

CISCO

Job 01

Cisco Packet Tracer est un logiciel de simulation de réseau développé par Cisco, utilisé principalement dans l'éducation et la formation en réseautage. Il permet aux utilisateurs de créer des topologies virtuelles, de configurer des dispositifs Cisco, d'émuler des protocoles réseau, et de visualiser le trafic en temps réel. Cet outil interactif facilite l'apprentissage pratique des concepts de réseau et est largement utilisé pour la préparation aux certifications Cisco, comme le CCNA. Packet Tracer est disponible gratuitement pour les étudiants, les enseignants et les professionnels.

Job 02

Qu'est-ce qu'un réseau ?

Un **réseau informatique** est une interconnexion d'ordinateurs et d'autres équipements (tels que des imprimantes ou des serveurs) qui communiquent entre eux. Les réseaux informatiques peuvent être locaux (LAN) ou étendus (WAN), en fonction de la distance sur laquelle ils s'étendent. Internet est un exemple de réseau étendu mondial.

À quoi sert un réseau informatique ?

Un réseau informatique a plusieurs fonctions et est utilisé pour diverses raisons dans le domaine de l'informatique et des communications. Les principales utilisations d'un réseau informatique sont :

Échange d'informations, accès à internet, collaboration, sécurité, centralisation des données, mobilité, automatisation

Quel matériel avons-nous besoin pour construire un réseau ?

Pour un réseau, les composants essentiels pour constituer un réseau **minimal** sont :

Routeur : Pour diriger le trafic entre le réseau local (LAN) et d'autres réseaux.

Commutateur (Switch) : Pour connecter les dispositifs au sein du réseau local.

Câbles Ethernet : Pour connecter les dispositifs au commutateur.

Ordinateurs : Les appareils principaux utilisés par les utilisateurs finaux.

Job 03

Comme vous avez pu le constater, il existe des câbles croisés, droits...
Quels câbles avez-vous choisis pour relier les deux ordinateurs ?

Câble Croisé : J'ai utilisé des câbles croisés pour connecter les deux dispositifs. Les broches des extrémités du câble sont croisées pour permettre une communication directe entre les deux dispositifs.

Job 04

Qu'est-ce qu'une adresse IP ?

Une **adresse IP** (Internet Protocol) est une série de chiffres assignée à chaque appareil connecté à un réseau informatique, lui permettant d'être identifié et de communiquer avec d'autres appareils sur Internet.

Il existe deux types d'adresses IP : IPv4, composées de quatre groupes de chiffres séparés par des points, et IPv6, qui utilise une notation alphanumérique plus étendue pour répondre à la croissance des appareils connectés.

Les adresses IP sont essentielles pour le routage des données sur Internet et la gestion des connexions réseau.

À quoi sert un IP ?

Une **adresse IP** sert à identifier de manière unique et à localiser un appareil sur un réseau informatique, notamment sur Internet. Cela permet aux appareils de communiquer entre eux en envoyant et en recevant des données, facilitant ainsi le routage des informations à travers le réseau. L'adresse IP joue un rôle crucial dans l'acheminement des données vers la destination correcte, permettant ainsi la connectivité et la communication au sein des réseaux informatiques.

Qu'est-ce qu'une adresse MAC ?

Une **adresse MAC** (Media Access Control) est un identifiant unique assigné à l'interface réseau d'un appareil pour la distinguer des autres dispositifs sur un réseau.

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

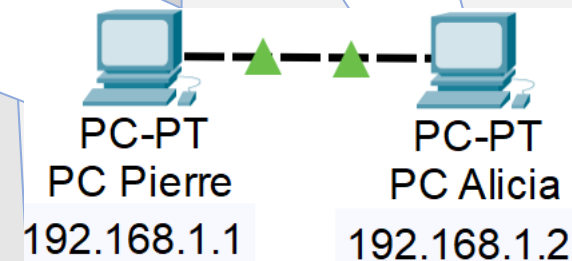
En réseau, une **adresse IP publique** est une adresse attribuée à un dispositif connecté à Internet et qui peut être directement accessible depuis le réseau mondial. Elle est utilisée pour identifier et communiquer avec ce dispositif sur une échelle globale. Les adresses IP publiques sont uniques et routables sur Internet.

D'un autre côté, une **adresse IP privée** est utilisée à l'intérieur d'un réseau local (LAN) et n'est pas directement accessible depuis Internet. Ces adresses sont souvent utilisées pour permettre aux dispositifs au sein d'un réseau local de communiquer entre eux sans être exposés directement à Internet. Les plages d'adresses IP privées sont définies dans des gammes réservées, comme 192.168.x.x, 172.16.x.x - 172.31.x.x, et 10.x.x.x.

Quelle est l'adresse de ce réseau ?

L'adresse de ce réseau est **192.168.1.0** car le masque de sous réseau est 255.255.255.0 donc les plages d'adresses IP valides sont de :

192.168.1.1 à 192.168.1.254



Job 05

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

La ligne de commande utilisé pour connaître l'adresse IP est : **ipconfig**

Le **ping** est utilisé pour tester la communication entre 2 machines.

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:58FF:FE30:5509
    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
```

Job 06

Quelle est la commande permettant de ping entre des PC ?

La ligne de commande permettant de ping entre deux PC est : **ping (l'adresse à ping)**

```
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),
```

Job 07

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

Non le PC de Pierre n'a **pas réussi à recevoir les paquets**.

Le PC de Pierre **étant éteins, la carte réseau n'est pas alimenté** donc il ne reçoit pas les paquets.

```
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),
```

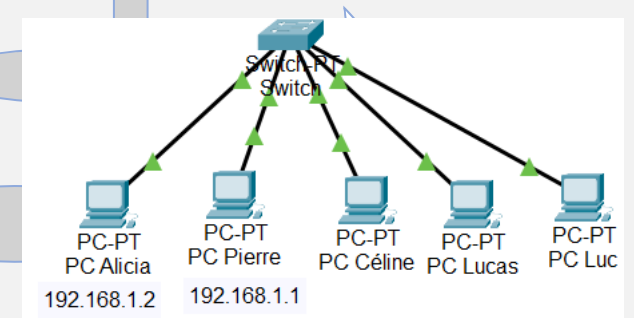

Job 08

Quelle est la différence entre un hub et un switch ?

Un hub est souvent utilisé pour **connecter des segments d'un réseau local**

(LAN). Un hub dispose, tout comme du commutateur, de plusieurs ports ; il sert comme **point de connexion** commun entre les périphériques d'un réseau.

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 ?

Un hub est un **dispositif de réseau** de base qui opère au niveau de la couche physique du modèle OSI. Il agit en tant que répéteur, transmettant les données reçues à tous les ports du hub, sans tenir compte de l'adresse MAC de destination. Les avantages du hub incluent **sa simplicité et son coût peu élevé**. Cependant, il présente des inconvénients tels que la **diffusion excessive de données à tous les ports**, entraînant une utilisation inefficace de la bande passante, et **l'absence de segmentation**, ce qui le rend moins adapté aux réseaux modernes. Les commutateurs sont souvent préférés pour des performances et une gestion plus efficace.

Quels sont les avantages et inconvénients d'un switch ?

Les switches offrent une commutation de données plus efficace que les hubs, car ils opèrent au niveau de la couche liaison du modèle OSI, permettant de transférer les données uniquement vers le port de destination en fonction des adresses MAC. Cela réduit la diffusion excessive et optimise la bande passante. Les avantages incluent une **meilleure performance**, **une segmentation des réseaux et une gestion des collisions**. Cependant, les switches sont **plus coûteux** que les hubs, et des attaques telles que les DDOS peuvent encore **surcharger le réseau**. La gestion de switch peut nécessiter une expertise supplémentaire.

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

Un switch gère le trafic réseau en fonction des adresses MAC des dispositifs connectés. Il maintient une table d'adresses MAC appelée "table de commutation" pour associer chaque adresse MAC à un port spécifique. Lorsqu'il reçoit des données, le switch examine l'adresse MAC de destination dans le cadre et envoie les données uniquement au port associé à cette adresse, minimisant la diffusion excessive et optimisant la bande passante. Cela permet une commutation efficace des données entre les dispositifs connectés au sein d'un réseau.

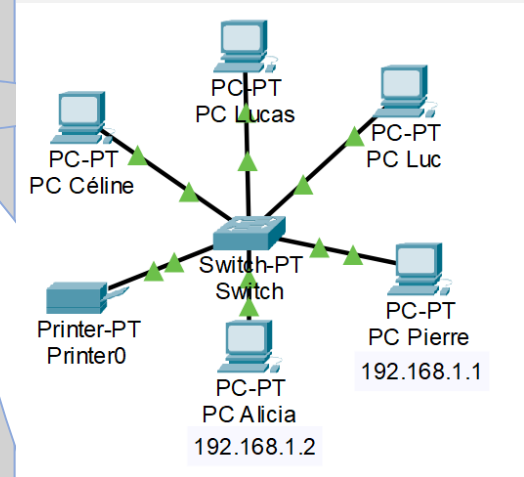
Job 09

Les **trois avantages** importants d'avoir un schéma :

Visualisation : Un schéma offre une représentation visuelle claire de la topologie du réseau, permettant aux administrateurs et aux utilisateurs de comprendre facilement comment les dispositifs sont interconnectés.

Planification : Lors de la planification ou de la conception d'un réseau, un schéma permet de prendre des décisions éclairées sur la disposition physique, les équipements nécessaires et les configurations requises.

Dépannage Facilité : En cas de problèmes, un schéma peut aider à identifier rapidement la source des problèmes en visualisant la configuration du réseau. Cela accélère le processus de dépannage.



Job 10

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

La principale différence entre un adresse IP statique et un IP d'un DHCP c'est que la statique on la fait **manuellement** alors que celle d'un DHCP est attribuée automatiquement par le DHCP, ce qui permet d'avoir un **réseau dynamique**.

Job 11

12 hôtes 1 sous-réseau	30 hôtes 5 sous-réseaux	120 hôtes 5 sous-réseaux	160 hôtes 5 sous-réseaux
Adresse réseau : 10.0.0.0	Adresse réseau : 10.0.0.16, 10.0.0.32, 10.0.0.48, 10.0.0.64, 10.0.0.80	Adresse réseau : 10.0.0.96, 10.0.0.224, 10.0.1.96, 10.0.1.224, 10.0.2.96	Adresse réseau : 10.0.3.0, 10.0.4.64, 10.0.5.128, 10.0.7.32, 10.0.8.96
Masque de sous-réseau : 255.255.255.240	Masque de sous-réseau : 255.255.255.224	Masque de sous-réseau : 255.255.255.128	Masque de sous-réseau : 255.255.255.192
Plage d'adresses utilisables : 10.0.0.1 à 10.0.0.14	Plage d'adresses utilisables pour chaque sous-réseau : 10.0.0.1 à 10.0.0.30 (X correspondant à l'octet de l'adresse du réseau)	Plage d'adresses utilisables pour chaque sous-réseau : 10.0.0.1 à X.X.X.126	Plage d'adresses utilisables pour chaque sous-réseau : X.X.X.1 à X.X.X.158

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

Une adresse de classe A offre un espace d'adressage extrêmement vaste (16 millions d'adresses). Cela permet de créer un grand nombre de sous-réseaux tout en satisfaisant les besoins spécifiques. Et aussi la création de 21 sous-réseaux nécessite une capacité importante, que seule une adresse de classe A peut fournir sans épuiser rapidement l'espace d'adressage.

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

Classe **A** :

Premier octet réservé pour le réseau, les trois autres octets pour les hôtes.

Plage d'adresses : 1.0.0.0 à 126.0.0.0

Utilisé pour de grands réseaux, car il offre une large plage d'adresses.

Classe **B** :

Deux premiers octets pour le réseau, deux derniers pour les hôtes.

Plage d'adresses : 128.0.0.0 à 191.255.0.0

Utilisé pour des réseaux de taille moyenne.

Classe **C** :

Trois premiers octets pour le réseau, un dernier pour les hôtes.

Plage d'adresses : 192.0.0.0 à 223.255.255.0

Utilisé pour des réseaux plus petits.

Les adresses de classe A sont donc adaptées ici car elles offrent suffisamment d'adresses pour créer plusieurs sous-réseaux tout en répondant aux exigences spécifiques en termes de nombre d'hôtes par sous-réseau.

Job 12

Les sept couches du modèle OSI

Chaque couche a une fonction spécifique et communique et travaille avec les couches inférieure et supérieure.

Couche 7 - Application : HTML - FTP - PPTP - SSL/TLS

Interface utilisateur directe, où les applications interagissent avec l'utilisateur. Exemples de protocoles : SMTP, HTTP.

Couche 6 - Présentation : SSL/TLS - HTML

Gère l'encodage/décodage des données pour la présentation à l'utilisateur. S'occupe également de la compression/décompression.

Couche 5 - Session : PPTP - FTP - SSL/TLS

Établit, gère et termine les sessions entre applications. Assure le transfert efficace des données, évitant la retransmission inutile.

Couche 4 - Transport : TCP - UDP

Divise les données en segments, ajoute des informations d'en-tête. Contrôle les erreurs et la retransmission pour garantir une livraison fiable.

Couche 3 - Réseau : IPv4 - IPv6 - Routeur

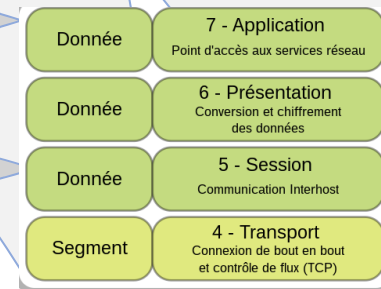
Achemine les paquets de données entre différents réseaux. Crée des petits paquets pour le transfert sur différents réseaux.

Couche 2 - Liaison de données : Ethernet - Wi-Fi - MAC - Câble RJ45

Facilite la communication sur le même réseau. Transforme les paquets en trames et contrôle les erreurs et le flux.

Couche 1 - Physique : Fibre optique - Cable RJ45

S'occupe du matériel concret nécessaire pour transférer les données, comme les câbles et les routeurs. Respecte les normes pour assurer l'interopérabilité.



Job 13

Quelle est l'architecture de ce réseau ?

Ce réseau à une architecture en **forme d'étoile** et il appartient à la **classe C**.

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 ?

Le nombre de machines que l'on peut brancher sur ce réseau est **254**.

Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion du réseau est **192.168.10.255** car c'est celle qui permettra de ping tout le monde.

Job 14

1= 0001

2= 0010

3= 0011

4= 0100

5= 0101

6= 0110

7= 0111

8= 1000

9= 1001

10= 1010

145.32.59.24

= 1001 0001 . 0010 0000 . 0011 1011 . 0001 1000

200.42.129.16

= 1100 1000 . 0010 1010 . 1000 0001 . 0001 0000

14.82.19.54

= 0000 1110 . 0101 0010 . 0001 0011 . 0011 0110

Job 15

Qu'est-ce que le routage ?

Le routage est le **processus de sélection du chemin dans un réseau**. Les principes de routage peuvent s'appliquer à tous les types de réseaux, des réseaux téléphoniques aux transports publics. Dans les réseaux à commutation de paquets, comme Internet, le routage sélectionne les chemins que doivent emprunter les paquets IP (Internet Protocol) pour se rendre de leur origine à leur destination. Ces décisions de routage Internet sont prises par des périphériques réseau spécialisés appelés routeurs.

Qu'est-ce qu'un gateway ?

Une gateway (passerelle en français) est un dispositif réseau qui fonctionne comme une passerelle entre deux réseaux distincts, permettant ainsi la communication entre eux. Sa principale fonction est de **transférer le trafic entre différents réseaux** qui peuvent utiliser des protocoles différents. Il agit comme une interface entre deux réseaux hétérogènes pour faciliter la transmission des données.

Qu'est-ce qu'un VPN ?

Un VPN, ou réseau privé virtuel, établit une connexion sécurisée entre des dispositifs par le biais d'Internet. Il permet le **transfert confidentiel de données sur des réseaux publics de manière sécurisée et anonyme**.

Qu'est-ce qu'un DNS ? (Domain Name System)

Le système de noms de domaine (DNS) est la méthode par laquelle une **adresse IP est convertie sur un ordinateur ou un autre dispositif connecté en un nom de domaine** lisible par l'homme.