le_reseau

JOB 2

Qu’est-ce qu’un réseau ?

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.

À quoi sert un réseau informatique ?

Le but d’un réseau informatique est de fournir à tous les utilisateurs une facilité d'échange de données et l'utilisation commune des ressources. Il permet le partage des données, des documents, des applications, des imprimantes.

Quel matériel avons-nous besoin pour construire un réseau ?

Un réseau se compose de trois éléments essentiels :

Endpoints (Périphériques Finaux) :

Ce sont les dispositifs tels que les ordinateurs, les smartphones, les imprimantes et les serveurs, qui sont les points de départ et d'arrivée des données dans le réseau.

Périphériques intermédiaires :

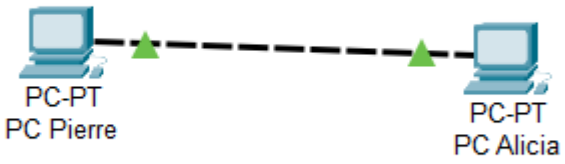
Ces équipements facilitent la communication entre les endpoints. On y trouve les commutateurs (switches) qui assurent la connectivité locale, les routeurs (routers) qui acheminent les données entre différents réseaux, et les pare-feu (firewalls) qui sécurisent le trafic.

Support de transmission :

Ce sont les canaux physiques ou sans fil par lesquels les données circulent. Les câbles, tels que les câbles Ethernet, RJ45 ou coaxiaux, ainsi que les liaisons en fibre optique, véhiculent des signaux électriques. De plus, les technologies sans fil, comme le Wi-Fi et le Bluetooth, transmettent des données sous forme d'ondes. En outre, des méthodes moins courantes, comme l'infrarouge (utilisé dans les télécommandes) ou le LiFi (transmission de données par la lumière), peuvent également être employées pour la communication.

Ces éléments interagissent pour permettre la connectivité, la transmission de données et la communication au sein du réseau.

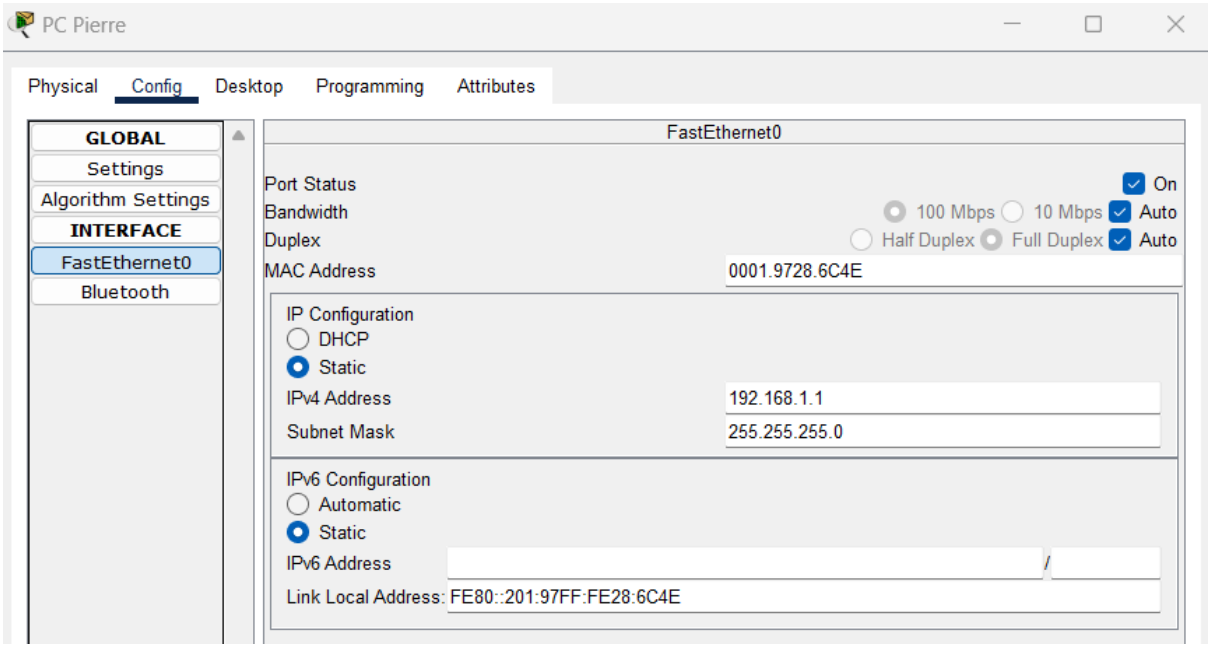
JOB 3

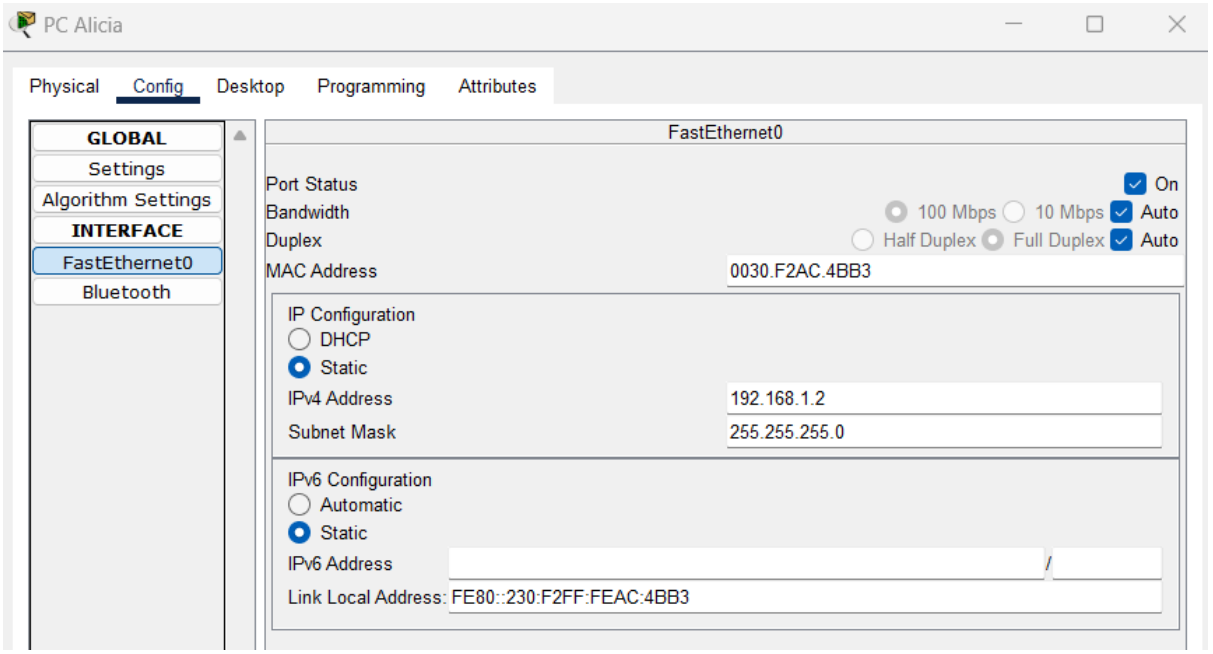


Le câble croisé sera choisi pour relier les deux ordinateurs, c'est un câble ethernet pour connecter les équipements opérant dans les mêmes couches du modèle OSI. Il permet au deux ordinateurs de s'envoyer et recevoir des données.

Cependant, il est tout à fait possible d'utiliser un câble droit (câble ethernet) pour connecter les équipements opérant dans les différentes couches du modèle OSI.

JOB 4





Qu’est-ce qu’une adresse IP ?

Une adresse IP (Internet Protocol) est un numéro d'identification unique attribué de façon permanente ou provisoire à chaque périphérique faisant partie d'un même réseau informatique utilisant l'Internet Protocol.

À quoi sert un IP ?

L’Internet Protocol, soit “protocole internet” en français. C’est une sorte de code qui permet l’identification de chaque terminal connecté au réseau internet. On retrouve différents matériels informatiques doté d’une adresse IP :
Routeur, ordinateur, smartphone, objets connectés, système embarqué, modem (ADSL, wifi, fibre ou câble), imprimante réseau, etc.) connecté à un réseau utilisant l’Internet.

Qu’est-ce qu'une adresse MAC ?

Une adresse MAC est un identifiant unique attribué à une interface réseau d'un périphérique. Elle est associée à la carte réseau (matérielle ou virtuelle) présente dans l'appareil, telle qu'un ordinateur, un smartphone, une tablette, ou tout autre dispositif connecté à un réseau.

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

Une adresse IP publique est une adresse IP directement accessible sur Internet. Elle est attribuée au routeur réseau par le fournisseur d’accès Internet (FAI). L’appareil personnel

possède également une adresse IP privée qui n’est pas divulguée lorsqu’on veut se connecter à Internet via l’adresse IP publique d’un routeur.

L’adresse IP privée est l’adresse que le routeur réseau attribue à l'appareil. Chaque appareil au sein d’un même réseau se voit attribuer une adresse IP privée unique (que l’on désigne parfois sous le nom d’adresse réseau privée). C’est de cette façon que les appareils d’un même réseau communiquent entre eux.

La principale différence entre les adresses IP publiques et privées se situe au niveau de leur portée et du réseau auquel elles sont connectées. Une adresse IP publique vous identifie auprès du réseau Internet, de telle sorte que toutes les informations que vous recherchez puissent vous retrouver. Une adresse IP privée est utilisée à l’intérieur d’un réseau privé pour établir une connexion sécurisée à d’autres appareils du réseau.

Quelle est l’adresse de ce réseau ?

Pour déterminer l’adresse de ce réseau, nous disposons d’éléments qui vont nous permettre de la trouver.

Adresse IP : 192.168.1.1
Masque de sous-réseau : 255.255.255.0

Avec une opération simple nous pouvons trouver le résultat.

Convertit l’adresse IP et le masque de sous-réseau en binaire.

11000000.10101000.00000000.00000001

11111111.11111111.11111111.00000000

Ensuite nous appliquons un raisonnement logique, 1+1 = 1; 1+0=0; 0+1=0; 0+0=0
Pour chaque 1=1 nous obtenons 1 et pour chaque 0=1 nous obtenons 0.

Nous obtenons une adresse en binaire :

11000000.10101000.00000000.00000000

Nous la convertissons en IP cela donne :

192.168.1.0

Nous obtenons notre adresse de réseau 192.168.1.0.

JOB 5

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:97FF:FE28:6C4E
   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
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::230:F2FF:FEAC:4BB3
   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
```

On utilise la commande “ipconfig” dans le terminal pour afficher les informations des machines.

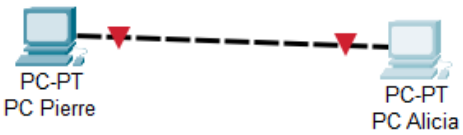
JOB 6

```
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
```

```
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
```

La commande utilisée pour vérifier le ping entre deux machines c'est "ping" suivi de l'adresse ip de destination.

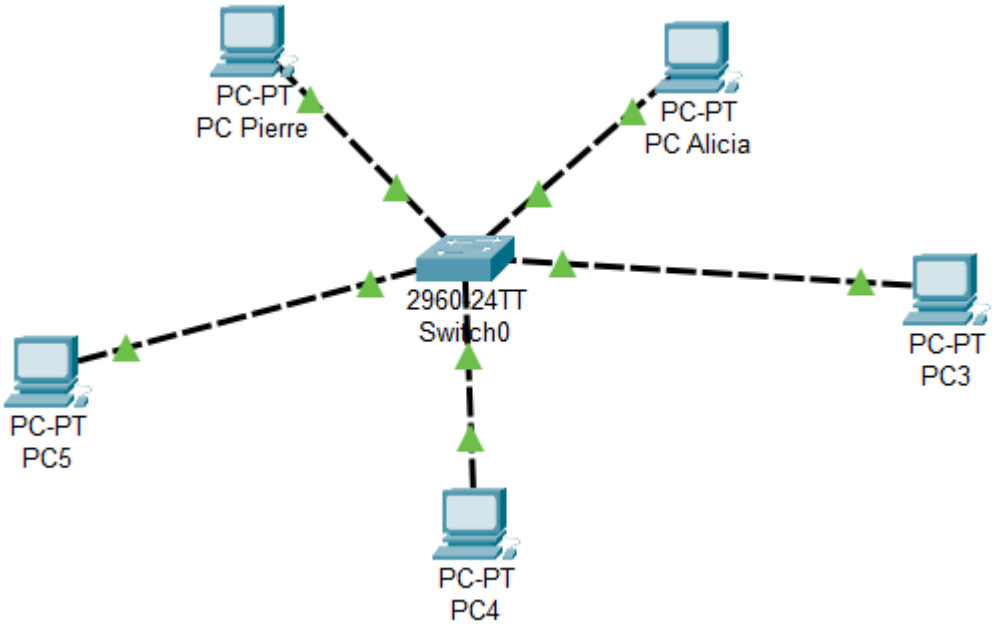
JOB7




```
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 reçu les paquets envoyés par Alicia. Le pc Pierre étant éteint les informations n'ont pas pu être transmises par le pc Alicia vers pc Pierre.

JOB 8



Quelle est la différence entre un hub et un switch ?

La différence entre le hub et le switch informatique est la façon dont les trames sont livrées. Le hub n'a aucun moyen de distinguer vers quel port une trame doit être envoyée, tandis que le switch effectue un tri des trames afin de les orienter vers le bon port, donc vers le bon équipement.

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

Le hub répète simplement les signaux entrant à tous les ports sans tenir compte de l'adresse MAC. Tous les périphériques connectés à un hub reçoivent toutes les données, ce qui peut entraîner un trafic inutile et une saturation du réseau. Les hubs sont moins chers que les switches mais moins efficaces pour gérer le trafic.

Quels sont les avantages et inconvénients d’un switch ?

Un switch est un appareil essentiel doté de multiples ports Ethernet, allant de quelques-uns à plusieurs centaines. Son rôle principal est de relier efficacement divers composants d'un réseau informatique.

Il offre la capacité de créer des connexions internes au sein d'un même réseau, permettant ainsi de recevoir des informations et de les diriger vers leur destination en utilisant le port approprié. Les switches apportent de nombreux avantages à la gestion de votre infrastructure informatique.

En premier lieu, ils renforcent la sécurité du réseau, assurant ainsi la protection des données en transit. De plus, les switches sont conçus pour connecter un nombre plus important de postes de travail au sein du réseau Ethernet. Leur principal atout réside dans leur capacité à acheminer les données de manière intelligente au sein de l'entreprise, en contrôlant et sécurisant le réseau pour prévenir les intrusions.

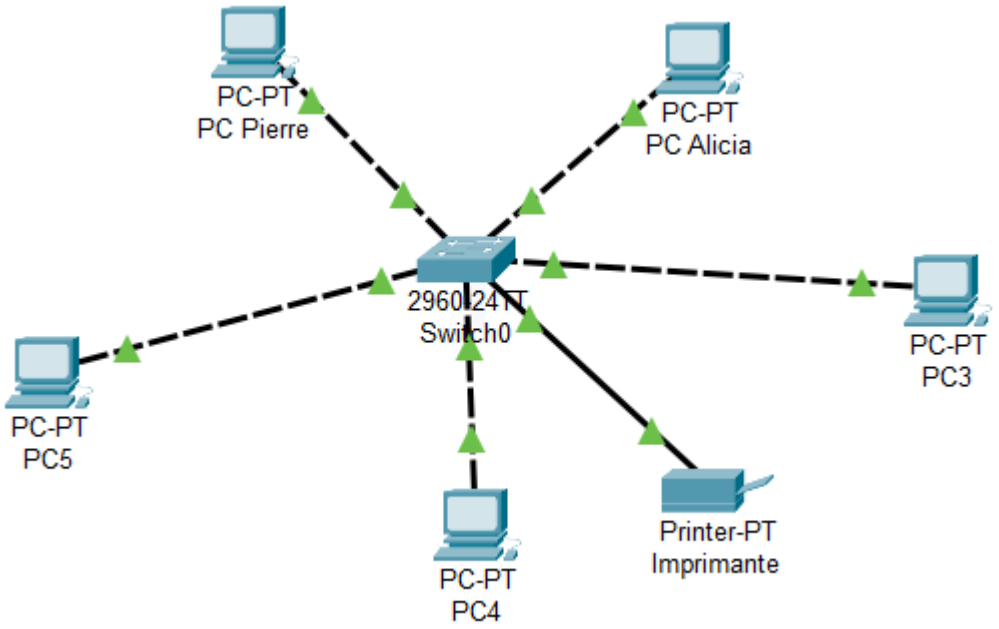
Une fois configurés par un professionnel de l'informatique, les switches distribuent les données uniquement aux utilisateurs autorisés, en fonction des spécificités des différents services au sein de l'entreprise (comme les départements finance, direction, marketing, etc.) et des restrictions définies. Cette approche améliore considérablement la confidentialité des données de l'entreprise.

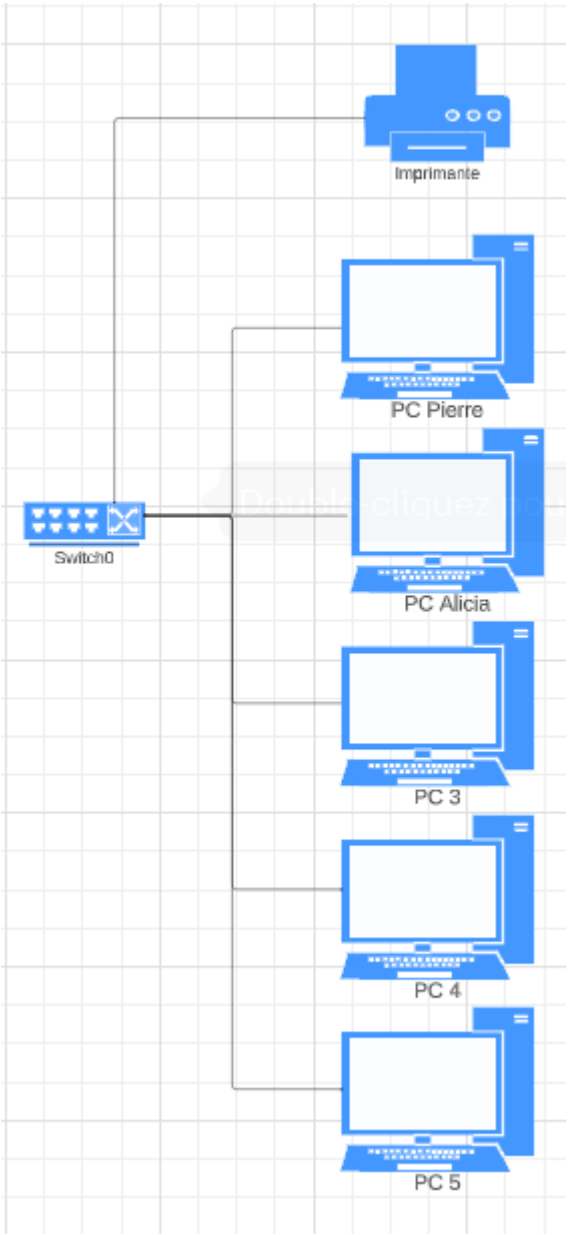
Comment un switch gère-t-il le trafic réseau ?

Les switches sont également utilisés pour relier plusieurs segments d'un réseau informatique. Ils analysent les trames entrantes sur les ports, effectuent une filtration des données et les acheminent vers leur destination correcte. Ils jouent ainsi un rôle essentiel en termes de filtrage et de connectivité.

Cependant, il est important de noter que l'acquisition d'un switch peut représenter un investissement financier, et son utilisation peut être complexe pour les individus moins familiers avec les équipements informatiques.

JOB 9


PC-PT
PC Pierre
PC-PT
PC Alicia
2960-24TT
Switch0
PC-PT
PC3
PC-PT
PC5
PC-PT
PC4
Printer-PT
Imprimante



Les raisons pour lesquelles on utilise un schéma de réseau :

- Peut servir de documentation pour la communication externe, l'intégration, etc.
- Permet d'effectuer le suivi de chaque élément d'un projet et de partager rapidement son état avec les autres.
- En cas de panne ou de problème sur le réseau, disposer d'un schéma de réseau à jour permet de localiser rapidement la source du problème. Les administrateurs peuvent suivre le chemin des données, identifier les points de défaillance potentiels et résoudre les problèmes plus rapidement.

La représentation visuelle des données permet d’améliorer la compréhension et la rétention.

JOB 10

Pour permettre l'ajout d'adresses IP plus facilement on doit ajouter et configurer un serveur DHCP. On doit procéder comme suit :

- Configurer tous les équipements en mode DHCP.
- Ajoutez le serveur DHCP, puis cliquez sur son icône.
- Configurer le serveur dans l'onglet "Config" puis ajouter son adresse IPv4 statique dans "FastEthernet0" (image 1).
- Aller dans l'onglet Services, DHCP est activer le service DHCP "On" (image 2).

Image 1

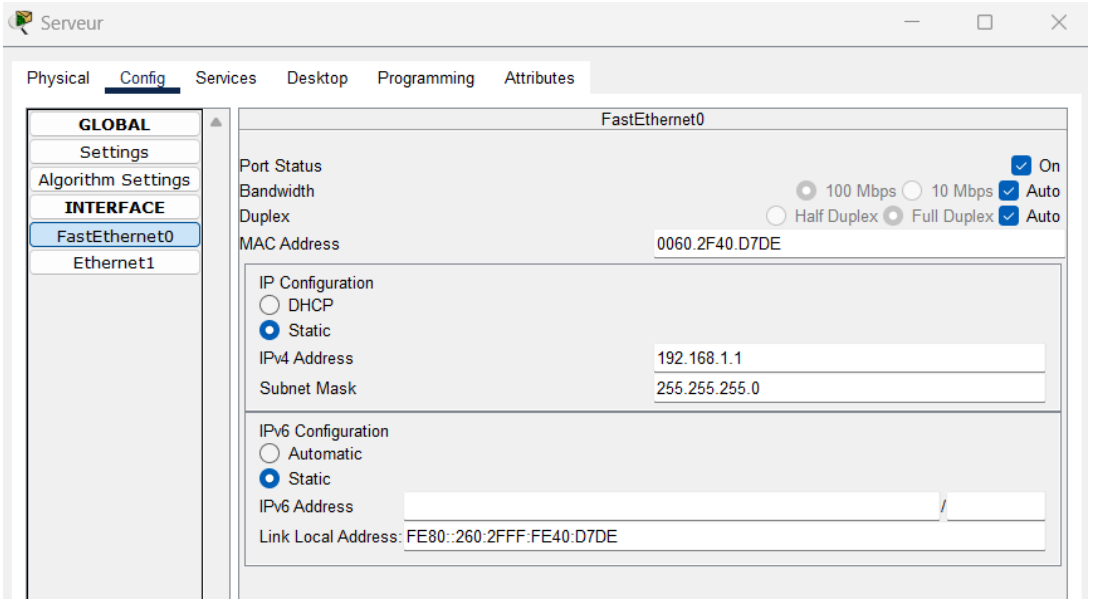
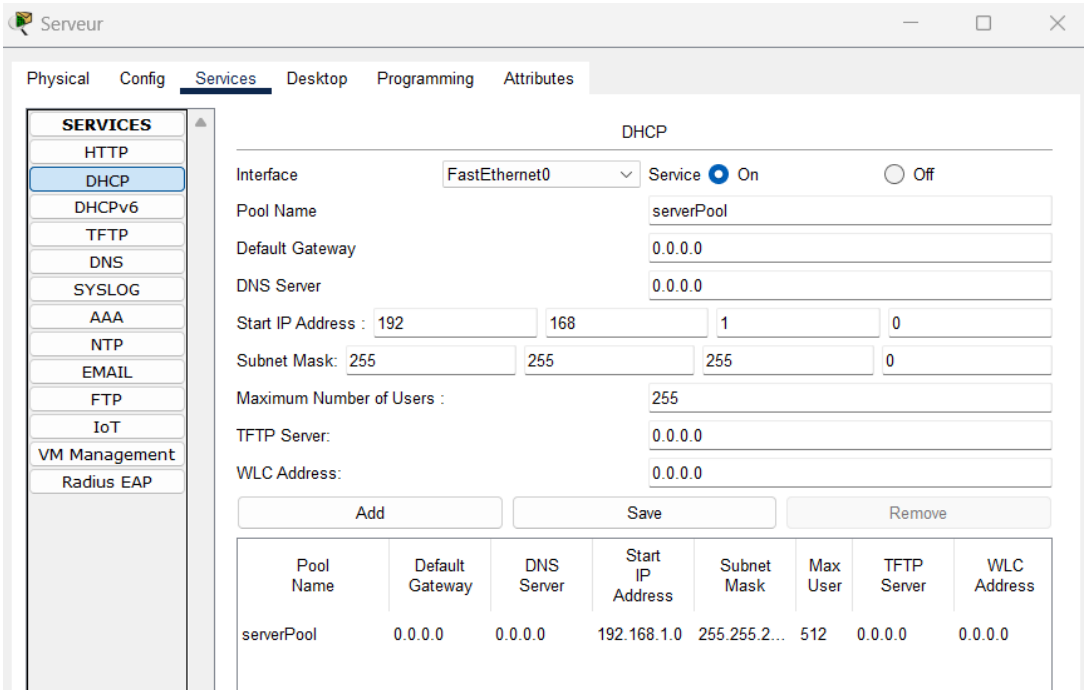


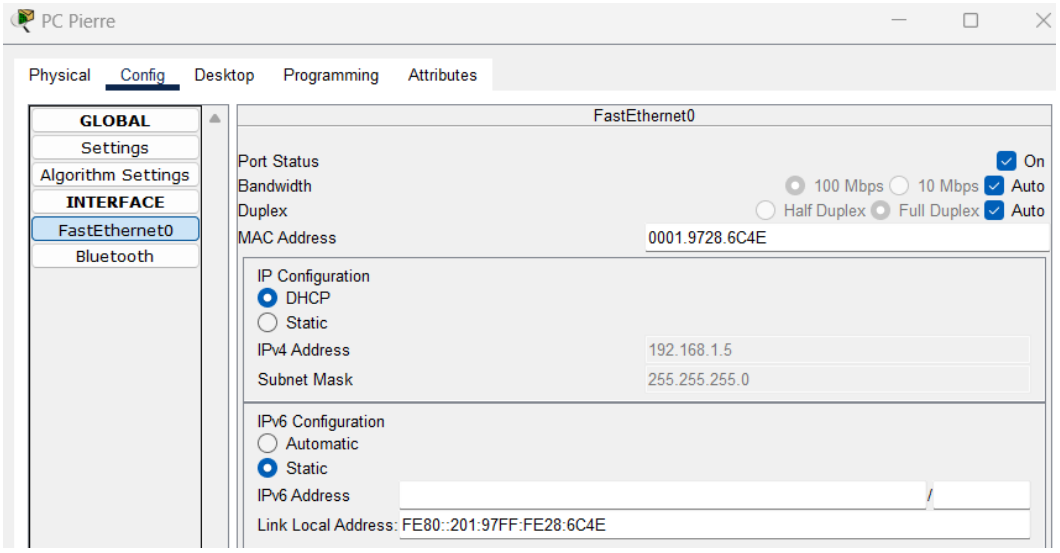
Image 2



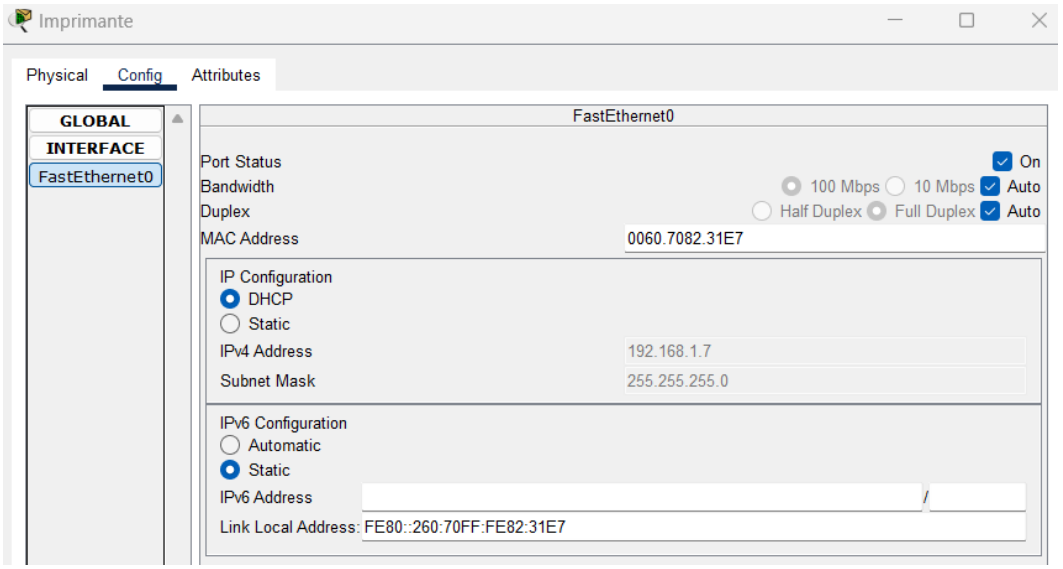
Cela génère alors des adresses IP à tous les équipements connectés à ce dernier, allant de 0 à 255 dans cette configuration.

En tapant “ipconfig” dans chaque console on retrouve bien pour chacun une adresse IP. Ces adresses sont données automatiquement par le serveur.

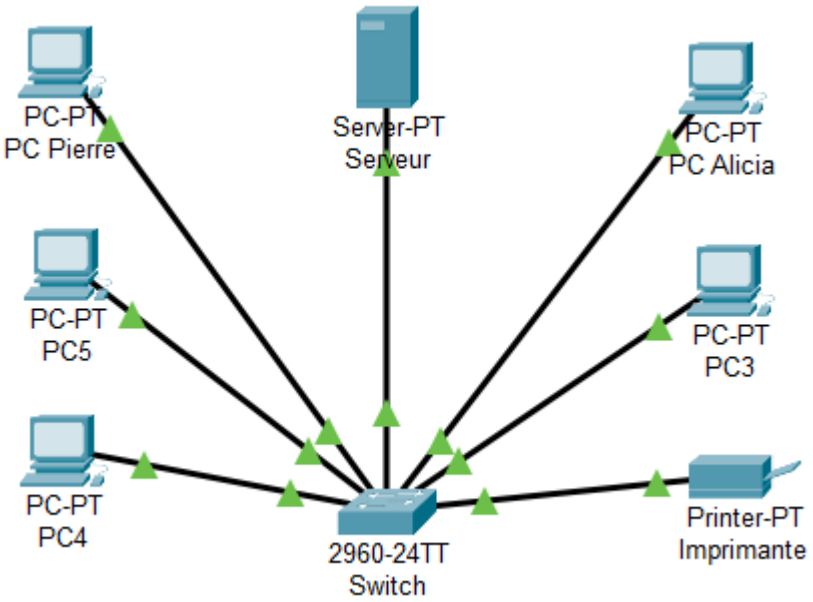
```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:97FF:FE28:6C4E
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.5
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0
```



Imprimante



Architecture réseaux



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

Les adresses IP statiques permettent aux dispositifs de réseau de conserver la même adresse IP en permanence. Un administrateur de réseau doit garder une trace de chaque dispositif attribué statiquement pour éviter de réutiliser la même adresse IP.

Comme l'adresse IP statique requiert des configurations manuelles, elle peut créer des problèmes de réseau en cas d'utilisation sans une bonne maîtrise du protocole TCP/IP.

DHCP est un protocole permettant d'automatiser la tâche d'attribution des adresses IP. Le DHCP est avantageux pour les administrateurs de réseau car il supprime la tâche répétitive consistant à attribuer plusieurs adresses IP à chaque appareil du réseau.

Cela peut ne prendre qu'une minute, mais lorsque vous configurez des centaines de périphériques réseau, cela peut devenir très fatigant. Les points d'accès sans fil utilisent également le DHCP afin que les administrateurs n'aient pas besoin de configurer eux-mêmes leurs appareils.

JOB 11

On peut procéder de différentes manières pour réaliser l’adressage réseau.

Cette première méthode, bien que fonctionnelle, présente des limites en termes d'efficacité et d'utilité pour les entreprises. Elle implique d'attribuer des adresses IP en fonction des besoins précis de chaque sous-réseau, ce qui peut être contraignant. De plus, elle nécessite une surveillance attentive de la part des techniciens pour éviter les erreurs d'adressage.

Tableau d’adressage 1 sous-réseau de 12 hôtes

Classe A	Plages d’adresses (utilisable)	Adresse réseau	Adresse de diffusion (broadcast)	Adresse de sous réseau
1 sous-réseau (12 hôtes)	10.0.0.1 à 10.0.0.14	10.0.0.0	10.0.0.15	/28 255.255.255.240

Tableaux d’adressage 5 sous-réseaux de 30 hôtes

Classe A	Plages d’adresses (utilisable)	Adresse réseau	Adresse de diffusion (broadcast)	Adresse de sous réseau
Premier sous-réseaux	10.0.0.17 à 10.0.0.46	10.0.0.16	10.0.0.47	/27 255.255.255.224
Deuxième sous-réseaux	10.0.0.49 à 10.0.0.78	10.0.0.48	10.0.0.79	
Troisième sous-réseaux	10.0.0.81 à 10.0.0.110	10.0.0.80	10.0.0.111	
Quatrième sous-réseaux	10.0.0.113 à 10.0.0.142	10.0.0.112	10.0.0.143	
Cinquième sous-réseaux	10.0.0.145	10.0.0.144	10.0.0.175	

Tableau d’adressage 5 sous-réseaux de 60 hôtes

Classe A	Plages d’adresses (utilisable)	Adresse réseau	Adresse de diffusion (broadcast)	Adresse de sous réseau
Premier sous-réseaux	10.0.0.177 à 10.0.0.237	10.0.0.176	10.0.0.238	/26 255.255.255.192
Deuxième sous-réseaux	10.0.0.240 10.0.1.45	10.0.0.239	10.0.1.46	
Troisième sous-réseaux	10.0.1.48 à 10.0.1.108	10.0.1.47	10.0.1.109	
Quatrième sous-réseaux	10.0.1.111 à 10.0.1.171	10.0.1.110	10.0.1.172	
Cinquième sous-réseaux	10.0.1.174 à 10.0.1.234	10.0.1.173	10.0.1.235	

Tableau d’adressage 5 sous-réseaux de 120 hôtes

Classe A	Plages d’adresses (utilisable)	Adresse réseau	Adresse de diffusion (broadcast)	Adresse de sous réseau
Premier sous-réseaux	10.0.1.237 à 10.0.2.102	10.0.1.236	10.0.2.103	/25 255.255.255.128
Deuxième sous-réseaux	10.0.2.105 à 10.0.2.125	10.0.2.104	10.0.2.126	
Troisième sous-réseaux	10.0.2.128 à 10.0.2.248	10.0.2.127	10.0.2.249	
Quatrième sous-réseaux	10.0.2.251 à 10.0.3.116	10.0.2.250	10.0.3.117	
Cinquième sous-réseaux	10.0.3.119 à 10.0.3.239	10.0.3.118	10.0.3.240	

Tableau d’adressage 5 sous-réseaux de 160 hôtes

Classe A	Plages d’adresses (utilisable)	Adresse réseau	Adresse de diffusion (broadcast)	Adresse de sous réseau
Premier sous-réseaux	10.0.3.242 à 10.0.4.147	10.0.3.241	10.0.4.161	/24 255.255.255.0
Deuxième sous-réseaux	10.0.4.163 à 10.0.5.68	10.0.4.162	10.0.5.68	
Troisième sous-réseaux	10.0.5.70 à 10.0.5.230	10.0.5.69	10.0.0.231	
Quatrième sous-réseaux	10.0.5.233 à 10.0.6.138	10.0.5.232	10.0.6.139	
Cinquième sous-réseaux	10.0.5.141 à 10.0.7.46	10.0.6.140	10.0.6.47	

Cette seconde méthode sera donc plus adaptée dans le contexte d’une entreprise voulant développer son réseau. Elle consiste à attribuer des plages d'adresses spécifiques à chaque sous-réseau au sein d'une entreprise.

Cette approche permet une gestion claire et structurée des adresses, ce qui est essentiel dans les environnements où la précision et la visibilité sont cruciales. Cela facilite également la planification de l'évolutivité, car chaque sous-réseau est défini de manière distincte.

Cependant, il nécessite une planification minutieuse et une documentation appropriée pour garantir une utilisation efficace de l'espace d'adressage.

Tableau d’adressage 1 sous-réseau de 12 hôtes

Classe A	**Plages d’adresses (utilisable)**	**Adresse réseau**	**Adresse de diffusion (broadcast)**	**Adresse de sous réseau**
1 sous-réseau (12 hôtes)	10.0.0.1 à 10.0.0.14	10.0.0.0	10.0.0.15	/28 255.255.255.240

Tableaux d’adressage 5 sous-réseaux de 30 hôtes

Classe A	Plages d’adresses (utilisable)	Adresse réseau	Adresse de diffusion (broadcast)	Adresse de sous réseau
Premier sous-réseaux	10.0.1.1 à 10.0.1.30	10.0.1.0	10.0.1.31	/27 255.255.255.224
Deuxième sous-réseaux	10.0.2.1 à 10.0.2.30	10.0.2.0	10.0.2.31	
Troisième sous-réseaux	10.0.3.1 à 10.0.1.30	10.0.3.0	10.0.3.31	
Quatrième sous-réseaux	10.0.4.1 à 10.0.1.30	10.0.4.0	10.0.4.31	
Cinquième sous-réseaux	10.0.5.1 à 10.0.5.30	10.0.5.0	10.0.5.31	

Tableau d’adressage 5 sous-réseaux de 60 hôtes

Classe A	Plages d’adresses (utilisable)	Adresse réseau	Adresse de diffusion (broadcast)	Adresse de sous réseau
Premier sous-réseaux	10.0.6.1 à 10.0.6.60	10.0.6.0	10.0.6.61	/26 255.255.255.192
Deuxième sous-réseaux	10.0.7.1 10.0.7.60	10.0.7.0	10.0.7.61	
Troisième sous-réseaux	10.0.8.1 à 10.0.8.60	10.0.8.0	10.0.8.61	
Quatrième sous-réseaux	10.0.9.1 à 10.0.9.60	10.0.9.0	10.0.9.61	
Cinquième sous-réseaux	10.0.10.1 à 10.0.10.60	10.0.10.0	10.0.10.61	

Tableau d’adressage 5 sous-réseaux de 120 hôtes

Classe A	Plages d’adresses (utilisable)	Adresse réseau	Adresse de diffusion (broadcast)	Adresse de sous réseau
Premier sous-réseaux	10.0.11.1 à 10.0.11.120	10.0.11.0	10.0.11.121	/25 255.255.255.128
Deuxième sous-réseaux	10.0.12.1 à 10.0.12.120	10.0.12.0	10.0.12.121	
Troisième sous-réseaux	10.0.13.1 à 10.0.13.120	10.0.13.0	10.0.13.121	
Quatrième sous-réseaux	10.0.14.1 à 10.0.14.120	10.0.14.0	10.0.14.121	
Cinquième sous-réseaux	10.0.15.1 à 10.0.15.120	10.0.15.0	10.0.15.121	

Tableau d’adressage 5 sous-réseaux de 160 hôtes

Classe A	Plages d’adresses (utilisable)	Adresse réseau	Adresse de diffusion (broadcast)	Adresse de sous réseau
Premier sous-réseaux	10.0.16.1 à 10.0.16.160	10.0.16.0	10.0.16.161	/24 255.255.255.0
Deuxième sous-réseaux	10.0.17.1 à 10.0.17.160	10.0.17.0	10.0.17.161	
Troisième sous-réseaux	10.0.18.1 à 10.0.18.160	10.0.18.0	10.0.18.161	
Quatrième sous-réseaux	10.0.19.1 à 10.0.19.160	10.0.19.0	10.0.19.161	
Cinquième sous-réseaux	10.0.20.1 à 10.0.20.160	10.0.20.0	10.0.20.161	

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

Une classe A offre une excellente évolutivité. En cas d'expansion future d'un réseau, l'entreprise disposera d'une réserve d'adresses IP suffisante pour accommoder de nouveaux hôtes ou sous-réseaux, sans nécessiter une refonte complète du schéma d'adressage.

Les classes d'adresses

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques	adresses uniques
E	non défini	240.0.0.0 - 255.255.255.255	adresses uniques	adresses uniques

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

Les réseaux disponibles en classe A vont de 1.0.0.0 à 126.0.0.0.
Convient aux grands réseaux, offrant de nombreuses adresses pour de nombreux hôtes.

Les réseaux disponibles en classe B vont de 128.0.0.0 à 191.255.0.0.
Appropriés pour les réseaux de taille moyenne.

Les réseaux disponibles en classe C vont de 192.0.0.0 à 223.255.255.0.
Conçue pour les réseaux plus petits, avec un nombre limité d'adresses.

Les catégories de classe de réseau, telles que A, B et C, sont utilisées pour organiser les adresses IP en fonction de la taille du réseau.

JOB 12

Tableau du modèle OSI

7 - Application	FTP
6 - Présentation	HTML
5 - Session	TCP
4 - Transport	TCP, UDP, SSL/TLS
3 - Réseau	Routeur, IPv4, IPv6
2 - Liaison	MAC
1 - Physique	Ethernet, Fibre optique, câble RJ45, Wi-Fi

JOB 13

Quelle est l’architecture de ce réseau ?

Nous sommes sur un réseau LAN architecture client-serveur,

Nous sommes sur une topologie en étoile. C’est la topologie la plus courante.
Toutes les machines sont reliées à un unique composant central : le concentrateur.
Quand une machine émet vers le concentrateur, celui-ci envoie les données à
celle qui en est le destinataire (switch) ou à toutes les autres machines (hub).

Cette topologie est plus performante, car les données n'ont pas à passer par chaque nœud.
Ce type de réseau est facile à mettre en place et à surveiller. De plus, la panne d’une station ne met pas en cause l’ensemble du réseau.

Par contre, il faut plus de câbles que pour les autres topologies, et si le concentrateur tombe en panne, tout le réseau est hors d’état de fonctionner.

Dans ce cas là, il aurait été préférable de lier un second switch pour garder un réseau stable en cas de panne du “Switch0”.

Indiquer quelle est l’adresse IP du réseau ?

Avec les éléments que nous avons à disposition on peut constater que l’adresse IP du réseau est de 192.168.10.0, avec une classe C.

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 disposons de 8 bits disponibles pour les adresses d'hôtes dans un réseau de classe C.
Cela signifie que nous avons 2^8, soit 256 combinaisons d'adresses possibles pour les hôtes (de 0 à 255 inclus).

Cependant, certaines adresses sont réservées, comme l'adresse de réseau (198.168.10.0) et l'adresse de diffusion (198.168.10.255). Donc on dispose en réalité de 256 - 2 = 254 adresses utilisables pour les machines.

Quelle est l’adresse de diffusion de ce réseau ?

Comme vu dans la précédente question, nous disposons de 256 adresses. Deux d’entre elles sont réservées, à l’adresse de réseau et la dernière, à l’adresse de diffusion.
Cette dernière adresse est 192.168.1.255

JOB 14

Adresse IP à convertir en binaire :

- 145.32.59.24
- 200.42.129.16
- 14.82.19.54

	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
145.32.59.24	1	0	0	1	0	0	0	1
	0	0	1	0	0	0	0	0
	0	0	1	1	1	0	1	1
	0	0	0	1	1	0	0	0
200.42.129.16	1	1	0	0	1	0	0	0
	0	0	1	0	1	0	1	0
	1	0	0	0	0	0	0	1
	0	0	0	1	0	0	0	0
14.82.19.54	0	0	0	0	1	1	1	0
	0	1	1	0	0	0	1	0
	0	0	0	1	0	0	1	1
	0	0	1	1	0	1	1	0

En convertissant l'adresse IP 145.32.59.24 en binaire, nous obtenons
10010001.00100000.001110111.00011000

En convertissant l'adresse IP 200.42.129.16 en binaire, nous obtenons
11001000.00101010.10000001.00010000

En convertissant l'adresse IP 14.82.19.54 en binaire, nous obtenons
00001110.01100010.00010011.00110110

JOB 15

Qu’est-ce que le routage ?

Le routage est le processus par lequel des données sont dirigées d'un point à un autre à travers un réseau, en sélectionnant le meilleur chemin à suivre.

Cela se fait généralement en fonction des adresses IP de destination pour acheminer les données depuis l'émetteur vers le destinataire, en passant par divers appareils réseau tels que des routeurs.

Le routage permet aux données de circuler efficacement à travers un réseau complexe, en suivant les chemins les plus appropriés, en évitant les obstacles et en optimisant la livraison des données.

Dans les principaux protocoles de routage, on retrouve :

1. **Le Protocole Internet (IP) :** Il spécifie l'origine et la destination de chaque paquet de données. Les routeurs inspectent l'en-tête IP de chaque paquet pour savoir où les envoyer.
2. **Le protocole de routage (BGP) :** BGP (Border Gateway Protocol) : Le BGP protocol est utilisé en ligne à titre de protocole de routage à vecteur de chemin. Il constitue le socle de tout échange de données sur l'accessibilité des routeurs disponibles et la gestion des paquets de données.
3. **OSPF :** La technologie OSPF (Open Shortest Path First), est un protocole servant à déterminer le meilleur chemin que peuvent emprunter des paquets pour transiter par une série de réseaux connectés.
4. **RIP :** Un protocole de routage à vecteur de distance utilisé pour déterminer les chemins optimaux dans un réseau IP. Il évalue les routes en comptant les sauts entre les routeurs. Ses avantages résident dans sa facilité de configuration et son adaptabilité aux petits réseaux.

Qu’est-ce qu’un gateway ?

Une gateway ou passerelle applicative désigne en informatique un dispositif matériel et logiciel qui permet de relier deux réseaux informatiques, ou deux réseaux de télécommunications, aux caractéristiques différentes. Le dispositif permet de vérifier la sécurité du réseau qui cherche à se connecter à l'autre.

La plupart du temps, la passerelle applicative a pour mission de relier un réseau local à Internet. La gateway la plus connue est ainsi, la box Internet.

Qu’est-ce qu’un VPN ?

Le VPN est un logiciel qui s’installe sur plusieurs appareils reliés à Internet. Une fois le VPN activés au serveur distant de ce dernier, un tunnel sécurisé se créer entre vous et le réseau Internet. De cette manière, les informations qui y transitent seront chiffrées. Les utilisateurs individuels peuvent choisir d'utiliser des VPN afin de protéger leur vie privée.
Ainsi, vous obtiendrez une nouvelle adresse IP d’emprunt et la vôtre sera masquée.

Ce service de sécurité Internet qui permet aux utilisateurs d'accéder à Internet comme s'ils étaient connectés à un réseau privé se distingue dans deux catégories.

VPN SSL

Les VPN SSL permettent aux appareils disposant d'une connexion Internet d'établir une connexion VPN d'accès à distance sécurisée avec un navigateur web. Une connexion VPN SSL utilise le chiffrement de bout en bout (E2EE) pour protéger les données transmises entre le logiciel client du terminal du dispositif et le serveur VPN SSL par l'intermédiaire duquel le client se connecte en toute sécurité à Internet.

La principale raison d'utiliser un produit SSL VPN est d'empêcher des parties non autorisées de s'écouter sur des communications réseau et d'extraire ou de modifier des données sensibles. Les systèmes VPN SSL offrent des options sûres et flexibles pour les employés des entreprises, les télétravailleurs et les entrepreneurs afin de se connecter à distance à des réseaux d'entreprises privées.

VPN IPSec

IPsec, également connu sous le nom de Internet Protocol Security, définit l'architecture officielle pour sécuriser le trafic de réseau IP. IPsec spécifie comment les hôtes IP peuvent chiffrer et authentifier des données envoyées au niveau de la couche de réseau IP.

IPsec est utilisé pour créer un tunnel sécurisé entre les entités qui sont identifiées par leurs adresses IP. Les VPN IPsec sont généralement utilisés pour connecter un hôte distant à un serveur VPN réseau. Le trafic envoyé sur l'Internet public est crypté entre le serveur VPN et l'hôte distant.

La différence majeure entre un VPN IPsec et un VPN SSL se résume aux couches de réseau auxquelles le chiffrement et l'authentification sont effectués.

Qu’est-ce qu’un DNS ?

Pour faciliter la recherche d’un site donné sur Internet, le système de noms de domaine (*DNS*) a été inventé. Le *DNS* permet d’associer un nom compréhensible, à une adresse IP. On associe donc une adresse logique, le nom de domaine, à une adresse physique l’adresse IP.

Le nom de domaine et l’adresse IP sont uniques. Le *DNS* permet à votre message d’atteindre son destinataire et non quelqu’un d’autre possédant un nom de domaine similaire. Il vous permet également de taper «www.google.com» sans avoir à saisir une longue adresse IP et d’accéder au site web approprié.

Lorsqu’un internaute saisit une adresse dans son navigateur, c’est donc un serveur *DNS* qui traduit cette adresse humainement compréhensible, en une adresse IP, compréhensible par les ordinateurs et les réseaux.