E5 : ÉTUDE DE CAS

Durée : 4 heures

CAS TRACE

Ce sujet comporte 12 pages dont 6 pages d'annexes.
Il est constitué de 4 dossiers qui peuvent être traités de façon indépendante.
Le candidat est invité à vérifier qu'il est en possession d'un sujet complet.

Aucune calculatrice n'est autorisée

Liste des annexes

Annexe 1 : fiche technique du matériel WIFI
Annexe 2 :architecture physique du réseau existant
Annexe 3 : schéma d'interconnexion des bâtiments
Annexe 4 : configuration logique du réseau existant
Annexe 5 : extrait du manuel de configuration des commutateurs
Annexe 6 : configuration du réseau final du projet TRACE
Annexe 7 : Extrait du manuel des commandes SHELL

Barème

Dossier 1 : 35 points
Dossier 2 : 25 points
Dossier 3 : 25 points
Dossier 4 : 15 points

Total : 100 points

Présentation du contexte

La société Mirbeau, est, depuis 1920, un moulin réputé dans la fabrication d'huiles de qualité.

A l'origine, l'Huilerie Mirbeau ne produit que de l'huile d'olive, les olives étant apportées par les agriculteurs des environs. Suite au gel intense de l'hiver 1956, qui détruira 90 % des oliviers français, le fondateur Noël Mirbeau se réoriente dans la trituration des graines de la région : tournesol, colza…En 1972, l'huilerie est la toute première huilerie en France à triturer des graines biologiques.

L'extraordinaire progression de l'entreprise peut se mesurer à l'étendue des locaux actuels. La construction, en 1998, d'un nouveau bâtiment de 6000 m2 s'est traduite par une réorganisation complète, tant au niveau du matériel que des équipes : nouvelle cuverie inox, agrandissement du laboratoire, mise en place d'un atelier de conditionnement automatisé de 1000 m2, d'un service achat et d'une zone logistique...

Les graines apportées par les producteurs régionaux ou par transport international sont triturées sur place dans les anciennes presses à vis des débuts, dans le respect de la tradition artisanale. La mise en bouteille est réalisée dans un atelier de conditionnement automatisé de 1000 m². Les bouteilles sont ensuite stockées et conservées à l'abri de la chaleur et de l'humidité dans la cave.

En 2000, l'entreprise achète une unité de production d'huile d'olive biologique en Andalousie (Espagne). En effet, après récolte, les olives doivent être pressées le plus rapidement possibles afin d'obtenir une huile de qualité.

En 2003, l'entreprise développe une activité « commerce équitable » en partenariat avec des producteur de graines étrangers (Maroc, Mali). .

Le Projet TRACE

Afin de répondre aux normes de qualité et de sécurité agro-alimentaires, l'huilerie a pour objectif d'assurer une traçabilité maximale des produits en amont et en aval. La traçabilité correspond à la capacité de suivre les déplacements d'un aliment parmi des stades précis de la production, de la transformation et de la distribution.

Actuellement le système de traçabilité est uniquement géré par des documents papiers qui identifient les différents lots (lots de matières premières, lots de trituration, lots de stockage, ...) ainsi que les échantillons correspondants traités au laboratoire. Ces documents sont remplis à tous les stades de la production (culture, récolte, transport, réception, analyse qualité, stockage, pressage, conditionnement, distribution), et transmis en fin de journée au service qualité qui enregistre les données dans le logiciel OLITRACK en version monoposte.

Afin de mieux répondre aux exigences des organismes de certification internationaux, l'huilerie souhaite améliorer son système de traçabilité en y intégrant toute la chaîne de production et de distribution. Elle décide d'acquérir la nouvelle version du logiciel de traçabilité OLITRACK qui fonctionne en client/serveur.

Le projet TRACE doit permettre d'automatiser l'ensemble du suivi de la chaine de production, de l'agriculteur jusqu'au consommateur, et d'assurer l'impression et la lecture des codes barres identifiants les lots et les dates de traitement à chaque étape de la chaine de production. Il est donc nécessaire d'étendre le réseau au bâtiment de production et au site de production espagnol, ainsi que de permettre l'accès à l'application aux différents producteurs partenaires de l'huilerie MIRBEAU.

Jeune diplômé(e), vous travaillez en tant que technicien(ne) dans l'équipe « réseau et systèmes», chargée de l'architecture et de la sécurité de celui-ci. Vous participez à l'élaboration et à la mise en oeuvre du projet TRACE.

DOSSIER 1	Modification de l'architecture réseau

Annexes à utiliser : 1,2,3,4,5 et 6

Le siège de la société est situé en Provence. Il est constitué de deux bâtiments distants de 50m :

- le bâtiment administratif de deux étages (services comptabilité, achats, commercial, qualité, et boutique au rez de chaussée). Le bâtiment est entièrement câblé, tous les services sont informatisés. L'architecture physique du réseau est décrite en *annexe 1*.
- le bâtiment de production de 6000m2, regroupant le moulin, le laboratoire, l'atelier de conditionnement, la cave, et une zone logistique pour le chargement et déchargement des camions de transports. Ce bâtiment n'est pas informatisé pour l'instant.

La première phase du projet d'extension du réseau au bâtiment de production est l'interconnexion des deux bâtiments. Deux solutions sont envisagées : fibre optique ou liaison Wifi directionnelle.

1.1 Rédiger un dossier de choix présentant les caractéristiques de chaque solution en terme de coût, débit, contraintes d'installation et sécurité.

La solution choisie est l'installation d'une fibre optique enterrée reliant les deux bâtiments. Le débit du réseau sur la liaison inter-bâtiment devra être de 1 Gb/s.

La deuxième phase du projet consiste à câbler le bâtiment de production. Le cahier des charges prévoit un débit dans le bâtiment de de 100Mb/s. Les postes informatiques à installer seront équipés de terminaux de lecture de code barre. Des terminaux batch ou WIFI portables de saisie et lecture de code barre seront fournis aux services logistiques et à la cave.

Le nombre de postes à prévoir dans chaque zone est le suivant :

- Sur la zone logistique : 5 postes fixes, 2 imprimantes réseau et 6 terminaux portables.
- Au moulin dans lequel est assuré la fabrication proprement dite des huiles : 6 postes fixes et une imprimante réseau.
- Dans l'atelier de conditionnement où les huiles sont mises en bouteille : 2 postes fixes.
- Dans la cave dans laquelle sont stockés les produits conditionnés : 2 postes fixes et 4 terminaux portables
- Au laboratoire qui analyse les échantillons de matière première et d'huile: 5 postes fixes et une imprimante réseau.

La solution retenue consiste en un réseau WIFI pour la zone logistique et un câblage UTP catégorie 6 pour le reste du bâtiment. La zone logistique sera couverte par deux points d'accès WIFI. Le matériel proposé par le fournisseur est décrit en *annexe 1*.

1.2 Décrire les risques liés à l'utilisation du wifi dans la zone logistique ainsi que les solutions techniques permettant de limiter ces risques.

L'architecture physique du réseau existant est décrite en *annexe 2*. Le nouveau commutateur SW5 choisi pour équiper le bâtiment de production est un commutateur de niveau 2 gérant les VLAN par port et comportant 24 ports 10/100BaseT (ports 1 à 24) et 1 module 1000BaseSX (port 25). Les deux points d'accès seront connectés aux ports 23 et 24, comme illustré sur le schéma d'interconnexion des bâtiments fourni en *annexe 3.*

Le réseau du bâtiment administratif repose sur une architecture VLAN décrite en *annexe 4*. Pour isoler le réseau WIFI de la zone logistique du reste du réseau, il est indispensable de le placer dans un VLAN séparé. Ce VLAN sera nommé VLAN logistique (VLAN 50). Le reste du réseau du bâtiment sera placé dans le VLAN 20 (postes). Le VLAN logistique sera associé au réseau IP 192.168.5.0/24.

1.3	Écrire les commandes nécessaires à la mise en place de cette configuration, en utilisant le manuel fourni en *annexe 5* en spécifiant, pour chaque commande, sur quel matériel elle doit être exécutée.

Les membres du VLAN logistique doivent pouvoir accéder à l'application client/serveur OLITRACK installée sur le serveur MIRAPPLI et qui écoute sur le port 1069. Par sécurité, tout autre accès provenant de ce VLAN sera interdit.

1.4	Modifier la configuration de SW1 pour répondre aux contraintes ci-dessus.

Afin de mettre en œuvre une traçabilité de toute la chaîne de production, les employés de l'unité de production espagnole doivent pouvoir accéder à l'application OLITRACK. L'interconnexion entre le site de production espagnol et le réseau de l'huilerie Mirbeau sera réalisée par un VPN (Réseau privé virtuel) mis en place au travers d'une liaison SDSL louée à un opérateur de télécommunications. La connexion SDSL remplacera l'accès ADSL actuel.

Les deux routeurs SDSL ont été installés et sont opérationnels sur les deux sites. Leurs tables de routage sont présentées en *annexe 6*. Le tunnel VPN a été configuré en mode SSL. Le tunnel VPN utilise des interfaces virtuelles sur le réseau 172.16.0.0/30, comme l'illustre l'*annexe 6*. Pourtant les deux sites n'arrivent pas à communiquer. Vous exécutez les commandes suivantes à partir de votre poste du service informatique (192.168.2.34):

```
ping 192.168.5.1 : 64 bytes from 192.168.5.1 : icmp_seq=1 ttl=64 time=9.67 ms …

ping 173.18.156.13 : 64 bytes from 173.18.156.13: icmp_seq=1 ttl=51 time=78.5 ms...

ping 192.168.8.23 : délai d'attente de la demande dépassé
```

Le poste 192.168.8.23 correspond au poste du responsable informatique du site espagnol, que vous avez contacté par téléphone. Son poste est opérationnel et accède à internet via la liaison SDSL.

1.5	Expliquer la cause du problème rencontré et proposer une solution pour permettre aux deux réseaux de communiquer.

Actuellement les données de traçabilité liées aux cultures, aux récoltes et au transport sont transmises par les producteurs sous forme de document manuscrit. Afin d'automatiser l'ensemble de la chaîne de production, ces données devront maintenant être saisies directement par le producteur dans une application web sécurisée qui permettra également d'imprimer les étiquettes apposées sur les lots permettant d'assurer la traçabilité lors de la récolte et du transport jusqu'au moulin.

L'application Web est un module optionnel de l'application OLITRACK, nommé OLITRACK-WEB qui s'installe de manière automatique sur un serveur Web.

L'application devra être accessible via une l'url https://trace.huilerie-mirbeau.com

1.6	Établir la liste des composants et services nécessaires à la mise à disposition de l'application web via cette url.

Cette application Web sera hébergée sur un nouveau serveur nommé MIRWEB et placé dans une « zone démilitarisée » (DMZ). Ce serveur est connecté au routeur SDSL par une interface supplémentaire. Pour rendre ce serveur accessible, l'entreprise MIRBEAU a acheté à son FAI le réseau IP public suivant : 196.65.239.20/30 pour adresser les deux interfaces du lien entre le routeur SDSL et le serveur Web, comme illustré dans l'*annexe 6*. Ce réseau est routé vers le routeur R-SDSL1.

1.7	Justifier l'utilisation d'un masque de 30 bits pour le réseau public acheté.
1.8	Proposer autre solution pour rendre le serveur MIRWEB accessible aux producteurs via internet sans acheter d'adresses IP publiques?

DOSSIER 2	**Tolérance aux pannes**

Annexes à utiliser 7 ,8

Afin d'assurer la tolérance aux pannes du service de traçabilité, on envisage de mettre en place une sauvegarde de la base de donnée SQL, nommée « olibd » de l'application OLITRACK et une haute disponibilité du serveur MIRWEB.

La sauvegarde de la base de donnée doit être automatisée, programmée chaque soir à 20h et enregistrée sur un serveur de fichier distant, hébergé chez un prestataire, et accessible par le nom backup.mirbeau.com, et par le protocole SSH.

2.1	Planifier et décrire les différentes étapes à réaliser pour mettre en place la solution de sauvegarde
2.2	Écrire le script de sauvegarde de l'application permettant de sauvegarder la base de donnée sur le serveur de fichier distant, en évitant d'écraser les sauvegardes précédentes.
2.3	Rédiger la procédure de restauration de la base de données.
2.4	Expliquer rapidement en quoi consiste la haute disponibilité, et quel est son objectif.
2.5	Proposer une solution pour mettre en place la haute disponibilité du serveur Web

DOSSIER 3	Gestion des utilisateurs

Afin d'améliorer la sécurité d'accès à l'infrastructure et aux services du réseau, il est nécessaire de mettre en place un annuaire centralisée des utilisateurs et des ressources. Le choix de Windows 2008 Serveur permettra de mieux gérer la sécurité des données. Le fonctionnement de ce système d'exploitation est sensiblement identique à sont prédécesseur Windows 2003 Serveur.

3,1	Énumérer les sites en présence.
3,2	Mettre en place une arborescence (UO, utilisateurs) cohérente afin de gérer les identités et les habilitations.
3,3	Indiquer les différentes étapes permettant de montez un lecteur réseau individuel pour chaque utilisateur.
3,4	Donner un nom de domaine ainsi que le nom de la forêt.

DOSSIER 4	Gestion d'investissement

l 'évolution matérielle demande infrastructure adapté afin de l'accueillir. La salle des serveurs est équipé d'une climatisation obsolète. Une nouvelle climatisation est acheté le 02/02/2012. Elle ne sera mise en service que le 16/05/2012 juste avant les grandes chaleurs.
Sa valeur se monte à 13 000 €.

4.1	Déterminez le calcul de la première et dernière année.
4,2	Réalisez le tableau d'amortissement

Afin de financer cet achat , un prêt à été accordé sur 3 ans à un taux de 2,5 %.

4,3	Réalisez le tableau d'amortissement de ce prêt par amortissement constant

Annexe 1 : Fiche technique du matériel WIFI

Cisco Aironet 1242AG **borne d'accès sans fil**	

Descriptif du produit

- **Description du produit**: Cisco Aironet 1242AG - borne d'accès sans fil
- **Type de périphérique**: Borne d'accès sans fil
- **Type de châssis**: Externe
- **Dimensions (LxPxH)**: 16.8 cm x 21.6 cm x 2.8 cm
- **Poids**: 0.9 kg
- **RAM installée (max.)**: 32 Mo
- **Mémoire flash installée (max)**: 16 Mo Flash
- **Protocole de liaison de données**: IEEE 802.11b, IEEE 802.11a, IEEE 802.11g
- **Protocole de gestion à distance**: SNMP, Telnet, HTTP, HTTPS
- **Caractéristiques**: Auto-détection par dispositif, Power over Ethernet (PoE), prise en charge de BOOTP, filtrage d'adresse MAC.
- **Algorithme de chiffrement:** LEAP, AES, WEP 128 bits, 40-bit WEP, TLS, PEAP, TTLS, TKIP, WPA, WPA2
- **Portée maxi en espace ouvert:** 290 m
- **Méthode d'authentification:** Secure Shell (SSH), MS-CHAP
- **Facteur de forme:** Externe
- **Système d'exploitation fourni:** Cisco IOS
- **Garantie du fabricant**: Garantie de 1 an

Annexe 2 : Architecture physique du réseau existant

Le bâtiment administratif, comporte 70 postes reliées en réseau.

- au rez de chaussée la boutique (5 postes, avec terminaux fixes de lecture de code barre),
- au premier étage le service commercial (30 postes), le service des achats (10 postes)
- au deuxième étage la direction (5 postes), le service comptabilité (10 postes), le service qualité (5 postes), le service informatique (5 postes),

Le réseau du bâtiment administratif est un réseau Ethernet 10/100BaseT, basé sur 4 commutateurs 24 ports en cascade installés dans le local technique situé au premier étage:

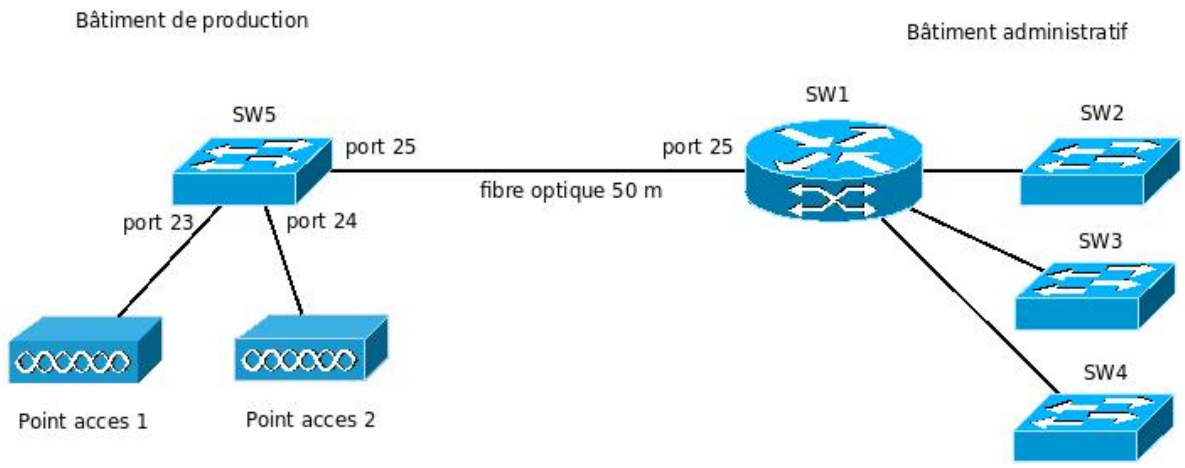
- SW1 : commutateur niveau 3 ,24 ports 10/100/1000baseT, 2 emplacements vides pour module.
- SW2, SW3, SW4 : 3 commutateurs de niveau 2 gérant les VLAN par port, 24 ports 10bT/100bT

Quatre serveurs sont également en place dans le local technique :

- serveur MIRPRIM (192.168.1.2) : serveur de fichiers,
- serveur MIRSEC (192.168.1.3) : serveur DHCP et serveur de communication.
- serveur d'application MIRAPPLI (192.168.1.4) : applications de gestion et traçabilité.
- serveur de sauvegarde MIRBACK (192.168.1.5) .

L'accès à internet est assuré par une connexion ADSL professionnelle, via un routeur ADSL fourni par l'opérateur, et placé dans le local technique. Le serveur DNS du FAI (adresse IP : 212.27.63.139) est utilisé pour la résolution des noms.

Annexe 3 : schéma d'interconnexion des bâtiments



Annexe 4 : Configuration logique du réseau existant

Ce réseau est segmenté en 4 VLAN par port, configurés sur le commutateur SW1 (commutateur de niveau 3) :

- VLAN 10 : « boutique », réseau IP 192.168.1.0/24
- VLAN 20 : « postes », réseau IP 192.168.2.0/24
- VLAN 30 : « serveurs », réseau IP 193.168. 3.0/28
- VLAN 40 : « internet », réseau IP 193.168. 4.0/30

Les interfaces virtuelles de SW1 dans chacun des VLAN correspondent aux adresses les plus basses de chaque réseau IP. Par exemple pour le VLAN 10 : 192.168.1.1

Table de routage du routing-switch SW1 (commutateur de niveau 3):

Réseau	*Interface*	*Passerelle*
192.168.1.0/24	192.168.1.1	192.168.1.1
192.168.2.0/24	192.168.2.1	192.168.2.1
192.168.3.0/28	192.168.3.1	192.168.3.1
192.168.4.0/30	192.168.4.1	192.168.4.1
0.0.0.0	192.168.4.1	192.168.4.2

Liste d'accès de SW1 permettant de spécifier les règles d'accès (tout est autorisé par défaut) :

N°	interface	sens	Proto-cole	IP source	Port source	IP dest	Port dest	Etat TCP	action
1	192.168.1.1	E	tous	192.168.1.0/24	tous	192.168.3.0/28	tous	tous	autorise
2	192.168.1.1	E	tous	tous	tous	tous	tous	tous	bloque
3	192.168.4.1	E	UDP	tous	53	192.168.0.0/16	tous	tous	autorise
4	192.168.4.1	E	TCP	tous	tous	192.168.0.0/16	tous	établi	autorise
5	192.168.4.1	E	tous	tous	tous	tous	tous	tous	bloque

Annexe 5 : extrait du manuel de configuration des commutateurs

- ajout d'une route (uniquement pour les commutateurs de niveau 3):
  ip route <adresse réseau> <masque> <passerelle> <interface>
  exemple : ip route 0.0.0.0 0.0.00 192.168.4.2 192.168.4.1
- création d'un vlan : *vlan <id-vlan> name <nom-vlan>*

exemple : vlan 10 name boutique

- association d'une IP à un VLAN (uniquement pour les commutateurs de niveau 3):

interface vlan <id-vlan> ip address <adresseIP> <masque>

exemple : interface vlan 10 192.168.1.1 255.255.255.0

- ajout d'une interface à un vlan : *interface <plage-ports> switchport access vlan <id-vlan>*
  exemple : interface 1-10 switchport access vlan 10 (ajout des port n°1 à 10 dans le VLAN 10)
- activation du protocole 802.1q sur une interface :

interface <id-port> switchport trunk encapsulation dot1q

Annexe 6 : Configuration du réseau final du projet TRACE

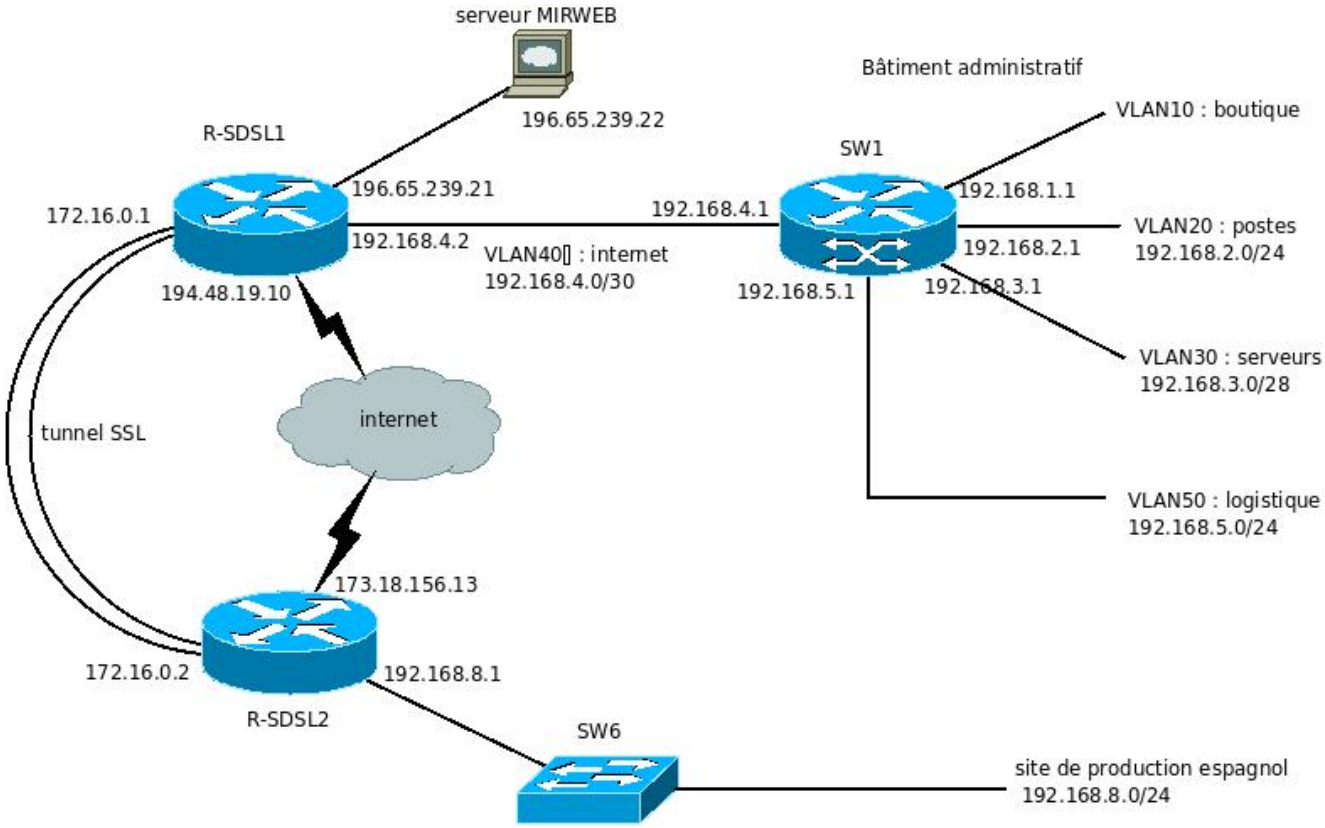


Table de routage de R-SDSL1

Réseau	*Interface*	*Passerelle*
172.16.0.0/30	172.16.0.1	172.16.0.1
192.168.4.0/30	192.168.4.1	192.168.4.1
194.48.19.8/29	194.48.19.10	194.48.19.10
196.65.239.20/30	196.65.239.2.21	196.65.239.21
192.168.0.0/21	192.168.4.2	192.168.4.1
0.0.0.0	194.48.19.10	194.48.19.17

Table de routage de R-SDSL2

Réseau	*Interface*	*Passerelle*
192.168.8.0/24	192.168.8.1	192.168.8.1
172.16.0.0/30	172.16.0.2	172.16.0.2
173.18.156.12/30	173.18.156.13	173.18.156.13
0.0.0.0	173.18.156.13	173.18.156.14

Annexe 7 : Extrait du manuel des commandes SHELL

Substitution de commandes

Syntaxe : **$(** *cmd* **)**

Une commande *cmd* entourée par une paire de parenthèses **()** précédées d'un caractère **$** est exécutée par le shell puis la chaîne **$(** *cmd* **)** est remplacée par les résultats de la commande *cmd* écrits sur la sortie standard, c'est à dire l'écran. Ces résultats peuvent alors être affectés à une variable ou bien servir à initialiser des paramètres de position.

$ pwd

/home/johndoe => résultat écrit par pwd sur sa sortie standard

$ echo mon repertoire est $(pwd)

mon repertoire est /home/johndoe

SCP(1)

NAME

scp — secure copy (remote file copy program)

SYNOPSIS

scp [-12346BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file] [-l limit] [-o ssh_option] [-P port] [-S program] [[user@]host1:]file1 ... [[user@]host2:]file2

DESCRIPTION

scp copies files between hosts on a network. It uses ssh(1) for data transfer, and uses the same authentication and provides the same security as ssh(1). Unlike rcp(1), scp will ask for passwords or passphrases if they are needed for authentication.

File names may contain a user and host specification to indicate that the file is to be copied to/from that host. Local file names can be made explicit using absolute or relative pathnames to avoid scp treating file names containing ':' as host specifiers. Copies between two remote hosts are also permitted.

….

DATE(1)

NAME

date - print or set the system date and time

SYNOPSIS

date [OPTION]... [+FORMAT]

FORMAT controls the output. Interpreted sequences are:

%A locale's full weekday name (e.g., Sunday)

%B locale's full month name (e.g., January)

%c locale's date and time (e.g., Thu Mar 3 23:05:25 2005)

%d day of month (e.g., 01)

%D date; same as %m/%d/%y

%F full date; same as %Y-%m-%d

…..

MYSQLDUMP(1)

NAME

mysqldump - a database backup program

SYNOPSIS

mysqldump [options] [db_name [tbl_name ...]]

….

MYSQL(1)

NAME

mysql - the MySQL command-line tool

SYNOPSIS

mysql [options] db_name

DESCRIPTION

mysql is a simple SQL shell with input line editing capabilities. It supports interactive and noninteractive use.

Using mysql is very easy. Invoke it from the prompt of your command interpreter as follows:

shell> mysql db_name

Or:

shell> mysql --user=user_name --password=your_password db_name

Then type an SQL statement, end it with “;”, \g, or \G and press Enter.

You can execute SQL statements in a script file (batch file) like this:

shell> mysql db_name < script.sql > output.tab