CORRIGE

Ces éléments de correction n'ont qu'une valeur indicative. Ils ne peuvent en aucun cas engager la responsabilité des autorités académiques, chaque jury est souverain.

E4R : ÉTUDE DE CAS

Durée : 5 heures **Coefficient : 5**

CAS CMM

ÉLÉMENTS DE CORRECTION

1. Barème

Dossier 1 : Gestion du siège	28	points
Dossier 2 : Gestion des chantiers	28	points
Dossier 3 : Surveillance du réseau - analyse du trafic à risque	29	points
Dossier 4 : Certification des échanges nomades	15	points
Total	100	points

DOSSIER 1 GESTION DU SIÈGE

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.* **5 points**

si cuivre 0
si fibre sans précision 2 pt
fibre muti 850 sans précision 3 pts
justification 2 pts (1 pour la distance, 1 pour la compatibilité avec le switch)

La solution à retenir :

- Câble 6 fibres optiques, multimode 850 nm : pas d'objections sur cette solution, *il convient tout de même de vérifier que la longueur de 190 mètres sera compatible avec un débit futur à 1Gbps, ce qui est le cas : si Ø 50 µm, 550 mètres, si Ø 62,5 µm, 275 mètres* Cette solution est adaptée au commutateur. Ce câble est compatible avec la distance de 190m.

Justifications pour ne pas retenir les autres solutions :

- Câble cuivre, 4 paires torsadées f/ftp cat 6 classe E : cette solution est à rejeter pour au moins 2 raisons :
  - Un câble cuivre ne peut dépasser 100 mètres (5+90+5),
  - *Câbler entre 2 bâtiments ne peut se faire en cuivre câbles blindés ou écrantés, les courants de fuite de terre passent par le blindage à moins d'effectuer une mise à la terre commune pour les 2 bâtiments ce qui est assez complexe.*

- Câble cuivre, 4 paires torsadées f/ftp cat 7 classe F : solution à écarter pour les mêmes raisons que la première, le fait de passer en cat7 et d'effectuer une certification en classe F ne change rien au problème.

- Câble 6 fibres optiques, monomode 1310 nm : pas d'impossibilité technologique pour cette solution car elle doit permettre une liaison aux débits demandés jusqu'à 2 km , mais elle n'est pas adaptée au commutateur existant.

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

Il faut insérer des modules sur les commutateurs adaptés à la réponse précédente (vérification de la cohérence) , exemple : 2 module 1000base SX/multimode.

remarque : l'étudiant a pu penser qu'il fallait installer un commutateur dans le nouveau bâtiment
Si commutateur sans module 2 pts,Si deux modules sans commutateur (en précisant que le commutateur est présent) 3 pts,Si commutateur + un ou deux modules 3 pts La réponse doit être cohérente avec la proposition faite en 1.1

Le choix du routeur mis dans le nouveau bâtiment est faux car il ne permet pas d'évoluer vers le gigabit.

1.3 Dire quels sont les éléments de configuration logicielle à initialiser ou à modifier sur les deux commutateurs. *Justifier la réponse.* **5 points**

Solution 1 (préconisée)

- Chaque commutateur doit gérer deux VLAN, un VLAN "bureau d'étude" et un VLAN "atelier/production". *2 pts*
- La liaison inter-commutateur doit donc être étiquetée 802.1Q *(taggée)*, (ports fibre optique *taggé*). *2pts*
- Il faut aussi *tagger* le port du commutateur atelier pour la liaison avec le routeur R3. *1pt*

Solution 2 (plus complexe pour l'administration)

- Chaque commutateur doit gérer deux VLAN, un VLAN "bureau d'étude" et un VLAN "atelier/production". *2pts*
- La liaison inter-commutateur doit donc être étiquetée 802.1Q *(taggée)*, (ports fibre optique taggé).*2pts*
- Activer le routage sur le commutateur atelier *1pt*
- Définir des IP aux interfaces virtuelles associées à chaque VLAN dans le réseau correspondant (ex 192.168.6.253 et 192.168.3.253)
- Ajouter toutes les lignes dans la table de routage du commutateur nécessaires pour joindre tous les réseaux de CMM
- Laisser le port du commutateur atelier pour la liaison avec le routeur R3 dans le VLAN "atelier/production".

1.4 Dire quels sont les éléments de configuration logicielle du routeur R3 à modifier. *Justifier la réponse.* **4 points**

Solution 1 (préconisée) cohérente avec la solution 1 précédente

Le lien entre le routeur et le commutateur est unique, il faut donc *tagger* les trames et associer chaque interface virtuelle à un VLAN différent.*2 pts*

Il faut définir 2 interfaces virtuelles sur l'interface réelle, une pour le réseau 192.168.3.0 et l'autre pour 192.168.6.0). *2 pts*

La table de routage du routeur R3 sera modifiée automatiquement par la définition des interfaces virtuelles.

Solution 2 *cohérente avec la solution 2 précédente*

Ajouter dans la table de routage du routeur une route pour joindre le réseau 192.168.6.0/24 qui passe par la passerelle 192.168.3.253 (interface virtuelle du commutateur associée au VLAN "atelier/production" en sortant par son interface 192.168.3.254. *4pts*

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. **6 points**

Adresse réseau	**Masque**	**Passerelle**	**Interface**
192.168.4.0	255.255.255.0	192.168.0.9	192.168.0.10

On acceptera un masque 255.255.255.128

On admet une solution avec une ligne pour chaque chantier (avec ou sans Lille).

Pas de pénalisation si référence au réseau d'interconnexion 192.168.5.0

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. **5 points**

Les tables de routage permettent aux postes de joindre le serveur proxy qui est aussi le pare-feu, utiliser ce proxy (192.168.0.5) dans la configuration des postes.

DOSSIER 2 CONFIGURATION POUR UN NOUVEAU CHANTIER

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.* **6 points**

3 pts L'adresse 192.168.4.48/28 en binaire sur le quatrième octet est 0011 0000 son masque (/28) sur le dernier octet est 1111 0000.
Il reste donc 4 bits pour les hôtes, soit 2^4-2=14 adresses possibles
Ce masque permet donc d'adresser les 10 postes du chantier.

3 pts Il permet de s'intercaler entre le réseau 192.168.4.32/29 (Angers) et le réseau 192.168.4.64/27 (Marseille), justifications :

- Compatibilité avec le réseau de Marseille
  Soit la dernière adresse disponible du nouveau réseau 192.168.4.48/28 (Lille) :
  Dernier octet : 0011 1111 (63), soit l'adresse 192.168.4.63/28

- Compatibilité avec le réseau d'Angers
  Soit la dernière adresse disponible du réseau 192.168.4.32/29 (Angers) :
  Dernier octet : 0010 0111 (39), soit l'adresse 192.168.4.39/29

Solution détaillée :
Voici le plan d'adressage du réseau des chantiers :

Adresse sous-réseau		$4^{ème}$ octet début fin	
192.168.4.0 / 28	Bordeaux	0000 0000 : 0 0000 1111 : 15	2^4=16 adresses 14 machines
192.168.4.16 / 29	Libre mais trop petit	00010 000 : 16 00010 111 : 23	2^3=8 adresses 6 machines
192.168.4.24 / 29	Mulhouse	00011 000 : 24 00011 111 : 31	2^3=8 adresses 6 machines
192.168.4.32 / 29	Angers	00100 000 : 32 00100 111 : 39	2^3=8 adresses 6 machines
192.168.4.40 / 29	Libre mais masque impossible	00101 000 : 40 00101 111 : 47	2^3=8 adresses 6 machines
192.168.4.48 / 28	Libre **possible**	0011 0000 : 48 0011 1111 : 63	2^4=16 adresses 14 machines
192.168.4.64 / 27	Marseille	010 00000 : 64 010 11111 : 95	2^5= 32adresses 30 machines
192.168.4.96 / 28	Libre **possible**	0110 0000 : 96 0110 1111 : 111	2^4=16 adresses 14 machines

2.2 Donner les conséquences de la non-diffusion du SSID sur la configuration des ordinateurs portables. **2 points**

L'existence d'un SSID diffusé signale la présence d'un point d'accès à un réseau à tous les postes *Wi-Fi* qui sont dans le rayon d'émission du point d'accès donc y compris à des personnes ne faisant pas partie du chantier. Si le SSID n'est pas diffusé il faut configurer les SSID sur les ordinateurs portables pour qu'ils puissent se connecter.

2.3 Donner les éléments techniques sur lesquels l'administrateur se base pour estimer que son système n'est pas complètement sécurisé. **3 points**

Un *sniffer Wi-Fi* permet de capturer un flux échangé entre une carte *Wi-Fi* et un point d'accès même si le SSID n'est pas diffusé. *Le SSID et les adresses Mac passent en clair dans les trames échangées (non exigée).* La clé *WEP* peut être cassée par des utilitaires disponibles librement *moyennant une capture de données* (2 pts).

Une fois toutes ces informations obtenues, une personne non autorisée peut usurper une adresse MAC (*mac spoofing*) (1pt).

2.4 Expliquer la cause majeure du dysfonctionnement du premier test et dire en quoi l'activation de relais DHCP a résolu le problème. **4 points**

Le début du dialogue entre un client et un serveur DHCP est réalisé en trames de diffusion (*broadcast)*, les diffusions (*broadcasts)* ne passent pas les routeurs, le serveur DHCP n'est pas joint. *2pts*

Le relais DHCP se charge de joindre le serveur DHCP *en unicast*, le dialogue s'établit. *2 pts*

2.5 Dire ce qui manque à la configuration du client et comment y remédier en respectant la centralisation des configurations. **4 points**

Il faut lui fournir une passerelle par défaut, pour l'objectif de centralisation, c'est le serveur DHCP qui communiquera ce paramètre au poste, par l'utilisation de l'option adéquate.

2.6 Proposer une solution pour répondre à cette contrainte. **4 points**

Il faut utiliser la fonctionnalité de réservation : affectation d'une adresse IP par rapport à une adresse MAC. *4 pts*

Si bail illimité *2 pts*

L'utilisation des baux longs est moins sécurisée car une machine peut perdre son bail, de plus, une machine inconnue peut obtenir une adresse IP si la totalité de l'étendue n'est pas affectée.

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. **5 points**

Interface d'arrivée	Adresse ip Source	Port Source	Adresse ip Destination	Port Destination	Protocole de transport	Action
192.168.0.2	192.168.5.6	tous	192.168.1.101	1812	UDP	accepter
192.168.0.5	192.168. 1.101	1812	192.168.5.6	tous	UDP	accepter

3pts pour la première ligne.
2pts pour la deuxième ligne.

-1pt par erreur sur la ligne

On acceptera un mode « miroir » ou une gestion des échanges UDP « établis » à la place de la seconde ligne .si le candidat(e) le précise.
On acceptera le mot radius à la place du numéro de port.
On accepte une notation CIDR sur les adresses IP.

DOSSIER 3 SURVEILLANCE DU RÉSEAU : ANALYSE DU TRAFIC À RISQUE

3.1 Écrire le programme d'extraction des données du fichier "*radius.log*" et leur insertion dans la table CONNEXION (*Le candidat est invité à utiliser le langage de son choix y compris un langage algorithmique*). **7 points**

Exemple de solution :

```
Variables
    unFic : Fichier
    ligne : Chaîne de caractères
    connexion : Booléen
    type_message, login_saisi : Chaîne de caractères
Début
    connexion ← Connect_Base("CMM", "admCMM", "password")
    Si connexion alors
            Ouvrir (unFic, "radius.log", lecture)
            Lire(unFic, ligne)
            Tant que non fin fichier(unFic) faire

               Si Contient_chaîne(ligne, "User-Name") alors
                     login_saisi ← Extraction(ligne)
               Fsi

               Si Contient_chaîne(ligne, "Access-Accept") alors
                     type_message ← "accepté"
                     Insert_Connexion (type_message, login_saisi)
               Fsi
               Si Contient_chaîne(ligne, "Access-Reject") alors
                     type_message ← "refusé"
                     Insert_Connexion(type_message, login_saisi)
               Fsi
               Lire(unFic, ligne)
            FtantQue
            Fermer(unFic)
            Deconnecte_Base()
    Sinon
       Afficher "Problème à la connexion"
    Fsi
Fin
```

Toute autre solution cohérente et juste est acceptée.

gestion de la connexion 1 pt
gestion du fichier séquentiel 2 pts
gestion des détections et des extractions 2pts
gestion des insertions 2pts
On enlève la moitié des points si l'algo est incohérent.

3.2 Écrire la requête SQL qui modifie la structure de la table CONNEXION pour ajouter la colonne *ip_authentificateur*. **(3 points)**

Alter table CONNEXION
add ip_authentificateur varchar(15)

celui qui met *not null* ne sera pas pénalisé
celui qui met *column* ne sera pas pénalisé

3.3 Écrire l'expression rationnelle permettant d'extraire d'une ligne du fichier "*radius.log*" l'adresse IP du système authentificateur. **3 points**

*if ($ligne =~ /nas-ip-address/i) {($variable)= (($ligne) =~/***(\d+\.\d+\.\d+\.\d+)***/) ;}*

Le seul élément exigé est l'expression (partie en gras).

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. **(3 points)**

Comme le montre l'extrait du fichier log, il peut y avoir des demandes de connexions rejetées sur des utilisateurs inconnus dans la base de données. On veut quand même enregistrer ces demandes de connexion, il ne faut donc pas mettre en place de contrainte d'intégrité référentielle.

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 points**

SELECT login_saisi, date, adresse
FROM CONNEXION, CHANTIER
WHERE CONNEXION.ip_authentificateur = CHANTIER.ip_authentificateur
AND login_saisi NOT IN (Select login from EMPLOYÉ)
ORDER BY adresse (ou 3)

1pt pour le tri, 1 pt pour la référence à la sous requête, 1 pt pour la jointure

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 points**

SELECT count(*)
FROM CONNEXION
WHARE date = "01/01/2008"
AND type_message = "refusé"

1pt pour le count et 1 pt par restriction

3.7 Écrire la requête SQL qui crée la vue limitant la table CONNEXION aux seules connexions du chantier n° 4. **3 points**

```
CREATE VIEW CONN-CHANTIER-4 as
SELECT CONNEXION.numéro, type_message, code_erreur, adresse_mac, date,
login_saisi, ip_authentificateur
FROM CONNEXION,CHANTIER
WHERE CONNEXION.ip_authentificateur = CHANTIER.ip_authentificateur
AND CHANTIER.numéro = 4
```

1pt pour la syntaxe correcte du create view
2pts pour la requête

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. **4 points**

```
GRANT SELECT ON CONN-CHANTIER-4 to DEMICHOT
```

Dossier 4 CERTIFICATIONS DES ÉCHANGES NOMADES

4.1 Indiquer quels sont les fichiers générés par l'installation d'un certificat. **3 points**

Remarque : le mot « fichier » doit être interprété comme « composant ».

3pts si référence au certificat numérique et à la clé privée (la clé publique étant souvent intégrée dans le certificat numérique)

Cette installation va générer une clé publique, partie intégrante et visible du certificat, une clé privée permettant la signature numérique de documents et le certificat proprement dit, carte d'identité numérique de celui à qui il a été délivré (cf norme ISO X.509)
Le certificat de la machine distante permettra l'identification, par le serveur, de l'utilisateur distant essayant de se connecter au serveur de l'entreprise et inversement.
Selon le produit utilisé ou le système, l'implémentation sera différente.

4.2 Expliquer la présence de plusieurs certificats électroniques sur l'ordinateur de certains techniciens. **3 points**

Un certificat permet l'identification et l'authentification d'un utilisateur. Un utilisateur peut, dans le cadre des diverses transactions distantes qu'il effectue, être contraint de s'identifier via des certificats différents propres au domaine de gestion concerné par la transaction.
La multiplicité des échanges dématérialisés peut donc conduire à installer plusieurs certificats pour un même utilisateur sur une même machine. Les navigateurs Web gèrent sans problèmes cette possibilité.

4.3 Proposer trois situations nécessitant la révocation d'un certificat. **6 points**

2 pts par situation cohérente (plafonné à 6)

Les certificats électroniques sont émis et gérés par un prestataire de certification électronique, Autorité de Certification. Cette gestion porte notamment sur le problème de validité dans le temps. La révocation est le fait de l'Autorité de Certification à la demande de l'entreprise cliente ou suite à un non renouvellement de contrat.

Différentes situations nécessitant une révocation :

- Perte (1) ou vol (2) du support de la clé (ordinateur portable, clé usb, ...)
- Départ (3) d'un employé ou changement de service (4) nécessitant une adaptation de ses droits
- Changement d'éléments d'identité (5) du titulaire (adresse électronique par exemple)
- Blocage du certificat (6)
- Oubli du code PIN (7),
- Divulgation du code PIN (8),
- ...

Remarque (non attendue dans la réponse) : Il appartient à l'entreprise de mettre à jour ses serveurs au regard des certificats électroniques « acceptables » c'est-à-dire non révoqués, suite par exemple au départ d'un collaborateur. Il arrive que cette mise à jour ne soit pas

assez fréquente ; un protocole spécifique OCSP (On Line Certificate Status Protocol) permet de centraliser et automatiser les vérifications.

4.4 Indiquer la démarche à suivre par la DSI de CMM pour obtenir la révocation d'un certificat électronique. **3 points**

La DSI de CMM doit s'adresser à l'autorité de certification émettrice, seule compétente pour révoquer le certificat attribué par ses services à un client.

La désinstallation des certificats ne répond pas à la question car le certificat n'est pas révoqué.

Grille de correction EDC 2008 (Cas CMM)

D1 (28 points)	
1.1 (5pts) si cuivre 0 pt,si fibre sans précision 2 pts,fibre muti 850 sans précision 3 pts justification 2 pts (1 pour la distance, 1 pour la compatibilité avec le switch) 1.2 (3pts) Si commutateur sans module 2 pts,Si deux modules sans commutateur (en précisant que le commutateur est présent) 3 pts,Si commutateur + un ou deux modules 3 pts 1.3 (5pts) (solution 1) déclaration 2vlan 2pts, liaison inter switch taggée 2pts, port routeur taggée 1pt (solution 2) déclaration 2vlan 2pts, liaison inter switch taggée 2pts,activation routage sur commutateur atelier 1pt 1.4 (4pts) (solution 1) définition de 2 interfaces virtuelles 2pts, association des interfaces à un vlan avec taggage 2pts (solution 2) route vers l'interface virtuelle du commutateur 4pts 1.5 (6pts) ligne(s) correcte(s) 1.6 (5pts) utilisation du proxy	
Total D1	
D2 (28 points)	
2.1 (6 points) justification nombre d'adresses 3pts, justification insertion sous-réseau 3pts 2.2 (2 points) Config SSID sur portable 2pts 2.3 (3 points) casser la clé WEPl 2pts, usurpation d'adresse MAC 1pt 2.4 (4 pts) Diffusion bloquée par routeur 2pts, relais DHCP joint serveur DHCP 2pts 2.5 (4pts) Passerelle obtenue par DHCP 2.6 (4 pts) réservation d'adresses 4pts, si bail illimité 2pts 2.7 (5 pts) première ligne 3pts, 2eme ligne 2pts (-1 pt par erreur sur ligne)	
Total D2	
D3 (29 pts)	
3.1 (7 pts) Gestion de la connexion 1pt, gestion fichier séquentiel 2pts,détection motif et extraction 2pts, insertions 2pts (moitié des pts si algo non cohérent) 3.2 (3 pts) Alter table 3pts 3.3 (3pts) Expression rationnelle 3pts 3.4 (3pts) existence de demande de connexion ne correspondant pas à un utilisateur 3.5 (3pts) 1pt pour le tri, 1pt pour la référence à la sous requête, 1pt pour la jointure 3.6 (3pts) 1 pt pour count, 1 pt par restriction 3.7 (3pts) 1pt pour la syntaxe correcte du create view, 2pts pour la requête 3.8 (4pts) Grant correct	
Total D3	
D4 (15 pts)	
4.1 (3 pts) référence au certificat numérique, et à la clé privée 4.2 (3 pts) identification et authentification propre à la transaction 4.3 (6 pts) 2pts par situation cohérente plafonnée à 6 4.4 (3 pts) Révocation par autorité de certification	
Total D4	