

E4R : ÉTUDE DE CAS

Durée : 5 heures

Coefficient : 5

CAS CHAUFFATLAN

Ce sujet comporte 15 pages dont 5 pages d'annexes.
Il est constitué de 5 dossiers qui peuvent être traités de façon indépendante.
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 : *Extrait du schéma réseau du groupe ChauffAtlan*
 Annexe 2 : *Extrait des configurations actuelles d'éléments du réseau*
 Annexe 3 : *Extrait de la documentation "InterLAN 2.0"*
 Annexe 4 : *Capture de trames*
 Annexe 5 : *Documentation sur les propositions de formation*
 Annexe 6 : *Extrait du schéma relationnel*

Barème

Dossier 1 : Architecture IP, routage et commutation	30 points
Dossier 2 : Optimisation et sécurité des échanges	30 points
Dossier 3 : Choix de gestion	14 points
Dossier 4 : Scripts de sauvegarde	12 points
Dossier 5 : Système d'information du service BIP	14 points

Total 100 points

CODE ÉPREUVE : ISE4R		EXAMEN : BREVET DE TECHNICIEN SUPÉRIEUR	SPÉCIALITÉ : INFORMATIQUE DE GESTION Option Administrateur de réseaux locaux d'entreprise	
SESSION 2011	SUJET	ÉPREUVE : ÉTUDE DE CAS		
Durée : 5 h	Coefficient : 5		Code sujet : 11AR04N	Page : 1/17

Présentation du contexte

Créé il y a une quarantaine d'années, le groupe ChauffAtlan est devenu le premier constructeur européen d'appareils de chauffage et de chauffe-eaux électriques.

Le groupe emploie 4 000 personnes et distribue de nombreuses marques d'équipement dans plus de cent pays. Ses sites (usines de production, filiales, agences, concessionnaires) sont répartis dans toute l'Europe, occidentale et orientale, jusqu'au Moyen-Orient.

Les directions générales et commerciales (DGC) sont installées en région parisienne mais les directions administratives du groupe sont installées en Vendée (85), à quelques kilomètres du site industriel d'origine.

La direction informatique concentre ainsi à La Roche-sur-Yon la quasi-totalité du personnel informatique du groupe, soit 50 personnes, réparties sur quatre missions : la gestion des projets applicatifs, le développement, le support aux utilisateurs (*helpdesk* accessible aux 2000 utilisateurs), et l'administration des systèmes et réseaux.

La cellule systèmes et réseaux emploie 9 personnes qui ont en charge l'ensemble des équipements informatiques portant le système d'information du groupe : serveurs, postes, matériels actifs et liaisons.

Cette cellule centrale est complétée par une équipe de RIS (responsable informatique de site). Cela représente une douzaine de personnes, dispersées sur les plus importants sites internationaux du groupe. Leur rôle est celui d'un correspondant technique, maîtrisant l'ensemble des compétences informatiques, capable de mettre en œuvre les choix de la direction informatique et de résoudre sur place l'essentiel des problèmes pouvant survenir.

Vous êtes actuellement employé(e) à l'essai au sein de la cellule systèmes et réseaux située dans la direction administrative à La Roche-sur-Yon. Le responsable, Monsieur MARTIN, aimerait bien voir en vous un(e) futur(e) RIS et souhaite tester vos connaissances sur quelques situations représentatives des activités d'un RIS.

Liaisons inter-sites

La plupart des sites du groupe ChauffAtlan sont interconnectés par des réseaux MPLS de plusieurs opérateurs. Ces réseaux *Multi-Protocol Label Switching* sont entièrement gérés par les opérateurs. Ils peuvent offrir plusieurs qualités de service (par exemple la différenciation des flux : données, voix, visio). Les réseaux locaux (LAN) du groupe accèdent aux réseaux MPLS via des lignes xDSL, le plus souvent des liaisons SDSL. Cette architecture rend transparent le routage des paquets entre les adresses publiques des différents sites du groupe. Sur le réseau de l'opérateur, les trames de l'entreprise sont marquées de telle sorte qu'elles n'atteignent jamais d'autres clients.

Pour relier certains sites français sans infrastructure informatique lourde ainsi que les sites de pays éloignés, dans lesquels les opérateurs français ne sont pas présents, le groupe ChauffAtlan utilise des liaisons VPN IPsec sur lignes xDSL.

Les différents LAN du groupe utilisent des adresses IP issues des trois plages privées des classes A, B et C du standard IPv4.

Dans chaque site, un serveur DHCP assure l'attribution des adresses IP aux équipements utilisant un adressage dynamique.

L'annexe 1 montre un extrait du réseau du groupe ChauffAtlan.

TRAVAIL À FAIRE	
1.1	Expliquer pourquoi les liaisons VPN sont des liaisons SDSL et non ADSL.
1.2	Lister les garanties apportées par ces liaisons VPN.

Adressage IP et routage

Suite à des travaux de maintenance, la cellule systèmes et réseaux vient d'être alertée par plusieurs collaborateurs de la direction commerciale de Bourg-la-Reine : plusieurs serveurs ne communiquent plus avec les serveurs de La Roche-sur-Yon.

Monsieur MARTIN connecte son ordinateur portable au réseau de la direction administrative (La Roche-sur-Yon) et lance une commande *ping* vers le serveur « Zimbra » situé à Bourg-la-Reine.

La commande échoue et le système affiche « Délai d'attente de la demande dépassée ». La liaison MPLS n'est pas en cause, et les routeurs et les serveurs sont tous actifs, le problème provient donc de la configuration d'un des routeurs.

Vous disposez en annexe 2 d'un extrait des configurations actuelles des équipements concernés.

TRAVAIL À FAIRE	
1.3	A. Reconstituer le cheminement de l'échange ICMP en donnant le nom du routeur et le numéro de la ligne utilisée dans la table de routage.
	B. Indiquer le ou les éléments de configuration qui ont dû être accidentellement modifiés, causant ainsi la panne.
	C. Proposer la ou les corrections nécessaires.

Actuellement, le site industriel ThermAtlan de Merville communique avec la direction administrative via le site de Bourg-la-Reine. Pour améliorer les performances, Monsieur MARTIN décide de permettre la communication directement entre les deux sites, via un nouveau routeur implanté à La Roche-sur-Yon (RW13) qui sera connecté au routeur de Merville (RW41).

Il vous demande de paramétrer les routeurs RW41 et RW13 qui utiliseront pour communiquer entre eux le réseau d'interconnexion 199.99.9.128/30.

TRAVAIL À FAIRE	
1.3	Déterminer les adresses IP qui pourront être affectées aux deux routeurs sur le réseau d'interconnexion. <i>Justifier la réponse.</i>

Commutation

À l'occasion de la rénovation du réseau informatique du site industriel RochAtlan de La Roche-sur-Yon, on envisage d'adopter le service « *Inter LAN 2.0 Ethernet* » proposé par FranceTélécom (Orange) pour interconnecter ce site avec la direction administrative, distante d'environ 2 kilomètres. La liaison actuelle entre les deux sites est une ligne louée à France Télécom (2 Mbps).

L'offre « *InterLAN 2.0 Ethernet* » assure une communication inter site en mode commuté (couche OSI 2). Adopter cette solution évite de recourir au routage pour des liaisons entre sites voisins pouvant partager un même réseau IP.

L'**annexe 3** présente la documentation fournie par l'opérateur.

Un test du service « *InterLAN 2.0 Ethernet* » vient d'être réalisé avec l'opérateur entre les deux sites. Les résultats du test montrent un important gain de latence, et un débit réel de 10 Mbps, comparable à ce qu'on obtient actuellement au sein d'un LAN.

En adoptant l'offre « *InterLAN 2.0 Ethernet* », on s'apprête à unifier l'adressage IP des deux sites (en étendant le réseau IP 10.1.0.0/16 à l'ensemble).

TRAVAIL À FAIRE	
1.4	Expliquer pourquoi une communication basée sur la commutation est plus rapide qu'une communication basée sur le routage.
1.5	Énumérer les matériels qui ne seront plus nécessaires pour assurer la liaison entre les deux sites après l'unification de l'adressage IP. <i>Justifier la réponse.</i>

Optimisation et sécurité des échanges sur le réseau local

La décision de déployer un réseau IP unique sur les deux sites de La Roche-sur-Yon a été adoptée. Pour augmenter la confidentialité entre les services et préserver la bande passante, les communications seront cloisonnées par des VLAN, comme cela se fait déjà dans plusieurs sites du groupe ChauffAtlan. Tous les serveurs devront être accessibles à partir des deux sites. On doit cependant conserver la même adresse réseau IP pour les deux sites (10.1.0.0/16).

Dans une salle réservée aux tests (salle "Labo"), trois solutions sont étudiées à l'aide de différentes maquettes.

On utilise la commande *ping* pour tester les communications. Cette commande renvoie une des trois réponses suivantes :

- délai d'attente dépassé
- impossible de joindre l'hôte de destination
- réponse de x.x.x.x (où x.x.x.x est l'adresse de l'hôte de destination)

Première solution (normalisée)

On décide de créer deux VLAN :

- le VLAN "Admin" dans lequel sont placés les postes de travail de la direction administrative.
- le VLAN "Indus" dans lequel sont placés les postes de travail du site industriel.

Tous les serveurs sont placés dans les deux VLAN. Les postes de travail n'ont pas de passerelle définie. On crée le sous-réseau 10.1.10.0/24 pour le VLAN "Admin" et le sous-réseau 10.1.20.0/24 pour le VLAN "Indus".

Chaque serveur a une carte réseau multi domiciliée dans les VLAN grâce à deux interfaces virtuelles. Celles-ci sont associées à chaque réseau IP et à chaque VLAN.

Chaque carte réseau des serveurs émet et reçoit des trames marquées 802.1q. Les ports des commutateurs auxquels sont rattachées les cartes réseaux des serveurs émettent et reçoivent des trames 802.1q et sont associés aux deux VLAN.

Les ports des commutateurs auxquels sont rattachés les postes de travail émettent et reçoivent des trames sans marque 802.1q.

A partir d'un poste du VLAN administratif d'adresse 10.1.10.1/24 on émet trois commandes :

- Un premier *ping* vers un poste de travail du VLAN "Indus" 10.1.20.1
- Un deuxième *ping* vers le serveur "IN1" en utilisant son adresse 10.1.20.200
- Un troisième *ping* vers ce même serveur "IN1" en utilisant son adresse 10.1.10.200

TRAVAIL À FAIRE

2.1	Indiquer quelles seront les réponses à chaque commande <i>ping</i> parmi les trois réponses attendues. <i>Justifier les réponses.</i>
------------	---

Deuxième solution (propriétaire)

Cette solution enrichit les VLAN de la spécificité suivante, un port appartenant à un VLAN peut être déclaré pour ce VLAN *isolated*, *promiscuous* ou *community* (ce dernier cas n'est pas étudié ici).

- Un port *isolated* ne peut émettre des trames que vers des ports *promiscuous* de son VLAN
- Un port *promiscuous* peut émettre des trames vers les ports *promiscuous* et *isolated* appartenant à son VLAN.

On déclare un seul VLAN "INAD" pour tous les postes de travail et les serveurs des deux sites. Les postes de travail sont placés sur des ports *isolated*, les serveurs sur des ports *promiscuous*. L'adresse réseau est 10.1.0.0/16. Les postes n'ont pas de passerelles définies.

À partir du poste du réseau administratif 10.1.10.1/16 on émet deux commandes :

- Un premier *ping* vers un poste de travail d'adresse 10.1.20.1/16
- Un deuxième *ping* vers le serveur "IN1" d'adresse 10.1.20.200/16

TRAVAIL À FAIRE	
2.2	Indiquer quelles seront les réponses à chaque commande <i>ping</i> parmi les trois réponses attendues. <i>Justifier les réponses.</i>

Troisième solution (autorisée par la norme dans une annexe informative)

Cette solution enrichit les VLAN de la spécificité suivante : un port **non taggué** appartient à un VLAN mais peut diffuser des trames émises par d'autres VLAN. On parle de **VLAN asymétriques**.

On déclare trois VLAN :

- le VLAN "Admin" auquel on associe tous les ports des postes de travail du site "administratif",
 - le VLAN "Indus" auquel on associe tous les ports des postes de travail du site "industriel",
 - le VLAN "Serveurs" auquel on associe tous les serveurs.
-
- Les ports du VLAN "Admin" émettent les trames dont ils sont à l'origine sur ce VLAN et peuvent diffuser les trames du VLAN "Serveurs".
 - Les ports du VLAN "Indus" émettent les trames dont ils sont à l'origine sur ce VLAN et peuvent diffuser les trames du VLAN "Serveurs".
 - Les ports du VLAN "Serveurs" émettent les trames dont ils sont à l'origine sur ce VLAN et peuvent diffuser les trames du VLAN "Admin" et du VLAN "Indus".

L'adresse réseau est 10.1.0.0/16. Les postes n'ont pas de passerelles définies.

A partir du poste du réseau administratif 10.1.10.1/16 on émet deux commandes :

- Un premier *ping* vers un poste de travail du VLAN "Indus" d'adresse 10.1.20.1/16
- Un deuxième *ping* vers le serveur "IN1" du VLAN "Serveurs" d'adresse 10.1.20.200/16

TRAVAIL À FAIRE	
-----------------	--

2.3	Indiquer quelles seront les réponses à chaque commande <i>ping</i> parmi les trois réponses attendues . <i>Justifier les réponses.</i>
-----	--

Monsieur MARTIN souhaite que la solution retenue prenne en compte les trois contraintes suivantes (le respect de la normalisation n'est pas une contrainte) :

- un plan d'adressage unifié (la même adresse réseau IP pour les deux sites)
- une étanchéité parfaite entre les deux sites.
- pas de communication des postes de travail entre eux, même à l'intérieur d'un VLAN.

TRAVAIL À FAIRE	
2.4	Indiquer la solution qui répond le mieux à ces trois contraintes. <i>Justifier la réponse.</i>

Sécurité des échanges sur le web

Monsieur MARTIN vous a présenté les outils logiciels qu'il a l'habitude d'utiliser pour analyser les problèmes techniques, parmi lesquels se trouve un analyseur de trames. Il vous soumet la capture de trames présentée en **annexe 4**.

Cette capture a été réalisée sur le poste d'un secrétaire situé à Barcelone alors que celui-ci validait dans son navigateur Internet l'URL d'un site *web* de la Sécurité Sociale française « assure.ameli.fr ».

La communication met en relation le poste du secrétaire (192.168.1.83) avec deux serveurs internet (93.174.145.36 et 199.16.83.72). La capture montre les six premières secondes de la navigation.

TRAVAIL À FAIRE	
2.5	Expliquer quel est l'objet des trames 1 et 2.
2.6	Donner le protocole <u>applicatif</u> employé entre le navigateur et le serveur <i>web</i> , à partir de l'étude des trames 3 à 9.
2.7	Expliquer à quelles étapes de la communication correspondent les trames 3 à 5 et 19 à 22.

On observe qu'avant la poursuite de la communication entre le navigateur *web* du secrétaire et le serveur *web* 93.174.145.36, a lieu un court échange entre le navigateur et un autre serveur *web* ayant pour adresse 199.16.83.72 (trames 12 à 22).

Monsieur MARTIN vous souligne que dans cet échange, la trame 18 contient un bloc nommé « *Online Certificate Status Protocol* », dont un champ nommé *responsesStatus* affiche la valeur *successful*.

TRAVAIL À FAIRE	
2.8	Indiquer, au vu du contenu des trames 10 à 22 résumé par l'analyseur de trames, à quoi correspond cette communication intermédiaire et quel est le rôle du serveur 199.16.83.72.

Choix d'un fournisseur d'accès à internet (FAI)

En Ukraine, le groupe ChauffAtlan possède un site industriel à Borispol et les locaux de sa filiale AtlanGeyser à Kharkov. Les deux sites, distants de 400 kilomètres, sont reliés par un tunnel VPN, qui s'appuie sur deux abonnements ADSL (1Mbit/s, 256Kbit/s) souscrits auprès du fournisseur d'accès local DataGroup, pour un coût mensuel de 25€ par site.

Cette liaison n'étant pas toujours fiable, il a été décidé de souscrire, pour chaque site, un 2ème abonnement auprès d'un autre fournisseur (le même fournisseur pour les deux sites).

- Le FAI Valor propose un abonnement ADSL (4Mbit/s, 512Kbit/s) au prix de 50 € par mois. Le débit n'étant pas garanti, on estime le débit réel moyen sur une telle ligne à 1,2Mbit/s et 400Kbit/s (soit 150 KiloOctets par seconde en débit descendant et 50 KiloOctets par seconde en débit montant).
- Le FAI [Infokom](#) propose de son côté un abonnement professionnel SDSL (2Mbit/s, 2Mbit/s) au prix de 250 € par mois. Le débit est garanti (soit 250 KiloOctets par seconde en débit montant et descendant).

Le trafic quotidien sur cette liaison est essentiellement composé du transfert, 4 fois par jour, d'une base de données de Borispol vers Kharkov (volume supposé de la base : 100 MegaOctets de données) et de la sauvegarde nocturne complète des données du site de Kharkov sur celui de Borispol (volume supposé : 500 MegaOctets de données).

On observe que les sites ukrainiens fonctionnent en moyenne 25 jours par mois.

Remarque : dans les calculs, considérer 1 GigaOctet (Go) = 1 000 MégaOctets (Mo).

TRAVAIL À FAIRE	
3.1	Déterminer pour chacune des deux offres le temps quotidien nécessaire à l'ensemble des transferts.
3.2	Déterminer pour ces deux offres le coût mensuel du Mo transporté sur un volume estimé à 1 Go par jour
3.3	Commenter les résultats obtenus.

Choix d'un mode de formation

La cellule systèmes et réseaux envisage l'adoption de la VoIP au sein de l'ensemble du groupe ChauffAtlan. Cela se fera avec le concours de la société STVY, prestataire installé à La Roche-sur-Yon, spécialisé dans les domaines de la téléphonie, de la sécurité et des réseaux. L'étude technique menée avec STVY a permis de dégager une solution qui englobe des matériels de la gamme Alcatel OmniPCX, des logiciels et des prestations, lesquels ont fait l'objet d'une offre détaillée et chiffrée.

Monsieur MARTIN souhaite que deux techniciens du groupe soient formés 4 jours aux technologies concernées (ToIP, VoIP, CTI -couplage téléphonie internet-). Comme l'explique l'**annexe 5A**, plusieurs méthodes de formation sont envisageables. Les **annexes 5B et 5C** proposent plusieurs modalités de formation pour ce projet.

TRAVAIL À FAIRE	
3.4	Exploiter les données de l' annexe 5 pour construire un tableau comparatif des trois modes de formation en termes de coût et d'adaptation aux besoins et conclure en justifiant le choix de la méthode de formation la plus adaptée pour les informaticiens du groupe ChauffAtlan.

Dossier 4 – Scripts de sauvegarde

L'administration des nombreuses bases de données du groupe est actuellement l'objet d'un projet de réalisation d'un « gestionnaire de tâches coopératif ». Le futur logiciel à développer servira à coordonner les opérations de sauvegardes de sécurité qui sont réalisées chaque jour dans les différents sites du groupe ainsi que les opérations de centralisation des données réclamées par les différentes directions commerciales du groupe. Sur chaque site est installé un serveur NAS chargé de sauvegarder quotidiennement les bases de données présentes sur le site. Le serveur NAS dispose des procédures et fonctions suivantes :

fonction listeTables(nomBase:chaîne):tableau[1 à 100] de chaîne <i>/* Renvoie un tableau contenant la liste des noms des tables d'une base de données */</i> fonction sauveTable(nomTable:chaîne):chaîne <i>/* Renvoie une chaîne de caractères correspondant au contenu d'une table (ensemble des données) */</i> procédure sauveBase(nomBase : chaîne) <i>/* Crée un fichier pour chacune des tables d'une base */</i> dateJour, nomFichier: chaîne nomTable : tableau[1 à 100] de chaîne i : entier	DEBUT dateJour ← date() <i>// renvoie date au format AAMMJJ</i> nomTable ← listeTables(nomBase) POUR i de 1 à 100 SI tables[i] <> "" ALORS nomFichier←"/BDDCOPY/"+dateJour+"/"+ nomBase+"/"+nomTable[i]+".txt" OUVRIER(nomFichier, écriture) ECRIRE(nomFichier, sauveTable(nomTable[i])) FERMER(nomFichier) FINSI FINPOUR FIN
--	--

Remarques : Les scripts sont à considérer comme indépendants des outils exploitant le langage SQL sur les SGBDR concernés. Par simplification, on ignorera ici les problèmes de connexion auprès des SGBDR

On souhaite modifier la procédure *sauveBase()* afin qu'il n'y ait qu'un seul fichier par base sauvegardée. Le nom de la base sera passé en paramètre. Le contenu d'un fichier associé à une base sera de la forme :

```
Nom de la table 1
Contenu de la table 1
Nom de la table 2
Contenu de la table 2
...
Nom de la table n
Contenu de la table n
```

TRAVAIL À FAIRE

4.1	Réécrire la procédure <i>sauveBase()</i> afin qu'elle réponde aux nouvelles attentes. La déclaration des variables n'est pas demandée.
------------	--

La procédure *sauveBase()* ne sauvegarde qu'une seule base de données à la fois et il est nécessaire de l'exécuter manuellement pour chaque base du site. On dispose d'un fichier contenant l'ensemble des noms des bases à sauvegarder (*listeBases.txt*).

On souhaite créer une procédure *sauveServeur()* qui permette la sauvegarde de toutes les bases de données du site en faisant appel à la procédure *sauveBase()*.

Exemple de fichier texte <i>listeBases.txt</i> :	Exemple d'appel :
gestion_comm gestion_stocks compta	sauveserveur("listeBases.txt")

TRAVAIL À FAIRE	
4.2	Écrire la procédure <i>sauveServeur()</i> .

Dossier 5 – Système d'information du service BIP

Document à utiliser : annexe 6

Pour son service d'assistance technique clients, le groupe ChauffAtlan utilise une application de gestion connue sous le nom de « service BIP » (bureau info produits). À la demande des opérateurs qui utilisent cette application, des modifications sont envisagées afin de répondre au mieux à la demande des clients et de faciliter l'interrogation de la base de données.

Monsieur MARTIN vous confie l'évolution du système d'information relatif à cette base de données.

La gestion des appels au service BIP

Les opérateurs téléphoniques et les techniciens qui travaillent au service BIP exploitent certains objets de la base de données BIP pour conserver la trace des appels et suivre les dossiers.

Lorsqu'un distributeur appelle pour signaler un problème sur un matériel, un dossier est ouvert. Les appels téléphoniques qui suivent sont accumulés dans ce dossier, jusqu'à la résolution du problème qui entraîne la fermeture du dossier.

On veut savoir quels sont les opérateurs qui ont suivi un dossier et les réponses qu'ils ont apportées. Un opérateur est identifié par un numéro et caractérisé par un nom et un prénom.

TRAVAIL À FAIRE	
5.1	Modifier le schéma relationnel pour prendre en charge cette nouvelle fonctionnalité.

Les opérateurs aimeraient repérer les matériels qui font l'objet de dossiers, de manière à mieux se former. Ils désirent connaître pour chaque type de matériel, le nombre de dossiers (quel qu'en soit l'état). La liste doit afficher le libellé du type de matériel avec le nombre de dossiers correspondant et devra être triée sur le nombre de dossiers, du plus grand au plus petit.

TRAVAIL À FAIRE	
5.2	Rédiger en langage SQL, la requête permettant d'obtenir ces informations.

Le responsable de la plateforme téléphonique, Monsieur SOLAIR, dont le login de connexion est « solair_d », désire pouvoir effectuer des modifications sur les tables DOSSIER_BIP et APPEL. Actuellement, il n'a que des droits restreints.

TRAVAIL À FAIRE	
5.3	Rédiger les requêtes permettant d'attribuer tous les droits à monsieur SOLAIR sur ces tables.

Monsieur SOLAIR souhaite que les opérateurs téléphoniques aient accès facilement à l'ensemble des attributs d'un dossier ouvert et la date du dernier appel associé à ce dossier.

TRAVAIL À FAIRE	
5.4	Écrire la requête qui permet la création de la vue DOSSIER_BIP_OUVERT répondant à la demande exprimée.
5.5	Indiquer l'intérêt des vues au sein d'un SGBDR.



ANNEXE 2 – Extrait des configurations actuelles d'éléments du réseau

Éléments concernés par la panne

Portable de l'administrateur de la direction administrative (La Roche-sur-Yon)

Adresse IP : 10.1.0.25

Masque : 255.255.0.0

Passerelle : 10.1.200.254

Serveur Zimbra de la direction commerciale (Bourg-la-Reine)

Adresse IP : 172.16.0.25

Masque 255.255.0.0

Passerelle : 172.16.200.254

Remarque ; le préfixe "RL" correspond à un routeur d'accès aux "réseaux locaux" le préfixe "RW" correspond à un routeur d'accès aux réseaux distants (MPLS).

Configuration du routeur RL1

Interface locale	10.1.200.254/16
Interface vers RW11	192.168.11.1/24
Interface vers RW12	192.168.12.1/24
Interface vers RW13	192.168.13.1/24
Interface vers RW14	192.168.14.1/24

Extrait de la table de routage du routeur RL1

	Destination	Masque	Passerelle	Interface
1	10.1.0.0	255.255.0.0	10.1.200.254	10.1.200.254
2	172.16.0.0	255.255.0.0	192.168.12.254	192.168.12.1
3	172.18.0.0	255.255.0.0	192.168.12.254	192.168.12.1
4	172.20.0.0	255.255.0.0	192.168.13.254	192.168.13.1
5	0.0.0.0	0.0.0.0	192.168.11.254	192.168.11.1

Configuration du Routeur RW12

Interface locale	192.168.12.254/24
Interface vers MPLS Bouygues	66.20.10.1/16

Extrait de la table de routage routeur RW12

	Destination	Masque	Passerelle	Interface
1	10.1.0.0	255.255.0.0	192.168.12.1	192.168.12.254
2	172.16.0.0	255.255.0.0	66.20.20.1	66.20.10.1
3	172.18.0.0	255.255.0.0	66.20.30.1	66.20.10.1

Configuration du routeur RW21

Interface locale	192.168.21.254/24
Interface vers MPLS Bouygues	66.20.20.1/16

Extrait de la table de routage routeur RW21

	Destination	Masque	Passerelle	Interface
1	172.16.0.0	255.255.0.0	192.168.21.1	192.168.21.254
2	172.18.0.0	255.255.0.0	66.20.30.1	66.20.20.1
3	10.1.0.0	255.255.0.0	66.20.1.1	66.20.20.1

Configuration du routeur RL2

Interface locale	172.16.200.254/16
Interface vers RW21	192.168.21.1/24
Interface vers RW22	192.168.22.1/24

Extrait de la table de routage routeur RL2

	Destination	Masque	Passerelle	Interface
1	172.16.0.0	255.255.0.0	172.16.200.254	172.16.200.254
2	172.18.0.0	255.255.0.0	192.168.21.254	192.168.21.1
3	172.20.0.0	255.255.0.0	192.168.22.254	192.168.22.1
4	10.1.0.0	255.255.0.0	192.168.21.254	192.168.21.1

ANNEXE 3 Extrait de la documentation « InterLAN 2.0 »

Le service "Inter LAN 2.0 Ethernet" est une offre de service de liaisons numériques à haut débit, destinée à interconnecter les réseaux locaux Fast Ethernet d'un client. [...]

Le service d'interconnexion proposé est limité au niveau 2 du modèle OSI (service de pontage). [...]. L'accès au service se fait sur le site client via un équipement AES (équipement d'accès au service) fourni par France Télécom qui délivre une interface de service *Fast Ethernet* sur laquelle se raccorde l'équipement du client. [...]

Le service "Inter LAN 2.0 Ethernet" est transparent aux VLAN que le client peut mettre en œuvre entre ses sites. Dans ce cas, les trames doivent être conformes à la norme **IEEE 802.1Q** et le marquage des trames Ethernet doit répondre à la norme **IEEE 802.3ac**.

ANNEXE 4 – Capture de trames

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.83	192.168.1.1	DNS	Standard query A assure.ameli.fr
2	0.072448	192.168.1.1	192.168.1.83	DNS	Standard query response A 93.174.145.36
3	5.719483	192.168.1.83	93.174.145.36	TCP	50106 > https [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8
4	5.764561	93.174.145.36	192.168.1.83	TCP	https > 50106 [SYN, ACK] Seq=0 Ack=1 win=4356 Len=0 MSS=1452 WS=0
5	5.764648	192.168.1.83	93.174.145.36	TCP	50106 > https [ACK] Seq=1 Ack=1 win=66560 Len=0
6	5.765080	192.168.1.83	93.174.145.36	SSL	Client Hello
7	5.813199	93.174.145.36	192.168.1.83	TLSv1	server Hello, Certificate, Server Hello Done
8	5.814394	192.168.1.83	93.174.145.36	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9	5.861428	93.174.145.36	192.168.1.83	TLSv1	Change Cipher Spec, Encrypted Handshake Message
10	5.897253	192.168.1.83	192.168.1.1	DNS	Standard query A ocsip.verisign.net
11	5.940936	192.168.1.1	192.168.1.83	DNS	Standard query response CNAME ocsip.verisign.net A 199.16.83.72
12	5.944084	192.168.1.83	199.16.83.72	TCP	50107 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8
13	5.986933	199.16.83.72	192.168.1.83	TCP	http > 50107 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1452 WS=7
14	5.987110	192.168.1.83	199.16.83.72	TCP	50107 > http [ACK] Seq=1 Ack=1 win=66560 Len=0
15	5.987687	192.168.1.83	199.16.83.72	HTTP	GET /MFEWtZBNMESwSTAJBgUrDgMCGGUABQ0iwh%2BdpR8i7ceU0B1nM962xjqywQUIGK
16	6.032801	199.16.83.72	192.168.1.83	TCP	http > 50107 [ACK] Seq=1 Ack=234 win=6912 Len=0
17	6.041357	199.16.83.72	192.168.1.83	TCP	[TCP segment of a reassembled PDU]
18	6.043153	199.16.83.72	192.168.1.83	OCSP	Response
19	6.043282	192.168.1.83	199.16.83.72	TCP	50107 > http [ACK] Seq=234 Ack=1810 win=66560 Len=0
20	6.043425	192.168.1.83	199.16.83.72	TCP	50107 > http [FIN, ACK] Seq=234 Ack=1810 win=66560 Len=0
21	6.043647	199.16.83.72	192.168.1.83	TCP	http > 50107 [FIN, ACK] Seq=1810 Ack=234 win=6912 Len=0
22	6.043711	192.168.1.83	199.16.83.72	TCP	50107 > http [ACK] Seq=235 Ack=1811 win=66560 Len=0
23	6.168914	192.168.1.83	93.174.145.36	SSL	Client Hello
24	6.217336	93.174.145.36	192.168.1.83	TLSv1	Server Hello, Certificate, Server Hello Done
25	6.218657	192.168.1.83	93.174.145.36	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
26	6.268870	93.174.145.36	192.168.1.83	TLSv1	Change Cipher Spec, Encrypted Handshake Message
27	6.270489	192.168.1.83	93.174.145.36	TLSv1	Application Data

Frame 18 (411 bytes on wire, 411 bytes captured)

Ethernet II, Src: NeufCege_14:ce:48 (00:25:15:14:ce:48), Dst: Dell_cd:b1:f7 (00:21:70:cd:b1:f7)

Internet Protocol, Src: 199.16.83.72 (199.16.83.72), Dst: 192.168.1.83 (192.168.1.83)

Transmission Control Protocol, Src Port: http (80), Dst Port: 50107 (50107), Seq: 1453, Ack: 234, Len: 357

[Reassembled TCP Segments (1809 bytes): #17(1452), #18(357)]

Hypertext Transfer Protocol

Online Certificate Status Protocol

responseStatus: successful (0)

responseBytes

Le poste du secrétaire sur lequel a été réalisée la capture est configuré comme suit :

adresse IP :	192.168.1.83
masque de sous-réseau :	255.255.255.0
passerelle par défaut :	192.168.1.254
serveur DNS :	192.168.1.1

ANNEXE 5 - Documentation sur les propositions de formation

Annexe 5A – Compte rendu d'entretien avec monsieur MARTIN

« L'architecture système et réseau du groupe ChauffAtlan repose sur de très nombreuses technologies que l'équipe s'efforce de maîtriser, de manière à rester le plus autonome possible vis-à-vis des prestataires et des fournisseurs.

Pour acquérir cette maîtrise, il faut se former. Et pour se former, il y a deux offres classiques.

La première est celle des fournisseurs, qui proposent souvent des journées de formation portant sur tel ou tel produit ou technologie qu'ils commercialisent.

L'autre offre est celle des centres de formations. Ils sont indépendants des constructeurs et des éditeurs. Ils ont un catalogue de formations spécialisées, pas forcément à jour, mais globalement pointues. Trop même !

Une troisième voie est envisageable : l'acquisition de compétences par transfert de compétences. Ces transferts ont lieu lorsque les informaticiens du groupe travaillent avec les techniciens des prestataires et des fournisseurs. Cela se passe lors des installations, des opérations de configuration ou de maintenance des équipements que nous leur achetons. Là, on est présent, on capte le plus d'informations possible.»

Annexe 5B – Extrait du catalogue de l'organisme PLC Formation Informatique Voix sur IP

Objectifs de la formation Voix IP

La VoIP est aujourd'hui une application-phare du monde des télécommunications, notamment pour les entreprises. À l'origine déployée pour des raisons d'économies, son succès est largement dû aux services innovants et utiles pour l'entreprise qu'elle propose : communications unifiées, conférences multimédia, nomadisme, intégration SI, applications mobiles...

Contenu de la formation Voix IP

- Introduction à la VOIP
- Infrastructure et protocoles dans le contexte ToIP
- Architectures et protocoles de signalisation VoIP
- Qualité de service des réseaux IP : impacts et outils
- Les « Best Practices » de la ToIP pour une implémentation réussie
- Administration de la ToIP
- Sécurisation d'une architecture ToIP

Travaux Pratiques

Durée de la formation Voix IP : 4 jours - Tarif 2011 de la formation Voix IP : 1 990 € par personne

Dates / Inscription en ligne :

Du 21/06/2011 au 24/06/2011, du 28/09/2011 au 01/10/2011, du 22/11/2011 au 25/11/2011

Des sessions supplémentaires sont créées régulièrement, n'hésitez pas à nous contacter pour en prendre connaissance.

Lieu de la formation : Paris - La Défense, ou dans vos locaux, sur vos équipements (surcoût forfaitaire dans ce cas : 600 €).

Annexe 5C – Extrait des offres de service rédigées par l'entreprise STVY concernant le projet VoIP

(...)

Offre Modules de Formation

Formation à la technique - STVY propose aux responsables informatiques et aux techniciens de maintenance deux modules de formation indissociables :

Module 1 : ToIP, VoIP, CTI (couplage Téléphone Informatique) – Concepts fondamentaux, protocoles, intégration, sécurité, confidentialité, évolutivité.

Durée : 2 jours. Coût : 600 € par participant.

Module 2 : Gamme Alcatel OmniPCX – Fonctionnalités, intégration, configuration, mise en œuvre, maintenance de base, programmation.

Durée : 2 jours. Coût : 800 € par participant.

Formation à l'usage - Pour vous aider à conserver votre image de marque, STVY propose une formation destinée aux standardistes et personnels de hotline.

Durée : 1 jour. Coût : 500 € pour un groupe, jusqu'à 6 participants.

Les formations ont lieu dans nos locaux (4 rue de la lune, Zone Beaufou, 85000 La Roche-sur-Yon).

Offre Assistance personnalisée

Pour vous aider à prendre en main les équipements matériels et logiciels de notre gamme Alcatel OmniPCX, STVY peut mettre à votre disposition un technicien spécialisé.

Axée sur les transferts de compétence, cette prestation est facturable 600 € la journée pour 3 techniciens auditeurs maximum.

(...)

Annexe 6 Extrait du schéma relationnel

TYPE_MATERIEL(id, libelle)

id : clé primaire

MATERIEL(ref, designation, idTypeMateriel)

ref : clé primaire

idTypeMateriel : clé étrangère en référence à

id de TYPE_MATERIEL

DISTRIBUTEUR(siret, raisonSoc, adRue,

adVille, cp, email, tel, fax)

siret : clé primaire

APPEL(numDossierBip, dateJour, descriptif, reponse)

numDossierBip, dateJour : clé primaire

numDossierBip : clé étrangère en référence à num de DOSSIER_BIP

DOSSIER_BIP(num, siretDistributeur, refMateriel, fermeture)

num : clé primaire

siretDistributeur clé étrangère en référence à siret de DISTRIBUTEUR

refMateriel clé étrangère en référence à ref de MATERIEL

// fermeture est un booléen prenant les valeurs false ou true. Lorsque le dossier est fermé, la valeur est true.