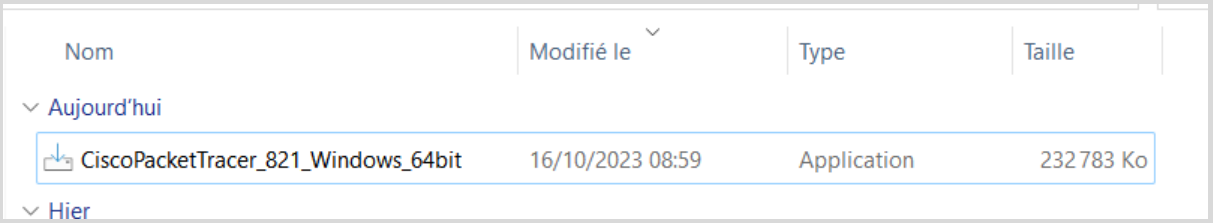
RunTrack Réseau

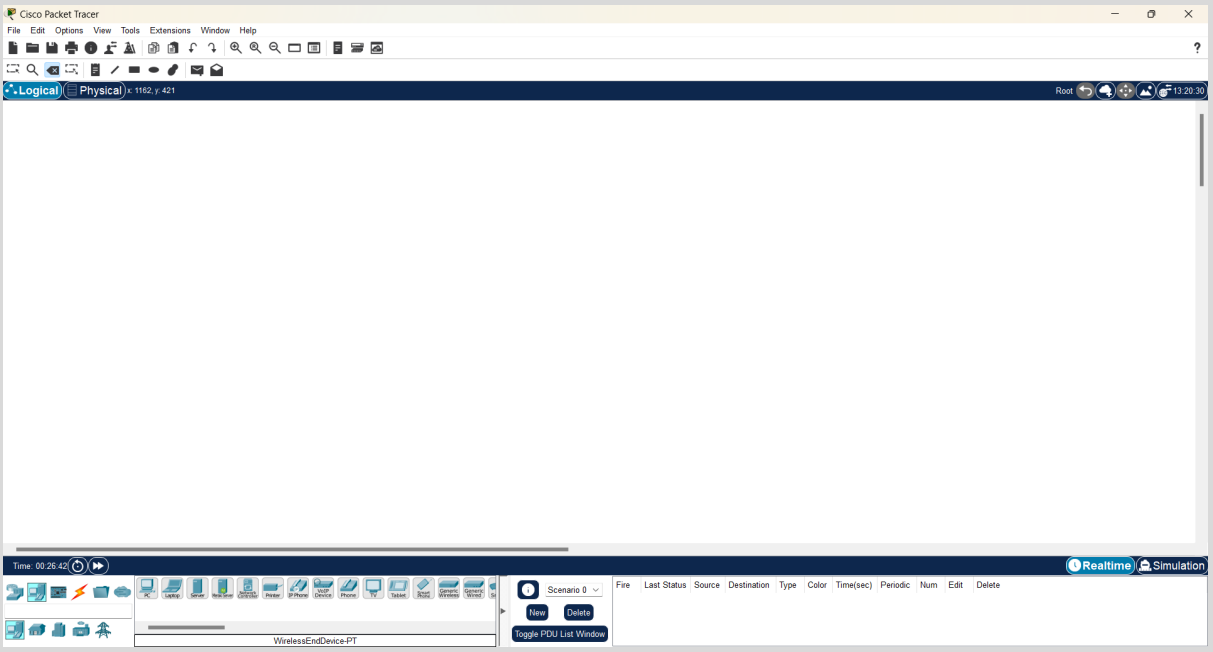
Lucas Bendia

Job 1 :

Tout d'abord il faut telecharger Cisco :



une fois installer il faut lancer Cisco et ce login avec ces identifiants

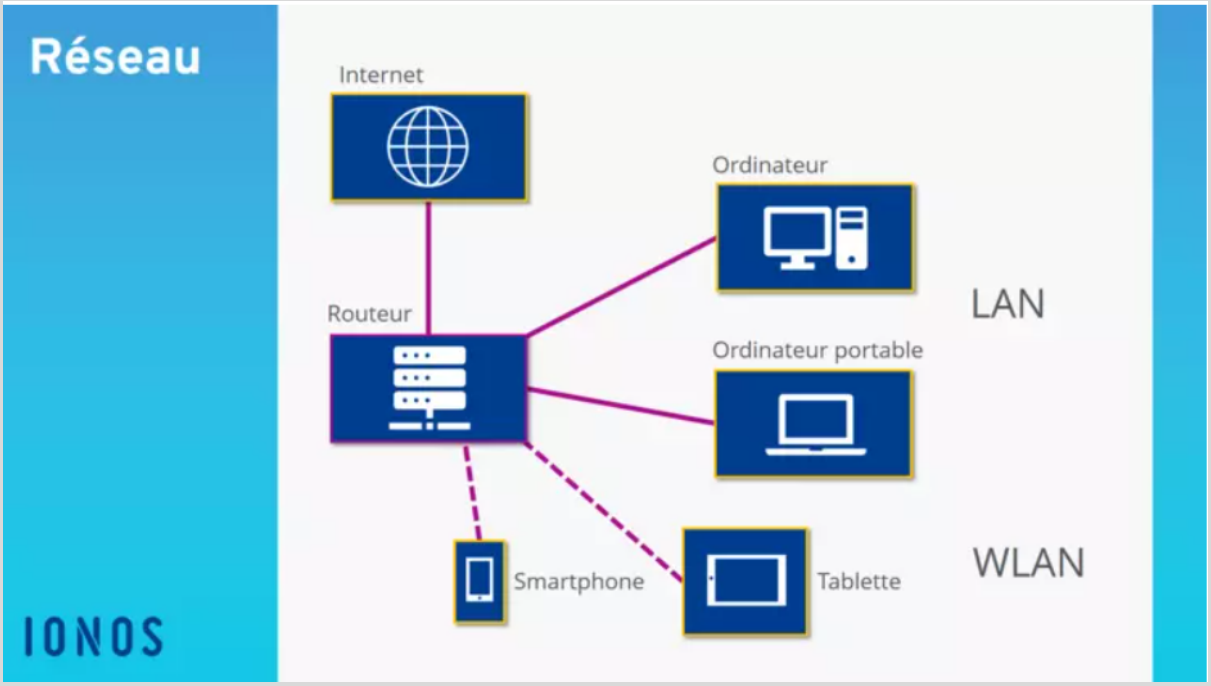


Job 2 :

Qu'est-ce qu'un réseau ?

Dans les technologies de l'information, 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. On parle aussi dans ce

cas de réseau peer-to-peer (P2P) ou en français pair à pair. 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 (imprimante, etc.).

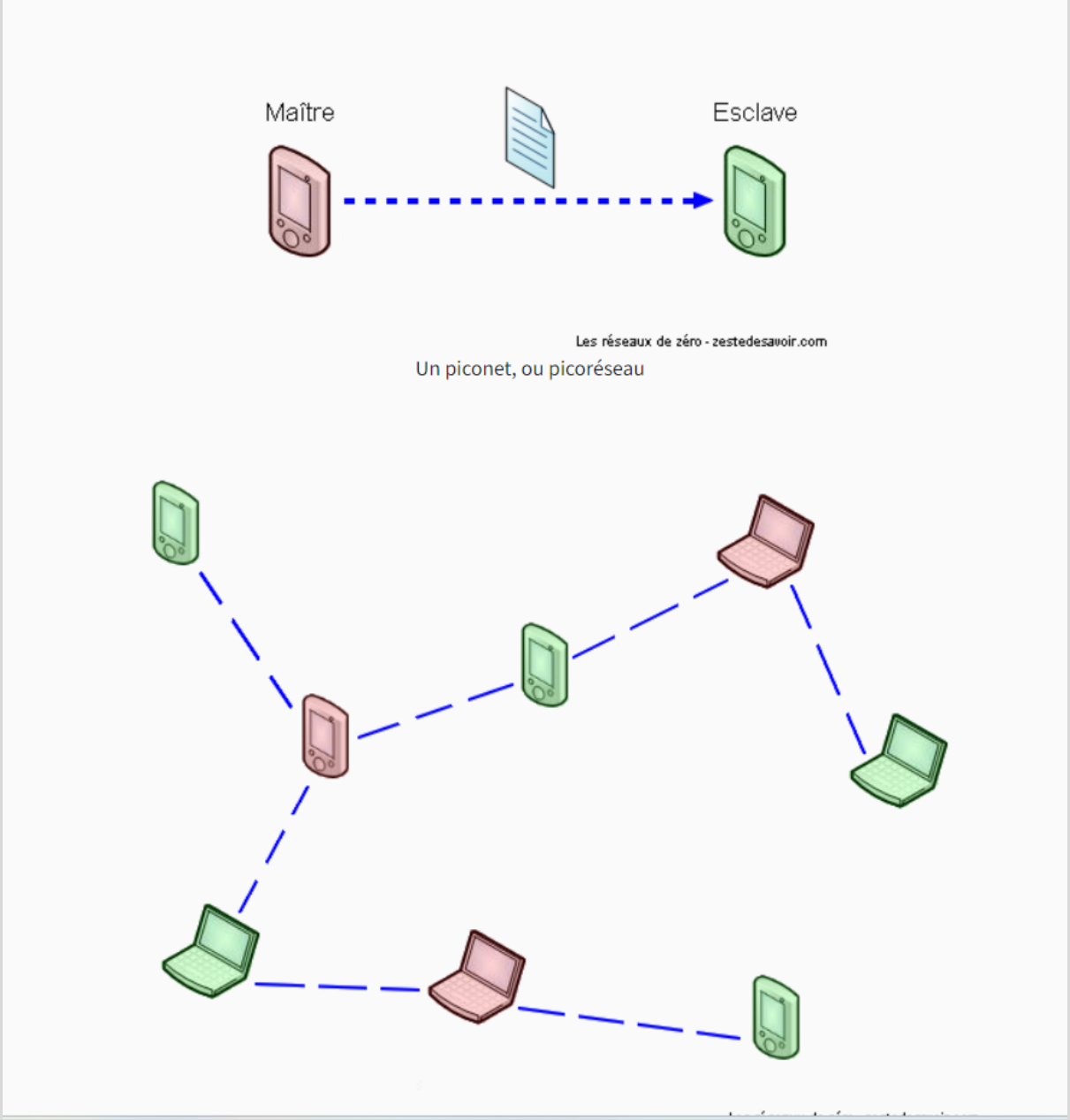


À quoi sert un réseau informatique ?

Les réseaux informatiques sont utilisés pour effectuer un grand nombre de tâches grâce au partage de l'information.
Les réseaux sont notamment utilisés pour :
Communiquer par courrier électronique, vidéo, messagerie instantanée et autres méthodes.
Partager des appareils tels que des imprimantes, des scanners et des photocopieurs,
Partager des fichiers, Partager des logiciels et des programmes d'exploitation sur des systèmes distants permet aux utilisateurs du réseau d'accéder facilement aux informations et de les mettre à jour.

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

Il faut savoir que pour construire un réseau, il faut du matériel. Tout comme il faut un moteur, des roues et autres pour construire une voiture. Nous verrons donc quels sont les appareils et comment ils sont reliés entre eux : câbles, transmission sans fil, etc.



Un piconet, ou picoréseau

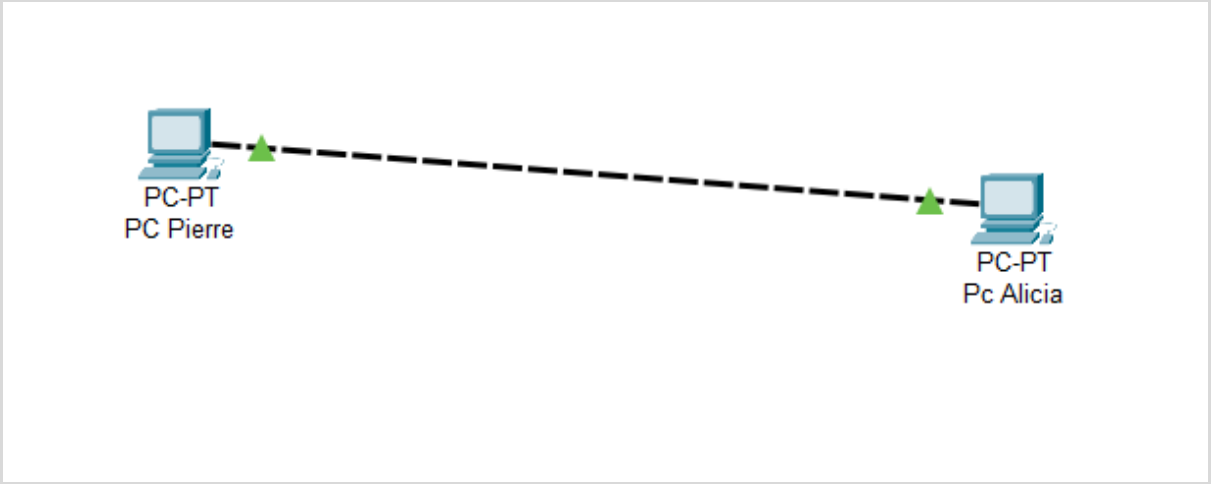
Afin de conclure ce chapitre, nous allons récapituler le matériel vu et son utilité. Un tableau récapitulatif vaut mieux qu'un long discours :

Matériel	Utilité
Carte réseau	La carte réseau est le matériel de base indispensable, qui traite tout au sujet de la communication dans le monde du réseau.
Concentrateur (*hub*)	Le concentrateur permet de relier plusieurs ordinateurs entre eux, mais on lui reproche le manque de confidentialité.
Commutateur (*switch*)	Le commutateur fonctionne comme le concentrateur, sauf qu'il transmet des données aux destinataires en se basant sur leurs adresses MAC (adresses physiques). Chaque machine reçoit seulement ce qui lui est adressé.
Routeur	Le routeur permet d'assurer la communication entre différents réseaux pouvant être fondamentalement différents (réseau local et Internet).
Répéteur	Le répéteur reçoit des données par une interface de réception et les renvoie *plus fort* par l'interface d'émission. On parle aussi de *relais* en téléphonie et radiophonie.

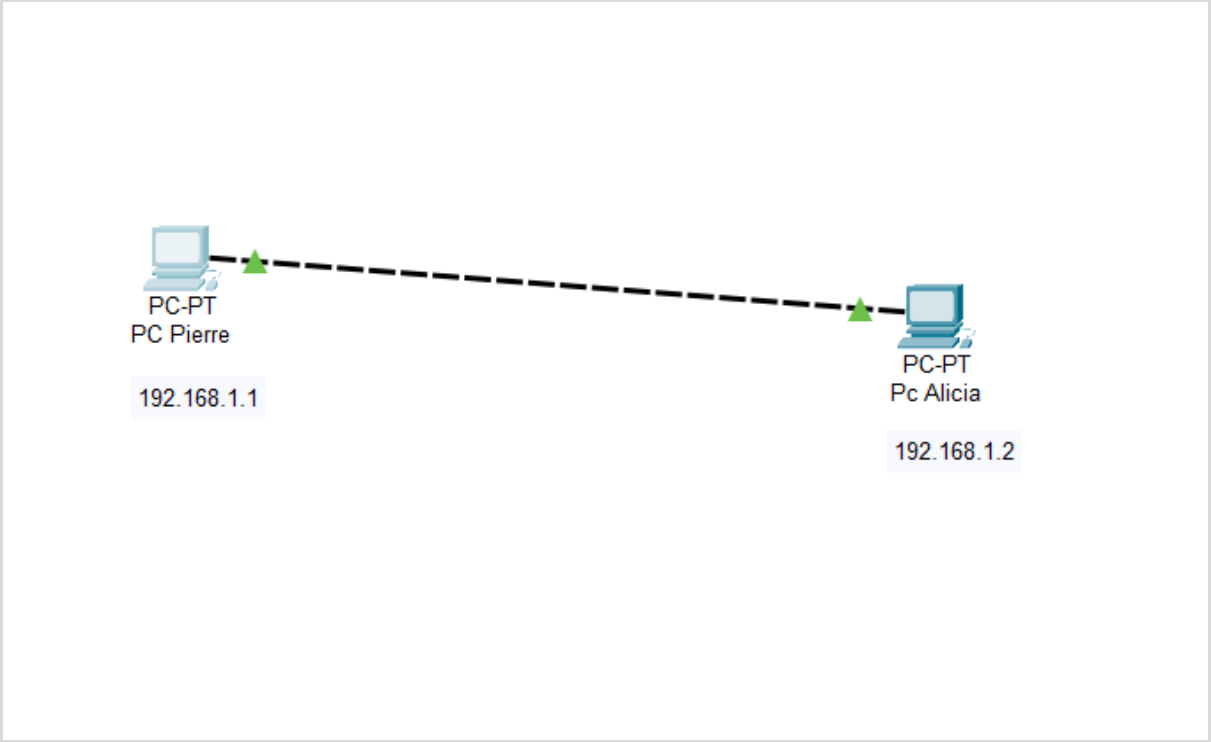
Job 3 :

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

j'ai choisi un câble croisé car il connecte deux dispositifs du même type pour communiquer, comme un ordinateur à un autre ordinateur, ou un commutateur à un autre commutateur.



Job 4 :



Qu’est-ce qu’une adresse IP ?

Une adresse IP (Internet Protocol) est une série de chiffres qui identifie de manière unique un appareil sur un réseau informatique, qu'il s'agisse d'un appareil connecté à Internet ou à un réseau local. Les adresses IP sont essentielles pour le routage des données sur Internet, car elles permettent de diriger le trafic vers l'appareil approprié. Il existe deux versions principales d'adresses IP : IPv4, qui utilise une notation décimale comme "192.168.1.1", et IPv6, qui utilise une notation hexadécimale plus longue pour répondre à la pénurie d'adresses IPv4.

À quoi sert un IP ?

Une adresse IP (Internet Protocol) sert à identifier de manière unique un appareil sur un réseau informatique. Cela a plusieurs utilisations essentielles, les adresses IP sont un élément clé de l'infrastructure d'Internet, permettant l'acheminement et la gestion du trafic, ainsi que l'identification et la communication entre les appareils connectés.

Qu’est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control) est un identifiant unique attribué à chaque carte réseau (NIC) d'un appareil, tel qu'un ordinateur, un smartphone ou un routeur, au niveau matériel. Contrairement aux adresses IP, qui sont attribuées logiquement et peuvent changer, les adresses MAC sont généralement permanentes et uniques à chaque appareil. Elles sont composées de 12 caractères hexadécimaux, par exemple, "00:1A:2B:3C:4D:5E".

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

Une adresse IP publique et une adresse IP privée sont deux concepts importants en réseau informatique.

L'adresse IP publique est utilisée pour communiquer avec des ressources sur Internet et est généralement partagée par tous les appareils de votre réseau local. C'est l'adresse que les sites web et les serveurs distants voient lorsque vous accédez à Internet.

Les adresses IP privées sont utilisées pour acheminer le trafic localement, en interne. Les adresses IP privées sont généralement attribuées selon des plages spécifiques définies par les normes, telles que les adresses IP qui commencent par "192.168.x.x," "10.x.x.x," ou "172.16.x.x" à "172.31.x.x." Elles sont utilisées pour identifier les appareils dans un réseau local et ne sont pas directement accessibles depuis Internet

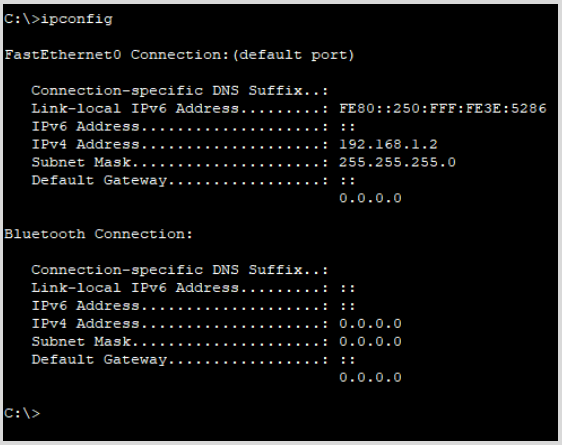
Quelle est l’adresse de ce réseau ?

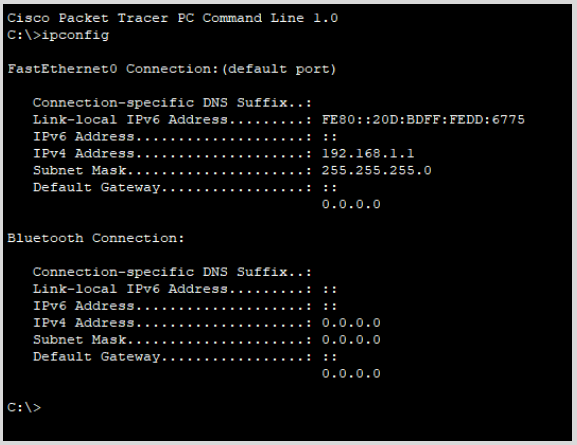
L’adresse IP privée pour un réseau local utilisera une ip telle que "192.168.x.x," en fonction du masque de sous-réseau. L'adresse spécifique du réseau local dépendra de la configuration de votre routeur ou commutateur.

Job 5 :

Quelle ligne de commande avez-vous utilisée pour vérifier l’id des machines ?

Pour vérifier l’ip des deux machines j’ai utiliser la commande “ipconfig”

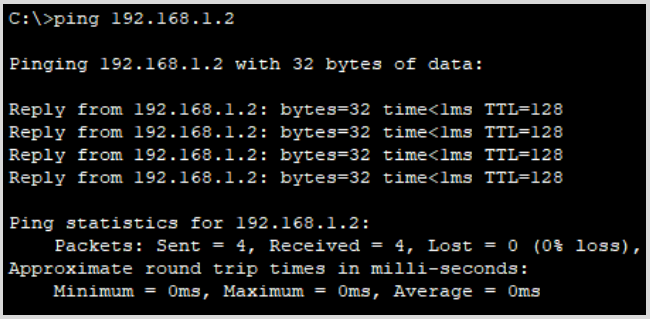




Job 6 :

Quelle est la commande permettant de Ping entre des PC ?

Pour vérifier que le ping c’est bien effectuer j'ai utiliser la commande “ping ip de la machine”



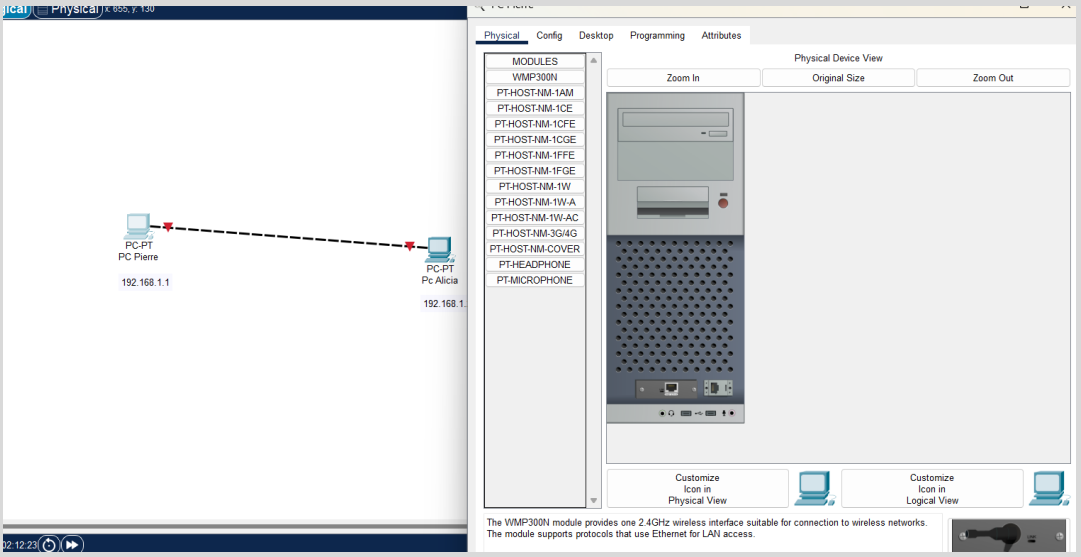
```
C:\>ping 192.168.1.1

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=4ms 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 = 4ms, Average = 1ms
```

Job 7 :




```
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 a-t-il reçu les paquets envoyés par Alicia ?

Non le pc de Pierre n’a pas de reçus les paquets d’Alicia

Expliquez pourquoi.

Il n’a pas pu recevoir les paquets d'Alicia car le pc de de Pierre est éteint.

Job 8 :

```
ping 192.168.1.7

Pinging 192.168.1.7 with 32 bytes of data:

Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Quelle est la différence entre un hub et un switch ?

Un hub et un switch sont deux dispositifs de réseau utilisés pour connecter plusieurs appareils ensemble, mais ils fonctionnent de manière fondamentalement différente. La différence entre un hub et un switch réside dans leur fonctionnalité et leurs capacités.

- Un hub est un dispositif réseau de la couche physique (couche 1 du modèle OSI). Il agit essentiellement comme un répétiteur passif. Lorsqu'un appareil envoie des données à travers un hub, le hub diffuse ces données à tous les ports connectés, quelle que soit la destination réelle. Cela signifie que tous les appareils connectés au hub reçoivent les données, mais seuls ceux avec l'adresse MAC de destination appropriée les acceptent.

- Un switch, en revanche, est un dispositif de la couche de liaison de données (couche 2 du modèle OSI). Il est beaucoup plus intelligent qu'un hub. Un switch maintient une table de correspondance d'adresses MAC (table CAM) qui répertorie les adresses MAC des appareils connectés à ses ports. Lorsqu'un appareil envoie des données à travers un switch, celui-ci utilise cette table pour acheminer les données uniquement vers le port auquel l'appareil de destination est connecté. Cela limite le trafic inutile sur le réseau, améliorant ainsi l'efficacité et la sécurité.

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

Un hub est un dispositif réseau très simple qui fonctionne au niveau physique (couche 1 du modèle OSI). Voici comment il fonctionne, ainsi que ses avantages et inconvénients :

Lorsqu'un hub reçoit des données sur l'un de ses ports, il répète simplement ces données sur tous les autres ports. Il ne prend pas de décision sur la destination des données ni ne maintient de table d'adresses.

Les avantages :

Les hubs sont extrêmement simples et peu coûteux à fabriquer, ce qui les rend accessibles pour les petits réseaux.

Ils sont compatibles avec tous les types d'appareils réseau, car ils se contentent de répéter les signaux.

Les inconvénients :

L'un des principaux inconvénients des hubs est leur inefficacité. En diffusant les données sur tous les ports, ils génèrent du trafic inutile et provoquent une congestion sur le réseau.

Étant donné que les données sont diffusées à tous les appareils connectés, un hub offre peu de sécurité. Tout appareil peut écouter le trafic des autres, ce qui le rend vulnérable aux écoutes indiscrètes.

Les hubs ne détectent pas les collisions de données (lorsque deux appareils envoient des données simultanément), ce qui peut entraîner des perturbations sur le réseau.

Les hubs sont largement obsolètes aujourd'hui, car les commutateurs (switches) sont devenus la norme en raison de leur efficacité et de leurs fonctionnalités avancées.

Quels sont les avantages et inconvénients d’un switch ?

Les switches sont des dispositifs de réseau qui offrent de nombreux avantages par rapport aux hubs. Voici les avantages et les inconvénients des switches :

Les avantages :

Les switches acheminent les données uniquement vers le port approprié en fonction de l'adresse MAC de destination.

Cela élimine la diffusion inutile de données sur tous les ports, ce qui rend le réseau plus rapide et plus efficace.

Parce qu'ils envoient des données uniquement au port de destination correct, les switches offrent une sécurité accrue. Les appareils ne reçoivent que les données qui leur sont destinées, ce qui empêche l'écoute indiscrète du trafic.

Les switches offrent souvent des fonctionnalités de gestion avancées, telles que la surveillance du trafic, la configuration de la qualité de service (QoS), et la prise en charge de VLAN (Virtual Local Area Network) pour segmenter le réseau en groupes logiques.

En raison de leur efficacité, les switches offrent de meilleures performances que les hubs. Ils sont adaptés aux réseaux exigeants en termes de bande passante.

Les switches évitent les collisions de données, car ils acheminent intelligemment le trafic vers son destinataire, améliorant ainsi la stabilité du réseau.

Les inconvénients :

Les switches sont plus coûteux que les hubs en raison de leurs fonctionnalités avancées. Cependant, les coûts ont considérablement diminué au fil du temps.

Les switches peuvent être plus complexes à configurer et à gérer en raison de leurs fonctionnalités avancées. Ils nécessitent des compétences techniques pour une utilisation optimale.

Les switches consomment généralement plus d'énergie que les hubs en raison de leur traitement plus avancé du trafic.

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

Un switch gère le trafic réseau de manière intelligente en utilisant des informations sur les adresses MAC (Media Access Control) des appareils connectés à ses ports. Voici comment un switch gère le trafic réseau :

Lorsqu'un appareil est connecté à un port du switch, le switch enregistre l'adresse MAC de cet appareil dans sa table de correspondance d'adresses MAC, également appelée table CAM (Content Addressable Memory). Cette table indique à quel port se trouve chaque adresse MAC connue.

Lorsqu'un appareil connecté à un port du switch envoie des données, le switch examine l'adresse MAC de destination de ces données. En se basant sur la table CAM, le switch détermine à quel port l'appareil de destination est connecté.

Le switch achemine ensuite les données uniquement vers le port où se trouve l'appareil de destination. Cela évite la diffusion de données inutiles sur tous les ports, améliorant ainsi l'efficacité et la sécurité du réseau.

Le switch met régulièrement à jour sa table CAM pour refléter les changements dans le réseau, tels que la déconnexion ou la connexion de nouveaux appareils. Ainsi, il maintient une vue précise de la topologie du réseau.

En acheminant le trafic uniquement vers le port de destination, le switch réduit les risques de collisions de données, ce qui améliore la stabilité du réseau.

Certains switches offrent des fonctionnalités de QoS permettant de prioriser le trafic en fonction de certaines règles, garantissant ainsi que les données sensibles, comme la voix sur IP, sont traitées en priorité.

Job 9 :

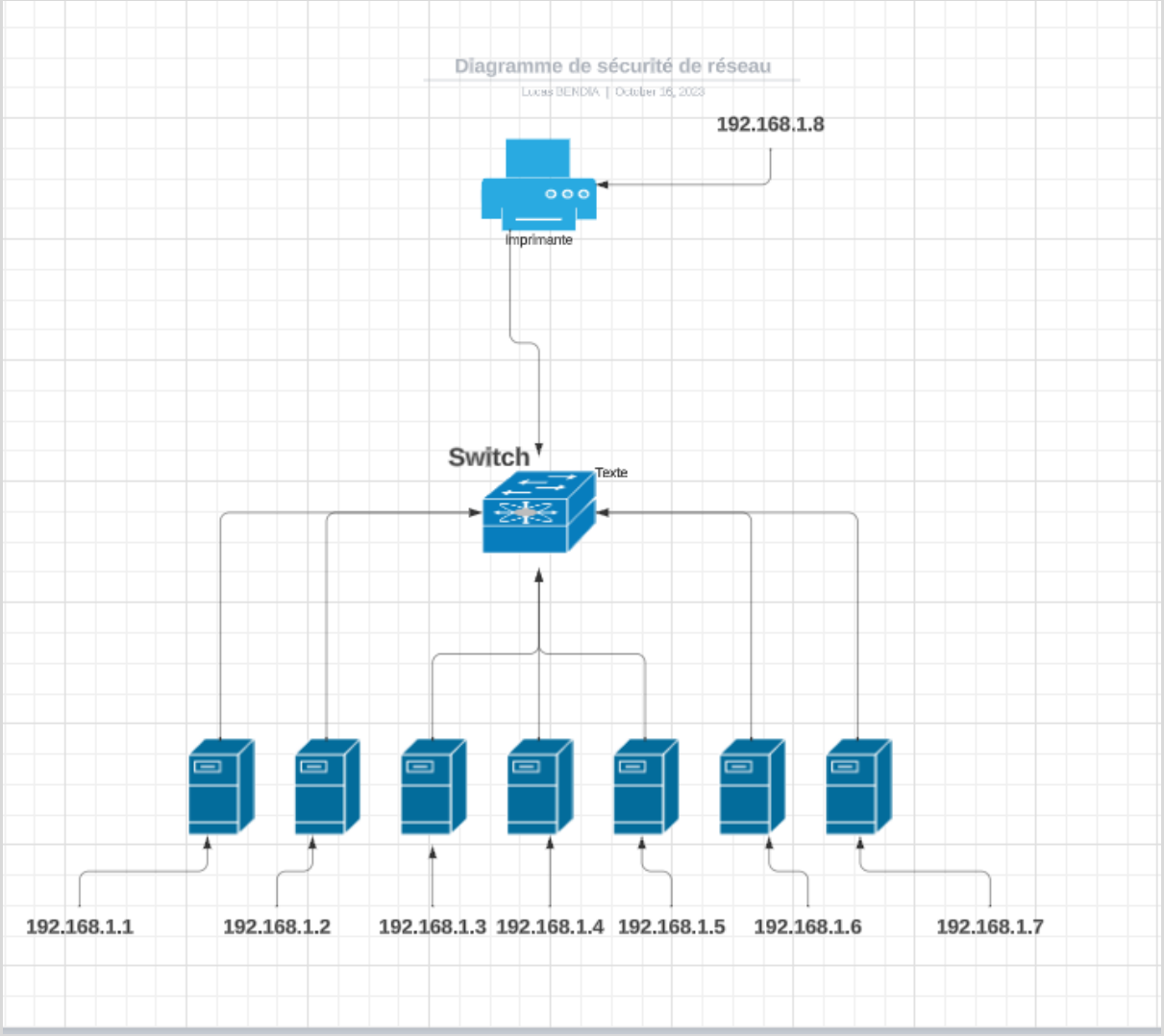
L'imprimante est bien relié au switch :

```
Pinging 192.168.1.8 with 32 bytes of data:

Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time=6ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

Schéma :



Les avantages importants à le faire de manière appropriée. Voici trois avantages :

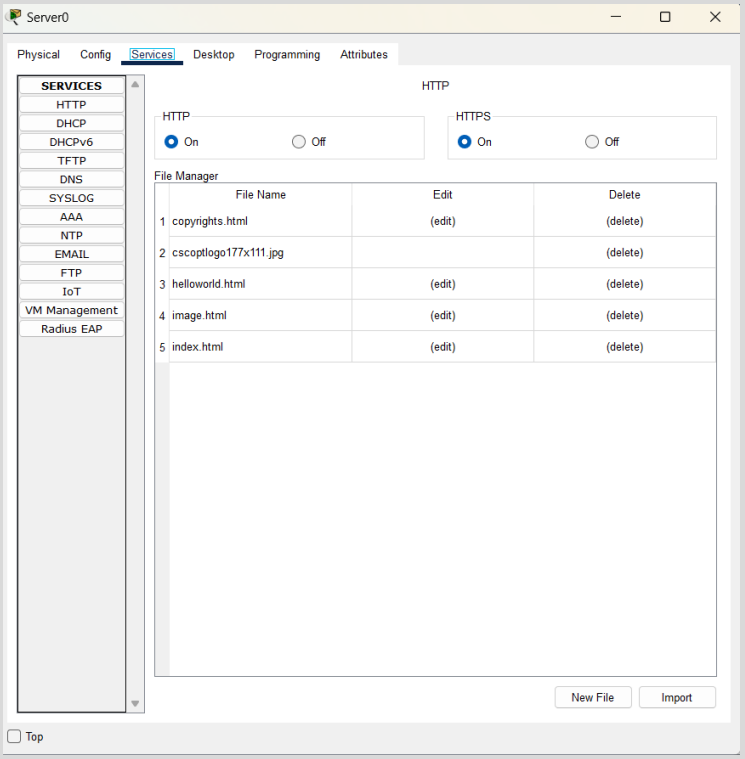
Un schéma réseau bien conçu permet une gestion plus efficace du réseau. Il fournit une vue d'ensemble des appareils, des connexions et des adresses IP, ce qui facilite la surveillance, la maintenance et la planification de la croissance du réseau. Cela permet également de diagnostiquer et de résoudre plus rapidement les problèmes réseau.

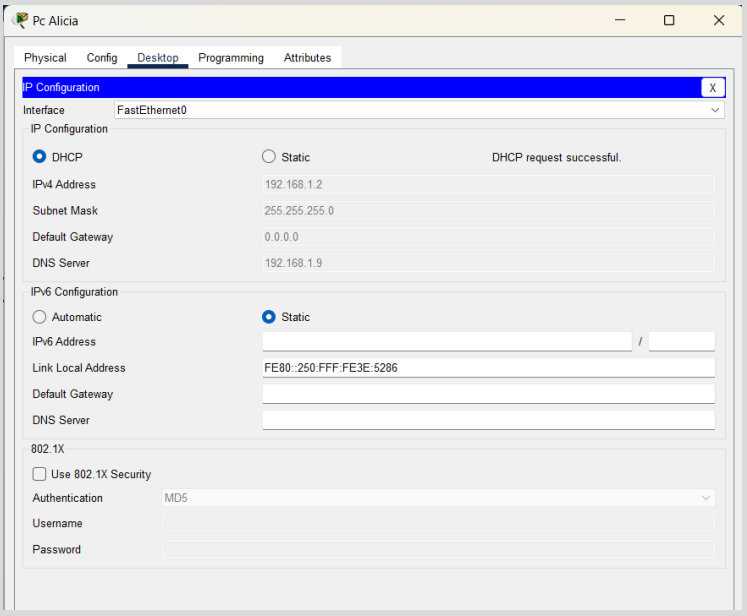
Un schéma réseau aide à identifier clairement les zones de sécurité et les zones à risque. Il facilite la mise en place de pare-feu, de contrôles d'accès et d'autres mesures de sécurité ciblées. En comprenant la topologie du réseau, les administrateurs peuvent mieux protéger les données et les ressources essentielles.

Un schéma réseau bien conçu permet d'optimiser les performances en identifiant les goulets d'étranglement potentiels et en planifiant l'allocation de la bande passante. Cela garantit que le trafic est acheminé efficacement et que les utilisateurs bénéficient de performances optimales, réduisant ainsi les retards et les ralentissements

Job 10 :

Les étapes que j’ai effectué pour utiliser DHCP pour un pc :





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

Les adresses IP statiques et les adresses IP attribuées par DHCP (Dynamic Host Configuration Protocol) sont deux méthodes de configuration des adresses IP sur un réseau. Voici leurs principales différences :

Adresse IP statique:

Dans le cas d'une adresse IP statique, l'administrateur réseau configure manuellement l'adresse IP sur chaque appareil du réseau. Cela signifie qu'une adresse IP spécifique est fixe et ne change pas, sauf si elle est modifiée manuellement.

Les adresses IP statiques sont prévisibles, ce qui facilite la gestion et le dépannage, car les adresses restent constantes.

Les adresses IP statiques sont couramment utilisées pour les serveurs, les équipements réseau, et d'autres appareils nécessitant une adresse IP constante.

Adresse IP attribuée par DHCP :

Avec DHCP, les adresses IP sont attribuées automatiquement par un serveur DHCP au moment de la connexion à un réseau. Le serveur DHCP peut également fournir d'autres informations de configuration réseau, telles que les adresses de passerelle et de serveur DNS.

Les adresses IP attribuées par DHCP sont dynamiques, ce qui signifie qu'elles peuvent changer à chaque connexion ou après un certain temps d'inactivité. Cela permet d'optimiser l'utilisation des adresses IP, en particulier dans les réseaux avec de nombreux appareils temporaires.

DHCP simplifie la gestion des adresses IP en centralisant le processus d'attribution. Il permet également de gérer plus efficacement les plages d'adresses IP disponibles.

Job 11 :

Méthode Luc :

RESEAU	Hotes	Adresse IP de depart	Adresse IP de fin	Masque sous reseau
principal 21	(+2 car on compte le 0 et le 1)	10.0.0.0		255.255.0.0
Sous reseau 1	12 hotes	10.1.0.1	10.1.0.14	255.255.255.240
sous reseau 5	30 hotes	10.2.0.1	10.2.0.32	255.255.255.224
		10.3.0.1	10.3.0.32	
		10.4.0.1	10.4.0.32	
		10.5.0.1	10.5.0.32	
		10.6.0.1	10.6.0.32	
sous reseau 5	120 hotes	10.7.0.1	10.7.0.122	255.255.255.128
		10.8.0.1	10.7.0.122	
		10.9.0.1	10.7.0.122	
		10.10.0.1	10.8.0.122	
		10.11.0.1	10.11.0.122	
sous reseau 5	160 hotes	10.12.0.1	10.12.0.162	255.255.255.0
		10.13.0.1	10.13.0.162	
		10.14.0.1	10.14.0.162	
		10.15.0.1	10.15.0.162	
		10.16.0.1	10.16.0.162	

Méthode Nadir :

RESEAU	Hotes	Gateway	Pool Adresses	Broadcast	Masque sous reseau
Sous reseau 1	12 hotes	10.0.0.0	10.0.0.1 - 10.0.0,14	10.0.0.15	255.255.255.240 / 28
sous reseau 5	30 hotes	10.0.0.16	10.0.0.17 - 10.0.0.46	10.0.0.47	255.255.255.224 / 27
		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 reseau 5	120 hotes	10.0.0.176	10.0.0.177 - 10.0.1.46	10.0.1.47	255.255.255.128 /25
		10.0.1.48	10.0.1.49 - 10.0.1.174	10.0.1.175	
		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	10.0.2.176 - 10.0.2.46	10.0.3.47	
sous reseau 5	160 hotes	10.0.3.48	10.0.3.49 - 10.0.4.49	10.0.4.47	255.255.255.0 / 24
		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 ?

L'adresse IP 10.0.0.0 a été choisie pour représenter une adresse de classe A dans le système d'adressage IP. Les adresses de classe A sont généralement utilisées pour les réseaux de grande taille, car elles offrent un grand nombre d'adresses disponibles. L'adresse 10.0.0.0 est le début de la plage d'adresses de classe A, ce qui signifie qu'elle peut être utilisée pour créer de nombreux sous-réseaux et héberger un grand nombre d'appareils connectés. Cependant, il est important de noter que le choix d'une adresse spécifique dépend des besoins et des exigences du réseau en question.

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

Voici les différents types d'adressage :

Entre 0 et 127 inclus : Classe A.
Entre 128 et 191 inclus : Classe B.
Entre 192 et 223 inclus : Classe C.
Entre 224 et 239 inclus : Classe D.
Entre 240 et 255 inclus : Classe E.

Job 12 :

		Outils	
Donnée	**7 - Application** point d'accès aux services réseau	-FTP	
Donnée	**6 - Présentation** conversion et chiffrement des données	-HTML	
Donnée	**5 - Session** communication interhost		
Segment	**4 - Transport**	-TCP	

	Connexion de bout en bout et contrôle de flux (TCP)	-UDP -SSL/TLS	
Paquet	**3 - Réseau** Détermine le parcours et l'adressage logique (IP)	-IPv4 -IPv6	
Trame	**2 - Liaison** Adressage physique (MAC et LLC)	-MAC -Wi-Fi -Ethernet -Routeur -PPTP	
Bit	**1 - Physique** Transmission binaire numérique ou analogique	-Fibre optique -cable RJ45.	

Job 13 :

Quelle est l'architecture de ce réseau ?

L'architecture de réseau et on LAN filière

Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est un réseau de class C car elle commence par "192" l'adresse du reseau principal est 192.168.10.0

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

Le nombre de machines que l'on peut brancher est definis grace au masque de sous reseau qui est 255.255.255.0 etant donner que l'adresse ip 192.168.10.0 est l'adresse de diffusion on ne la prend pas en compte ce qui fait que l'on peut prendre en charge 254 machines.

Quelle est l'adresse de diffusion de ce réseau ?

L'adresse IP du réseau de diffusion est de 192.168.10.255

Job 14 :

Convertir ces IP en binaire :

145.32.59.24 = binaire 10010001.00100000.00111011.00011000
200.42.129.16 = binaire 11001000.00101010.10000001.00010000
14.82.19.54 = binaire 00001110.01010010.00010011.00110110

Job 15 :

Qu’est-ce que le routage ?

Le routage est le processus par lequel les données sont acheminées à travers un réseau informatique. Il s'agit essentiellement de déterminer le chemin optimal pour que les paquets de données atteignent leur destination. Les routeurs, qui sont des dispositifs réseau spéciaux, jouent un rôle clé dans le routage en analysant les adresses IP des paquets de données et en les transférant vers le prochain nœud du réseau qui les rapproche de leur destination finale. Le routage permet de connecter différents réseaux entre eux, qu'il s'agisse de réseaux locaux (LAN) ou de réseaux étendus (WAN), en assurant un transfert efficace et fiable des données. Cela permet aux utilisateurs d'accéder à des ressources distantes et de communiquer avec d'autres appareils connectés sur le réseau.

Qu’est-ce qu’un gateway ?

En informatique, un "gateway" (ou passerelle en français) est un dispositif ou un logiciel qui agit comme une interface entre deux réseaux informatiques distincts. Il peut être utilisé pour relier des réseaux qui utilisent différents protocoles de communication ou qui fonctionnent à des niveaux différents. Les gateways sont utilisés pour permettre la communication et l'échange de données entre ces réseaux, même s'ils ont des configurations différentes.

Qu’est-ce qu’un VPN ?

VPN est l’abréviation de « virtual private network » (réseau privé virtuel). Il s’agit d’un service qui vous aide à préserver votre confidentialité en ligne en chiffrant la connexion entre votre appareil et Internet. Cette connexion sécurisée fournit un tunnel privé pour vos données et communications lorsque vous utilisez des réseaux publics.

Qu’est-ce qu’un DNS ?

Le DNS (Domain Name System) est un système fondamental sur Internet qui permet de traduire les noms de domaine conviviaux que nous utilisons pour naviguer sur le Web en adresses IP numériques que les ordinateurs utilisent pour identifier chaque autre appareil connecté au réseau. En termes simples, le DNS est comme un annuaire téléphonique d'Internet.