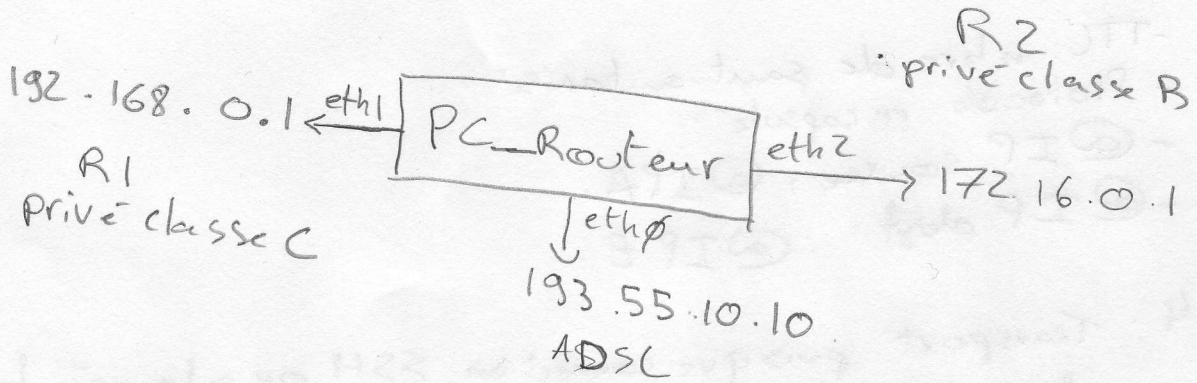


Exercice 1

1-a



b - Commande:

Windows: netstat -r

Unix: route -n

Table routage PC-Routeur

Destination	Passerelle	Masque	Interface
127.0.0.0	127.0.0.1	255.0.0.0	lo
192.168.0.0	192.168.0.1	255.255.255.0	eth1
172.16.0.0	172.16.0.1	255.255.0.0	eth2
0.0.0.0	192.168.0.1	0.0.0.0	eth1

2-a - Connection SSH => TCP port 22.

Le sniffeur est en eth1.

On capte donc:

Couche 2: Permet la communication sur le même médium.

Donc on obtient

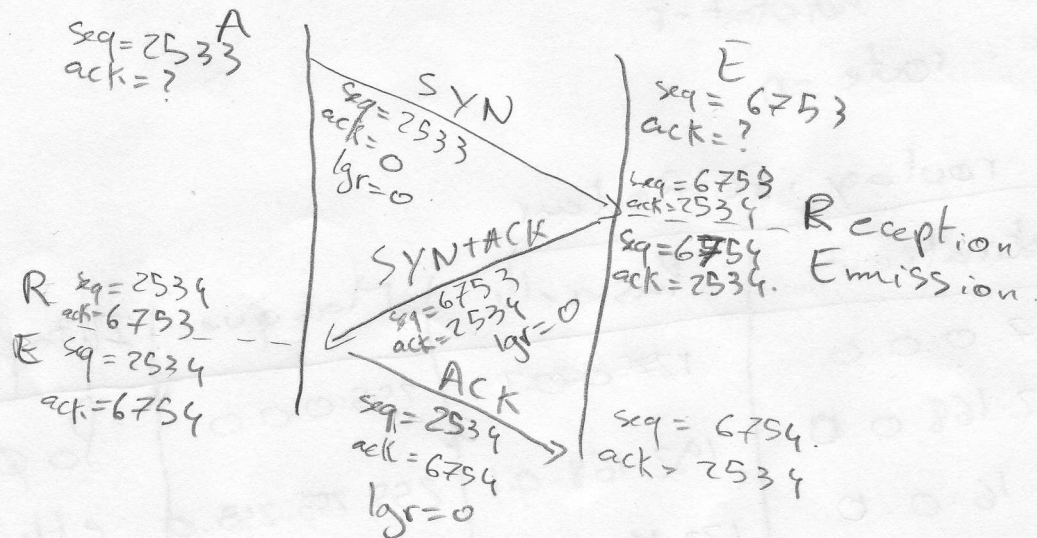
- @ Mac Dest : @ Mac PC-Routeur
- @ Mac Src : @ Mac A.
- Si lg > 1500

Si $lg \leq 05Dc$ (en decimal:)
 → longueur des données
 Sinon protocole encapsule

Cache 3: Permet la communication sur des médiums ≠

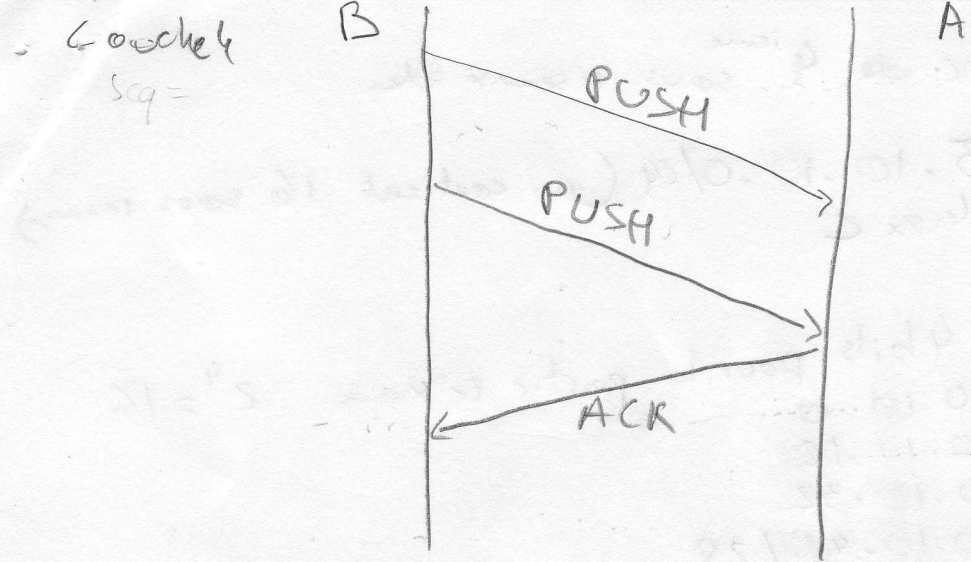
- TTL: nbre de saut autorisé
- Protocole encapsule
- @IP source: @IPA
- @IP dest: @IPE

Cache 4: Transport puisque connection SSH on a lancé la demande de connection avec l'échange des numéros de seq et ack entre A et E.



b- B envoie à A et A répond par ACK. Comme précédemment A et B sur un médium

	B	A
Couche 2	@Mac A, @Mac B + taille donnée / protocole couche 3	@Mac B, @Mac A + taille donnée / protocole couche 3
Couche 3	@IP B, @IP A + protocole couche 4	@IP A, @IP B + protocole couche 4
Couche 4	Port src sur B Port dst sur A - type: Push. - longueur=200	- Port src sur A - Port dst sur B. - type: ACK. - lgr=0



- C- Les postes B et D sont sur des médiums \neq , donc les informations contenues dans la couche 2 seront \neq . De plus le PC-Routeur permet de router les paquets entre le réseau 1 et 2, il intervient donc au niveau 3. Il a pour rôle de modifier le TTL mais aussi de changer les @src sources et destinations de la couche 2.

- 3- Dans un premier temps ajouter une règle dans la table de routage afin de permet l'accès au réseau FAI.

Destination	Passerelle	Masque
0.0.0.0	193.55.10.10	0.0.0.0

- 4-a-Il faut que l'on fasse partie du réseau du FAI, donc c'est cet organisme qu'il faut demander les IP, publiques

b-

b. i On souhaite utiliser de 4^{ème} sous-réseau du
et ii

195.10.1.0/24 (qui contient 16 sous réseaux)
classe C

16 sous-réseaux \Rightarrow 4 bits pour la partie réseau. $2^4 = 16$.

1	0 0 0 0	195.10.10.0
2	0 0 0 1	195.10.10.16
3	0 0 1 0	195.10.10.32
4	0 0 1 1	\rightarrow 195.10.10.48/28.

16 1 1 1 1 195.10.10.0011/0000.

On a donc @ réseau : 195.10.10.48/28.
Masque : 255.255.255.240.
broadcast : 195.10.10.63.

On a donc 24 machines disponibles = 16 machines

c.

Destination	Passerelle	Masque	Interface
127.0.0.0	127.0.0.1	255.0.0.0	lo0
172.16.0.0	172.16.0.1	255.255.0.0	eth2
195.10.10.48	195.10.10.49	255.255.240.0	eth1
0.0.0.0	195.10.10.10	0.0.0.0	

d. Un serveur DHCP permet de distribuer dynamiquement
des adresses IP aux postes qu'il gère.

ii Le but du DHCP est d'attribuer de manière
dynamique des @IP, puisque le FAI nous en
permet la création d'un sous-réseau pour le
réseau 1, il faut laisser le FAI donner des adresses
aux postes A, B, C du Réseau 1.

Exercice 2

1- Ethernet Structures \neq .
Wi-fi
ATM
LLC

2- En ethernet, on peut SOIT écouter SOIT envoyer
mais pas les 2 en même temps.
Carrier Sense Medium Access / Collision Detect.

Lorsque l'on envoie une trame on écoute pendant un
certain temps pour savoir si il y a eu collision entre 2
trames.

3- Classe C 192.100.0.0/24.

128 sous réseaux = 7 bits $2^7 = 128$.

En classe C on dispose de 8 bits, on pourrait donc
avoir 1 machine par sous réseau.

Le masque de sous-réseau serait de la forme.

192.100.0.254.

L'adresse de la seule machine = @ broadcast.
 \Rightarrow Ne marche pas

64 @ sous-réseaux Max

5 - Un annuaire LDAP permet de centraliser les informations d'authentification sur les postes. Le serveur permet donc de réunir les informations pour l'administration + Gestion Machine/IP.

6 - Pour télécharger via les réseaux P2P les utilisateurs ont besoin d'utiliser des applications basées sur TCP ou UDP, c'est 2 protocoles s'appliquent sur les ports de la machine. Il suffit donc de mettre en place un pare-feu bloquant les entrées/sorties de tous les ports SAUF ceux autorisés. (Ex: HTTP: 80, SMTP: 25, ...)

7 - a - Un VPN (Virtual Private Network) permet d'intégrer au réseau un poste qui n'est pas physiquement dans le réseau. Le commercial n'est pas dans son entreprise mais son poste fait virtuellement partie du réseau.

b -
★ Cryptage symétrique: même clé pour le chiffrement et le déchiffrement des messages.

Cryptage asymétrique: 2 clés 1 publique pour que les personnes chiffrent les messages qu'ils souhaitent m'envoyer. 1 clé privée qui me permet de déchiffrer les messages

1^{er} cryptage Entre Client et Serveur Authentification
2^{ème} cryptage Entre Client et Serveur Distant.