DOSSIER 1 Gestion du siège

Annexes à utiliser : 1, 2 et 3.

Au siège de l'entreprise CMM, un bâtiment regroupait les ateliers affectés à la fabrication mécanique (machines-outils à commandes numériques) et les différents bureaux, comprenant ceux affectés à la conception des gammes de fabrication (CAO des programmes d'usinage des pièces) et au bureau d'études (CAO des produits industriels). Ce bâtiment étant devenu trop exigu, la société a construit un nouveau bâtiment sur le site du siège, qui accueille désormais les bureaux, ce qui a permis d'étendre les ateliers dans l'ancien bâtiment, appelé désormais « bâtiment atelier » (cf. *annexe 1*).

Le nouveau bâtiment doit bien sûr être relié au réseau du siège. La disposition des bâtiments fait qu'il a été décidé de relier ce nouveau bâtiment à l'atelier. Le nouveau bâtiment accèdera par cette connexion au réseau du siège, avec toutes les fonctionnalités. Lors de sa construction, une gaine technique a été enterrée entre les deux bâtiments offrant la possibilité de faire passer tout type de câble pour relier les deux locaux techniques. La longueur de la gaine est de 190 mètres.

Il est prévu que l'ensemble des équipements puisse à terme disposer d'une bande passante à 1 Gb/s, tout en gardant la possibilité de conserver le matériel existant qui fonctionne actuellement à 100 Mb/s.

Dans un souci d'uniformisation des équipements, les trois routeurs R1, R2, R3 sont identiques. Il en va de même pour les commutateurs qui équipent les différents bâtiments. Le nouveau bâtiment sera donc équipé avec un ou plusieurs de ces matériels.

CHOIX DU MÉDIA

On envisage d'utiliser différents types de média :

- câble cuivre, 4 paires torsadées ftp cat 6 classe E,
- câble cuivre, 4 paires torsadées ftp cat 7 classe F,
- câble 6 fibres optiques, multimode 850 nm,
- câble 6 fibres optiques, monomode 1310 nm.

TRAVAIL À FAIRE

1.1 Choisir le type de média à utiliser pour relier le nouveau bâtiment en tenant compte des contraintes techniques et des équipements. *Le choix doit être justifié.*

1.2 Préciser quel matériel est nécessaire, et en quelle quantité, pour connecter le média choisi ci-dessus, et finaliser le raccordement du nouveau bâtiment à l'atelier. Choisir le matériel parmi ceux proposés en *annexe 3.*

CONFIGURATION DE L'ÉLECTRONIQUE ACTIVE

On a attribué un numéro de réseau indépendant pour le bureau d'études, le réseau 192.168.6.0/24. Le réseau de l'atelier, qui englobe encore la partie préparation de fabrication, garde son adressage IP : 192.168.3.0/24.

Pour des impératifs organisationnels, les utilisateurs de ces deux réseaux 192.168.6.0/24 et 192.168.3.0/24 se répartissent dans les deux bâtiments.

On vous donne les informations suivantes :

- Le routeur R3 et un commutateur sont déjà installés dans le bâtiment atelier. Les postes de ce bâtiment sont déjà connectés au commutateur, certains dans le réseau 192.168.3.0/24, d'autres dans le réseau 192.168.6.0/24.
- Un commutateur est déjà installé, dans le nouveau bâtiment, auquel sont déjà connectés les postes du bâtiment, certains dans le réseau 192.168.3.0/24, d'autres dans le réseau 192.168.6.0/24.
- Le média choisi précédemment est installé dans sa gaine et relie le commutateur de l'atelier avec le commutateur du nouveau bâtiment.
- On veut que les domaines de diffusion associés au réseau bureau d'études et au réseau fabrication soient séparés.
- Il faut qu'un poste du nouveau bâtiment dans le réseau bureau d'études puisse joindre tout poste du réseau général de l'entreprise.
- Le routeur R3 est relié par une interface au commutateur de l'atelier, cette connectique ne sera pas modifiée ; on n'utilisera pas une autre interface physique sur ce routeur.

TRAVAIL À FAIRE

1.3 Dire quels sont les éléments de configuration logicielle à initialiser ou modifier sur les deux commutateurs. *Justifier la réponse.*

1.4 Dire quels sont les éléments de configuration logicielle du routeur R3 à modifier. *Justifier la réponse.*

À partir du siège, il faut pouvoir joindre les réseaux installés dans les chantiers. Le routeur R1 est correctement configuré et le routeur R3 est en cours de configuration.

Mais, dans la description de la table de routage de R2 (cf. *annexe 2*) il manque la route pour atteindre les réseaux des chantiers à partir du réseau administratif. Les réseaux des chantiers sont correctement définis dans le routeur VPN du siège.

Pour des raisons de sécurité, le responsable réseau ne veut pas définir de route par défaut dans les routeurs.

TRAVAIL À FAIRE

1.5 Donner, pour le routeur R2, la (ou les) ligne(s) de sa table de routage qui permet(tent) au réseau administratif d'entrer en relation avec les postes de tous les chantiers.

L'absence de route par défaut ne doit pas empêcher l'accès à Internet pour les postes du réseau du siège. Cet accès doit être contrôlé.

TRAVAIL À FAIRE

1.6 A l'aide du schéma de l'annexe 1, donner la solution de configuration au niveau des postes, pour que tous les employés du siège de la société puissent accéder à Internet.

DOSSIER 2 Gestion des chantiers

Annexes à utiliser : 1 et 2.

Chaque chantier dispose d'un point d'accès *Wi-Fi* (ou ASFI, accès sans fil à internet), d'un commutateur et d'un routeur VPN.

La CMM ouvre un nouveau chantier sur Lille, dans un ensemble commercial proche du centre-ville. Les équipements informatiques prévus nécessiteront 10 adresses IP. La société a établi des règles pour gérer l'attribution d'une plage d'adresses IP à un nouveau chantier afin de limiter les conflits d'adressage et de respecter une certaine homogénéité.

L'adresse du réseau des chantiers est 192.168.4.0/24. Ce réseau est ensuite décomposé en sous-réseaux en fonction du besoin d'adresses de chaque chantier. On affecte à un nouveau chantier l'adresse du premier sous-réseau disponible.

Pour le nouveau chantier de Lille où 10 postes seront installés, l'administrateur affecte l'adresse réseau IP 192.168.4.48/28.

TRAVAIL À FAIRE

2.1 Dire si l'adresse réseau affectée répond aux contraintes et est compatible avec les adresses réseaux des chantiers existants (*annexe 2*). *Justifier la réponse.*

Des problèmes de connexion pirate, notamment à partir d'ordinateurs portables utilisés sur les chantiers, ont décidé la direction à modifier la configuration du réseau reliant les chantiers au siège.

Les points d'accès (bornes HP420 ou CISCO AIRONET 1200) connectés aux commutateurs ont été configurés pour ne plus diffuser leur SSID.

TRAVAIL À FAIRE

2.2 Donner les conséquences de la non-diffusion du SSID sur la configuration des ordinateurs portables.

L'authentification sera faite par un serveur d'authentification utilisant le protocole *Radius* (*Remote Authentification Dial-in User Service*) installé au siège. L'authentification se fera sur la base de l'adresse *MAC* (*MAC-Based*) et utilisera le chiffrement *WEP-128*. Les adresses *MAC* seront stockées dans un fichier de données présent au siège et interrogé par le serveur *Radius*.

L'administrateur réseau sait que son système n'est pas complètement sécurisé mais il estime suffisant son niveau de protection compte tenu des risques encourus.

TRAVAIL À FAIRE

2.3 Donner les éléments techniques sur lesquels l'administrateur se base pour estimer que son système n'est pas complètement sécurisé.

L'adressage des machines clientes des chantiers était jusqu'à maintenant réalisé de façon statique. On souhaite passer à des adresses IP fournies de manière centralisée.

L'administrateur teste la nouvelle configuration sur le réseau de Mulhouse. Le découpage en sous-réseaux et le routage ne sont pas remis en cause.

L'attribution d'une adresse IP à une machine d'un chantier est faite par un serveur DHCP d'adresse IP 192.168.1.100, situé au siège (on n'utilisera pas la fonction serveur DHCP du routeur VPN tête de réseau du chantier).

Un premier test après configuration d'un client du chantier en « client DHCP » n'a pas donné satisfaction : le client n'a pas reçu d'adresse IP.

On effectue un second test. Après activation de la fonctionnalité « relais DHCP » sur le routeur du chantier et quelques réglages sur le pare-feu pour que les échanges ne soient pas filtrés, le poste obtient bien l'adresse IP souhaitée.

TRAVAIL À FAIRE

2.4 Expliquer la cause majeure du dysfonctionnement du premier test et dire en quoi l'activation de relais DHCP a résolu le problème.

Le poste qui vient d'être configuré communique bien avec les autres postes du même chantier mais ne parvient pas à joindre un serveur du siège, même pas le serveur DHCP qui lui a pourtant fourni son adresse IP.

TRAVAIL À FAIRE

2.5 Dire ce qui manque à la configuration du poste client et comment y remédier en respectant la centralisation des configurations.

Pour faciliter l'exploitation des journaux d'événements, l'administrateur souhaite qu'un poste client DHCP ait toujours la même adresse IP.

TRAVAIL À FAIRE

2.6 Proposer une solution pour répondre à cette contrainte. *Justifier la réponse.*

Le poste client d'un chantier s'authentifie auprès d'un serveur d'authentification utilisant le protocole *Radius* qui dialogue avec le serveur d'annuaire. La liaison avec le serveur d'authentification passe par un tunnel VPN géré par les routeurs VPN des chantiers.

Un technicien teste l'authentification d'accès d'une machine du chantier de Mulhouse au réseau du siège.

Le poste client du chantier, filaire ou *Wi-Fi*, est configuré pour être authentifié par le serveur d'authentification d'adresse IP 192.168.1.101.

Le commutateur-routeur-VPN d'adresse 192.168.5.6 du chantier doit pouvoir dialoguer avec le serveur d'authentification.

Ce premier test échoue et le technicien retrouve dans le journal d'erreurs du pare-feu du siège une trame rejetée. Une capture de cette trame effectuée en entrée de ce serveur est donnée ci-dessous.

Synthèse extraite de la capture

No.	Time	Source	Destination	Protocol Info
1	0.000000	192.168.5.6	192.168.1.101	RADIUS Access-Request(1) (id=26, l=257)

Résumé par couche de la trame

```
Frame 1 (299 bytes on wire, 299 bytes captured)

Ethernet II, Src: D-Link_84:c3:46 (00:11:95:84:c3:46), Dst:
AcctonTe_db:27:2f (00:00:e8:db:27:2f)

Internet Protocol, Src: 192.168.5.6 (192.168.5.6), Dst:
192.168.1.101 (192.168.1.101)

User Datagram Protocol, Src Port: 2745 (2745), Dst Port: radius
(1812)

Radius Protocol
```

TRAVAIL À FAIRE

2.7 En vous aidant des informations contenues dans cette trame et en reproduisant le cadre ci-dessous, proposer la ou les lignes de la table de filtrage du pare-feu, pour que celui-ci ne bloque pas le dialogue.

Interface d'arrivée	Adresse IP Source	Port Source	Adresse IP Destination	Port Destination	Protocole de transport	Action

DOSSIER 3 Surveillance du réseau – analyse du trafic à risque

Annexes à utiliser : 4, 5, 6 et 7.

Pour renforcer la sécurité, l'administrateur réseau a décidé d'authentifier les clients *Wi-Fi* par *login* et mot de passe en modifiant la configuration du serveur d'authentification (RADIUS) existant.

La société CMM souhaite maintenant enregistrer les informations fournies par les fichiers de *log* du serveur d'authentification dans une base de données. On ne s'intéresse ici qu'aux connexions des clients *Wi-Fi*. Le responsable base de données a mis à jour le schéma relationnel existant en créant la table suivante :

CONNEXION(numéro, type_message, code_erreur, adresse_mac, date, login_saisi)
numéro : Clé primaire

Le fichier *log* du serveur d'authentification se nomme "*radius.log*", il est séquentiel. Un extrait de ce fichier vous est fourni en *annexe 4*. Une tentative de connexion génère plusieurs lignes dans ce fichier. La première ligne contient la chaîne "*access request*" et la dernière ligne contient la chaîne "*sending*". Un fichier de *log* contient plusieurs tentatives de connexion.

Chaque tentative de connexion dans le fichier *log* se traduira par l'insertion d'un enregistrement dans la table CONNEXION comme le montre l'*annexe 5* :

- soit un enregistrement pour le message d'acceptation *ACCESS-ACCEPT* (le champ *type_message* aura la valeur "accepté" dans la table CONNEXION),
- soit un enregistrement pour le message de refus *ACCESS-REJECT* (le champ *type_message* aura la valeur "refusé" dans la table CONNEXION).

Conscient de la difficulté du projet, le responsable de la base de données vous a demandé dans un premier temps de rédiger un programme qui ne renseigne que les champs *type_message* et *login_saisi*. Il vous fournit les fonctions et procédures utiles à votre programme. Les en-têtes de ces procédures et de ces fonctions sont décrits ici :

Extraction(uneLigne : Chaîne) : Chaîne */* Cette fonction extrait une information dans une ligne en fonction de son format. Il s'agit dans un premier temps de l'information de "login" */*

.

Contient_chaîne(uneLigne : Chaîne, uneChaîne : Chaîne) : Booléen
/ Cette fonction recherche une chaîne de caractères dans une ligne et renvoie VRAI si la chaîne existe, FAUX sinon. */*

Exemple d'utilisation de ces deux fonctions :

```
Ouvrir(unFic, "radius.log"», lecture)
Lire(unFic, ligne)
...
Si Contient_chaîne(ligne, "User-Name") alors
        login_saisi ← Extraction(ligne)
finsi
...
```

Insert_Connexion(unTypeMessage : Chaîne, unLoginSaisi : Chaîne)

*/*Cette procédure réalise l'insertion d'une ligne dans la table connexion en mettant à jour uniquement les champs type_message et login_saisi.*/*

Exemple d'utilisation :

```
Si Contient_chaîne(ligne, "Access-Reject") alors
    type_message ← "refusé"
    Insert_Connexion(type_message, login_saisi)
finsi
```

Connect_Base(uneBase : Chaîne, unUser : Chaîne, unPassword : Chaîne) : Booléen

/ Cette fonction réalise la connexion à la base de données Elle renvoie la valeur VRAI si la connexion a réussi. */*

Exemple pour CMM : *connexion ← Connect_Base("CMM", "admCMM", "password")*

Deconnect_Base() *// Cette procédure effectue la déconnexion de la base de données.*

TRAVAIL À FAIRE

3.1 Écrire le programme d'extraction des données du fichier "*radius.log*" et leur insertion dans la table CONNEXION (*le candidat est autorisé à utiliser le langage de son choix y compris un langage algorithmique*).

Le responsable base de données souhaite aussi pouvoir identifier le chantier à l'origine de chaque tentative de connexion.

Le rattachement d'une connexion à un chantier s'effectuera via le champ *NAS-IP-Address* qui représente l'adresse IP du système authentificateur du chantier.

Par exemple dans l'extrait du fichier *log* fourni en *annexe 4*, ce champ a la valeur 192.168.5.6, ce qui correspond au système authentificateur du chantier de Mulhouse.

TRAVAIL À FAIRE

3.2 Écrire la requête SQL qui modifie la structure de la table CONNEXION pour ajouter la colonne *ip_authentificateur*.

Une fois la structure de la table modifiée, il faut maintenant modifier la fonction existante d'extraction des champs du fichier "*radius.log*".

Cette fonction extrait des informations d'une ligne passée en paramètre en fonction d'un mot clé contenu dans la ligne et du format des informations à extraire.

Au départ la fonction *Extraction()* n'extrayait que le *login*, elle a été enrichie pour extraire les autres champs nécessaires à la table des connexions. Cependant, il faut la compléter pour extraire aussi l'adresse IP du système authentificateur.

Pour vous aider, le responsable base de données vous fournit la fonction actuelle décrite en *annexe 7*. Pour vous familiariser avec le langage utilisé, il vous fournit aussi le document présenté en *annexe 6*.

TRAVAIL À FAIRE

3.3 Écrire l'expression rationnelle permettant d'extraire d'une ligne du fichier "*radius.log*" l'adresse IP du système authentificateur.

La table des connexions maintenant à jour, l'administrateur base de données vous présente le schéma relationnel complet :

CONNEXION(numéro, type_message, code_erreur, adresse_mac, date, login_saisi, ip_authentificateur)
numéro : Clé primaire

EMPLOYÉ(numéro, login, nom, fonction)
numéro : Clé primaire

CHANTIER(numéro, adresse, responsable, ip_authentificateur)
numéro : Clé primaire

POSTE(numéro, adresse_mac, marque, type)
numéro : Clé primaire

HABILITER(utilisateur, poste)
utilisateur, poste : Clé primaire
utilisateur : Clé étrangère en référence à numéro de EMPLOYÉ
poste : Clé étrangère en référence à numéro de POSTE

TRAVAIL À FAIRE

3.4 En étudiant l'*annexe 5*, expliquer pourquoi l'administrateur de la base de données n'a pas créé de contrainte d'intégrité référentielle entre l'attribut *login_saisi* de la table CONNEXION et l'attribut *login* de la table EMPLOYÉ.

À partir du schéma relationnel ci-dessus, l'administrateur vous demande d'établir les requêtes SQL suivantes :

TRAVAIL À FAIRE

3.5 Écrire la requête SQL qui liste toutes les connexions qui ne concernent pas un employé enregistré dans la base (*login_saisi*, *date*, *adresse*), triées par chantier.

3.6 Écrire la requête SQL qui calcule le nombre de connexions en échec (type_message = "refusé") dans la journée du 1er janvier 2008.

3.7 Écrire la requête SQL qui crée la vue limitant la table CONNEXION aux seules connexions du chantier n° 4.

3.8 Écrire la requête SQL qui autorise l'accès en lecture à cette vue au responsable du chantier n° 4, dont l'identifiant est DEMICHOT.

DOSSIER 4 Certification des échanges nomades

Annexe à utiliser : 8

La CMM envisage d'autoriser l'accès à ses applicatifs par Internet ; ce projet vise à simplifier le travail des utilisateurs nomades et à réduire les opérations de mise à jour sur les machines distantes.

Quelques techniciens utilisent actuellement le mécanisme de VPN SSL pour les échanges avec certains fournisseurs soucieux d'authentification.

La DSI (direction des systèmes d'information) réfléchit à une extension de ce mécanisme pour l'accès aux applications de CMM afin d'éviter le recours systématique à un mécanisme de VPN intervenant au niveau de la couche réseau, plus coûteux et limitant l'accès aux seules machines du parc de CMM.

La CMM envisage de faire appel à un prestataire extérieur, opérateur de service de certification, pour l'émission et la délivrance des certificats électroniques. Les certificats sont émis par l'opérateur de service de certification, avec contrôle par échange de courriels, puis installés sur chaque machine concernée ou sur un support amovible, dans le respect de la charte interne d'utilisation des certificats.

TRAVAIL À FAIRE

4.1 Indiquer quels sont les fichiers générés par l'installation d'un certificat.
4.2 Expliquer la présence de plusieurs certificats électroniques sur l'ordinateur de certains techniciens.

La CMM souhaite porter une attention particulière à la validité des certificats acquis.

TRAVAIL À FAIRE

4.3 Proposer trois situations nécessitant la révocation d'un certificat.
4.4 Indiquer la démarche à suivre par la DSI de CMM pour obtenir la révocation d'un certificat électronique.