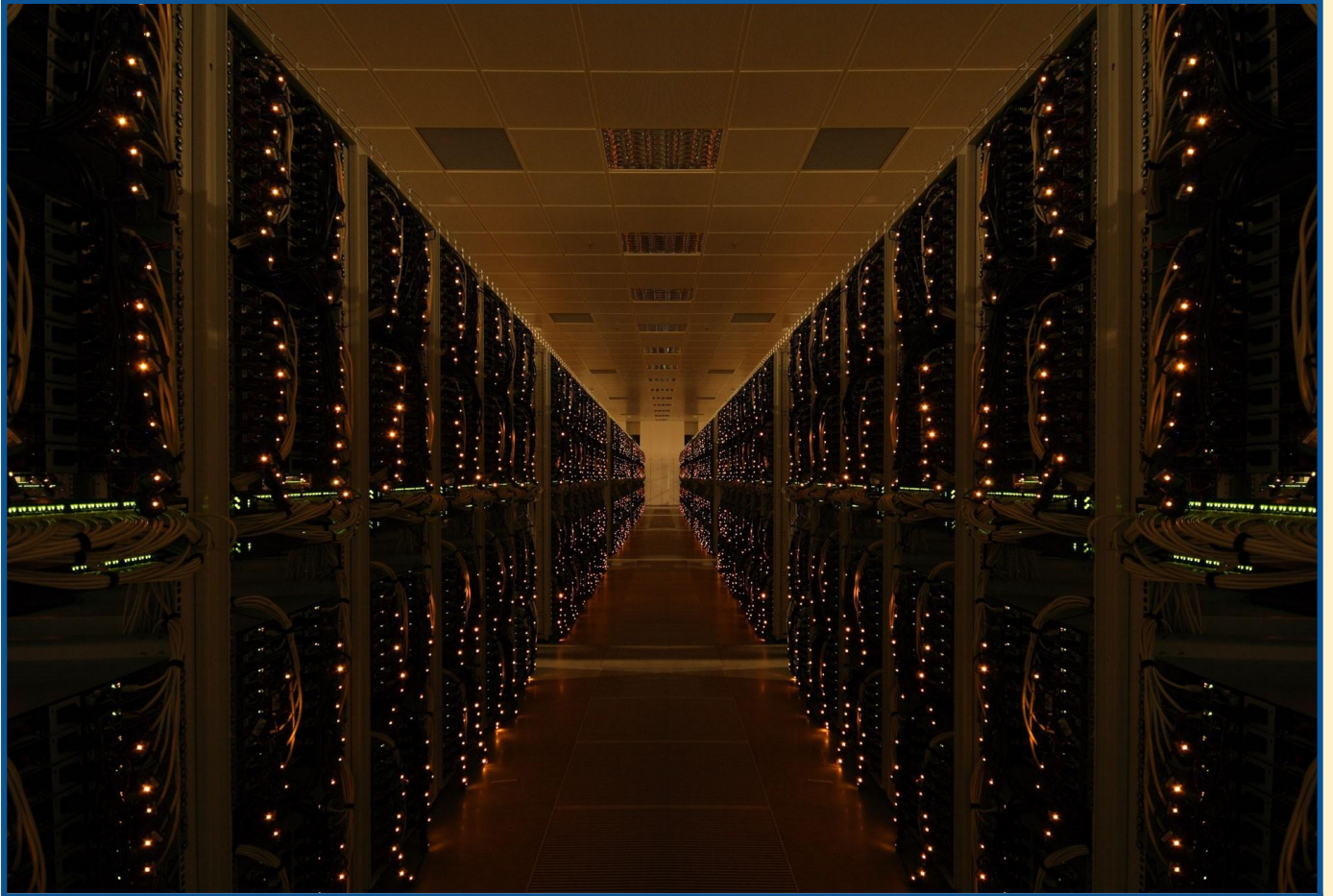


LE RÉSEAU



Lemelle Thanh-Son



La Plateforme

Sommaire

Sommaire	2
Job 02	3
Qu'est-ce qu'un réseau ? :	3
À quoi sert un réseau informatique ? :	3
Quel matériel avons-nous besoin pour construire un réseau ?	3
Job 03	5
Quels câbles avez-vous choisis pour relier les deux ordinateurs ?	5
Job 04	5
Qu'est-ce qu'une adresse IP ?	5
À quoi sert une adresse IP ?	5
Qu'est-ce qu'une adresse MAC ?	6
Qu'est-ce qu'une IP publique et privée ?	6
Quelle est l'adresse de ce réseau ?	6
Job 05	7
Screenshot des consoles du PC de Pierre et d'Alicia lors du ipconfig	7
Job 06	8
Screenshot des consoles du PC de Pierre et d'Alicia lors du ping	8
Job 07	9
Screenshot de la consoles du PC d'Alicia lors du ping vers le PC de Pierre (éteint)	9
Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?	9
Job 08	10
Quelle est la différence entre un hub et un switch ?	10
Fonctionnement d'un hub et ses avantages et inconvénients :	11
Avantages et inconvénients d'un switch :	11
Comment un switch gère le trafic réseau :	11
Job 09	12
Avantages de disposer d'un schéma de réseau :	12
Job 10	12
Différence entre une adresse IP statique et une adresse IP attribuée par DHCP :	12
Job 11	14
Job 12	15
Job 13	18
Quelle est l'architecture de ce réseau ?	20
Indiquer quelle est l'adresse IP du réseau ?	20
Déterminer le nombre de machines que l'on peut brancher sur ce réseau ?	20
Quelle est l'adresse de diffusion de ce réseau ?	20
Job 14	20
Convertissez les adresses IP suivantes en binaires :	20
Job 15	21
Qu'est-ce que le routage ?	21
Qu'est-ce qu'un gateway ?	21
Qu'est-ce qu'un VPN ?	21
Qu'est-ce qu'un DNS ?	22
index	23

Job 02

Qu'est-ce qu'un réseau ? :

Un réseau est un ensemble d'éléments **interconnectés** entre eux pour **échanger** des informations, des ressources ou des services. omniprésents dans notre vie quotidienne, ils peuvent prendre de nombreuses formes. (Réseaux de communication, réseau électrique et de transport, réseau informatique, etc ...)

À quoi sert un réseau informatique ? :

Un réseau informatique sert à :

- Partager **des données**
- Partager **des ressources physiques**, comme des imprimantes et des scanners
- Partager **des applications et des logiciels** sans les installer
- **Stocker et sauvegarder** des données de manière centralisée
- **Rechercher des informations** sur internet
- **Communiquer** à distance
- Partager **la puissance de calcul** et **la capacité de stockage**

Quel matériel avons-nous besoin pour construire un réseau ?

La construction d'un réseau informatique nécessite plusieurs composants essentiels pour fonctionner de manière efficace. Voici les principaux éléments et leurs fonctions :

Périphériques réseau :

- Ordinateurs : Les dispositifs clients qui se connectent au réseau pour accéder à des ressources partagées et communiquer avec d'autres utilisateurs.
- Serveurs : Les dispositifs qui fournissent des services, des ressources ou des données aux clients du réseau. Les serveurs peuvent inclure des serveurs de fichiers, des serveurs web, des serveurs de messagerie, etc.

Câblage réseau :

- Câbles Ethernet : Les câbles en cuivre ou en fibre optique qui connectent les dispositifs entre eux. Les câbles Ethernet sont essentiels pour le transfert de données à haute vitesse.
- Connecteurs et prises murales : Ils permettent de connecter les câbles Ethernet aux dispositifs et aux prises murales pour établir des connexions physiques.

Matériel de réseau :

- Commutateurs (switches) : Les commutateurs sont des dispositifs qui acheminent le trafic réseau entre les dispositifs connectés. Ils sont utilisés pour créer des réseaux locaux (LAN) et garantir que les données parviennent aux bons destinataires.
- Routeurs : Les routeurs sont responsables de la transmission de données entre les réseaux, tels que la connexion d'un réseau local à Internet. Ils acheminent les paquets de données entre les réseaux en fonction des adresses IP.
- Firewalls : Les pare-feu sont des dispositifs de sécurité qui filtrent le trafic réseau entrant et sortant pour protéger le réseau contre les menaces en ligne.
- Points d'accès sans fil (Access Points - AP) : Ils permettent aux dispositifs de se connecter sans fil au réseau, étendant ainsi la connectivité sans fil (Wi-Fi) du réseau.

Serveurs et services réseau :

- Serveurs de fichiers : Ils stockent des fichiers et permettent aux utilisateurs de les partager et d'y accéder.
- Serveurs d'impression : Ils gèrent les imprimantes partagées sur le réseau.
- Serveurs de messagerie : Ils gèrent les services de messagerie électronique.
- Serveurs DNS (Domain Name System) : Ils traduisent les noms de domaine en adresses IP.
- Serveurs DHCP (Dynamic Host Configuration Protocol) : Ils attribuent automatiquement des adresses IP aux dispositifs sur le réseau.
- Serveurs Web : Ils hébergent des sites web accessibles via Internet.

Logiciels de réseau :

- Système d'exploitation réseau : Un système d'exploitation conçu pour gérer les fonctions réseau, comme Windows Server ou Linux.
- Protocoles réseau : Les protocoles définissent les règles de communication entre les dispositifs du réseau. Des exemples incluent TCP/IP, HTTP, FTP, etc.

Systèmes de sécurité :

- Systèmes de détection d'intrusion (IDS) : Ils surveillent le trafic réseau pour détecter les activités suspectes.
- Systèmes de prévention d'intrusion (IPS) : Ils réagissent aux activités suspectes en bloquant ou en limitant l'accès.

Administration et gestion réseau :

- Logiciels de gestion réseau : Ils permettent de surveiller et de gérer les dispositifs, les performances et la sécurité du réseau.
- Personnel qualifié : L'administration et la maintenance du réseau nécessitent une expertise pour assurer son fonctionnement optimal.

Énergie électrique et secours :

- Une alimentation électrique stable et des dispositifs d'alimentation de secours, comme des onduleurs, sont nécessaires pour garantir la disponibilité du réseau.

Ensemble, ces composants forment un réseau informatique fonctionnel qui peut être utilisé pour partager des données, des ressources et des services, ainsi que pour faciliter la communication au sein d'une organisation ou entre des dispositifs connectés. La conception et la gestion d'un réseau dépendent des besoins spécifiques de l'utilisateur ou de l'organisation.

[Construire un réseau : le matériel - Les réseaux de zéro • Tutoriels • Zeste de Savoir](#)

Job 03

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

Expliquez votre choix.

Si vous reliez **deux ordinateurs** directement **l'un à l'autre** sans passer par un commutateur ou un routeur, vous devez utiliser **“un câble croisé”** dans Cisco Packet Tracer pour que la communication fonctionne correctement entre les deux ordinateurs.

En résumé, le choix entre **un câble droit** et un **câble croisé** dépend du type de dispositifs que vous reliez et de la topologie du réseau que vous configurez. Pour relier deux ordinateurs directement, utilisez un câble croisé, tandis que pour relier un ordinateur à un commutateur ou un routeur, utilisez un câble droit.

Job 04

Qu'est-ce qu'une adresse IP ?

Une adresse IP (Internet Protocol Address) **est une série unique de nombres** attribuée à chaque appareil connecté à un réseau, qu'il s'agisse d'un ordinateur, d'un smartphone, d'un routeur, ou d'un autre périphérique. Les adresses IP servent à **identifier** chaque dispositif sur un réseau et à permettre la communication entre eux.

À quoi sert une adresse IP ?

Les adresses IP sont essentielles pour **acheminer le trafic de données** sur Internet et les réseaux locaux. Elles permettent aux données de **trouver leur chemin** d'un point à un autre, de sorte que les appareils puissent échanger des informations et accéder à des services en ligne. En bref, les adresses IP sont les "coordonnées" des dispositifs sur un réseau.

Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control Address) est **un identifiant unique** associé à l'interface réseau **matériel d'un dispositif**, comme une carte réseau ou une carte Wi-Fi. Contrairement aux adresses IP, les adresses MAC sont **fixées en usine** et sont **spécifiques** à chaque dispositif matériel. Elles sont utilisées au niveau de la couche de liaison de données **du modèle OSI** pour identifier les dispositifs sur un réseau local.

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

- **Adresse IP publique** : Une adresse IP publique est attribuée à un dispositif qui est directement accessible depuis Internet. Ces adresses sont utilisées pour identifier un dispositif sur le réseau mondial, ce qui signifie qu'elles sont routables sur Internet. Les fournisseurs de services Internet (FAI) attribuent généralement des adresses IP publiques à leurs clients, ou ces derniers partagent des adresses IP publiques à travers un routeur.
- **Adresse IP privée** : Une adresse IP privée est utilisée à l'intérieur d'un réseau local (comme un réseau domestique ou d'entreprise) pour identifier les dispositifs au sein du réseau. Les adresses IP privées ne sont pas routables sur Internet et ne peuvent être utilisées que localement. Les plages d'adresses IP privées sont définies dans des normes, comme celles du RFC 1918, et incluent des adresses comme 192.168.x.x, 172.16.x.x, 10.x.x.x.

Quelle est l'adresse de ce réseau ?

Étant donné que les adresses IP de PC Pierre et PC Alicia sont les mêmes dans la partie réseau (**192.168.1**), elles se trouvent dans le même sous-réseau IP. Par conséquent, **l'adresse de ce réseau est 192.168.1.0** avec **un masque de sous-réseau de 255.255.255.0**. Le masque de sous-réseau de 255.255.255.0 indique que les trois premiers octets de l'adresse IP sont utilisés pour identifier le réseau, tandis que le dernier octet est utilisé pour identifier les hôtes individuels sur ce réseau. En résumé, l'adresse de ce réseau est 192.168.1.0 avec un masque de sous-réseau de 255.255.255.0, et le PC Pierre et le PC Alicia se trouvent dans ce réseau.

Job 05

Screenshot des consoles du PC de Pierre et d'Alicia lors du ipconfig

The image shows two overlapping windows from Cisco Packet Tracer. The top window is titled 'PC Pierre - 192.168.1.1' and the bottom window is titled 'PC Alicia - 192.168.1.2'. Both windows have tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. Inside each window is a 'Command Prompt' window showing the output of the 'ipconfig' command. The output for PC Pierre shows an IPv4 address of 192.168.1.1 and a Link-local IPv6 address of FE80::201:C9FF:FE10:CA73. The output for PC Alicia shows an IPv4 address of 192.168.1.2 and a Link-local IPv6 address of FE80::260:3EFF:FE3C:E0C9. Both PCs have a subnet mask of 255.255.255.0 and a default gateway of 0.0.0.0.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:C9FF:FE10:CA73
    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

C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:3EFF:FE3C:E0C9
    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

C:\>
```

La ligne de commande utilisé pour afficher l'ip sur chaque machine est **ipconfig**

Job 06

Screenshot des consoles du PC de Pierre et d'Alicia lors du ping

```
PC Alicia - 192.168.1.2
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

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

C:\>

PC Pierre - 192.168.1.1
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

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

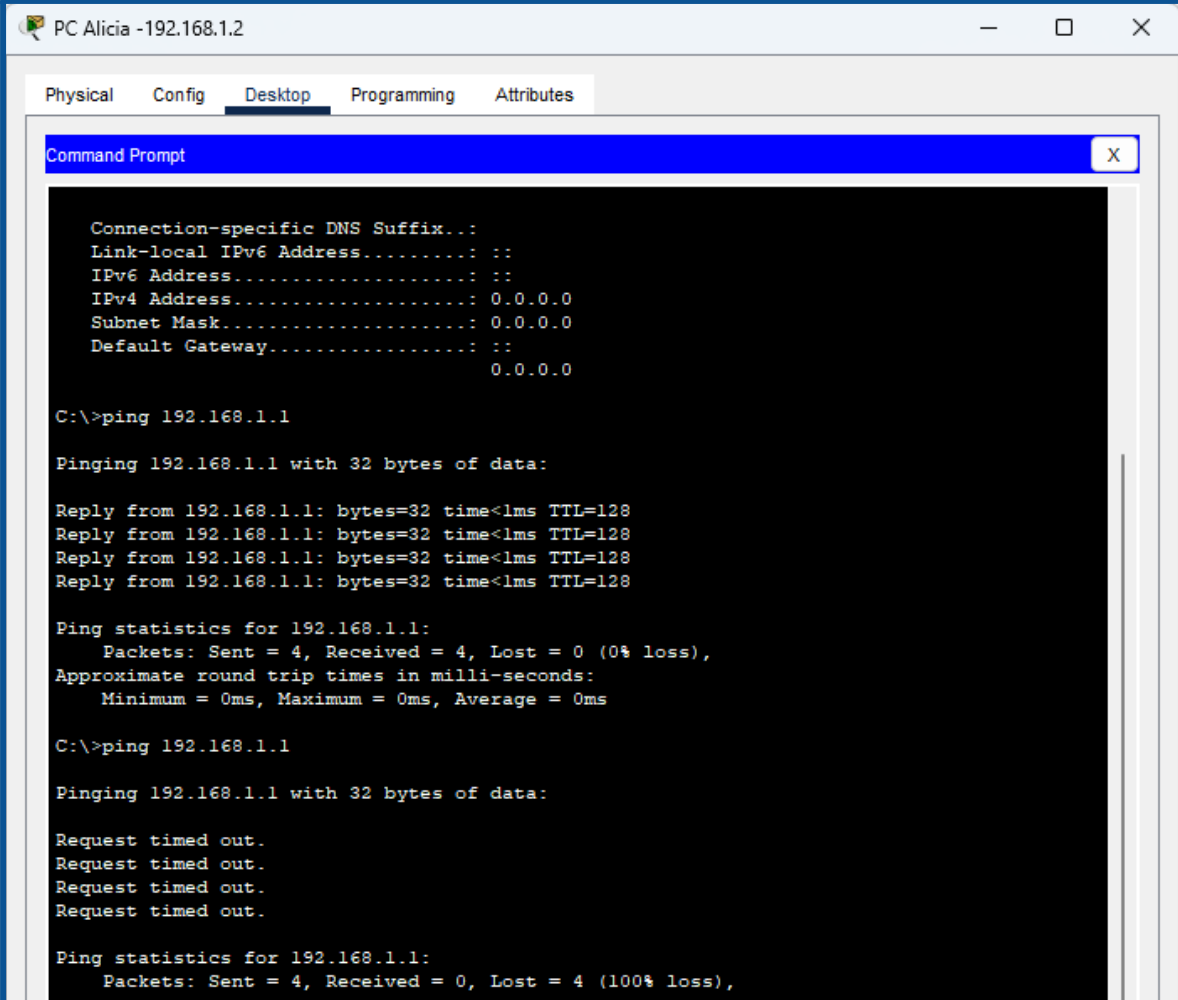
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Quelle est la commande permettant de Ping entre des PC ? `ping <adresse IP de la machine de destination>`

Job 07

Screenshot de la consoles du PC d'Alicia lors du ping vers le PC de Pierre (éteint)



```
PC Alicia -192.168.1.2
Physical Config Desktop Programming Attributes
Command Prompt X

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

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

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 ?

Expliquez pourquoi.

Le PC de Pierre ne recevra pas les paquets si l'ordinateur est **éteint**, car il ne sera pas en mesure de répondre aux requêtes ICMP. Le ping est un outil utilisé pour tester la connectivité réseau, et il nécessite que l'ordinateur **de destination** soit **en ligne** pour répondre aux requêtes.

Job 08

[Cisco Packet Tracer : le simulateur de réseaux idéal pour les débutants > Gandal Smart](#)

Quelle est la différence entre un hub et un switch ?

Un hub et un switch sont deux dispositifs couramment utilisés dans les réseaux informatiques pour connecter plusieurs ordinateurs. Cependant, ils fonctionnent de manière très différente :

Fonctionnement d'un hub et ses avantages et inconvénients :

Hub :

- Fonctionnement : Un **hub** est un dispositif simple qui opère au niveau de **la couche 1** (physique) du modèle OSI. Il reçoit les données de chaque port et les transmet à **tous** les autres ports, indépendamment du destinataire. En d'autres termes, un hub ne fait aucune distinction entre les adresses MAC des ordinateurs connectés.
- Avantages : Les hubs sont généralement **peu coûteux** et **faciles à configurer**. Ils ne nécessitent pas de gestion complexe.
- Inconvénients : Le principal inconvénient d'un hub est qu'il génère **un trafic inutile** sur le réseau, car il diffuse les données à tous les ports, ce qui peut **entraîner des collisions** et **réduire les performances**. De plus, la sécurité est **limitée**, car toutes les données sont accessibles à tous les périphériques connectés.

Comment un switch gère le trafic réseau :

Un switch opère aux **niveaux de la couche 2** (liaison de données) et **3** (réseau) du modèle OSI. Il apprend les adresses MAC des ordinateurs connectés à ses ports et **dirige** le trafic **uniquement** vers le port où se trouve le destinataire, ce qui **limite** le trafic inutile.

Avantages et inconvénients d'un switch :

- Avantages : Les switches offrent **une meilleure performance** que les hubs, car ils **réduisent le trafic inutile et les collisions**. De plus, ils **améliorent la sécurité** en isolant les flux de données sur des segments de réseau distincts.

- Inconvénients : Les switches sont **plus coûteux** que les hubs et nécessitent parfois une **configuration plus complexe**. De plus, si mal configurés, ils peuvent entraîner des problèmes de boucles (boucles de réseau) qui affectent la stabilité du réseau.

Job 09

Avantages de disposer d'un schéma de réseau :

Documentation et compréhension : Un schéma de réseau est une documentation visuelle qui aide à comprendre la configuration du réseau. Il est particulièrement utile pour les administrateurs réseau et le personnel informatique qui travaillent sur la maintenance, le dépannage et l'expansion du réseau.

Dépannage et maintenance : En cas de problème ou de panne sur le réseau, un schéma de réseau peut être une ressource précieuse pour identifier rapidement la source du problème. Il facilite également la maintenance, car il permet de localiser les composants et les connexions.

Planification et expansion : Un schéma de réseau peut être utilisé pour planifier de futures extensions ou améliorations du réseau. Il vous aide à visualiser où vous pourriez ajouter de nouveaux dispositifs ou optimiser les connexions.

Job 10

Différence entre une adresse IP statique et une adresse IP attribuée par DHCP :

Adresse IP statique :

- Une adresse IP statique est **attribuée manuellement** à un dispositif réseau. Cela signifie que l'administrateur réseau configure spécifiquement une adresse IP pour un dispositif, et cette adresse **reste constante**, sauf si elle est modifiée manuellement.
- Les adresses IP statiques sont souvent utilisées pour **les serveurs** ou les dispositifs nécessitant une adresse IP fixe pour une raison précise, comme l'hébergement de services spécifiques.
- Elles sont généralement **moins flexibles** en termes de gestion, car chaque dispositif doit être **configuré individuellement**.

Adresse IP attribuée par DHCP :

- Une adresse IP attribuée par DHCP est **automatiquement obtenue** par un dispositif à partir d'**un serveur DHCP**.
- Les dispositifs client **envoient une demande** au serveur DHCP lors de leur connexion au réseau, et le serveur attribue une adresse IP disponible **dans un pool d'adresses défini**.
- Les adresses IP attribuées par DHCP **sont temporaires** et peuvent changer si le dispositif se déconnecte et se reconnecte au réseau.
- Le DHCP offre **une gestion centralisée et automatisée** des adresses IP, ce qui facilite la configuration et la maintenance du réseau, en particulier dans les environnements avec de nombreux dispositifs.

Job 11

Adresses IPv4 et le calcul des masques de sous-réseaux | IT-Connect

Sous-réseau	masque de sous-réseau	Adresse de sous réseau	Plage d'adresse IP	Adresse de diffusion
1 sous-réseau de 12 hôtes	255.255.255.240/28	10.0.0.0	10.0.0.1-10.0.0.14	10.0.0.15
5 sous réseaux de 30 hôtes	255.255.255.224/27	10.0.1.0	10.0.1.1-10.0.1.30	10.0.1.31
		10.0.2.0	10.0.2.1-10.0.2.30	10.0.2.31
		10.0.3.0	10.0.3.1-10.0.3.30	10.0.3.31
		10.0.4.0	10.0.4.1-10.0.4.30	10.0.4.31
		10.0.5.0	10.0.5.1-10.0.5.30	10.0.5.31
5 sous réseaux de 120 hôtes	255.255.255.128/25	10.0.6.0	10.0.6.1 - 10.0.6.126	10.0.6.127
		10.0.7.0	10.0.7.1 - 10.0.7.126	10.0.7.127
		10.0.8.0	10.0.8.1 - 10.0.8.126	10.0.8.127
		10.0.9.0	10.0.9.1 - 10.0.9.126	10.0.9.127

Sous-réseau	masque de sous-réseau	Adresse de sous réseau	Plage d'adresse IP	Adresse de diffusion
		10.0.10.0	10.0.10.1 - 10.0.10.126	10.0.10.127
5 sous réseaux de 160 hôtes	255.255.255.0/24	10.0.11.0	10.0.11.1 - 10.0.11.254	10.0.11.255
		10.0.12.0	10.0.12.1 - 10.0.12.254	10.0.12.255
		10.0.13.0	10.0.13.1 - 10.0.13.254	10.0.13.255
		10.0.14.0	10.0.14.1 - 10.0.14.254	10.0.14.255
		10.0.15.0	10.0.15.1 - 10.0.15.254	10.0.15.255

Job 12

Couche OSI	Description du rôle	Matériels, Protocoles et Technologies Associés
7 (Application)	Cette couche fournit des services de communication aux applications utilisateur. Elle est responsable de la communication directe avec les logiciels et les utilisateurs. Elle gère les protocoles d'application, tels que HTTP, FTP, SMTP, etc.	HTML, FTP, SSL/TLS
6 (Présentation)	La couche de présentation gère la traduction, la compression et le chiffrement des données. Elle assure que les données sont correctement formatées pour la communication.	SSL/TLS, HTML

Couche OSI	Description du rôle	Matériels, Protocoles et Technologies Associés
5 (Session)	La couche de session établit, maintient et termine les sessions de communication entre les applications. Elle gère la synchronisation des données et la reprise en cas de panne.	PPTP
4 (Transport)	La couche de transport est responsable de la communication de bout en bout. Elle segmente, gère le contrôle de flux, garantit la fiabilité de la transmission et corrige les erreurs.	TCP, UDP
3 (Réseau)	La couche réseau gère la communication entre les réseaux. Elle est responsable du routage des données, de la détermination du meilleur chemin et de la gestion des adresses IP.	IPv4, IPv6, routeur
2 (Liaison de données)	La couche liaison de données assure la connectivité directe entre les nœuds adjacents. Elle gère la détection d'erreurs, le contrôle d'accès au support et la segmentation des trames.	Ethernet, MAC, Wi-Fi, câble RJ45

Couche OSI	Description du rôle	Matériels, Protocoles et Technologies Associés
1 (Physique)	La couche physique est la couche matérielle du réseau. Elle spécifie les caractéristiques matérielles, telles que les câbles, les connecteurs et les signaux électriques.	Fibre optique

Veillez noter que ce tableau associe les matériels, protocoles et technologies aux couches du modèle OSI en fonction de leur rôle ou de leur position dans la pile protocolaire. Certains éléments, comme Ethernet, peuvent être pertinents à plusieurs couches, car ils opèrent à la fois au niveau physique (couche 1) et au niveau de liaison de données (couche 2).

OSI MODEL

Layer 7: Application Layer

- Defines interface to user processes
- Provides standardized network services

Layer 6: Presentation Layer

- Specifies architecture-independent data transfer format
- Encodes and decodes data; Encrypts and decrypts data; Compresses and decompresses data

Layer 5: Session Layer

- Manages user sessions and dialogues
- Controls establishment and termination of logical links between users

Layer 4: Transport Layer

- Provides reliable and sequential end-to-end packet delivery
- Provides connectionless oriented packet delivery

Layer 3: Network Layer

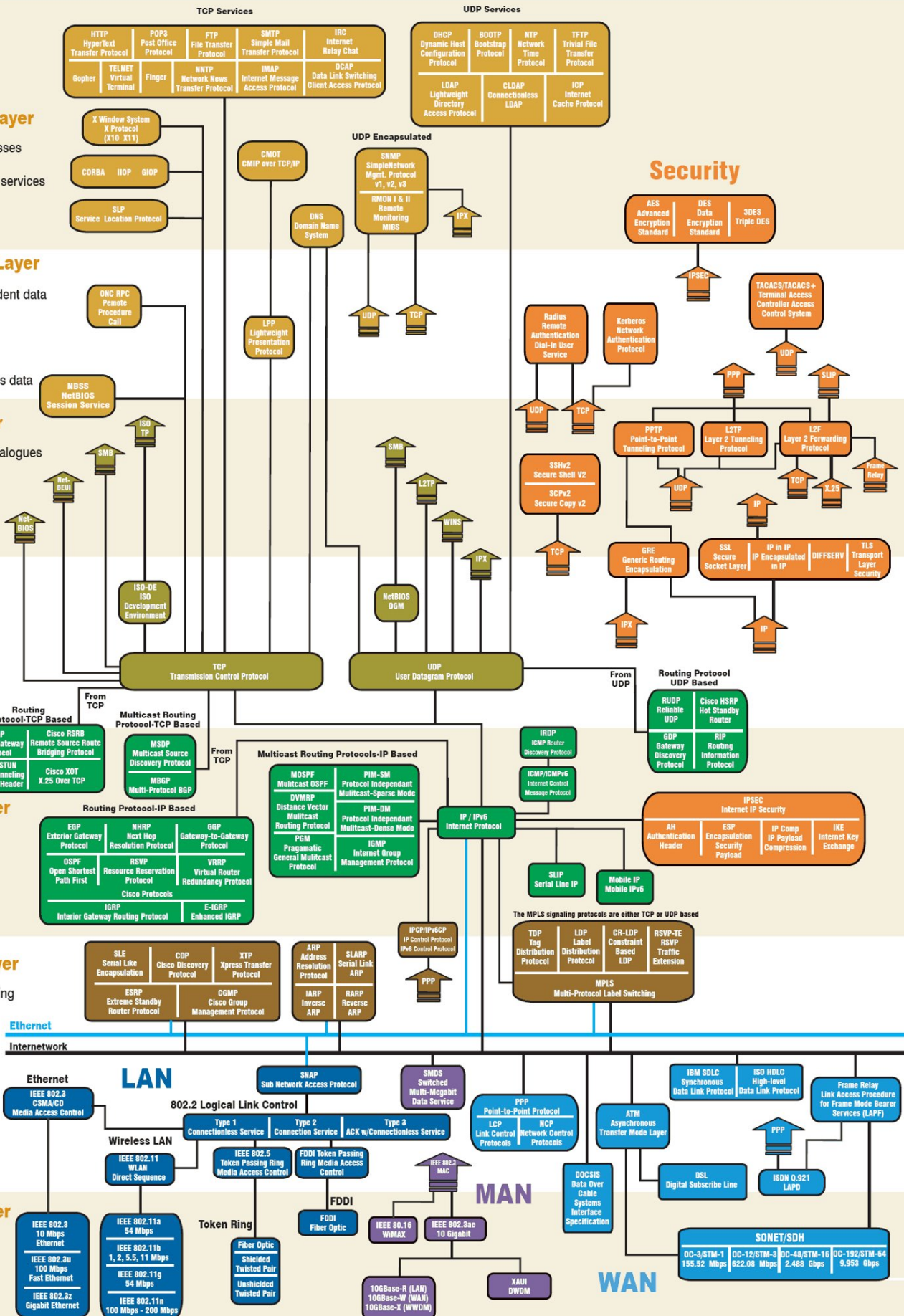
- Routes packets according to unique network addresses

Layer 2: Data Link Layer

- Defines procedures for operating the communication link
- Provides framing and sequencing

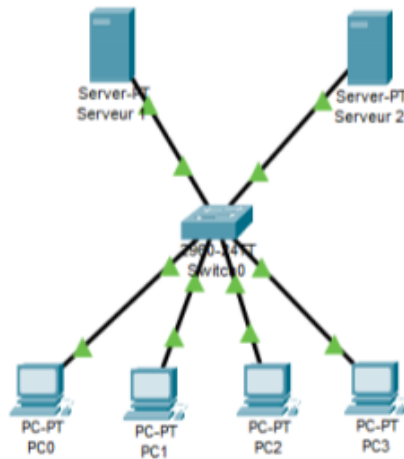
Layer 1: Physical Layer

- Defines physical means of sending data over network devices



Job 13

Vous êtes étudiants à l'école de la plateforme qui possède un parc informatique composé de 4 PCs. 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**

Avec un masque de sous-réseau :
255.255.255.0

[reseau.pdf\(ac-versailles.fr\)](http://reseau.pdf(ac-versailles.fr))

Catégorie de réseaux informatiques

On distingue **quatre catégories** de réseaux informatiques selon leur taille (nombre de machines) et leur étendue :

- **Le réseau personnel** (PAN : Personal Area Network), relie des machines sur quelques mètres.
- **Le réseau local** (LAN : Local Area Network), est adapté à la taille d'un site d'entreprise.
- **Le réseau métropolitain** (MAN : Metropolitan Area Network), est un réseau étendu à l'échelle d'une ville.
- **Le réseau étendu** (WAN : Wide Area Network), couvre une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent.

Topologie des réseaux de type LAN

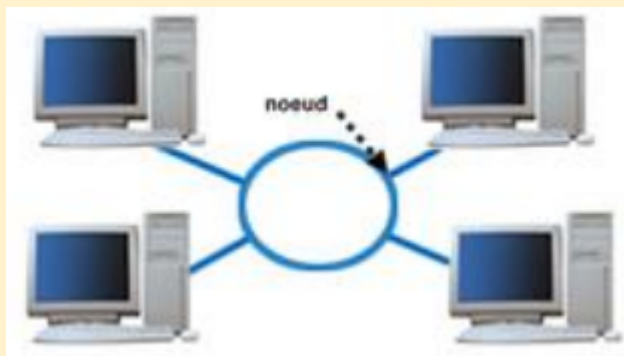
Il existe **trois topologies** de base pour concevoir un réseau : bus, anneau et étoile.

Topologie en bus



Le bus est **un segment central** où circulent les informations. Il s'étend sur toute la longueur du réseau et les machines viennent s'y accrocher. Lorsqu'une station émet des données, elles circulent sur toute la longueur du bus et la station destinataire peut les récupérer. Une seule station peut émettre à la fois. En bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre. L'avantage du bus réside dans la simplicité de sa mise en œuvre. Par contre, en cas de rupture du bus, le réseau devient inutilisable. Notons également que le signal n'est jamais régénéré, ce qui limite la longueur des câbles.

Topologie en anneau



Développée par IBM, cette architecture est principalement utilisée par les réseaux Token Ring. Elle utilise la technique d'accès par «jeton». Les informations circulent de station en station, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données

reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite... Cette topologie permet d'avoir un débit proche de 90% de la bande passante. De plus, le signal qui circule est régénéré par chaque station. En réalité les ordinateurs d'un réseau en anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre eux un temps de parole.

Topologie en étoile



C'est la topologie **la plus courante**. Toutes les stations sont **reliées à un unique composant central** : le concentrateur. Quand une station émet vers le concentrateur, celui-ci envoie les données à celle qui en est le destinataire (switch) ou à toutes

les autres machines (hub). Ce type de réseau est facile à mettre en place et à surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau. Par contre, **il faut plus de câbles** que pour les autres topologies, et si le concentrateur tombe en panne, tout le réseau est hors d'état de fonctionner. De plus, le débit pratique est moins bon que pour les autres topologies.

Quelle est l'architecture de ce réseau ?

L'architecture du réseau est 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 ?

Le masque de sous réseau étant 255.255.255.0 nous pouvons brancher 254 clients

Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion correspond à 192.168.10.255

Job 14

Convertissez les adresses IP suivantes en binaires :

decimal	145	32	59	24
binaire	1 0 0 1 0 0 0 1	0 0 1 0 0 0 0 0	0 0 1 1 1 0 1 1	0 0 0 1 1 0 0 0

decimal	200	42	129	16
binaire	1 1 0 0 1 0 0 0	0 0 1 0 1 0 1 0	0 0 1 1 1 0 1 1	0 0 0 1 0 0 0 0

decimal	14	82	19	54
binaire	0 0 0 0 1 1 1 0	0 1 0 1 0 0 1 0	0 0 0 1 0 0 1 1	0 0 1 1 0 1 1 0

Job 15

Qu'est-ce que le routage ?

Routage : Le routage est le **processus de transmission de données** d'un réseau à un autre. Il consiste à **déterminer le meilleur chemin** pour acheminer des données d'une source à une destination à travers un réseau. Les routeurs sont des dispositifs clés dans ce processus, car ils prennent des décisions de routage en fonction des adresses IP et des informations de routage pour diriger le trafic vers sa destination.

Qu'est-ce qu'un gateway ?

Gateway (Passerelle) : Une passerelle est un dispositif ou un logiciel qui **permet la communication entre des réseaux informatiques différents**, en traduisant les protocoles, les adresses, ou en fournissant une interface entre eux. Une passerelle est souvent utilisée pour connecter un réseau local à un réseau externe, comme Internet. Les routeurs agissent souvent comme des passerelles.

Qu'est-ce qu'un VPN ?

VPN (Virtual Private Network) : Un VPN est un réseau privé virtuel qui permet de **créer un tunnel sécurisé** à travers un réseau public, comme Internet. Il est utilisé pour **protéger la confidentialité et la sécurité des communications** en chiffrant les données qui circulent entre un appareil et un serveur VPN distant. Les VPN sont largement utilisés pour l'accès distant aux réseaux d'entreprise, la protection de la vie privée en ligne et le contournement des restrictions géographiques.

Qu'est-ce qu'un DNS ?

DNS (Domain Name System) : Le DNS est un système de noms de domaine qui **traduit les noms de domaine conviviaux**, tels que "www.example.com", **en adresses IP numériques** compréhensibles par les ordinateurs. Il sert de répertoire centralisé pour la résolution des noms de domaine, permettant aux utilisateurs d'accéder aux sites Web et aux services en utilisant des noms plutôt que des adresses IP. Le DNS est essentiel pour la navigation sur Internet et pour d'autres types de communication réseau.