Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 1ère année

UE Réseaux Avancés I

Corrections — janvier 2012

Durée : 2h — Documents autorisés — Format des données réseaux en p.4

Protocole RTP, « Real Time Protocol » (2 points)

Vous pouvez compléter le tableau sur le sujet et le rendre avec votre copie (sans oublier d'indiquer dessus votre numéro d'anonymat).

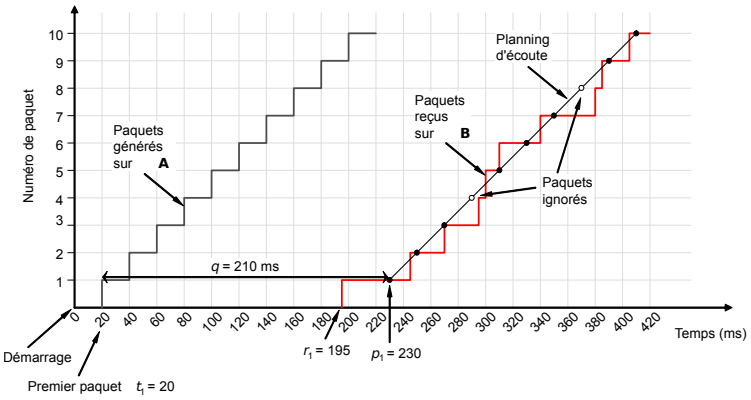
1 – 2pts Soit une session de téléphonie IP, *VoIP*, entre un hôte A et un hôte B :

- ⋆ chaque paquet contenant un échantillon sonore et partant de A à destination de B est numéroté ;
- ⋆ l'utilisateur sur A commence à parler au temps 0 ;
- ⋆ l'hôte A envoie un paquet toutes les $20ms$;
- ⋆ les paquets arrivent sur l'hôte B avec les temps indiqués dans le tableau ci-dessous ;
- ⋆ l'hôte B utilise un temps de retard dans son utilisation du contenu de chaque paquet $q = 210ms$.

a. Pourquoi certains paquets risquent d'être ignorés ?
Le récepteur choisit un temps de retard suffisamment grand pour annuler le jitter, puis utilise/joue chaque échantillon sonore au même rythme que le récepteur les construit et les envoie (toutes les 20ms). Les paquets reçus après le temps prévu de leur utilisation sont ignorés.

b. Complétez le tableau en indiquant le temps d'utilisation de chacun des paquets reçus (vous pouvez vous aider du graphe ci-dessous).

N°paquet	Tps arrivée r_i	Tps utilisation
1	195ms	230
2	245ms	250
3	270ms	270
4	295ms	ignoré > 290
5	300ms	310
6	310ms	330
7	340ms	350
8	380ms	ignoré > 370
9	385ms	390
10	405ms	410



Audit réseau (4 points)

2 – 4pts Analysez le contenu de la trame suivante :

```
0000   00 22 AA 01 21 31 00 D0  F1 10 12 13 88 47 00 00   ."..!1.......G..
0010   A0 17 45 00 00 28 00 83  00 00 17 06 13 3B A4 51   ..E..(.......;.Q
0020   22 43 A4 51 25 2D 00 50  20 00 00 00 00 00 00 00   "C.Q%-.P .......
0030   00 00 50 12 20 00 DF 6F  00 00                     ..P. ..o..
```

▷ que contient-elle ?

`'Ether / MPLS / IP / TCP 164.81.34.67:www > 164.81.37.45:8192 SA'`

- ▷ où transite-t-elle, entre quels matériels ?
  Cette trame est une trame possédant une étiquette MPLS, elle transite entre des routeurs MPLS.
- ▷ que pouvez-vous apprendre sur le réseau, les services ?
  - ◇ *Les adresses réseaux sont :*
    - ⋆ *toutes les deux de classe B,* `/16` *;*
    - ⋆ *de réseaux différents, du fait de passer par des routeurs MPLS : ce qui donne un réseau au minimum en* `/22` *:*
      - ○ *pour le troisième octet de l'@IP* `164.81.34.67` *:*

        34 $\Longrightarrow$

0	0	1	0	0	0	1	0
128	64	32	16	8	4	2	1

      - ○ *pour le troisième octet de l'@IP* `164.81.37.45` *:*

        37 $\Longrightarrow$

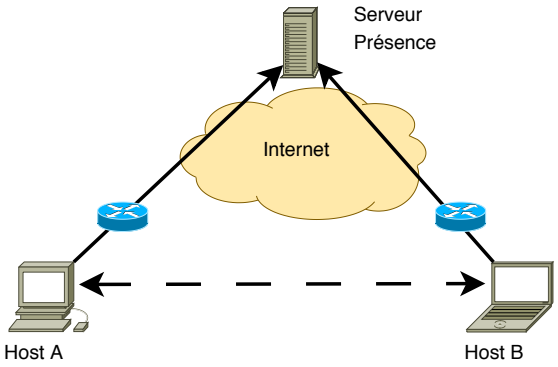
0	0	1	0	0	1	0	1
128	64	32	16	8	4	2	1

  - ◇ *Les services ? Un serveur Web, port 80, devrait être installé sur la machine* `164.81.34.67` *qui, d'après la trace, répond par un* `SA` *à une demande d'établissement de connexion.*

▬▬▬ Programmation « Socket » (6 points)

3 – Programmation d'un serveur de présence pour la mise en œuvre de chat direct

6pts Le but de ce projet est de permettre à deux clients de communiquer par chat directement entre eux (lien en pointillé sur le schéma ci-contre) :



- ▷ chaque client se connecte au serveur de présence à l'aide d'une connexion TCP ;
- ▷ chaque client indique sa « présence » grâce à cette connexion, et il fournit :
  - ◇ un identifiant « humain » : un pseudo ;
  - ◇ un TSAP pour la communication de chat pouvant être utilisé par un interlocuteur ;
- ▷ le serveur peut :
  - ◇ renseigner un client de la « présence » d'un autre client ;
  - ◇ fournir le TSAP du client avec qui on veut chatter.

Analyse du problème – 2 points

a. Sachant que :
   - ◇ chaque client appartient à un réseau différent ;
   - ◇ un client peut être derrière un routeur avec un firewall filtrant « extérieur $\Longrightarrow$ intérieur » et/ou réalisant du NAT (par exemple en ADSL) ;

   Est-ce qu'il est possible d'utiliser pour la communication directe de chat entre deux clients :

   i. le protocole UDP ?
      Le protocole UDP étant « sans connexion », dans le cas où l'un des deux clients est derrière un firewall/nat ce ne sera pas possible sans configurer explicitement ce firewall.

   ii. le protocole TCP ?
      Le protocole TCP étant « avec connexion » :
      - ⋆ *dans le cas où les deux clients sont derrières un firewall/nat : tout chat est impossible ;*
      - ⋆ *si un seul des client est derrière un nat alors seul ce client peut démarrer le chat vers l'autre client.*

b. Est-ce qu'il est possible de résoudre les problèmes évoqués en question a), en configurant **explicitement** le firewall présent sur le routeur d'un client ? Si oui, comment ?
   Dans le cas de la présence d'un client derrière un firewall/nat il faut mettre en place du « port forwarding », c-à-d du DNAT sur le firewall.

Programmation – 4 points

c. Écrire le programme en Algorithmique/Python réalisant le travail du client.

```python
#!/usr/bin/python
import socket,os,re

re_extraire_tsap = re.compile(r'^([\d\.]+):([\d]+)')
pseudo = 'dobby_is_dead'
port_service = 5555
port_chat = 6666
serveur_presence = "localhost"
tsap_serveur = (serveur_presence, port_service)
tsap_chat = ('', port_chat)

def traitement_chat(ma_socket):
      pid = os.fork()
      if (pid):
         while 1:
            ligne = ma_socket.recv(100)
            print ligne
      else:
         while 1:
            saisie = raw_input('>')
            ma_socket.sendall(saisie)
def attente_chat():
   # attente du chat
   socket_chat = socket.socket(socket.AF_INET, socket.SOCK_STREAM,socket.IPPROTO_TCP)
   socket_chat.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR,1)
   socket_chat.bind(tsap_chat)
   socket_chat.listen(socket.SOMAXCONN)
   while 1:
      (nouvelle_connexion, tsap_depuis) = socket_chat.accept()
      traitement_chat(nouvelle_connexion)

def enregistrement():
   # enregistrement sur le serveur de presence
   socket_enregistrement = socket.socket(socket.AF_INET, socket.SOCK_STREAM,socket.IPPROTO_TCP)
   socket_enregistrement.connect(tsap_serveur)
   socket_enregistrement.sendall("Enregistrement de : %s\n"%pseudo)
   socket_enregistrement.close()

def communiquer():
   pseudo_interlocuteur = raw_input('Avec qui voulez vous communiquer ?')
   socket_enregistrement = socket.socket(socket.AF_INET, socket.SOCK_STREAM,socket.IPPROTO_TCP)
   socket_enregistrement.connect(tsap_serveur)
   socket_enregistrement.sendall("Demande TSAP : %s\n"%pseudo_interlocuteur)
   reponse = socket_enregistrement.recv(100)
   socket_enregistrement.close()

   resultat = re_extraire_tsap.search(reponse)
   if resultat :
      IP_interlocuteur, port_interlocuteur = resultat.groups()
      tsap_interlocuteur = (IP_interlocuteur, int(port_interlocuteur))
      print tsap_interlocuteur
      socket_chat = socket.socket(socket.AF_INET, socket.SOCK_STREAM,socket.IPPROTO_TCP)
      socket_chat.connect(tsap_interlocuteur)
      traitement_chat(socket_chat)

print "Bienvenu dans mon programme de chat"
enregistrement()
pid = os.fork()
if (pid) :
   communiquer()
else :
   attente_chat()
```

▬▬▬ Firewall & QoS (8 points)

4 – Soit la trace suivante :

3pts

```
Chain FORWARD (policy DROP 345 packets, 23678 bytes)
 pkts bytes target     prot opt in     out     source               destination
   57  2280 REJECT     tcp  --  eth1   eth2    210.12.56.35         164.81.45.78   tcp dpt:22 reject-with tcp-reset
```

a. Quelle commande a fourni cette trace ?

```
iptables -nvL
```

b. Donnez la commande « `iptables` » qui a défini cette règle.

```
iptables -A FORWARD -i eth1 -o eth2 -s 210.12.56.35 -d 164.81.45.78 -p tcp --dport 22
-j REJECT --reject-with tcp-reset
```

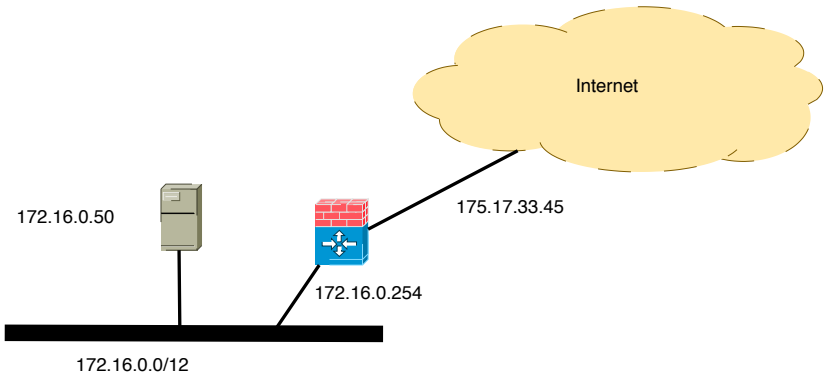
c. Cette règle a-t-elle été déjà utilisée ?
Oui, le compteur d'activation associé à la règle indique `57` *paquets traités.*

d. La « règle » est-elle bien adaptée à la « *policy* » ?
Si on compare les deux :
- ◇ *la « policy » est* `DROP`*, c-à-d que si aucune règle ne « match », correspond, au paquet alors le paquet sera supprimé.*
- ◇ *la règle rejette le paquet en informant l'émetteur par un « tcp-reset ».*

Dans tous les cas, le paquet est supprimé, par contre avec la règle on choisit d'informer l'émetteur de cette suppression.
Du point de vue strict de l'effet, on peut dire que la règle ne sert à rien.

e. Qu'est-ce qu'indiquerait l'outil « `nmap` », s'il « auditait » ce firewall ?
L'outil « `nmap` » teste successivement différents ports à la recherche de services « sensibles ».
Dans le cas d'un rejet avec un « tcp-reset » l'outil interprète le port comme inexistant, comme si le service n'était pas présent sur la cible.
Sans la règle, l'outil « `nmap` » indiquerait « filtered » ce qui peut trahir la présence du service et de sa protection.

5 – 5pts Une petite PME vous contacte pour configurer le routeur/firewall dans la configuration réseau suivante :



La **politique de sécurité** est la suivante :

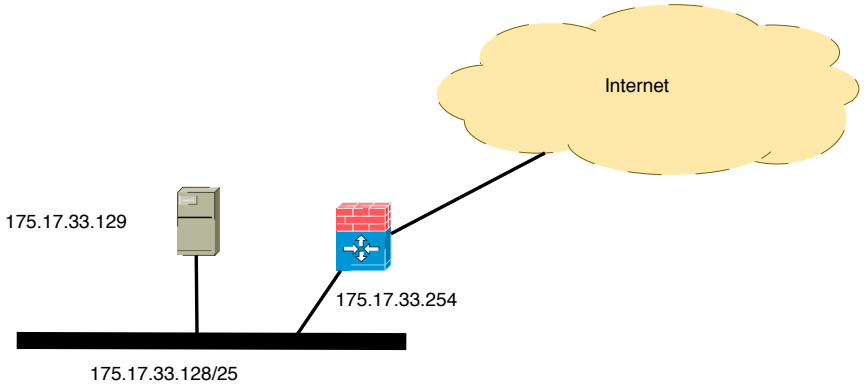
- ⋆ autoriser les communications « intérieur $\Longrightarrow$ extérieur » (l'extérieur correspondant à Internet) ;
- ⋆ bloquer les communications « extérieur $\Longrightarrow$ intérieur » ;
- ⋆ autoriser les communications vers la machine `172.16.0.50` depuis l'extérieur vers les services :
  - ◇ web (http) et web sécurisé (https) ;
  - ◇ ssh.

Questions :

a. Dans quel type de réseau est installé le serveur `172.16.0.50` ?
Dans un réseau privé.
Donnez la configuration du routeur Netfilter à l'aide de commandes « `iptables` » conformément à cette politique de sécurité.
Le réseau de l'entreprise étant privé, il est naturellement protégé contre les accès extérieurs :
- ◇ *pour permettre aux communications de sortir il faut faire du SNAT, ou « masqerading », avec comme @IP source, l'@IP globale du routeur ;*
- ◇ *pour permettre les communications entrantes, il faire du « port forwarding », c-à-d du DNAT.*

```
iptables -t filter -P FORWARD ACCEPT
iptables -t nat -A POSTROUTING -s 172.16.0.0/12 -j MASQUERADE
iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT --to-destination 172.16.0.50
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 172.16.0.50
iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination 172.16.0.50
```

La PME a investi dans l'achat du réseau `175.17.33.128/25` et a reconfiguré son réseau de la manière suivante :



Elle vous contacte pour reconfigurer son routeur/firewall.

b. Donnez la nouvelle configuration à l'aide de commandes « `iptables` » du firewall conformément à la politique de sécurité définie précédemment ;
Le réseau de l'entreprise est un réseau global, il faut donc le protéger par défaut et il n'y a plus de traduction d'adresses à faire.

```
iptables -t filter -P FORWARD DROP
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -d 175.17.33.129 -p tcp --dport 80  -m state --state NEW -j ACCEPT
iptables -A FORWARD -d 175.17.33.129 -p tcp --dport 443  -m state --state NEW -j ACCEPT
iptables -A FORWARD -d 175.17.33.129 -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

c. le responsable de la PME vous demande :
   i. de protéger l'accès au serveur SSH de la machine `175.17.33.129` contre les attaques « brute force » ;
   On va limiter dans le temps les tentatives de connexion, ce qui ralentira et rendra très difficile les attaques « brute force », en modifiant la règle précédente (autorisant le trafic vers ssh) :

```
iptables -A FORWARD -d 175.17.33.129 -p tcp --syn --dport 22 -m limit --limit 3/min --
limit-burst 1 -j ACCEPT
```

   Seul une demande de connexion toutes les 20s est autorisée, ce qui va ralentir et rendre impossible une attaque « brute force ».

   ii. de limiter le trafic en sortie du serveur Web à 30Mbps sachant que le réseau de l'entreprise dispose d'une ligne en sortie de 100Mbps.
   On désignera eth0 comme étant le nom de l'interface connectant le firewall au réseau `175.17.33.128/25`.

```
# tc qdisc add dev eth0 root handle 1: htb default 10
# tc class add dev eth0 parent 1: classid 1:10 htb rate 100Mbit
# tc class add dev eth0 parent 1: classid 1:20 htb rate 30Mbit
# iptables -A PREROUTING -t mangle -p tcp --sport 80 -j MARK --set-mark 1
# tc filter add dev eth0 protocol ip parent 1:0 handle 1 fw flowid 1:20
```

   iii. de lui expliquer si souscrire à une offre MPLS est intéressant ou non pour son entreprise.
   Son entreprise n'utilisant qu'un seul réseau local, MPLS ne lui servirait à rien.