

LE RÉSEAU

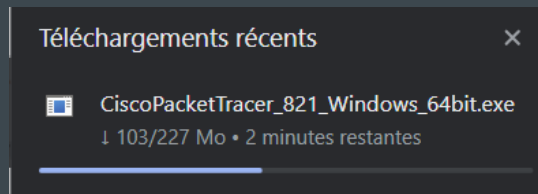
Marion BORNE

TABLE DES MATIÈRES

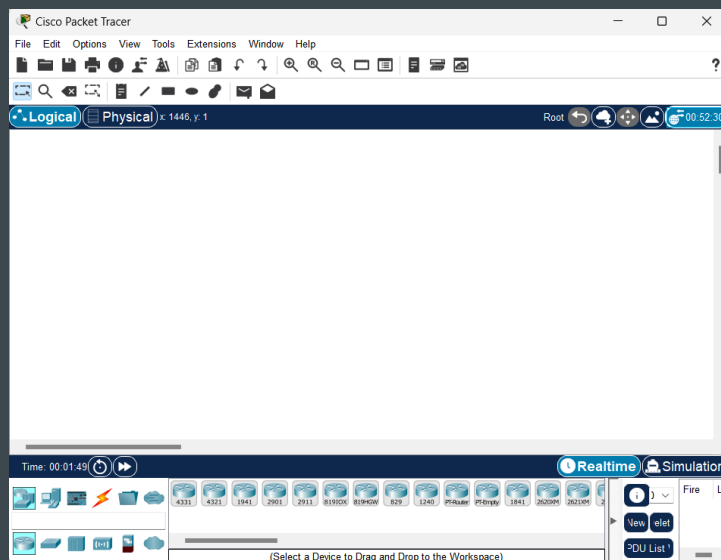
JOB 01	1
JOB 02.....	1
JOB 03	3
JOB 04	4
JOB 05	6
JOB 06	7
JOB 07	7
JOB 08.....	8
JOB 09	11
JOB 10	13
JOB 11	14
JOB 12	16
JOB 13	17

JOB 01 -

installation de Cisco Packet Tracer



Une fois l'installation faite et mon compte Sisco connecté, voici la page sur laquelle nous sommes.



JOB 02 -

Qu'est ce qu'un réseau ?

Le réseau est un ensemble d'équipements reliés entre eux pour échanger des informations.

À quoi sert un réseau informatique ?

Le réseau sert à des appareils informatiques interconnectés à échanger des données et partager des ressources entre eux. Ces appareils en réseau utilisent un système de règles, appelées protocoles de communication, pour transmettre des informations sur des technologies physiques ou sans fil.

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

1. Un médias d'accès

Cela peut être un câble ethernet ou une connexion sans fil, dans notre cas ce sera sans fil.

2. Une carte Réseau

elle est indispensable. C'est par elle que transitent toutes les données à envoyer et à recevoir du réseau par un ordinateur. La seule chose que vous devez connaître, c'est la notion d'adresse MAC : c'est l'adresse physique de la carte. Elle permet d'identifier la machine dans un réseau, un peu comme l'adresse IP.

3. Un concentrateur

Un *hub* est un dispositif en réseau qui permet de mettre plusieurs ordinateurs en contact. Il reçoit des données par un port, et envoie ce qu'il reçoit aux autres. Il a une interface de réception (un port) et une interface de diffusion (plusieurs autres ports par où les autres ordinateurs sont connectés).

4. Un commutateur (Switch)

Un commutateur fonctionne à peu près comme un *hub*, sauf qu'il est plus discret et intelligent. Il n'envoie pas tout ce qu'il reçoit à tout le monde, mais il l'envoie uniquement au destinataire. Afin de déterminer l'ordinateur à qui il faut renvoyer les données, le *switch* se base sur les adresses physiques (adresses MAC) des cartes réseau.

Un commutateur transmet donc des données aux autres ordinateurs en se basant sur leurs adresses MAC. Les transmissions sont plus confidentielles, les autres ne savent rien des données ne leur étant pas destinées. Son utilisation reste limitée aux réseaux locaux.

5. Un routeur.

Un routeur ressemble à un *switch* sur le plan de l'utilisation : en effet, il permet de mettre plusieurs ordinateurs en réseau. Mais cela va plus loin : il permet de mettre en contact 2 réseaux fondamentalement différents. Dans une petite installation, avec un ou plusieurs ordinateurs connectés à une « box » (qui est en fait un routeur), il est la frontière entre le réseau local et Internet.

Un routeur a plusieurs interfaces. Pour continuer dans notre exemple de frontière avec Internet, il possède une interface connectée à Internet

6. Un répéteur

Un répéteur (*repeater* en anglais) agit un peu comme un *hub*, mais ce dernier n'a que 2 interfaces. Son intérêt est de renvoyer ce qu'il reçoit par l'interface de réception sur l'interface d'émission, mais plus fort. On dit qu'il régénère et réémet le signal

Un répéteur permet de couvrir des distances plus grandes que les distances maximales fixées par le matériel que l'on utilise : par exemple, dans un réseau sans fil (Wi-Fi), la portée maximale entre 2 appareils est d'environ 50 mètres en intérieur. En plaçant un répéteur peu avant ces 50 mètres, vous pouvez connecter 2 appareils à 100 mètres de distance. Toutefois, le fait que les informations soient renvoyées « plus fort » peut dégrader la qualité du signal dans les réseaux sans fil.

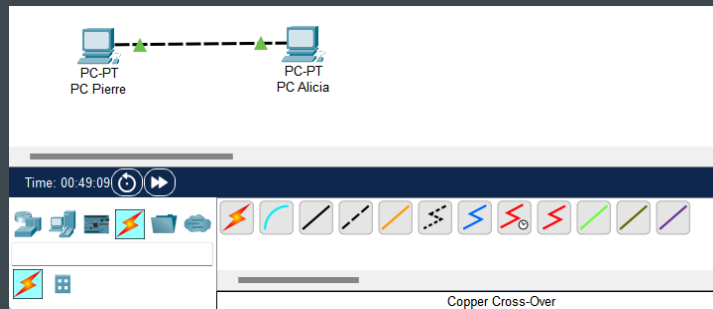
Pour résumer simplement nous avons besoin de ces 5 matériaux pour créer un réseau :

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 (<i>hub</i>)	Le concentrateur permet de relier plusieurs ordinateurs entre eux, mais on lui reproche le manque de confidentialité.
Commutateur (<i>switch</i>)	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 <i>plus fort</i> par l'interface d'émission. On parle aussi de <i>relais</i> en téléphonie et radiophonie.

JOB 03 -

Créer mon premier réseau :

J'utilise un câble croisé car celui ci connecte deux dispositifs du même type pour communiquer, comme un ordinateur à un autre ordinateur, ou un commutateur à un autre commutateur. Ici on cherche à connecter deux ordinateurs similaires de bureau l'un à l'autre.

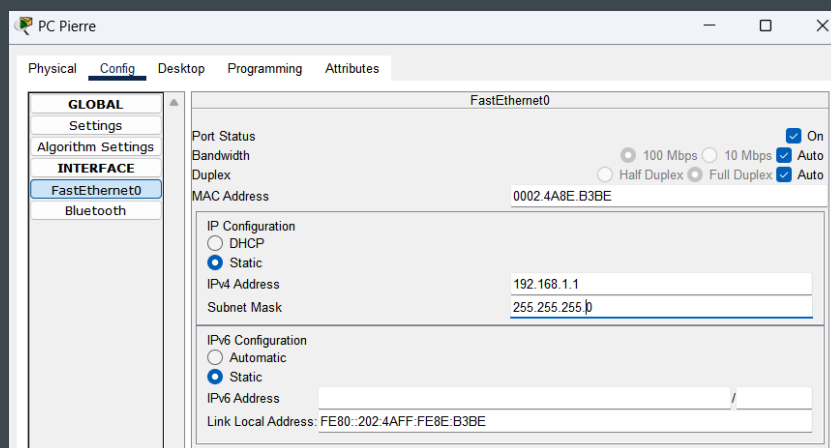


JOB 04 -

Configuration du PC Pierre et PC Alicia :

Entrer adresse IP (et l'afficher sous le nom du PC dans le schémas)

Rentrer masque de sous-réseau



Qu'est-ce qu'une adresse IP ?

Une adresse IP (*Internet Protocol*) est un numéro d'identification unique attribué de façon permanente ou provisoire à chaque périphérique faisant partie d'un même réseau informatique utilisant l'Internet Protocol. L'adresse IP est à l'origine du système d'acheminement (le routage) des paquets de données sur Internet.

Il existe deux grandes versions d'adresses IP : la version 4 (IPv4) codée sur 32 bits, et la version 6 (IPv6) codée sur 128 bits. La version 4 est actuellement la plus utilisée : elle est généralement représentée en notation décimale avec quatre nombres compris entre 0 et 255, séparés par des points, ce qui donne par exemple « 181.174.87.53 ».

À quoi sert un IP ?

Il sert à identifier les machines et à leur permettre de dialoguer entre elles, en échangeant des données sur Internet.

Les adresses IP peuvent servir à bloquer ou autoriser l'accès d'un ordinateur à certaines ressources, ou à mieux connaître le profil des utilisateurs

L'adresse IP identifie de manière unique chaque appareil sur Internet. Sans elle, il n'y a aucun moyen de les contacter. Les adresses IP permettent aux appareils informatiques (tels que les PC et les tablettes) de communiquer avec des destinations telles que les sites Web et les services de streaming, et ils permettent aux sites Web de savoir qui se connecte.

Une adresse IP sert également d'adresse de retour, au même sens qu'une adresse de retour sur courrier postal. Lorsque vous postez une lettre et qu'elle est livrée à la mauvaise adresse, vous récupérez la lettre si vous incluez une adresse de retour sur l'enveloppe. Il en va de même pour le courrier électronique.

Lorsque vous écrivez à un destinataire non valide (par exemple, un correspondant qui a quitté son entreprise), votre adresse IP permet au serveur de messagerie de l'entreprise de vous envoyer un e-mail de renvoi indiquant que la destination est introuvable.

Qu'est-ce qu'une adresse MAC ?

MAC signifie "*Media Access Control*" et cette adresse correspond à l'adresse physique d'un équipement réseau. Cette adresse est un identifiant, normalement unique, permettant d'identifier un équipement réseau par rapport à un autre.

La carte réseau d'un PC quant à elle, dispose d'une adresse MAC unique qui sert à l'identifier. En théorie, un constructeur utilise une adresse MAC différente pour chaque équipement commercialisé. En pratique, il existe des logiciels offrant la possibilité de modifier son adresse MAC (d'un point de vue logiciel seulement), et plus couramment c'est une fonctionnalité offerte par les solutions de virtualisation.

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

La principale différence entre les adresses IP publiques et privées se situe au niveau de leur portée et du réseau auquel elles sont connectées. Une adresse IP publique vous identifie auprès du réseau Internet, de telle sorte que toutes les informations que vous recherchez puissent vous retrouver. Une adresse IP privée est utilisée à l'intérieur d'un réseau privé pour établir une connexion sécurisée à d'autres appareils du réseau.

Votre adresse IP privée est comprise dans une plage d'adresses spécifique réservée par l'IANA (Internet Assigned Numbers Authority) et ne doit jamais être visible sur Internet. Il existe des millions de réseaux privés dans le monde.

Sans surprise, la plage d'adresses IP publiques comprend tous les numéros qui ne sont *pas* réservés pour la plage d'adresses IP privées. Puisqu'une adresse IP publique est un identifiant unique affecté à chaque appareil connecté à Internet, tout ce qu'on lui demande, c'est d'être unique.

Quelle est l'adresse de ce réseau ?

Les réseaux domestiques ont une adresse IP privée commençant par 192.168, Il s'agit du format par défaut le plus courant attribué aux routeurs réseau.

L'adresse de mes deux PC commence par 192.168, c'est donc cette adresse qui est celle de notre réseau.



JOB 05 -

Pour vérifier que l'IP du PC de Pierre et celui du PC d'Alicia fonctionnent,

J'ai utilisé la **commande ipconfig**

Pour celui de Pierre par exemple ci dessous :

```

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::202:4AFF:FE8E:B3BE
    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:\>

```

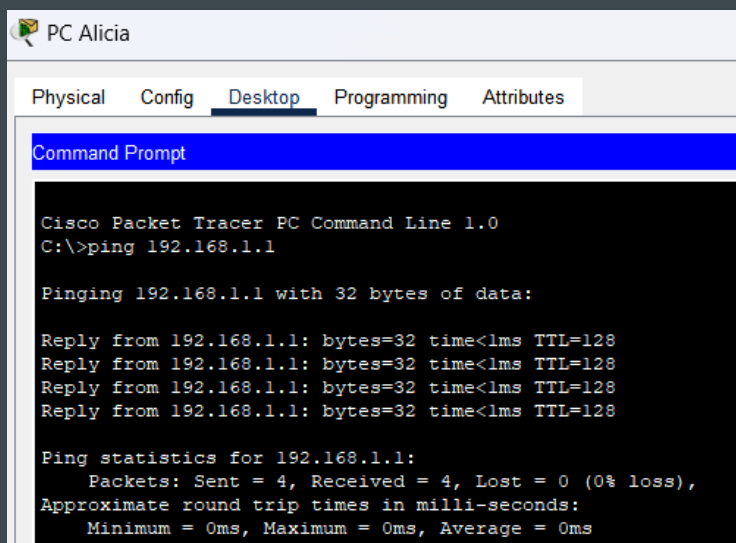
Je refais la même opération pour le PC d'Alicia.
Nos deux IP sont correctes.

JOB 06 -

J'ai testé la connectivité entre les deux PC de Pierre et d'Alicia grâce à la commande :

ping "adresse IP de l'autre ordinateur"

Notre connectivité est bonne entre les deux PC.



```

PC Alicia
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

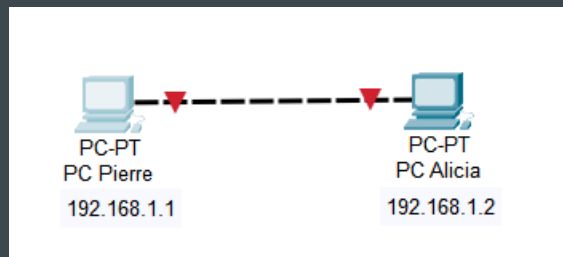
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

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

```


JOB 07 -

Pour éteindre mon ordinateur sur Cisco, je vais dans mon menu "Physical" et éteint ma machine.



On voit que le PC de Pierre est éteint et que la connexion ne marche pas entre les deux PC.

Je vérifie quand même avec la **commande ping** depuis le PC d'Alicia : Ca ne marche pas.

```
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 n'a pas reçu les paquets envoyés par Alicia.

C'est logique puisque l'ordinateur vers lequel celui d'Alicia veut communiquer est éteint, il ne reçoit donc aucun signal.

JOB 08 -

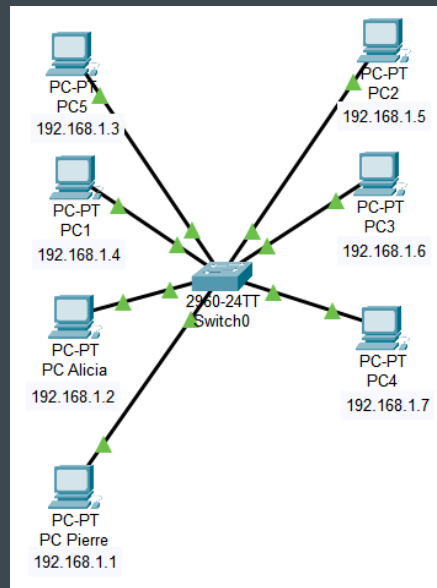
J'ai agrandi mon réseau en ajoutant 5 ordinateurs à mes deux existants.

Pour les connecter entre eux, j'utilise un switch.

Je leur attribue à tous une adresse IP commençant par 192.168

Je vérifie mes connectivités en leur affectant un ping à chacun.

Ils sont bien tous connectés (ci dessous l'exemple du ping entre le PC2 et le PC3)



```

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\> ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.6:
    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 différence entre un hub et un switch ?

Un Hub est un périphérique qui connecte plusieurs périphériques Ethernet sur un même réseau et les faire fonctionner ensemble en un seul réseau. Un Hub ne collecte pas d'informations. Tandis qu'un switch est un périphérique réseau qui effectue le même travail que le Hub mais qui est considéré comme un Hub plus intelligent car il collecte des informations sur les paquets de données qu'il reçoit et les transmet au seul réseau auquel il était destiné.

Ce tableau comparatif est très clair pour bien comprendre les différences entre Hub et Switch :

	Hub	Switch
Couche	Couche physique. Les Hubs fonctionnent sur la couche 1 selon le modèle OSI.	Couche de liaison de données. Les Switch fonctionnent sur la couche 2 du modèle OSI.
Fonction	Pour connecter un réseau d'ordinateurs, vous pouvez les connecter via un hub central.	Autoriser les connexions à plusieurs périphériques, gérer les ports, gérer les paramètres de sécurité du VLAN
Les ports	4/12 ports	Le switch est un bridge multi-port ou de 24/48 ports
Type d'appareil	Périphérique passif (sans logiciel)	Périphérique actif (avec logiciel)
Utilisé dans	LAN	LAN
Adresse MAC	Un Hub ne peut comprendre ou stocker une adresse MAC.	Un Switch comprend et stocke les adresses MAC.
Mode de transmission	Half duplex	Half/Full duplex
Domaine de Broadcast	Hub a un domaine de Broadcast	Switch a un domaine de Broadcast, sauf si le VLAN est implémenté
La vitesse	10Mbps	10/100 Mbps, 1 Gbps
Catégorie de l'appareil	Dispositif non intelligent	Dispositif intelligent

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.

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.

Avantages : Les hubs peuvent toujours être utilisés dans le cadre d'une analyse réseau. Dans ce cas, leur manque de flexibilité est plutôt avantageux : comme chaque port stocke l'ensemble des données du réseau, aucun miroir de port supplémentaire n'est nécessaire pour la lecture et l'analyse.

Inconvénients : En plus de la perte de vitesse 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'un switch ?

Le principal avantage des commutateurs est qu'ils permettent une vitesse de transfert de données plus élevée que celle des hubs.

Un autre avantage du switch est qu'il offre une plus grande sécurité. Les commutateurs sont conçus pour envoyer des paquets de données uniquement aux appareils qui les demandent, ce qui signifie que les données ne sont pas envoyées à tous les appareils connectés, ce qui peut constituer une faille de sécurité.

L'un des principaux inconvénients est qu'ils peuvent être plus chers que les hubs. Un autre inconvénient est que les commutateurs peuvent être plus difficiles à configurer et à entretenir que les hubs. Les commutateurs ont plus d'options de configuration que les hubs, ce qui signifie que la configuration correcte d'un commutateur peut prendre plus de temps.

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

Un commutateur réseau fonctionne intelligemment avec les adresses MAC pour s'assurer que le trafic qui est envoyé entre les appareils aboutit au bon endroit.

Pour ce faire, il surveille en permanence le trafic qui entre dans le commutateur à partir des appareils connectés.

Il apprend ensuite où les différentes adresses MAC de ces appareils sont connectées.

Pour ce faire, il examine le trafic qui arrive des ordinateurs pour lire l'adresse MAC source du trafic.

Ainsi lorsqu'un paquet est envoyé d'un équipement à l'autre.

Le commutateur réseau sait sur quel port physique envoyer la trame.

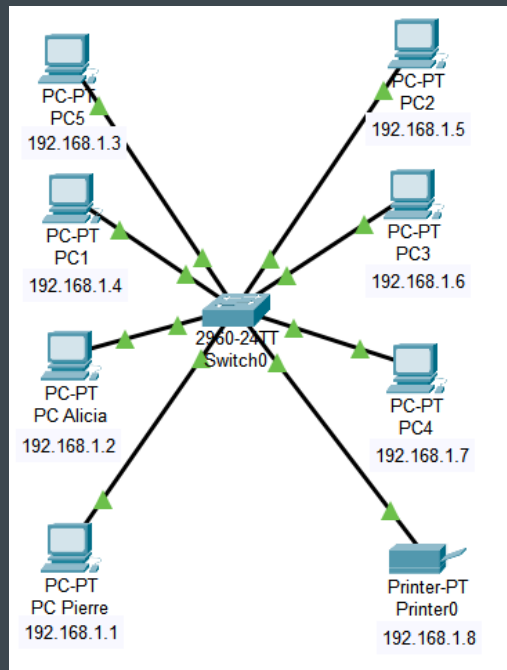
Cela permet d'économiser la bande passante du réseau, car le switch n'envoie que les trames au bon destinataire.

Contrairement à son ancêtre le hub qui réplique le trafic à tous les appareils (broadcast).

JOB 09 -

J'ai rajouté une imprimante et l'ai relié au switch après lui avoir attribué une adresse IP.

J'ai fait un ping pour vérifier ma connexion entre mon PC4 et mon imprimante : ça marche.



PC4

Physical Config Desktop Programming Attributes

Command Prompt

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.8

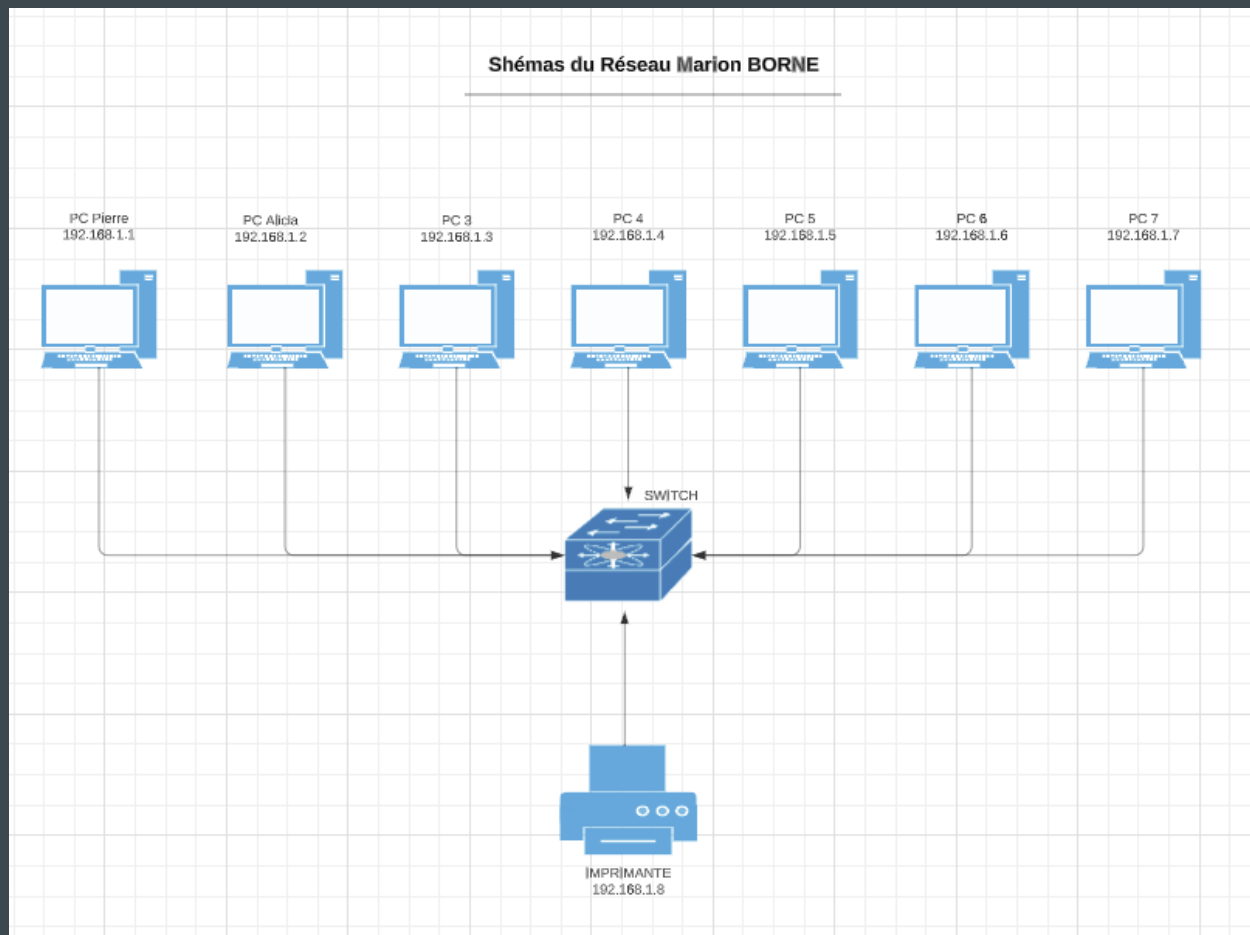
Pinging 192.168.1.8 with 32 bytes of data:

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<1ms 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 = 0ms, Average = 0ms

C:\>
  
```

J'ai ensuite crée un schémas via le site [Lucid Chart](#)

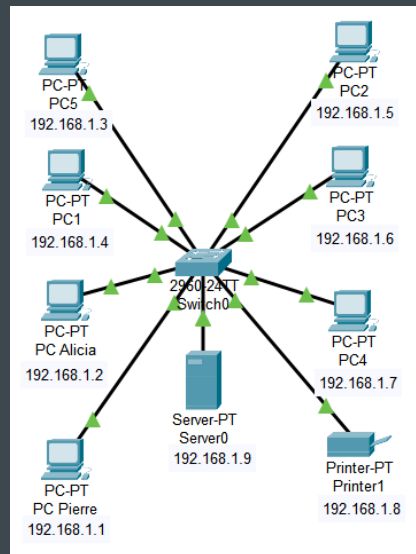


3 avantages d'un schémas de réseau tel que celui fait ci-dessus :

- Bonne lisibilité du réseau par un tiers (explication pour documentation par exemple)
 - Meilleure organisation (besoin d'être précis pour être compris)
 - Enregistrer toutes nos configurations et revenir sur les précédentes.

JOB 10 -

Pour mettre en place un serveur DHCP, j'ai installé un serveur, puis je l'ai configuré en DHCP (captures ci-dessous).



Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Maximum Number of Users: 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Marion Serveur	0.0.0.0	192.168.1.9	192.168.1.0	255.255.255.0	100	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.1.0	255.255.255.0	512	0.0.0.0	0.0.0.0

J'ai vérifié que mon serveur DHCP fonctionne correctement en installant un nouveau PC. Lorsque je demande à mon serveur DHCP de générer une adresse IP, ça marche.

PC7

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

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

Lorsque vous vous connectez à l'Internet, votre appareil a besoin d'une adresse IP pour communiquer avec d'autres appareils. Une adresse IP statique est une adresse fixe attribuée manuellement à votre appareil et qui ne change jamais. En revanche, le DHCP est un protocole qui attribue automatiquement des adresses IP aux appareils d'un réseau. Une adresse DHCP est donc une adresse temporaire qui peut changer périodiquement.

JOB 11 -

J'ai créé un plan d'adressage sous la forme de tableau pour les besoins suivants :

21 sous réseaux avec une adresse de réseaux de Classe A 10.0.0.0

RESEAUX	BESOINS HOTES	GATEWAY IP	HOST RANGE ADRESSES IP	BROADCAST IP	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
5 SOUS RESEAUX	30 HOTES	10.0.0.16	10.0.0.17 - 10.0.0.46	10.0.0.47	255.255.255.224
		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	
5 SOUS RESEAUX	120 HOTES	10.0.0.176	10.0.0.177 - 10.0.1.46	10.0.1.47	255.255.255.128
		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 - 10.0.2.176	10.0.2.175	
		10.0.2.176	10.0.2.179 - 10.0.3.48	10.0.3.47	
5 SOUS RESEAUX	160 HOTES	10.0.3.48	10.0.3.49 - 10.0.4.46	10.0.4.47	255.255.255.0
		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	

Voici une première méthode d'adressage de Classe A permettant un très grand nombre d'hôtes. Mais cette méthode n'est pas très lisible.

RESEAU	HOTES	ADRESSE IP DE DEPART	ADRESSE IP DE FIN	MASQUE SOUS RESEAU
RESEAU PRINCIPAL	(+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	

Voici une deuxième méthode plus lisible qui permet de bien voir les différents réseaux. Cette méthode permet un moins grand nombre d'hôtes (tout de même déjà très grand)

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

Votre adresse IP privée est comprise dans une plage d'adresses spécifique réservée par l'IANA (Internet Assigned Numbers Authority) et ne doit jamais être visible sur Internet. Il existe des millions de réseaux privés dans le monde. Tous les appareils qui y sont connectés possèdent une adresse IP privée comprise dans les plages suivantes : Classe A : 10.0.0.0 — 10.255.255.255

Nous avons donc choisi cette adresse car celle-ci est privée.

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

Chaque adresse IP appartient à une classe qui correspond à une plage d'adresses IP. Ces classes d'adresses sont au nombre de 5 c'est-à-dire les classes A, B, C, D et E. Le fait d'avoir des classes d'adresses permet d'adapter l'adressage selon la taille du réseau c'est-à-dire le besoin en termes d'adresses IP.

La classe A de l'adresse IP 0.0.0.0 à 126.255.255.255 (adresses privées et publiques).

La classe B de l'adresse IP 128.0.0.0 à 191.255.255.255 (adresses privées et publiques).

La classe C de l'adresse IP 192.0.0.0 à 223.255.255.255 (adresses privées et publiques).

La classe D de l'adresse IP 224.0.0.0 à 239.255.255.255 (adresses de multicast).

La classe E de l'adresse IP 240.0.0.0 à 255.255.255.255 (adresses réservées par l'IETF)

JOB 12 -

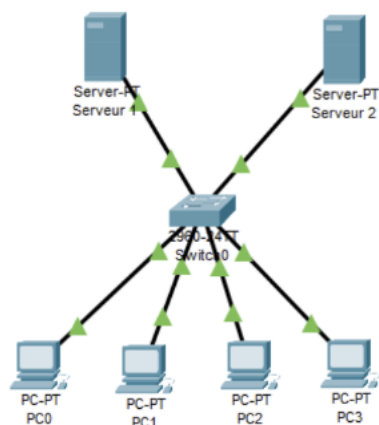
Voici un tableau selon le **modèle OSI** avec les sept couches de ce modèle et les descriptions de leurs rôles.

J'y ai associé différents matériaux et protocoles.

	Couches		Description	Unités	Matériaux / Protocoles
Couches hautes	7	Application	Point d'accès aux services réseau	Données	FTP
	6	Présentation	Conversion et chiffrement des données	Données	HTML
	5	Session	Communication Interhost	Données	
	4	Transport	Coordination du transfert de segments	Segments	TPC, UDP, SSL/TLS
Couches matérielles	3	Réseau	Détermine le parcours et l'adressage logique (IP)	Paquets	IPv4, IPv6
	2	Liaison	Adressage physique (MAC et LLC)	Trames	Ethernet, MAC, Wi-Fi, routeur, PPTP
	1	Physique	Transmission binaire numérique ou analogique	Bits	cable RJ45, fibre optique

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 :



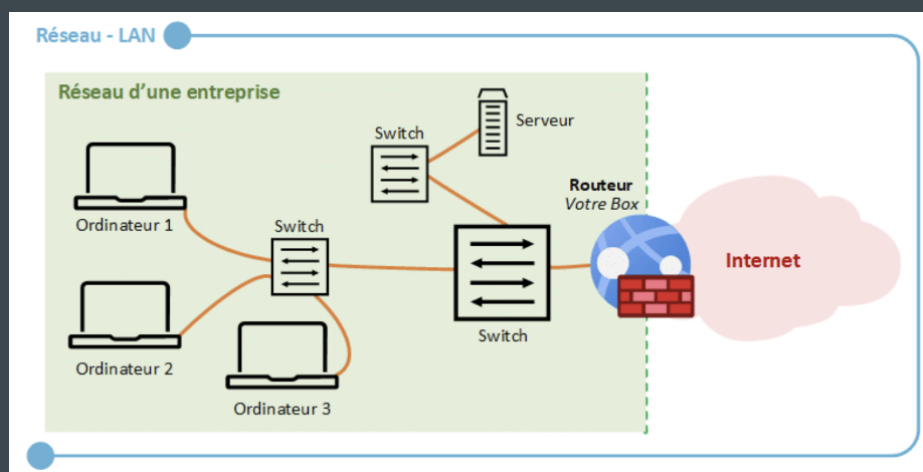
est :

- 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

Quelle est l'architecture de ce réseau ?

L'architecture de ce réseau est de type LAN



Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est **192.168.10.0**

C'est une adresse de Classe C

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

Nombre d'hôtes dans mon réseau							
128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)
1	1	1	1	1	1	1	1

Si l'on additionne la valeur de chaque bit, on obtient : $128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$

Le résultat en décimal est 255, donc nous avons 255 adresses disponibles pour nos hôtes... Enfin pas tout à fait !

Il y a 256 adresses IP disponibles dans ce réseau et non 255 adresses IP, car l'adresse en ".0" compte : $255 + 1 = 256$. S'il y a 8 bits pour la partie hôte, il suffit de faire 2^8 (2 puissance 8) = 256 adresses IP

Sur ce total de 256 adresses IP disponibles, il y a deux adresses que l'on ne pourra jamais attribuer (peu importe le réseau, peu importe le masque) : 192.168.1.0, car il s'agit de l'adresse du réseau et 192.168.1.255, car il s'agit de l'adresse de diffusion du réseau (broadcast) et l'adresse de gateway. Peu importe le nombre d'adresses IP disponibles dans un réseau, il faut toujours soustraire deux adresses IP correspondantes à l'adresse IP du réseau et à l'adresse IP de diffusion

En résumé, on peut considérer que la plage d'adresses IP que l'on peut attribuer à nos hôtes (routeur, ordinateurs, smartphones, etc.) est la suivante : 192.168.1.1 à 192.168.1.254. Soit un total de 254 adresses IP, non 255 ni 256

Quelle est l'adresse de diffusion de ce réseau ?

Une adresse de diffusion (ou broadcast en anglais) est une adresse spéciale du protocole Internet (IP) utilisée pour transmettre des messages et des paquets de données aux systèmes du réseau.

Le paquet IP avec une adresse de diffusion est envoyé à tous les nœuds du réseau. Tous les bits de la partie hôte d'une adresse IP sont mis à un pour identifier l'adresse de diffusion.

Par exemple, l'adresse IP 192.168.5.50 avec le masque de sous-réseau 255.255.255.0 a l'adresse de diffusion suivante 192.168.5.255/24.

Ici, l'adresse de diffusion de mon réseau est donc 192.168.10.255

JOB 14 -

Conversion d'adresse IP décimal en binaire :

IP : 145.32.59.24

Binaire : 10010001.00100000.00111011.00011000

IP : 200.42.129.16

Binaire : 11001000.00101010.10000001.00010000

IP : 14.82.19.54

Binaire : 00001110.01010010.00010011.00110110

JOB 15 -

Qu'est-ce que le routage ?

Le routage réseau est le processus de sélection d'un chemin à travers un ou plusieurs réseaux. 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 ?

Le Gateway est le dispositif par lequel deux réseaux informatiques ou deux réseaux de télécommunication de nature différentes sont reliés. Le dispositif permet de vérifier la sécurité du réseau qui cherche à se connecter à l'autre. La Gateway est aussi appelée passerelle applicative. Le réseau que vous cherchez à connecter à un autre réseau doit respecter les conditions fixées par l'administrateur de ce nouveau réseau.

La plupart du temps, l'opération consiste à relier un réseau local à Internet. Parmi les Gateways, la plus connue est la box Internet, ou passerelle domestique. Il s'agit du boîtier qui sert de lien entre un fournisseur d'accès Internet et un abonné au haut débit. Parmi les types de passerelles, mentionnons le routeur, le répéteur et le pont.

Qu'est-ce qu'un VPN ?

VPN signifie « Virtual Private Network » et décrit la possibilité d'établir une connexion réseau protégée lors de l'utilisation de réseaux publics. Les VPN chiffrent votre trafic Internet et camouflent votre identité en ligne. Il est ainsi plus difficile pour des tiers de suivre vos activités en ligne et de voler des données. Le chiffrement est effectué en temps réel. Un VPN masque votre adresse IP en laissant le réseau la rediriger vers un serveur distant spécialement configuré et géré par l'hôte d'un VPN.

Qu'est-ce qu'un DNS ?

Le DNS (Domain Name System, système de nom de domaine) est en quelque sorte le répertoire téléphonique d'Internet. Les internautes accèdent aux informations en ligne via des noms de domaine (par exemple, nytimes.com ou espn.com), tandis que les navigateurs interagissent par le biais d'adresses IP (Internet Protocol, protocole Internet). Le DNS traduit les noms de domaine en adresses IP afin que les navigateurs puissent charger les ressources web.

Chaque appareil connecté à Internet dispose d'une adresse IP unique que les autres appareils utilisent afin de le trouver. Grâce aux serveurs DNS, les internautes n'ont pas à mémoriser les adresses IP (par exemple, 192.168.1.1 en IPv4) ni les adresses IP alphanumériques plus récentes et plus complexes (par exemple, 2400:cb00:2048:1::c629:d7a2 en IPv6).