



OFPPT

مكتب التكوين المهني وإنعاش الشغل
Office de la Formation Professionnelle et de la Promotion du
Travail

WWW.TRI.ON.MA

**Examen de Fin de Formation
Session Juin 2009**

Filière : *Techniques des Réseaux Informatiques (TRI)* **Epreuve** : *Théorique*

Durée : *4 heures*

Barème : */40*

Eléments de correction

Barème de notation

Partie 1 : 8 points

Question 1 : 2 points (0,5 point pour chaque bonne réponse)

Question 1 : 2 points

Question 3 : 2 points (1 point pour 3.1, et 0,5 point pour 3.2 et 3.3)

Question 4 : 2 points (0,5 point pour 4.1, 1 point pour 4.2 et 0,5 point pour 4.3)

Partie 2 : 32 pts

1 : 12 points

1.1 : 1 point

1.2 : 1 point

1.3 : 1 point

1.4 : 1 point

1.5 : 2 points

1.6 : 2 points

1.7 : 2 points

1.8 : 2 points

2 : 12 pts

2 points pour chaque question

3 : 8 pts

3.1 : 3 points

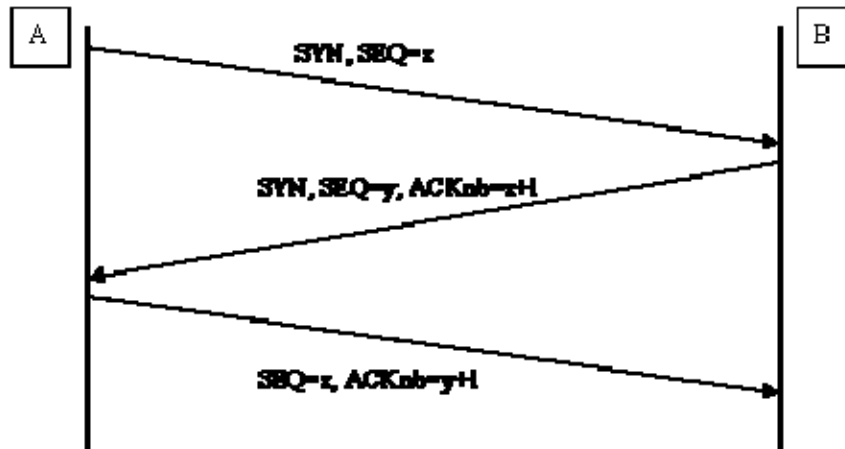
3.2 : 4 points

3.3 : 0,5 point

3.4 : 0,5 point

Partie 1 (Questions de cours)

1.1.



1.2.

Un échange en deux phases ne fonctionne que si le réseau est fiable avec séquençement garanti.

Le service réseau fourni par IP ne correspond pas à ce modèle. L'établissement des connexions TCP doit prendre en compte :

- le déséquencement des paquets introduit par leur errance à l'intérieur du réseau. Les paquets suivent des chemins différents dans le réseau et peuvent connaître des temps de traversée très aléatoires (problèmes d'algorithme de routage ou de congestion). Le réseau "stocke" des datagrammes pendant un temps (de transit) indéfini. Une TPDU de données émise par A peut parvenir à B avant que la connexion soit formellement établie. La TPDU est soit stockée alors que la connexion n'est pas établie ou elle est rejetée. Il faut interdire à l'appelé d'émettre avant d'avoir reçu l'autorisation. ceci est fait par la procédure d'initialisation en trois étapes (three-way handshake). La connexion est établie pour l'entité appelante que lorsqu'elle reçoit la confirmation de connexion, alors qu'elle n'est établie pour l'appelée que lorsqu'elle a reçu un acquittement.
- la résurrection de datagrammes contenant une demande ou une confirmation de connexion (paquets survivants d'une connexion libérée)
- les erreurs de transmission, pertes et duplications affectant les unités de protocoles d'établissement de connexion.

En cas de perte de l'acquittement, la reprise est faite par temporisateur. La procédure d'initialisation en trois étapes sert à résoudre ces problèmes en fournissant une synchronisation minimum entre les deux extrémités d'une connexion.

1.3.

Une connexion est définie par une paire de sockets. Si la connexion est répétitivement ouverte et fermée, ou si la connexion est rompue puis réétablie. Un problème se pose à TCP: Comment identifier les segments appartenant aux connexions précédentes ? Si ces segments sont compris comme appartenant à la connexion, ils entraînent des pertes et des duplications de segments qui ne seront pas détectées par TCP. Le transfert n'est alors plus fiable.

Pour éviter toute confusion, le numéro de séquence initiale est différent pour chaque connexion. Cela sert à différencier les connexions. Pour plus de sécurité, quand la connexion est fermée, TCP reste dans un état de purge pendant la durée de vie maximale d'un paquet (120 s). Ceci pour garantir que des segments appartenant à des connexions précédentes ne puissent ressurgir.

Lorsqu'une connexion est créée, une valeur de ISN sur 32 bits est déterminée. En simplifiant, ceci est fait en utilisant un compteur, incrémenté de 1 toutes les 4 μ s : la séquence de numérotation reboucle alors approximativement toutes les 4.55 heures, ce qui est largement supérieur à la durée de vie maximum d'un segment dans le réseau.

1.4

Le segment est l'unité de contrôle. Les contrôles de fiabilité sont faits sur le segment.

2.

- Etablissement de connexion en trois phases
- Libération en quatre phases et utilisant un temporisateur de déconnexion
- Numérotation en séquence des données et des acquittements
- ISN (initial sequence numbers : numéro de séquence initial)
- Temporisateur de retransmission
- Temporisateur de persistance (pour éviter les deadlocks suite à une perte de réouverture de fenêtre)
- Acquittements positifs (au minimum)
- Détection d'erreurs
- Contrôle de flux
- Contrôle de congestion
- Détection d'inactivité (optionnel)

3.1

L'adresse identifie une connexion à un sous-réseau. Un routeur reliant N réseaux aura donc N adresses différentes. De même, une station reliée à M sous-réseaux différents, possèdera M adresses différentes.

- - Cette séparation entre l'adresse du sous-réseau et celle de la station attachée à ce sous-réseau permet un routage effectif dans les routeurs uniquement d'après l'adresse du sous-réseau. L'adresse complète n'est utilisée qu'une fois le datagramme arrivé au routeur auquel est connecté le sous-réseau destinataire. Le fait de séparer l'adresse en deux parties permet ainsi de réduire la taille mémoire des passerelles car elles ne conservent que l'adresse des sous-réseaux (et celle des stations des sous-réseaux directement rattachées).
- - Il est facile d'envoyer un paquet sur toutes les stations d'un sous-réseau. Il suffit d'utiliser une adresse de station particulière qui signifie que le paquet doit être diffusé sur tout le sous-réseau. On peut garder par exemple l'adresse de station avec tous les bits à 1 pour envoyer un paquet à toutes les stations d'un sous-réseau.
- - décentralisation de la gestion des host id
- - si un hôte change de réseau, son adresse doit changer (cas des portables) mais seul la partie préfixe réseau change dans le cas IPv6.
- - si un réseau de classe C passe au-delà de 255 hôtes, il doit changer pour la classe B
- - un hôte peut avoir plusieurs IP ; comme le routage utilise le net id, le chemin suivi par les paquets vers un hôte possédant plusieurs adresses dépend de l'adresse utilisée

3.2

L'adresse IP ne doit pas être seulement unique mais elle doit aussi refléter la structure de l'interconnexion. Elle est constituée par une partie réseau. Ce que n'a pas l'adresse Ethernet par exemple.

Toutes les machines connectées au réseau physique ont le même préfixe réseau.

3.3

Au minimum, 2 car c'est un équipement d'interconnexion.

4.1

Le routage IP, Il consiste à déterminer le meilleur voisin pour atteindre le destinataire.

4.2

A ne connaît pas l'adresse MAC de B, La station A ne connaît que l'adresse IP de B. L'adresse Mac de B sera connue par la station qui effectuera la remise directe du datagramme.

4.3

Au moyen du protocole ARP.

Partie 2 (Etude de cas)

Etape 1

1.1

- L'adresse 20.0.0.0 correspond appartient à la classe A.
- Le masque de sous-réseau associé à la classe A est 255.0.0.0.

1.2

- Le plan d'adressage prévoit 16 bits pour le masque de sous réseau des filiales, soit 8 bits (16 – 8) pour la partie sous réseau. Ce qui permet d'adresser 256 (2^8) sous-réseaux.

1.3

- Pour adresser un minimum de 11 sous-réseaux, il faut emprunter 4 bits de la partie hôte. On dispose alors de 16 (2^4) sous-réseaux.

- Pour les filiales, le masque est déjà sur 16 bits, pour les divisions du Maroc, le masque sera donc sur 20 bits (16 + 4). Soit 255.255.240.0

1.4

- La première ligne de la table de routage fait référence à un masque de 20 bits donc toutes les adresses disposant des mêmes 20 premiers bits seront routées :

Soit les divisions :

D2 : 00010100.00001010.00010001.0	soit 20.10.17.0
D3 : 00010100.00001010.00010010.0	soit 20.10.18.0
D4 : 00010100.00001010.00010100.0	soit 20.10.20.0

1.5

Table de routage du routeur *R.Central*

Adresse réseau	Passerelle	Interface
20.1.0.0 /16	20.1.0.254	20.1.0.254
20.30.0.0 /16	195.0.0.13	195.0.0.1
20.20.0.0 /16	195.0.0.12	195.0.0.1
20.10.0.0 /16	195.0.0.11	195.0.0.1

1.6

Permet de diviser l'espace de noms et de déléguer la gestion d'une partie de l'espace de nom DNS à chaque Filiale. L'extension de l'espace de noms sera ainsi simplifiée et sous la responsabilité de chaque Filiale. La modification d'un nom d'hôte sera réalisée par la filiale qui gère la zone concernée.

1.7

- Le nom d'hôte **sap.dz.coknet** est situé dans le sous-domaine **dz.coknet**. Le serveur primaire qui gère cette zone est situé en Algérie. Il a pour adresse IP 20.10.32.2 et pour nom dns.dz.coknet.

1.8

- Un serveur DNS supplémentaire peut être rajouté au niveau de chaque division permettant ainsi d'offrir une redondance de zone. Les informations de zone seront répliquées sur chacun d'eux.

- Une autre solution consiste à utiliser le serveur racine (parent) de la zone coknet pour répliquer l'ensemble des zones.

Etape 2

2.1

Il y a **3 (ou 4) domaines de collision et 1 domaine de diffusion**, le segment entre le routeur et le commutateur peut-être considéré comme un domaine de collision (soit considérer les deux réponse justes)

2.2

Pour isoler les trois services, il est donc nécessaire de créer trois VLAN.

Tous les postes d'un service doivent appartenir au même VLAN pour communiquer ensemble. Ces postes sont reliés par des concentrateurs connectés sur un port du commutateur. Ces ports doivent donc être affectés à un VLAN.

Il est donc possible de conserver les concentrateurs existants. La solution est de configurer des VLAN de niveau 1 sur le commutateur existant en affectant le numéro de Vlan du service au port connecté au concentrateur du service. Mais le fait de conserver les concentrateurs impose que tous les postes appartiennent au même VLAN.

2.3

Le routeur filtrant agit aux niveaux 3 et 4 du modèle OSI. Les filtres sont basés sur l'analyse des adresses IP source et destination et les ports de protocole. Il n'est capable ni de comprendre le contexte du service qu'il rend, ni d'identifier le demandeur du service.

Le serveur mandataire agit au niveau application du modèle OSI. Le filtrage se situe donc au niveau applicatif. Les règles de filtrage peuvent être plus élaborées (discriminantes) et faire référence à l'identité de l'utilisateur ou à la nature du service fourni.

2.4

Les règles 1 et 2 permettent au poste de l'administrateur d'adresse IP 20.1.0.50 d'accéder à tous les services disponibles sur Internet.

La règle 3 bloque en sortie tout autre trafic de façon à ce qu'il faille passer par le serveur mandataire (*proxy*) pour accéder à Internet.

La règle 4 bloque en entrée tout autre trafic provenant d'Internet.

Les règles 1 et 2 sont placées avant les règles 3 et 4 qui bloquent tout le trafic

2.5

Règle	direction	IP source	Port source	IP destination	Port destination	Action
1	Sortie	10.1.0.50 /32	Tous	Tous	Tous	Router
2	Entrée	Tous	Tous	10.1.0.50 /32	Tous	Router
3	Sortie	10.1.0.100 /32	Tous	Tous	80 / HTTP	Router
4	Entrée	Tous	80 / HTTP	10.1.0.100 /32	Tous	Router
5	Sortie	Tous	Tous	Tous	Tous	Bloquer
6	Entrée	Tous	Tous	Tous	Tous	Bloquer

2.6

Il convient d'indiquer au niveau des applications, voire au niveau du système d'exploitation, que les accès se font via un serveur mandataire (*proxy*) dont on indiquera l'adresse IP ou le nom.

Etape 3

3.1

Les mécanismes de signature et de chiffrement permettent d'assurer les fonctions de confidentialité, d'authentification, de non-répudiation et d'intégrité.

- Le chiffrement assure la confidentialité : l'information échangée entre deux entités du réseau, ne doit pas être intelligible pour une tierce personne qui serait à l'écoute ou récupérerait le message.
- L'action de signer assure authentification et imputabilité (non-répudiation).
 - L'authentification (ou identification) permet de prouver que la provenance de l'information est bien celle qu'elle dit être.
 - La non-répudiation (ou non-désaveu) concerne la validité juridique des signatures. Émetteur et récepteur ne pourront nier l'émission et la réception de l'objet.

Le chiffrement assure l'intégrité : le destinataire est assuré que l'information qui lui parvient est bien l'information qui a été transmise.

3.2

Lors d'un échange entre la succursale S1 et le siège, S1 utilisera la clé publique du destinataire (le siège) pour chiffrer le message. Puis le siège utilisera à réception sa clé privée pour déchiffrer. En outre S1 peut utiliser sa propre clé privée pour signer son envoi et garantir ainsi l'authentification du message. Toute transmission à l'initiative du siège générera un processus inverse quant à la mise en œuvre des clés. (chiffrement avec la clé publique de S1 qui déchiffrera avec sa propre clé privée, le siège utilisant éventuellement sa clé privée pour signer son envoi).

3.3

	1	2	3	4	Formules
Chiffre d'affaires supplémentaire	65 000	65 000	60 000	60 000	-
Charges supplémentaires	40 000	40 000	50 000	50 000	-
Dotations aux amortissements	10 000	10 000	10 000	10 000	Investissement / 4
Résultat avant IS	15 000	15 000	0	0	CA – (Charges + Dotations)
IS	5 000	5 000	0	0	Résultat avant IS / 3
Résultat après IS	10 000	10 000	0	0	Résultat avant IS – IS
CAF	20 000	20 000	10 000	10 000	Résultat après IS + Dotations aux amortissements

3.4

Valeur Actuelle Nette = somme des CAF actualisées – investissement

FNT	20 000	20 000	10 000	10 000
FNT actualisés	19 048	18 140	8 638	8 227

Sur le critère de la Valeur Actuelle Nette, le projet est rentable :

$$\text{VAN} = - 40\,000 + 19\,048 + 18\,140 + 8\,638 + 8\,227 = 14\,053 \text{ soit } 14\,053 \text{ €}$$