

Runtrack Réseau

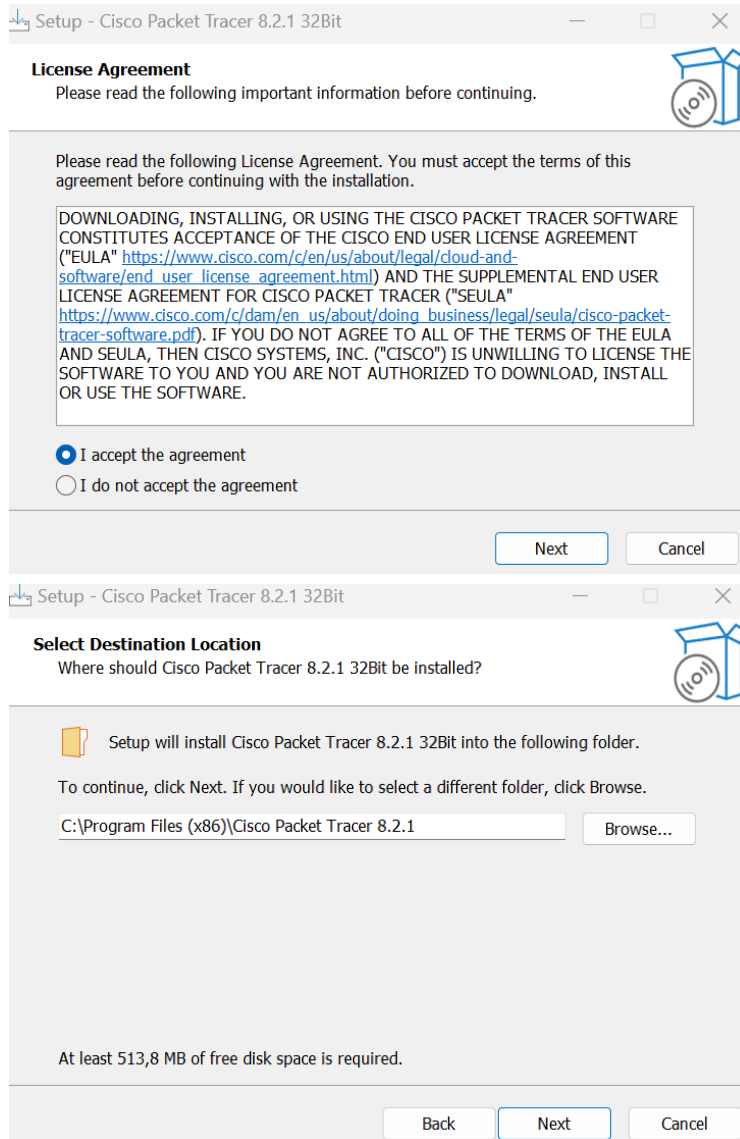
JOB 01

installer packet tracer

- Pour en savoir plus, consultez la [FAQ](#), ainsi que les [tutoriels](#).

Bureau Windows, version 8.2.1 (anglais)

[Télécharger la version 64 bits](#) [Télécharger la version 32 bits](#)



Setup - Cisco Packet Tracer 8.2.1 32Bit

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

DOWNLOADING, INSTALLING, OR USING THE CISCO PACKET TRACER SOFTWARE CONSTITUTES ACCEPTANCE OF THE CISCO END USER LICENSE AGREEMENT ("EULA" https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html) AND THE SUPPLEMENTAL END USER LICENSE AGREEMENT FOR CISCO PACKET TRACER ("SEULA" https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/cisco-packet-tracer-software.pdf). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE EULA AND SEULA, THEN CISCO SYSTEMS, INC. ("CISCO") IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND YOU ARE NOT AUTHORIZED TO DOWNLOAD, INSTALL OR USE THE SOFTWARE.

☒ I accept the agreement
☐ I do not accept the agreement

Next Cancel

Setup - Cisco Packet Tracer 8.2.1 32Bit

Select Destination Location

Where should Cisco Packet Tracer 8.2.1 32Bit be installed?

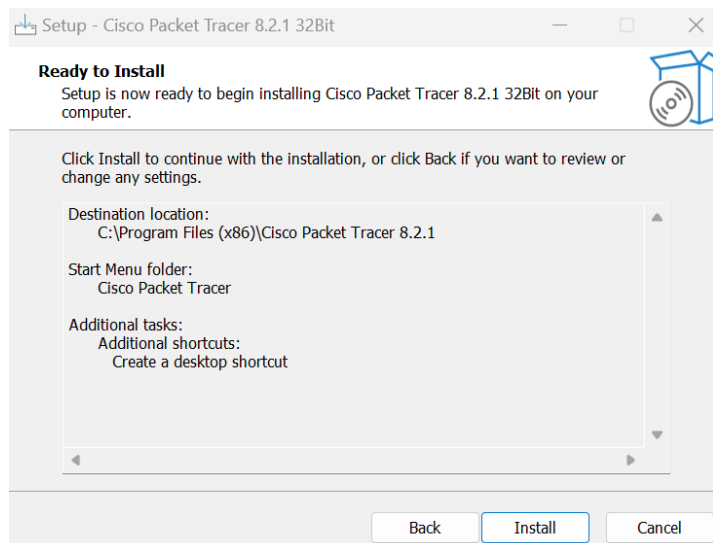
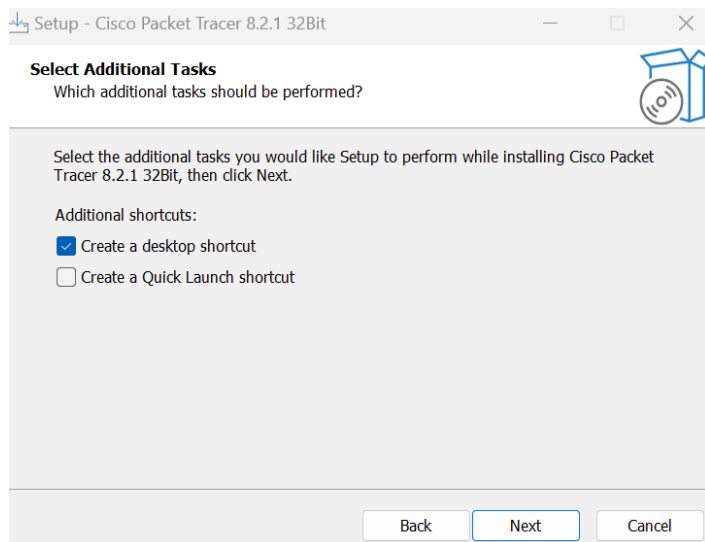
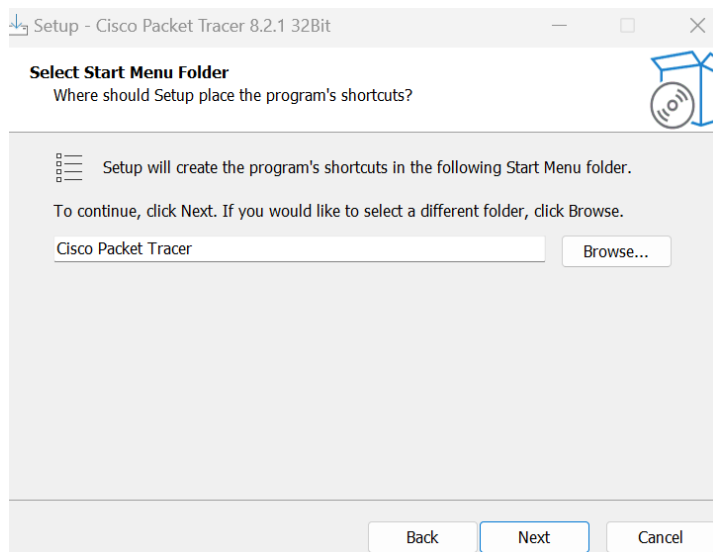
Setup will install Cisco Packet Tracer 8.2.1 32Bit into the following folder.

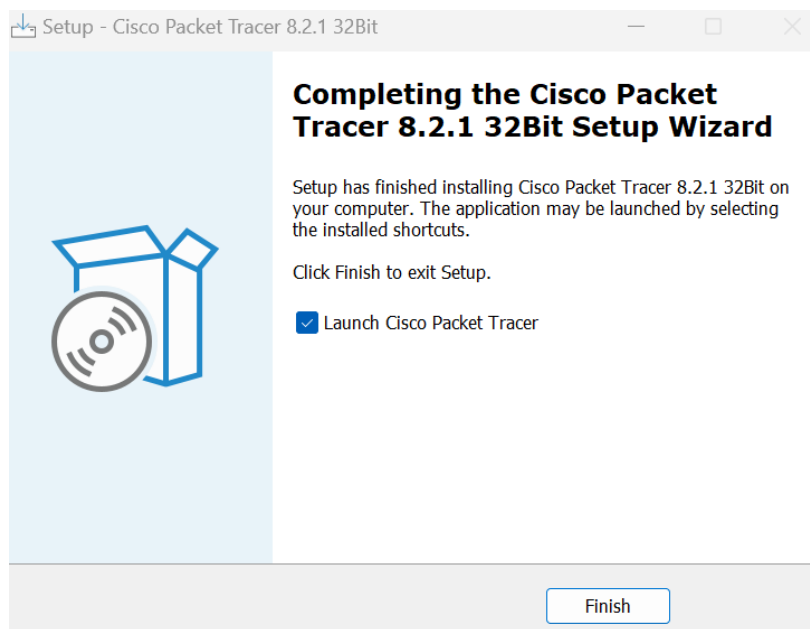
To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\Cisco Packet Tracer 8.2.1 Browse...

At least 513,8 MB of free disk space is required.

Back Next Cancel





← Retour

Inscription

Votre compte de réseau social sera connecté à votre nouveau compte Cisco.

E-mail
aaron.agustin@laplateforme.io

Prénom

Aaron

Nom

Agustin

Poursuivre

JOB 02

Qu'est-ce qu'un réseau?

Un réseau est un groupement de deux ou plusieurs ordinateurs ou autres appareils électroniques permettant l'échange de données et le partage de ressources communes.

À quoi sert un réseau informatique ?

Un réseau informatique est un ensemble d'ordinateurs et d'autres dispositifs électroniques interconnectés qui communiquent entre eux. Ces réseaux servent à faciliter le partage de ressources, d'informations et de services.

Quel matériel avons-nous besoin pour construire un réseau ? Détaillez les

fonctions de chaque pièce.

La construction d'un réseau informatique nécessite différents composants matériels qui remplissent des fonctions spécifiques pour assurer la connectivité et la communication entre les dispositifs. Voici une liste de certains composants matériels clés nécessaires pour construire un réseau, avec une brève explication de leurs fonctions :

1. Ordinateurs (Nœuds) : Les ordinateurs constituent les nœuds du réseau, où les utilisateurs accèdent aux ressources partagées et communiquent entre eux.

2. Serveurs : Les serveurs sont des ordinateurs spécialement configurés pour fournir des services spécifiques au réseau, tels que le stockage de fichiers, la gestion d'applications, le courrier électronique, etc.

3. Routeurs : Les routeurs dirigent le trafic entre différents réseaux. Ils prennent des décisions de routage pour déterminer le chemin optimal pour acheminer les données d'un réseau à un autre.

4. Commutateurs (Switches) : Les commutateurs connectent plusieurs dispositifs au sein d'un même réseau local (LAN). Ils opèrent au niveau de la couche de liaison de données du modèle OSI et permettent une communication efficace entre les nœuds.

5. Hubs : Bien que moins courants aujourd'hui en raison de leur fonctionnement de diffusion inefficace, les hubs étaient utilisés pour connecter plusieurs dispositifs dans un réseau. Cependant, les commutateurs sont généralement préférés en raison de leur efficacité supérieure.

6. Câbles : Les câbles sont utilisés pour connecter physiquement les dispositifs au sein d'un réseau. Les câbles Ethernet sont couramment utilisés pour les réseaux filaires, tandis que les câbles de fibre optique offrent une connectivité haut débit.

7. Cartes réseau (NIC - Network Interface Card) : Les cartes réseau sont des composants matériels installés dans les ordinateurs, leur permettant de se connecter au réseau. Elles peuvent être intégrées à la carte mère ou ajoutées sous forme de cartes d'extension.

8. Points d'accès (Access Points) : Pour les réseaux sans fil (Wi-Fi), les points d'accès permettent aux dispositifs équipés de cartes réseau sans fil de se connecter au réseau.

9. Modems : Les modems convertissent les signaux numériques des ordinateurs en signaux analogiques pour la transmission sur des lignes de communication analogiques. Ils sont souvent utilisés pour la connexion à Internet via des lignes téléphoniques, câble ou fibre optique.

10. Firewalls : Les pare-feu sont des dispositifs ou des logiciels qui surveillent et contrôlent le trafic réseau en fonction de règles de sécurité prédéfinies. Ils protègent le réseau contre les accès non autorisés.

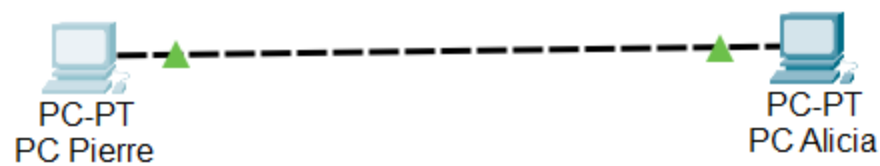
11. Systèmes de stockage en réseau (NAS - Network Attached Storage) : Les dispositifs NAS fournissent un stockage centralisé accessible par le réseau. Ils permettent de stocker et de partager des fichiers de manière centralisée.

12. Imprimantes réseau : Les imprimantes réseau sont des imprimantes connectées au réseau, permettant à plusieurs utilisateurs d'imprimer à partir de différents emplacements.

Chaque composant a une fonction spécifique dans l'infrastructure réseau, contribuant à assurer une connectivité stable, des performances efficaces et une sécurité adéquate. La combinaison de ces éléments forme un réseau fonctionnel capable de répondre aux besoins spécifiques de l'environnement.

Job 03

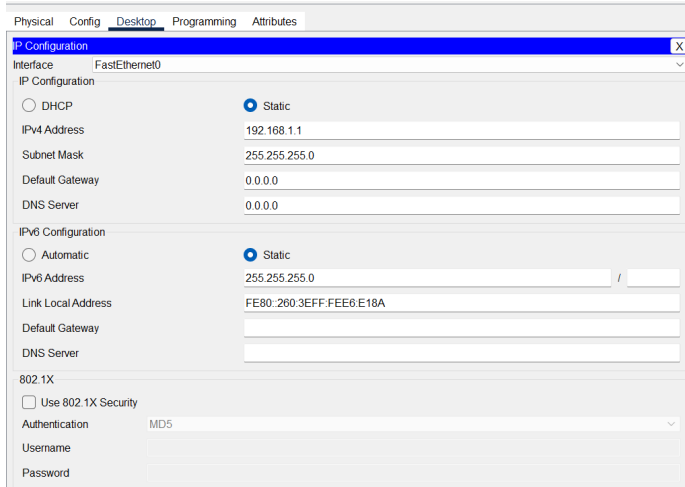
On doit connecter deux pc en sélectionnant un câble qui va permettre d'établir une connexion réseau fast ethernet.



J'ai décidé de partir sur le câble croisée (crossover cable) car elles sont généralement utilisées pour connecter des dispositifs similaires, par exemple, deux ordinateurs ou deux commutateurs.

Job 04

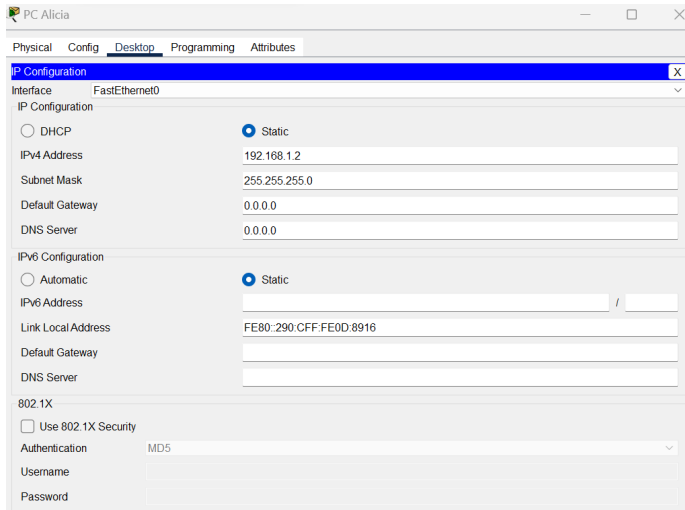
On donne une adresse ip à chaque pc voici l'adresse ip du pc de Pierre



The screenshot shows the 'IP Configuration' window for the 'FastEthernet0' interface. The 'Static' radio button is selected under 'IP Configuration'. The 'IPv4 Address' is set to 192.168.1.1, the 'Subnet Mask' is 255.255.255.0, and the 'Default Gateway' is 0.0.0.0. The 'DNS Server' is also 0.0.0.0. Under 'IPv6 Configuration', the 'Static' radio button is selected, with an 'IPv6 Address' of 255.255.255.0 and a 'Link Local Address' of FE80::260:3EFF:FEE6:E18A. The '802.1X' section is expanded, showing 'Use 802.1X Security' as unchecked, 'Authentication' as MD5, and empty fields for 'Username' and 'Password'.

Field	Value
Interface	FastEthernet0
IP Configuration	Static
IPv4 Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0
IPv6 Configuration	Static
IPv6 Address	255.255.255.0
Link Local Address	FE80::260:3EFF:FEE6:E18A
Default Gateway	
DNS Server	
802.1X	
Use 802.1X Security	Unchecked
Authentication	MD5
Username	
Password	

et voici l'adresse ip du pc d'alicia



The screenshot shows the 'IP Configuration' window for the 'FastEthernet0' interface. The 'Static' radio button is selected under 'IP Configuration'. The 'IPv4 Address' is set to 192.168.1.2, the 'Subnet Mask' is 255.255.255.0, and the 'Default Gateway' is 0.0.0.0. The 'DNS Server' is also 0.0.0.0. Under 'IPv6 Configuration', the 'Static' radio button is selected, with an 'IPv6 Address' field, a 'Link Local Address' of FE80::290:CFF:FE0D:8916, and empty fields for 'Default Gateway' and 'DNS Server'. The '802.1X' section is expanded, showing 'Use 802.1X Security' as unchecked, 'Authentication' as MD5, and empty fields for 'Username' and 'Password'.

Field	Value
Interface	FastEthernet0
IP Configuration	Static
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0
IPv6 Configuration	Static
IPv6 Address	
Link Local Address	FE80::290:CFF:FE0D:8916
Default Gateway	
DNS Server	
802.1X	
Use 802.1X Security	Unchecked
Authentication	MD5
Username	
Password	

Questions :

Qu'est-ce qu'une adresse IP ?

Une adresse IP 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 des paquets de données sur Internet.

À quoi sert un IP ?

Votre adresse IP est votre numéro d'identification qui a été attribué à votre ordinateur connecté à un réseau Internet. Concrètement, ce matricule sert à identifier les machines et à leur permettre de dialoguer entre elles, en échangeant des données sur Internet.

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.

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

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.

JOB 05

La ligne de commande qu'on doit utiliser pour vérifier l'id des machines est " show processes"

```
Router>show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID QTy PC Runtime (ms) Invoked uSecs Stacks TTY Process
 1 Csp 602F3AF0 0 1627 0 2600/3000 0 Load Meter
 2 Lwe 60C5BE00 4 136 29 5572/6000 0 CEF Scanner
 3 Lst 602D90F8 1676 837 2002 5740/6000 0 Check heaps
 4 Cwe 602D08F8 0 1 0 5568/6000 0 Chunk Manager
 5 Cwe 602DF0E8 0 1 0 5592/6000 0 Pool Manager
 6 Mst 60251E38 0 2 0 5560/6000 0 Timers
 7 Mwe 600D4940 0 2 0 5568/6000 0 Serial Backgrou
 8 Mwe 6034B718 0 1 0 2584/3000 0 OIR Handler
 9 Mwe 603FA3C8 0 1 0 5612/6000 0 IPC Zone Manage
10 Mwe 603FA1A0 0 8124 0 5488/6000 0 IPC Periodic Ti
11 Mwe 603FA220 0 9 0 4884/6000 0 IPC Seat Manage
12 Lwe 60406818 124 2003 61 5300/6000 0 ARP Input
13 Mwe 60581638 0 1 0 5760/6000 0 HC Counter Time
14 Mwe 605E3D00 0 2 0 5564/6000 0 DDR Timers
15 Msp 80164A38 0 79543 0 5608/6000 0 GraphIt
16 Mwe 802DB0FC 0 2 011576/12000 0 Dialer event
17 Cwe 801E74BC 0 1 0 5808/6000 0 Critical Bkgnd
18 Mwe 80194D20 4 9549 010428/12000 0 Net Background
19 Lwe 8011E9CC 0 20 011096/12000 0 Logger
20 Mwe 80140160 8 79539 0 5108/6000 0 TTY Background
--More--
```

PC Pierre :

```
C:\>Ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: FE80::205:5EFF:FE79:E751
    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
```

PC Alicia :

```
C:\>Ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: FE80::20C:CFFF:FE4D:CA54
    IPv6 Address...: ::
    IPv4 Address...: 192.168.1.2
    Subnet Mask...: 255.255.255.0
    Default Gateway...: ::
                                0.0.0.0

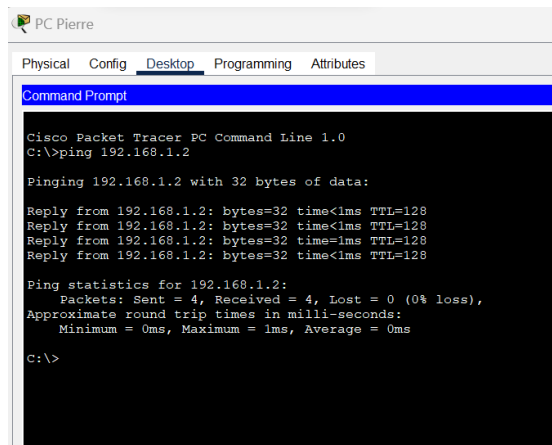
Bluetooth Connection:

    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
```

La commande que j'ai utilisé pour vérifier l'ip est "Ipconfig"

JOB 06 :

On doit désormais ping les deux pc entre eux en utilisant la commande “ping” suivit de



```
PC Pierre
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

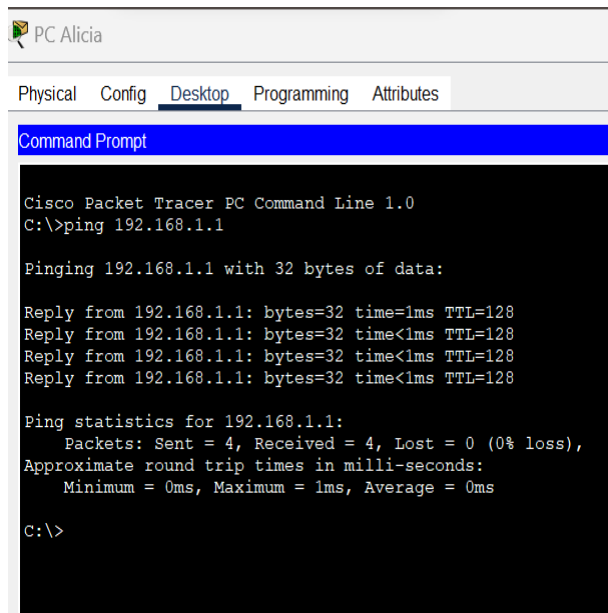
Pinging 192.168.1.2 with 32 bytes of data:

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 = 1ms, Average = 0ms

C:\>
```

l'adresse IP du pc qu'on veut ping.



```
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 = 1ms, Average = 0ms

C:\>
```

JOB 07 :

```
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 n'a rien reçu car lorsqu' on éteint un PC, sa carte réseau est généralement éteinte avec lui. En conséquence, le PC ne peut pas répondre aux requêtes de ping ou à toute autre forme de communication réseau tant qu'il est éteint.

JOB 08 :

Quelle est la différence entre un hub et un switch ?

La grande différence entre le hub et le switch informatique est la façon dont les trames sont livrées. Le hub n'a aucun moyen de distinguer vers quel port une trame doit être envoyée tandis que Le commutateur effectue un tri des trames afin de les orienter vers le bon port et donc vers le bon équipement.

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

Un hub (concentrateur en français) est un dispositif de réseau qui opère au niveau de la couche physique (couche 1) du modèle OSI. Sa fonction principale est de retransmettre les données qu'il reçoit à toutes les machines connectées à ses ports, indépendamment de l'adresse de destination.

Les avantages d'un Hub :

Coût : Les hubs sont généralement moins chers que d'autres dispositifs de réseau plus intelligents comme les commutateurs.

Facilité d'utilisation : Ils sont simples à utiliser car ils ne nécessitent généralement aucune configuration. Il vous suffit de les connecter, et ils commencent à fonctionner.

Les inconvénients d'un Hub :

Collision de données : Étant donné que le hub transmet les données à tous les ports, il peut y avoir des collisions de données si plusieurs machines tentent de transmettre simultanément. Cela peut entraîner une perte de performances et des temps d'attente.

Bande passante partagée : Tous les dispositifs connectés à un hub partagent la même bande passante. Si plusieurs machines sont actives simultanément, la bande passante disponible est divisée entre elles, ce qui peut entraîner des performances médiocres.

Manque de sécurité : Comme toutes les données sont diffusées à tous les ports, il est plus difficile de sécuriser le réseau. Un utilisateur peut potentiellement capturer et analyser le trafic destiné à d'autres machines.

Limitations d'évolution : Les hubs sont obsolètes dans les réseaux modernes en raison de leurs limitations. Les commutateurs sont maintenant préférés car ils offrent des performances meilleures et plus prévisibles.

Avantage d'un switch :

Élimination des collisions : Contrairement aux hubs, les commutateurs utilisent des tables de commutation pour diriger le trafic uniquement vers le port destinataire, éliminant ainsi les collisions de données.

Meilleure performance : Les commutateurs offrent une meilleure performance que les hubs, car ils réduisent la congestion du réseau en transmettant sélectivement les données aux périphériques concernés.

Bande passante dédiée : Chaque port du switch dispose de sa propre bande passante, ce qui signifie que la bande passante totale du switch est partagée entre tous les périphériques connectés. Cela permet une utilisation plus efficace de la bande passante.

Sécurité améliorée : Étant donné que les commutateurs transmettent les données uniquement au périphérique destinataire, il est plus difficile pour les utilisateurs non autorisés de capturer et d'analyser le trafic réseau.

Évolutivité : Les commutateurs offrent une meilleure évolutivité que les hubs. Les réseaux peuvent être étendus en ajoutant simplement des commutateurs supplémentaires.

Prise en charge de la communication full-duplex : Les commutateurs permettent une communication full-duplex, ce qui signifie que les données peuvent être transmises et reçues simultanément, améliorant ainsi l'efficacité.

Inconvénient d'un switch :

Coût : Les commutateurs sont généralement plus coûteux que les hubs en raison de leur complexité et de leurs fonctionnalités avancées.

Complexité de configuration : Bien que la plupart des commutateurs ne nécessitent pas une configuration étendue pour une utilisation de base, des configurations plus avancées peuvent être complexes.

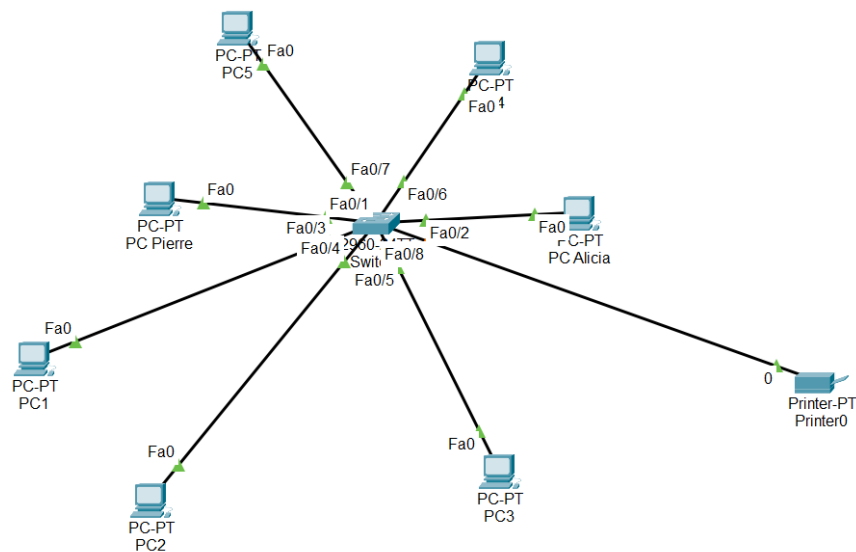
Dépendance aux protocoles réseau : Les commutateurs dépendent des protocoles réseau tels que le protocole Spanning Tree Protocol (STP) pour éviter les boucles de commutation. Une mauvaise configuration ou un réseau instable peuvent entraîner des problèmes.

Limitations de ports : Les commutateurs peuvent avoir une limite physique sur le nombre de ports disponibles. Des commutateurs empilables ou modulaires peuvent être nécessaires pour étendre le nombre de ports disponibles.

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

Un switch gère le trafic réseau de manière efficace en utilisant des tables de commutation (ou tables MAC) pour diriger les trames vers les ports appropriés.

JOB 09 :



Les 3 avantages d'un schéma est que premièrement elle offre une compréhension de lecture claire et simple.

Elle vous permettra d'obtenir une vue d'ensemble sur les étapes à faire dans le futur.

Et facilite l'apprentissage.

Sur le schéma on peut comprendre de façon claire que les ordinateurs sont reliés à une switch, on peut également apercevoir que l'imprimante est également connectée au réseau.

JOB 10 :

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

Comme l'adresse IP statique requiert des configurations manuelles, elle peut créer des problèmes de réseau en cas d'utilisation sans une bonne maîtrise du protocole TCP/IP. DHCP est un protocole permettant d'automatiser la tâche d'attribution des adresses IP.

Pour mettre en place le serveur DHCP il faut tout d'abord ajouter une switch sur notre composition



Ensuite on ajoute également un serveur

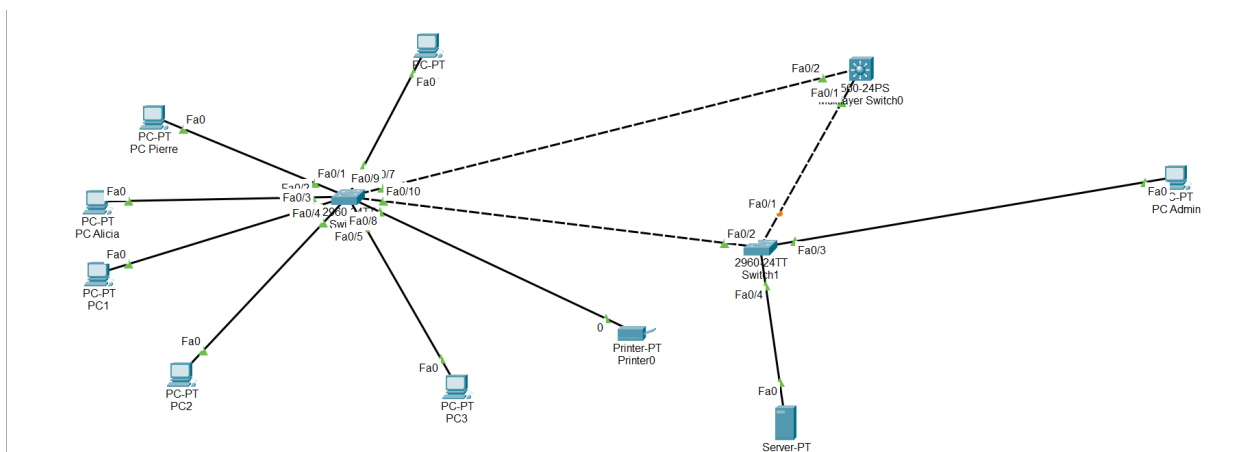


On ajoute ensuite une switch multilayer



Une fois que tout ça est fait, on connecte un ordinateur à la nouvelle switch et on connecte également le serveur à la switch.

On connecte ensuite les deux switch vers la switch multilayer formant un triangle comme ceci.



Une fois que c'est fait on va désormais commencer la configuration de notre serveur DHCP, on commence tout d'abord par renommer le serveur en DHCP.

DHCP

Physical **Config** Services Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

FastEthernet0

Port Status

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ On

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 000D.BD1B.A547

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 192.168.1.3

Subnet Mask 255.255.255.0

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address /

Link Local Address: FE80::20D:BDFF:FE1B:A547

On va dans config et on lui créer une adresse IP ainsi qu'un sous masque réseau.

On va ensuite dans "services" et dans "DHCP" on ajoute une default gateway ici c'est "192.168.1.1" et DNS server qui sera "10.10.0.1". On finit ensuite en cochant la case "on" pour activer le service.

DHCP

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

InterfaceFastEthernet0ServiceOnOff

Pool NamePOOL1

Default Gateway192.168.1.1

DNS Server10.10.0.1

Start IP Address :19216810

Subnet Mask:2552552550

Maximum Number of Users :256

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
POOL1	192.168.1.1	10.10.0.1	192.168.1.0	255.255.2...	256	0.0.0.0	0.0.0.0

Et pour attribuer des adresses IP automatiquement au autres ordinateurs il suffit d'aller sur le pc en question dans "desktop" cliquez sur "ip configuration"

The screenshot shows the 'PC3' desktop environment with the following icons and labels:

- IP Configuration**: Represented by an icon of a server rack with the number 106.
- Dial-up**: Represented by an icon of a network router.
- Terminal**: Represented by an icon of a computer monitor with a command prompt symbol (>).
- Command Prompt**: Represented by an icon of a document with the word 'run' on it.
- Web Browser**: Represented by an icon of a globe with the text 'http:'.

PC3

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::290:2BFF:FEA4:660D

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

On coche alors la case “DHCP” ce qui devrait nous donner ceci :

PC3

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address 192.168.1.5

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

Elle génère donc automatiquement une adresse IP.

JOB 11 :

1 sous réseau de 12 hôtes

10.2.0.1 a 10.2.0.12	255.255.255.0
----------------------	---------------

5 sous-réseaux de 30 hôtes

10.3.0.1 a 10.3.0.30	255.255.255.0
10.4.0.1 a 10.3.0.30	255.255.255.0
10.5.0.1 a 10.5.0.30	255.255.255.0
10.6.0.1 a 10.6.0.30	255.255.255.0
10.7.0.1 a 10.7.0.30	255.255.255.0

5 sous-réseaux de 120 hôtes

10.8.0.1 a 10.8.0.120	255.255.255.0
10.9.0.1 a 10.9.0.120	255.255.255.0
10.10.0.1 a 10.10.0.120	255.255.255.0
10.11.0.1 a 10.11.0.120	255.255.255.0
10.12.0.1 a 10.12.0.120	255.255.255.0

5 sous-réseaux de 160 hôtes

10.13.0.1 a 10.13.0.160	255.255.255.0
10.14.0.1 a 10.14.0.160	255.255.255.0
10.15.0.1 a 10.15.0.160	255.255.255.0
10.16.0.1 a 10.16.0.160	255.255.255.0
10.17.0.1 a 10.17.0.160	255.255.255.0

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

On a choisi une adresse IP 10.0.0.0 de classe A car c'est tout d'abord une adresse privée et que l'on peut utiliser dans réseau local, de plus les adresses IP privées ne peuvent pas être utilisées sur internet. Les hôtes qui les utilisent sont visibles uniquement dans votre réseau local.

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

Classe A

Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

Classe B

Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

Classe C

Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

JOB 12 :

7 Application	<p>Point d'accès au services réseau</p> <p><i>La couche 7 est connue de la plupart des gens car elle communique directement avec l'utilisateur. Une application qui s'exécute sur un appareil peut communiquer avec d'autres couches OSI, mais l'interface fonctionne sur la couche 7.</i></p>	<p>FTP : Il fournit des services de transfert de fichiers et d'interaction avec l'utilisateur. Cette couche est la plus proche de l'utilisateur final et gère les échanges entre les applications. FTP opère à un niveau d'abstraction plus élevé, permettant aux utilisateurs de naviguer dans les répertoires, télécharger et téléverser des fichiers, et effectuer des opérations de gestion des fichiers.</p>
6 Présentation	Conversion et chiffrement de données	
5 Session	Communication interhost	
4 Transport	<p>Connexion de bout en bout et contrôle de flux (TCP)</p> <p><i>C'est à cette couche que se trouvent les méthodes courantes de cryptage et de sécurité des pare-feu.</i></p>	<p>TCP :</p> <p>La couche transport du modèle OSI se concentre sur deux protocoles, TCP (Transmission Control Protocol) et UDP (User Datagram Protocol). Les professionnels du secteur considèrent le TCP comme un protocole fiable ou orienté connexion.</p>

		<p><u>SSL/TLS</u> : fonctionne au niveau de la couche de transport pour sécuriser les connexions entre deux entités communicantes. Il s'agit principalement de sécuriser les échanges de données entre l'expéditeur et le destinataire, offrant une couche de chiffrement pour protéger la confidentialité et l'intégrité des données.</p> <p><u>L'UDP</u> : Se trouve à la couche 4 du modèle OSI, car c'est là qu'il gère la communication entre applications sur différents appareils. Il offre une méthode légère, rapide et sans connexion pour transmettre des données. L'UDP n'assure pas la livraison garantie des données, mais il est utilisé dans des situations où la rapidité est plus importante que la fiabilité, comme dans la diffusion en temps réel, les jeux en ligne, ou les applications de streaming vidéo.</p>
--	--	--

3 Réseau

Détermine le parcours et l'adressage logique (IP)

Cette couche est responsable du routage des paquets de données à travers un réseau, fournissant un mécanisme pour que les données atteignent leur destination finale.

IPv4 :

Le fait que l'IPv4 est dans la couche 3 s'explique par le rôle fondamental d'IPv4 dans la transmission de données sur un réseau et la fourniture d'un service de routage.

IPv6 : Est positionné à la couche 3 du modèle OSI en raison de son rôle fondamental dans la gestion des adresses IP, le routage des paquets, et l'encapsulation des données pour la transmission sur les réseaux.

Le routeur : Se situe à la couche 3 du modèle OSI, la couche réseau, car il joue un rôle clé dans le routage des paquets de données entre différents réseaux. En utilisant des adresses IP pour identifier les destinations, le routeur prend des décisions de routage pour diriger efficacement les paquets à travers des réseaux interconnectés.

2 Liaison de données

Adressage physique (MAC et LLC)

La couche de liaison de données établit et met fin à une connexion entre deux nœuds connectés physiquement sur un réseau. Il divise les paquets en cadres et les envoie de la source à la destination.

L'ethernet : A pour rôle de découper les informations en trames ayant une certaine signification et la reconnaissance de ces trames à la réception. Elle a aussi pour rôle de gérer les erreurs sur le support physique.

MAC :

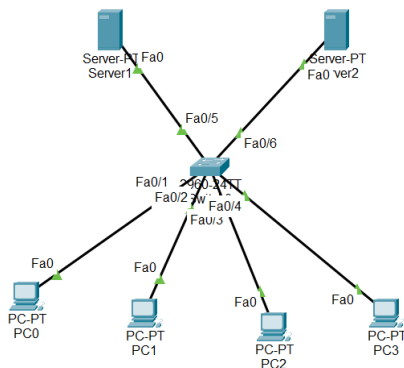
La couche MAC couvre l'adressage physique du périphérique réseau, comme l'adresse MAC des cartes d'interface. Il s'agit d'une adresse de 48 bits qui rend toutes les cartes uniques par rapport à toutes les autres cartes sur tous les autres périphériques.

Fibre optique : Cette couche est responsable de la gestion des erreurs et du contrôle d'accès au support. Dans le contexte de la fibre optique, cette couche peut être impliquée dans des aspects tels que la détection et la correction d'erreurs qui peuvent survenir lors de la transmission des données sur la fibre.

PPTP : utilise cette couche pour encapsuler les paquets PPP dans des trames de liaison de données, généralement sur des connexions de type point à point. Cela permet la création de tunnels virtuels pour transporter le trafic PPP sur des réseaux IP, tels qu'Internet.

		<p>Wi-Fi : La couche liaison de données gère le partage du canal radio entre plusieurs périphériques et organise le formatage des trames qui sont transmises sans fil.</p>
<p>1 Physique</p>	<p>Transmission non binaire numérique ou analogique</p> <p><i>Cette couche est la première couche du modèle et est responsable de la transmission brute des bits sur un support physique. Elle fournit l'interface matérielle entre le périphérique émetteur et le périphérique récepteur.</i></p>	<p>Fibre optique : Cette couche est responsable de la transmission brute des bits sur un support physique, qu'il s'agisse de câbles en cuivre, de fibres optiques, d'ondes radio, etc. La fibre optique, étant le support physique pour la transmission de la lumière, est principalement associée à la couche physique.</p> <p>Wi-Fi : Cela inclut la modulation des signaux radiofréquences pour la communication sans fil. Les aspects tels que la fréquence, la modulation, la puissance de transmission et d'autres caractéristiques physiques du signal Wi-Fi sont définis à cette couche.</p> <p>Câble RJ45 : Le câble RJ45 est une composante physique qui se situe à la couche 1 du modèle OSI, facilitant la transmission des données à travers les différentes couches du modèle OSI.</p>

JOB 13 :



Quelle est l'architecture de ce réseau ?

L'architecture de ce réseau est un réseau de type LAN (Local Area Network), c'est un réseau local simple où tous les périphériques partagent la même plage d'adresses IP et peuvent communiquer directement les uns avec les autres.

Indiquer quelle est l'adresse IP du réseau ?

L'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 le réseau est de 254 et non 255, 255 étant l'adresse de diffusion.

Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion de ce réseau est 192.168.10.255

cette adresse permet de diffuser, communiquer avec toutes les machines du réseau donc si on veut envoyer une information à tous les ordinateurs du réseau on utilise alors cette adresse.

JOB 14 :

Convertissez les adresses IP suivantes en binaires :

145.32.59.24 = 10010001.00100000.00111011.00011000

200.42.129.16 = 11001000.00101010.10000001.00010000

14.82.19.54 = 00001110.01010010.00010011.00110110

JOB 15 :

Qu'est-ce que le routage ?

Le routage est le processus de sélection du chemin dans un réseau. Un réseau informatique est composé de nombreuses machines, appelées nœuds, et de chemins ou de liaisons qui relient ces nœuds. La communication entre deux nœuds d'un réseau interconnecté peut s'effectuer par de nombreux chemins différents.

Qu'est-ce qu'un gateway ?

La Gateway est le dispositif par lequel deux réseaux informatiques ou deux réseaux de télécommunication de nature différente 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.

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.

Qu'est-ce qu'un DNS ?

Les serveurs DNS traduisent des demandes de noms en adresses IP, en contrôlant à quel serveur un utilisateur final va se connecter quand il tapera un nom de domaine dans son navigateur. Ces demandes sont appelées requêtes.