

BTS INFORMATIQUE DE GESTION - ISE4R

SESSION 2009

ÉTUDE DE CAS

Durée : 5 heures

Coefficient : 5

CAS FEFORT

ÉLÉMENTS DE CORRECTION

Barème

Dossier 1 : Architecture du réseau du siège	30 points
Dossier 2 : Architecture du réseau inter-sites	20 points
Dossier 3 : Gestion du parc informatique – Analyse - conception	15 points
Dossier 4 : Gestion du parc informatique – algorithmes des scripts	15 points
Dossier 5 : Passage à la norme ISO 9001 – G.E.D.	20 points
Total	100 points

CODE ÉPREUVE : ISE4R		EXAMEN : BREVET DE TECHNICIEN SUPÉRIEUR		SPÉCIALITÉ : INFORMATIQUE DE GESTION Option Administrateur de réseaux locaux d'entreprise	
SESSION 2009	CORRIGÉ	ÉPREUVE : ÉTUDE DE CAS			
Durée : 5 h	Coefficient : 5		Code sujet : 08AR04N		Page : 1/14

DOSSIER 1 – 30 pts

1.1 Donner l'écriture décimale pointée de ce masque et indiquer combien de sous réseaux pourront être créés à l'aide de celui-ci.

255.255.240.0

4 bits → $2^4 = 16$ sous-réseaux possibles (*on tolère 16-2 – obsolète depuis 1995...*)

1.2 Proposer une adresse IP pour chacun des services. *La proposition doit être compatible avec les adresses statiques existantes indiquées dans l'annexe 2.*

Tous les sous-réseaux commencent par 172.16 et se terminent par 0.

Ils s'écrivent donc sous la forme 172.16.x.0/20 où x représente un nombre multiple de 16 (puissance de 2 correspondant au dernier bit à 1 du masque de sous-réseau) : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 et 240.

Tous les ordinateurs du service informatique sont en 172.16.200.x : ils doivent donc appartenir au sous réseau 172.16.192.0 car celui-ci va jusqu'à l'adresse 172.16.207.255.

Le pare-feu possède une adresse 172.16.220.1 : il est donc dans le réseau 172.16.208.0

Pour les différents services, puisqu'ils n'ont que des adresses dynamiques fournies par le DHCP, on peut choisir n'importe quel autre sous-réseau non encore attribué.

sous-réseaux	services
172.16.0.0	
172.16.16.0	Gestion/comptabilité
172.16.32.0	Commercial
172.16.48.0	Relation Client
172.16.64.0	Marketing
172.16.80.0	Direction
172.16.96.0	Q, R & D
172.16.112.0	
172.16.128.0	
172.16.144.0	
172.16.160.0	
172.16.176.0	
172.16.192.0	Service informatique
172.16.208.0	Accès pare-feu (pour information : non exigé)
172.16.224.0	
172.16.240.0	

} Au choix
} Obligatoire

La liste complète des sous réseaux possibles n'est pas demandée et les deux derniers réseaux sont aussi utilisables.

1.3 Donner l'adresse de la passerelle par défaut des postes du service commercial, sachant qu'il s'agit de l'adresse disponible la plus élevée pour ce sous-réseau.

172.16.47.254

L'adresse fournie doit être cohérente avec l'adresse du sous réseau retenue pour le service commercial (ici 172.16.32.0).

1.4 Expliquer la raison de ce dysfonctionnement et préciser les modifications à apporter, d'une part au serveur DHCP, d'autre part au nouveau routeur.

Raison

En l'état actuel des choses, le routeur ne laisse pas passer les paquets DHCP *Discover* qui sont des paquets de diffusion générale (adresse 255.255.255.255). Seuls les clients du service informatique sont susceptibles de recevoir leurs paramètres IP.

Mise à jour du routeur

Sur le routeur, il faut :

- attribuer au routeur une adresse dans chaque sous-réseau (fait à la question précédente donc pas exigée);
- activer le relais DHCP sur toutes les interfaces du routeur sauf celle du service informatique; *La citation de l'agent relais est exigée mais pas sa présence sur toutes les interfaces.*
- lui indiquer l'adresse du serveur DHCP : 172.16.200.3.

Mise à jour du serveur

Sur le serveur DHCP, il faut :

- supprimer l'étendue existante (*pas exigée*);
- créer une étendue par sous-réseau utilisé, donc par service

Par exemple, pour le service Comptabilité/Gestion :

Étendue : 172.16.16.1 à 172.16.16.100 (doit contenir au moins 50 adresses)

Masque : 255.255.240.0

Options :

Passerelle : 172.16.31.254 (adresse de routeur sur ce sous-réseau)

serveur DNS : 172.16.200.2

Il n'était pas demandé d'exemple. Une simple phrase précisant une création d'étendue par sous-réseau sera donc admise.

1.5 En utilisant le formalisme donné en *annexe 4*, donner les règles applicables en entrée de l'interface concernée permettant de respecter les consignes données. Vous veillerez à limiter le nombre de règles à définir.

Interface concernée (pas demandé) :

172.16.220.1 (côté siège) en entrée pour la communication siège vers sites distants

172.17.0.1 (côté site) en entrée pour la communication retour

Ou bien une de ces interfaces en entrée et en sortie (on n'exige pas les deux).

N° de règle	Adresse source	Port source	Adresse destination	Port destination	Protocole transport	Action
1	Toutes	Tous	proxy	3128	TCP	Accepter
2	Adresse proxy	3128	Toutes	Tous	TCP	Accepter
3	172.0.0.0/8	Tous	172.16.192.0/20	Tous	Tous	Accepter
4	172.16.192.0/20	Tous	172.0.0.0/11	Tous	Tous	Accepter
Défaut	Toutes	Tous	Toutes	Tous	Tous	Refuser

1^{ère} consigne : les règles 1 et 2 permettent les échanges entre le siège et le proxy du fournisseur d'accès.

2^{ème} consigne : la règle 3 permet aux unités d'envoyer des paquets à tous les services disponibles du service informatique et la règle 4 permet les réponses.

3^{ème} consigne : la règle 4 permet au service informatique de contacter les unités et la règle 3 permet les réponses.

La règle finale (non exigée) par défaut interdit tout trafic non spécifiquement autorisé donc les échanges directs entre les services du siège et les unités du groupe. Le pare-feu n'intervient pas dans les échanges entre les services du siège.

On acceptera :

- toute adresse proxy cohérente.
- toute façon cohérente d'exprimer le mot "tous".
- tout masque de sur-réseau cohérent (/11, /12, et avec deux lignes /14 et /15)
- Une solution avec une ligne spécifique pour le poste de l'administrateur (/32).

La ligne par défaut n'est pas exigée.

1.6 Indiquer les modifications à apporter afin de distribuer des adresses valides aux stations de Villeurbanne, sur une étendue de même taille.

Il faut créer une étendue pour Villeurbanne, par exemple :

Plage d'adresses : 172.22.1.1 à 172.22.1.149

Masque : 255.255.0.0

Options Passerelle : 172.22.250.204 (adresse interne du routeur 4)

DNS : 172.16.200.2

La seule modification par rapport à l'étendue du serveur DHCP de Villeurbanne concerne la plage d'adresses distribuées.

Bien évidemment, il faudra activer le relais DHCP du routeur 4 et lui indiquer l'adresse du serveur DHCP du siège ... mais cela n'est pas demandé.

1.7 Apporter les modifications nécessaires au fichier de la zone *fefort.loc* (annexe 5) et écrire le fichier de la zone *villeurbanne.fefort.loc*.

Il faut ajouter le serveur DNS de Villeurbanne. Ce serveur aura **par exemple** les caractéristiques suivantes :

Machine	@ IP	F.Q.D.N.
serveur DNS	172.22.200.2	ns.villeurbanne.fefort.loc

Exemple avec BIND :

Dans la zone *fefort.loc* :

- il faut rajouter une ligne de délégation de zone pour chaque unité ainsi qu'une ligne de déclaration de l'adresse du serveur. Exemple pour villeurbanne
villeurbanne.fefort.loc. IN NS ns.villeurbanne.fefort.loc.
ns.villeurbanne.fefort.loc. IN A 172.22.200.2

On n'exige qu'une seule zone.

- il faut supprimer la déclaration des serveurs de Villeurbanne (sauf le serveur DNS déclaré ci-dessus bien sûr)

Le fichier zone de *villeurbanne.fefort.loc*. ressemblera à ceci :

```
villeurbanne.fefort.loc.      IN SOA ns.villeurbanne.fefort.loc. admin.fefort.loc.
                              (3; 36000; 3600; 360000; 86400)
                              IN  NS  ns.villeurbanne.fefort.loc.
; serveurs de Villeurbanne
log-vi                       IN  A   172.22.200.1    ; serveur d'authentification
dhcp-vi                       IN  A   172.22.200.3    ; serveur dhcp
fic-vi                        IN  A   172.22.200.6    ; serveur de fichiers
ns                            IN  A   172.22.200.2    ; serveur de nom
```

Exemple sur un serveur MS-Windows :

Dans la zone *fefort.loc* :

- Sélectionner la zone *fefort.loc*
- Créer une nouvelle délégation
- Saisir le nom de la sous-zone (ici : "villeurbanne")
- Ajouter le nom (*ns.villeurbanne.fefort.loc*) et l'adresse IP (172.22.200.2) du serveur DNS qui a obtenu la délégation.

Ajout de la zone de *villeurbanne.fefort.loc* :

- Sélectionner les zones de recherche directes
- Ajouter une nouvelle zone principale
- Saisir le nom de la zone (ici : "villeurbanne.fefort.loc").

1.8 Expliquer les modifications à apporter au serveur DNS du siège d'une part et à celui du site de Villeurbanne d'autre part.

Exemple avec BIND :

Au siège :

Sur le serveur du siège, il faut ajouter l'information selon laquelle il sera serveur « esclave » pour la zone « villeurbanne.fefort.loc ».

```
zone "villeurbanne.fefort.loc" {  
    type slave;  
    masters {  
        172.22.200.2;  
    };  
};
```

À Villeurbanne :

Sur le serveur DNS de Villeurbanne, il faut ajouter une ligne NS pour le serveur ns.fefort.loc, ce qui nous donne :

```
villeurbanne.fefort.loc.      IN SOA  ns.villeurbanne.fefort.loc.  admin.fefort.loc.  
                              (3; 36000; 3600; 360000; 86400)  
                              IN  NS   ns.villeurbanne.fefort.loc.  
                              IN  NS   ns.fefort.loc
```

Exemple sur un serveur MS-Windows :

Au siège :

- Sélectionner "Zones de recherche directes".
- Définir une nouvelle zone secondaire
- Saisir le nom de la zone (ici : "villeurbanne.fefort.loc").
- Saisir l'adresse IP du serveur DNS principal (ici : 172.22.200.2)

À Villeurbanne :

- Sélectionner la zone "villeurbanne.fefort.loc"
- Ajouter un serveur de nom
- Saisir nom et adresse IP du nouveau serveur NS.

DOSSIER 2 – 20 pts

2.1 Déterminer la configuration matérielle et préciser les protocoles que devra supporter le nouveau commutateur. *Le rôle des fonctions et protocoles qu'il prendra en charge sera expliqué.*

Exemple de réponse :

Fonctions/protocoles	Rôle, explication
Configuration matérielle : 8 ports au moins + ports de liaison	Connectivité
Supporter la redondance de lien en évitant les tempêtes de diffusion <i>Protocole 802.1D, STP</i>	Arbre de recouvrement (Spanning tree), Tolérance de panne par agrégation de liens
Gérer les VLAN <i>Protocole 802.1q</i>	Marquage de trames pour identifier les VLAN
Gérer la priorité de flux <i>Protocole 802.1p</i>	Gestion de la priorité de trames
Protocoles SNMP, Telnet, HTTP	Accès en mode administrateur

2.2 Proposer une solution matérielle complémentaire pour permettre aux postes de travail des différents services d'accéder aux serveurs du service informatique. Expliquer brièvement comment elle doit-être mise en œuvre.

Pour la solution basée sur un routeur, il faut soit une interface réelle par VLAN sans nécessité de taguer les trames soit une interface virtuelle par VLAN dans ce dernier cas le routeur doit taguer les trames.

Pour la solution basée sur des serveurs multidressés , il faut une interface virtuelle par VLAN et le serveur doit taguer les trames.

Pour la solution basée sur un commutateur-routeur il y a une interface réelle par VLAN, il n'est pas nécessaire de taguer.

Il existe aussi une réponse non détaillée ici avec des VLAN asymétriques?

Réponses possibles :

Prise en charge de la fonction de routage par l'ajout d'un routeur avec une interface taguée multi adressée afin d'interconnecter logiquement tous les VLAN.

Une solution avec un commutateur de niveau 3 peut assurer l'ensemble de ces fonctionnalités. Chaque port du commutateur s'interconnectant à un autre commutateur est associé à un VLAN et on affecte une adresse IP. Les liaisons ne gérant pas plusieurs VLAN il n'est pas nécessaire de taguer.

Si les serveurs gèrent les VLAN (protocole 802.1Q) on peut multiadresser les serveurs en définissant une interface virtuelle par VLAN, dans ce cas la liaison entre les commutateurs et les serveurs doit être taguée.

2.3 Proposer une solution permettant de garantir la continuité du service d'accès aux serveurs du siège lors d'une panne du routeur. Expliquer les principes de fonctionnement de votre solution.

Exemples :

Mettre en place un routeur de secours et le protocole VRRP (Virtual Redondancy Router Protocol) (HSRP pour Cisco) pour activer/désactiver le routeur de secours.

Prévoir une redondance des routeurs avec répartition de charges

On accepte une solution qui n'assure pas la continuité de service mais la reprise rapide de service

Par exemple :

Prévoir un routeur de secours avec une reprise d'activité basée sur modification dynamique de l'adresse de passerelle sur les postes ...

VRRP permet à deux routeurs R1 et R1' de partager une adresse IP virtuelle. De même pour leur adresse MAC. L'un des routeurs est actif comme s'il était seul. Mais s'il tombe en panne l'autre le détecte. (Arrêt des échanges mutuels de messages signalant leurs présences). R1' ne reçoit plus de messages, il devient alors actif et répond aux requêtes adressées aux adresses communes (IP et MAC).

DOSSIER 3 – 15 pts

3.1 Indiquer les modifications à apporter à l'ébauche du schéma relationnel donnée en *annexe 8* pour intégrer l'attribut *nbLicencesAchat*.

L'attribut *nbLicencesAchat* doit être ajouté à la relation LOGICIEL.

On acceptera une prise en compte de l'historisation impliquant une table supplémentaire.

3.2 Écrire les requêtes SQL qui affectent ces droits au compte utilisateur *gpiTechUser*.

GRANT ALL ON EQUIPEMENT, LOGICIEL, INSTALLER TO *gpiTechUser*
On pourra aussi trouver la liste des permissions SELECT, UPDATE, INSERT, DELETE au lieu de ALL

GRANT SELECT ON USER TO *gpiTechUser*

3.3 Écrire la requête SQL qui ajoute le logiciel (66, "cindoc", "1.0") à la base de données.

INSERT INTO LOGICIEL VALUES (66, "cindoc", "1.0")

Intégration du champ NbLicencesAchat pas exigée

3.4 Écrire la requête SQL qui interroge la base de données pour détecter les logiciels (*désignation*) dont le nombre d'installations (nombre de *keyProduct*) dépasse le nombre de licences possédées (*nbLicencesAchat*).

La requête utilise l'attribut nbLicencesAchat qui a été intégrée au MLD par le candidat à la question 3.1

```
SELECT    désignation, count(*) as "nombre installations"  
FROM      LOGICIEL LOG, INSTALLER INS  
WHERE     LOG.numéro = INS.idLog  
GROUP BY designation, nbLicencesAchat  
HAVING    count(*) > nbLicencesAchat
```

```
SELECT    désignation, count(*) as "nombre installations"  
FROM      LOGICIEL LOG join INSTALLER INS  
ON        LOG.numéro = INS.idLog  
GROUP BY designation, nbLicencesAchat  
HAVING    count(*) > nbLicencesAchat
```

```
SELECT    désignation, count(*) as "nombre installations"  
FROM      LOGICIEL LOG join  INSTALLER INS  
On        LOG.numéro = INS.idLog  
GROUP BY  designation, NbLicenceAchat  
HAVING    count(*) > ( select nbLicencesAchat  
                        From LOGICIEL  
                        Where logiciel.numero = INS.idlog)
```

On accepte toute solution cohérente, notamment avec requête corrélée sans GROUP BY ou avec utilisation d'une vue.

3.5 Écrire la requête SQL créant un index sur la rubrique *nomHote* de la table EQUIPEMENT.

```
CREATE INDEX indexNomHote ON EQUIPEMENT(nomHote)
```

DOSSIER 4 – 15 pts

4.1 Écrire l'algorithme du script "gpi-kawa-client" en langage algorithmique ou dans un langage de script de votre choix. *Vous prendrez soin de commenter le script pour qu'il soit compréhensible par vos collègues du service informatique.*

Exemple d'écriture possible

Algo gpi-kawa-client

Type // n'est pas exigé

DataConfig : Structure

 marque : Chaîne

 modele : Chaîne

 nomHote : Chaîne

 adresseMAC : Chaîne

 adresselP : Chaîne

 nbPartitions : Entier

 pourcentPartitions : Tableau [] de Entier

//espace occupé

FinStructure

Constantes

 nomHoteServeur ← "fichiers.fefort.loc"

Variables

 maConfig : DataConfig

 nomFichierConfig : chaîne

 ligneConfig : chaîne

Début

// Récupère les données machine

maConfig ← getDataConfig()

// Crée un fichier texte ayant pour nom : nomHote.gpi

nomFichierConfig ← maConfig.nomHote + ".gpi"

Ouvrir(nomFichierConfig,création,écriture)

/* Pour chaque rubrique de la structure DataConfig, fabrique puis écrit la ligne dans le fichier */

ligneConfig ← maConfig.marque

Ecrire(nomFichierConfig, ligneConfig)

ligneConfig ← maConfig.modele

Ecrire(nomFichierConfig, ligneConfig)

ligneConfig ← maConfig.nomHote

Ecrire(nomFichierConfig, ligneConfig)

ligneConfig ← maConfig.adresseMAC

Ecrire(nomFichierConfig, ligneConfig)

ligneConfig ← maConfig.adresselP

Ecrire(nomFichierConfig, ligneConfig)

ligneConfig ← maConfig.nbPartitions

Ecrire(nomFichierConfig, ligneConfig)

// Boucle pour le traitement des partitions

Pour i de 1 à maConfig.nbPartitions

 ligneConfig ← maConfig.pourcentPartitions[i]

 Ecrire(nomFichierConfig,ligneConfig)

FinPour

// Ferme le fichier

Fermer(nomFichierConfig)

// Envoie le fichier au serveur

Send(nomHoteServeur, nomFichierConfig)
Fin

4.2 Écrire l'algorithme du script "gpi-kawa-serveur" en langage algorithmique ou dans un langage de script de votre choix. *Dans tous les cas prendre soin de commenter le script pour qu'il soit compréhensible par vos collègues du service informatique.*

Exemple :

Algo *gpi-kawa-serveur*

Variables

fichierListe, fichierRapport, chemin, nomFichier, ligneRapport : Chaîne
nbFichier : Entier
ok : Booléen

Début

fichierListe ← "listeNomFichier.txt"
fichierRapport ← "rapport.txt"
nbFichier ← 0
chemin ← "c:\audit\log"
//Construction de la liste des fichiers
Ouvrir(fichierRapport, Ecriture)
creationListeFichier(fichierListe)
//Traitement pour chaque fichier
Ouvrir(fichierListe, Lecture)
Lire(fichierListe, nomFichier)
Tant que non FinFichier(fichierListe) Faire

// attention dans certains langages de script il n'y a plus de lecture initiale explicite (exemples : vbs, perl ...)

//Incréméntation du nombre de fichiers traités

nbFichier ← nbFichier + 1

//Ajoute les informations dans la base de données

ok ← ajoutBdd(chemin & nomFichier))

//Enregistrement des problèmes rencontrés lors de l'insertion

Si Non(ok) alors

ligneRapport ← nomFichier & " : erreur insertion des données"

Ecrire(fichierRapport, ligneRapport)

Finsi

Lire(fichierListe, nomFichier)

FinTantque

//Report du nombre total de fichiers traités

ligneRapport ← "Nombre de fichiers traités : " & nbFichier

Ecrire(fichierRapport, ligneRapport)

Fermer(fichierRapport)

Fermer(fichierListe)

Fin

DOSSIER 5 – 20 pts

5.1 Indiquer en quoi l'usage de *tags* de type code QR permet de répondre à l'exigence de traçabilité des documents sortis de l'application GED.

Le document est tracé lors de l'impression car le tag code QR généré pourra comprendre par *exemple* des informations relatives au contenu, à la date et à l'identité de l'utilisateur ayant réclamé l'édition. Il sera ainsi possible à tout moment de connaître l'origine du document par l'interprétation du code QR par un lecteur de flash code.

5.2 Pour chacun des documents cités dans l'extrait du tableau de la page précédente, proposer un choix de support de stockage à la date du 15 mai 2009. *Justifier cette stratégie de rangement.*

Voici un exemple de réponse :

Nature du document	Stockage optique	Stockage magnétique
Directive Européenne Cafe (Clean Air For Europe)	x	
Facture N° 200511C90H	x	
Analyse prospects		x
Etude opportunité RZPH35		x
Cahier des charges projet brûlerie Marseille	x	

Les documents fréquemment consultés doivent être stockés sur un support rapide, accessible en lecture et écriture type disque magnétique ; les documents peu consultés peuvent être stockés sur un support plus lent, type disque optique. Une bonne pratique d'archivage permettra par ailleurs de migrer du support magnétique vers un support optique les documents dont la fréquence de consultation devient très faible.

5.3 Proposer un tableau répertoriant les avantages et les inconvénients de chaque solution, notamment en termes de coût total de possession et de facilité d'usage.

Voici un exemple de réponse :

Solutions	Avantages	Inconvénients
Installer les logiciels complets sur les postes.	<ul style="list-style-type: none"> • L'utilisateur peut ajouter, « modifier » le document. • Possibilité de « copier » des éléments depuis le document sans perte de qualité (image, dessins vectoriels...). 	<ul style="list-style-type: none"> • Explosion du nombre de versions existantes. • Lourdeur d'installation. • Gestion et coût des licences important.
Installer des visionneuses.	<ul style="list-style-type: none"> • L'utilisateur peut, avec un applicatif « léger », visualiser le document. • Facile à déployer. • Possibilité de « copier » des éléments depuis le document sans perte de qualité (image, dessins vectoriels...). • Logiciels gratuits. 	<ul style="list-style-type: none"> • Une visionneuse par application. • Mise à jour nécessaire en fonction du logiciel qui a créé le document primitif (primaire).
Utiliser des formats pivots (PDF).	<ul style="list-style-type: none"> • L'utilisateur peut visionner tous les documents à ce format. • Applicatif léger. • Gratuité des lecteurs. • Facile à déployer. • Modification difficile, d'où sécurité. 	<ul style="list-style-type: none"> • Nécessite de créer des « versions pivots » de tous les documents. • Qualité inférieure au document original surtout s'il ya des images.
Utiliser les formats images (jpg, tiff...).	<ul style="list-style-type: none"> • Qualité importante, surtout pour les documents comportant des photographies. • Gratuité des lecteurs. 	<ul style="list-style-type: none"> • Nécessite de créer des « versions image » de tous les documents. • Très lourd au niveau du stockage.
Recourir à XML	<ul style="list-style-type: none"> • Indépendance de la solution. • Coûts moindres, à priori. 	<ul style="list-style-type: none"> • Nécessite d'acquérir une compétence XML. • Obligation de migration des documents et applicatifs propriétaires.