CAS BONNÉTÉ

Présentation du contexte

La société Bonnété a été créée à la fin du XIX^{ème} siècle par un architecte naval qui construisait des bateaux de pêche à voile. La société s'est peu à peu spécialisée dans les navires à voilure imposante.

Au milieu des années 1960, sous l'impulsion des héritiers du créateur de l'entreprise, la société Bonnété s'est intéressée au marché de la navigation de plaisance. Les premiers voiliers conçus à cette fin sont alors présentés au Salon Nautique de Paris et y rencontrent un public passionné. En une vingtaine d'années, la société Bonnété s'est hissée au premier rang des constructeurs mondiaux de voiliers de plaisance.

La Salon Nautique International de Paris est une manifestation annuelle qui a lieu au mois de décembre pendant une dizaine de jours. Il offre un panorama complet des activités et des loisirs nautiques. Le salon accueille plus de 300 000 visiteurs passionnés par la navigation de loisir et environ 1 200 exposants représentant 1 500 marques. La surface totale de l'exposition est de 116 000 m². Plus de 1 400 bateaux y sont présentés.

La société Bonnété est présente chaque année sur deux stands du Salon Nautique international de Paris. Le salon constitue l'évènement commercial essentiel de la société : les commandes des clients passées au salon représentent plus de 70% du chiffre d'affaires annuel de la société. Il est donc essentiel que le système informatique mis en place réponde parfaitement aux besoins métiers (accès à l'information, prise de commandes, etc.) et soit opérationnel (continuité de service, débit, accès, sécurité).

Pour le salon de décembre prochain, l'analyse des besoins a montré la nécessité de déporter localement une copie d'une partie du système d'information commercial permettant la prise des commandes pour éviter tout problème de coupure de liaison. Les commandes passées au salon seront périodiquement remontées vers le système d'information du siège de Bonnété. Il est également prévu d'offrir un accès Internet aux clients présents sur le site du salon.

DOSSIER 1 - Plan d'adressage IP et solution sans fil

Documents à utiliser : annexes 1, 2 et 3.

Le cahier des charges concernant la mise en place du plan d'adressage IP pour le prochain salon comporte les règles suivantes :

- Les commerciaux sont régulièrement en mouvement sur les stands. Ils sont au nombre de 15, équipés d'ordinateurs portables et doivent pouvoir accéder en permanence à l'intranet mis en place et donc aux serveurs du stand secondaire ainsi qu'à Internet.
- L'adresse du réseau des commerciaux est 192.168.10.0/27.
- Les clients visiteurs équipés d'ordinateurs portables doivent pouvoir accéder à Internet. On estime à 10 au maximum le nombre de visiteurs qui se connecteront à Internet simultanément sur le stand.
- Les réseaux IP pour les commerciaux et les visiteurs seront distincts.
- La configuration IP des portables des commerciaux et des visiteurs sera dynamique.
- Le masque de sous-réseaux des visiteurs doit limiter au minimum nécessaire le nombre d'adresses IP utilisables sur le stand.
- L'adresse réseau IP des visiteurs doit être la première immédiatement disponible après le réseau des commerciaux.
- Le routeur d'accès à Internet disposera d'une adresse sur chacun des réseaux. Cette adresse sera fixe et devra être la dernière adresse de la plage d'adresses des réseaux.

TRAVAIL À FAIRE

1.1 Proposer un masque de sous réseau pour le sous-réseau des visiteurs. *Justifier la réponse.*

1.2 Proposer une adresse de réseau IP pour le sous réseau des visiteurs et préciser l'adresse du routeur pour ce sous réseau.

Les deux stands sont reliés entre eux par une liaison sans fil.

Chaque stand dispose d'un équipement *Wifi* configuré pour jouer le double rôle de point d'accès et de pont *Wifi*. Le pont *Wifi* permet d'étendre la liaison *Wifi* de façon directionnelle entre les deux zones à couvrir.

Le point d'accès du stand a été configuré en pont racine et celui du stand de démonstration en pont non racine. Les deux ponts émettent sur le canal 6.

Sur chacun des points d'accès deux SSID ont été configurés et nommés respectivement BonnetCom et BonnetVIS. Chaque SSID a été associé à un VLAN : BonnetCom est associé au VLAN 100 et BonnetVIS est associé au VLAN 200.

Le protocole 802.1Q a été activé entre les deux ponts *Wifi*.

Un commutateur est installé dans le stand technique. L'*annexe 3* décrit les connexions sur ce commutateur.

TRAVAIL À FAIRE

1.3 Expliquer pourquoi on a associé un SSID à chaque VLAN.

1.4 Écrire un tableau associant les numéros de ports du commutateur aux numéros de VLAN.

1.5 Indiquer le ou les ports du commutateur qui recevront et émettront des trames étiquetées 802.1Q. *Justifier la réponse.*

Le routeur ADSL inclut la fonction de serveur DHCP et de relais DNS.

Sur le serveur DHCP on a défini deux plages d'adresses pour chacun des sous réseaux. Les baux attribués aux visiteurs ont une durée de 30 minutes et ceux attribués aux commerciaux sont d'une journée. Le service agent relais DHCP est disponible mais non activé sur le routeur.

TRAVAIL À FAIRE

1.6 Indiquer si un utilisateur peut utiliser son adresse plus de 30 minutes. *Justifier la réponse.*

1.7 Expliquer le rôle d'un agent relais DHCP.

1.8 Indiquer s'il est nécessaire d'activer la fonction agent relais DHCP dans la configuration décrite.

Le serveur DHCP délivrera une adresse de passerelle différente pour chaque sous réseau mais la même adresse de serveur DNS (192.168.10.30) à tous les clients DHCP.

Il s'agit d'un relais DNS ne gérant pas de fichier de zones mais interrogeant les serveurs DNS sur Internet et mettant en cache leur réponse.

TRAVAIL À FAIRE

1.9 Expliquer le rôle d'un fichier de zone DNS et préciser quel est le type des serveurs DNS qui ont autorité sur ces fichiers.

1.10 Indiquer si un poste appartenant à un visiteur pourra joindre le serveur DNS pour faire une résolution de noms. *Justifier la réponse.*

DOSSIER 2 - Sécurité des accès et utilisation de l'annuaire de la société

Documents à utiliser : annexes 2, 4 et 5

Pour les visiteurs du stand désirant se connecter à internet, la connexion au point d'accès ne sera pas contrôlée, elle utilisera cependant une clé de cryptage WEP fournie par les commerciaux à tous les visiteurs qui en feront la demande. Cette clé WEP sera renouvelée tous les jours.

Les commerciaux devront par contre s'authentifier auprès d'un serveur RADIUS qui vérifiera les droits de connexion à partir d'un serveur d'annuaire LDAP. La connexion, une fois autorisée, sera cryptée par le protocole de chiffrement WPA2.

Le serveur Radius est contacté par les deux points d'accès lorsqu'un utilisateur se connecte au SSID BonnetCom. Le protocole d'authentification utilisé est EAP/PEAP.

Le certificat de l'autorité qui a émis le certificat du serveur Radius a été installé sur les postes des commerciaux.

Les commerciaux s'authentifient par un code utilisateur et un mot de passe.

TRAVAIL À FAIRE

2.1 Justifier le choix du cryptage WPA par rapport au cryptage WEP pour les commerciaux.

2.2 Expliquer l'utilité du certificat de l'autorité de certification installé sur les postes des commerciaux.

L'établissement d'une liaison sur le réseau *Wifi* est accordé aux ordinateurs portables des commerciaux par le point d'accès seulement si l'autorisation est donnée par le serveur Radius.

Une liaison ouverte permettra aux portables d'intégrer un VLAN puis de récupérer une adresse IP via DHCP. Si la connexion est refusée, le portable ne pourra pas accéder au sous réseau des commerciaux.

L'ouverture d'une liaison contrôlée par un serveur Radius utilise schématiquement le principe suivant :

- Le client (appelé SUPPLICANT) fait une demande de connexion pour établir une liaison à un équipement réseau (ici le point d'accès) en utilisant le protocole EAP encapsulé dans une trame 802.11.
- L'équipement réseau (appelé NAS *Network Access Server*) récupère la partie EAP, l'encapsule dans le protocole RADIUS puis transmet le tout par l'intermédiaire des couches UDP et IP au serveur RADIUS.
- Le serveur RADIUS répond au NAS. En fonction de la réponse le NAS ouvre ou non la liaison.

Une adresse IP a donc été définie sur chaque point d'accès.

TRAVAIL À FAIRE

2.3 Justifier la nécessité d'une adresse IP pour les points d'accès.

2.4 Indiquer si le protocole de transport utilisé par le serveur RADIUS travaille en mode connecté.

Le routeur d'accès à Internet inclut les fonctions de NAT/PAT et de pare-feu SPI (*Statefull Packet Inspection)*, cette dernière option permet de n'autoriser que les paquets correspondant à une connexion TCP établie.

Les règles de filtrage s'écrivent ainsi :

Interface	Numéro de règle	Source Adresse IP/masque CIDR	Port Source	Destination AdresseIP / masque CIDR	Port Destination	État TCP établi Oui/Non	Action (A : accepter, R : refuser)

Une étoile (*) placée dans une colonne signifie « tout ».

Le routeur applique les règles de filtrage dans l'ordre des numéros de règles. Si une règle s'applique, les règles suivantes ne sont pas vérifiées.

Les règles de filtrage suivantes doivent être définies :

- On doit permettre au serveur applicatif de communiquer en employant le protocole SSH (port 22) avec le serveur applicatif 82.10.10.10 situé au siège.
- On doit autoriser les deux sous-réseaux commerciaux et visiteurs à communiquer en utilisant le protocole HTTP (port 80). Une seule règle sera écrite pour les deux sous-réseaux dont l'adresse commence dans les deux cas par 192.168.10.
- On doit autoriser les deux sous-réseaux commerciaux et visiteurs à communiquer en employant le protocole HTTPS (port 443). Une seule règle sera écrite aussi pour les deux sous-réseaux.
- Aucune connexion TCP ne doit être autorisée à partir d'Internet.
- Tout le reste est interdit.

L'adresse IP de l'interface Internet du routeur est 80.9.155.226.

TRAVAIL À FAIRE

2.5 Indiquer si la fonction NAT/PAT du routeur doit être activée. *Justifier la réponse*.

2.6 Écrire uniquement les règles de filtrage à appliquer sur les paquets en provenance d'Internet. *Remarque : quelle que soit la réponse à la question précédente les adresses IP utilisées doivent être les adresses des sous-réseaux internes*.

Depuis quelques temps, la société Bonnété gère les comptes informatiques de ses employés à l'aide d'un annuaire utilisant le protocole LDAP.

La décision a été prise de ne plus se limiter à la simple tâche d'authentification des utilisateurs sur le réseau mais d'exploiter au maximum les possibilités offertes par les annuaires.

Ainsi, la direction des ressources humaines a fait migrer les informations de gestion du personnel actuellement stockées dans une base de données relationnelle vers les entrées LDAP correspondant à chaque salarié (adresse, téléphone, etc.).

À titre d'illustration, l'*annexe 4* présente les informations concernant l'employée nommée Jeannette LAGACHE telles qu'elles sont stockées actuellement dans le système d'information de la société Bonnété.

L'*annexe 5* présente quelques rappels sur le format d'échange LDIF et sur les URL LDAP.

Jeannette LAGACHE a été mutée au service comptabilité, son numéro de téléphone interne a changé (4405), son nouveau responsable est la comptable dont le nom est Annie SAVRE. On souhaite ajouter deux informations supplémentaires dans l'annuaire, l'adresse et le numéro de portable qu'on connaît grâce à une requête SQL (*annexe 4*).

TRAVAIL À FAIRE

2.7 Écrire le fichier LDIF qui permet de prendre en compte dans l'annuaire le changement de situation de Jeannette LAGACHE.

2.8 Expliquer le rôle de l'URL LDAP suivante :

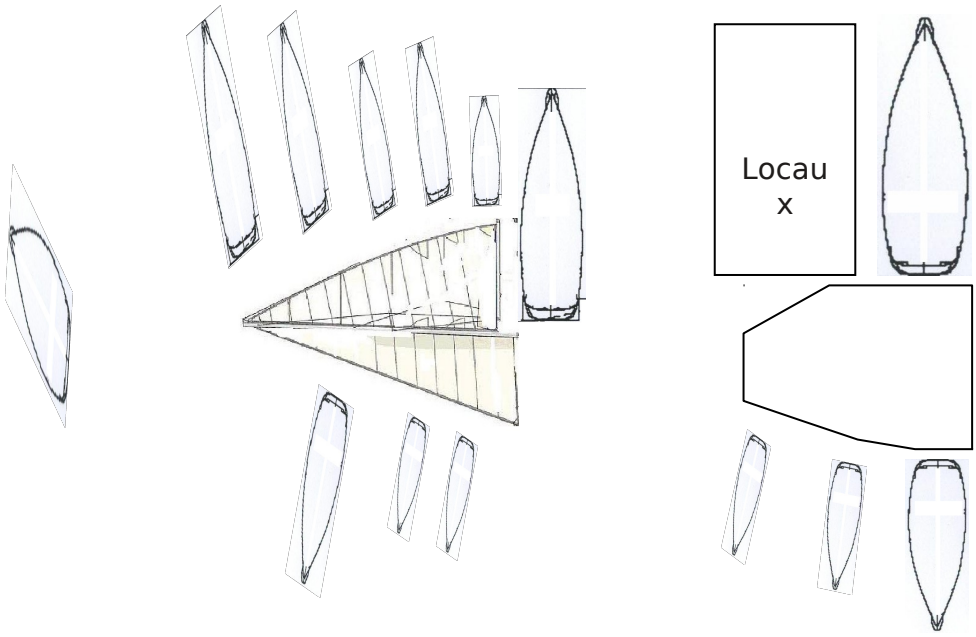
ldap://ldap.bonnete.fr/ou=Personnel,o=bonnete,c=fr?cn,mail?sub?
(&(objectClass=inetOrgPerson) (businessCategory=Ventes))

Annexe 1 - Plan des stands

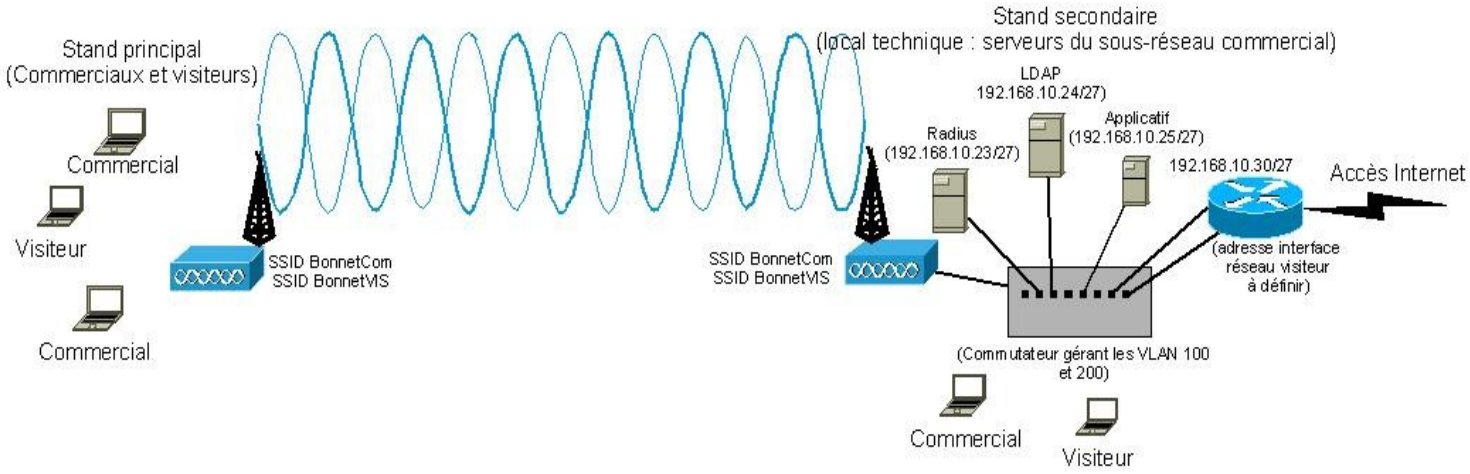
Les deux stands de la société Bonnété se caractérisent par :

- une partie principale de 36 × 36 mètres constituée d'une estrade en forme de voiles stylisées entourée d'une partie des voiliers exposés. L'estrade est surélevée de manière à permettre l'accès aux ponts des voiliers sans devoir passer par des échelles. Cette partie est idéalement placée dans le salon et constitue la vitrine de la société.
- une partie secondaire de 15 × 36 mètres constituée d'une estrade polygonale entourée du reste des voiliers exposés et de locaux interdits au public (bureaux, salles informatiques, local technique, ateliers, matériels annexes .etc.). Cette partie est plus en retrait.

Les stands sont séparés par une distance de 80m environ et notamment par un couloir d'une largeur de 4m où passent les visiteurs du salon ainsi que des véhicules d'entretien.



Annexe 2 - Schéma du réseau



Annexe 3 - Tableau de connexion du commutateur

Matériel	Point d'accès	Radius	LDAP	Applicatif	Interface routeur Réseau commercial	Interface routeur Réseau visiteur
Numéro de port	10	12	14	16	18	20

Annexe 4 - Système d'information des ressources humaines

Extrait de l'annuaire (au format LDIF en « mode import ») :

```
dn: cn=Jeannette LAGACHE,ou=Personnel,o=Bonnete,c=fr
objectClass: inetOrgPerson
cn: Jeannette LAGACHE
title: Mme
sn: LAGACHE
givenName: Jeannette
uid: jlagache
password: {SHA1}AgtHyF34-FC4Vu91P--
telephoneNumber: 2305
mail: jlagache@bonnete.fr
businessCategory: Secrétariat
manager: cn=Hugues SOCHAUX,ou=Personnel,o=Bonnete,c=fr
```

Extrait de la base de données

Résultat de la requête « SELECT * FROM PERSONNEL WHERE nom = 'LAGACHE' AND prenom = 'Jeannette' » :

id	nom	prenom	titre	adresse	telInterne	service	idResp	portable
31	LAGACHE	Jeannette	Mme	4 rue du sirocco 29000 BREST	2305	Secrétariat	18	06.14.20.62.89

Annexe 5 - Formes générales d'un fichier LDIF et d'une URL LDAP

La **forme générale d'un fichier LDIF en « mode commande »** est la suivante :

```
dn: nom distinctif
changetype: identificateur de modification
[opérateur de modification]
liste des attributs…
[-
opérateur de modification
liste des attributs…]
```

Le caractère « - » spécifie le séparateur entre deux instructions portant sur le même « dn ».

Pour créer un nouvel enregistrement	changetype: add
Pour détruire un enregistrement	changetype: delete
Pour renommer une entrée	changetype: modrdn
Pour modifier un enregistrement	changetype: modify Un *opérateur de modification* doit alors être spécifié. add : ajouter des attributs et leurs valeurs. replace : remplacer des valeurs d'attributs par d'autres. delete : détruire l'attribut spécifié

Annexe 5 (suite)

Les URLs LDAP, définies par la RFC 2255, permettent aux clients *web* d'avoir un accès direct au protocole LDAP. La syntaxe est de la forme suivante :

ldap://<serveur>:<port>/<dn_départ>?<attributs>?<scope>?<filtre>

- Il n'est pas nécessaire de préciser le port si c'est celui par défaut (389/tcp).
- <dn_départ> est le DN de l'entrée qui est le point de départ de la recherche.
- <attributs> sont les attributs qu'on souhaite consulter.
- <scope> peut valoir « base », « one » ou « sub ».
- <filtre> est le filtre de recherche (par défaut : objectClass=*).

  Exemples de filtres de recherche :

  - attribut **=** valeur (correspondance exacte)
  - attribut **~=** valeur (orthographe proche)
  - attribut **<** valeur *[ou* **>***, ou* **<=***, ou* **>=** *]* (comparaison)
  - attribut = v*****le***** (caractère « joker »)
  - attribut = ***** (l'attribut est présent)
  - (**&**(attribut1 = valeur1)(attribut2 = valeur2)) (ET logique)
  - (**|**(attribut1 = valeur1)(attribut2 = valeur2)) (OU logique)
  - (**!**(attribut = valeur)) (NON logique)

scope : profondeur de la recherche. Il y a trois types de profondeur possible :

base : la recherche ne s'effectuera que sur le *baseObject*. La recherche devient alors l'équivalent d'une lecture, à condition toutefois que le *baseObject* réponde positivement au filtre.

one : tous les enfants directs du *baseObject* et seulement les enfants directs sont concernés par la recherche.

sub : tous les descendants de *baseObject*, ainsi que *baseObject* lui même sont concernés par la recherche.