8 – RESEAUX ET SECURITE

Exercices

1 Masques de réseaux et adresses IP

« A faire vous-même » n° 1, 2 et 3 à la page indiquée au lien ci-dessous :
Introduction au réseau (pixees.fr)

2 Masques de réseaux et adresses IP

Trois machines ont respectivement pour adresses IP 90.8.220.5, 90.8.220.20 et 90.8.220.37. Est-ce que ces machines appartiennent toutes les trois au réseau 90.8.220.0/27 ?

Sinon combien de routeurs sont nécessaires pour faire communiquer ces machines ? Quelles sont les adresses de leurs cartes réseau (interfaces) ?

3 Réseaux et adresses IP

Une machine M1 a pour adresse IP 192.168.1.12 et elle se trouve dans un réseau d'adresses 192.168.1.0/24. Elle est reliée à un routeur qui possède deux interfaces réseau qui ont pour adresses respectives 192.168.1.1/24 et 172.20.121.1/24. Une seconde machine M2 a pour adresse IP 172.20.121.17 et se trouve dans le réseau d'adresses 172.20.121.0/24, reliée au routeur.

1. Compléter la table de routage de ce routeur.

Adresse	Masque	Passerelle	Interface
192.168.1.0	...	...	...
172.20.121.0	...	...	...

2. Compléter la table de routage de la machine M1.

Adresse	Masque	Passerelle	Interface
192.168.1.0	...	...	...
0.0.0.0	...	...	...

3. Compléter la table de routage de la machine M2.

Adresse	Masque	Passerelle	Interface
172.20.121.0	...	...	...
0.0.0.0	...	...	...

4 Représentation d'un réseau

Une machine M1 a pour adresse IP 192.168.1.12 et elle se trouve dans un réseau d'adresses 192.168.1.0/24. Elle est reliée à un switch S1 lui-même relié à un routeur R1 qui possède deux interfaces réseau qui ont pour adresses respectives 192.168.1.1/24 et 172.16.8.1/24.

Le routeur R1 est relié à un switch S2 relié à un routeur R2 qui possède deux interfaces réseau qui ont pour adresses respectives 172.16.8.2/24 et 172.20.121.1/24. Cette dernière interface est reliée à un routeur R3, possédant une interface d'adresse 172.20.121.2/24, et relié lui-même à une machine M3 ainsi qu'à Internet par une autre interface.

Une machine M2 a pour adresse IP 172.16.8.17 et elle se trouve dans le réseau d'adresses 172.16.8.0/24, reliée au switch S2.

Faire le schéma du réseau en indiquant les adresses IP des machines et des interfaces.

5 Réseaux et adresses IP

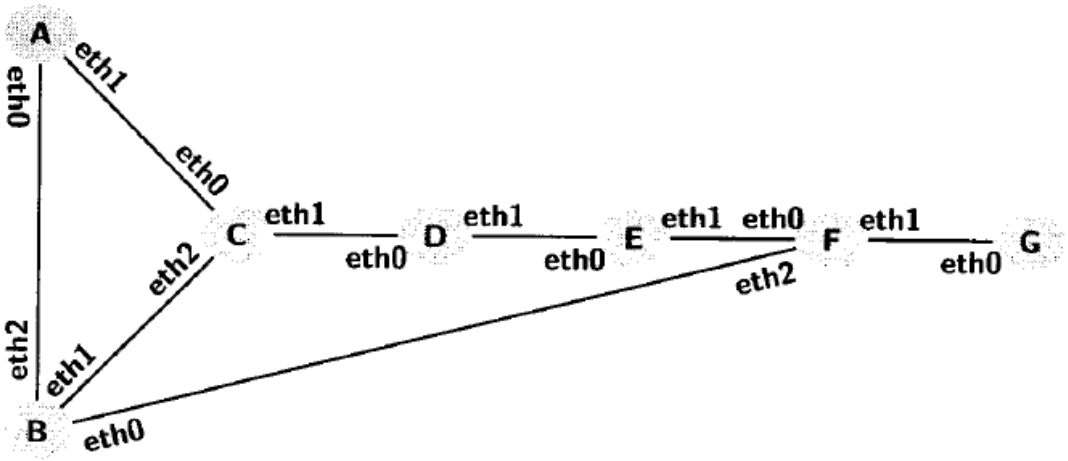
« A faire vous-même » n° 1, 2 et 3 à la page indiquée au lien ci-dessous :
https://pixees.fr/informatiquelycee/n_site/nsi_term_archi_routage.html

6 Chemin particulier

En utilisant la ligne de commande, déterminer un itinéraire pour atteindre la page d'accueil du site :

societe-informatique-de-france.fr

7 Table de routage RIP



Dans le réseau ci-dessus, les nœuds A à F sont des routeurs dont on veut calculer les tables de routage. On suppose que l'on a exécuté le protocole RIP sur ce réseau. Compléter la table suivante, qui indique pour chaque machine la portion de la table de routage pour la destination G.

machine	destination	passerelle	interface	distance
A	G	B	eth0	2
B	G	F	eth0	1
C	G	B	eth2	2
D	G	E	eth1	2
E	G	F	eth1	1
F	G	F	eth1	0

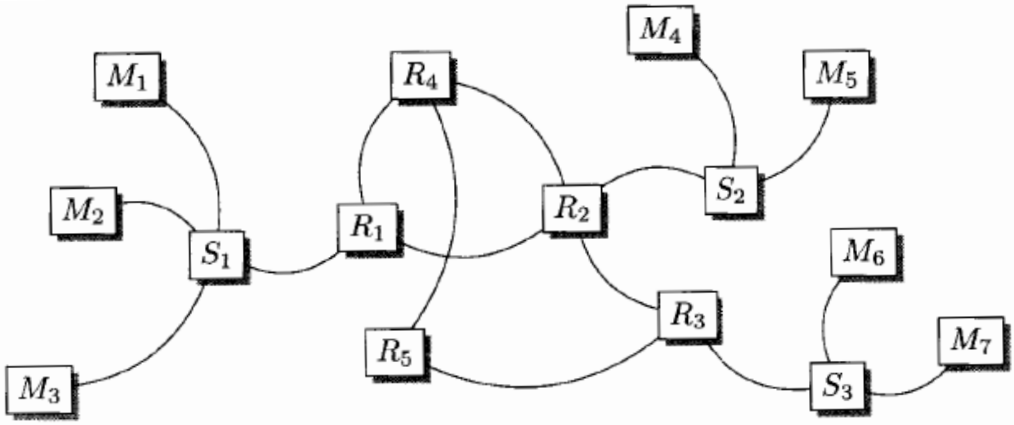
8 Tables de routage

« A faire vous-même » n° 4, 5 et 6 à la page indiquée au lien ci-dessous :

https ://pixees.fr/informatiquelycee/n_site/nsi_term_archi_routage.html

. . . /

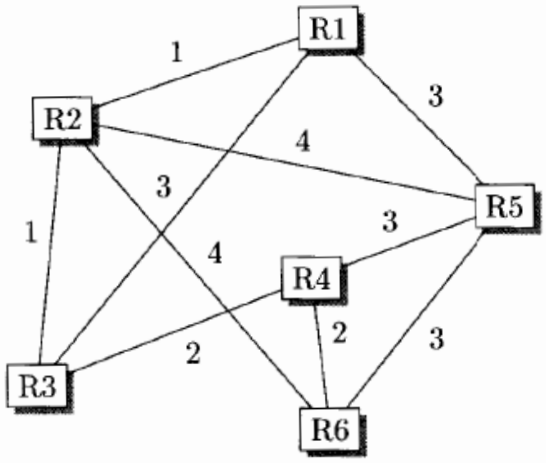
9 Pannes sur le réseau



1. Combien de routes différentes peut prendre un paquet entre les machines M1 et M7 ? Une route ne peut passer qu'une seule fois par un routeur donné.
2. Examiner les conséquences d'une panne d'un des cinq routeurs. Envisager tous les cas possibles.

10 Protocole OSPF

On considère le graphe suivant, où le nombre situé sur l'arête joignant deux sommets représente une distance :



1. Quel est le plus court chemin entre R1 et R4 ?
2. Quel est le plus court chemin entre R1 et R6 ?
3. Combien de chemins entre R1 et R6 passent par tous les sommets sans passer deux fois par le même sommet ?

11 Chiffrement asymétrique RSA (Rivest-Shamir-Adleman)

Exemple avec de petits nombres premiers (en pratique il faut de très grands nombres premiers) :

1. on choisit deux nombres premiers $p = 3$, $q = 11$;
2. leur produit $n = 3 \times 11 = 33$ est le module de chiffrement ;
3. $\varphi(n) = (3 - 1) \times (11 - 1) = 2 \times 10 = 20$;
4. on choisit $e = 3$ (premier avec 20) comme exposant de chiffrement ;
5. l'exposant de déchiffrement est $d = 7$, l'inverse de 3 modulo 20 (en effet $ed = 3 \times 7 \equiv 1 \bmod 20$).

La clé publique d'Alice est $(n, e) = (33, 3)$, et sa clé privée est $(n, d) = (33, 7)$. Bob transmet un message à Alice.

- Chiffrement de $M = 4$ par Bob avec la *clé publique* d'Alice : $4^3 \equiv 31 \bmod 33$, le chiffre est $C = 31$ que Bob transmet à Alice ;
- Déchiffrement de $C = 31$ par Alice avec sa *clé privée* : $31^7 \equiv 4 \bmod 33$, Alice retrouve le message initial $M = 4$.

Le mécanisme de signature par Alice, à l'aide de sa clé privée, est analogue, en échangeant les clés.

1. Ecrire un programme en Python fournissant une clé publique (n, e) et une clé privée (n, d), en fonction de p, q et e, sachant que e doit être strictement inférieur à f = (p-1)(q-1).

Aide:

- le programme demande à l'utilisateur de choisir p, q, nombres premiers strictement supérieurs à 2, puis calcule f = (p-1)(q-1)

- on demande ensuite à l'utilisateur de choisir e, strictement inférieur à f et premier avec f ;

- le programme détermine d, inverse de e modulo f ; pour cela, on part de d=3, et on incrémente d tant que la division euclidienne de ed par f donne un reste différent de 1. On doit avoir d < f.

(rappel: en Python, le reste par division euclidienne de a par b s'écrit "a % b").

- enfin le programme retourne la clé publique (n, e) et la clé privée (n, d).

2. Se regrouper par binômes ou trinômes. Chacun fait coder par un camarade, avec une clé publique, un nombre strictement inférieur à n, puis le décode avec sa clé privée. Intervertir les rôles.

12 Chiffrement symétrique AES (Advanced Encryption Standard)

« A faire vous-même » n° 1 : https://pixees.fr/informatiquelycee/n_site/nsi_term_archi_secu.html .

13 Codage et décodage binaire avec l'opérateur XOR

On considère l'octet m1 = 1010 1010 et la clé K = 110.

1. En s'inspirant de l'exercice 12, coder m1 avec la clé K pour produire un octet c.
2. Décoder c avec K pour produire un octet m2. Vérifier que m2 = m1.
3. La clé K est-elle symétrique ou asymétrique ?

14 Certificat de sécurité

Consulter la page d'accueil du site https://www.societe-informatique-de-france.fr .

Préciser les informations disponibles sur le certificat de sécurité (clic droit sur le cadenas) : société émettrice, chiffrements utilisés, clés.