

JOB 2 :

Qu'est-ce qu'un réseau ?

- Un réseau est un système de dispositifs interconnectés qui communiquent pour partager des informations et des ressources, allant des réseaux locaux (LAN) dans un bureau aux réseaux étendus (WAN) couvrant de vastes régions géographiques. Ces réseaux facilitent la communication, le partage de données et d'autres services essentiels.

À quoi sert un réseau informatique ?

- Un réseau informatique sert à connecter des dispositifs pour partager des données, des ressources et des services, améliorant la communication, la productivité et l'accès à l'information.

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

- Pour mettre en place un réseau informatique fonctionnel, vous aurez besoin d'une variété de composants essentiels. Les ordinateurs, en tant qu'acteurs principaux, génèrent et traitent les données, tandis que les cartes réseau leur permettent de se connecter au réseau. Les câbles réseau, tels que les câbles Ethernet (câbles RJ45), assurent le transport des données entre les ordinateurs. Les switchs jouent un rôle crucial en reliant plusieurs ordinateurs, dirigeant les données vers les ports appropriés pour créer un réseau local efficace. Enfin, les routeurs permettent de connecter différents réseaux, facilitant ainsi la communication entre eux et offrant un accès aux réseaux étendus, comme Internet. En combinant ces composants, vous établissez un réseau capable de répondre à divers besoins de communication et d'accès aux ressources.

JOB 3 :

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

- J'ai choisi le câble croisé, il permet un meilleur échange des données

JOB 4 :

Qu'est-ce qu'une adresse IP ?

- Une adresse IP est une étiquette numérique attribuée à chaque appareil sur un réseau, permettant de les identifier et de les connecter. Cela facilite le routage des données sur Internet et les réseaux locaux. Les deux versions principales sont IPv4 et IPv6.

À quoi sert un IP ?

- Une adresse IP sert à identifier un appareil sur un réseau et à diriger les données vers leur destination, que ce soit sur Internet ou en réseau local.

Qu'est-ce qu'une adresse MAC ?

- Une adresse MAC est une adresse matérielle unique attribuée à chaque carte réseau d'un appareil et utilisée pour l'identifier sur un réseau local.

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

- Une adresse IP publique est celle utilisée sur Internet pour identifier un réseau ou un dispositif. Une adresse IP privée est utilisée en interne, au sein d'un réseau local, et n'est pas directement accessible depuis Internet. Les adresses privées sont traduites en une seule adresse publique pour accéder à Internet, via la NAT.

Quelle est l'adresse de ce réseau ?

- L'adresse de ce réseau est 255.255.255.0

JOB 5 :

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

- J'ai utiliser la commande **ipconfig**

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::230:F2FF:FE64:7E99
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0
```

```
FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:70FF:FE68:6B0B
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0
```

JOB 6 :

Quelle est la commande permettant de Ping entre des PC ?

- J'ai utiliser la commande **ping (adresse IP)**

```
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=4ms TTL=128
```

JOB 7 :

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
```

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

- Non, le PC de Pierre n'a pas reçu les paquets envoyés par Alicia.

Expliquez pourquoi.

- L'ordinateur de Pierre n'a reçu aucun paquet car il est éteint et sa carte réseau ne fonctionne pas car elle n'est pas en marche.

JOB 8 :

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.7: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.8: bytes=32 time=19ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.7: bytes=32 time=1ms TTL=128
Reply from 192.168.1.8: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=14ms TTL=128
Reply from 192.168.1.4: bytes=32 time=14ms TTL=128
Reply from 192.168.1.5: bytes=32 time=14ms TTL=128
Reply from 192.168.1.6: bytes=32 time=14ms TTL=128
Reply from 192.168.1.7: bytes=32 time=14ms TTL=128
Reply from 192.168.1.8: bytes=32 time=14ms TTL=128
Reply from 192.168.1.2: bytes=32 time=14ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 28, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

Les machines sont bien connectées et appartiennent au même réseau, grâce à un ping sur l'adresse IP de diffusion nous pouvons voir toutes les machines connectées.

Quelle est la différence entre un hub et un switch ?

- La grande 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 commutateur effectue un tri des trames afin de les orienter vers le bon port et donc vers le bon équipement.

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

- Lorsqu'un hub reçoit des données, il transfère l'intégralité de celles-ci à tous les appareils connectés (ou hôtes) sur le mode du semi-duplex. Tous les raccordements (ou ports) d'un hub fonctionnent à la même vitesse et se trouvent dans un même domaine de collision (regroupant tous les appareils connectés en réseau). Contrairement à d'autres périphériques réseau, un hub ne permet pas de cibler ou d'exclure uniquement certains de ces récepteurs. En cas de transfert, tous les paquets sont invariablement transmis à l'ensemble des ordinateurs. Tous les appareils reçoivent donc le paquet de données en question, même si celui-ci ne leur est pas initialement destiné. Étant donné que tous les hôtes sont occupés par ce transfert, aucun autre appareil ne peut envoyer de données tant que ce processus est en cours. Les demandes simultanées sont donc traitées les unes après les autres.
- La technologie qui se cache derrière les hubs est donc considérée comme étant vulnérable et obsolète. En plus de la perte de vitesse mentionnée ci-dessus et du manque de flexibilité relatif au transfert de données et à la sélection des récepteurs, un système de hubs est souvent assez vulnérable face aux failles de sécurité. Comme un tel système ne peut être mis en quarantaine, le trafic de données n'est pas protégé. Les potentiels problèmes de sécurité ou les éventuelles préoccupations liées à la protection des données concernent forcément tous les hôtes connectés.

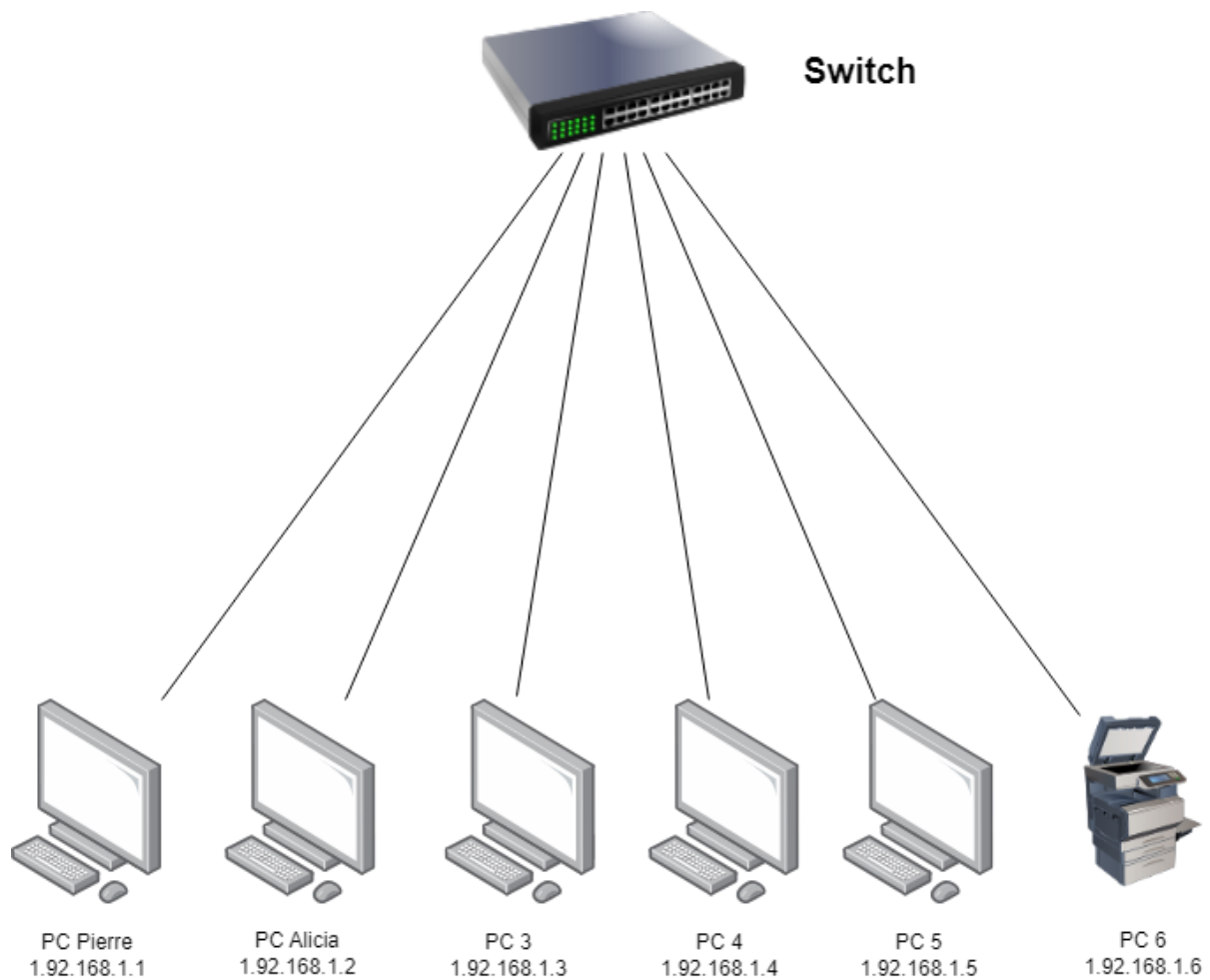
Quels sont les avantages et inconvénients d'une switch ?

- Le switch présente plusieurs avantages dans la gestion de votre parc informatique. Il contribue à la sécurité du réseau et à la protection des données échangées via le réseau. D'autre part, il permet de connecter davantage de postes de travail sur le même réseau Ethernet.
- Bien que les switch présentent de nombreux avantages, ils présentent également certains inconvénients. L'un des principaux inconvénients est qu'ils peuvent être plus chers que les hubs. À mesure que la technologie progresse, les prix ont baissé, mais les switch peuvent néanmoins être plus chers que les hubs.

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

- Un switch gère le trafic réseau en utilisant des adresses MAC pour acheminer les données vers leurs destinations. Il maintient une table de correspondance des adresses MAC, et lorsqu'il reçoit un paquet, il le dirige vers le port approprié en fonction de cette table. Si l'adresse de destination est inconnue, il diffuse le paquet à tous les ports sauf celui d'origine. Le switch met à jour sa table au fur et à mesure que les périphériques se connectent et se déconnectent, assurant un trafic réseau efficace.

JOB 9 :



Intégrer des schémas dans la documentation offre de nombreux atouts, parmi lesquels une communication plus claire, une simplification de la compréhension des concepts complexes, et une mise en ordre visuelle des idées. Les schémas facilitent la communication en transcendant les barrières linguistiques et contribuent à structurer de manière efficace l'information.

JOB 10 :

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

- Une adresse IP statique est définie manuellement et reste la même, tandis qu'une adresse IP attribuée par DHCP est assignée automatiquement par un serveur et peut changer.

JOB 11 :

	.1 sous-réseau de 12 hôtes	5 sous-réseaux de 30 hôtes	5 sous-réseaux de 120 hôtes	5 sous-réseaux de 160 hôtes
Masque de sous-réseaux	255.255.255.24 0	255.255.255.19 2	255.255.255.12 8	255.255.255.0
Plages d'adresses	10.1.0.0 à 10.1.0.14	de 10.2.0.0 à 10.2.0.31 de 10.3.0.0 à 10.3.0.31 de 10.4.0.0 à 10.4.0.31 de 10.5.0.0 à 10.5.0.31 de 10.6.0.0 à 10.6.0.31	de 10.7.0.0 à 10.7.0.121 de 10.8.0.0 à 10.8.0.121 de 10.9.0.0 à 10.9.0.121 de 10.10.0.0 à 10.10.0.121 de 10.11.0.0 à 10.11.0.121	de 10.12.0.0 à 10.12.0.161 de 10.13.0.0 à 10.13.0.161 de 10.14.0.0 à 10.14.0.161 de 10.15.0.0 à 10.15.0.161 de 10.16.0.0 à 10.16.0.161

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

- L'adresse de classe A 10.0.0.0 a été choisie pour sa capacité à créer de multiples sous réseaux

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

- Les diverses catégories d'adresses se distinguent par leur portée et leur fonction au sein des réseaux informatiques. Les adresses IP publiques, par exemple, ont pour vocation l'identification unique des appareils sur Internet, favorisant ainsi les échanges à l'échelle mondiale. À l'inverse, les adresses IP privées servent à identifier les appareils au sein de réseaux locaux (LAN) et ne sont pas destinées à être routées sur Internet, ce qui les rend courantes dans de nombreux réseaux locaux. Les adresses IP réservées, quant à elles, possèdent des usages spécifiques, comme l'exemple de l'adresse 127.0.0.1 dédiée au bouclage local.
-
- Les adresses MAC (Media Access Control) sont responsables de l'identification physique des cartes réseau au sein d'un réseau local, tandis que les adresses de diffusion sont employées pour diffuser des données à l'ensemble des appareils d'un réseau donné. Chacune de ces catégories d'adresses remplit un rôle distinct dans les communications réseau, adapté à la portée et à l'utilisation requises.
-

JOB 12 :

Couche de l'OSI	Description des rôles	Protocols / Matériels
Couche 7 (Application)	La couche application est la couche supérieure du modèle OSI et interagit directement avec les applications utilisées par les utilisateurs. Elle fournit des services de communication aux applications, comme l'accès aux ressources réseau, l'authentification, la gestion des sessions, et la présentation des données à l'utilisateur.	HTML, FTP, PPTP, SSL/TLS
Couche 6 (Présentation)	Cette couche est responsable de la traduction, de la compression et du chiffrement des données pour garantir que les applications sur différents dispositifs puissent interpréter les informations correctement. Elle s'occupe également de la gestion des jeux de caractères et de la syntaxe des données.	SSL/TLS, HTML
Couche 5 (Session)	La couche de session établit, maintient et termine les sessions de communication entre les applications sur des dispositifs différents. Elle gère la synchronisation, le contrôle des dialogues et la reprise après panne.	PPTP, FTP, SSL/TLS

Couche 4 (Transport)	Cette couche assure la communication de bout en bout entre les applications sur différents appareils. Elle divise les données en segments, gère le contrôle de flux, la correction d'erreurs, et la séquence des données. Le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol) sont couramment utilisés à ce niveau.	TCP, UDP
Couche 3 (Réseau)	La couche réseau est chargée du routage des données à travers le réseau. Elle détermine le meilleur chemin pour les données en fonction des adresses logiques (généralement des adresses IP). Les routeurs opèrent à ce niveau.	IPv4, IPv6, routeur
Couche 2 (Liaison de données)	Cette couche assure la fiabilité de la transmission des données entre deux nœuds adjacents sur le réseau. Elle effectue la détection et la correction d'erreurs, organise les données en trames et gère l'accès au support partagé. Les commutateurs opèrent principalement à ce niveau.	Ethernet, MAC, Wi-Fi, câble RJ45

Couche 1 (Physique)	Cette couche est responsable de la transmission des bits bruts sur un support physique, comme des câbles ou des signaux sans fil. Elle définit les caractéristiques physiques du support, telles que la tension, la fréquence, et la topologie du réseau.	Fibre optique, câble RJ45
---------------------	---	---------------------------

JOB 13 :

Quelle est l'architecture de ce réseau ?

- Ce réseau est construit sur une architecture IP de classe C, utilisant l'adresse 192.168.10.0, avec une topologie en étoile, et un masque de sous-réseau de 255.255.255.0.

Indiquer quelle est l'adresse IP du réseau ?

- L'adresse IP de réseau est 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, notre réseau présente une plage d'adresses allant de 192.168.10.0 à 192.168.10.255. Cependant, il convient de noter que les adresses réseau 192.168.10.0 et de diffusion 192.168.10.255 ne sont pas attribuées aux appareils. Cela signifie que les adresses IP peuvent être assignées aux hôtes dans la plage de 192.168.10.1 à 192.168.10.254, ce qui permet de connecter jusqu'à 254 machines au réseau.

Quelle est l'adresse de diffusion de ce réseau ?

- L'adresse de diffusion de ce réseau est 192.168.10.255, ce qui implique que tout message envoyé à cette adresse sera diffusé à l'ensemble des machines du réseau.

JOB 14 :

145.32.59.24 = 10010001.00111011.00011000

200.42.129.16 = 11001000.00101010.10000001.00010000

14.82.19.54 = 00001110.01010010.00110110

JOB 15 :

Qu'est-ce que le routage ?

- Le routage est le processus de transmission de données d'un point source à un point de destination à travers un réseau en utilisant des dispositifs tels que des routeurs pour déterminer le meilleur chemin.

Qu'est-ce qu'un gateway ?

- Une gateway est un dispositif qui relie et facilite la communication entre deux réseaux informatiques différents, permettant le transfert de données entre eux.

Qu'est-ce qu'un VPN ?

- Un VPN est un réseau privé virtuel qui chiffre et sécurise votre connexion Internet, masque votre adresse IP et vous permet d'accéder à Internet de manière anonyme et sécurisée.

Qu'est-ce qu'un DNS ?

- Un DNS est un système qui traduit les noms de domaine en adresses IP, permettant aux utilisateurs d'accéder aux sites web en utilisant des noms au lieu de chiffres.