Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 1ère année

UE Réseaux Avancés I

Examen — 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).

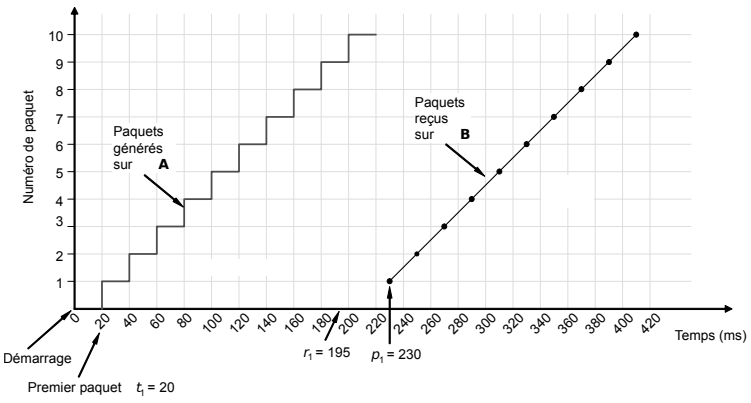
1 – 2pts Soit une session de téléphonie IP, *VoIP*, entre un hôte A et un hôte B :

- ⋆ 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 ?

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

N°paquet	Tps arrivée r_i	Tps utilisation
1	195ms	
2	245ms	
3	270ms	
4	295ms	
5	300ms	
6	310ms	
7	340ms	
8	380ms	
9	385ms	
10	405ms	



Audit réseau (4 points)

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

- ▷ que contient-elle ?
- ▷ où transite-t-elle, entre quels matériels ?
- ▷ que pouvez-vous apprendre sur le réseau, les services ?

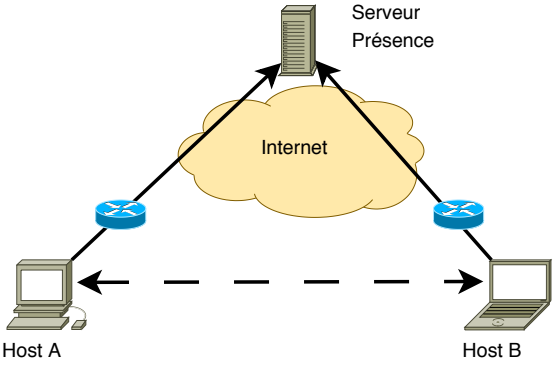
```
0000   00 22 AA 01 21 31 00 D0  F1 10 12 13 88 47 00 00   ."..!1.......G..
0010   A0 17 45 00 00 28 00 83  00 00 17 06 13 3B A4 51   ..E..(.......;.Q
0020   22 43 A4 51 25 2D 00 50  20 00 00 00 00 00 00 00   "C.Q%-.P .......
0030   00 00 50 12 20 00 DF 6F  00 00                     ..P. ..o..
```

Programmation « Socket » (6 points)

Vous pouvez répondre aux questions de « l'analyse du problème » sans tenir compte de la programmation Socket/Python.

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 ?
   ii. le protocole TCP ?

   Vous justifierez votre réponse et énumérerez les différents cas possibles.

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 ?
   Vous indiquerez juste la méthodologie, pas la ou les règles « `iptables` ».

Programmation – 4 points

c. Écrire le programme en Algorithmique/Python réalisant le travail du client.
   Vous ne tiendrez pas compte des problèmes de firewalls et vous considérerez que le client est dans un réseau « ouvert ».

Firewall & QoS (8 points)

4 – 3pts Soit la trace suivante :

```
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 ?

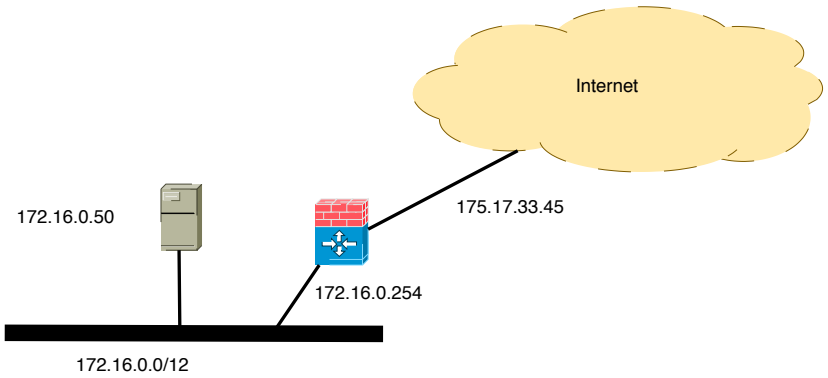
b. Donnez la commande « `iptables` » qui a défini cette règle.

c. Cette règle a-t-elle été déjà utilisée ?

d. La « règle » est-elle bien adaptée à la « *policy* » ?

e. Qu'est-ce qu'indiquerait l'outil « `nmap` », s'il « auditait » ce firewall ?

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



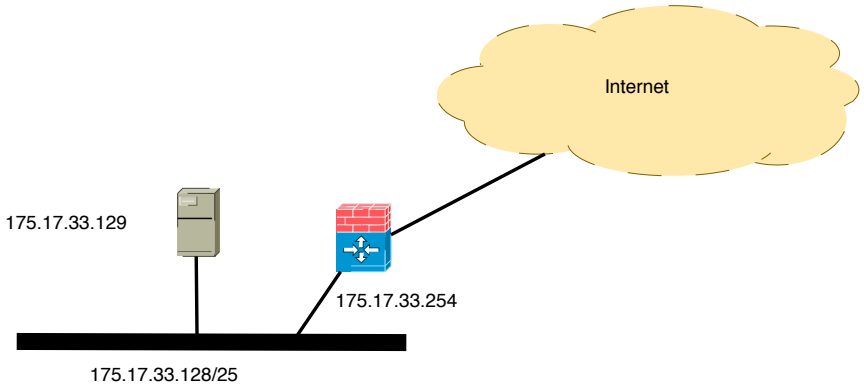
La **politique de sécurité** est la suivante :

- ⋆ 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` ?
Donnez la configuration du routeur Netfilter à l'aide de commandes « `iptables` » conformément à cette politique de sécurité.

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



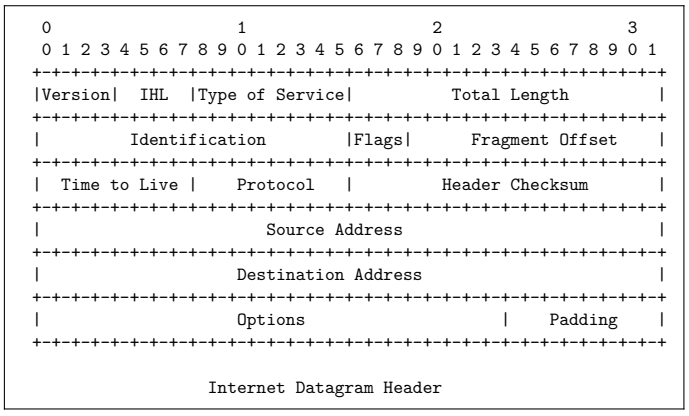
Elle vous contacte pour reconfigurer son routeur/firewall.

b. Donnez la nouvelle configuration à l'aide de commandes « `iptables` » du firewall conformément à la politique de sécurité définie précédemment ;

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 » ;
   Vous indiquerez la ou les commandes « `iptables` » à utiliser.

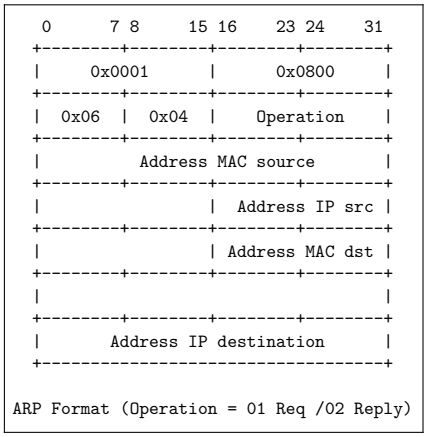
   ii. de limiter le trafic en sortie du serveur Web à 30Mbps sachant que le réseau de l'entreprise dispose d'une ligne en sortie de 100Mbps.
   Vous donnerez la liste des commandes à exécuter sur le firewall.

   iii. de lui expliquer si souscrire à une offre MPLS est intéressant ou non pour son entreprise.

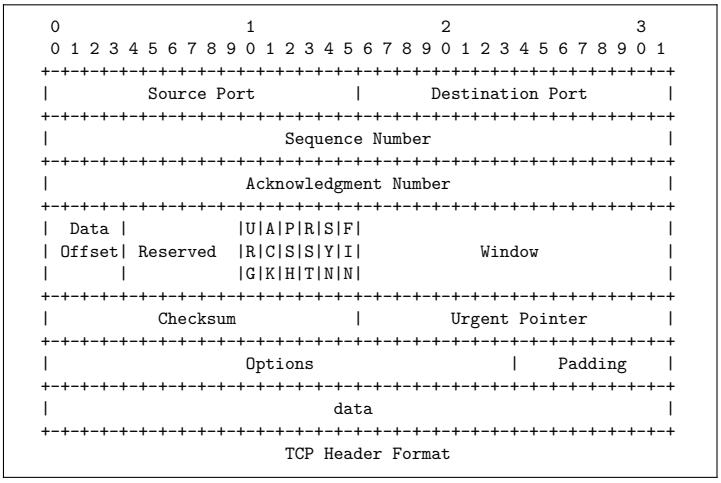


Internet Datagram Header

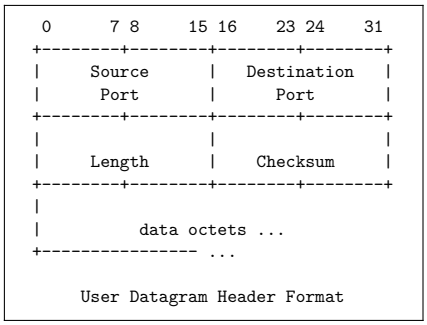
Decimal	Keyword	Protocol
0		Reserved
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
4	IP	IP in IP (encapsulation)
5	ST	Stream
6	TCP	Transmission Control
7	UCL	UCL
8	EGP	Exterior Gateway Protocol
9	IGP	any private interior gateway
10	BBN-RCC-MON	BBN RCC Monitoring
11	NVP-II	Network Voice Protocol
12	PUP	PUP
13	ARGUS	ARGUS
14	EMCON	EMCON
15	XNET	Cross Net Debugger
16	CHAOS	Chaos
17	UDP	User Datagram



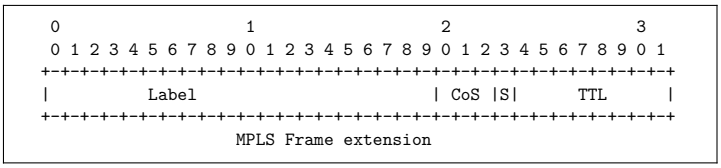
ARP Format (Operation = 01 Req /02 Reply)



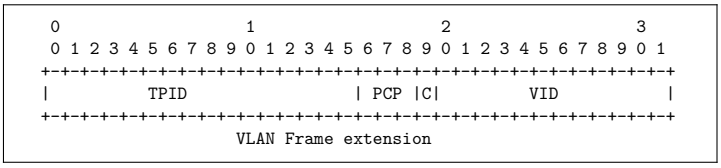
TCP Header Format



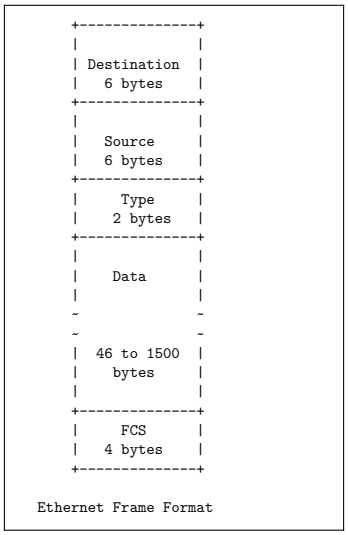
User Datagram Header Format



MPLS Frame extension



VLAN Frame extension



Ethernet Frame Format

EtherType	Protocol
0x0800	Internet Protocol, Version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x8035	Reverse Address Resolution Protocol (RARP)
0x809b	AppleTalk (Ethertalk)
0x8100	VLAN IEEE 802.1Q-tagged frame
0x8137	Novell IPX (alt)
0x8138	Novell
0x86DD	Internet Protocol, Version 6 (IPv6)
0x88a8	Provider Bridging (IEEE 802.1ad)
0x8847	MPLS unicast
0x8848	MPLS multicast
0x8863	PPPoE Discovery Stage
0x8864	PPPoE Session Stage
0x888E	EAP over LAN (IEEE 802.1X)
0x889A	HyperSCSI (SCSI over Ethernet)
0x88A2	ATA over Ethernet
0x88E5	MAC security (IEEE 802.1AE)
0x8906	Fibre Channel over Ethernet
0x9100	Q-in-Q
0xCAFE	Veritas Low Latency Transport (LLT)