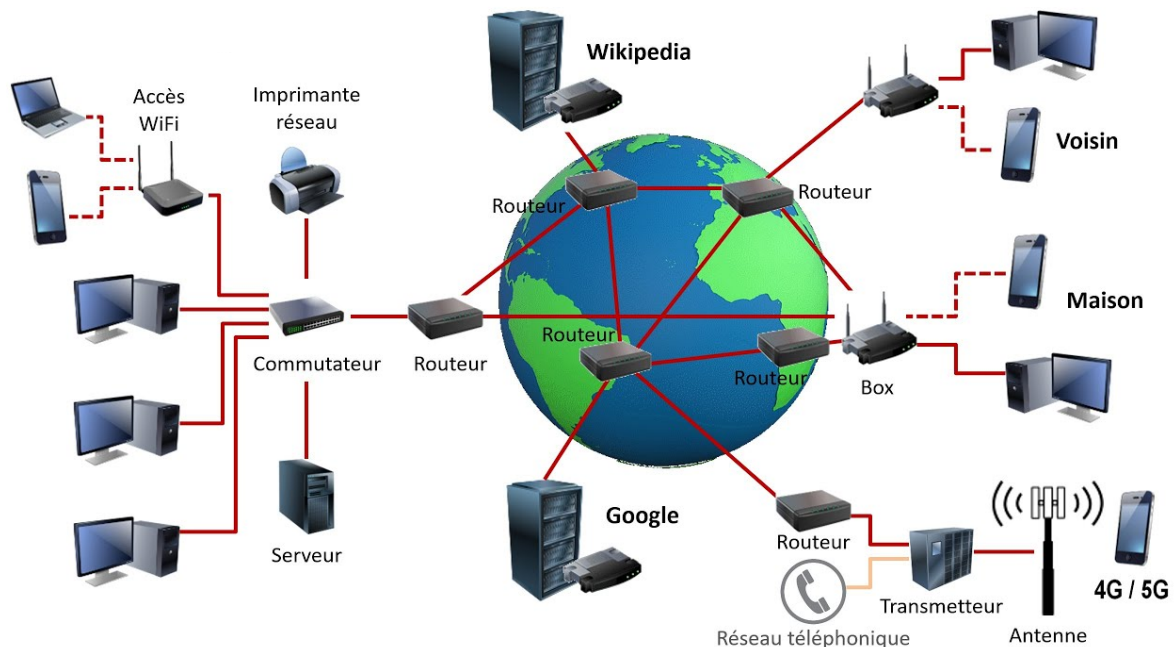


Run Track Réseau

Pourquoi les administrateurs réseau aiment-ils les oiseaux ? Parce qu'ils ont des protocoles de migration bien définis !



Job 1

Cisco Packet Tracer

Cisco Packet Tracer est un logiciel permettant de simuler le fonctionnement d'un réseau informatique. Avec Cisco Packet Tracer, vous pouvez concevoir, configurer et dépanner des réseaux informatiques simples et complexes.

Job 2

→ Qu'est-ce qu'un réseau ?

Le réseau informatique désigne les appareils informatiques interconnectés (ordinateurs, serveurs, routeurs...) qui peuvent échanger des données et partager des ressources entre eux. Ces appareils en réseau utilisent un système de règles, appelées protocoles de communication, pour transmettre des informations sur des technologies physiques ou sans fil. Ils peuvent être locaux (LAN), étendus (WAN) ou mondiaux (Internet).

→ À quoi sert un réseau informatique ?

Les réseaux informatiques servent à faciliter la communication et le partage de ressources entre les ordinateurs et les dispositifs électroniques en les connectant entre eux. Ils ont de multiples usages et offrent de nombreux avantages, notamment le partage des ressources, l'accès à l'information, la communication, la sauvegarde et reprise des données, la gestion centralisée, l'accès à internet, le partage des périphériques, la sécurité et la collaboration entre les individus.

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

Routeurs : Ils permettent de router le trafic entre différents réseaux, comme Internet et un réseau local (LAN).

Commutateurs (Switches) : Ils relient les périphériques au sein d'un réseau local et dirigent le trafic vers sa destination.

Concentrateurs (Hubs) : Moins courants de nos jours, ils sont utilisés pour connecter plusieurs périphériques au sein d'un réseau local, mais ils ne sont pas aussi intelligents que les commutateurs.

Dispositifs de point d'accès (Access Points) : Ils sont utilisés pour créer un réseau sans fil (Wi-Fi) et permettent aux périphériques sans fil de se connecter au réseau câblé.

Modems : Ils permettent de se connecter à Internet via diverses technologies, comme DSL, câble, fibre optique ou liaison satellitaire. Les routeurs modernes intègrent souvent des modems.

Câbles : Vous aurez besoin de câbles pour connecter les dispositifs entre eux. Les types de câbles courants incluent les câbles Ethernet (Cat 5e, Cat 6, etc.) pour les connexions filaires et les câbles coaxiaux ou de fibre optique pour les connexions haut débit.

Cartes réseau (NIC) : Chaque ordinateur ou dispositif qui se connecte au réseau doit avoir une carte réseau (soit intégrée, soit sous forme de carte d'extension) pour se connecter au réseau.

Serveurs : Dans un réseau d'entreprise, vous pouvez avoir des serveurs dédiés pour stocker des données, des applications, des bases de données, etc.

Périphériques réseau : Cela peut inclure des imprimantes réseau, des caméras IP, des dispositifs de stockage en réseau (NAS), etc.

Équipements de sécurité : Les dispositifs de sécurité tels que les pare-feu et les systèmes de détection d'intrusion sont essentiels pour protéger le réseau contre les menaces.

Alimentation ininterrompue (UPS) : Les UPS assurent une alimentation de secours en cas de coupure de courant pour éviter des interruptions critiques du réseau.

Rack ou armoire réseau : Si vous créez un réseau pour une entreprise ou un centre de données, un rack ou une armoire réseau permet de ranger proprement les équipements.

Outils et accessoires : Vous aurez besoin d'outils tels que des pinces à sertir, des testeurs de câbles, des câbles patch, des serre-câbles, des étiquettes, etc., pour installer et maintenir le réseau.

Job 3

Quels câbles avez-vous choisis pour relier les deux ordinateurs ? Expliquez votre choix.

L'utilisation d'un câble droit ou croisé dépend du type de connexion que l'on souhaite établir. De nombreux dispositifs réseau modernes, y compris la plupart des commutateurs (switches) et des routeurs, prennent en charge la détection automatique et peuvent s'adapter à n'importe quel type de câble.

Par conséquent, l'utilisation d'un câble droit est devenue plus courante, car il fonctionne généralement dans la plupart des situations et en cas de doute, un câble droit est un choix sûr.

Cependant le câble croisé a été conçu pour relier deux appareils similaires, , c'est donc celui-ci que nous avons choisi ici.

Job 4

→ Qu'est-ce qu'une adresse IP ?

Une adresse IP (Internet Protocol) est une série de chiffres et/ou de lettres qui identifie de manière unique un appareil ou un nœud (ordinateur, serveur, routeur ou périphérique réseau) sur un réseau informatique qui utilise le protocole Internet.

Les adresses IP sont essentielles pour acheminer des données sur Internet ou sur un réseau local, car elles permettent de déterminer l'origine et la destination des paquets de données.

Il existe deux versions principales d'adresses IP :

IPv4 (Internet Protocol version 4) : Les adresses IPv4 sont composées de quatre nombres décimaux, séparés par des points, tels que 192.168.1.1. Chaque nombre décimal peut varier de 0 à 255. Il existe un espace limité d'adresses IPv4, ce qui a conduit à l'épuisement progressif des adresses IPv4.

IPv6 (Internet Protocol version 6) : Les adresses IPv6 sont plus longues que les adresses IPv4 et sont composées de huit groupes de caractères alphanumériques séparés par des deux-points, tels que 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IPv6 a été introduit pour remédier à la pénurie d'adresses IPv4 en fournissant un espace d'adressage considérablement plus vaste.

→ À quoi sert un IP ?

L'Internet Protocol ou IP est un ensemble de règles et de normes qui servent à régir la manière dont les données sont transmises et reçues sur les réseaux informatiques, y compris sur Internet.

Autrement dit le Protocole Internet définit la structure des paquets de données, les règles de routage, les adresses IP et d'autres aspects fondamentaux de la communication réseau.

Une adresse IP est essentielle pour l'identification, le routage et la communication des données sur un réseau informatique. Elle permet de distinguer chaque appareil connecté, de l'adresser de manière unique, et de garantir que les données sont acheminées de manière appropriée entre les différents nœuds du réseau.

→ Qu'est-ce qu'une adresse MAC ?

Une adresse MAC ou adresse matérielle (Media Access Control) est un identifiant unique attribué à chaque carte réseau d'un appareil (ordinateur, smartphone, imprimante, routeur ou autre périphérique réseau). À l'inverse des adresses IP, qui sont attribuées logiquement et peuvent changer, les adresses MAC sont intégrées au matériel de la carte réseau lors de sa fabrication et sont permanentes.

Les adresses MAC sont essentielles pour le fonctionnement des réseaux locaux (LAN), car elles permettent de déterminer comment les trames de données sont acheminées au sein du réseau. Elles sont utilisées pour garantir que les données parviennent à la bonne carte réseau sur le réseau local.

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

Adresse IP publique :

Une adresse IP publique est une adresse attribuée à un appareil ou à un réseau qui est accessible depuis Internet.

C'est l'adresse IP visible par le monde extérieur, utilisée pour identifier un appareil sur Internet.

Les fournisseurs d'accès à Internet (FAI) attribuent généralement des adresses IP publiques à leurs clients.

Ces adresses permettent aux appareils de communiquer avec d'autres dispositifs sur Internet.

Une adresse IP publique peut être utilisée pour accéder à un serveur web, envoyer et recevoir des courriels, jouer à des jeux en ligne, etc.

Adresse IP privée :

Une adresse IP privée est une adresse utilisée au sein d'un réseau local (LAN) ou d'un réseau privé. Elle n'est pas accessible directement depuis Internet.

Les adresses IP privées sont souvent utilisées pour l'attribution d'adresses locales aux dispositifs connectés à un routeur dans un réseau domestique ou d'entreprise.

Les adresses IP privées sont généralement utilisées pour des raisons de sécurité et de gestion. Elles permettent à plusieurs appareils de partager une seule adresse IP publique pour accéder à Internet, grâce à la fonctionnalité de NAT (Network Address Translation) fournie par le routeur.

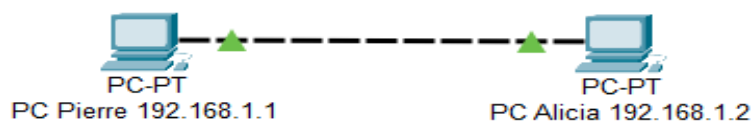
En bref, une adresse IP publique est utilisée pour identifier un appareil sur Internet, tandis qu'une adresse IP privée est utilisée pour identifier un appareil au sein d'un réseau local ou privé.

Les adresses IP privées sont généralement utilisées pour la gestion des réseaux locaux et pour permettre à plusieurs appareils de partager une seule adresse IP publique pour l'accès à Internet.

→ Quelle est l'adresse de ce réseau ?

La première partie d'une adresse IP est utilisée comme adresse réseau, la dernière partie comme adresse hôte. Si on prend pour exemple : 192.168.1.1 et que l'on divise en ces deux parties, on obtient 192.168.1 pour le réseau et .1 pour l'hôte.

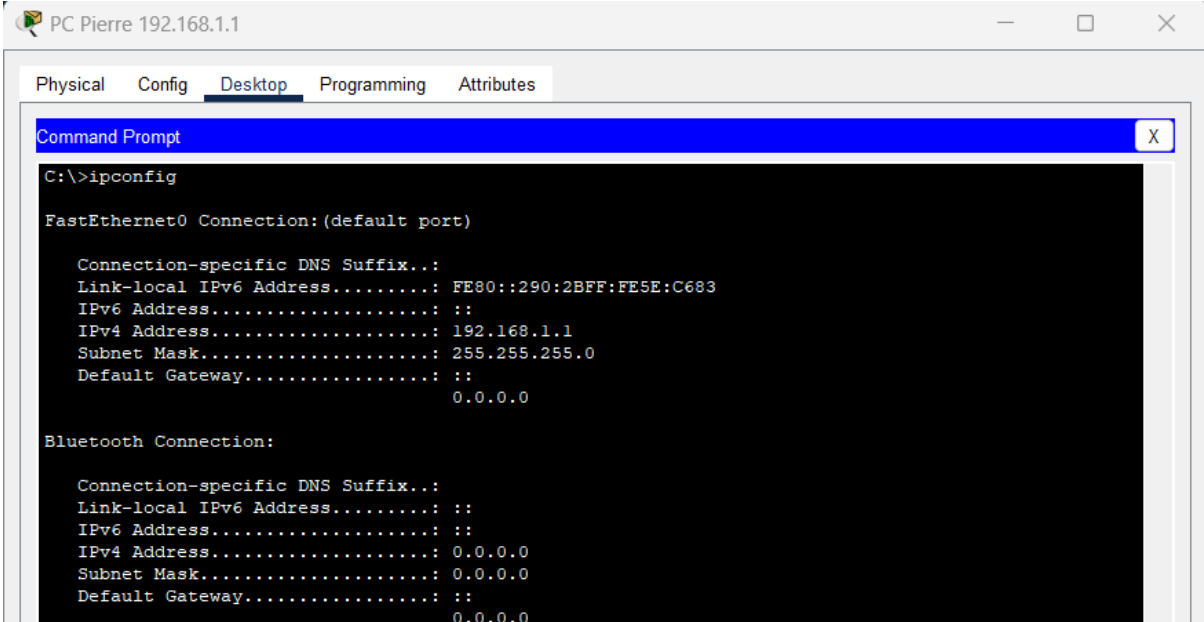
L'adresse réseau ici est 192.168.1.0



Job 5

→ Quelle ligne de commande utilisée pour vérifier l'id des machines ?

La commande utilisée sur le terminal pour vérifier que les IP de Pierre et Alicia sont corrects est : **ipconfig**



The screenshot shows a window titled "PC Pierre 192.168.1.1" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the output of the "ipconfig" command, detailing network settings for FastEthernet0 and Bluetooth connections.

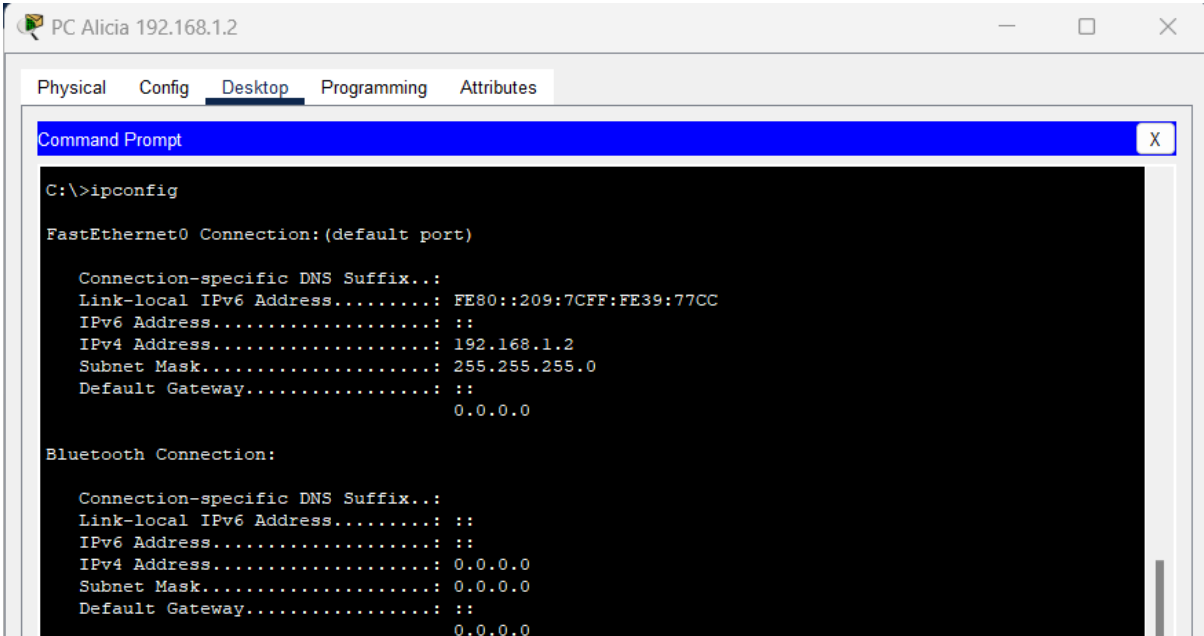
```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::290:2BFF:FE5E:C683
    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
```



The screenshot shows a window titled "PC Alicia 192.168.1.2" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the output of the "ipconfig" command, detailing network settings for FastEthernet0 and Bluetooth connections.

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::209:7CFF:FE39:77CC
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

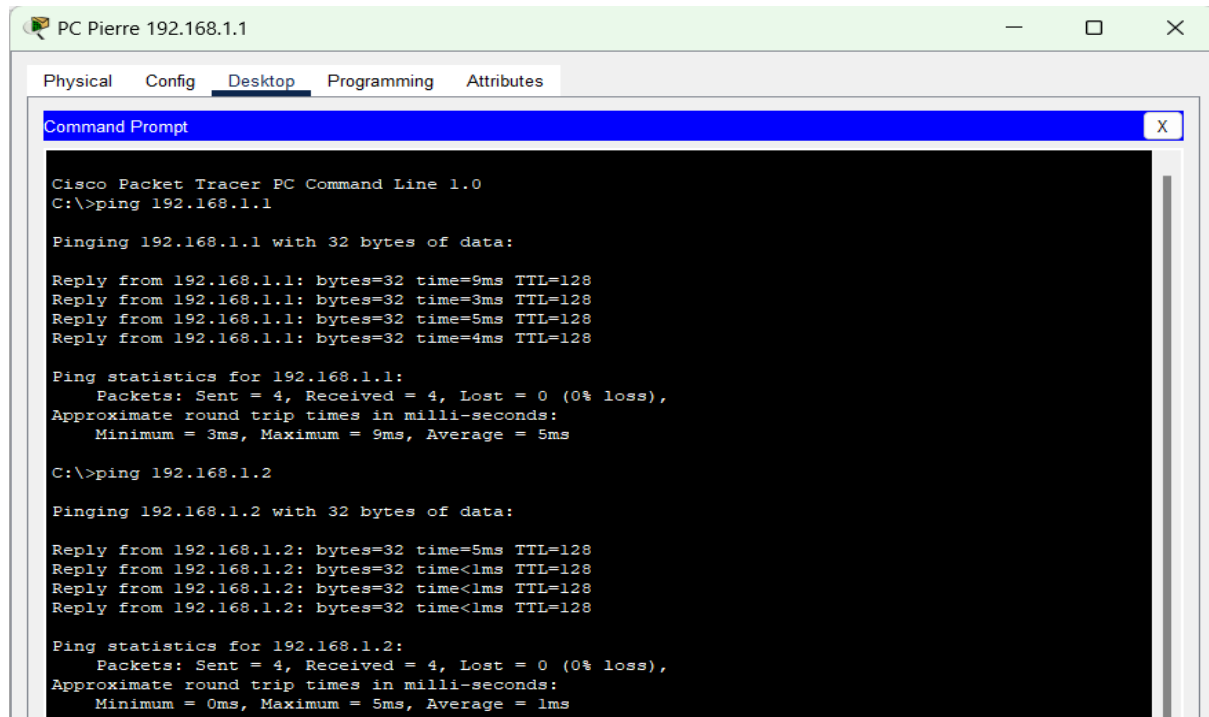
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0
```

Job 6

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

La commande utilisée sur le terminal de commande permettant de ping entre les PC est : **ping adresse Ip**

Exemple : ping 192.168.1.1 et ping 192.168.1.2



```
PC Pierre 192.168.1.1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
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=9ms TTL=128
Reply from 192.168.1.1: bytes=32 time=3ms TTL=128
Reply from 192.168.1.1: bytes=32 time=5ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128

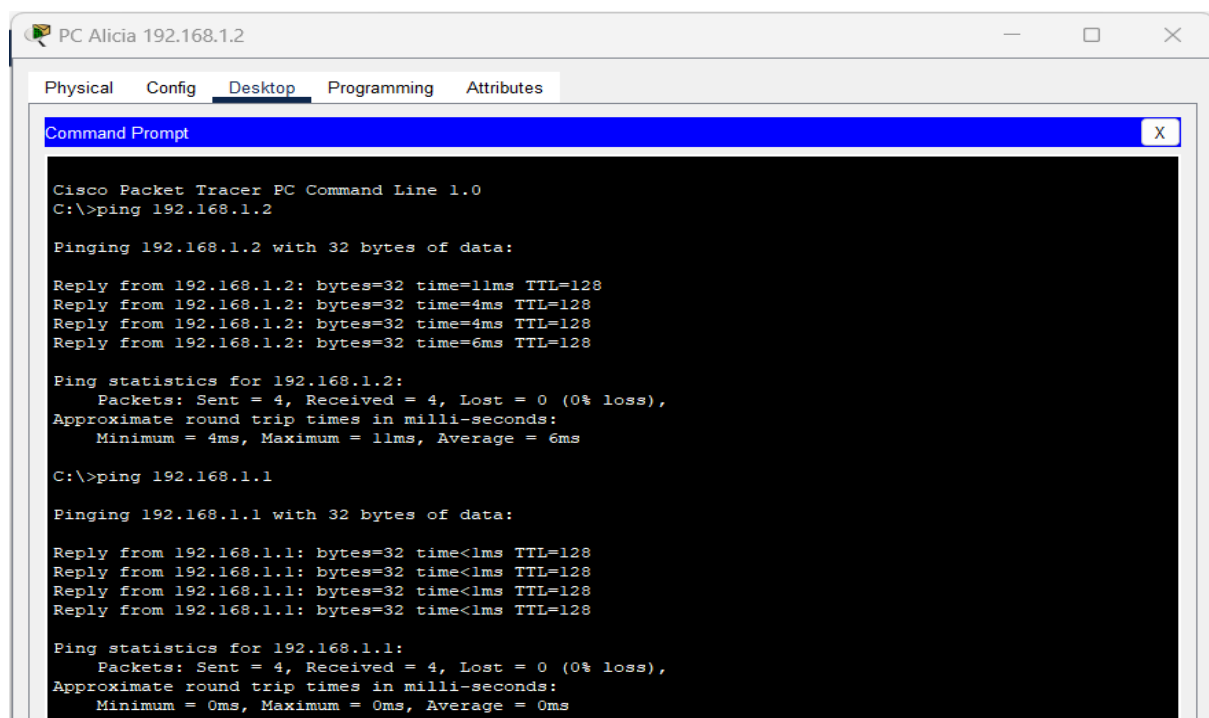
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 9ms, Average = 5ms

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=5ms 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 = 5ms, Average = 1ms
```



```
PC Alicia 192.168.1.2
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
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=11ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms 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 = 4ms, Maximum = 11ms, Average = 6ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

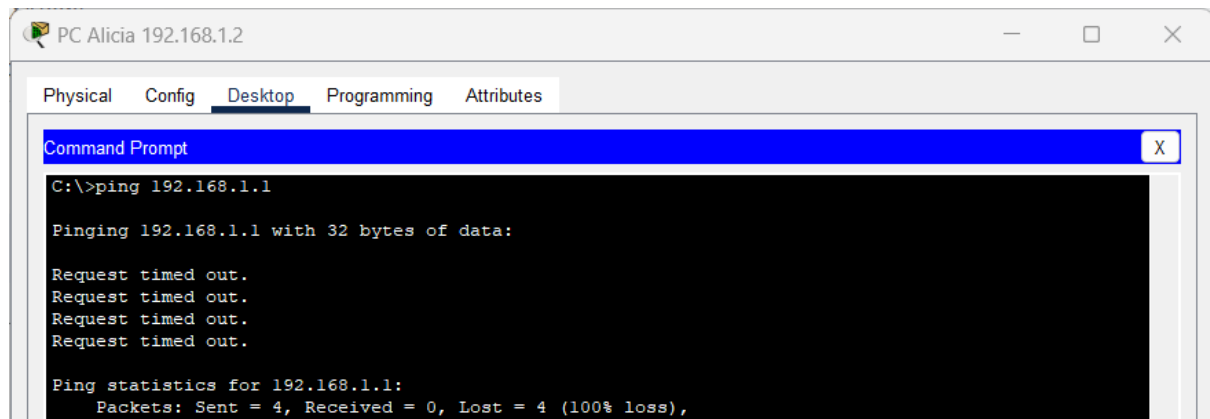
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

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
```

Job 7

→ Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?

En éteignant le PC de Pierre, la connexion réseau avec le PC d'Alicia a été interrompue, de ce fait les paquets envoyés par Alicia ne peuvent pas être reçus.



Job 8

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

Un hub diffuse les données à tous les ports, ce qui entraîne des collisions et des performances limitées, tandis qu'un switch analyse les adresses MAC et dirige le trafic uniquement vers le port approprié, offrant ainsi de meilleures performances et une gestion plus efficace du réseau. Les switches sont préférés pour les réseaux modernes en raison de leur meilleure performance et de leur capacité à éviter les collisions.

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

Un hub fonctionne au niveau de la couche physique (couche 1) du modèle OSI. Il opère en diffusant les données à tous les ports, sans tenir compte de l'adresse MAC des appareils connectés. Tous les appareils reçoivent les données, même si elles ne leur sont pas destinées.

Avantages :

- le coût, moins cher qu'un switch
- la facilité d'installation
- la conception simple

Inconvénients :

- la bande passante est partagée
- les collisions entre les transmissions des données
- le manque de sécurité
- l'obsolescence

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

Les switches sont plus performants que les hubs car ils éliminent les collisions. Chaque port dispose de sa propre bande passante dédiée, ce qui permet un débit plus élevé et une communication plus efficace entre les appareils.

Les switches sont largement utilisés dans les réseaux modernes. Ils offrent une meilleure performance, une sécurité améliorée (couche 2 du modèle OSI) et la capacité de gérer des réseaux de taille variable, des petits réseaux locaux (LAN) aux réseaux d'entreprise complexes.

Avantages :

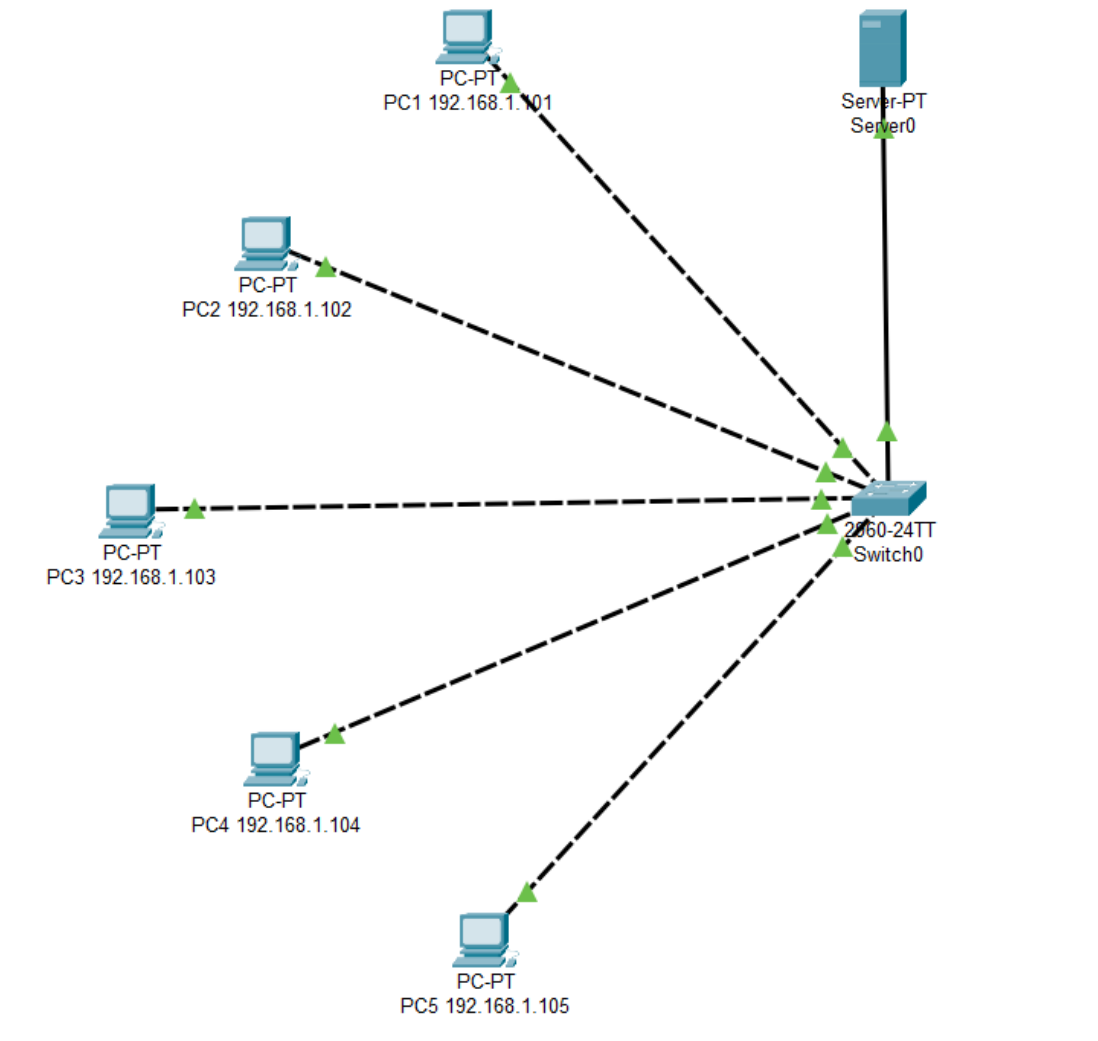
- la performance, bande passante dédiée à chaque port
- la sécurité, (couche 2 de OSI) filtre le trafic vers le port destinataire
- la gestion avancée du réseau
- l'isolation des erreurs en isolant le port défaillant
- l'évolutivité, réseaux de petites tailles à grandes
- prise en charge de nombreux médias (Ethernet, fibre optique...)

Inconvénients :

- le coût, les commutateurs sont généralement plus chers que les hubs
- la complexité, plus complexes à configurer et à gérer que les hubs
- la maintenance, les commutateurs requièrent une gestion continue et des mises à jour du firmware pour garantir des performances optimales.
- l'électricité, contrairement aux hubs, les commutateurs nécessitent une alimentation électrique, ce qui peut être un inconvénient dans certaines situations.

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

Le switch gère le trafic de manière intelligente en utilisant sa table d'adresses MAC pour déterminer sur quel port chaque appareil est connecté, puis redirige le trafic uniquement vers le port approprié. Cela permet d'optimiser la bande passante, d'améliorer la sécurité et de réduire la diffusion inutile du trafic sur le réseau.



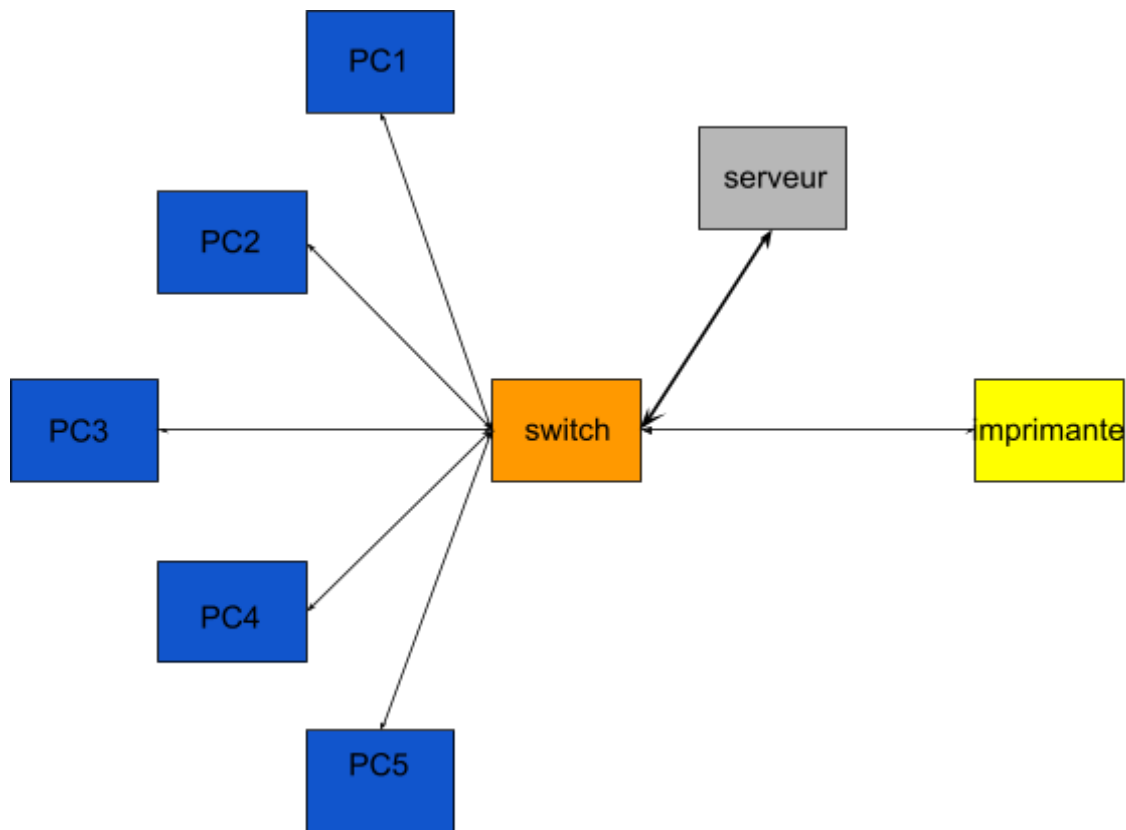
Job 9

Le réseau est un réseau dit en “étoile”, en effet les équipements du réseau sont reliés à un système matériel central, ici, un switch (ou commutateur).

Celui-ci a pour rôle d'assurer la communication entre les différents équipements du réseau. Notamment utilisée par les réseaux Ethernet actuels en RJ45, elle concerne maintenant la majorité des réseaux.

Dans cette topologie tous les hôtes sont interconnectés grâce au switch (sorte de multiprise pour les câbles réseaux placés au centre de l'étoile).

Les stations émettent vers ce concentrateur qui renvoie les données vers tous les autres ports réseaux (hub) ou uniquement au destinataire (switch).



Les avantages d'avoir un schéma sont les suivants :

- *Il favorise l'attention, la compréhension et la mémorisation*
- *Il permet d'expliciter des informations concrètes qui ne sont pas directement visibles à l'œil nu.*
- *Il peut également rendre compréhensibles des informations abstraites ou non perceptibles en permettant leur visualisation, et donc leur analyse.*
- *Le schéma qui utilise l'image réconcilie l'hémisphère droit (qui traite les images) et l'hémisphère gauche (qui traite les textes) du cerveau grâce à l'utilisation conjointe du texte et de l'image qui, réunis, font sens. Le lecteur utilise donc la globalité des capacités de son cerveau.*
- *Il sollicite tant l'esprit de synthèse (il permet d'avoir une vision globale et immédiate du sujet présenté) que l'esprit d'analyse (il permet de visualiser et de comprendre chacun des éléments composant le schéma et comment ces éléments sont liés entre eux).*

En bref, le schéma est beaucoup plus attractif et donc plus intéressant !

Job 10

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

L'adresse IP statique et l'adresse IP attribuée par DHCP sont deux méthodes de configuration d'adresses IP pour les appareils sur un réseau.

La principale différence réside dans la manière dont les adresses IP sont attribuées. L'adresse IP statique est configurée manuellement et reste constante, tandis que l'adresse IP attribuée par DHCP est distribuée automatiquement et peut changer à chaque connexion.

Job 11

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

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

Les adresses IP sont généralement divisées en cinq classes principales (A, B, C, D et E) pour aider à organiser les réseaux en fonction de leur taille et de leur utilisation prévue.

Classe A (1.0.0.0 à 126.0.0.0) :

La classe A est réservée aux très grands réseaux. Le premier octet est réservé pour le réseau, tandis que les trois octets restants sont utilisés pour les hôtes.

Classe B (128.0.0.0 à 191.255.0.0) :

La classe B est adaptée aux réseaux de taille moyenne. Les deux premiers octets sont réservés pour le réseau, tandis que les deux derniers octets sont utilisés pour les hôtes.

Classe C (192.0.0.0 à 223.255.255.0) :

La classe C est destinée aux petits réseaux. Les trois premiers octets sont utilisés pour le réseau, tandis que le dernier octet est réservé pour les hôtes.

Classe D (224.0.0.0 à 239.255.255.255) :

La classe D est réservée aux adresses IP multicast. Les adresses de classe D sont utilisées pour le trafic multicast, ce qui signifie qu'elles sont destinées à être reçues par plusieurs hôtes en même temps.

Classe E (240.0.0.0 à 255.255.255.255) :

La classe E est réservée à un usage expérimental et n'est généralement pas utilisée dans les réseaux publics. Elle est utilisée pour la recherche et le développement.

Nous utilisons une adresse IP de classe A car nous avons besoin de créer 21 sous réseaux pour accueillir plus de 300 hôtes, ce qui en fait un grand réseau.

Sous réseaux	Nombre d'hôtes	Adresse Réseau	Masque	Broadcast
1	12	10.0.0.0 10.0.0.14	255.255.255.240	10.0.0.15
2	30	10.0.1.0 10.0.1.32	255.255.255.224	10.0.1.33
3	30	10.0.2.0 10.0.2.32	255.255.255.224	10.0.2.33
4	30	10.0.3.0 10.0.3.32	255.255.255.224	10.0.3.33
5	30	10.0.4.0 10.0.4.32	255.255.255.224	10.0.4.33
6	30	10.0.5.0 10.0.5.32	255.255.255.224	10.0.5.33
7	120	10.0.6.0 10.0.6.122	255.255.255.128	10.0.6.123
8	120	10.0.7.0 10.0.7.122	255.255.255.128	10.0.7.123
9	120	10.0.8.0 10.0.8.122	255.255.255.128	10.0.8.123
10	120	10.0.9.0 10.0.9.122	255.255.255.128	10.0.9.123
11	120	10.0.10.0 10.0.10.122	255.255.255.128	10.0.10.123
12	160	10.0.11.0 10.0.11.162	255.255.255.0	10.0.11.163
13	160	10.0.12.0 10.0.12.162	255.255.255.0	10.0.12.163
14	160	10.0.13.0 10.0.13.162	255.255.255.0	10.0.13.163
15	160	10.0.14.0 10.0.14.162	255.255.255.0	10.0.14.163
16	160	10.0.15.0 10.0.15.162	255.255.255.0	10.0.15.163

17	Inutilisé			
18	Inutilisé			
19	Inutilisé			
20	Inutilisé			
21	Inutilisé			

Job 12

	Unité de données	Couche	Exemples
Couche Haute	Donnée	7 - Application	FTP
Couche Haute	Donnée	6 - Présentation	HTML
Couche Haute	Donnée	5 - Session	
Couche Haute	Segment	4 - Transport	TCP, UDP, PPTP, SSL/TLS
Couche Matérielle	Paquet	3 - Réseaux	Routeur, IPV6, IPV4
Couche Matérielle	Trame	2 - Liaison	Ethernet, MAC,
Couche Matérielle	Bit	1 - Physique	RJ45, Wifi, Fibre Opt

Couche 1 - Physique : La couche physique est la plus basse et gère la transmission brute des données sur le support physique, que ce soit sous forme de signaux électriques, optiques ou radio. Elle comprend le câblage, les adaptateurs, les commutateurs et d'autres composants matériels.

Couche 2 - Liaison : La couche de liaison de données assure la communication entre des appareils directement connectés. Elle organise les données en trames, gère l'accès au support (comme Ethernet), détecte et corrige les erreurs.

Couche 3 - Réseau : La couche réseau est responsable de l'acheminement des données sur le réseau. Elle détermine le chemin optimal pour atteindre la destination en utilisant des adresses IP. Les routeurs opèrent à cette couche.

Couche 4 - Transport : La couche de transport assure un transfert de données fiable et transparent entre les deux systèmes en communication. Elle gère la segmentation et la réassemblage des données, le contrôle de flux, et la correction d'erreurs.

Couche 5 - Session : La couche de session établit, maintient et termine les connexions entre les applications des deux côtés de la communication. Elle gère également la synchronisation et la reprise des sessions en cas de panne.

Couche 6 - Présentation : La couche de présentation gère la traduction, la compression et le chiffrement des données, assurant ainsi que les données sont dans un format compréhensible par les deux parties de la communication.

Couche 7 - Application : Cette couche est la plus proche de l'utilisateur final. Elle gère les applications et les services directement accessibles aux utilisateurs. Cela inclut des applications telles que les navigateurs Web, les clients de messagerie électronique, etc.

Job 13

Parc informatique de la Plateforme (4 PC)

L'adressage IP du réseau est :

- *PC0 : 192.168.10.6*
- *PC1 : 192.168.10.7*
- *PC2 : 192.168.10.8*
- *PC3 : 192.168.10.9*
- *Serveur 1 : 192.168.10.100*
- *Serveur 2 : 192.168.10.200*

Masque de sous-réseau :
255.255.255.0

→ Quelle est l'architecture de ce réseau ?

L'architecture de ce réseau est une topologie en étoile

→ Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est 192.168.10.0

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

On peut brancher 254 machines sur ce réseau

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

L'adresse de diffusion de ce réseau est 192.168.10.255

Job 14

→ Conversion des adresses IP suivantes en binaires :

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

Tableau de conversion Binaire

Bit	128	64	32	16	8	4	2	1
Octet	1	0	0	1	0	0	0	1

Job 15

→ Qu'est-ce que le routage ?

Le routage est le processus de transmission de données entre des réseaux informatiques distincts, que ce soit à l'intérieur d'un réseau local (LAN) ou entre différents réseaux étendus (WAN). Le routage permet de déterminer la meilleure façon de faire passer les données d'un point à un autre sur un réseau, en prenant en compte la topologie du réseau, les adresses IP, les métriques et d'autres facteurs.

→ Qu'est-ce qu'un gateway ?

C'est un dispositif matériel ou logiciel qui permet la communication entre deux réseaux informatiques utilisant des protocoles de communication différents. Les passerelles sont essentielles dans le routage des données entre les réseaux en convertissant les données d'un format (ou protocole) pour une communication fluide.

→ Qu'est-ce qu'un VPN ?

Un VPN ou Réseau Privé Virtuel, est un service ou une technologie qui permet de créer une connexion sécurisée et cryptée entre deux réseaux ou entre un utilisateur et un réseau, généralement via Internet. Les VPN sont largement utilisés pour garantir la confidentialité, la sécurité et l'anonymat des communications en ligne.

→ Qu'est-ce qu'un DNS ?

Le DNS ou Domain Name System, est un système essentiel qui permet de traduire les noms de domaine conviviaux que nous utilisons pour accéder à des sites web en adresses IP numériques. Il agit comme un annuaire d'Internet, permettant aux ordinateurs de trouver les ressources en ligne en fonction de leur nom de domaine.