INSTITUT SUPERIEUR INFORMATIQUE ISI
المعهد العالي للإعلامية

الجمهورية التونسية
وزارة التعليم العالي
جامعة تونس المنار
المعهد العالي للإعلامية

Examen Administration et sécurité des réseaux

Session : principale**, Classes:** 3SIL, **Enseignants** : M.H. Hdhili, E. Garoui

Documents non autorisés

Exercice 1[5pts]: DNS

Considérez la description du DNS donnée en annexe pour répondre aux questions suivantes

1) L'exemple de communication décrit par la figure 1 (voir annexe) représente un scénario de résolution en mode récursif ou itératif ? Expliquer. ==> **récursif car le DNS du FAI joue le role de résolveur pour le client (il a interrogé d'autres serveurs jusqu'à obtention de la réponse qu'il a forwardé au client) (1pts)**
2) S'agit-il d'une résolution inverse ou directe ? Expliquer. ==>**Directe car on donne le nom et on cherche l@ IP (0,5ps)**
3) Quels sont les avantages apportés par l'utilisation d'un cache pour le FAI, les serveurs DNS (particulièrement ceux de haut niveau et ceux correspondant à des domaines très demandés, par exemple google.com) et l'utilisateur ? ==> **minimiser le temps de résolution + minimiser les requêtes DNS vers les serveurs + minimiser la charge sur les serveurs DNS + minimiser les communications réseaux (1pts)**
4) N'importe qui peut créer un serveur DNS qui prétend connaître les adresses IP des machines d'un domaine donné (et qui pourrait donc donner de fausses adresses IP). Pourquoi n'est-ce pas un problème? ==> **ce n'est pas un problème car ce DNS ne sera pas consulté par les clients ou par les DNS (0,5pts)**
5) Compléter dans le tableau suivant l'entête DNS correspondante à la réponse envoyé par le serveur DNS du FAI à l'ordinateur du client (voir format de l'entête DNS en annexe). **(2pts)**

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0x3d9a															
1	0				0	1	1	1	----------			0			
1															
1															
1															
0															

Exercice 2 [9 pts]:

Partie1: chiffrement symétrique (6pts)

Soit **M** un message divisé en blocs $\{x_2,x_3,\ldots x_p\}$chacun de taille **n** bits et soit **K** une clé de même taille que les blocs (n bits). Soit $\{c_2,c_3,\ldots c_p\}$les cryptogrammes des blocs obtenus en appliquant la clé K aux blocs. Le chiffrement des blocs se fait selon le schéma suivant:

C_0= IV0 (valeur initiale) ; C_1= IV2 (valeur initiale) ;pour j de 2 à p, $c_j=E_K(C_{j-2} \oplus C_{j-1} \oplus x_j)$

La fonction E_K est inversible et son inverse est D_K c'est-à-dire que $D_K(E_K(x))=x$

1. Donner l'opération de déchiffrement ? (rappel : $A \oplus A=0$; $A \oplus 0=A$, $A \oplus B= B \oplus A$) ==> $D_K(c_j) \oplus C_{j-2} \oplus C_{j-1}=x_j$)
2. Peut-on chiffrer un bloc quelconque du message M sans chiffrer les blocs qui le précèdent ? Expliquer ? ==> **non, le chiffrement d'un bloc x_j dépend C_{j-2}et C_{j-1}**
3. Peut-on déchiffrer un bloc quelconque c_i sans déchiffrer les blocs qui le précèdent ? Expliquer ?==> **oui, voir formule de la première question**
4. Peut-on déchiffrer un bloc c_j en l'absence des autres blocs chiffrés ? Expliquer ?==> **oui, voir formule de la première question**
5. Prenons le cas où $E_K(x)=D_K(x) = K \oplus x$. Supposons qu'un attaquant a pu récupérer deux blocs

consécutifs (x_{j-1},x_j) ainsi que leurs cryptogrammes correspondants (c_{j-1},c_j). Cet attaquant peut-il en déduire la clé de chiffrement K ? ==> non il aura besoin de cj-2

6. Soient A et B deux entités utilisant le procédé de chiffrement décrit dans cet exercice. La clé K est fixée par l'une des deux entités puis transmise à la deuxième entité. Proposer une solution permettant aux deux entités d'échanger la clé K d'une façon **sécurisé et authentifié**. ==> obtenir la clé publique authentique (à partir du certificat) de B et l'utiliser pour chiffrer K. B déchiffre le cryptogramme avec sa clé privée et retrouve K

Partie 2: Chiffrement asymetrique RSA (3pts)

7. Un Professeur **P** envoie, par mail, les notes de ses étudiants au service examen **SE** de l'école. Les clés publique de **P** et **SE** sont (e_P=3,n_P=55) et (e_{SE}=3,n_{SE}=33) respectivement.
   a. Déterminer la clé privée (d_P) de **P** et celle de **SE** (d_{SE}). ==> (d_P)=27 de **P** et celle de **SE** (d_{SE})=7
   b. Afin d'assurer la confidentialité, **P** chiffre chaque note avec la clé du **SE**. Donner le message chiffré correspondant à la note 12 ? 12^3mod 33=12
   c. Pour assurer l'authenticité et la confidentialité, P signe chaque note puis il la chiffre avec la clé du SE. SE reçoit le message 23. Donner la note correspondante ? 23^7 mod 33=23 puis 23^3mod 33=

Algorithm Key generation for RSA public-key encryption

SUMMARY: each entity creates an RSA public key and a corresponding private key. Each entity A should do the following:

1. Generate two large random (and distinct) primes p and q, each roughly the same size.
2. Compute $n = pq$ and $\phi = (p-1)(q-1)$. (See Note 8.5.)
3. Select a random integer e, $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
4. Use the extended Euclidean algorithm (Algorithm 2.107) to compute the unique integer d, $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
5. A's public key is (n, e); A's private key is d.

Algorithm RSA public-key encryption

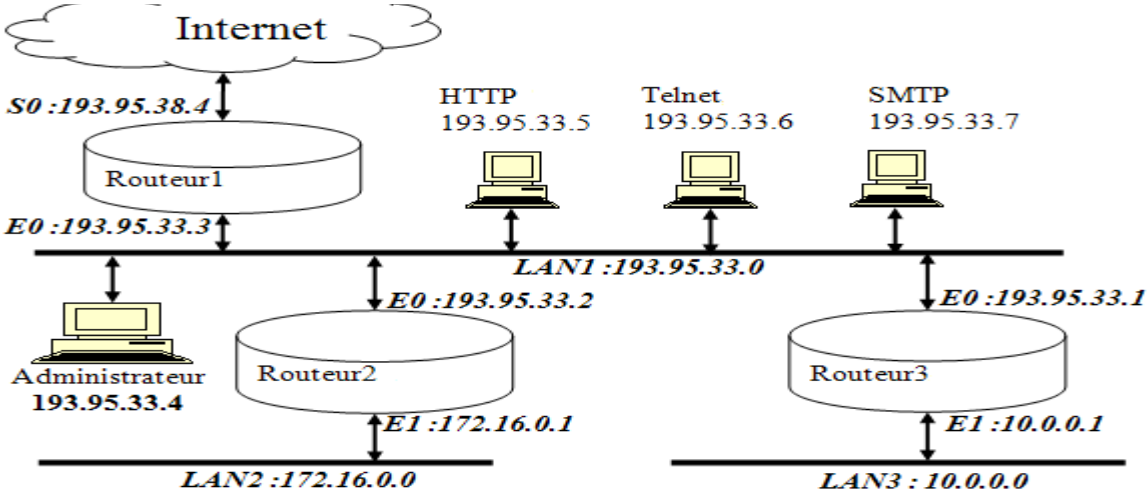
SUMMARY: B encrypts a message m for A, which A decrypts.

1. *Encryption.* B should do the following:
   (a) Obtain A's authentic public key (n, e).
   (b) Represent the message as an integer m in the interval $[0, n-1]$.
   (c) Compute $c = m^e \bmod n$ (e.g., using Algorithm 2.143).
   (d) Send the ciphertext c to A.
2. *Decryption.* To recover plaintext m from c, A should do the following:
   (a) Use the private key d to recover $m = c^d \bmod n$.

Exercice 3 [6pts]:

Soit le réseau suivant d'une entreprise.

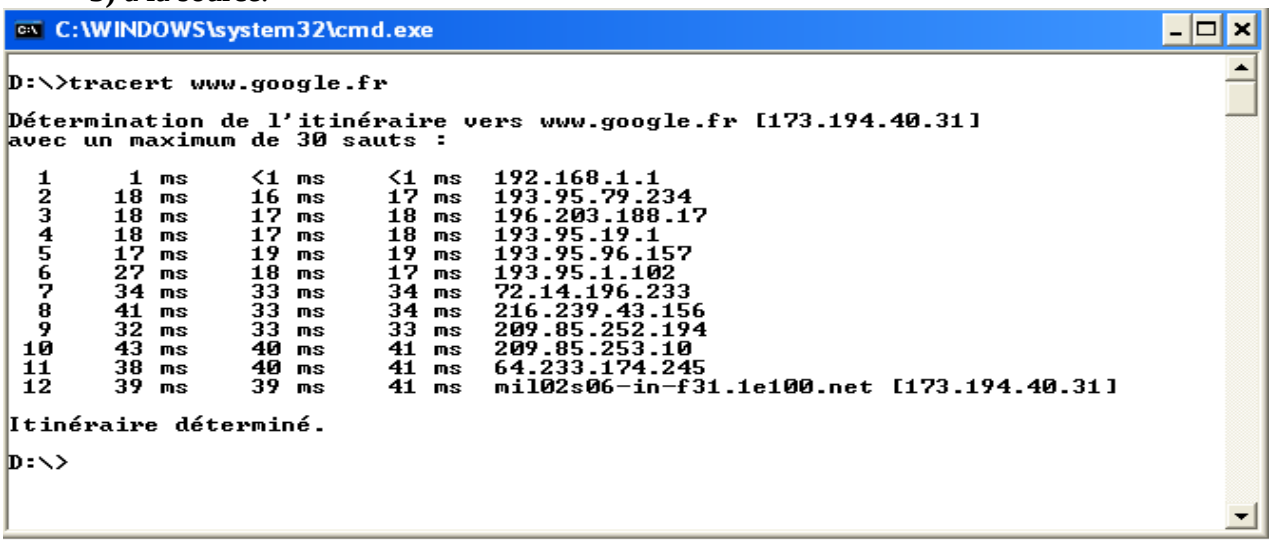
1) Donner les tables de routage des trois routeurs et de la machine administrateur permettant d'accéder aux différents LAN et à Internet. Utiliser le format (destination, routeur suivant)



2) Soit l'application **Traceroute (ou « tracert » sous windows)** qui montre la route prise par les paquets IP vers une certaine destination comme le montre l'exemple de la figure suivante.

Le fonctionnement de traceroute est décrit dans les points suivants :

- Traceroute envoie des datagramme UDP avec des ports généralement supérieurs à 32768
- Traceroute modifie le champ TTL (time to live) pour déterminer le chemin qu'un paquet prend pour atteindre la destination.
- Chaque paquet passe par un routeur, le champ TTL est décrémenté de 1.
- Quand le TTL d'un paquet est égal à 1, le paquet est détruit et un **message ICMP « Time exceeded » (type 11)** est envoyé à la source.
- Traceroute envoie un paquet avec un TTL égal à 1, ensuite 2, ensuite 3, et ainsi de suite, jusqu'à atteindre sa destination.
- Ceci force chaque routeur intermediaire d'envoyer à la source des **messages ICMP « Time exceeded » (type 11)**, qui sont utilisés pour identifier la route empruntée par le paquet. Lorsque la destination est ateinte, elle envoit un **message ICMP « Time exceeded » (type 3)** à la source.



Question :

Donner les règles de filtrage permettant de refuser le trafic traceroute entrant (quelqu'un de l'extérieur qui exécute traceroute sur le réseau de l'entreprise) en se limitant aux critères suivants :

@source	@destination	protocole	Port source	Port destination	Type de message ICMP	action

Annexe 1:

DNS (*Domain Name System)* est un protocole permettant d'associer à des noms de domaine (par exemple www.chezmoi.fr) une adresse IP (par exemple 140.78.132.45). Les machines se connectent entre-elles à l'aide d'adresses IP, mais les noms de domaine servent à faciliter la mémorisation et l'utilisation pour les humains et permettent également de structurer hiérarchiquement l'ensemble du réseau (en domaines, sous-domaines, etc.). Lorsqu'un utilisateur veut contacter la machine nommée www.banque.net, il doit obtenir son adresse IP. Ceci se fait en plusieurs étapes (illustrées sur la Figure 1) :

a. le client demande l'IP de www.banque.net au serveur DNS de son fournisseur d'accès à Internet (FAI) ;
b. le serveur DNS du FAI ne connaît pas l'adresse. Il demande alors au serveur DNS responsable de tous les noms de domaines (a.root-servers.net) l'adresse de www.banque.net ;
c. bien évidemment, ce serveur ne connaît pas toutes les adresses. Mais il sait que le serveur responsable du domaine .net est b.gtld.servers.net. Il renvoie alors le nom et l'adresse IP de ce serveur ;
d. le FAI demande alors à ce serveur l'adresse de www.banque.net ;
e. le DNS du domaine .net renvoie alors le nom et l'adresse du serveur DNS responsable du domaine .banque.net ;
f. le FAI interroge ce dernier serveur DNS, qui connaît l'adresse de la machine www.banque.net et la lui envoie ;
g. le serveur DNS du FAI peut finalement renvoyer l'adresse IP de la machine demandée par l'utilisateur.

En pratique les serveurs DNS des FAI mémorisent les réponses aux questions qu'ils ont posées dans un *cache*, ce qui leur permet d'éviter de faire certaines requêtes s'ils connaissent déjà la réponse.

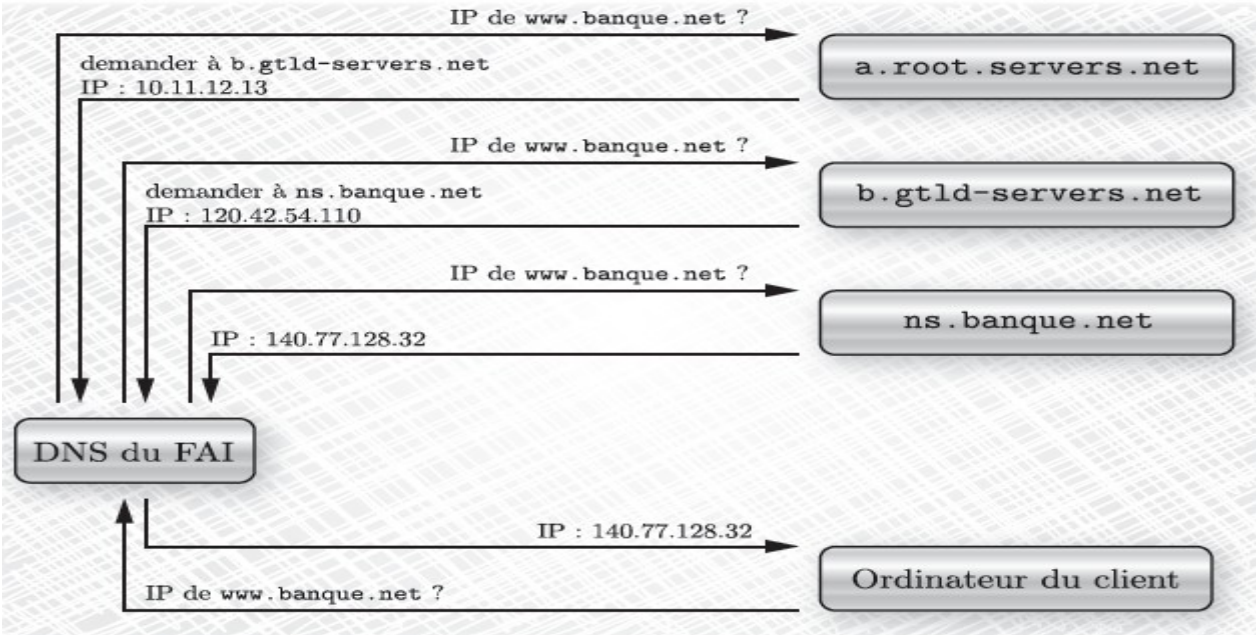


Figure 1 : Exemple de communications lors d'une requête DNS.

Format de l'entête DNS

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
identificateur de la requête (recopié dans la réponse)															
qr	opcode				aa	tc	rd	ra	Z			rcode			
QDCOUNT nombre d'entrées dans la section question															
ANCOUNT nombre d'entrées (RR) dans la section réponse															

NCOUNT	nombre d’entrées (NS) dans la section réponse
ARCOUNT	nombre d’entrées (RR) dans la section additionnel

qr: question (0) ou réponse (1)
Opcode:
0 - Requête standard (Query)
1 - Requête inverse (Iquery)
2 - Status d'une requête serveur (Status)
3-15 - Réservé pour des utilisations futures
aa : réponse d’une autorité
tc : message tronqué
rd : récursion désiré
ra : récursion acceptée
Z: utilisation futur
rcode: type de réponse
0 - Pas d'erreur
1 - Erreur de format dans la requête
2 - Problème sur serveur
3 - Le nom n'existe pas
4 - Non implémenté
5 - Refus
6-15 - Réservés