**Introduction**

Il est essentiel que vous compreniez les bases du fonctionnement des réseaux et comment utiliser différents appareils pour créer des réseaux. En plus du fait que les réseaux sont constitués de différents appareils réseau, il existe plusieurs aspects à prendre en compte. Par exemple, les protocoles de communication réseau exigent que des adresses réseau soient attribuées aux appareils. Vous devez également sécuriser votre réseau pour protéger les ressources et biens de votre organisation.

Dans ce module, vous explorez comment les réseaux communiquent les uns avec les autres. Vous apprenez également les protocoles et les normes réseau, ainsi que la différence entre un réseau étendu (**WAN**) et un réseau local (**LAN**). Enfin, vous étudiez en détail le protocole **TCP/IP (Transmission Control Protocol and Internet Protocol)**, les adresses **IP** et les ports.

Bien que le contenu de ce module s’applique à tous les réseaux, nous vous montrons où et comment les concepts s’appliquent aux réseaux gérés avec Azure.

**Objectifs d’apprentissage**

Dans ce module, vous allez découvrir comment :

Expliquer les différences entre réseau étendu (**WAN**), réseau personnel **(PAN**) et réseau local (**LAN**)

Lister les différents protocoles et normes réseau

Expliquer les concepts de communication réseau comme le modèle TCP/IP, le DNS et les ports

Découvrir le lien qui existe entre ces composants de base et le réseau Azure

**Types de réseaux et topologies à utiliser lors de la conception d’un réseau**

Tous les réseaux reposent sur les mêmes principes. Vous pouvez appliquer ces principes pour concevoir et créer les réseaux locaux ou cloud de votre organisation. Lorsque vous créez un réseau, vous devez connaître les différents types de réseaux qui existent, leurs topologies et leurs utilisations.

Dans cette unité, vous explorez certains des principaux types de topologies de réseau qui sont utilisés pour créer des réseaux Internet.

**Qu’est-ce qu’un réseau ?**

Un réseau est un ensemble d’appareils réseau, comprenant généralement des ordinateurs, des commutateurs, des routeurs, des imprimantes et des serveurs. Les réseaux occupent une place très importante dans notre quotidien, que ce soit au domicile, au bureau ou dans les lieux publics. Les réseaux permettent à tous les types d’appareils réseau de communiquer.

**Types de réseaux**

Les réseaux varient en taille, en forme et en utilisation. Pour faciliter l’identification des différents types de réseaux, nous les avons classés dans l’une des catégories suivantes :

Réseaux personnels (**PAN**)

Réseaux locaux (**LAN**)

Réseaux métropolitains (**MAN**)

Réseaux étendus **(WAN**)

**Qu’est-ce qu’un réseau personnel ?**

Un réseau personnel **(PAN**) couvre les besoins en réseau d’une personne. Par exemple, un réseau **PAN** est celui qui est utilisé par nos smartphones, montres connectées, tablettes et ordinateurs portables pour communiquer et partager des données sans avoir à se connecter à un point d’accès ou à d’autres services réseau tiers. Les réseaux **PAN** utilisent généralement le Bluetooth pour communiquer, car il fournit une fonctionnalité de partage de données à courte portée et à faible puissance. Les normes réseau associées à un **PAN** sont Bluetooth et **IEEE 802.15.**

**Qu’est-ce qu’un réseau local ?**

Un réseau local (**LAN**) couvre les besoins en réseau d’un site. Il peut s’agir d’une entreprise, d’une école, d’une université, d’un hôpital, d’un aéroport, etc. Généralement, un réseau local est privé et y accéder demande une authentification et une autorisation. Parmi les différents types de réseaux, le réseau LAN est de loin le réseau le plus utilisé.

**Qu’est-ce qu’un réseau métropolitain ?**

Un réseau métropolitain (**MAN**) permet de connecter deux sites différents au sein d’une ville ou d’une zone urbaine, afin de fournir un réseau étendu unique. En général, un réseau **MAN** nécessite une connexion dédiée et sécurisée entre chaque réseau local qui y est connecté.

**Qu’est-ce qu’un réseau étendu ?**

Le réseau étendu (**WAN**) permet de connecter deux zones géographiques à l’échelle locale ou mondiale. Par exemple, vous pouvez utiliser un réseau étendu pour connecter le siège social d’une organisation aux succursales qui se trouvent dans toute la région. Un **WAN** relie plusieurs **LAN** ensemble afin de créer un super réseau. Avec un réseau **WAN**, vous utilisez un réseau privé virtuel (**VPN**) pour gérer la connexion entre les différents réseaux **LAN.**

Différences entre les réseaux **LAN** et **WAN**

Plusieurs aspects distinguent un **LAN** d’un **WAN**. Le fait de connaître ces éléments permet de planifier plus facilement les services à déployer sur ces réseaux.

**LAN**

Un réseau local est un réseau privé généralement limité à un seul bâtiment.

**WAN**

Un réseau étendu (**WAN**) permet de relier entre eux des bureaux situés dans une zone géographique différente. Plusieurs organisations peuvent exploiter des réseaux étendus.

Un **LAN** fournit des débits de 10 Gbit/s ou plus.

Un **WAN** fournit généralement des débits inférieurs à **1 Gbit/s.**

Un **LAN** est moins encombré que les autres types de réseau.

Un **WAN** est plus encombré que les autres types de réseau.

Un **LAN** peut être géré et administré en interne.

Un **WAN** nécessite généralement le recours à un tiers pour sa configuration, ce qui augmente son coût.

**Topologies de réseau**

Une **topologie** de réseau décrit la composition physique d’un réseau. Examinons quatre des topologies qui sont disponibles lors de la conception d’un réseau LAN. Les voici :

**Bus**

**Anneau**

**Maillage**

**Étoile**

**Topologie de bus**

Dans une topologie de bus, chaque appareil réseau est connecté à un seul câble réseau. Même s’il s’agit du type de réseau le plus simple à mettre en œuvre, il présente certaines limitations. La première limitation concerne la longueur du câble principal ou du bus. Plus il est long, plus le risque de perte de signal est élevé. Cette limitation conditionne la disposition physique du réseau. Tous les appareils doivent être physiquement situés à proximité les uns des autres, par exemple, dans la même pièce. Enfin, en cas rupture du câble du bus, c’est tout le réseau qui tombe en panne.

**Topologie en anneau**

Dans une topologie en anneau, chaque appareil réseau est connecté à son voisin pour former un anneau. Cette forme de réseau est plus résiliente que la topologie de bus. Une rupture de l’anneau du câble affectera également les performances du réseau.

**Topologie de maillage**

**La topologie de maillage est décrite comme un maillage physique ou un maillage logique.**

Dans un maillage physique, chaque appareil réseau se connecte à tous les autres appareils du réseau. Cette topologie augmente considérablement la résilience du réseau, mais elle nécessite une connexion physique de tous les appareils. Aujourd’hui, peu de réseaux reposent sur un maillage complet. La plupart des réseaux utilisent un maillage partiel dans lequel certaines machines s’interconnectent, tandis que d’autres se connectent via un seul appareil.

Il existe une légère différence entre un réseau à maillage physique et un réseau à maillage logique. La plupart des réseaux modernes sont basés sur un maillage, car chaque appareil peut voir et communiquer avec tous les autres appareils du réseau. Toutefois, cette topologie décrit un réseau de maillage logique et est essentiellement possible en utilisant des protocoles réseau.

La topologie en étoile est la topologie de réseau la plus courante. Chaque périphérique réseau se connecte à un hub ou à un commutateur centralisé. Les commutateurs et les hubs peuvent être reliés entre eux afin d’étendre et de construire des réseaux plus étendus. Ce type de topologie est, de loin, le plus robuste et le plus évolutif.

**Ethernet**

Ethernet est une norme réseau dédiée principalement à des réseaux LAN filaires, mais également utilisée dans les réseaux **MAN** et **WAN**. Utilisée en remplacement d’autres technologies de LAN câblé comme ARCNET et Token Ring, Ethernet s’est imposée comme une norme.

Même si on associe Ethernet aux réseaux câblés, cette norme ne se limite pas à ce type de réseau, car elle peut être utilisée dans les liaisons à fibre optique.

La norme Ethernet définit un cadre pour la transmission des données, le traitement des erreurs et les seuils de performance. Elle décrit les règles de configuration d’un réseau Ethernet, et comment les différents éléments de ce réseau interagissent.

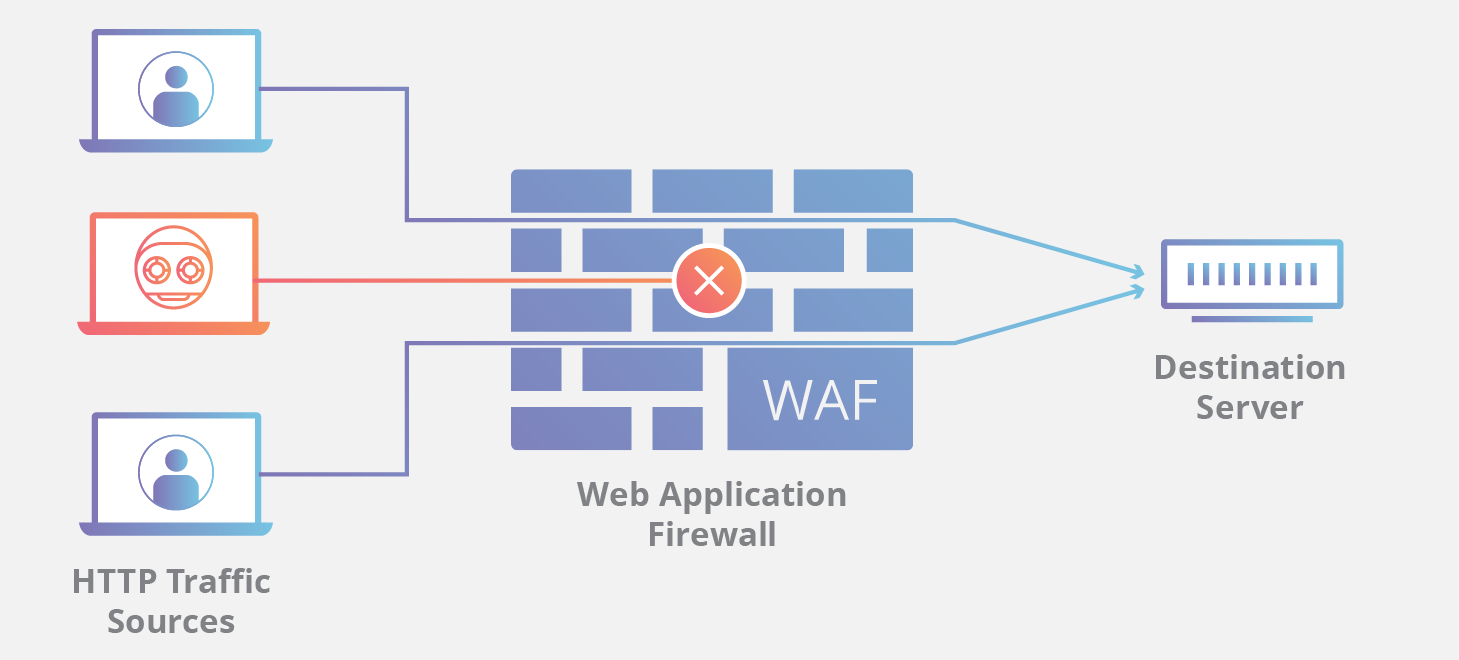
**Topologie en étoile**

Ethernet est utilisé dans le modèle OSI au niveau de la liaison de données et des couches physiques. Il a servi de base à la norme IEEE 802.3. Cette norme a permis d’unifier le développement des réseaux et des composants matériels.

Ethernet est une norme en constante évolution. Sa première version n’offrait qu’une vitesse de transmission de données de 2,94 Mbit/s. Au cours des dernières années, plusieurs versions ont été publiées pour répondre aux demandes d’augmentation de la vitesse. Aujourd’hui, la vitesse peut monter jusqu’à 400 Gbits/s.

**Qu'est-ce qu'un pare-feu ?**

Un pare-feu est un système de sécurité qui surveille et contrôle le trafic réseau en fonction d'un ensemble de règles de sécurité. Les pare-feu sont généralement placés entre un réseau approuvé et un réseau non approuvé ; Le réseau non fiable est souvent Internet. Par exemple, [les réseaux d'entreprise](https://www.cloudflare.com/learning/network-layer/enterprise-networking/) utilisent souvent un pare-feu pour protéger leur réseau contre les menaces en ligne.



Les pare-feu décident s’ils autorisent ou non le passage du trafic entrant et sortant. Ils peuvent être intégrés au matériel, aux logiciels ou à une combinaison des deux. Le terme « pare-feu » a été emprunté à une pratique de construction consistant à construire des murs entre ou à travers des bâtiments pour contenir un incendie. De la même manière, les pare-feu réseau sont destinés à contenir les menaces en ligne.

Pourquoi utiliser un pare-feu ?

Le principal cas d’utilisation d’un pare-feu est la sécurité. Les pare-feu peuvent intercepter le trafic malveillant entrant avant qu'il n'atteigne le réseau, ainsi qu'empêcher les informations sensibles de quitter le réseau.

Les pare-feu peuvent également être utilisés pour filtrer le contenu. Par exemple, une école peut configurer un pare-feu pour empêcher les utilisateurs de son réseau d'accéder au matériel réservé aux adultes. De même, dans certains pays, les gouvernements disposent d'un pare-feu qui peut empêcher les habitants de cet État-nation d'accéder à certaines parties d'Internet.

Pare-feu de filtrage de paquets IP

Un pare-feu de filtre de paquets IP vous permet de créer un ensemble de règles pour éliminer ou accepter le trafic sur une connexion réseau.

Un pare-feu de filtre de paquets IP vous permet de créer un ensemble de règles qui suppriment ou acceptent le trafic sur une connexion réseau. Le pare-feu lui-même n'affecte en rien ce trafic. Étant donné que le filtre de paquets ne peut éliminer que le trafic qui lui est envoyé, le périphérique de filtrage de paquets doit effectuer le routage IP ou être la destination du trafic.

Un filtre de paquets possède un ensemble de règles avec des actions d'acceptation ou de rejet. Lorsque le filtre de paquets reçoit un paquet d'informations, il le compare à l'ensemble de règles préconfiguré. Lorsque la première correspondance se produit, le filtre de paquets accepte ou rejette le paquet d'informations. La plupart des filtres de paquets ont une règle implicite « refuser toutes les règles » à la fin du fichier de règles.

En règle générale, les filtres de paquets autorisent ou refusent le trafic réseau en fonction de :

* Adresses IP source ou destination
* Protocole, tel que TCP, UDP ou ICMP
* Ports source et de destination, codes et types ICMP
* Indicateurs dans l'en-tête TCP, par exemple si le paquet est une demande déconnexion
* Direction (entrée ou sortie)
* L'interface physique que traverse le paquet

**Comment fonctionne un VPN ? Tout ce que vous devez savoir sur les VPN**

De nos jours, il semble que presque tout le monde utilise un **VPN** pour débloquer des sites Web et protéger sa confidentialité en ligne. Mais que sont exactement les **VPN** et comment fonctionnent-ils ?

**Qu'est-ce qu'un réseau privé virtuel (VPN)**

**Un réseau privé virtuel, ou VPN (Virtual Private Network),** est un réseau privé qui crypte toutes les données envoyées ou reçues sur Internet. Il vous aide à accéder en toute sécurité et en privé aux sites Web et à utiliser vos programmes et applications, quel que soit le réseau que vous utilisez.

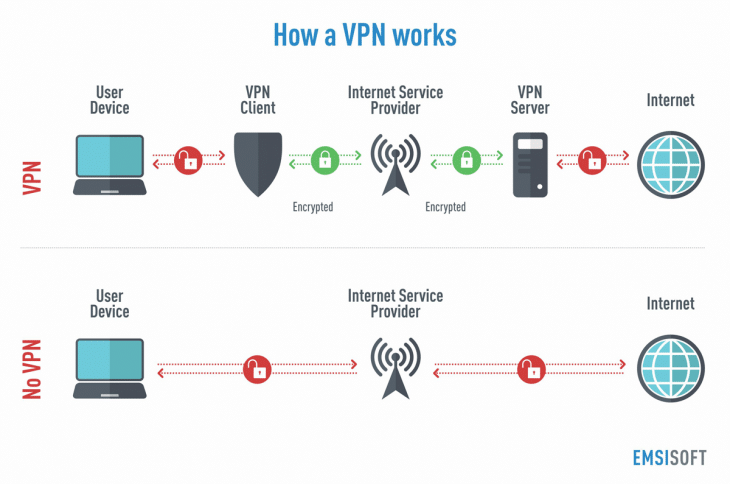
Considérez-le comme un messager sécurisé, récupérant les données du site Web et les transmettant en toute sécurité à votre ordinateur. Tout comme une voiture blindée transporterait de l’argent vers et depuis un guichet automatique.

Il masque également votre **IP** (voici comment vérifier votre IP) et vous permet de modifier votre emplacement afin que vous puissiez accéder au contenu géo-restreint. Par exemple, si votre émission préférée n’est pas disponible sur Netflix dans le pays que vous visitez.

Vous pouvez également accéder à distance au système de fichiers de votre entreprise avec une « adresse **IP** de bureau.

Un **VPN** fonctionne au niveau du système d'exploitation et crypte tout le trafic Internet entrant et sortant.

**Comment fonctionne un VPN ?**



Lors de la communication avec le serveur **VPN,** le client **VPN** utilise le cryptage des données, qui accède à distance au site Web ou aux données que vous avez en tête. Vous avez un intermédiaire des deux côtés. Le client cache votre requête à votre routeur et au fournisseur d'accès Internet (**FAI**), tandis que le serveur **VPN** cache votre identité au site Web ou au service que vous utilisez.

Il existe une grande différence en matière de sécurité lors de l’utilisation de tout type de réseau Wifi public. Les achats en ligne, les opérations bancaires ou même l'envoi d'e-mails professionnels sur un réseau ouvert sont beaucoup plus sûrs avec un **VPN.**

Étant donné que le **VPN** crypte votre connexion, les pirates potentiels ne peuvent pas « écouter » la transmission pour voler des données vulnérables, comme votre numéro de compte, ou pire, votre mot de passe.

Cela empêche également votre FAI ou votre employeur d'espionner votre trafic et ce que vous faites en ligne en reniflant le trafic du routeur.

Si votre entreprise utilise un routeur compatible **VPN,** vous pouvez utiliser un **VPN** pour vous connecter à distance au réseau de votre bureau et accéder aux fichiers de bureau, au CRM ou à d'autres logiciels depuis la route.

**Qu'est-ce qu'un serveur proxy ?**

Un serveur proxy est généralement un serveur public distant accessible via une application Web ou un programme de bureau qui accède aux pages Web en votre nom.

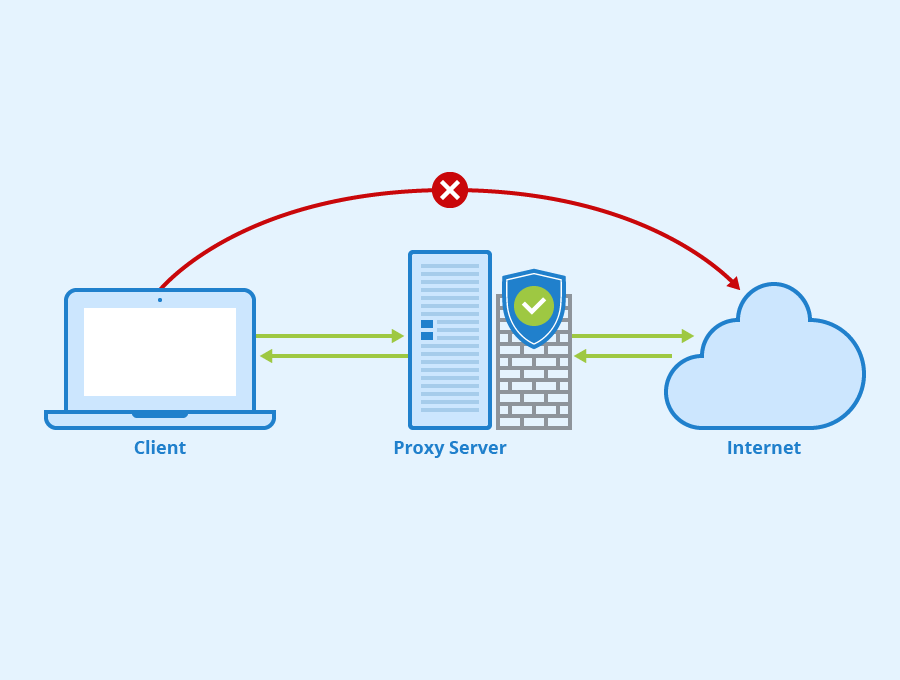
Un serveur proxy fonctionne au niveau de l'application, agissant comme proxy pour une seule application (telle que votre navigateur) à la fois.

De nombreux serveurs proxy ne prennent pas en charge les transferts de données **HTTPS** sécurisés et ne sont pas sécurisés par défaut.

**Comment fonctionne un serveur proxy ?**

Lorsque la plupart des gens utilisent le mot serveur proxy, ils font référence aux proxys HTTP.

Ces serveurs proxy sont des serveurs Web qui accèdent à une page Web via Internet et envoient ensuite les données à votre navigateur.



Contrairement à un **VPN**, votre connexion proxy n'est pas cryptée. Il agit uniquement comme intermédiaire entre votre ordinateur et le serveur final.

En conséquence, un proxy HTTP masquera votre identité sur le site Web, mais ne protégera aucune donnée sensible.

**Introduction**

L'authentification auprès des réseaux sociaux est une pratique de plus en plus courante sur Internet, permettant aux utilisateurs d'accéder à différentes plateformes et services en utilisant les identifiants de leurs comptes sur les réseaux sociaux tels que Facebook, Google, Twitter, entre autres. Dans ce glossaire, nous explorerons en détail ce qu'est l'authentification sociale, son fonctionnement, ses avantages et ses inconvénients, ainsi que les meilleures pratiques pour la mettre en œuvre sur votre site Web ou votre application.

**Qu’est-ce que l’authentification sur les réseaux sociaux ?**

L'authentification sur les réseaux sociaux est un processus qui permet aux utilisateurs d'accéder à un site Web ou à une application spécifique à l'aide des informations d'identification de leur compte de réseau social. Au lieu de créer un nouveau login et mot de passe, l'utilisateur peut simplement cliquer sur un bouton de connexion avec le réseau social de son choix et autoriser l'accès. Cela rend le processus de connexion plus facile et l’expérience utilisateur plus pratique.

**Comment fonctionne l'authentification sur les réseaux sociaux ?**

Lorsqu'un utilisateur choisit de se connecter à un site Web ou à une application à l'aide d'un réseau social, le site Web ou l'application demande l'autorisation d'accéder aux informations du compte de l'utilisateur sur le réseau social choisi. Une fois que l'utilisateur autorise l'accès, le site Web ou l'application reçoit un jeton d'authentification qui valide l'identité de l'utilisateur. Ce **token** est utilisé pour permettre à l'utilisateur d'accéder au site Internet ou à l'application sans avoir à saisir un identifiant et un mot de passe.

**Avantages de l'authentification sur les réseaux sociaux**

L’un des principaux avantages de l’authentification sur les réseaux sociaux est la commodité pour l’utilisateur. En un seul clic, l'utilisateur peut accéder à différentes plateformes et services sans avoir à mémoriser plusieurs identifiants et mots de passe. De plus, l’authentification des réseaux sociaux peut accroître la sécurité, car les réseaux sociaux disposent de systèmes avancés de protection des données.

**Inconvénients de l'authentification sur les réseaux sociaux**

Malgré ses avantages, l’authentification sur les réseaux sociaux présente également certains inconvénients. L’un d’eux est la dépendance aux réseaux sociaux, qui peut limiter l’expérience utilisateur si le réseau social choisi présente un problème d’indisponibilité. De plus, l’authentification auprès d’un réseau social peut soulever des inquiétudes quant à la confidentialité des données des utilisateurs, dans la mesure où le site Web ou l’application peut avoir accès aux informations personnelles du compte du réseau social.

Meilleures pratiques pour la mise en œuvre de l'authentification des réseaux sociaux

Pour mettre en œuvre l’authentification sur les réseaux sociaux de manière efficace et sécurisée, il est important de suivre quelques bonnes pratiques. L’un d’eux consiste à garantir que le processus d’authentification est transparent pour l’utilisateur, en expliquant clairement quelles informations seront consultées et comment elles seront utilisées. De plus, il est essentiel de protéger les données des utilisateurs en utilisant des méthodes de cryptage et d’authentification à deux facteurs.

**Conclusion**

En résumé, l'authentification sur les réseaux sociaux est une pratique et sécurisée qui facilite l'accès des utilisateurs aux différentes plateformes et services sur Internet. En suivant les meilleures pratiques de mise en œuvre, vous pouvez garantir une expérience utilisateur positive et accroître la sécurité des données. Par conséquent, envisagez de mettre en œuvre l’authentification sociale sur votre site Web ou votre application pour améliorer l’expérience utilisateur et accroître la sécurité des données.

**Qu’est-ce qu’un réseau informatique ? Apprenez-en davantage sur la technologie qui nous connecte**

On parle beaucoup de « **réseau** » ou de réseaux informatiques. Le réseau téléphonique et l'infrastructure logique des ordinateurs que nous connaissons sont généralement connectés et forment un grand réseau qui permet la communication entre tous les systèmes.

**Qu’est-ce qu’un réseau informatique ?**

Le réseau informatique est un système informatique pour transmettre des données. Également appelés nœuds, ces appareils interconnectés envoient, reçoivent et échangent des données, du trafic voix et vidéo, grâce au matériel et aux logiciels qui composent l'environnement.

**A quoi sert un réseau ?**

Le réseau informatique brise les barrières géographiques et permet de partager des informations entre des personnes et des entreprises du monde entier, rendant les informations disponibles au niveau local ou mondial, et est utile pour fournir divers services essentiels.

**Partage de fichiers :** vous permet de partager des fichiers de données sur un réseau ;

Accès et utilisation des applications : permet d'accéder et d'utiliser des applications sur le réseau ;

**Partager du matériel :** permet aux utilisateurs d'un réseau de partager des périphériques matériels, tels que des imprimantes et des disques durs.

**Modèle client-serveur :** permet de stocker les données sur des serveurs, où les appareils des utilisateurs finaux **(clients**) peuvent accéder à ces informations.

Voix sur IP **(VoIP**) : permet aux utilisateurs d'envoyer des données vocales via des protocoles Internet ;

Communication : peut inclure des vidéos, des images, du texte et de la voix ;

Commerce électronique : permet aux utilisateurs de vendre et d’acheter des produits et services sur Internet ;

**Jeux :** permet aux utilisateurs de jouer simultanément, même s'ils se trouvent dans des endroits différents.

Les périphériques réseau utilisent divers matériels et logiciels pour spécifier et standardiser la manière dont les données sont envoyées ou reçues.

Les deux types de réseaux les plus connus et utilisés dans notre vie quotidienne : le réseau local (**LAN**) et le réseau étendu (**WAN**).

Tout réseau informatique nécessite des équipements et des règles pour établir la communication entre les nœuds, tels que des câbles, des modems, des routeurs, des cartes et des ports de communication.

De plus, certains protocoles (règles) régissent la communication entre ces systèmes et garantissent que la transmission des données se fera sans problème, grâce à des normes de transmission, de vérification et d'envoi des données.

La norme Ethernet, par exemple, établit un langage commun pour la communication sur les réseaux filaires (**LAN**) et la norme 802.11 fait de même pour les réseaux locaux sans fil (**WLAN – Wireless Local Area Network**).

Le protocole **TCP/IP**

Un protocole réseau est le langage utilisé par deux ordinateurs pour communiquer. Pour qu’il y ait communication entre deux nœuds, ils doivent être sur le même réseau et « parler le même langage ».

Cette initiative a donné naissance au protocole TCP/IP (**Transmission Control** **Protocol/Internet Protocol**), établissant des normes de communication à travers un ensemble de protocoles de transmission de données.

Cinq ans après la création du protocole **TCP/IP**, l'Organisation internationale de normalisation (**ISO)** a créé le modèle OSI, qui établit une norme pour faciliter le processus d'interconnectivité entre les machines de différents fabricants.

**Qu'est-ce que l'adresse IP ?**

Chaque appareil sur un réseau possède un identifiant unique, qui sert à indiquer la source ou la destination de la transmission : cet identifiant est appelé adresse réseau.

L'adresse IP est l'identifiant le plus courant d'un périphérique réseau, mais il existe également d'autres identifiants tels que l'adresse MAC (**Media Access Control Address**), qui sont utilisés dans des configurations plus avancées.

La capacité de transmission de chaque réseau

Lorsque nous parlons de capacité de transmission du réseau, nous faisons référence à la quantité de trafic qu'il peut gérer pendant son fonctionnement.

Cette capacité de transmission varie selon l'équipement, le support de communication (fibre, câble, onde), les applications et est qualifiée par le terme « bande passante », mesurée au travers de l'unité « débit de transfert supporté ».

Alors que la bande passante est quantifiée par le nombre maximum théorique de bits par seconde (bps) pouvant traverser un maillage de réseau, le taux de transfert est la vitesse réelle atteinte par une transmission, généralement mesurée en Mo/s (mégaoctets par seconde).

Malgré les informations théoriques sur la bande passante, le taux de transfert varie en fonction de plusieurs facteurs tels que l'équipement, l'infrastructure, la latence, la puissance de traitement et la surcharge du protocole.

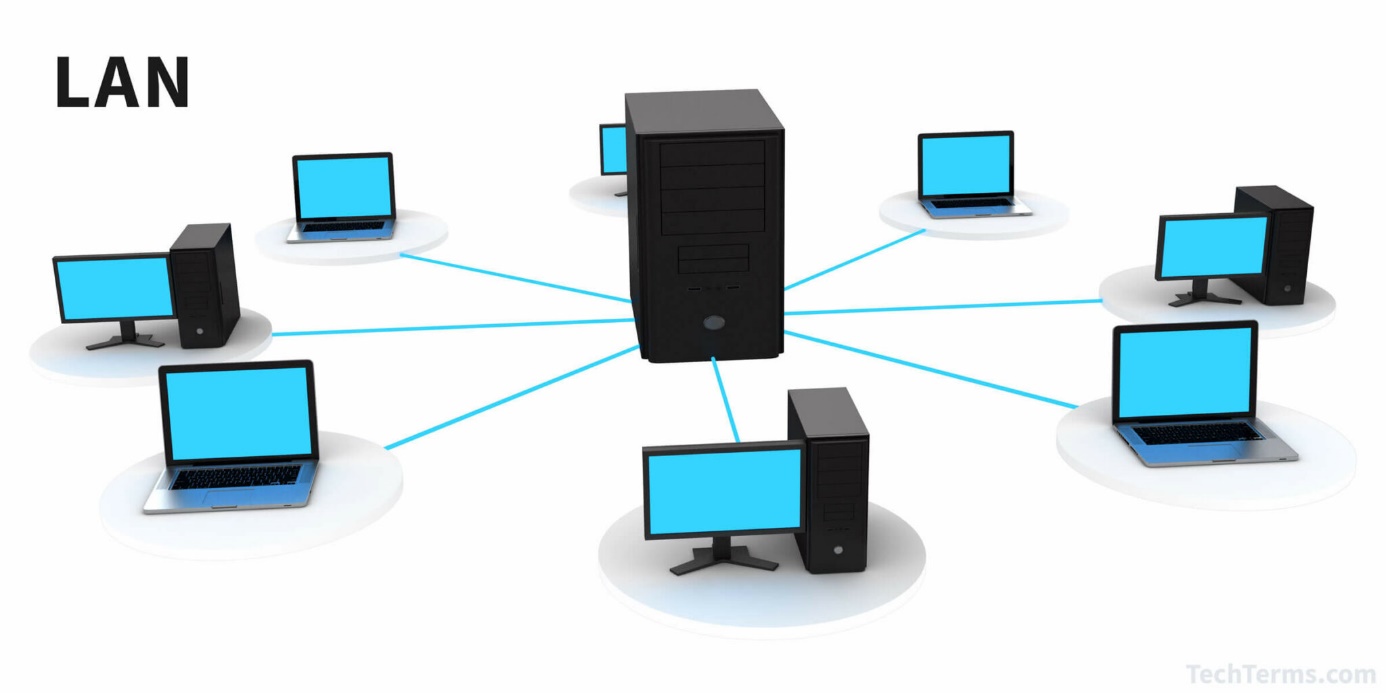
**Quels sont les types de réseaux informatiques ?**

Actuellement, il existe différents types de réseaux, tels que les réseaux filaires, les réseaux sans fil, les réseaux locaux, les réseaux externes, les réseaux privés virtuels, entre autres.

Les nomenclatures telles que **LAN, MAN, WLAN, WMAN, WWAN, SAN** et **PAN** se fondent généralement en seulement deux concepts : les réseaux locaux et les réseaux distants.

Les maillages de communication utilisés au sein d'une entreprise ou d'un domicile sont généralement simplement classés comme **LAN**, tandis que les réseaux étendus tels que ceux qui fournissent un accès Internet sont appelés **WAN.**

**Qu'est-ce qu'un réseau local (LAN) ?**



Un réseau local est un réseau composé de serveurs, d'ordinateurs et d'autres appareils situés au même emplacement physique, que ce soit au sein d'une maison, d'une entreprise ou d'une organisation gouvernementale.

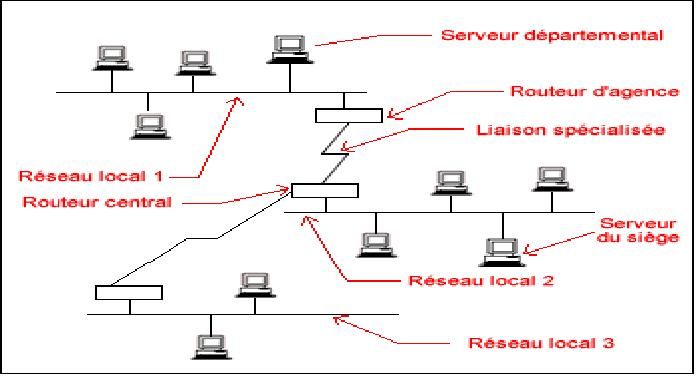
Un réseau local permet d'échanger des informations entre ordinateurs connectés au réseau, mais il ne suffit pas à fournir un accès Internet à l'un de ces appareils.

Pour que cela se produise, le réseau local doit être connecté à un réseau **WAN**, via des équipements tels que des modems, des routeurs et une connexion haut débit.

**Qu’est-ce que le WAN ?**

L'acronyme **WAN** est l'acronyme de Wide Area Network, qui signifie « **réseau longue** **distance** ». Ces réseaux sont responsables de la communication mondiale, interconnectant les systèmes composés d'ordinateurs, de stockage et de serveurs à travers le monde.

En bref, Internet est un exemple de WAN que nous utilisons dans notre vie quotidienne. C'est via le WAN que nous envoyons et recevons des e-mails, regardons YouTube, Netflix et utilisons les services cloud.



**Comment se passe l’accès au réseau ?**

Les réseaux peuvent être publics ou privés. Alors que n'importe qui peut accéder à l'Internet public, l'accès aux réseaux privés nécessite que l'utilisateur dispose d'informations d'accès, telles que des informations d'identification ou des certificats, pour pouvoir se connecter au réseau.

Au sein des entreprises, les systèmes de contrôle d'accès au réseau (**NAC)** utilisent généralement des politiques de sécurité pour contrôler l'accès au réseau de l'entreprise.

Cela signifie que les appareils doivent être autorisés à se connecter, répondant aux exigences d'authentification et de sécurité stipulées par l'entreprise.

Ces contrôles sont fournis et gérés par des politiques d'un système de contrôle central et la plupart peuvent utiliser un contrôleur de domaine pour contrôler l'accès des utilisateurs, garantissant ainsi qu'ils disposent des autorisations nécessaires.

Appareils pouvant intégrer un réseau informatique

En plus des câbles, commutateurs , modems, routeurs, ordinateurs et serveurs, un réseau informatique peut contenir un stockage pour le stockage des données et une série de logiciels pour gérer la transmission des données.

Les systèmes tels que les stockages **NAS** peuvent facilement centraliser le stockage des données sur un réseau local, libérant ainsi le serveur de cette tâche et servant de référentiel de données centralisé.

**Quelle est la fonction d'un routeur ?**

Les routeurs connectent les ordinateurs et autres appareils à Internet. Un routeur agit en tant que directeur, choisissant le meilleur itinéraire pour que vos informations circulent. Il connecte votre entreprise au monde, protège les informations contre les menaces de sécurité et peut même décider quels ordinateurs ont la priorité sur les autres.

**Pourquoi ai-je besoin d’un nouveau routeur ?**

Un routeur permet de connecter plusieurs appareils à Internet et de connecter les appareils entre eux. De plus, vous pouvez utiliser des routeurs pour créer des réseaux de périphériques locaux. Ces réseaux locaux sont utiles si vous souhaitez partager des fichiers entre appareils ou permettre aux employés de partager des outils logiciels.

Si vous ne disposez pas de routeurs, les données de votre entreprise ne seront pas dirigées au bon endroit. Par exemple, si vous souhaitez imprimer un document, vous avez besoin d'un routeur pour l'envoyer vers une imprimante, et non vers un autre ordinateur ou scanner.

**Quelle est la différence entre les modems et les routeurs ?**

Un modem connecte votre entreprise à l'accès Internet via votre fournisseur d'accès Internet (FAI). Un routeur, quant à lui, connecte plusieurs appareils à un réseau, y compris des modems. Avec un routeur installé, les modems et autres appareils peuvent transférer des données d'un emplacement à un autre.

**Quels sont les différents types de routeurs ?**

Routeurs filaires

Les routeurs filaires se connectent souvent directement aux modems ou aux réseaux étendus (WAN) via des câbles réseau. Ils sont généralement dotés d'un port qui se connecte aux modems pour communiquer avec Internet.

**Routeurs sans fil**

Les routeurs peuvent également se connecter sans fil à des appareils compatibles répondant aux mêmes normes sans fil. Les routeurs sans fil peuvent recevoir et envoyer des informations vers et depuis Internet.

**Création d'une table de routage**

Une table de routage, stockée sur votre routeur, est une liste de tous les chemins possibles sur le réseau. Lorsque les routeurs reçoivent des paquets IP qui doivent être transférés vers un autre emplacement du réseau, le routeur vérifie l'adresse IP de destination du paquet, puis recherche les informations de routage dans la table de routage.

Si vous gérez un réseau, vous devez vous familiariser avec les tables de routage car elles vous aideront à résoudre les problèmes de réseau. Par exemple, si vous comprenez la structure et le processus de recherche des tables de routage, vous serez en mesure d'y diagnostiquer n'importe quel problème, quel que soit votre niveau de familiarité avec un protocole de routage spécifique.

**Réduction des coûts opérationnels**

Les routeurs augmentent la rentabilité. Les petites entreprises peuvent économiser de l'argent en partageant des équipements comme des imprimantes et des serveurs, ainsi que des services comme l'accès à Internet. Un réseau rapide et fiable construit avec des routeurs peut également se développer avec votre entreprise, vous n'avez donc pas besoin de réorganiser l'ensemble de votre réseau et d'acheter de nouveaux appareils pour suivre la croissance de votre entreprise.

**Une plus grande sécurité**

Si vos routeurs offrent des pare-feu intégrés ou un filtrage Web, qui examine les données entrantes et les bloque si nécessaire, ils peuvent également vous aider à protéger les précieuses données de votre entreprise contre les attaques.

**Activation des connexions à distance sécurisées**

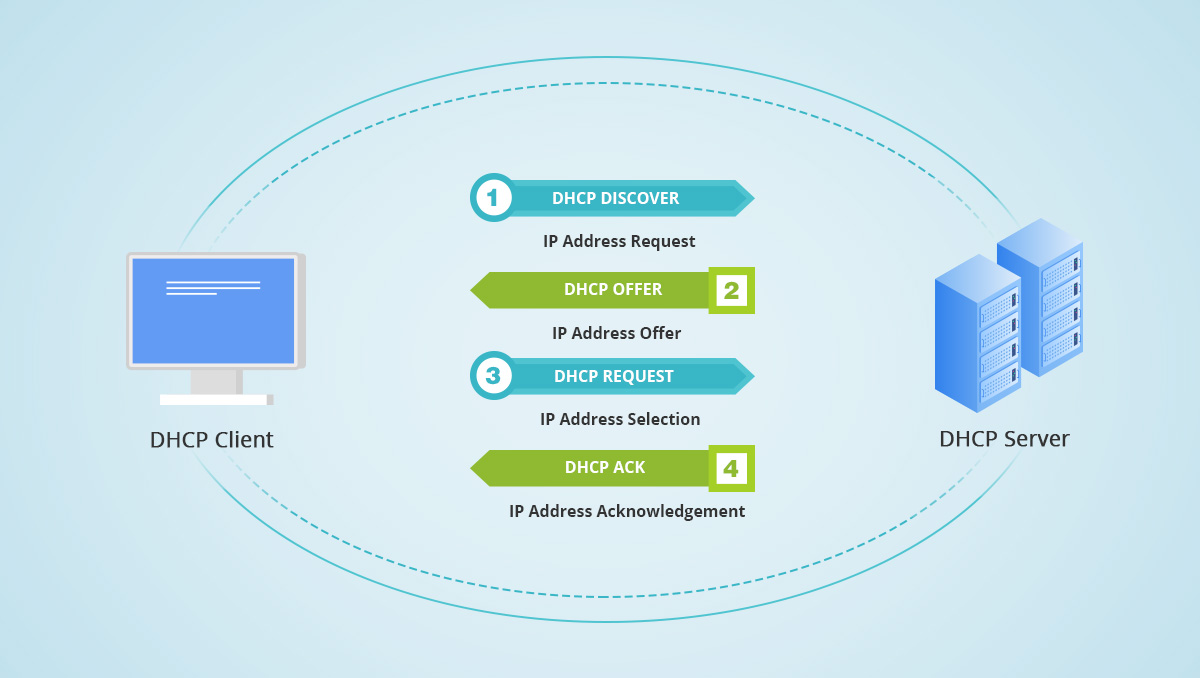
Les routeurs aident votre entreprise à fournir un accès à distance sécurisé aux travailleurs mobiles qui ont besoin de communiquer avec d'autres employés ou d'utiliser les applications de l'entreprise. Il s'agit d'un scénario courant dans de nombreuses entreprises disposant d'équipes virtuelles et de travailleurs à distance qui ont besoin de partager des informations commerciales importantes à toute heure du jour ou de la nuit.

**Que sont DHCP et DNS et quelles sont les différences entre eux ?**

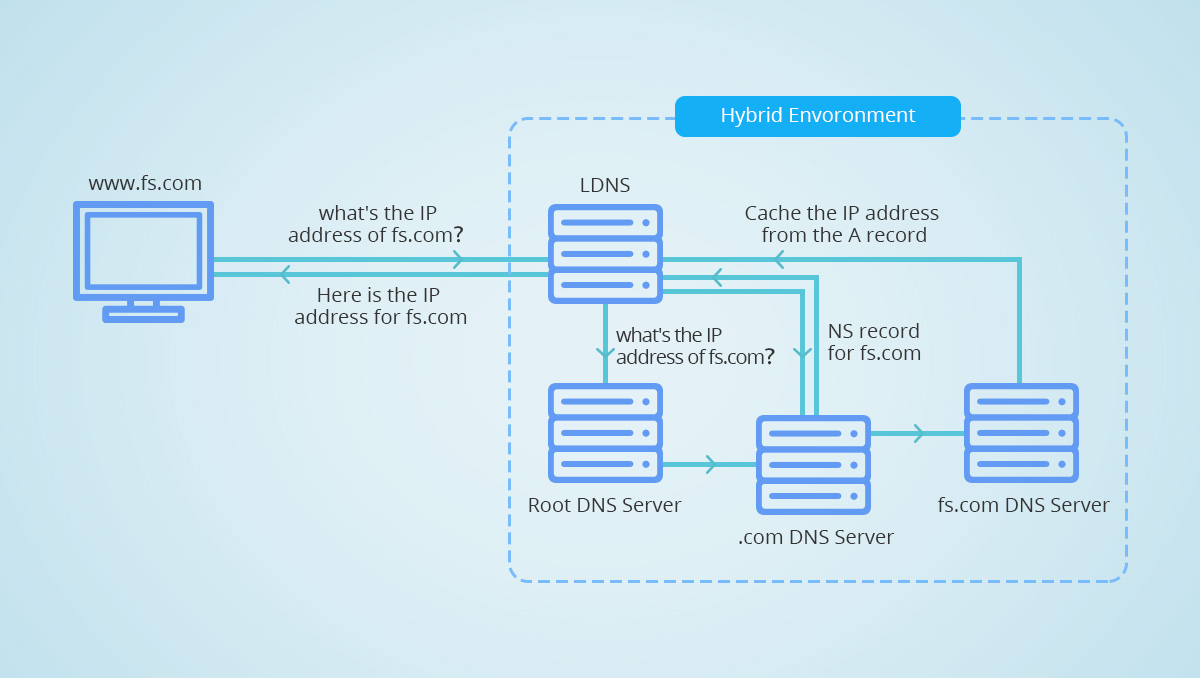
Les créations de **DHCP (Dynamic Host Configuration Protocol) et de DNS (Domain Name System)** nous facilitent l'utilisation du réseau ou d'Internet. Cependant, les deux sont différents dans leurs applications**. DHCP** est un protocole qui nous aide à attribuer une adresse **IP** et les informations **IP** associées aux ordinateurs. De nombreux commutateurs réseau utilisent également **DHCP** pour fournir des services réseau **TCP/IP** précieux, tels que la mise à jour automatique des logiciels sur le système client. Alors que le **DNS** est utilisé pour convertir le nom d'un site Web comme **FS**.com en son adresse **IP** et vice versa. Cela garantit que notre ordinateur trouve le bon site, car un ordinateur recherchera un site uniquement via son adresse **IP** et non via son nom de domaine.

**Comment fonctionne le DHCP ?**

**DHCP** fonctionne en louant des adresses **IP** et des informations **IP** aux clients du réseau sur une période donnée. Pour y parvenir, les clients **DHCP** doivent interagir avec les serveurs **DHCP** via une série de messages comprenant principalement **DHCP DISCOVER, DHCP OFFER, DHCP REQUEST et DHCP ACK**, comme le montre la figure suivante. Comme indiqué ci-dessus, les procédures de fonctionnement du serveur **DHCP.** attribue une adresse **IP** dynamique sont les suivantes.

[**Comment fonctionne le DNS ?**](https://community.fs.com/es/article/dhcp-and-dns-difference.html)

Comme indiqué ci-dessous, lorsque vous saisissez un nom de domaine dans le navigateur, par exemple fs.com, le navigateur n'a souvent aucune idée de l'endroit où se trouve **FS**.com. Par conséquent, il enverra une requête au **LDNS (Local DNS Server)** posant des questions telles que « quelle est l'adresse **IP** de FS.com ». Si le **LDNS** n'a aucun enregistrement pour **FS**.com, il effectuera une recherche sur Internet pour découvrir à qui appartient www.fs.com. Les procédures de travail détaillées sont les suivantes.

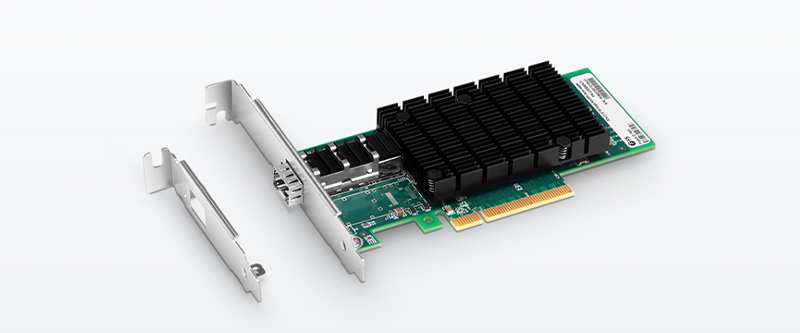


**Quelles sont les différences entre DHCP et DNS ?**

D’après ce qui précède, bien que **DHCP** et **DNS** soient liés aux adresses **IP**, ils remplissent des fonctions totalement différentes. Pour être clair, un graphique est utilisé ici pour conclure les différences entre **DHCP** et **DNS**.

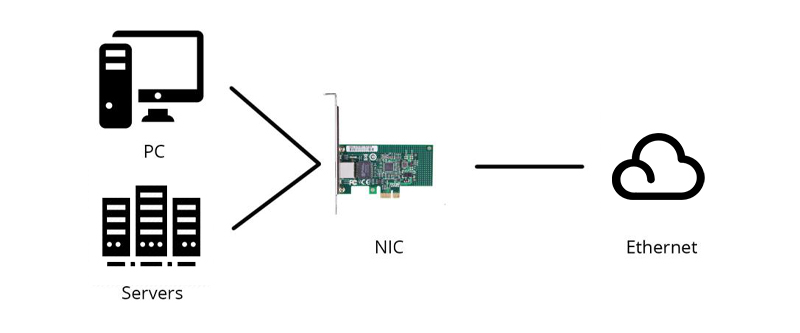
Qu’est-ce qu’une carte réseau ou **NIC** ? Définition, fonction et types de **NIC**

La carte réseau **(NIC**) est un composant matériel important utilisé pour fournir des connexions réseau. En raison de ses larges applications, différents types de cartes réseau sont apparus sur le marché, telles que les cartes **PCI** et les cartes réseau serveur.



**Qu'est-ce qu'une carte réseau ?**

Avant d'expliquer en quoi consiste la carte **NIC**, il est nécessaire de préciser qu'il existe différents noms pour les cartes d'interface réseau selon les différentes régions. Par exemple, dans certains endroits, ils sont appelés : contrôleur d'interface réseau, carte Ethernet, carte **LAN**, adaptateur réseau ou carte adaptateur réseau (**NAC**). Ce qui précède peut-être un peu déroutant, cependant, quels que soient les noms de la carte réseau, ils font tous référence à des cartes de circuits imprimés qui permettent à des périphériques tels que des ordinateurs et des serveurs réseau de se connecter sur le réseau. Actuellement, la carte **NIC** conçue dans un style intégré se trouve couramment dans la plupart des ordinateurs et certains serveurs réseau. De plus, des cartes réseau de serveur peuvent également être insérées dans les connecteurs d'extension des appareils.



**Fonction de la carte NIC**

La définition de carte **NIC** est très simple, mais à quoi sert une carte réseau et quelle est sa fonction ? Fonctionnant comme une interface au niveau de la couche **TCP/IP**, une carte réseau peut transmettre des signaux au niveau de la couche physique et des paquets de données au niveau de la couche réseau. Quelle que soit la couche dans laquelle se trouve le contrôleur d’interface réseau, il agit comme intermédiaire entre l’ordinateur/serveur et le réseau de données. Lorsqu'un utilisateur demande une page Web, la carte **LA**N obtient les données du périphérique de l'utilisateur et les envoie au serveur sur Internet, puis reçoit les données requises d'Internet pour les afficher aux utilisateurs.

**Composants ou pièces de la carte NIC**

Généralement, une carte réseau est principalement composée d'un contrôleur, d'un socket **ROM** de démarrage, d'un ou plusieurs ports **NIC**, d'une interface de connexion à la carte mère, de voyants **LED**, d'un support et de quelques autres composants électroniques. Chaque composant de la carte **LAN** a ses propres caractéristiques :

Contrôleur : Le contrôleur est comme un mini CPU qui traite les données reçues. Étant l'élément central de la carte réseau, le pilote détermine directement les performances de l'appareil.

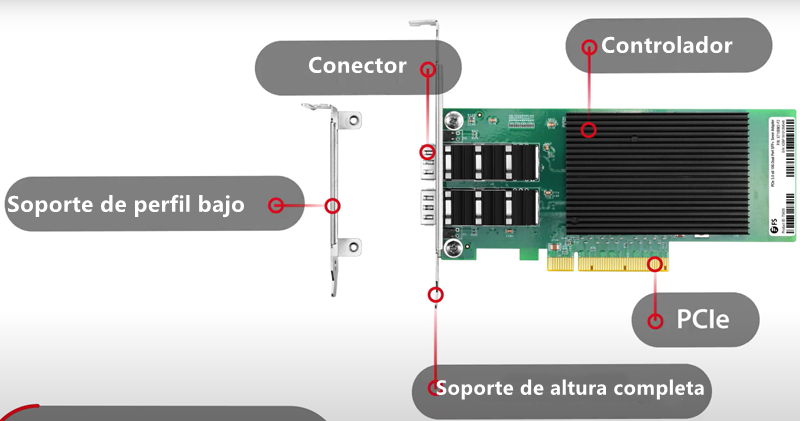
Socket **ROM** de démarrage : Ce socket active la fonction **ROM** de démarrage sur la carte, ce qui permet aux postes de travail sans disque de se connecter au réseau, augmentant ainsi la sécurité et réduisant les coûts matériels.

Port **NIC** câble/émetteur-récepteur : généralement, ce port se connecte directement à un câble réseau ou à un émetteur-récepteur qui peut générer et recevoir des signaux électroniques placés sur le câble réseau ou le câble à fibre optique.

Interface de bus : Cette interface est située sur le côté du circuit imprimé, qui est utilisée pour connecter la carte réseau à un ordinateur ou un serveur via son slot d'extension.

Indicateur **LED** : les indicateurs sont utilisés pour aider les utilisateurs à identifier si la carte réseau est connectée au réseau et si des données sont en cours de transmission.

Support : Il existe deux types de supports profilés sur le marché. Le premier est le support pleine hauteur d'une longueur de **12 cm**, et le second est le support à profil bas d'une longueur de 8 cm. Ce support peut aider les utilisateurs à réparer la carte réseau dans le connecteur d'extension d'un ordinateur ou d'un serveur.



Travail à faire : Combien de machines peut-on en avoir dans un réseau de classe A ?

Un réseau de classe A peut avoir 16,777,214 machines ou hôtes.

Combien de machines peut- on avoir dans un réseau de classe B ?

Un réseau de classe B peut avoir 65,534 machines ou hôtes.

un réseau de classe C peut avoir 254 machines ou hôtes.