

E4R : ÉTUDE DE CAS

Durée : 5 heures

Coefficient : 5

CAS A'CLICK

Ce sujet comporte **13** pages dont **4** pages d'annexes.
Le candidat est invité à vérifier qu'il est en possession d'un sujet complet.

Matériels et documents autorisés

- Lexique SQL sans commentaire ni exemple d'utilisation des instructions
- Règle à dessiner les symboles informatiques

Aucune calculatrice n'est autorisée.

Liste des annexes

- Annexe 1 : Réseau Ethernet de la société A'CLICK*
Annexe 2 : Rappel sur les VLAN
Annexe 3 : Plan d'adressage IP en fonction des réseaux locaux virtuels
Annexe 4 : Configuration des commutateurs et des réseaux locaux virtuels
Annexe 5 : Le réseau VPN (Virtual Private Network)

Barème

Dossier 1 : Gestion du réseau de la société A'CLICK	23 points
Dossier 2 : Interconnexion des collaborateurs	27 points
Dossier 3 : Gestion des parutions	20 points
Dossier 4 : Suivi des logiciels	15 points
Dossier 5 : Mise en place d'un collecticiel	15 points
Total	100 points

CODE ÉPREUVE : ISE4R		EXAMEN : BREVET DE TECHNICIEN SUPÉRIEUR	SPÉCIALITÉ : INFORMATIQUE DE GESTION Option Administrateur de réseaux locaux d'entreprise
session 2008	SUJET	ÉPREUVE : ÉTUDE DE CAS	
Durée : 5 h	Coefficient : 5		Code sujet : 08AR05N
			Page : 1 / 13

PRÉSENTATION

La société A'CLICK est spécialisée dans la production et la distribution de logiciels ludiques et pédagogiques destinés aux enfants. Les logiciels distribués sont toujours accompagnés d'un fascicule sous forme de bandes dessinées qui permet à l'enfant d'appréhender plus simplement l'histoire, les personnages, les énigmes et les jeux du logiciel.

Par ailleurs, la société dispose d'un service rédaction pour l'élaboration de magazines quotidiens pour enfants.

L'impression des magazines et fascicules est réalisée par un imprimeur situé à 160 km environ.

Vingt personnes de la société A'CLICK collaborent à l'élaboration des logiciels, dont quatre en télétravail (à partir de leur domicile) et trois autres chez l'imprimeur pour la mise en forme des magazines et fascicules.

La société A'CLICK dispose déjà d'un réseau informatique reliant les collaborateurs à domicile (essentiellement des développeurs) et l'imprimeur.

Vous êtes chargé(e) dans un premier temps de participer à l'évolution de ce réseau afin d'optimiser les échanges internes dans la société et d'améliorer l'interconnexion des différents partenaires qui collaborent à la réalisation des logiciels et des magazines.

DOSSIER 1	GESTION DU RÉSEAU DE LA SOCIÉTÉ A'CLICK
------------------	------------------------------------------------

Annexes à utiliser : 1, 2, 3 et 4

Vous disposez du plan du réseau de la société (*annexe 1*).

Le réseau de la société A'CLICK dessert le rez-de-chaussée et le premier étage de deux bâtiments distants d'une trentaine de mètres.

Les serveurs principaux sont placés au premier étage du bâtiment A dans un local technique. Les personnels sont répartis sur les deux bâtiments.

Les développeurs sur site travaillent essentiellement dans le bâtiment B.

La société a mis en place un réseau basé sur une architecture Ethernet 100 Mbit/s commutée bidirectionnelle avec des liaisons fibres optiques entre les commutateurs ayant un débit de 1 Gbit/s.

Pour la configuration des commutateurs, l'administrateur a choisi une solution basée sur des **VLAN** (*Virtual Local Area Network*) de niveau 1 (*annexe 2*).

TRAVAIL À FAIRE	
1.1	Présenter les critères qui plaident en faveur de l'utilisation de réseaux locaux virtuels.

Le plan d'adressage IP en fonction des réseaux locaux virtuels et la configuration actuelle des commutateurs sont spécifiés dans les *annexes 3 et 4*.

TRAVAIL À FAIRE	
1.2	Indiquer la classe, l'adresse réseau et le masque par défaut correspondant au plan d'adressage spécifié à l'annexe 3. Justifier les réponses.
1.3	Calculer le nombre d'hôtes que peut accueillir chacun des réseaux virtuels avec ce plan d'adressage.
1.4	Donner le nombre de domaines de diffusion (<i>broadcast</i>) mis en place par la configuration des commutateurs C2, C3, C4 et C5.

L'administrateur du réseau souhaite modifier la configuration des commutateurs (*annexe 4*).

L'administrateur connecte un poste (appartenant au réseau IP 192.168.10.32/27 et configuré sans passerelle) sur le port libre **c2e8** du commutateur **C2** pour le configurer. Il lance ensuite la commande **http://192.168.10.33** pour accéder à la page d'accueil de l'outil d'administration du commutateur C2.

Il obtient le message "**page web non disponible hors connexion**" "**terminé**".

Pour comprendre la nature du problème, il effectue les trois tests suivants :

Test1 : Il lance la commande **ping 192.168.10.33**

Il obtient le message "**Délai d'attente de la demande dépassé**".

Test2 : Depuis le poste il branche un câble console sur le commutateur C2 et lance une connexion série avec les propriétés (Bits par seconde : 9600, Bits de données : 8, Parité : Aucun, Bits d'arrêt : 1, Contrôle de flux : Matériel).

Il obtient le message de connexion « **Login :** » permettant d'accéder à l'outil d'administration.

Test3 : Il connecte alors directement le poste (en Ethernet) sur le port libre c3e8 du commutateur C3 et lance la commande **http://192.168.10.34**

Il obtient la page *web* d'accueil de l'outil d'administration du commutateur C3.

TRAVAIL À FAIRE	
1.5	Donner la raison pour laquelle l'administration du commutateur C2 ne peut se faire actuellement que par le câble console. Proposer une solution pour résoudre ce problème.

Suite à une réorganisation des équipes de projet, il est nécessaire de déplacer le poste de travail d'un développeur, identifié **Dev5**, pour l'installer au rez-de-chaussée du bâtiment **B**. Ce poste est relié par l'intermédiaire d'une prise murale, au port **c4e7** du commutateur **C4**.

Après ce changement, l'administrateur constate que le poste **Dev5** ne peut plus communiquer avec son serveur d'applications **Sappl**. Il réalise différents tests à partir de la prise et en conclut que ce n'est pas un problème de connexion physique.

TRAVAIL À FAIRE	
1.6	Expliquer pourquoi ce déplacement a généré ce problème. Proposer une solution pour que le poste Dev5 puisse de nouveau communiquer avec son serveur d'applications à partir de son nouvel emplacement.

Tous les postes du réseau peuvent communiquer entre eux grâce à la fonction de routage activée sur C2 qui est un commutateur de niveau 3. Cependant, l'administrateur n'a pas encore ajouté dans la table de routage de C2, la route par défaut pour accéder à Internet. La syntaxe de la commande pour ajouter une route dans la table de routage de C2 est décrite dans l'*annexe 4*.

TRAVAIL À FAIRE	
1.7	Écrire l'instruction qui ajoute une route dans la table de routage de C2 pour autoriser tous les postes du réseau à accéder à Internet.

L'étude des flux sur les réseaux montre qu'après le redémarrage de l'ensemble des commutateurs une multitude de trames de diffusion ARP parviennent au portable de l'administrateur.

Celui-ci entreprend des recherches sur Internet et obtient des réponses lui expliquant un problème de "**tempête de broadcast**".

TRAVAIL À FAIRE	
1.8	Expliquer l'expression "tempête de broadcast" et ce qui a provoqué ce problème. Indiquer quel protocole (ou algorithme) l'administrateur doit activer sur les commutateurs pour résoudre ce problème.

Annexes à utiliser : 1 et 5

Les pages des magazines sont stockées dans une base de données. Elles sont composées de textes et d'images numérisées et d'attributs de mise en forme. Les flux de communication avec l'imprimeur sont de simples transferts de données composant le magazine : texte, images et attributs de mise en page.

La solution utilisée actuellement pour relier l'entreprise à la société **A'CLICK** repose sur une liaison à distance Numéris à 64 Kbit/s point à point.

L'impression quotidienne des magazines pour enfant étant en constante augmentation, l'adaptation de la ligne de communication reliant la société **A'CLICK** à l'imprimeur devient une priorité.

Le responsable du réseau estime en effet que le transfert des pages d'un magazine est trop long. Ainsi, pour le transfert d'une page de 300 Ko à laquelle s'ajoute 15 % de données de gestion (des différents protocoles mis en œuvre lors du transfert), il faut près de 44 secondes.

TRAVAIL À FAIRE	
2.1	Déterminer la bande passante minimum nécessaire, exprimée en Kbit/s, que doit supporter la liaison pour ramener le temps de transfert d'une page à environ 10 secondes (<i>justifier la réponse, prendre 1 Ko = 1 000 octets</i>).

L'administrateur constate que pour obtenir des temps de transfert de pages et un coût acceptables, il va falloir augmenter considérablement les débits de transfert.

Lors d'une réunion, la direction de la société a donné son accord pour augmenter les débits via Internet.

Pour améliorer les capacités d'accès, l'administrateur propose la mise en place d'une technologie ADSL pour les développeurs à domicile et d'une technologie SDSL **pour l'imprimeur**.

TRAVAIL À FAIRE	
2.2	Expliquer les principales différences techniques qui existent entre l'ADSL et le SDSL proposées par l'administrateur.

La connexion devra se faire de manière cryptée, virtuelle, point à point, avec une passerelle **VPN** (*Virtual Private Network*) dite aussi **RPV** (Réseau Privé Virtuel), située sur le routeur **Rte_A'click** de la société. Elle offrira ainsi aux développeurs et à l'imprimeur une extension du réseau privé.

Les développeurs à domicile pourront se connecter à Internet, puis établir une connexion VPN vers le réseau de la société.

Pour la mise en place de ce tunnel VPN, le routeur **Rte_A'click** doit posséder une adresse IP publique fixe, utiliser un pare-feu effectuant de la translation d'adresses et être capable de rediriger une demande vers une adresse IP privée (*annexes 1 et 5*).

TRAVAIL À FAIRE	
2.3	Expliquer la démarche que doit suivre l'administrateur du réseau pour obtenir une adresse IP publique fixe.
2.4	Lister les avantages (en dehors des débits) d'une solution DSL/VPN en lieu et place de l'ancienne solution Numéris.

Après ces démarches, l'adresse IP attribuée à l'interface publique est **66.101.21.12**. En plus des accès à Internet, les données circulant sur le routeur **Rte_A'click** proviennent des échanges entre l'imprimeur et le serveur de base de données **Ssgbd** ainsi que des échanges entre les développeurs à domicile et le serveur Intranet **Sweb**.

TRAVAIL À FAIRE	
2.5	Écrire la table de routage du routeur Rte_A'click, à partir des informations de l'annexe 1.

Les fonctions de filtrage du routeur **Rte_A'click** sont déjà activées sur l'interface publique 66.101.21.12 et sur l'interface privée 172.16.120.253. Les tableaux ci-dessous donnent un extrait des tables de filtrage correspondant à chacune de ces interfaces :

Table de filtrage de l'interface publique (66.101.21.12) du routeur Rte_A'click

N° de règle	Adresse source	Port source	Adresse destination	Port destination	Protocole	Action
1	Toutes	Tous	66.101.21.12/32	tous	GRE	Accepter
2	66.101.21.12/32	1723	Toutes	tous	TCP (établi)	Accepter
3	Toutes	Tous	66.101.21.12/32	1723	TCP	Accepter
4	Toutes	Tous	66.101.21.12/32	500	UDP	Accepter
6	Toutes	Tous	66.101.21.12/32	1701	UDP	Accepter
7	Toutes	Tous	66.101.21.12/32	4500	UDP	Accepter
...	...					
Défaut	Toutes	Tous	Toutes	Tous	Tous	Bloquer

Table de filtrage de l'interface privée (172.16.120.253) du routeur Rte_A'click

N° de règle	Adresse source	Port source	Adresse destination	Port destination	Protocole	Action
...	...					
Défaut	Toutes	Tous	Toutes	Tous	Tous	Accepter

TRAVAIL À FAIRE	
2.6	Expliquer les règles de filtrage 2 et 3 appliquées sur l'interface publique.

Lors de la mise en place du tunnel à la connexion, le serveur VPN doit attribuer aux développeurs à domicile une adresse IP, prise sur une étendue statique allant de **172.16.120.8** à **172.16.120.15**. L'imprimeur, quant à lui, doit toujours recevoir l'adresse IP **172.16.120.100**.

Les développeurs à domicile ont accès au serveur de base de données **Ssgbd** et au serveur Intranet **Sweb**, mais en aucun cas l'imprimeur ne pourra accéder au serveur Intranet **Sweb**.

Ni les développeurs à domicile, ni l'imprimeur ne doivent avoir accès au réseau interne de la société.

TRAVAIL À FAIRE	
2.7	Ajouter la (les) règle(s) de filtrage à mettre en place sur l'interface 172.16.120.253 du routeur Rte_A'click, afin de respecter les accès précisés ci-dessus, sachant que l'action de la règle par défaut est « Accepter ».

Une base de données relationnelle a été implantée pour suivre la création et l'impression des différentes parutions (magazines et fascicules). Sa description est la suivante :

PARUTION(num, titre, redacteur, dateParution)

num *clé primaire*

PAGE(id, numero, miseEnForme, numParution)

id *clé primaire*

numParution *clé étrangère en référence à num de PARUTION*

TEXTE(num, titre, descriptif, nombreLignes)

num *clé primaire*

IMAGE(num, titre, descriptif, largeur, hauteur, poids)

num *clé primaire*

COMPORTE_TEXTE(numTexte, idPage)

numTexte, idPage *clé primaire*

idPage *clé étrangère en référence à id de PAGE*

numTexte *clé étrangère en référence à num de TEXTE*

COMPORTE_IMAGE(numImage, idPage)

numImage, idPage *clé primaire*

idPage *clé étrangère en référence à id de PAGE*

numImage *clé étrangère en référence à num de IMAGE*

miseEnForme dans PAGE désigne la police du texte et sa taille.

nombreLignes dans TEXTE désigne le nombre de lignes dans un texte.

poids dans IMAGE désigne la taille de l'image sur le disque dur, exprimée en Kilo-octets.

TRAVAIL À FAIRE	
3.1	Construire le schéma entité-association correspondant à l'ensemble des relations décrites.
3.2	Écrire la requête SQL permettant d'obtenir la liste (numéro, titre et poids) des images dont le poids est supérieur à 1 000 Kilo-octets.
3.3	Écrire la requête SQL permettant d'obtenir le nombre de lignes pour chaque parution, trié par ordre décroissant du nombre de lignes.
3.4	Écrire la requête SQL permettant d'obtenir le(s) rédacteur(s) qui participe(nt) au plus grand nombre de parutions.

Vous êtes l'administrateur de cette base de données et vous devez enregistrer les droits de l'utilisateur Dupont. Sur la table PARUTION celui-ci est autorisé à consulter tous les attributs mais ne peut modifier que la date de parution.

TRAVAIL À FAIRE	
3.5	Écrire la requête SQL permettant d'attribuer les droits à l'utilisateur Dupont.

Le responsable financier de la société A'CLICK souhaite évaluer le temps qui a été nécessaire aux développeurs pour réaliser les logiciels. Au maximum un développeur ne peut travailler que sur cinq logiciels différents par semaine.

Sur le serveur Intranet **Sweb**, une application *Web* est mise en place pour collecter les renseignements auprès des développeurs. En fin de semaine, les développeurs se connectent sur le serveur pour renseigner l'application.

Exemple : Le développeur Titouan Dupont, de matricule D1, a travaillé durant la semaine du 21/04/2008, sur trois logiciels (L1, L3 et L7) et a passé respectivement 800, 400 et 600 minutes pour chaque logiciel.

TRAVAIL À FAIRE	
4.1	Élaborer la maquette du formulaire de saisie de l'application à partir de l'exemple précédent.
4.2	Indiquer le(s) contrôle(s) à mettre en place pour valider la saisie.

Un script de l'application génère un fichier séquentiel qui contient les différents relevés hebdomadaires du temps passé par les développeurs.

Le fichier contient des enregistrements qui se présentent sous la forme suivante :

Dev structure de

numDev : chaîne
 numLog : chaîne
 dateSem : Date
 temps : entier (exprimé en minute)

Fin structure

fDev : fichier de Dev

Extrait du fichier :

numDev	numLog	dateSem	temps
D1	L1	14/04/2008	220
D1	L1	21/04/2008	800
D2	L1	07/04/2008	320
D3	L1	07/04/2008	484
D2	L2	28/04/2008	421
D4	L2	21/04/2008	314
D1	L3	21/04/2008	400
...			

Le fichier est trié en premier lieu (critère majeur) sur le numéro de logiciel et, en deuxième lieu (critère mineur) sur le numéro de développeur.

Vous disposez de la fonction CONVERT qui permet de convertir un temps, exprimé en minutes, sous la forme d'un temps exprimé en heures et minutes (hh : mm) :

Fonction CONVERT(tps : entier) : chaîne

TRAVAIL À FAIRE	
4.3	Présenter l'algorithme qui permet d'afficher pour chaque logiciel, le temps total de développement. <i>NB : L'affichage du temps sera exprimé en heures et minutes</i>

DOSSIER 5**MISE EN PLACE D'UN COLLECTICIEL**

Actuellement les équipes qui travaillent sur un magazine, un fascicule ou un logiciel, se réunissent une fois par mois dans les locaux de la société A'CLICK.

Ces réunions sont l'occasion pour les membres d'une équipe de soumettre des modifications à apporter aux projets. Toute demande de modification doit être soumise préalablement au chef de projet, puis discutée au cours de cette réunion.

Afin d'améliorer la productivité et de profiter de la nouvelle architecture réseau mise en place, il a été décidé de mettre en place un collecticiel sur le serveur Intranet.

Une consultation du personnel a permis de définir les besoins des utilisateurs de ce collecticiel.

Le tableau ci-dessous vous présente les différentes tâches planifiées.

Numéro	Description des tâches	Durée en jours	Tâches précédentes
A	Évaluation du coût	7	
B	Consultation du personnel	15	
C	Achat du logiciel	5	A, B, G
D	Mise en place du système	7	A, C
E	Formation à l'utilisation	10	D
F	Tests	15	C, D
G	Recherche du mode de financement	7	A, B, H
H	Choix du logiciel	7	

Le choix du logiciel doit commencer au moins trois jours après le début de la consultation du personnel.

L'évaluation des coûts doit commencer, quant à elle, sept jours après cette même consultation.

TRAVAIL À FAIRE	
5.1	Établir le graphe utilisant la méthode MPM ou PERT (les dates de début au plus tôt et au plus tard, marge totale et marge libre devront figurer sur votre graphe ainsi que le chemin critique).

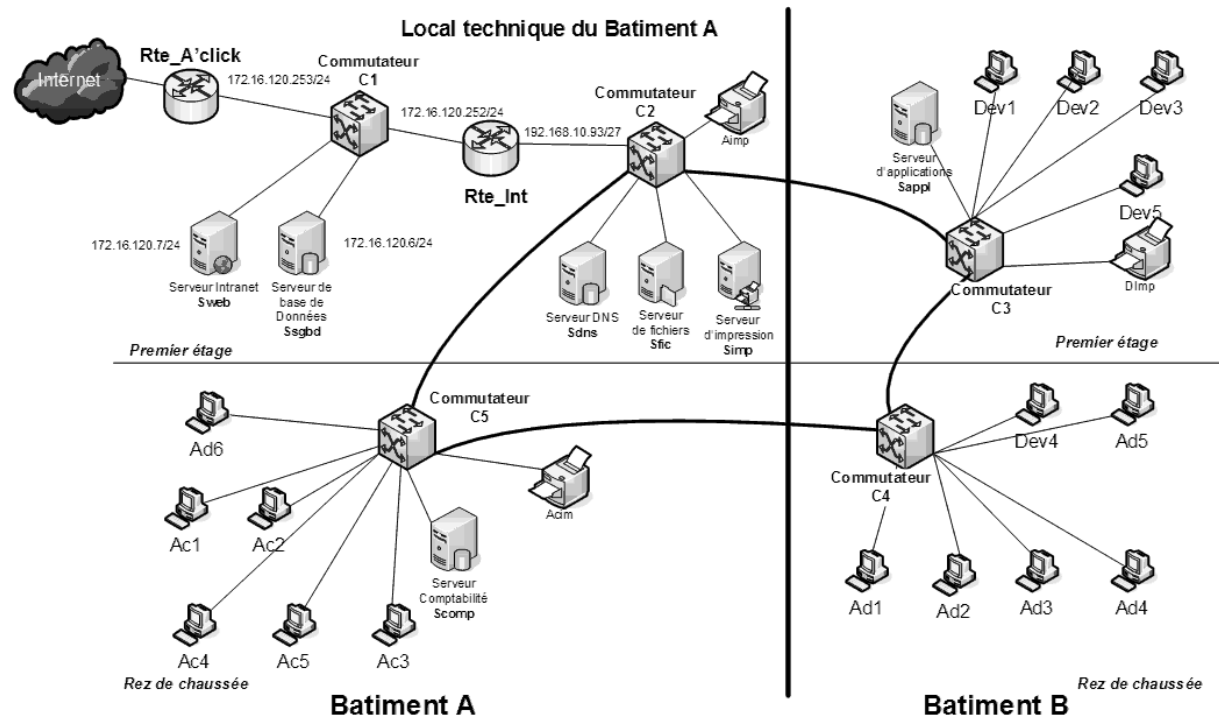
La durée de la tâche "Évaluation du coût" a été sous estimée. Elle passe de 7 à 9 jours.

TRAVAIL À FAIRE	
5.2	Préciser la conséquence de cette modification.

L'installation de ce nouvel environnement de travail va provoquer des changements dans l'organisation actuelle de la société.

TRAVAIL À FAIRE	
5.3	Expliquer les apports de la mise en œuvre d'un collecticiel dans l'organisation du travail de la société. Indiquer les freins éventuels à sa mise en œuvre

ANNEXE 1 : Réseau Ethernet de la société A'CLICK



ANNEXE 2 : Rappel sur les VLAN

Les réseaux locaux virtuels (VLAN) permettent de créer des domaines de diffusion, gérés par des commutateurs. Une trame ne peut être associée qu'à un VLAN et cette trame ne peut être diffusée que sur les ports du commutateur associés à ce VLAN. Une trame ou un port peuvent être associés à un VLAN de manière statique ou dynamique :

- **Statique** : chaque port du commutateur est affecté à un VLAN par l'administrateur, une trame en entrée sur ce port sera associée au VLAN du port. On parle de **VLAN de niveau 1** ou VLAN par port.
- **Dynamique** : chaque port du commutateur se voit affecté dynamiquement à un VLAN à partir d'une information contenue dans la trame en entrée sur ce port. Cette affectation peut être définie en fonction de l'adresse MAC émettrice, de l'adresse IP émettrice, d'un protocole, etc. contenues dans la trame. On parle de **VLAN de niveau 2** (VLAN d'adresse MAC) **de niveau 3** (VLAN d'adresse IP) ou de **niveau applicatif** (VLAN basé sur les protocoles d'application).

On considère qu'un port de commutateur ne sera associé qu'à un seul VLAN à l'exception des ports d'interconnexion 802.1q. Un port 802.1q (dit *tagged port*) transporte des trames étiquetées avec un en-tête 802.1q qui permet d'associer la trame à un VLAN. Ce port est généralement réservé à la communication entre commutateurs.

Une trame ne peut être associée qu'à un seul VLAN. Chaque VLAN peut être géré par un commutateur ou par plusieurs et un commutateur peut gérer un ou plusieurs VLAN.

Lorsqu'un commutateur reçoit une trame de diffusion (*broadcast*), il la transmet d'une part à l'ensemble des ports sur lesquels sont reliés les postes appartenant au même VLAN que l'émetteur, d'autre part aux ports 802.1q affectés à ce VLAN.

ANNEXE 3 : Plan d'adressage IP en fonction des réseaux locaux virtuels

Chaque VLAN correspond à un sous-réseau IP.

- VLAN 1 (VLAN par défaut) : Pour les postes du service administratif, adresse réseau 192.168.10.32 masque 255.255.255.224
- VLAN 2 : Pour les postes du service de comptabilité, adresse réseau 192.168.10.64 masque 255.255.255.224
- VLAN 3 : Pour les postes du service développement et serveurs, adresse réseau 192.168.10.96 masque 255.255.255.224

La communication entre les VLAN est assurée par la fonction de routage activée sur C2, commutateur de niveau 3. Pour constituer la table de routage de C2, une adresse IP est affectée à chaque VLAN sur le commutateur C2, soit :

VLAN 1 : 192.168.10.62/27 VLAN 2 : 192.168.10.94/27 VLAN 3 : 192.168.10.126/27

Chaque poste du réseau est configuré avec une passerelle par défaut qui est l'adresse IP du VLAN correspondant, mis en place sur le commutateur C2, soit :

- Service administratif, VLAN 1 (VLAN par défaut), passerelle par défaut : 192.168.10.62
- Service de comptabilité, VLAN 2, passerelle par défaut : 192.168.10.94
- Service de développement et serveurs, VLAN 3, passerelle par défaut : 192.168.10.126

ANNEXE 4 : Configuration des commutateurs et des réseaux locaux virtuels

Commutateur C2 :

Administrable sur le VLAN2,

192.168.10.33/27

Protocole 802.1q activé, ports : c2f1, c2f2

Routage activé

Table gérée du C2

VLAN1		VLAN2		VLAN3	
Port	Poste	Port	Poste	Port	Poste
c2e1	Aimp	c2e2	Rte_Int	c2e3	Sdns
c2e6				c2e4	Sfic
c2e7				c2e5	Simp
c2e8					
c2e9					
c2ea					
c2eb					
c2ec					

Commutateur C5 :

Administrable sur le VLAN3,

192.168.10.97/27

Protocole 802.1q activé, ports : c5f1, c5f2

Table gérée du C5

VLAN1		VLAN2		VLAN3	
Port	Poste	Port	Poste	Port	Poste
c5e1	Ad6	c5e2	Ac1	c5e8	Scomp
c5e9		c5e3	Ac2		
c5ea		c5e4	Ac3		
c5eb		c5e5	Ac4		
c5ec		c5e6	Ac5		
		c5e7	Acim		

Commutateur C3 :

Administrable sur le VLAN1, 192.168.10.34/27

Protocole 802.1q activé, ports : c3f1, c3f2

Table gérée du C3

VLAN1		VLAN2		VLAN3	
Port	Poste	Port	Poste	Port	Poste
c3e7				c3e1	Sappl
c3e8				c3e2	Dev1
c3e9				c3e3	Dev2
c3ea				c3e4	Dev3
c3eb				c3e5	Dev5
c3ec				c3e6	Dimp

Commutateur C4 :

Administrable sur le VLAN1, 192.168.10.35/27

Protocole 802.1q activé, ports : c4f1, c4f2

Table gérée du C4

VLAN1		VLAN2		VLAN3	
Port	Poste	Port	Poste	Port	Poste
c4e1	Ad1			c4e6	Dev4
c4e2	Ad2				
c4e3	Ad3				
c4e4	Ad4				
c4e5	Ad5				
c4e7					
c4e8					
c4e9					
c4ea					
c4eb					
c4ec					

Chaque commutateur dispose d'au moins une adresse IP et est administrable **sur un seul VLAN**.

Seul C2 est un commutateur de niveau 3 qui possède une fonction de routage. Il est configuré pour assurer la communication entre les réseaux locaux virtuels.

La commande pour ajouter une route dans la table de routage de C2 est la suivante :

Syntaxe :

ADD IP ROUTE=ipadd1 INTERFACE=vlan NEXTHOP=ipadd2 [MASK=ipadd3]

Paramètres :

ROUTE

ipadd1 : définit l'adresse IP du réseau destinataire (0.0.0.0 pour la route par défaut).

INTERFACE

vlan : définit le VLAN sur lequel est associée la route à ajouter (par exemple : INTERFACE=vlan1).

NEXTHOP

ipadd2 : définit l'adresse IP du prochain saut (routeur) pour cette route.

MASK

ipadd3 : définit le masque associé à cette route (réseau destinataire). Ce paramètre est facultatif.

S'il n'est pas défini, c'est le masque de la classe de l'adresse IP du réseau destinataire qui est utilisé (0.0.0.0 pour la route par défaut).

ANNEXE 5 : Le réseau VPN (*Virtual Private Network*)

Ce réseau VPN utilise soit le protocole **PPTP** (*Point to Point Tunneling Protocol*), soit le protocole **L2TP** (*Layer Two Tunneling Protocol*) pour établir une connexion.

Le serveur VPN : Le serveur VPN doit posséder une **adresse IP publique fixe** afin que les clients VPN puissent utiliser cette adresse ou un nom DNS correspondant pour établir leur connexion VPN.

Lors de la demande de connexion du client VPN, le serveur VPN attribue aux clients VPN une adresse IP privée prise sur une étendue statique prédéfinie.

Les paquets VPN entrent sur l'interface publique du serveur VPN. Après vérification des filtres en entrée, celui-ci les désencapsule du tunnel crypté (déchiffrement des données) et envoie le datagramme IP privé en sortie sur l'interface privée qui applique les filtres avant de transmettre le paquet vers le réseau privé.

Le filtrage du serveur VPN :

Le pare-feu doit laisser entrer sur l'interface publique les paquets VPN suivants :

- **Pour un tunnel PPTP (*Point to Point Tunneling Protocol*) :**
Adresse IP source : adresse IP publique du client VPN source
Adresse IP destination : adresse IP publique du serveur VPN destination
Port de destination : TCP/1723 (pour l'établissement et la maintenance du tunnel)
ID de protocole : GRE/47 (protocole spécifique pour les données encapsulées dans le tunnel)
- **Pour un tunnel L2TP/IPSec (*Layer Two Tunneling Protocol / Internet Protocol Security*) :**
Adresse IP source : adresse IP publique du client VPN source
Adresse IP destination : adresse IP publique du serveur VPN destination
Port de destination : UDP/500 (pour la gestion des clés d'authentification utilisées
pour sécuriser les informations)
Port de destination : UDP/1701 (trafic L2TP)
Port de destination : UDP/4500 (IPSec NAT-Transversal)