



GUILLAUME BOMBEN



DOCUMENTATION RUNTRACK RÉSEAU

JOB 2

QU'EST-CE QU'UN RÉSEAU ? / À QUOI SERT UN RÉSEAU INFORMATIQUE ?

Un réseau est défini par la mise en relation d'au moins deux systèmes informatiques au moyen d'un câble ou sans fil, par liaison radio.

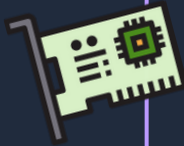
Le réseau le plus basique comporte deux ordinateurs reliés par un câble. Ce genre de réseau n'a pas de hiérarchie : les deux participants sont au même niveau. Chaque ordinateur a accès aux données de l'autre et ils peuvent partager des ressources, comme un disque de stockage, des programmes ou des périphériques .

Les réseaux modernes sont un peu plus complexes en général et comportent bien plus que deux ordinateurs.

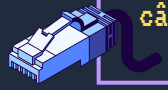
La fonction principale d'un réseau est de fournir aux participants une plateforme pour l'échange de données et l'utilisation commune des ressources.

QUEL MATÉRIEL AVONS-NOUS BESOIN POUR CONSTRUIRE UN RÉSEAU ?

Pour construire un réseau informatique il faut :



Carte réseau	Permet de mettre plusieurs ordinateurs en contact . Il reçoit des données par un port, et envoie ce qu'il reçoit aux autres.
Concentrateur (hub)	Permet de mettre plusieurs ordinateurs en contact . Il reçoit des données par un port, et envoie ce qu'il reçoit aux autres.
Commutateur (switch)	Permet de recevoir des données et de les transmettre a une machine spécifique en l'identifiant grâce a son adresse mac .
Routeur	Permet de faire la liaison entre différent réseau .
Répéteur	Permet de renvoyer des données de manière plus puissante .
câbles Ethernet	Permet de relier tout les composant entre eux.





JOB 3

Cisco nous donne le choix de plusieurs type de câble pour relier les différent appareil d'un réseau ensemble qui sont :

Câble Console	Ce câble est utilisé pour établir une connexion série entre un périphérique réseau, comme un routeur ou un commutateur, et un ordinateur. Il est couramment utilisé pour configurer et dépanner des équipements réseau via une interface en ligne de commande.
Câble droit	Un câble droit est utilisé pour connecter des périphériques de type différent, comme un commutateur à un routeur. Les broches à une extrémité du câble correspondent aux broches à l'autre extrémité, ce qui signifie que les câbles sont identiques des deux côtés.
Câble croisé	Un câble croisé est utilisé pour connecter des périphériques de même type, comme un commutateur à un commutateur ou un routeur à un routeur. Les broches à une extrémité du câble sont croisées par rapport aux broches à l'autre extrémité, ce qui permet de connecter deux dispositifs similaires directement.
Fibre optique	Ce câble est utilisé pour transmettre des données à l'aide de signaux lumineux. Il offre une grande capacité de bande passante et est utilisé pour des connexions longue distance à haute vitesse.
Ligne téléphonique	Ce câble est utilisé pour simuler la connexion téléphonique traditionnelle. Il peut être utilisé pour connecter des téléphones analogiques à des commutateurs.

Câble Coaxial	Ce câble est utilisé pour simuler les connexions par câble, notamment pour la transmission de signaux de télévision et d'Internet par câble.
Câbles DCE et DTE	Ces câbles sont utilisés pour établir des connexions série entre des équipements réseau. DCE (Data Communications Equipment) est généralement un dispositif comme un modem, tandis que DTE (Data Terminal Equipment) est généralement un ordinateur.
Octal	Les câbles octal sont utilisés pour connecter un routeur à plusieurs périphériques, tels que des commutateurs ou des modules d'interface.
IOT câble custom	Ce câble personnalisé peut être utilisé pour représenter divers types de connexions en fonction de vos besoins spécifiques.
USB	Ce câble USB est utilisé pour connecter des périphériques USB, tels que des clés USB ou des adaptateurs réseau, à des ordinateurs ou des équipements réseau.

QUELS CÂBLES AVEZ-VOUS CHOISIS POUR RELIER LES DEUX ORDINATEURS ?

Ici nous voulons relier deux appareils du même type. Pour cela nous utilisons donc un câble croisé qui est le plus adapté dans cette situation.

JOB 4

QU'EST-CE QU'UNE ADRESSE IP ?

Une adresse IP est un numéro d'identification unique attribué de façon permanente ou provisoire à chaque périphérique faisant partie d'un même réseau informatique. Il est très courant que plusieurs appareils possède la même IP si il sont connecter à la même box internet . Une IP est composer de quatre bloc de nombre pouvant aller de 0 à 255 et séparer par un point .

À QUOI SERT UN IP ?

Une adresse IP permet d'identifier un appareil sur un réseau et d'échanger des données entre les appareils. Elle peut aussi permettre d'accéder a des serveurs spécifique ou être utiliser pour accéder à la géolocalisation de l'appareil.

QU'EST-CE QU'UNE ADRESSE MAC ?

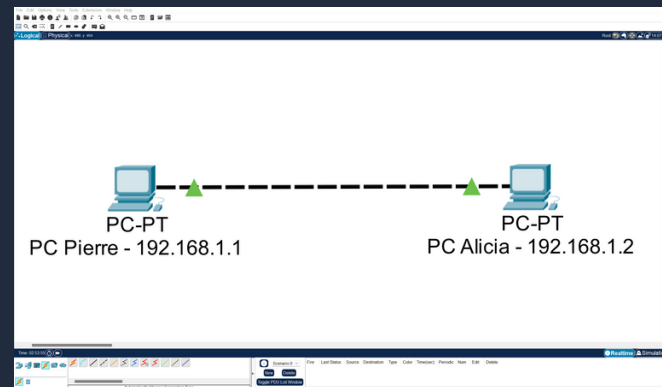
Une adresse MAC est l'identifiant de la machine physique qui est unique pour chaque machine contrairement a l'adresse IP. Une adresse MAC est composer de douze caractères hexadécimal (des chiffres de 0 à 9 ou des lettre de A à F) . Les six premier caractère de l'adresse MAC permette d'identifier le constructeur .

QU'EST-CE QU'UNE IP PUBLIQUE ET PRIVÉE ?

- Les adresses IP privées s'utilisent dans un réseau interne. Ces adresses IP permettent aux appareils connectés au même réseau de communiquer entre eux sans se connecter à Internet. Elle permette renforcent la sécurité au sein d'un réseau spécifique.
- Une adresse IP publique est une adresse IP directement accessible sur Internet. Elle est attribuée par votre fournisseur d'accès Internet. Cette adresse IP permet d'accéder aux site internet ou de recevoir des mails.

QUELLE EST L'ADRESSE DE CE RÉSEAU ?

Le masque du réseau étant 255.255.255.0 nous pouvons en déduire que pour trouver l'adresse du réseau il suffit de prendre les trois premiers blocs de l'adresse IP et de remplacer le quatrième bloc par 0. Ainsi nous obtenons l'IP 192.168.1.0 qui correspond à l'IP du réseau.



JOB 5

Pour vérifier l'IP d'un PC on utilise la commande ipconfig

```
PC Alicia - 192.168.1.2
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . .: FE80::260:70FF:FEBE:C79
IPv6 Address . . . . .: ::
IPv4 Address. . . . .: 192.168.1.2
Subnet Mask . . . . .: 255.255.255.0
Default Gateway . . . . .: 0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . .: ::
IPv6 Address . . . . .: ::
IPv4 Address . . . . .: 0.0.0.0
Subnet Mask . . . . .: 0.0.0.0
Default Gateway . . . . .: 0.0.0.0

C:\>
```

PC ALICIA

```
PC Pierre - 192.168.1.1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . .: FE80::250:FFF:FE11:C33C
IPv6 Address . . . . .: ::
IPv4 Address. . . . .: 192.168.1.1
Subnet Mask . . . . .: 255.255.255.0
Default Gateway . . . . .: 0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . .: ::
IPv6 Address . . . . .: ::
IPv4 Address . . . . .: 0.0.0.0
Subnet Mask . . . . .: 0.0.0.0
Default Gateway . . . . .: 0.0.0.0

C:\>
```

PC PIERRE

JOB 6

Pour ping deux PC entre eux on utilise la commande ping suivie de l'IP de l'appareil cible.

```
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<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
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 = 0ms, Average = 0ms
```

PC PIERRE

```
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<1ms 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 = 0ms, Average = 0ms
```

PC ALICIA

JOB 7

```
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),
```

Le PC de Pierre n'a pas put recevoir les paquets envoyer par Alicia car il faut que les deux PC soit connecter aux réseau pour envoyer et recevoir des données. Ce qui n'est pas possible car le pc de pierre n'est pas allumer et donc pas connecter aux réseau.

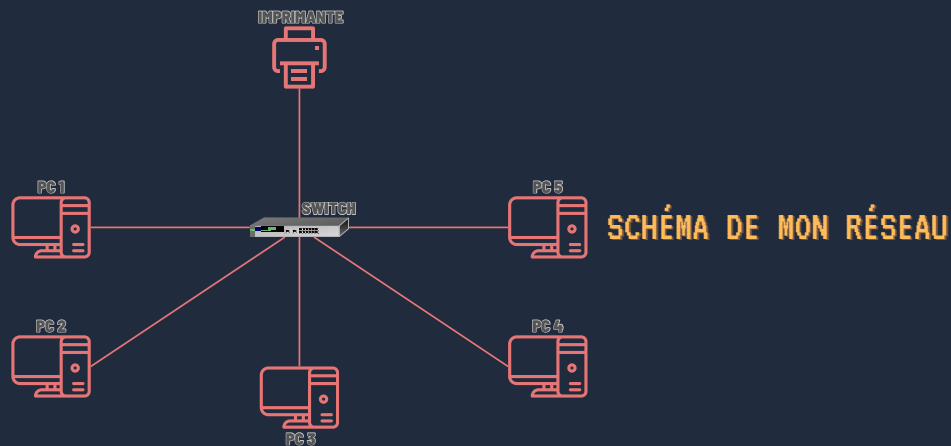
JOB 8

- Un hub renvoi les données qu'il reçoit a tout les appareils avec qui il est connecter. Il n'a aucun moyen de distinguer vers qu'elle appareils il doit envoyer des données. Il doit partager sa bande passante entre tout ces port et génère beaucoup de charge sur le réseau et peut conduire a des temps de réponse plus long.
- Un switch peut distinguer les différents appareils du réseau ainsi lorsque le switch reçoit des données il peut les envoyés à un appareil spécifique. Il envoie la puissance maximal a chacun des ports connecter et permet d'avoir un temps de réponse plutôt stable.

JOB 9

Les avantages à avoir un schéma sont :

Clarté	Permet de simplifier des informations complexes en une forme visuelle facile à comprendre.
Visualisation	Met en évidence les connexions et les interrelations entre les composants, ce qui peut aider à identifier des tendances, des problèmes ou des opportunités.
Problèmes	permettent d'analyser visuellement une situation ou un processus, ce qui peut aider à repérer des



JOB 10

QUELLE EST LA DIFFÉRENCE ENTRE UNE ADRESSE IP STATIQUE ET UNE ADRESSE IP ATTRIBUÉE PAR DHCP ?

- Une adresse IP statique doit être définie manuellement pour chaque appareil et ne changera pas à moins de la changer manuellement. Elle nécessite donc une configuration et une gestion manuelle.
- Une adresse IP attribuée par DHCP est attribuée automatiquement, peuvent changer au fil du temps et sont simple à gérer.

JOB 11

Pour le sous-réseau de 12 hôte :

sous réseau	masque	plage d'adresse IP
10.0.0.0/28	255.255.255.240	10.0.0.0 à 10.0.0.15

Pour les 5 sous-réseau de 30 hôte :

sous réseau	masque	plage d'adresse IP
10.0.0.16/27	255.255.255.224	10.0.0.16 à 10.0.0.47
10.0.0.48/27		10.0.0.48 à 10.0.0.79
10.0.0.80/27		10.0.0.80 à 10.0.0.111
10.0.0.112/27		10.0.0.112 à 10.0.0.143
10.0.0.144/27		10.0.0.144 à 10.0.0.175

Pour les 5 sous-réseau de 120 hôte :

sous réseau	masque	plage d'adresse IP
10.0.0.176/25	255.255.255.128	10.0.0.176 à 10.0.1.42
10.0.1.43/25		10.0.1.43 à 10.0.1.164
10.0.1.165/25		10.0.1.165 à 10.0.2.31
10.0.2.32/25		10.0.2.32 à 10.0.2.153
10.0.2.154/25		10.0.2.154 à 10.0.3.20

Pour les 5 sous-réseau de 160 hôte :

sous réseau	masque	plage d'adresse IP
10.0.3.21/24	255.255.255.0	0.0.3.20 à 10.0.3.181
10.0.3.182/24		10.0.3.182 à 10.0.4.88
10.0.4.89/24		10.0.4.89 à 10.0.4.250
10.0.4.251/24		10.0.4.251 à 10.0.5.157
10.0.5.158/24		10.0.5.158 à 10.0.6.64

POURQUOI A-T-ON CHOISI UNE ADRESSE 10.0.0.0 DE CLASSE A ?

Nous avons choisi une adresse de classe A car elle convient très bien aux réseau de grande entreprise comme ici car elle permet de créer plus de 16 Million d'adresse IP.

QUELLE EST LA DIFFÉRENCE ENTRE LES DIFFÉRENTS TYPES D'ADRESSES ?

- Les adresses de classe A sont généralement utilisées pour de grands réseaux, car elles peuvent prendre en charge un grand nombre d'hôtes (environ 16 millions d'hôtes).
- Les adresses de classe B sont utilisées pour des réseaux de taille moyenne, prenant en charge un nombre modéré d'hôtes (environ 65 000 réseaux et 65 000 hôtes par réseau).
- Les adresses de classe C sont principalement utilisées pour des réseaux de petite à moyenne taille, car elles prennent en charge un nombre limité d'hôtes (environ 254 hôtes par réseau).
- Les adresses de classe D sont réservées pour les adresses multicast, utilisées pour l'acheminement de données à un groupe de destinataires.
- Les adresses de classe E sont réservées à des fins expérimentales et ne sont pas utilisées couramment.

JOB 12

Couche OSI	Description des rôles
Couche 7 : Application	Cette couche est responsable des interfaces entre l'application utilisateur et le réseau. Elle gère la communication, la présentation des données et les services d'application, tels que le courrier électronique, le transfert de fichiers, et les navigateurs web. (HTML , FTP , PPTP , SSL/TLS)
Couche 6 : Présentation	La couche de présentation est responsable de la conversion, de la traduction et du chiffrement des données pour s'assurer qu'elles sont correctement interprétées par les applications. Elle gère également la compression et le formatage des données. (SSL/TLS)
Couche 5 : Session	La couche de session établit, gère et termine les sessions de communication entre les applications. Elle assure le contrôle du dialogue et la synchronisation des données, permettant ainsi une communication cohérente. (PPTP)
Couche 4 : Transport	Cette couche assure le transport fiable des données entre les appareils sur un réseau. Elle gère le contrôle de flux, la segmentation, la réassemblage des données, la détection d'erreurs, et la correction. (TCP , UDP)
Couche 3 : Réseau	La couche réseau est responsable du routage des données à travers le réseau. Elle détermine le chemin optimal pour les paquets de données, en utilisant des adresses IP, afin de les acheminer de l'émetteur au destinataire. Les routeurs opèrent principalement à cette couche. (IPv4 , IPv6 , Router)

Couche 2 : Liaison de données	<p>Cette couche gère la communication entre des dispositifs directement connectés. Elle organise les données en trames, les adresses matérielles (MAC) pour la livraison, et gère la détection d'erreurs sur le réseau local.</p> <p>Les commutateurs réseau fonctionnent à ce niveau.</p> <p>(MAC , Ethernet)</p>
Couche 1 : Physique	<p>La couche physique est responsable de la transmission des bits bruts sur le support de communication physique, qu'il s'agisse de câbles, de fibres optiques ou d'ondes radio. Elle définit les spécifications électriques, mécaniques et fonctionnelles du matériel.</p> <p>(Fibre optique , Câble RJ45 , WIFI)</p>

JOB 13

QUELLE EST L'ARCHITECTURE DE CE RÉSEAU ?

Il existe plusieurs type d'architecture réseau qui sont :

Architecture en étoile	Tous les dispositifs sont connectés à un concentrateur central (comme un commutateur ou un routeur). Cela permet une gestion centralisée et facilite l'ajout ou le retrait de dispositifs.
Architecture en bus	Les dispositifs sont connectés à une ligne unique, qui agit comme un bus de données. Les données sont transmises le long du bus, et chaque dispositif peut lire les données qui le concernent. Les inconvénients incluent la vulnérabilité aux collisions de données et la limitation de la longueur du bus.
Architecture en anneau	Les dispositifs sont connectés dans un cercle, de sorte que les données circulent en boucle. Chaque dispositif reçoit les données et les transmet au dispositif suivant. Les réseaux en anneau sont moins courants de nos jours.
Architecture en maillage	Chaque dispositif est connecté à plusieurs autres dispositifs, créant un réseau interconnecté. Les réseaux maillés offrent une redondance et une robustesse élevées, mais ils nécessitent plus de câblage.

Architecture en cascade	Ce type d'architecture est couramment utilisé dans les réseaux d'entreprise. Il consiste en une hiérarchie de dispositifs, avec des dispositifs de niveau supérieur (comme des routeurs principaux) connectés à des dispositifs de niveau inférieur (comme des commutateurs).
Architecture sans fil	Les dispositifs communiquent via des ondes radio plutôt que par des connexions filaires. Cela inclut les réseaux Wi-Fi et les réseaux cellulaires.

Ici nous avons une architecture en étoile.

INDIQUER QUELLE EST L'ADRESSE IP DU RÉSEAU ?

Pour déterminer l'adresse IP du réseau il faut regarder le masque du sous-réseau qui ici est 255.255.255.0 ,ce qui signifie que l'IP du réseau correspond au trois premier bloc de l'adresse IP. L'adresse IP du réseau est donc 192.168.10.0

DÉTERMINER LE NOMBRE DE MACHINES QUE L'ON PEUT BRANCHER SUR CE RÉSEAU?

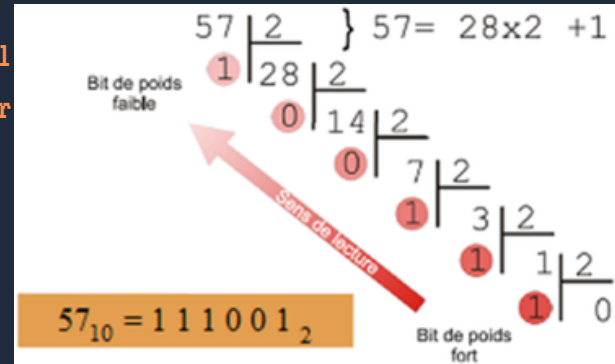
Avec un masque de sous-réseau de 255.255.255.0, nous disposez de 8 bits pour les adresses IP des machines (car les 24 premiers bits sont réservés pour le réseau). Cela signifie qu'il y a $2^8 = 256$ combinaisons possibles pour les adresses IP des machines. Cependant, 2 adresses IP sont réservées (l'adresse de diffusion et l'adresse de réseau), vous avez donc $256 - 2 = 254$ adresses IP utilisables pour les machines.

QUELLE EST L'ADRESSE DE DIFFUSION DE CE RÉSEAU ?

L'adresse de diffusion d'un réseau est généralement la dernière adresse IP du réseau. Dans ce cas, l'adresse de diffusion est donc 192.168.10.255

JOB 14

Pour convertir un nombre décimal en nombre binaire il suffit de faire la division euclidienne du nombre par 2 jusqu'à que le résultat soit égale à 0 .En lisant les restes dans le sens inverse des divisions on obtient le nombre binaire correspondant au nombre de départ. Ainsi on obtient :



- 145.32.59.24 => 10010001.00100000.00111011.00011000
- 200.42.129.16 => 11001000.00101010.10000001.00010000
- 14.82.19.54 => 00001110.01010010.00010011.00110110

JOB 15

QU'EST-CE QUE LE ROUTAGE ?

Le routage est le processus de transmission de données entre différents réseaux informatiques ou sous-réseaux. Il s'agit de déterminer le meilleur chemin pour faire passer des paquets de données d'une source à une destination. Le routage permet aussi de relier efficacement divers réseaux et de faire en sorte que les données atteignent leur destination de manière fiable et efficace.

QU'EST-CE QU'UN GATEWAY ?

Un Gateway est un dispositif qui relie deux réseaux informatiques , permettant ainsi la communication entre eux. Les Gateway sont souvent utilisées pour relier des réseaux avec des protocoles de communication différents, comme un réseau local (LAN) et un réseau étendu (WAN). Elles traduisent les données d'un réseau pour qu'elles soient compatibles avec le réseau auquel elles sont destinées, facilitant ainsi la communication entre ces réseaux distincts.

QU'EST-CE QU'UN VPN ?

Un VPN est un réseau privé virtuel qui permet d'avoir une connexion sécurisée sur un réseau public, . Il est utilisé pour sécuriser et protéger les communications en chiffrant les données qui circulent entre un appareil ou un utilisateur et un serveur distant. Les VPN sont couramment utilisés pour garantir la confidentialité et la sécurité des données, masquer l'emplacement géographique de l'utilisateur, contourner la censure en ligne et permettre un accès sécurisé aux ressources réseau, notamment pour les entreprises.

QU'EST-CE QU'UN DNS ?

Le DNS est un service essentiel sur Internet qui permet de traduire les noms de domaine en adresses IP, qui sont les véritables identifiants numériques des serveurs et des dispositifs connectés. Les serveurs DNS servent de répertoires qui permettent de localiser les ressources en ligne en fonction des noms de domaine. Lorsque vous saisissez une URL dans votre navigateur, un serveur DNS est utilisé pour traduire ce nom en une adresse IP afin de trouver la ressource demandée sur le réseau.