Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 1ère année

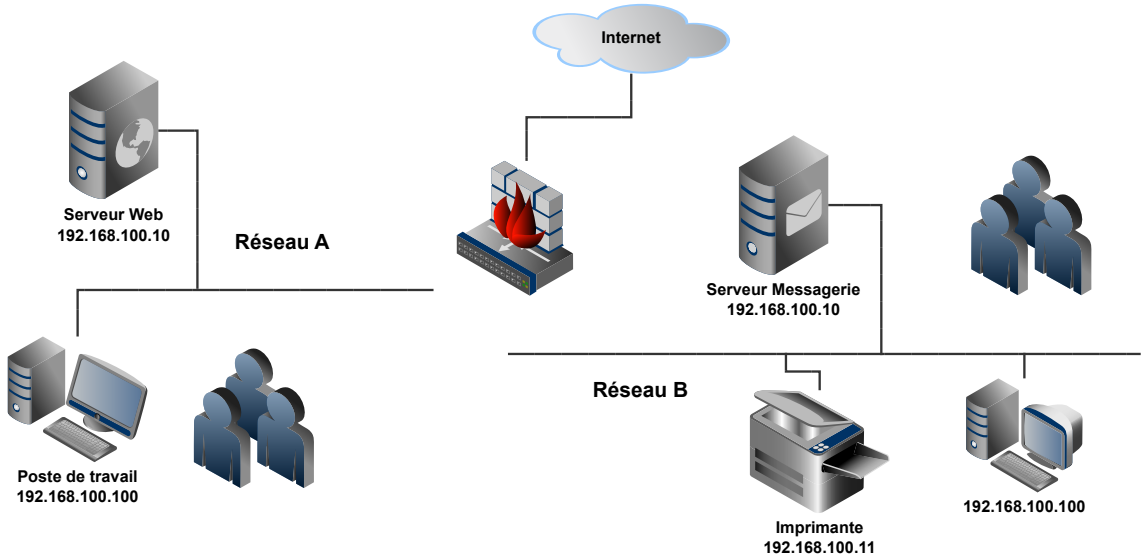
UE Réseaux Avancés I

Examen — décembre 2012

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

NetFilter & Gestion de congestion (12 points)

1 – 5pts Le responsable d'une petite entreprise vous appelle pour vous confier la tâche de « fusionner » le réseau de son entreprise avec celui d'une autre entreprise qu'il vient de racheter.



Les deux réseaux sont organisés de la même manière :

- le réseau A : en `192.168.100.0/24` :
  - un serveur Web est accessible à l'adresse `192.168.100.10` ;
  - les postes clients possèdent des adresses à partir de l'adresse `192.168.100.100` ;
- le réseau B : également en `192.168.100.0/24` :
  - une imprimante, qui permet d'imprimer par TCP sur le port 9100, est accessible à l'adresse `192.168.100.11` ;
  - un serveur de messagerie interne, accessible en POP et en SMTP, est accessible à l'adresse `192.168.100.10` ;
  - les postes clients possèdent des adresses à partir de l'adresse `192.168.100.100` ;
- les deux réseaux ne disposent d'aucun accès vers Internet.

Un routeur sous Linux a été acheté afin de servir de routeur et de firewall entre les deux réseaux, ainsi que de passerelle vers Internet.

Le responsable vous expose les contraintes :

- il ne faut pas modifier la configuration réseau des matériels connectés dans les réseaux A et B ;
- les utilisateurs du réseau A doivent pouvoir accéder au serveur de messagerie et à l'imprimante du réseau B ;
- les utilisateurs du réseau B doivent pouvoir accéder au serveur Web du réseau A ;

a. Est-il possible, grâce aux possibilités de NetFilter, de proposer une solution ?
Quels types d'opérations vous allez mettre en place, et comment les utilisateurs accéderont aux services proposés dans l'autre réseau que le leur ?

b. Donnez la configuration complète du firewall, après avoir choisi une adresse de connexion pour le routeur/firewall dans le réseau A et dans le réseau B.

c. Le responsable désire maintenant donner l'accès à Internet pour tous les utilisateurs des deux réseaux.
Donnez les règles de firewall à ajouter.

d. Le responsable voudrait maintenant donner l'accès à Internet **uniquement** aux utilisateurs du réseau A.
Est-ce possible ? et si oui, donnez la configuration du firewall le permettant.

2 – 4pts Soit la configuration suivante de NetFilter sur la machine A `192.168.127.186` (seule la table « `filter` » est utilisée) :

```
Chain INPUT (policy DROP 198 packets, 10591 bytes)
 pkts bytes target     prot opt in     out     source         destination
    6   321 ACCEPT     tcp  --  *      *       192.168.127.1  0.0.0.0/0     tcp dpt:50000 limit: avg 1/min burst 6

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source         destination

Chain OUTPUT (policy ACCEPT 175 packets, 8030 bytes)
 pkts bytes target     prot opt in     out     source         destination
```

a. Décrivez l'effet de ces règles.

b. On lance la commande suivante sur la machine A hébergeant le firewall :

```
$ socat stdio tcp-listen:50000
```

Est-ce que si l'on lance la commande suivante sur la machine B `192.168.127.1` :

```
$ socat stdio tcp:192.168.127.186:50000
```

la connexion s'établiera ?

c. La machine B veut envoyer $18000ko$ vers la machine A, après une connexion réussie.
Décrivez comment va évoluer dans les 5 premières secondes de communication la fenêtre de congestion en considérant que :
- la machine B utilise l'algorithme Tahoe ;
- le MSS est de $1500ko$;
- la taille de la fenêtre de réception de A est de taille $20ko$;
- le RTT est de $1sec$;
- le RTO sur B est de $3sec$.

Vous tiendrez compte de la présence du firewall et des paquets nécessaires au « handshake » TCP.

3 – 3pts Étude et correction de fichier de configuration de firewall

a. Soit le fichier de configuration de firewall suivant :

```
1 sudo iptables -t filter -F
2 sudo iptables -t filter -P FORWARD DROP
3 sudo iptables -t filter -A FORWARD -p tcp --dport 80 --syn -j ACCEPT
```

Est-ce qu'il est correct pour autoriser les connexions vers le service HTTP ? Si non, pouvez-vous le corriger ?

b. Soit le fichier de configuration suivant :

```
1 sudo tc qdisc add dev eth0 root handle 1: htb default 10
2 sudo tc class add dev eth0 parent 1: classid 1:10 htb rate 30mbps
3 sudo tc class add dev eth0 parent 1: classid 1:20 htb rate 20mbps
4 sudo tc class add dev eth0 parent 1: classid 1:30 htb rate 50mbps
5 sudo tc filter add dev eth0 protocol ip parent 1: handle 1 fw classid 1:10
6 sudo tc filter add dev eth0 protocol ip parent 1: handle 2 fw classid 1:20
7 sudo tc filter add dev eth0 protocol ip parent 1: handle 3 fw classid 1:30
```

Donnez la règle de firewall permettant de limiter le trafic à 20mbps, en provenance de la machine `193.50.87.18` et à destination d'Internet pour le protocole TCP à destination du port 5900.

Analyse de trame (3 points)

4 – 3pts Soit la trame suivante :

```
0000   FF FF FF FF FF FF 00 D0  F1 10 12 13 81 00 00 01   ................
0010   08 06 00 01 08 00 06 04  00 01 00 D0 F1 10 12 13   ................
0020   C0 A8 01 79 00 00 00 00  00 00 A4 51 01 04         ...y.......Q..
```

a. Analysez cette trame : que contient-elle ?
b. Où cette trame circule-t-elle, entre quels matériels ?
c. Est-ce que cette trame est « normale » ou a-t-elle été « forgée » ?

Vous justifierez votre réponse.

Programmation Python (5 points)

5 – 5pts Le responsable du système d'information d'une entreprise vous demande de programmer un outil permettant à des connexions TCP issues de postes de travail de traverser automatiquement un firewall :

- le réseau où se trouve les postes de travail est le `10.10.0.0/16` ;
- le routeur/firewall possède l'adresse IP `10.10.10.10` dans ce réseau ;
- un serveur logiciel TCP attend sur le routeur/firewall sur le port 6800 et exécute le protocole suivant :
  - il attend la connexion d'un poste de travail ;
  - lorsqu'une connexion se réalise, le serveur dispose d'une **connexion initiale** avec le poste de travail ;
  - il reçoit, sur cette **connexion initiale**, une ligne contenant le TSAP de la machine que le client veut atteindre de l'autre côté du firewall :

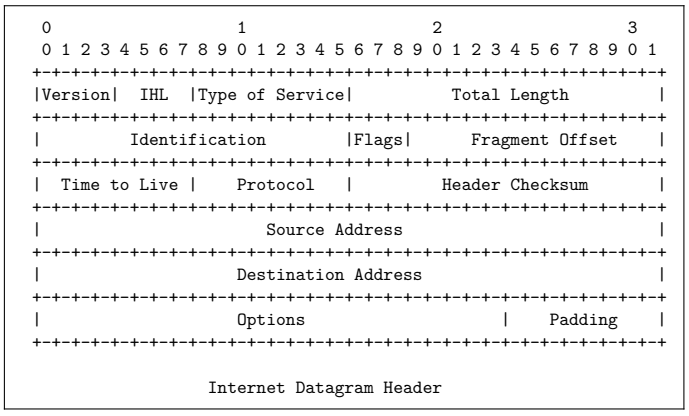
    `adresseIP:numéroPort\r\n`

  - le serveur récupère cette ligne et l'analyse pour établir une **nouvelle connexion** vers le TSAP indiqué ;
  - à partir de cet instant :
    - tout ce que le poste de travail envoie sur la **connexion initiale** est renvoyer sur la **nouvelle connexion** ;
    - tout ce que le serveur reçoit sur la **nouvelle connexion** est renvoyé vers le poste de travail sur la **connexion initiale** ;
  - *vous ne vous occuperez par de la terminaison de ces deux connexions*.

a. indiquez la configuration de base du firewall pour :
   - permettre le travail du serveur logiciel ;
   - empêcher les postes de travail de traverser le firewall ;

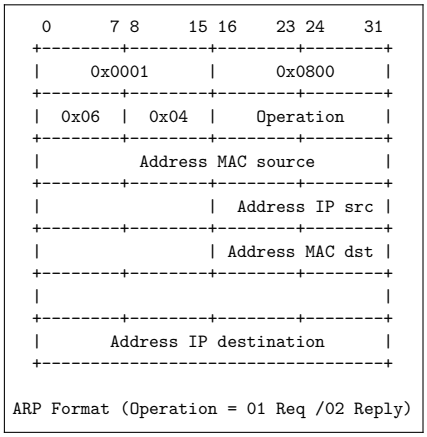
b. Donnez le programme Python réalisant le travail du serveur logiciel.

c. Il existe une ancienne version du logiciel client sur certains postes de travail qui utilise le même protocole **mais** qui utilise le port de destination 7800 pour se connecter au firewall.
Est-il possible, à l'aide du firewall, de les rediriger automatiquement vers la nouvelle version du serveur utilisant le port 6800 ? Si oui, indiquez comment.

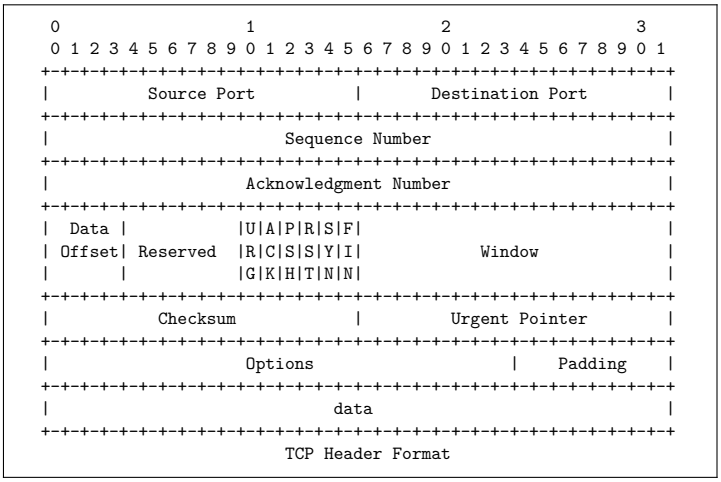


Internet Datagram Header

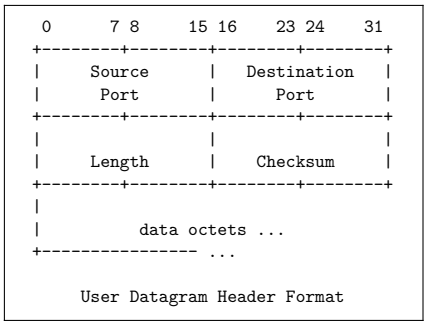
Decimal	Keyword	Protocol
0		Reserved
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
4	IP	IP in IP (encapsulation)
5	ST	Stream
6	TCP	Transmission Control
7	UCL	UCL
8	EGP	Exterior Gateway Protocol
9	IGP	any private interior gateway
10	BBN-RCC-MON	BBN RCC Monitoring
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



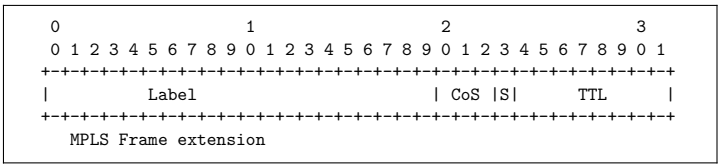
ARP Format (Operation = 01 Req /02 Reply)



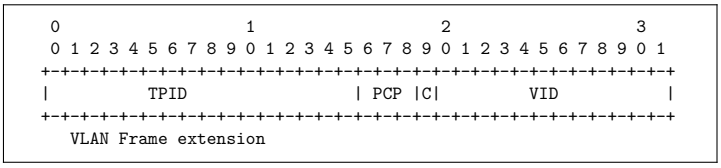
TCP Header Format



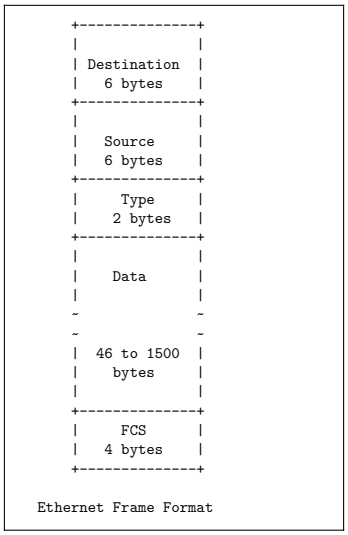
User Datagram Header Format



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)