8 – RESEAUX ET SECURITE

Compléments sur le cours de Bonnefoy & Petit

Points d'histoire

1958 : premier modem, permettant de transmettre des données entre deux ordinateurs
1983 : le protocole TCP/IP devient le standard pour les réseaux
1993 : le CERN de Genève présente le web

Définitions à retenir (cf B.O.)

Concentrateur (« **hub** ») : appareil diffusant des trames simultanément vers plusieurs machines d'un réseau local.

Commutateur (« **switch** ») : appareil renvoyant des trames au destinataire d'un réseau local. On peut voir le switch comme un hub sélectif.

Routeur (« **router** ») : appareil renvoyant des trames vers un réseau ou un autre routeur, en optimisant l'acheminement du message.

Pour approfondir les notions de routeur, switch et hub :
https://community.fs.com/fr/blog/whats-the-difference-hub-vs-switch-vs-router.html

Passerelle (« **gateway** ») : routeur reliant deux réseaux de types différents. Ex. : la box permet de relier un réseau domestique à internet. Elle joue à la fois le rôle de passerelle et de switch.
NB : certains comprennent la passerelle comme le premier routeur prenant en charge le message émis par la machine considérée. Ainsi, dans le chemin R1-R2-R3-M, le routeur R2 serait considéré comme une passerelle vis-à-vis du routeur R1, quand celui-ci transmet un message à destination d'une machine M.

Interface : port permettant à une machine de communiquer sur un réseau. Une machine peut disposer de plusieurs interfaces. Chaque interface est dotée d'une adresse physique MAC (Medium Access Control) et d'une adresse IP.

Masque : série de 32 bits permettant d'extraire l'adresse réseau de l'adresse IPv4 d'une machine. Le masque commence par une série de 1 et enchaîne avec une série de zéros. Les zéros, associés aux bits de l'adresse IP via des portes ET, masquent les bits spécifiques à la machine. Ainsi ne sont conservés que les bits propres au réseau local. Ex. : le masque 11111111 11111111 11111111 00000000 s'écrit « 255.255.255.0 » en base 10, et indique que dans l'adresse IP considérée, les trois premiers octets désignent le réseau, et le quatrième la machine.
NB : pour que deux machines puissent communiquer sans l'intermédiaire d'un routeur, leurs adresses IP doivent comporter la même adresse de réseau local.

Métrique : distance, dans une table de routage, séparant la machine de son correspondant.

Protocole RIP (« Routing Information Protocol ») : protocole de mise à jour des tables de routages où les métriques sont comptées en nombre de sauts (i.e. nombre de routeurs par lesquels transiter pour atteindre le correspondant).
Le protocole RIP s'appuie sur l'**algorithme de Bellman-Ford**, permettant de trouver le chemin le plus court entre deux sommets d'un graphe.

. . . /

Protocole OSPF (« Open Shortest Path First") : protocole de mise à jour des tables de routages où les métriques sont comptées en somme de coûts de liaisons. Un coût C se calcule par la formule $C = 10^8/D$, où D est le débit de la liaison (« bande passante ») en bits/s.
Le protocole OSPF s'appuie sur l'**algorithme de Dijkstra**, permettant de trouver le chemin le plus court entre deux sommets d'un graphe. L'algorithme de Dijkstra se distingue de celui de Bellman-Ford par le fait qu'il s'applique à des graphes non orientés, dont les arcs ont des poids nécessairement positifs.
NB : on utilise aussi cet algorithme pour déterminer le chemin routier le plus rapide, ou le plus économique, entre deux points géographiques.

Chiffrement symétrique : sécurisation des communications par « clé partagée » : la clé, connue de chaque interlocuteur, est utilisée pour coder et décoder.

Chiffrement asymétrique : sécurisation des communications par une clé publique et une clé privée : la clé publique, connue de tous les interlocuteurs, permet de coder les messages. Seule la clé privée, connue d'un seul participant, permet de décoder les messages dans un temps raisonnable.

Divers

Rappel : internet est un réseau de réseaux.

Comparaison des protocoles RIP et OSPF

	RIP	OSPF
Avantages	simplicité	pas de limitation de sauts mise à jour seulement si modification réseau
Inconvénients	limité à 15 sauts mises à jour périodiques fréquentes	

Le RIP reste avantageux pour les petits réseaux, mais il est progressivement remplacé par le protocole OSPF.

Buts du chiffrement des communications :

- l'authentification de l'interlocuteur (par exemple grâce à un certificat en chiffrage asymétrique)
- la confidentialité
- l'intégrité des données (non modifiables par une tierce personne)
- la gestion des droits d'accès ou de modifications

Le chiffrement asymétrique est plus sûr, mais aussi plus complexe et plus long à opérer que le chiffrement symétrique.

Etablissement d'une communication HTTPS : cf manuel ou site pixees.

Pour approfondir:
http://www.gatoux.com/index.php/sommaire-routage-ip/ : cours sur réseaux, routage : très clair
https://qkzk.xyz/docs/nsi/cours_terminale/architecture/routage/cours/ : bon résumé cours routage