés par des organismes agréés.

Le réseau commercial des boutiques Espace Santé Nature offre des produits alimentaires de consommation courante certifiés *« AB » (agriculture biologique)*, mais également des compléments alimentaires. Ces produits, dits « nutraceutiques », ont un effet physiologique bénéfique ou protecteur contre les maladies chroniques. Ils sont fabriqués à partir de substances alimentaires et sont commercialisés sous forme de comprimé, de poudre, de potion ou d'autres formes médicinales. Par ailleurs, l'enseigne propose des produits d'entretien naturels pour la maison (sans produits chimiques), des cosmétiques biologiques (crème de jour et nuit, gel douche, shampooing) et de nombreux éco-produits tels que de la vaisselle compostable, des couches pour bébés biodégradables à 100 % et non blanchies.Encouragée par l'essor du marché des nutraceutiques, la société a décidé de faire évoluer son système d'information pour accompagner le développement de son enseigne Espace Santé Nature.

Le premier objectif est d'accroître la performance du réseau informatique du siège qui centralise les ressources accessibles par l'ensemble des boutiques sur le territoire français et ponctuellement par les commerciaux itinérants.Dans un second temps, le service informatique est chargé d'enrichir le site *web* de la société de façon à y intégrer une fonctionnalité de vente en ligne associée à un paiement sécurisé. Ceci nécessite de rationaliser l'infrastructure qui accueille les informations publiques.

Les locaux du siège de la société ESN accueillent un réseau informatique d'architecture « FastEthernet », entièrement commuté et distribué sur deux bâtiments principaux (A et B). Au moment de votre collaboration, le projet d'évolution de l'architecture du réseau local est en cours de réalisation.L'ensemble des serveurs et le cœur de l'électronique active ont été migrés vers un nouveau bâtiment appelé « local technique général ». Celui-ci permet de bénéficier de locaux mieux adaptés notamment en termes de sécurité d'accès physique (utilisation de badges), de climatisation, de système anti-incendie et de tolérance aux pannes.

Dossier 1 : Évolution du réseau

Annexes à utiliser : **annexes 1, 2 et 3**

Chacun des trois bâtiments dispose d'un commutateur : CA, CB et CG (***annexe 1***). Pour gérer la tolérance aux pannes des liaisons, l'administrateur a relié les trois commutateurs entre eux en formant un circuit. Pour éviter les **tempêtes de diffusion**, il a activé le protocole 802.1d. Ce protocole utilise un algorithme d'arbre de recouvrement minimum *(spanning tree)* pour transformer un circuit en arbre. Les liaisons redondantes doivent être invalidées quand elles ne sont pas utiles et validées en cas de rupture d'une liaison. L'administrateur influe sur le choix des liaisons invalidées en pondérant chaque liaison. Les serveurs sont situés dans le local technique général. Il n'y a pas de trafic réseau entre les postes du bâtiment A et ceux du bâtiment B.

1.1 **Expliquer ce qu'est une « tempête de diffusion » et sa cause.**
1.2 Identifier le lien qui doit être invalidé par le protocole 802.1d en justifiant la réponse.

La séparation des flux entre bâtiments est assurée par la mise en place de réseaux locaux virtuels (VLAN) sur les commutateurs. Le commutateur CG dispose également d'une fonction de routage qui n'est pas activée. L'***annexe 2*** présente la configuration des réseaux virtuels et IP de la société.

1.3 **Expliquer pourquoi les ports d'interconnexion entre commutateurs doivent être étiquetés (*taggés*).**
1.4 Expliquer s'il est nécessaire d'activer le routage sur le commutateur CG pour permettre la communication entre un poste du bâtiment B et le serveur SRV-ESN.

Tous les postes obtiennent dynamiquement leur configuration IP (adresse, routeur, DNS) à partir du serveur SRV-ESN. Mais un commercial connecté avec son portable à un point d'accès sans fil du bâtiment A n'a pas pu accéder au serveur SRV-SAGE. La liaison entre le portable et le point d'accès est pourtant opérationnelle.

1.5 Définir les adresses IP des passerelles par défaut affectées aux postes fixes du bâtiment A et du bâtiment B pour aller vers Internet.
1.6 **Expliquer la cause du dysfonctionnement observé sur l'ordinateur portable.**

Afin de remplacer des serveurs de données obsolètes, on a fait l'acquisition d'un unique serveur nommé SRV-NAS plus performant, dont les caractéristiques sont présentées en ***annexe 3***. Il dispose notamment de caractéristiques matérielles permettant d'assurer la continuité d'exploitation en cas de panne.

1.7 Comparer les solutions RAID 0, RAID 1 et RAID 5 de ce serveur :
- en terme de volume utile à justifier par un calcul,
- en terme de tolérance aux pannes.
1.8 Dire quels sont les autres éléments du serveur NAS qui permettent d'assurer la continuité de service et la tolérance aux pannes.

Dossier 2 : Architecture ouverte à Internet

Annexes à utiliser : annexes 1, 2 et 4

La société ESN a mis en place un catalogue en ligne accessible à tous sur Internet. Mais elle a aussi développé pour son réseau commercial de boutiques un accès *web* permettant de passer des commandes en ligne.Les sites *web* public et privé sont installés sur le serveur SRV-3W. Ils se distinguent par des numéros de port différents (80 et 8000). Le SGBDR utilisé par le site *web* est situé sur le serveur SRV-SAGE.

Dans le cadre de son nouveau contrat d'accès à Internet, la société ESN bénéficie d'une liaison haut débit SDSL à 2 Mbps, d'une plage d'adresses IP sur le sous-réseau 217.167.171.128 de masque 255.255.255.248 et d'un nom de domaine géré par le fournisseur d'accès (**espace-sante-nature.com**).

2.1. **Justifier le choix d'une offre d'accès à Internet de type SDSL.**
2.2. Déterminer la classe, le nombre d'adresses et la plage d'adresses IP offertes par le FAI (fournisseur d'accès Internet) à ESN.

Les boutiques sont identifiées par la plage d'adresses 195.200.10.65 à 195.200.10.126 réservée auprès du FAI. **Dans un premier temps**, l'administrateur n'a pas mis en place de DMZ, il a utilisé les fonctionnalités NAT/PAT et de redirection du routeur SDSL pour rendre accessibles le site public et le site privé. Puis sur le pare-feu SRV-WALL, il a élaboré les règles de filtrage suivantes sur l'interface externe (***annexes 1 et 2 uniquement***) :

Extrait de la table de filtrage qui ne montre pas les flux bidirectionnels :

(Information sur les ports utilisables : DNS (53), HTTP site public (80), HTTP site privé (8000), SMTP (25), POP3 (110) et SGBDR (3306), tous(ports > 1024))

N°	Source		Destination		Décision
	IP	Port	IP	Port	
…	**….**	**…**	**…**	**…**	**…**
20	**Toutes**	**Tous**	**192.168.0.7/32**	**80**	**Accepter**
30	**Toutes**	**Tous**	**192.168.0.7/32**	**8000**	**Accepter**
40	Toutes	Tous	192.168.0.9/32	25	Accepter
41	Toutes	Tous	192.168.0.9/32	110	Accepter
Défaut	Toutes	Tous	Toutes	Tous	Bloquer

2.3. Donner la signification de la règle n° 20.
2.4. Donner la signification de la règle n° 30 et expliquer pourquoi cette règle ne répond pas précisément aux contraintes d'accès.

Dans un deuxième temps, l'administrateur a décidé de créer une zone démilitarisée (DMZ) pour améliorer la sécurité des accès Internet (***annexe 4***). Les deux interfaces du routeur SDSL sont configurées avec l'adresse IP 217.167.171.126 sur l'interface externe et 217.167.171.133 sur l'interface interne. Les adresses IP affectées aux serveurs SRV-MAIL et SRV-3W sont désormais 217.167.171.129 et 217.167.171.130. Sur le routeur SDSL les fonctionnalités NAT/PAT et de redirection ne sont plus nécessaires.

2.5. Donner la table de routage du pare-feu SRV-WALL.

Le pare-feu du routeur SDSL et le pare-feu SRV-WALL disposent désormais des règles de filtrage permettant l'accès au site *web* public et au serveur SMTP et POP. L'administrateur vous demande d'écrire les nouvelles règles qui permettent l'accès **au site *web* privé depuis les boutiques** pour la mise à jour des commandes dans la base de données.

2.6. Établir la nouvelle règle de filtrage sur l'interface externe 217.167.171.126 du routeur SDSL.
2.7. Établir la règle de filtrage sur l'interface externe de SRV-WALL sachant que le SGBDR (implanté sur le serveur SRV-SAGE) écoute sur le port 3306.

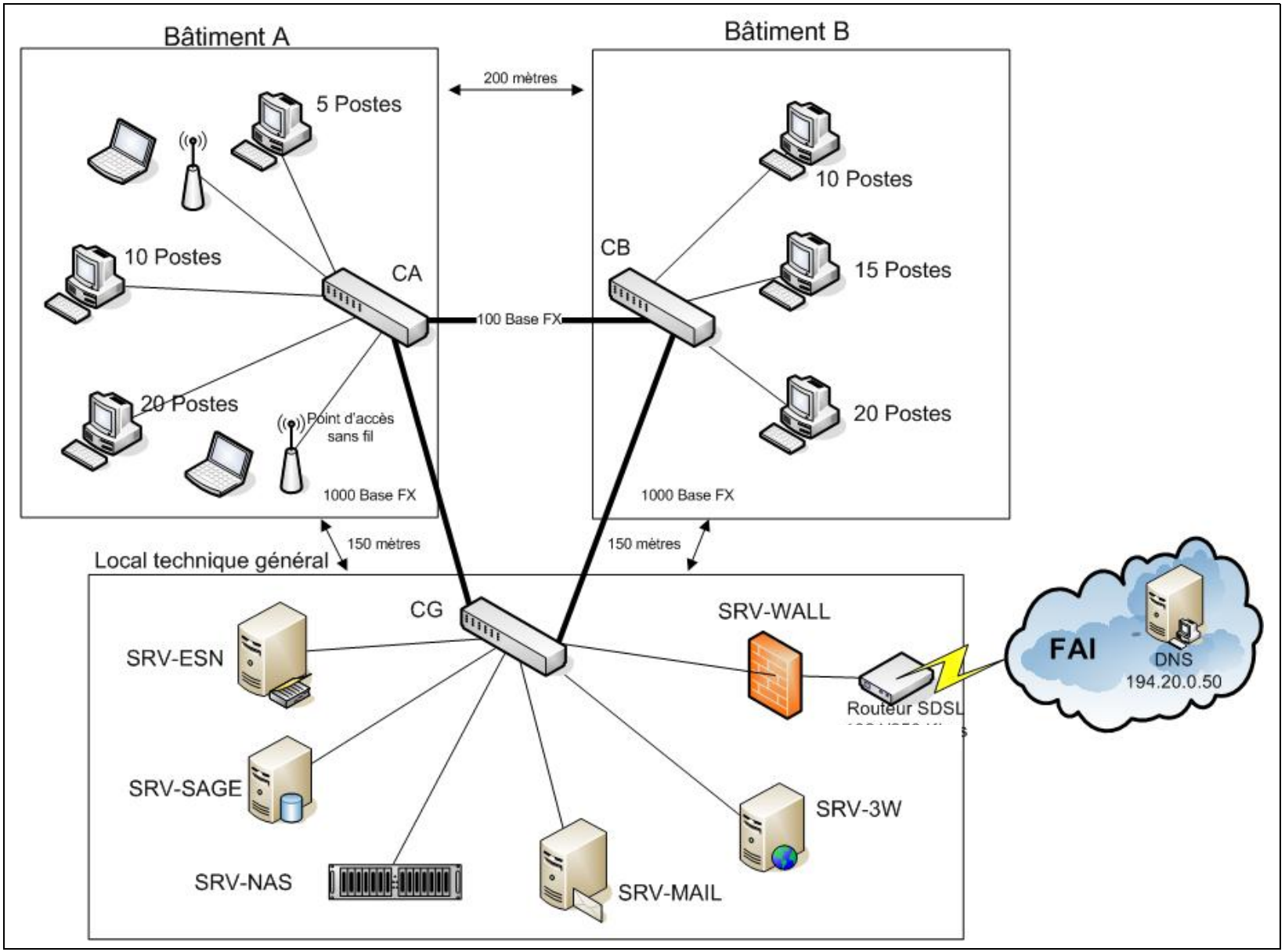
Le serveur SRV-MAIL assure les services SMTP et POP. Ces deux services ont été testés et fonctionnent correctement. Ils utilisent les mêmes mots de passe de connexion. Depuis un poste du service informatique dans le réseau local, l'administrateur a configuré un compte de messagerie existant ainsi :

SMTP : 217.167.171.129 POP : pop.espace-sante-nature.com

Il envoie les courriels avec succès, mais il ne parvient pas à en recevoir. Le logiciel client de messagerie affiche l'erreur suivante: Échec de la connexion au serveur. Compte : 'admin', Serveur : 'pop.espace-sante-nature.com', Protocole : POP3, Port : 110

2.8. Expliquer la cause de l'échec de réception du courriel, sachant que le FAI n'a pas été informé du nouveau plan d'adressage.

ANNEXE 1 : Nouvelle architecture du réseau



ANNEXE 2 : Configuration des réseaux virtuels et IP de la société

Architecture générale de l'interconnexion : Chaque bâtiment (A, B et local technique général) dispose d'un commutateur principal qui s'interconnecte avec les commutateurs principaux des autres bâtiments.

Architecture des VLAN

Commutateurs principaux	CA	CB	CG
Emplacement	Bâtiment A	Bâtiment B	Local Technique général
VLAN gérés	1,100, 200	1,100, 200	1,100, 200

Remarque : Le commutateur CG est un commutateur / routeur. À chaque VLAN défini sur le commutateur peut être associée une adresse IP qui permet le routage entre VLAN. Cette fonction de routage n'est pas activée.

Tableau d'affectation Ports - VLAN avec statut 802.1q des ports

	VLAN 1	VLAN 100	VLAN 200	Etiquetés 802.1q (*taggés*)
Ports de connexion des points d'accès sans fil du bâtiment A	X			NON
Ports de connexion des postes fixes filaires et des autres équipements du Bâtiment A		X		NON
Ports de connexion des postes fixes filaires et des autres équipements du bâtiment B			X	NON
Ports de connexion des serveurs et des équipements du local technique général		X	X	OUI
Ports d'interconnexion des commutateurs CA, CB et CG	X	X	X	OUI

Adresse IP du sous-réseau associé à chaque VLAN

VLAN 1 (par défaut)	VLAN 100	VLAN 200
Pas d'adresse IP affectée	192.168.0.0/24	192.168.1.0/24

Adressage IP des postes de travail : Tous les postes des bâtiments A et B doivent obtenir une adresse dynamiquement à partir du serveur DHCP SRV-ESN. Ce serveur gère deux plages d'adresses, une pour chaque réseau IP.

Adressage IP des serveurs : Le protocole 802.1q est activé sur les interfaces réseau des serveurs. Ces interfaces sont associées au VLAN 100 et au VLAN 200 et disposent d'une adresse IP par VLAN. Les cartes réseaux de ces serveurs sont donc multi-adresses. Elles associent à un VLAN la trame reçue en fonction de l'étiquette contenue dans la trame et remettent le paquet à l'adresse IP correspondante. En émission, elles étiquettent la trame en fonction du VLAN d'émission.

Tableau d'affectation serveurs / VLAN et adressage IP des serveurs (avant le déplacement dans la DMZ des serveurs SRV-3W et SRV-MAIL)

	VLAN 100	VLAN 200
SRV-ESN (serveur d'authentification – DHCP – DNS cache)	192.168.0.1	192.168.1.1
SRV-SAGE (serveur d'applications de gestion et SGBDR)	192.168.0.3	192.168.1.3
SRV-NAS (stockage des fichiers et des bases de données)	192.168.0.5	192.168.1.5
SRV-3W (serveur *web* interne et externe)	192.168.0.7	192.168.1.7
SRV-MAIL (serveur de messagerie interne et externe)	192.168.0.9	192.168.1.9
SRV-WALL (pare-feu, accès Internet des postes sur l'interface interne)	192.168.0.254	192.168.1.254

Remarque : le pare-feu SRV-WALL dispose de l'adresse IP 217.167.171.134 sur l'interface externe.

ANNEXE 3 : Informations techniques sur le serveur NAS

Le **serveur NAS** est une solution simple pour ajouter du stockage disque en réseau. Le NAS est un périphérique réseau de stockage (serveur de fichiers). Il se connecte sur un réseau Ethernet et se comporte comme un serveur autonome de fichiers. Sa simplicité d'installation et d'administration, la redondance de ses composants en font une solution fiable et efficace pour le stockage et la sauvegarde des données sur un réseau hétérogène.

Caractéristiques du serveur NAS

Matériel

- Pentium 4 2.8GHz avec 512KB L2 cache et 2 DIMM slots for 2GB ECC DDR 266/333 *memory*,
- 2 interfaces intégrées Intel Gigabit Ethernet
- 8 disques SATA *hot-swappable* (250 GB chacun)
- RAID 0, 1, 5
- Gravure sur CD-R/RW et DVD+RW (Option)
- Alimentation redondante et compatibilité UPS

Administration et Compatibilité

- Microsoft Windows NT/2000/2003 *support Domaine* et *Active Directory*
- UNIX, Solaris, FreeBSD, Linux, support Network Information Service (NIS),
- MacOS 8.x, 9.x, OS X
- TCP/IP, AppleTalk, IPX
- HTTP, CIFS/SMB, NFS v3, NCP, FTP, AFP
- BOOTP, RARP, DHCP, DNS, WINS, SMTP, SNMP, NTP, SSL

ANNEXE 4 : Schéma de la DMZ