~$ le_réseau

Apprentissage et compréhension des réseaux informatiques

Ilian Bonsens
LA PLATEFORME

Table des matières

Job 2

- Qu'est-ce qu'un réseau ?

Un réseau est un groupe d'appareils interconnectés qui peuvent échanger entre eux des ressources et des données. Ils sont régis par ce que l'on appelle des protocoles de communication, qui sont des ensembles de règles. Ils peuvent être connectés physiquement mais aussi en réseau sans-fil.

- À quoi sert un réseau informatique ?

Un réseau informatique sert principalement à échanger des données entre différents appareils. Ces données sont échangées sous forme de paquets de bits ; les bits pouvant prendre deux valeurs (0 ou 1) sont réunis en groupes de 8 que l'on appelle alors un octet (qui peuvent eux-mêmes êtres réunis en plus grand groupes).

- Quel matériel avons-nous besoin pour construire un réseau ? Détaillez les fonctions de chaque pièce.

Pour construire un réseau, il y a trois types de composants : les périphériques finaux (qui envoient et reçoivent les données, les périphériques intermédiaires (qui font transiter les données) et les supports de réseau (qui connectent le tout). Prenons l'exemple d'un réseau composé de deux postes de travail, d'une imprimante, d'un commutateur et d'un routeur. Les trois premiers appareils sont les périphériques finaux, qui vont envoyer et recevoir les données. Le commutateur et le routeur sont les intermédiaires. Les câbles seront eux les supports de ce réseau. Le commutateur est connecté physiquement aux 3 appareils précédents et leur permet de communiquer entre eux ; en plus de centraliser la connexion des trois appareils au routeur qui va leur permettre d'accéder à internet. Pour connecter tous ces appareils entre eux, on utilise des câbles droits Ethernet.

Job 3

- Quels câbles avez-vous choisis pour relier les deux ordinateurs ?

Pour relier les deux ordinateurs, j'ai choisi un câble croisé Ethernet car il permet le transfert des données dans les deux sens, transmission et réception. C'est ce type de câble qu'il faut généralement utiliser pour relier deux appareils du même type.

Job 4

- Qu'est-ce qu'une adresse IP ?

L'adresse IP est l'adresse qui permet d'identifier un équipement au sein d'un réseau. Elle se base sur le protocole Internet, duquel elle tire son abréviation (Internet Protocol).

Il existe deux types d'adresse : les IPv4 et les IPv6.

Le premier type, l'IPv4, est le plus utilisé actuellement. L'adresse est composée de 32 bits convertis en nombres, ce qui nous donne des adresses telles que 000.000.000.000. Néanmoins ce type d'adresse a un gros désavantage, il a une limite fixe de 4,3 milliards d'adresses possibles.

D'où la mise au point du second type d'adresse, l'IPv6. Ces dernières sont composées cette fois de 128 bits, ce qui augmenter le nombre d'adresses possibles à près de 340 sextillions (37 zéros), on a donc un nombre d'adresses de ce type quasi illimité.

- À quoi sert un IP ?

Les adresses IP sont indispensables car elles permettent une identification claire de chaque appareil d'un réseau. C'est ça qui permet les échanges de données entre appareils expéditeurs et destinataires. Lors d'un transfert de données, le routeur s'appuie l'en-tête des IP, qui correspond à la partie réseau de l'adresse. Si les en-têtes des deux adresses correspondent, les données sont envoyées.

- Qu'est-ce qu'une adresse MAC ?

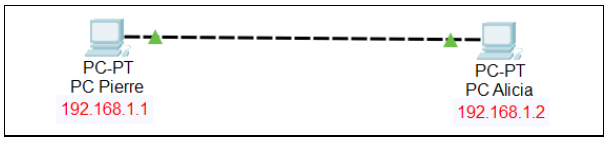
L'adresse MAC (Media Access Control) est une adresse physique unique qui permet d'identifier chaque équipement d'un réseau. Elle est constituée de douze caractères en hexadécimal (des chiffres de 0 à 9 et des lettres de A à F).

- Qu'est-ce qu'une IP publique et privée ?

Une adresse IP publique est l'adresse IP qui va être utilisée pour accéder à internet. Elle doit unique à l'échelle planétaire pour que l'appareil en question soit tout de même identifiable parmi tous les appareils connectés à Internet. Une adresse IP privée quant à elle sera utilisée dans un réseau local. Dans le cadre de ce dernier, les adresses IP doivent être toutes différentes mais seulement au sein du réseau ; elles ne communiquent pas avec les adresses extérieures il n'est donc pas important qu'elles aient la même que d'autres équipements.

- Quelle est l'adresse de ce réseau ?

Ici notre adresse réseau est la suivante : 192.168.10.0 ; en effet pour trouver une adresse réseau il suffit de remplacer tous les bits de la partie hôte par des 0, ce qui donne forcément un 0 pour la partie hôte de l'adresse réseau.



Job 5

- Quelle ligne de commande avez-vous utilisée pour vérifier l'ip des machines ?

Il faut utiliser la commande `ipconfig` dans le terminal de commande des deux PC dans Cisco Packet Tracer. Cela nous montre bien l'adresse IP et le masque de sous-réseau rentrés précédemment.

Job 6

- Quelle est la commande permettant de Ping entre des PC ?

Pour ping entre des PC, il faut utiliser la commande `ping [adresse ip]`. S'ils sont bien connectés sur le même réseau, les paquets devraient correctement s'envoyer et revenir. Voici ce que cela donne dans notre configuration :

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=29ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 29ms, Average = 7ms

C:\>
```

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=13ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>
```

Job 7

- Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ? Expliquez pourquoi.

Après l'avoir éteint, il apparait que lorsqu'on essaye de le ping, le PC de Pierre ne reçoit plus les paquets. C'est normal car une fois hors tension, son adresse IP n'est plus visible sur le réseau, ce qui a pour résultat l'échec de l'envoie des paquets d'une adresse IP à l'autre.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Job 8

- Quelle est la différence entre un hub et un switch ?

Que ce soit un switch ou un hub, ils servent tous les deux à connecter les appareils entre eux et à les faire communiquer. Cependant, en utilisant un hub, on ne peut pas choisir à quel appareil sera envoyer les données que l'on veut envoyer. Le hub ne faisant pas la différence entre les appareils, ils recevront tous les données partagées par l'un d'entre eux. Un switch permet lui de faire la distinction et donc d'envoyer des paquets à un ou des appareils en particulier.

- Comment fonctionne un hub et quels sont ses avantages et ses inconvénients ?

Le hub (concentrateur en français) est un périphérique réseau qui sert à relier plusieurs appareils entre eux, à relayer des données et à centraliser le trafic du réseau. Les hubs sont de nos jours assez peu utilisés, ayant été remplacés par leurs successeurs, les switchs. En effet, lorsqu'il reçoit des données, il va les transférer à tous les ports connectés sans faire de distinction, même si cela ne leur était pas destiné. De plus, un hub ne peut gérer qu'un transfert de données à la fois ; tous les ports étant mobilisés pendant l'opération, les autres transferts sont mis en fil d'attente et seront traités les uns après les autres. Cela peut représenter une certaine perte de temps si l'on a de nombreuses opérations à traiter simultanément. Enfin, comme ils fonctionnent directement sur le matériel (niveau 1 modèle OSI), ils sont plus vulnérables aux failles de sécurité. Néanmoins, les hubs ont toujours un principal avantage : ils stockent l'ensemble des données du réseau dans chacun des pots ce qui peut s'avérer pratique pour faire une analyse du réseau. Il peut aussi être possible de diffuser du contenu multimédia avec une synchronisation parfaite sur plusieurs appareils.

- Quels sont les avantages et inconvénients d'un switch ?

Le switch est un périphérique qui fonctionne sur le même principe que le hub, en corrigeant ses principaux défauts. En effet, il peut bien traiter l'envoi et la réception de paquets en même temps en plus de pouvoir faire la différence entre ses ports ce qui permet d'envoyer des données à un terminal en particulier.

Sa bande passante n'est plus limitée comme celle du hub (qui était entre 10 Mb/s et 100 Mb/s). Enfin, il fonctionne sur la couche 2 du modèle OSI ce qui le rend plus sécurisé.

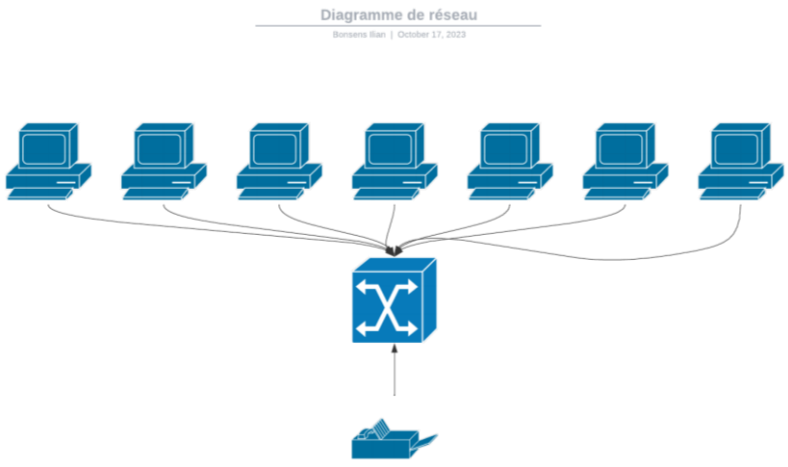
- Comment un switch gère-t-il le trafic réseau ?

Pour savoir à quel port, et donc à quel terminal, il faut envoyer les données qu'il a précédemment reçues, le switch utilise les adresses MAC. Lorsque les différents terminaux sont en fonctionnement, le switch lit les adresses MAC d'origine du trafic pour savoir quel port est relié à quelle machine. C'est ça qui permet au switch d'envoyer des données provenant d'un port précis vers un autre port cible.

Job 9

- Identifiez au moins trois avantages importants d'avoir un schéma.

- Un schéma offre une vision claire et facile à comprendre de notre réseau, sa structure, les composants qui y sont utilisés.
- Permet de le modifier pour visualiser les changements que l'on veut effectuer dans le réseau ; pour éviter de mal faire les choses mieux vaut s'en faire une idée claire avant
- Au niveau de la sécurité, le schéma nous permet de repérer plus facilement les failles potentielles et les moyens d'y remédier (lorsque ce sont des failles matérielles).



Job 10

- Quelle est la différence entre une adresse IP statique et une adresse IP attribuée par DHCP ?

Une adresse IP statique est, comme son nom l'indique, une adresse IP qui ne changera jamais. Elle doit être configurée manuellement, ainsi que le masque de sous-réseau, la passerelle et le serveur DNS. Dans un réseau, chaque IP statique doit être unique sans qu'il y ait de redondance. Généralement, ce sont les serveurs que l'on veut pouvoir retrouver n'importe quand qui disposent d'une IP statique ; comme ceux qui hébergent des sites webs ou des services d'email et de messagerie. A l'opposé, il existe les IP dynamiques attribuées par un serveur DHCP. Ce dernier attribut automatiquement une adresse IP disponible (ainsi que le reste de la configuration réseau) à chaque appareil du réseau.

Cela un représente un grand avantage lorsque le nombre d'adresses IP à attribuer devient très élevé. De plus, l'attribution d'adresses IP par DHCP à tendance à revenir moins cher qu'une attribution manuelle, car les FAI facturent des frais supplémentaires pour obtenir des IP statiques.

Job 11

Voici notre plan d'adressage final, incluant bien nos 16 sous-réseaux. On retrouve aussi les adresses IP réseau, les plages d'adresses disponibles et les adresses de diffusion.

	Nombre d'hôtes	Masque de sous-réseau	IP Gateway	IP Utilisables	IP Broadcast
Sous-réseau 1	12	255.255.255.240 /28	10.0.0.0	10.0.0.1 - 10.0.0.14	10.0.0.15
Sous-réseau 2	5 * 30	255.255.255.224 /27	10.0.0.16	10.0.0.17 - 10.0.0.46	10.0.0.47
			10.0.0.48	10.0.0.49 - 10.0.0.78	10.0.0.79
			10.0.0.80	10.0.0.81 - 10.0.0.110	10.0.0.111
			10.0.0.112	10.0.0.113 - 10.0.0.142	10.0.0.143
			10.0.0.144	10.0.0.145 - 10.0.0.174	10.0.0.175
Sous-réseau 3	5 * 120	255.255.255.128 /25	10.0.0.176	10.0.0.177 - 10.0.1.46	10.0.1.47
			10.0.1.48	10.0.1.49 - 10.0.1.174	1.0.1.175
			10.0.1.176	10.0.1.177 - 10.0.2.46	10.0.2.47
			10.0.2.48	10.0.2.49 - 10.0.2.174	10.0.2.175
			10.0.2.176	10.0.2.177 - 10.0.3.46	10.0.3.47
Sous-réseau 4	5 * 160	255.255.255.0 /24	10.0.3.48	10.0.3.49 - 10.0.4.46	10.0.4.47
			10.0.4.48	10.0.4.49 - 10.0.5.46	10.0.5.47
			10.0.5.48	10.0.5.49 - 10.0.6.46	10.0.6.47
			10.0.6.48	10.0.6.49 - 10.0.7.46	10.0.7.47
			10.0.7.48	10.0.7.49 - 10.0.8.46	10.0.8.47

- Pourquoi a-t-on choisi une adresse 10.0.0.0 de classe A ?

On a choisi cette adresse IP de la classe A comme adresse de départ car elle correspond au début de la plage des adresses privées dans la classe A ; qui va jusqu'à 10.255.255.255. Ainsi, dans notre réseau et nos sous-réseaux, il n'y a que des adresses IP privées, ce qui signifie qu'elles ne peuvent pas être connectée à Internet. C'est idéal dans le cadre d'un réseau local car il n'y a pas besoin de faire attention à les différencier des adresses publiques et elles ne seront visibles que par les autres adresses de ce même réseau. De plus, la classe A laissant libre

- Quelle est la différence entre les différents types d'adresses ?

Il existe différents types et différentes classes d'adresses IP. Commençons par les classes, qui sont au nombre de 5 : A, B, C, D et E. Chaque classe d'adresses IP correspond à un cas d'usage. Les classes A, B et C correspondent à l'ensemble des adresses IP publiques et privées ; que nous allons expliquer ensuite. Celles de classe D sont des adresses multicast et enfin celles de la classe E sont réservé par l'IETF (Internet Engineering Task Force), organisation qui élabore les standards d'Internet. Revenons sur les trois premières classes ; au sein de ces dernières, il existe à chaque fois une plage d'adresses dédiées aux adresses IP privées. Ce type d'adresse IP est destiné à des usages locaux car elles ne peuvent pas être connectée à Internet. On peut par exemple les utiliser dans le cadre d'un réseau local d'entreprise ou pour un petit réseau local domestique. Le reste des adresses IP de ces classes qui ne sont pas comprises dans les plages d'adresses IP privées correspondent à l'ensemble des adresses IP publiques utilisables. Etant connectées à Internet, ces adresses publiques doivent être uniques à l'échelle mondiale, on ne peut pas utiliser simultanément deux fois la même adresse IP publique, sinon on ne peut pas identifier clairement l'utilisateur.

Job 12

Le modèle OSI, acronyme d'Open System Interconnection, est une norme informatique qui définit une organisation à respecter pour assurer une bonne communication entre tous les systèmes. Ce modèle, dont la mise au point a débuté dans les années 70 n'a été adopté qu'en 1984. Son but principal était de définir un cadre d'organisation des connexions pour faciliter les créations et améliorations futures. Il comprend 7 couches différentes dans le système, chacune ayant une fonction précise et qui couvre l'ensemble du système jusqu'à l'utilisateur.

	Rôle	Matériels / Protocoles
Niveau 7 : application	Fournit les interfaces pour accéder aux applications du réseau	FTP (P) (unité de mesure = segments)
Niveau 6 : présentation	Chiffre/déchiffre les données transmises ; peut les rendre affichables ou non	SSL/TLS (P), HTML (P) (unité de mesure = données)
Niveau 5 : session	Gère ouvertures et fermetures de sessions entre les applications	PPTP (P) (unité de mesure = segments)
Niveau 4 : transport	Gère les communications de d'un point à un autre ; contrôle le flux de données ; gère les ports	TCP (P), UDP (P) (unité de mesure = segments)
Niveau 3 : réseau	Gère le parcours des données entre réseaux locaux ; gère l'adressage réseau	IPv4 (P), IPv6 (P) (unité de mesure = paquets)
Niveau 2 : liaison	Elle gère les communications entre appareils d'un même réseau local ; gère l'adressage physique.	MAC (P), Ethernet (P), Wi-Fi (P) (unité de mesure = trames)
Niveau 1 : physique	Elle se limite à la transmission des bits entre les différents composants du système	Cable RJ45 (M), fibre optique (M), Ethernet (P), Wi-Fi (P) (unité de mesure = bits)

Job 13

- Quelle est l'architecture de ce réseau ?

Ce réseau est composé d'assez peu de terminaux : il y a 4 PCs, deux serveurs et un switch pour relier le tout. C'est donc bel et bien un réseau local LAN. Il se limite à l'enceinte de l'école et il y est géré localement.

- Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est telle que : 192.168.10.0. Comme nous l'avons expliqué précédemment, il suffit de remplacer les bits de la partie hôte de l'adresse par des 0 ; ce qui nous renvoie une adresse qui se termine par un 0.

- Déterminer le nombre de machines que l'on peut brancher sur ce réseau ?

Nous savons que notre adresse réseau est 192.168.10.0, est de classe C car si l'on converti 192 en binaire on obtient 11000000. Les deux premiers bits sont bien 1 et 1, ce qui correspond aux adresses de classe C. On sait que le masque de sous-réseau est 255.255.255.0. Le 0 qui correspond à la partie hôte est composé de 8 bits, il suffit alors de faire le calcul suivant : 2^8 = 256. D'après ce résultat il y aurait 256 adresses IP disponibles, mais il faut retirer l'adresse réseau et celle de diffusion ; il est donc possible de brancher 254 appareils sur ce réseau.

- Quelle est l'adresse de diffusion de ce réseau ?

Pour trouver l'adresse de diffusion de ce réseau, il faut suivre le même principe que pour l'adresse réseau avec une modification. Cette fois on va remplacer les bits de la partie hôte de l'adresse IP par des 1 ; ce qui va nous donner l'adresse de diffusion suivante : 192.168.10.255.

Job 14

On peut faire les conversions très simplement en ligne, mais il est aussi très simple de les faire manuellement avec le tableau suivant. Prenons par exemple le nombre 187, il faut additionner certains de ces nombres pour l'atteindre ; chaque nombre utilisé donne un 1 et le reste donne 0.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	1	0	1	1

On obtient 10111011 car on a fait 128+32+16+8+2+1 pour arriver à 187.

Ainsi, en appliquant ceci aux adresses IP suivantes on obtient :

- 145.32.59.24 → 10010001 00100000 00111011 00011000
- 200.42.129.16 → 11001000 00101010 10000001 00010000
- 14.82.19.54 → 00001110 01010010 00010011 00110100

Job 15

- Qu'est-ce que le routage ?

On le sait, un réseau informatique peut être composé de nombreux appareils différents, ce qui peut représenter beaucoup de chemins possibles pour les transferts de données. C'est pour cela que l'on utilise le routage, qui est le processus de sélection du meilleur chemin possible dans notre réseau pour transférer des données d'un point A à un point B. Il permet une plus grande efficacité de notre réseau et donc un certain gain de temps. L'appareil en charge de cette tâche sera le routeur de notre réseau.
Il en existe deux types : le routage statique et le routage dynamique. Dans le cas du premier, c'est l'administrateur du réseau qui va déterminer manuellement les chemins possibles. C'est une technique fastidieuse mais qui peut être utile dans les cas où les chemins doivent toujours rester les mêmes. Il existe aussi le routage dynamique, qui est le plus pratique et efficace. Ce sont les routeurs qui vont régulièrement rechercher et mettre à jours leurs tables de routages avec les meilleurs chemins possibles. L'avantage de ce système est son adaptabilité en fonctions des évolutions du réseau.

- Qu'est-ce qu'un gateway ?

Un gateway (passerelle) est comme son nom peut l'indiquer, un dispositif qui va jouer le rôle d'intermédiaire entre deux réseaux informatiques (qui peuvent être différents). Il permet des échanges de données entre des réseaux qui peuvent utiliser des protocoles différents en traduisant d'un protocole à l'autre ou d'un langage à un autre. Ils jouent donc un rôle très important dans la construction de réseaux informatiques complexes.

- Qu'est-ce qu'un VPN ?

Un VPN (Virtual Private Network) est un logiciel qui permet de créer une connexion privée sécurisée entre des appareils, en passant par Internet. La plupart des VPN utilisent aujourd'hui le protocoles IPsec, qui fonctionne sur la couche directement sur la couche réseau de l'appareil ; ce qui les rend très sécurisés. Un VPN va en fait créer un tunnel de données entre la machine sur laquelle il fonctionne et un des serveurs du service de VPN. Cela a pour effet de faire apparaître toute l'activité de la machine comme étant celle du serveur. On utilise généralement un VPN pour des questions de confidentialité et de sécurité. En effet, en utilisant un VPN, notre véritable adresse IP n'est plus visible par les sites et services que l'on va utiliser et notre FAI n'aura pas accès à notre activité pendant que nous utilisons le VPN. De plus, grâce au fonctionnement en tunnel de données, ces dernières sont sécurisées car personne ne peut y accéder, elles sont chiffrées et toute personne ne disposant pas des accès ne pourra pas les consulter.

- Qu'est-ce qu'un DNS ?

Un DNS (Domain Name System) est un type de serveur dont le rôle est de traduire les noms de domaines en adresses IP pour que les navigateurs puissent afficher les contenus web. En effet, chaque sites web ou services disponibles sur Internet disposent de leur propre adresse IP. Mais lorsque nous effectuons nos recherches sur Internet, nous utilisons les noms de domaines au lieu de chercher à joindre directement les adresses IP. Sans ces serveurs DNS, cela ne serait pas possible et il faudrait noter et/ou mémoriser à chaque fois les adresses IP qui nous intéressent.

Une requête d'un utilisateur pour une recherche implique 3 serveurs DNS différents. Au début, le nom de domaine demandé est converti en adresse IP par le serveur DNS résolveur. Ce dernier va ensuite interroger avec l'adresse IP un serveur DNS noms de racines, qui va lui renvoyer dans quel serveur se trouvera finalement le service auquel on souhaite accéder. Enfin, c'est dans le serveur TLD (domaine de premier niveau), qui est le serveur que nous a indiqué le serveur DNS racine, que l'on va finalement trouver l'emplacement du site auquel on va se connecter. Ainsi, pour une seule requête d'un utilisateur, il y a trois serveurs DNS différents qui agissent.