

Runtrack réseau

JOB 2 :

Qu'est-ce qu'un réseau ? Un réseau est une structure interconnectée permettant la communication et le partage d'informations ou de ressources entre différents points. En informatique, un réseau se réfère à un ensemble de dispositifs et de connexions permettant à des ordinateurs et à d'autres appareils de communiquer et de partager des ressources, qu'il s'agisse de réseaux locaux (LAN), étendus (WAN), de stockage (SAN) ou sans fil (WLAN). Ces réseaux impliquent des infrastructures telles que des commutateurs, des routeurs, des serveurs, des câbles et des logiciels de gestion, et peuvent être privés ou publics, comme Internet.

À quoi sert un réseau informatique ? Un réseau informatique permet la communication, le partage de ressources et de données entre les ordinateurs et appareils connectés. Il favorise la collaboration, facilite l'accès à distance aux données et offre un stockage centralisé pour une gestion efficace des informations au sein d'une organisation ou d'un groupe d'utilisateurs.

Quel matériel avons-nous besoin pour construire un réseau ?

Détaillez les fonctions de chaque pièce. : Pour construire un réseau informatique, vous aurez besoin de plusieurs composants matériels essentiels. Voici les principaux composants nécessaires et leurs fonctions respectives:

1 - Modem : Permet de se connecter à Internet via une ligne téléphonique, un câble coaxial ou une connexion sans fil. Il convertit le signal numérique en signal compréhensible pour les appareils connectés.

2 - Routeur : Dirige le trafic réseau entre les appareils et les réseaux. Il fournit également une passerelle vers Internet, permettant aux appareils de se connecter à d'autres réseaux et à Internet.

3 - Commutateur (Switch) : Il permet de relier plusieurs appareils au sein d'un même réseau local (LAN) en acheminant les données vers les appareils

destinataires. Il fournit une communication directe entre les appareils connectés.

4 - Point d'accès sans fil (WAP) : Fournit une connexion sans fil au réseau pour les appareils compatibles Wi-Fi. Il permet aux appareils tels que les ordinateurs portables, les smartphones et les tablettes de se connecter au réseau sans l'utilisation de câbles.

5 - Carte réseau (NIC) : Installée sur chaque appareil, elle permet à l'ordinateur ou à l'appareil de se connecter physiquement au réseau. Elle permet la communication entre l'appareil et le réseau auquel il est connecté.

6 - Câbles réseau : Les câbles Ethernet sont utilisés pour connecter les appareils au réseau. Ils assurent la transmission rapide et fiable des données entre les appareils connectés.

7 - Firewall (pare-feu) : Il sécurise le réseau en surveillant et en contrôlant le trafic entrant et sortant. Il protège le réseau des menaces potentielles en bloquant les accès non autorisés.

8 - Serveur: Fournit des services, des données ou des ressources à d'autres appareils du réseau. Il peut être un serveur de fichiers pour le stockage centralisé, un serveur d'impression pour la gestion des impressions ou un serveur d'applications pour héberger des applications logicielles.

9 - Modem/routeur sans fil : Combine les fonctionnalités d'un modem et d'un routeur, tout en fournissant une connectivité sans fil pour les appareils compatibles Wi-Fi.

En utilisant ces composants, on peut construire un réseau informatique fiable et fonctionnel, adapté aux besoins spécifiques de l'environnement ou l'organisation.

Job 3:

Quels Câbles avez-vous choisis pour relier les deux ordinateurs ?

Expliquez votre choix. Le câble que j'ai choisi est le A.C.C.T, car il est le plus simple à se connecter pour une personne lambda.

Job 4:

1 - Qu'est-ce qu'une adresse IP ? Une adresse IP (Internet Protocol) est une étiquette numérique attribuée à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet pour la communication.

2 - À quoi sert un IP ? Une adresse IP (protocole Internet) est utilisée pour identifier de manière unique un appareil sur un réseau, permettant ainsi le routage des données vers la bonne destination.

3 - Qu'est-ce qu'une adresse MAC ? Une adresse MAC (Media Access Control) est un identifiant unique attribué à une carte réseau pour les appareils connectés à un réseau informatique. Elle est utilisée au niveau de la couche de liaison de données dans les protocoles de communication réseau.

4 - Qu'est-ce qu'une IP publique et privée ? Une adresse IP publique est une adresse unique attribuée à un appareil sur un réseau internet mondial, permettant à cet appareil d'être identifié et de communiquer avec d'autres appareils sur Internet.

Une adresse IP privée est utilisée à l'intérieur d'un réseau local pour identifier les appareils individuels au sein de ce réseau. Les adresses IP privées ne sont pas routables sur Internet et servent principalement à la communication au sein d'un réseau local.

5 - Quelle est l'adresse de ce réseau ?

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::20C:85FF:FEA3:935B
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   0.0.0.0
```

Job 5:

L'IP De Pierre

```

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::20C:85FF:FEA3:935B
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.1
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                        0.0.0.0

```

L'IP D'Alicia

```

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::2E0:B0FF:FEB3:6BC3
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.2
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                        0.0.0.0

```

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

La commande que j'ai utilisé est "ipconfig" et cette commande a pour but de vérifier le réseau des machines.

Job 6:

Ping exécutez sur PC Pierre & Pc Alicia

```

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
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms 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 = 2ms, Maximum = 4ms, Average = 2ms

```

```

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=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms 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 = 2ms, Maximum = 2ms, Average = 2ms

```

Quelle est la commande permettant de Ping entre des PC ?

Du Pc de Pierre je me suis servie de L'IPv4 D'Alicia

Du Pc D'Alicia je me suis servie de L'IPv4 De Pierre.

Grâce à la commande "**Ping**"

Job 7:

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

Non il l'est à pas reçu.

Expliquez pourquoi.

Non, le PC de Pierre n'a probablement pas reçu les paquets envoyés par Alicia, car il était éteint au moment de l'envoi des paquets. Cette absence de réponse est attendue lorsque le PC cible est hors tension.

Il est important de noter que pour que les paquets ICMP soient reçus avec succès, le PC cible doit être en ligne et fonctionnel, prêt à répondre aux requêtes réseau.

Job 8:

Quelle est la différence entre un hub et un switch ?

Un hub transmet les données à tous les ports, provoquant une congestion du réseau,

tandis qu'un switch achemine les données spécifiquement vers le port destinataire, améliorant ainsi l'efficacité du réseau. De plus, un switch offre une meilleure sécurité et segmentation du réseau, mais il est plus coûteux qu'un hub en raison de ses fonctionnalités de gestion avancées et de sa meilleure performance.

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

Un hub fonctionne en répliquant les données reçues sur tous ses ports connectés, ce qui signifie que toutes les données sont transmises à tous les appareils connectés au hub.

Avantages :

- Moins coûteux que les switches.
- Facile à installer et à utiliser.
- Utile pour les réseaux de petite taille.

Inconvénients :

- Peut entraîner une congestion du réseau car il transmet les données à tous les ports.
- Ne fournit pas de sécurité intégrée ou de segmentation de réseau.
- Moins efficace que les switches en termes de gestion du trafic.

Quels sont les avantages et inconvénients d'un switch ?

switch :

Avantages :

- Achemine les données spécifiquement vers le port destinataire, améliorant ainsi l'efficacité du réseau.
- Offre une meilleure sécurité en isolant le trafic vers des ports spécifiques.
- Permet une segmentation de réseau plus efficace.
- Gère plus efficacement le trafic par rapport à un hub.

Inconvénients :

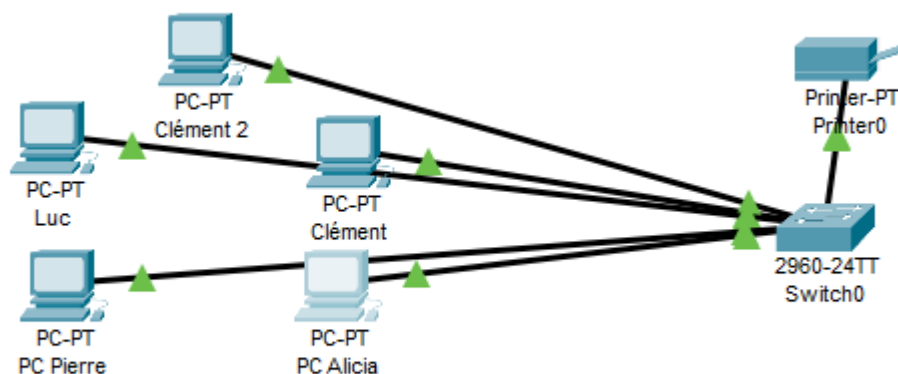
- Plus coûteux que les hubs en raison de ses fonctionnalités de gestion avancées.
- Peut nécessiter une configuration et une gestion plus complexes.
- Peut être surdimensionné pour les réseaux de petite taille ou peu complexes.

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 les ports spécifiques auxquels les appareils sont connectés. Il maintient une table de correspondance des adresses MAC des appareils connectés à chaque port, ce qui lui permet de transmettre les données uniquement aux destinataires appropriés, évitant ainsi la congestion du réseau. Cela améliore l'efficacité du réseau et permet une transmission plus rapide des données.

Job 9:

Voici mon schéma.



Voici trois avantages principaux :

1. ****Visualisation de la topologie**** : Un schéma de réseau vous permet de visualiser clairement la topologie de votre réseau, c'est-à-dire comment les appareils, les commutateurs, les routeurs, les serveurs, etc., sont connectés les uns aux autres. Cela facilite la compréhension de la structure de votre réseau.
2. ****Dépannage facilité**** : En cas de problème ou de panne sur le réseau, un schéma bien documenté peut être un outil précieux pour le dépannage. Vous pouvez rapidement identifier les connexions, les composants ou les chemins potentiellement problématiques.

3. ****Planification et amélioration du réseau**** : Un schéma de réseau vous permet de planifier des améliorations ou des mises à niveau en identifiant les zones de congestion, les points faibles et les opportunités d'optimisation. Cela vous aide à prendre des décisions éclairées pour améliorer les performances et la sécurité du réseau.

Maintenant, vous pouvez ajouter ces avantages à votre documentation, accompagnés du schéma de votre réseau pour illustrer ces concepts. Assurez-vous d'utiliser un logiciel de dessin ou de conception graphique pour créer un schéma clair et informatif de votre réseau. Les logiciels courants pour cela incluent Microsoft Visio, Lucidchart, [Draw.io](https://draw.io), ou même des outils de dessin gratuits comme draw.io. Une fois que vous avez créé votre schéma, insérez-le dans votre documentation et ajoutez des explications pour mettre en évidence les avantages que j'ai

Job 10:

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

Une adresse IP statique et une adresse IP attribuée par DHCP diffèrent principalement par leur méthode d'attribution et leur nature persistante ou dynamique. Voici les principales différences entre les deux :

1. **Adresse IP statique :**

- Est configurée manuellement par un administrateur réseau.
- Ne change pas, sauf si elle est modifiée explicitement par l'administrateur.
- Reste constante à chaque connexion au réseau.
- Convient aux périphériques qui ont besoin d'une adresse IP permanente pour des applications spécifiques, comme les serveurs ou les imprimantes réseau.

2. **Adresse IP attribuée par DHCP :**

- Est distribuée automatiquement par un serveur DHCP (Dynamic Host Configuration Protocol).
- Peut varier à chaque connexion au réseau en fonction des disponibilités de l'adresse IP dans la plage définie par le serveur DHCP.
- Est temporaire et peut être libérée pour être réaffectée à un autre périphérique lorsque le bail DHCP expire.
- Est utilisée pour les périphériques clients ordinaires, tels que les ordinateurs de bureau, les ordinateurs portables et les appareils mobiles, qui n'ont pas besoin d'une adresse IP permanente.

En résumé, une adresse IP statique est configurée manuellement et ne change pas, tandis qu'une adresse IP attribuée par DHCP est automatiquement attribuée par un serveur DHCP et peut varier à chaque connexion en fonction de la disponibilité des adresses IP.

Job 11:

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

L'adresse de classe A a une grande plage d'adresses disponibles, ce qui est nécessaire pour créer de nombreux sous-réseaux. Dans ce cas, une adresse de classe A est suffisante pour répondre à vos besoins en termes de sous-réseaux et d'hôtes.

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

Les classes d'adresses (A, B, C, D, E) déterminent la plage d'adresses disponibles dans un réseau. Les adresses de classe A ont un préfixe de réseau de 8 bits, ce qui signifie qu'elles peuvent être utilisées pour un grand nombre de sous-réseaux avec un grand nombre d'hôtes. Les autres classes ont des préfixes de réseau de différentes tailles, ce qui limite le nombre d'adresses de réseau et d'hôtes possibles. Les sous-réseaux sont créés en empruntant des bits d'adresse d'hôte pour les répartir en sous-réseaux plus petits. La taille des sous-réseaux et le nombre d'hôtes possibles varient en fonction de la classe de l'adresse et du nombre de bits empruntés pour l'adressage du sous-réseau.

Job 12:

Voici un tableau qui présente les sept couches du modèle OSI avec une description des rôles de chaque couche, ainsi que les associations entre les différents matériels et protocoles et les couches respectives du modèle OSI :

<u>Couche OSI</u>	<u>Description des rôles</u>	<u>Matériels/Protocoles associés</u>
7. Application	Fournit des interfaces pour les services réseau aux applications	HTTP, FTP,HTML,SSL/TLS
6.Présentation	Convertit,chiffre et comprime les données pour l'échange entre systèmes	SSL/TLS,HTML

5.Session	Établit, gère et termine les sessions entre les applications	SSL/TLS,PPTP
4.Transport	Assure le transfert de bout en bout fiable les données	TCP,UDP
3.Réseau	Gère les adresses logiques et le routage des données	IPv4, IPv6, Routeur
2.Liaison de Données	Gère les communications entre les entités réseau sur le même lien physique	Ethernet,Wi-fi, MAC, Câble RJ45
1.Physique	Gère les signaux électriques ou optiques pour le transport de données	Fibre Optique, Câble RJ45

Job 13:

Architecture du réseau : Le réseau est configuré en utilisant une adresse IP de la classe C (192.168.10.X) avec un masque de sous-réseau de 255.255.255.0, ce qui signifie que le réseau est un réseau de classe C.

2. Adresse IP du réseau : L'adresse IP du réseau est la première adresse de la plage d'adresses IP, c'est-à-dire 192.168.10.0.

3. Nombre de machines sur le réseau : Avec un masque de sous-réseau de 255.255.255.0 (ou /24 en notation CIDR), vous avez 8 bits pour les adresses d'hôtes. Cela signifie qu'il y a $2^8 - 2$ adresses IP disponibles pour les machines, car 2 adresses sont réservées (l'adresse réseau et l'adresse de diffusion). Donc, le nombre de machines possibles est $2^8 - 2 = 256 - 2 = 254$.

4. Adresse de diffusion du réseau : L'adresse de diffusion pour ce réseau est la dernière adresse de la plage d'adresses IP, c'est-à-dire 192.168.10.255.

Donc, pour résumer :

- Architecture du réseau : Classe C (192.168.10.X)

- Adresse IP du réseau : 192.168.10.0
- Nombre de machines possibles : 254
- Adresse de diffusion : 192.168.10.255

Le réseau est capable de prendre en charge jusqu'à 254 machines, et l'adresse de diffusion permet de diffuser des données à toutes les machines du réseau.

Job 14:

Voici les adresses IP converties en binaire :

Pour l'adresse IP 145.32.59.24 :

145 : 10010001.00100000.00111011.00011000
32 : 00100000
59 : 00111011
24 : 00011000

Pour l'adresse IP 200.42.129.16 :

200 : 11001000.00101010.10000001.00010000
42 : 00101010
129 : 10000001
16 : 00010000

Pour l'adresse IP 14.82.19.54 :

14 : 00001110
82 : 01010010
19 : 00010011
54 : 00110110

Ces conversions en binaire permettent de représenter les adresses IP de manière plus concise pour les opérations logiques et les calculs sur les réseaux informatiques.

Job 15:

Qu'est-ce que le routage ?

Le routage est le processus de sélection du meilleur chemin pour transférer des données entre différents nœuds sur un réseau informatique. Les routeurs utilisent des algorithmes pour prendre des décisions en fonction de divers

facteurs tels que la disponibilité, la congestion et la vitesse. Il existe deux types de routage, statique et dynamique. Le routage joue un rôle crucial dans la gestion efficace des réseaux modernes, assurant la connectivité et la communication entre les utilisateurs et les ressources.

Qu'est-ce qu'un gateway ?

Un gateway, ou passerelle en français, est un dispositif matériel ou logiciel qui agit comme un point d'entrée ou de sortie pour un réseau. Il permet de relier des réseaux informatiques différents qui utilisent des protocoles de communication différents, facilitant ainsi la communication et le transfert de données entre ces réseaux. Les gateways sont essentiels pour assurer l'interopérabilité et la connectivité entre des réseaux hétérogènes.

Qu'est-ce qu'un VPN ?

Un VPN, ou réseau privé virtuel en français, est un outil de sécurité et de confidentialité qui établit une connexion cryptée et sécurisée entre un appareil et un réseau privé via Internet. Il permet aux utilisateurs d'accéder à des ressources réseau à distance de manière sécurisée tout en masquant leur adresse IP et en cryptant leurs données. Les VPN sont couramment utilisés pour sécuriser les connexions Wi-Fi publiques, contourner les restrictions géographiques et protéger la vie privée en ligne.

Qu'est-ce qu'un DNS ?

Le DNS, ou système de noms de domaine en français, est un système crucial sur Internet qui traduit les noms de domaine compréhensibles par l'homme en adresses IP, qui sont les identifiants numériques des appareils connectés au réseau. Il agit comme un répertoire permettant de mapper des noms de domaine tels que `www.example.com` en adresses IP comme `192.0.2.1`, facilitant ainsi la navigation sur Internet. Le DNS joue un rôle vital en assurant la convivialité et l'accessibilité d'Internet pour les utilisateurs.

