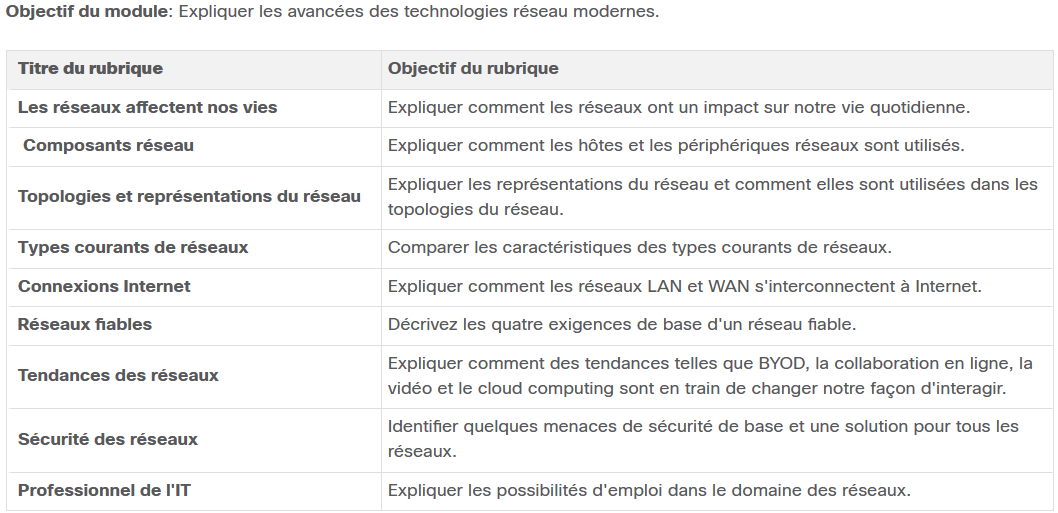
*Cours CISCO et réseaux :*

**CHAPITRE 1 – Introduction aux Réseaux**



Les élèves utilisent généralement Packet Tracer pour:

* Se préparer à un examen de certification.
* Mettre en pratique ce qu'ils ont appris pendant les cours.
* Affiner leurs connaissances en vue d'un entretien d'embauche.
* Examiner l'impact de l'ajout de nouvelles technologies dans des conceptions de réseau existantes.
* Développer leurs compétences pour des postes dans le domaine de l'Internet des objets.
* Relever des challenges mondiaux de conception (examinez le challenge de conception PT7 2017 sur Facebook).

Packet Tracer est un outil de formation indispensable utilisé dans de nombreux cours de la Cisco Networking Academy.

Pour obtenir et installer votre copie de Cisco Packet Tracer, suivez ces étapes :

**Étape 1**. Connectez-vous à votre Espace étudiant dans la Cisco Networking Academy.  
**Étape 2**. Sélectionnez les ressources.  
**Étape 3**. Sélectionnez Télécharger Packet Tracer.  
**Étape 4**. Sélectionnez la version de Packet Tracer dont vous avez besoin.  
**Étape 5**. Enregistrez le fichier sur votre ordinateur.  
**Étape 6**. Lancez le programme d'installation de Packet Tracer.

Packet Tracer est un outil qui vous permet de simuler des réseaux réels. Il propose trois menus principaux:

* Vous pouvez ajouter des périphériques et les connecter via des câbles ou sans fil.
* Vous pouvez sélectionner, supprimer, inspecter, étiqueter et regrouper des composants au sein de votre réseau.
* Vous pouvez gérer votre réseau en ouvrant un réseau existant/échantillon, en enregistrant votre réseau actuel et en modifiant votre profil utilisateur ou vos préférences.

Si vous avez utilisé un programme tel qu'un traitement de texte ou un tableur, vous êtes déjà familiarisé avec les commandes du menu Fichier situées dans la barre de menu supérieure. Les commandes Ouvrir, Enregistrer, Enregistrer sous et Quitter fonctionnent comme elles le feraient pour n'importe quel programme, mais il existe deux commandes spéciales pour Packet Tracer.

La commande Ouvrir des échantillons affiche un répertoire d'exemples prédéfinis de fonctionnalités et de configurations de divers périphériques réseau et Internet des objets inclus dans Packet Tracer.

La commande Quitter et Déconnexion supprimera les informations d'enregistrement de cette copie de Packet Tracer et demandera au prochain utilisateur de cette copie de Packet Tracer de refaire la procédure de connexion.

Plus de frontières :

Les avancées en matière de technologies réseau constituent probablement les facteurs d'évolution les plus importants dans le monde actuel. Ils contribuent à créer un monde dans lequel les frontières nationales, les distances géographiques et les limitations physiques perdent de leur pertinence et présentent des obstacles de plus en plus petits.

L'internet a changé la manière dont se déroulent nos interactions sociales, commerciales, politiques et personnelles. La nature immédiate des communications sur l'internet encourage la création de communautés mondiales. Les communautés internationales permettent des interactions sociales pour lesquelles géographie et fuseaux horaires n’ont aucune importance.

La création de communautés en ligne échangeant idées et informations peut potentiellement accroître les occasions d'améliorer la productivité sur l'ensemble du globe.

La création du cloud nous permet de stocker des documents et des images et d'y accéder n'importe où et n'importe quand. Ainsi, que nous soyons dans un train, dans un parc ou au sommet d'une montagne, nous pouvons accéder en toute transparence à nos données et applications sur n'importe quel appareil.

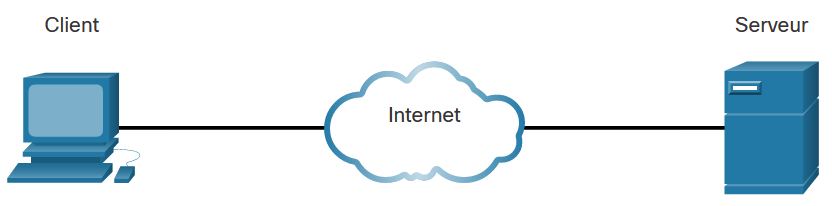
Le Rôle de l’Hôte :

Si vous souhaitez faire partie d'une communauté en ligne mondiale, votre ordinateur, votre tablette ou votre téléphone intelligent doit d'abord être connecté à un réseau. Ce réseau doit être connecté à l'internet. Cette rubrique traite des parties d'un réseau. Voyez si vous reconnaissez ces composants dans votre propre réseau familial ou scolaire !

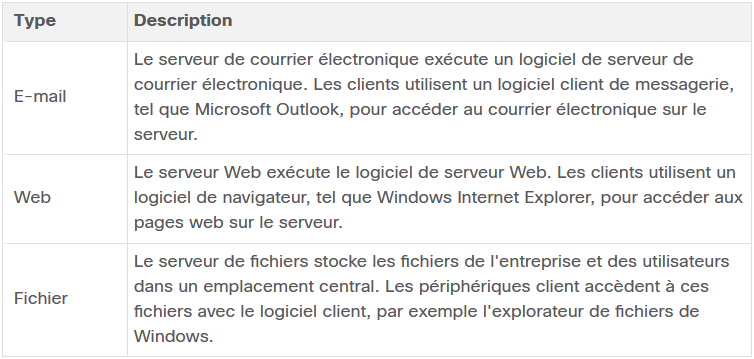
Tous les ordinateurs connectés à un réseau et qui participent directement aux communications transmises sur le réseau sont des hôtes. Les hôtes sont également appelés des périphériques finaux. Certains hôtes sont également appelés clients. Cependant, le terme hôte fait spécifiquement référence aux périphériques du réseau auxquels un numéro est attribué à des fins de communication. Ce numéro identifie l'hôte d'un réseau particulier. Ce numéro est appelé l'adresse IP (Internet Protocol). Une adresse IP identifie l'hôte et le réseau auquel l'hôte est connecté.

Les serveurs sont des ordinateurs équipés de logiciels leur permettant de fournir des informations, comme des messages électroniques ou des pages web, à d'autres périphériques finaux sur le réseau. Chaque service nécessite un logiciel serveur distinct. Par exemple, un serveur nécessite un logiciel de serveur web pour pouvoir offrir des services web au réseau. Un ordinateur équipé d'un logiciel serveur peut fournir des services à un ou plusieurs clients en même temps.

Comme mentionné précédemment, les clients sont un type d'hôte. Les clients disposent d'un logiciel pour demander et afficher les informations obtenues à partir du serveur, comme le montre la figure.

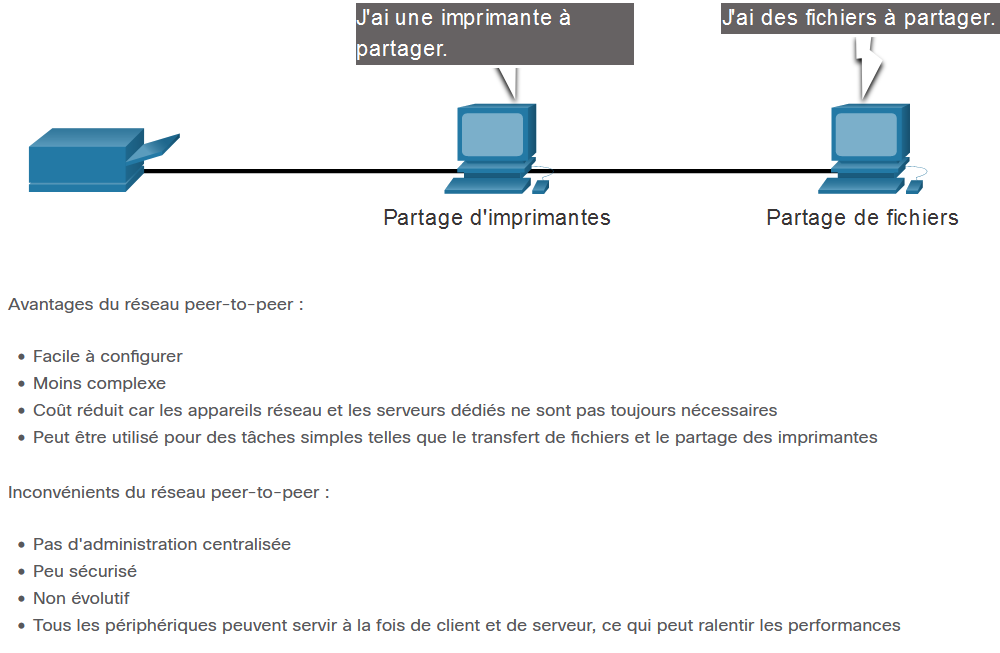


Un navigateur web, tel que Chrome ou Firefox, est un exemple de logiciel client. Un seul ordinateur peut également exécuter différents types de logiciel client. Par exemple, un utilisateur peut vérifier son courrier électronique et consulter une page web tout en utilisant la messagerie instantanée et en écoutant un flux audio. Le tableau répertorie trois types courants de logiciels serveur.



Le PEER-TO-PEER :

Les logiciels client et serveur fonctionnent généralement sur des ordinateurs séparés, mais il est également possible d'utiliser un seul ordinateur pour les deux rôles en même temps. Dans le cas des réseaux de particuliers et de petites entreprises, il arrive souvent que les ordinateurs fassent à la fois office de serveur et de client sur le réseau. Ce type de réseau est appelé réseau Peer to peer.

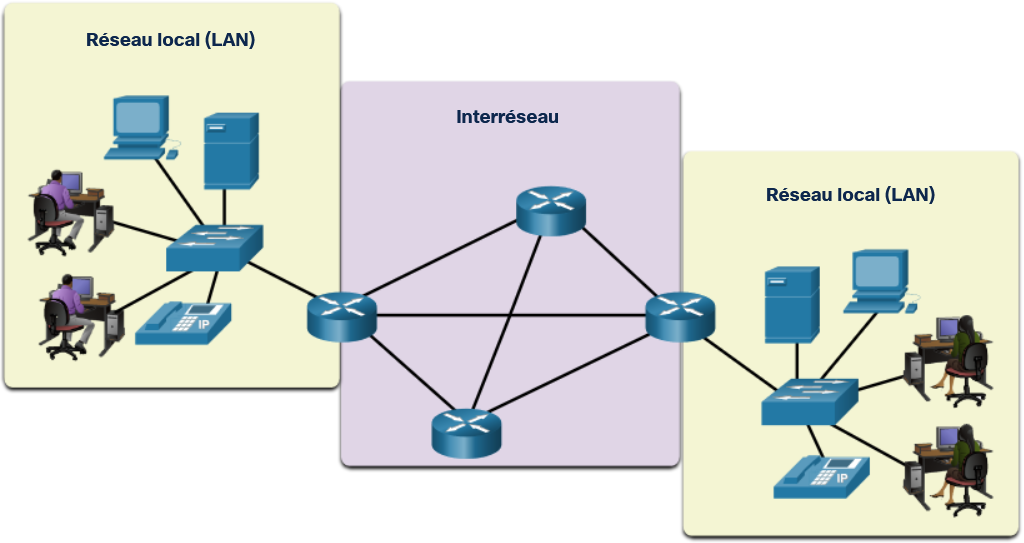


Périphériques finaux :

Les périphériques réseau auxquels les personnes sont le plus habituées sont appelés terminaux. Pour pouvoir les distinguer les uns des autres, tous les périphériques terminaux d'un réseau sont identifiés au moyen d'une adresse. Lorsqu'un périphérique terminal initialise la communication, il utilise l'adresse du périphérique terminal de destination pour spécifier où délivrer le message.

Un périphérique final constitue soit la source soit la destination d'un message transmis à travers le réseau.

Dans la figure, cliquez sur Lecture pour voir une animation du flux de données sur un réseau.

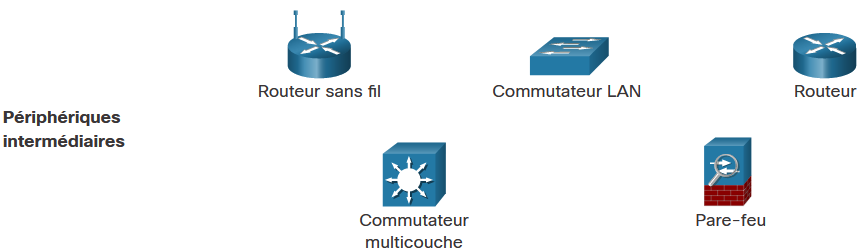


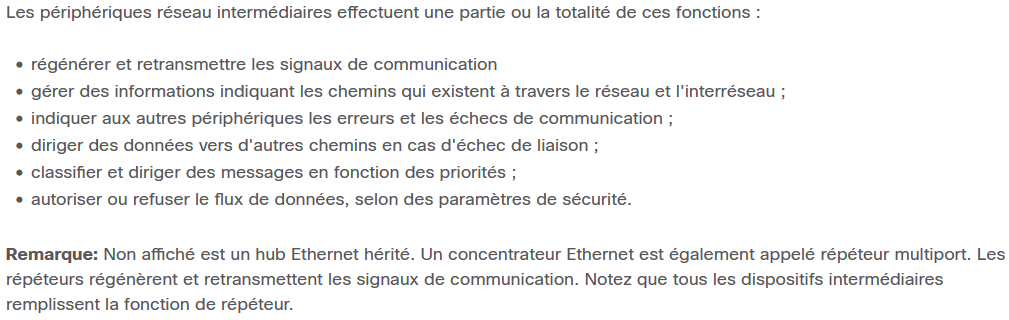
Les données proviennent d’un périphérique final, traversent le réseau et arrivent sur un périphérique final.

Equipements actifs :

Des dispositifs intermédiaires relient les différents dispositifs finaux au réseau. Ils peuvent connecter plusieurs réseaux individuels pour former un interréseau. Ils fournissent la connectivité et s'assurent que les données sont transmises sur le réseau.

Les périphériques intermédiaires utilisent l'adresse du périphérique final de destination, ainsi que les informations concernant les interconnexions réseau, pour déterminer le chemin que doivent emprunter les messages à travers le réseau. Des exemples des périphériques intermédiaires les plus courants ainsi qu'une liste des fonctions sont présentés dans la figure.



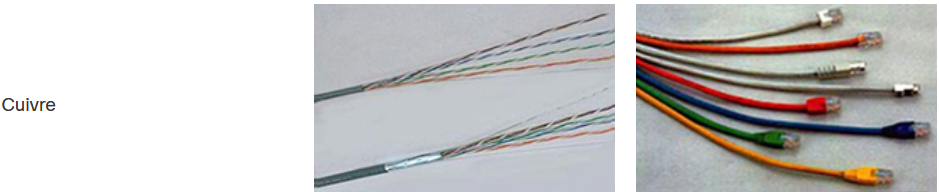


Supports réseau :

La communication se transmet à travers un réseau sur les supports. Celui-ci fournit le canal via lequel le message se déplace de la source à la destination.

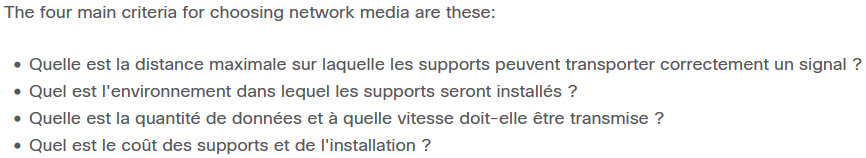
Les réseaux modernes utilisent principalement trois types de supports pour la connexion des périphériques.

* **Fils métalliques dans les câbles** - Les données sont encodées en impulsions électriques.
* **Verre ou fibres plastiques (câble à fibre optique)** - les données sont encodées en pulsations lumineuses
* **Transmission sans fil** - Les données sont codées par modulation de fréquences spécifiques d'ondes électromagnétiques.

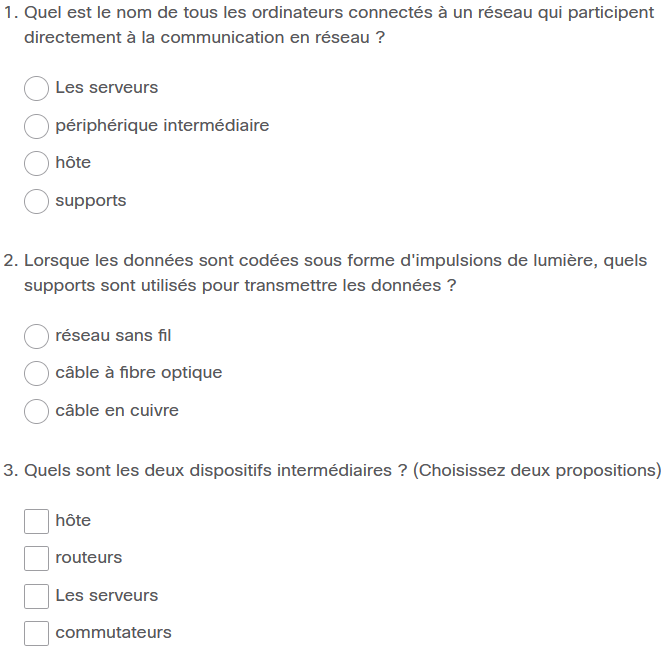








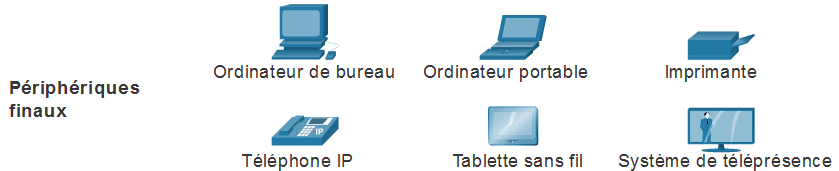
**Vérifiez votre compréhension - Composants du Réseau**



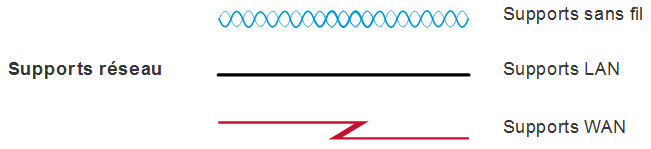
**TOPOLOGIES et représentations du réseau**

Représentations du réseau

Les architectes et administrateurs réseau doivent être en mesure de montrer à quoi ressembleront leurs réseaux. Ils doivent être en mesure de voir facilement quels composants se connectent à d'autres composants, où ils seront situés et comment ils seront connectés. Les diagrammes de réseaux utilisent souvent des symboles, comme ceux illustrés dans la figure, pour représenter les différents appareils et connexions qui composent un réseau.







Un diagramme permet de comprendre facilement comment les appareils se connectent dans un grand réseau. On appelle ce type de schéma de réseau « diagramme de topologie ». La capacité à reconnaître les représentations logiques des composants réseau physiques est essentielle pour être en mesure de visualiser l'organisation et le fonctionnement d'un réseau.

En plus de ces représentations, une terminologie spécialisée est utilisée pour décrire comment chacun de ces appareils et supports se connectent les uns aux autres :

* **Carte d'interface réseau (NIC)** - Une NIC relie physiquement le dispositif terminal au réseau.
* **Port physique** - Un connecteur ou une prise sur un dispositif de réseau où le support se connecte à un dispositif terminal ou à un autre dispositif de réseau.
* **Interface** - Ports spécialisés sur un dispositif de réseau qui se connecte à des réseaux individuels. Comme les routeurs connectent les réseaux, les ports d'un routeur sont appelés interfaces de réseau.

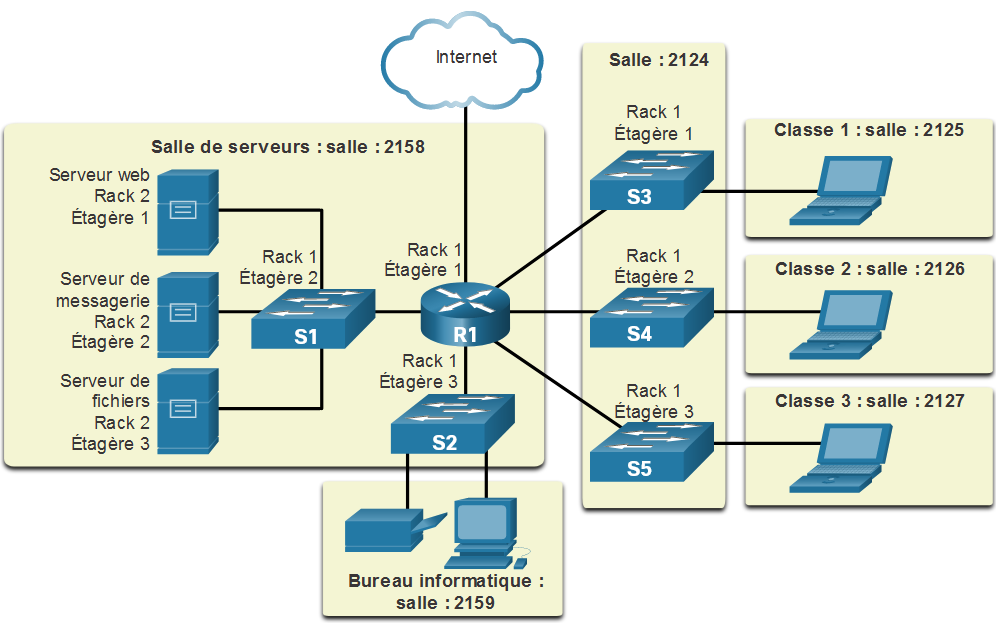
**Remarque**: les termes «port» et «interface» sont souvent utilisés l'un pour l'autre.

## Diagrammes de topologie

Les diagrammes de topologie sont obligatoires pour toute personne qui travaille sur un réseau. Ils fournissent une représentation visuelle des connexions réseau. Il existe deux types de diagrammes topologiques, physiques et logiques.

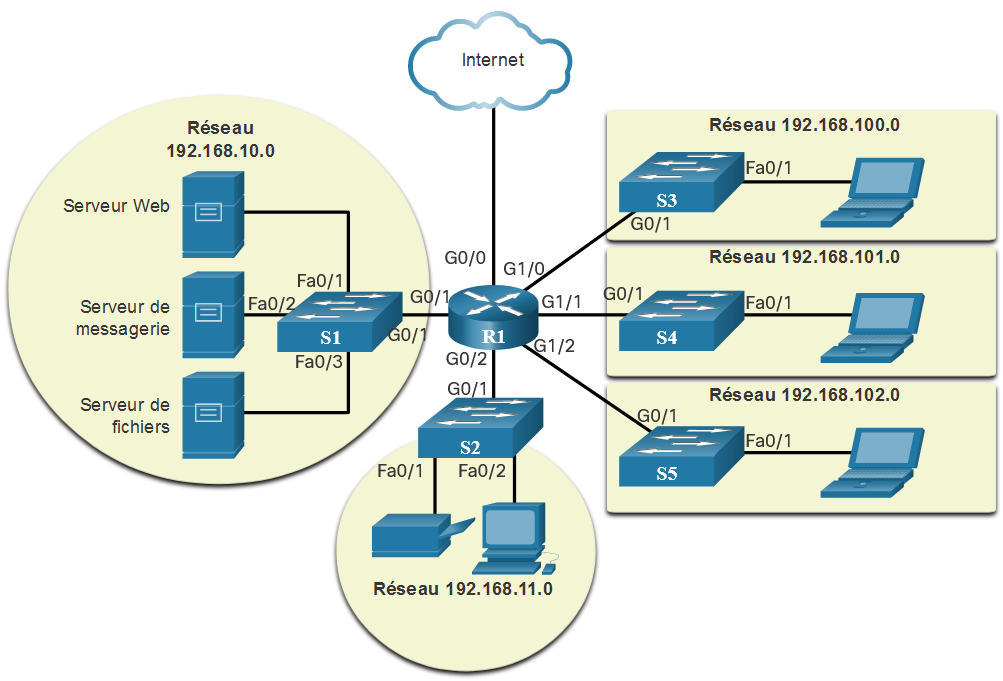
**Schémas de topologie physique**

Les diagrammes de topologie physique illustrent l'emplacement physique des dispositifs intermédiaires et de l'installation des câbles, comme le montre la figure. Vous pouvez voir que les pièces dans lesquelles se trouvent ces périphériques sont étiquetées dans cette topologie physique.



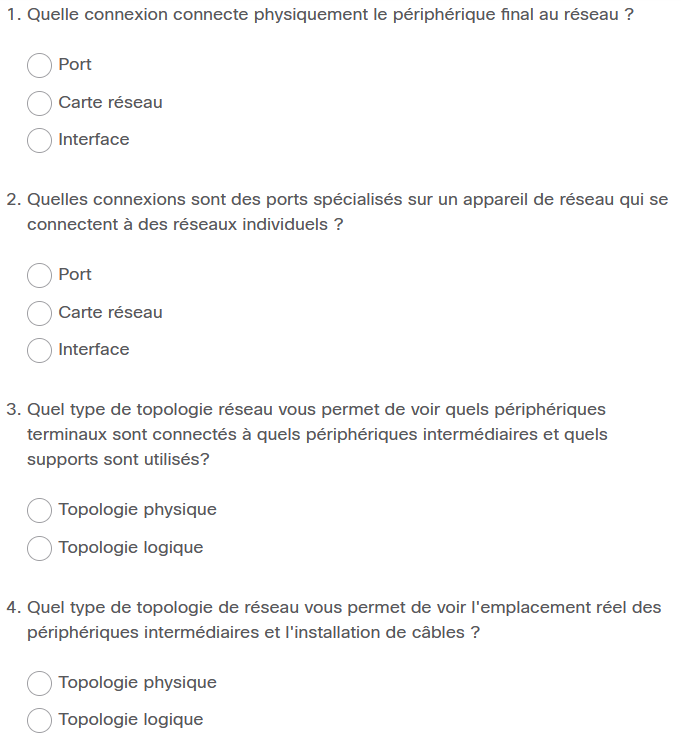
**Schémas de topologie logique**

Les diagrammes de topologie logiques illustrent les périphériques, les ports et le schéma d'adressage du réseau, comme illustré sur la figure. Vous pouvez voir quels périphériques terminaux sont connectés à quels périphériques intermédiaires et quels supports sont utilisés.



Les topologies illustrées dans les diagrammes physiques et logiques sont adaptées à votre niveau de compréhension à ce stade du cours. Cherchez sur Internet des "diagrammes de topologie de réseau" pour voir des exemples plus complexes. Si vous ajoutez le mot "Cisco" à votre phrase de recherche, vous trouverez de nombreuses topologies utilisant des icônes qui sont similaires à ce que vous avez vu dans ces figures.

## Vérifiez votre compréhension - Représentations et topologies des réseaux



# **Types courants de réseaux**

## Réseaux de tailles diverses

Maintenant que vous êtes familier avec les composants qui composent les réseaux et leurs représentations dans les topologies physiques et logiques, vous êtes prêt à en apprendre davantage sur les différents types de réseaux.

Les réseaux peuvent être de différentes tailles. Ils vont du simple réseau composé de deux ordinateurs aux réseaux reliant des millions d'appareils.

Les réseaux domestiques simples vous permettent de partager des ressources, telles que des imprimantes, des documents, des images et de la musique, entre quelques terminaux locaux.

Les réseaux de petits bureaux et bureaux à domicile (SOHO) permettent aux gens de travailler à domicile ou à distance. En outre, de nombreux entrepreneurs indépendants utilisent des réseaux domestiques ou des réseaux de petits bureaux pour faire la promotion de leurs produits, les vendre, commander des fournitures et communiquer avec les clients.

Les entreprises et les grandes organisations utilisent les réseaux pour assurer la consolidation, le stockage et l'accès aux informations sur des serveurs de réseau. Les réseaux permettent le courrier électronique, la messagerie instantanée et la collaboration entre les employés. De nombreuses organisations utilisent la connexion de leur réseau à l'internet pour fournir des produits et des services à leurs clients.

Internet est le plus grand réseau existant. En réalité, le terme « Internet » signifie « réseau de réseaux ». Internet est un ensemble de réseaux privés et publics interconnectés.

Dans les petites entreprises et les foyers, de nombreux ordinateurs fonctionnent à la fois comme serveurs et comme clients sur le réseau. Ce type de réseau est appelé réseau Peer to peer.



**Petits réseaux domestiques**

Les petits réseaux domestiques relient quelques ordinateurs entre eux et à Internet.



**Réseaux de petits bureaux et de bureaux à domicile**

Le réseau SOHO (réseau de petits bureaux/bureaux à domicile) permet aux ordinateurs d'un bureau à domicile ou d'un bureau distant de se connecter à un réseau d'entreprise ou d'accéder à des ressources centralisées et partagées.



**Moyens et grands réseaux**

Les réseaux de taille moyenne à grande, tels que ceux utilisés par les entreprises et les écoles, peuvent avoir de nombreux emplacements avec des centaines ou des milliers d'hôtes interconnectés.



**Réseaux mondiaux**

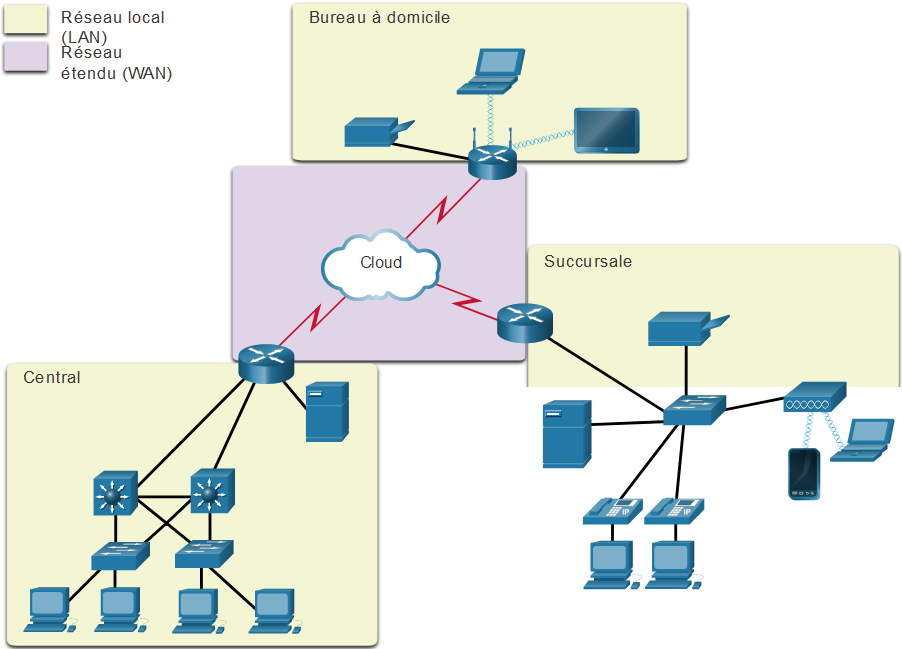
L'internet est un réseau de réseaux qui relie des centaines de millions d'ordinateurs dans le monde entier.

LAN et WAN

Les infrastructures de réseau varient beaucoup en termes de :

* La taille de la zone couverte
* Le nombre d'utilisateurs connectés
* Le nombre et les types de services disponibles
* Le domaine de responsabilité

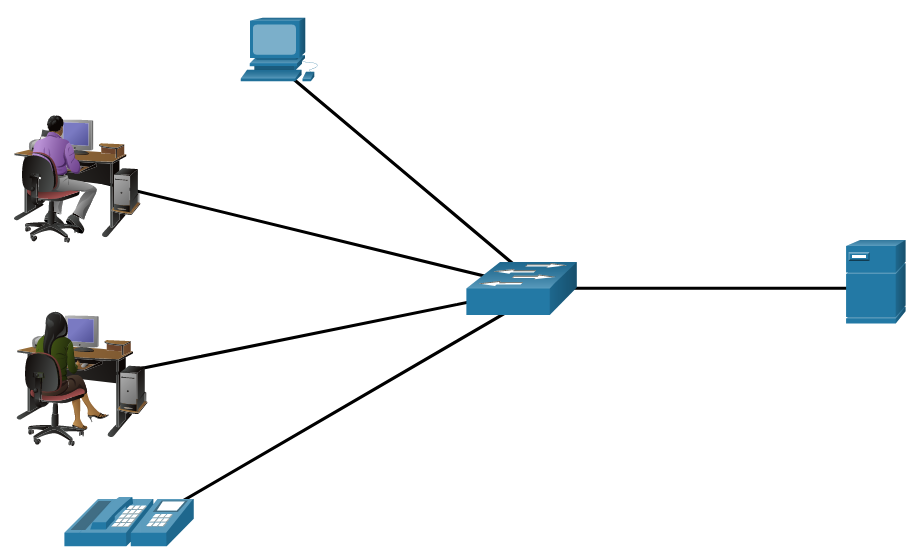
Les deux types d'infrastructures de réseau les plus courants sont les réseaux locaux (LAN) et les réseaux étendus (WAN). Un réseau local est une infrastructure de réseau qui fournit un accès aux utilisateurs et aux dispositifs finaux dans une petite zone géographique. Un réseau local est généralement utilisé dans un département au sein d'une entreprise, d'une maison ou d'un réseau de petites entreprises. Un WAN est une infrastructure de réseau qui donne accès à d'autres réseaux sur une vaste zone géographique, qui est généralement détenue et gérée par une grande entreprise ou un fournisseur de services de télécommunications. La figure montre les LAN connectés à un réseau étendu.



**Réseaux locaux**

Un LAN est une infrastructure de réseau qui couvre une zone géographique restreinte. Les réseaux locaux ont des caractéristiques spécifiques :

* Les LAN relient des périphériques finaux dans une zone limitée telle qu'une maison, une école, un immeuble de bureaux ou un campus.
* En règle générale, un réseau local est administré par une seule entreprise ou une seule personne. Le contrôle administratif est appliqué au niveau du réseau et régit les politiques de sécurité et de contrôle d'accès.
* Les réseaux locaux fournissent une bande passante à haut débit aux périphériques terminaux internes et aux périphériques intermédiaires, comme le montre la figure.



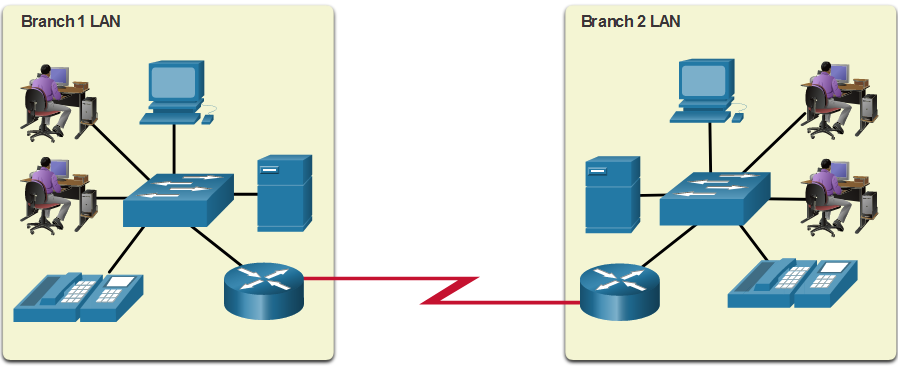
Un réseau servant une maison, un petit bâtiment ou un petit campus, est considéré comme un réseau local.

**Réseaux WAN**

La figure montre un réseau étendu qui interconnecte deux réseaux locaux. Un WAN est une infrastructure de réseau qui couvre une vaste zone géographique. Les réseaux étendus sont généralement gérés par des fournisseurs de services (PS) ou des fournisseurs de services Internet (ISP).

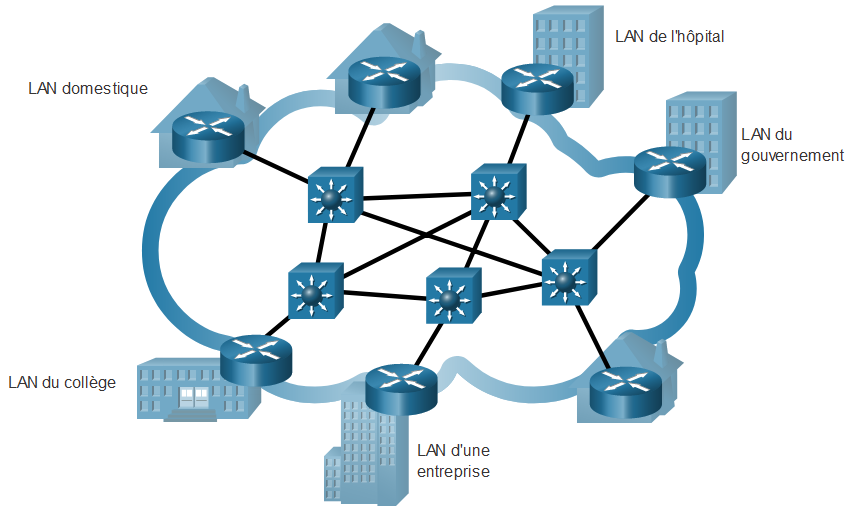
Les WAN ont des caractéristiques spécifiques :

* Les WAN relient des LAN sur des zones étendues couvrant des villes, des états, des provinces, des pays ou des continents.
* Les WAN sont habituellement gérés par plusieurs prestataires de services.
* Les réseaux WAN fournissent généralement des liaisons à plus bas débit entre les réseaux locaux.



Internet

L'internet est un ensemble mondial de réseaux interconnectés (internetworks, ou internet en abrégé). La figure montre une façon d'envisager l'internet comme un ensemble de réseaux locaux et étendus interconnectés.



Les services WAN permettent d’interconnecter les LAN.

Dans cet exemple, certains des LAN sont reliés entre eux par le biais d'une connexion WAN. Les WAN sont ensuite connectés les uns aux autres. Les lignes rouges des connexions WAN illustrent les différentes façons dont les réseaux sont reliés entre eux. Les WAN peuvent se connecter par des fils de cuivre, des câbles à fibres optiques et des transmissions sans fil (non illustrées).

L'internet n'est la propriété d'aucun individu ou groupe. Garantir une communication efficace sur cette infrastructure hétérogène requiert l'application de technologies et de normes cohérentes et communément reconnues, ainsi que la coopération entre de nombreux organismes gouvernementaux. Il existe des organisations qui ont été développées pour aider à maintenir la structure et la normalisation des protocoles et des processus Internet. Ces organismes incluent l'Internet Engineering Task Force (IETF), l'Internet Corporation for Assigned Names and Numbers (ICANN) et l'Internet Architecture Board (IAB), entre autres.

Intranets et Extranets

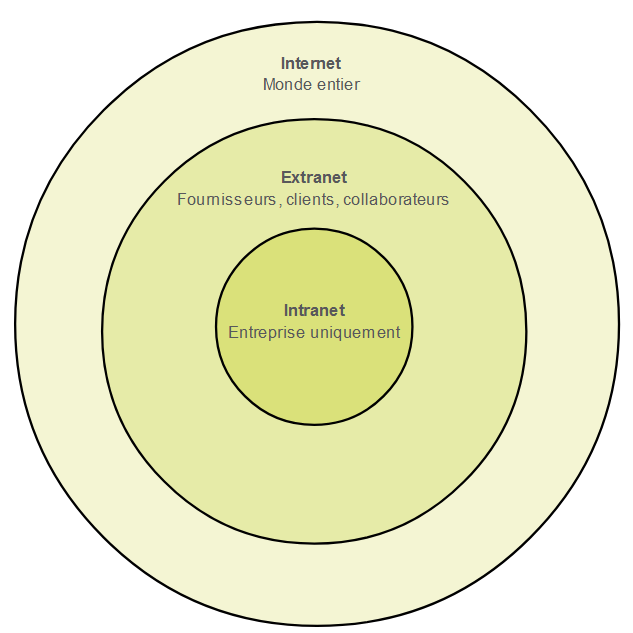
Il existe deux autres termes qui sont similaires au terme internet : intranet et extranet.

Intranet est un terme souvent utilisé pour désigner une connexion privée de LAN et de WAN qui appartient à une organisation. Il offre un accès aux membres de l'entreprise, à ses employés ou à d'autres personnes sous réserve d'une autorisation.

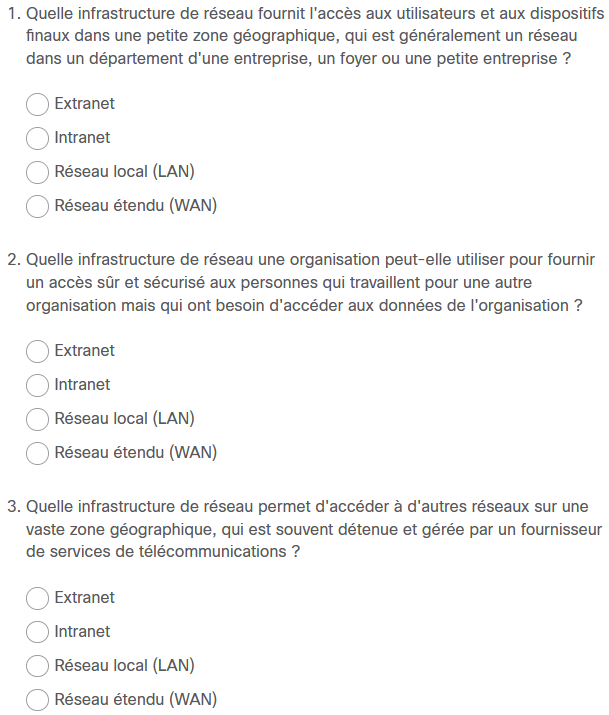
Une entreprise peut utiliser un extranet pour fournir un accès sûr et sécurisé aux personnes qui travaillent pour une organisation différente mais qui ont besoin d'accéder aux données de l'organisation. Voici quelques exemples d'extranets :

* Une entreprise qui donne accès aux fournisseurs et entrepreneurs extérieurs
* Un hôpital qui fournit un système de réservation aux médecins afin qu'ils puissent prendre des rendez-vous pour leurs patients
* Un bureau local de l'éducation qui fournit des informations sur le budget et le personnel aux écoles de son district

La figure illustre les niveaux d'accès que les différents groupes ont à un intranet d'entreprise, à un extranet d'entreprise et à Internet.



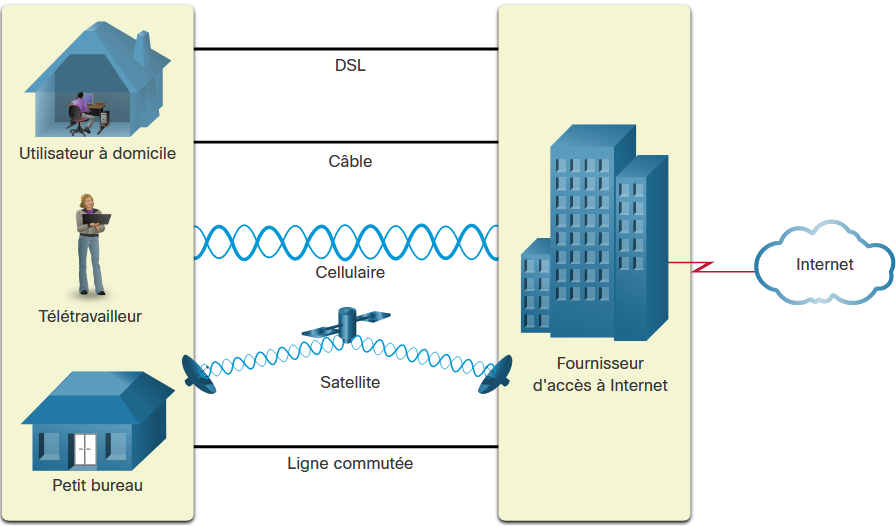
Types de réseaux communs



Technologie d’accès à Internet

## Connexions Internet des bureaux à domicile et des petits bureaux

La figure illustre les options de connexion courantes pour les utilisateurs de petits bureaux et de bureaux à domicile.



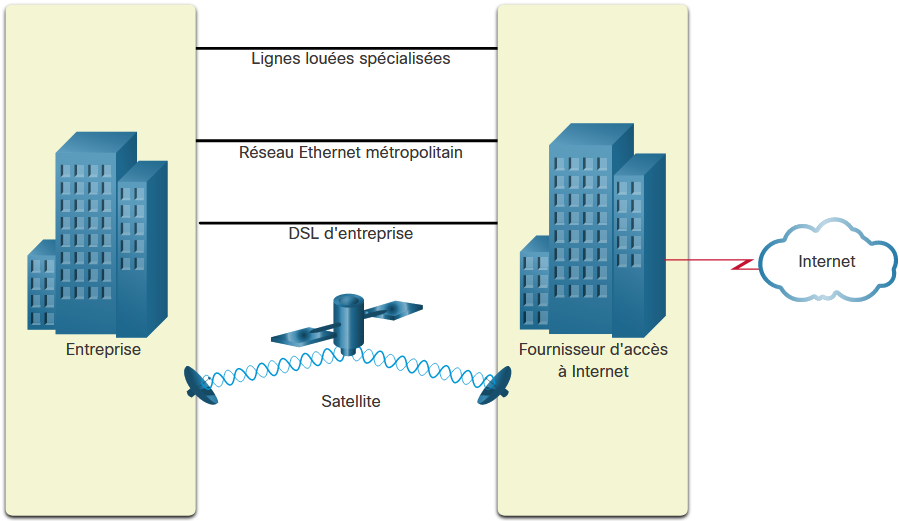
* **Câble** - Généralement proposé par les fournisseurs de services de télévision par câble, le signal de données Internet est transmis sur le même câble que celui qui achemine la télévision par câble. Il offre une large bande passante, une grande disponibilité et une connexion permanente à l'internet.
* **DSL** -Les lignes d'abonné numériques DSL offrent également une large bande passante, une grande disponibilité et une connexion permanente à l'internet. La technologie DSL utilise une ligne téléphonique. En général, un utilisateur de bureau à domicile ou de petit bureau se connecte à l'aide d'une ligne ADSL (Asymmetric Digital Subscriber Line), sur laquelle la vitesse descendante est supérieure à la vitesse ascendante.
* **Cellulaire** - L'accès à Internet par téléphone cellulaire utilise un réseau de téléphonie mobile pour se connecter. Partout où vous captez un signal cellulaire, vous pouvez accéder à Internet. Les performances sont limitées par les capacités du téléphone et de la tour de téléphonie cellulaire à laquelle il est connecté.
* **Satellite** - La disponibilité de l'accès à l'internet par satellite est un avantage dans les régions qui, autrement, n'auraient aucune connectivité internet. Les antennes paraboliques nécessitent une ligne de vue claire vers le satellite.
* **Ligne commutée** - Une option peu coûteuse qui utilise n'importe quelle ligne téléphonique et un modem. La faible bande passante des connexions par ligne commutée n'est généralement pas suffisante pour les transferts de données importants, mais cette solution reste utile pour accéder à Internet lors d'un déplacement.

Le choix de la connexion dépend de l'emplacement géographique et de la disponibilité du fournisseur d'accès.

Connexions Internet d’Entreprise

Les options de connexion pour les entreprises sont différentes des options disponibles pour les utilisateurs à domicile. Les entreprises peuvent nécessiter une bande passante plus élevée, une bande passante spécialisée et des services gérés. Les options de connexion disponibles diffèrent selon le type de fournisseurs de services situés à proximité.

La figure illustre les options de connexion communes pour les entreprises.



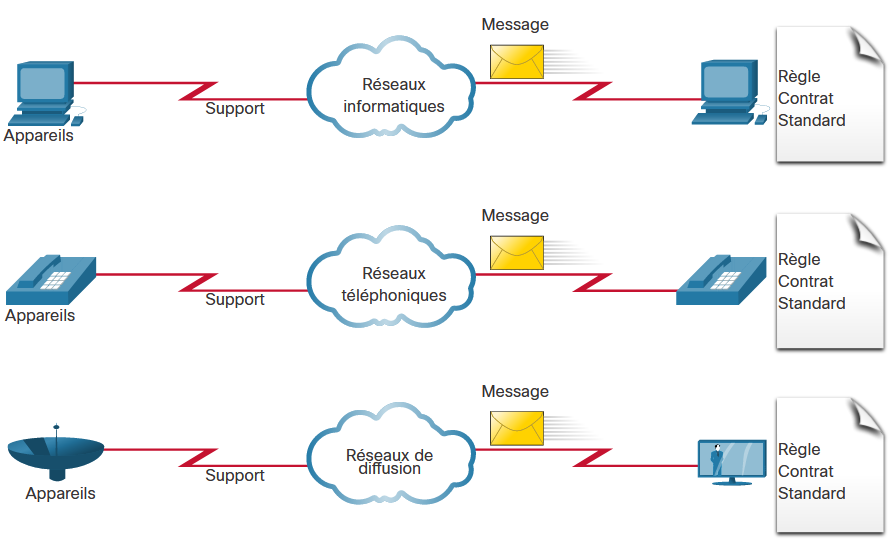
* **Ligne louée dédiée** - Les lignes louées sont des circuits réservés au sein du réseau du fournisseur de services qui relient des bureaux géographiquement séparés pour un réseau privé de voix et/ou de données. Les circuits sont généralement loués sur une base mensuelle ou annuelle.
* **Metro Ethernet** - Ceci est parfois connu sous le nom Ethernet WAN. Dans ce module, nous l'appellerons Metro Ethernet. Les Metro ethernets étendent la technologie d'accès au LAN au WAN. Ethernet est une technologie LAN que vous découvrirez dans un autre module.
* **Business DSL** - Business DSL est disponible dans différents formats. Un choix populaire est la ligne d'abonné numérique symétrique (SDSL) qui est similaire à la version grand public de la DSL mais qui permet les téléchargements en amont et en aval aux mêmes vitesses élevées.
* **Satellite** - Le service par satellite peut fournir une connexion lorsqu'une solution câblée n'est pas disponible.

Le choix de la connexion dépend de l'emplacement géographique et de la disponibilité du fournisseur d'accès.

Réseau Convergent

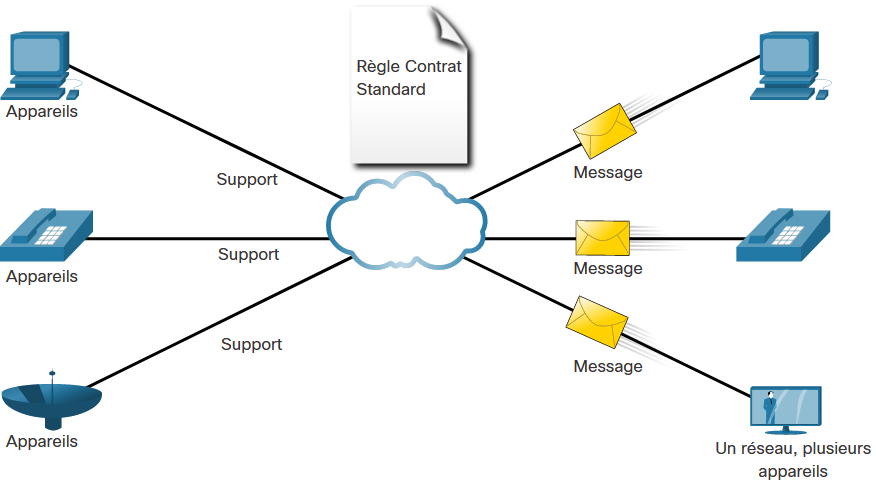
**Réseaux séparés traditionnels**

Imaginez une école construite il y a trente ans. À cette époque, certaines classes étaient reliées au réseau de données, au réseau téléphonique et au réseau de télévision. Ces réseaux séparés ne pouvaient pas communiquer entre eux. Chaque réseau utilisait des technologies différentes pour le transport du signal de communication. Chaque réseau avait son propre ensemble de règles et de normes pour garantir le bon fonctionnement des communications. Plusieurs services s'exécutent sur plusieurs réseaux.



**Réseaux convergents**

Aujourd'hui, les réseaux distincts de données, de téléphone et de vidéo convergent. Contrairement aux réseaux spécialisés, les réseaux convergents sont capables de transmettre des données, de la voix et de la vidéo entre de nombreux types d'appareils différents sur la même infrastructure de réseau. Cette infrastructure réseau utilise le même ensemble de règles, de contrats et de normes de mise en œuvre. Les réseaux de données convergents exécutent plusieurs services sur un même réseau.



Réseaux Fiables

Architecture réseau

Avez-vous déjà été occupé à travailler en ligne, seulement pour avoir "l'internet en panne" ? Comme vous le savez maintenant, l'Internet n'est pas tombé, vous venez de perdre votre connexion à elle. C'est très frustrant. Comme tant de personnes dans le monde dépendent de l'accès au réseau pour travailler et apprendre, il est impératif que les réseaux soient fiables. Dans ce contexte, la fiabilité signifie plus que votre connexion à Internet. Cette rubrique se concentre sur les quatre aspects de la fiabilité du réseau.

Le rôle du réseau a changé, passant d'un réseau de données uniquement à un système qui permet la connexion des personnes, des appareils et des informations dans un environnement de réseau convergent riche en supports. Pour que les réseaux fonctionnent efficacement et se développent dans ce type d'environnement, le réseau doit être construit sur une architecture de réseau standard.

Les réseaux doivent donc être capables de prendre en charge un large éventail d'applications et de services. Ils doivent fonctionner sur de nombreux types de câbles et de dispositifs différents, qui constituent l'infrastructure physique. Le terme "architecture de réseau", dans ce contexte, fait référence aux technologies qui soutiennent l'infrastructure et les services programmés et les règles, ou protocoles, qui font circuler les données sur le réseau.

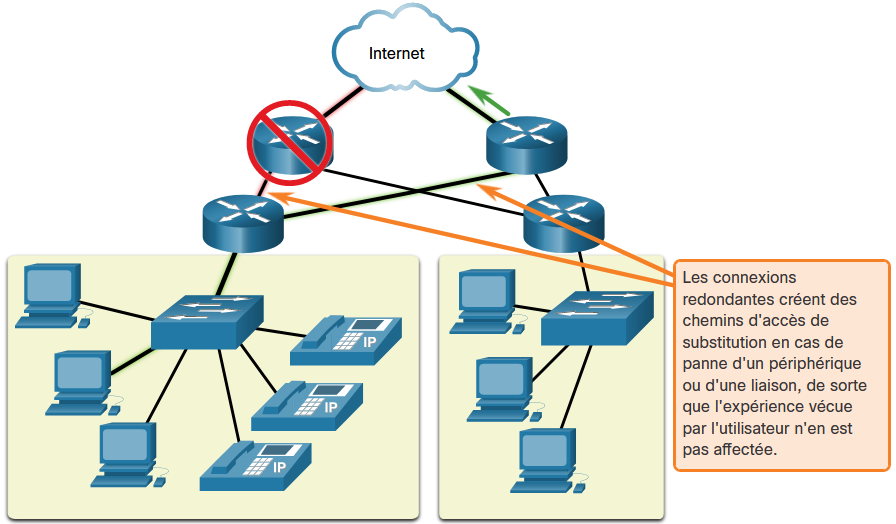
Au fur et à mesure de l'évolution des réseaux, nous avons appris qu'il existe quatre caractéristiques de base que les architectes de réseaux doivent prendre en compte pour répondre aux attentes des utilisateurs :

* Tolérance aux pannes
* Évolutivité
* Qualité de service (QoS)
* Sécurité

Tolérance aux pannes

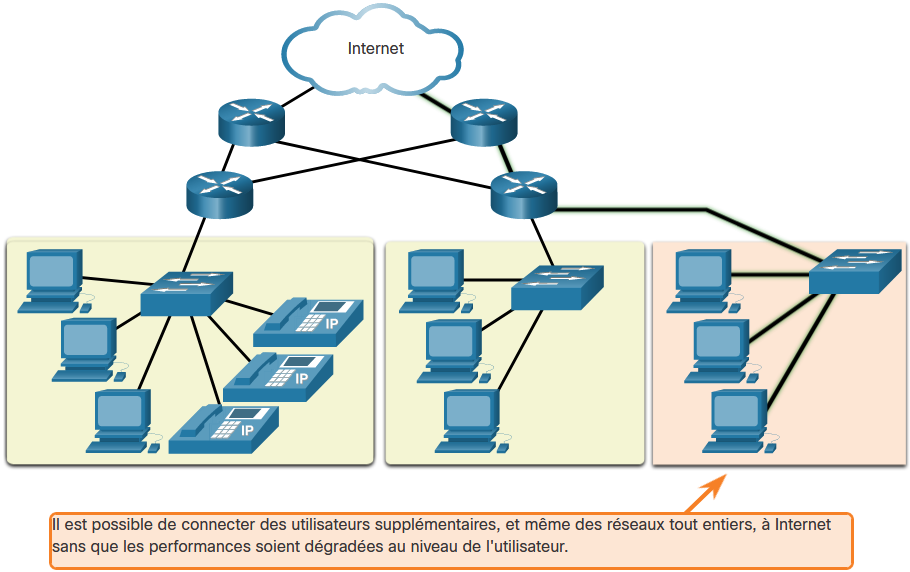
Un réseau tolérant aux pannes est un réseau qui limite le nombre de dispositifs affectés lors d'une panne. Il est également conçu de façon à permettre une récupération rapide en cas de panne. De tels réseaux s'appuient sur plusieurs chemins entre la source et la destination d'un message. Si un chemin échoue, les messages sont instantanément envoyés sur un autre lien. Le fait de disposer de plusieurs chemins vers une destination s'appelle la redondance.

La mise en place d'un réseau à commutation de paquets est l'un des moyens par lesquels des réseaux fiables assurent la redondance. La commutation de paquets fractionne le trafic en paquets qui sont acheminés sur un réseau partagé. Un message unique, tel qu'un e-mail ou un flux vidéo, est fractionné en de nombreux blocs de message appelés paquets. Chaque paquet comporte les informations d'adressage nécessaires de la source et de la destination du message. Les routeurs du réseau commutent les paquets en fonction de l'état du réseau à ce moment-là. Cela signifie que tous les paquets d'un même message peuvent emprunter des chemins très différents pour atteindre la même destination. Dans la figure, l'utilisateur n'est pas conscient et n'est pas affecté par le routeur qui modifie dynamiquement l'itinéraire lorsqu'une liaison est défaillante.



Evolutivité

Un réseau évolutif se développe rapidement pour prendre en charge les nouveaux utilisateurs et applications. Il le fait sans dégrader les performances des services auxquels les utilisateurs existants accèdent. La figure ci-contre montre comment un nouveau réseau peut être facilement ajouté à un réseau existant. En outre, les réseaux sont évolutifs étant donné que les concepteurs font appel à des normes et à des protocoles reconnus. Ainsi, les fournisseurs de logiciel et de matériel peuvent se concentrer sur l'amélioration des produits et des services, sans se soucier d'avoir à développer un nouvel ensemble de règles pour assurer leur fonctionnement dans le réseau.

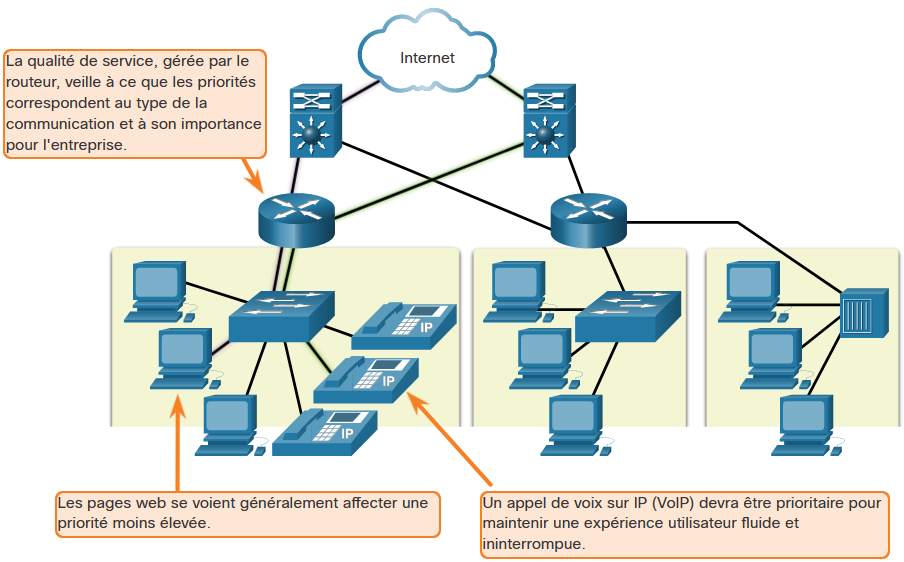


Qualité de Service (QOS)

La qualité de service (QoS) est une exigence croissante des réseaux aujourd'hui. Les nouvelles applications mises à la disposition des utilisateurs sur les réseaux, telles que les transmissions vocales et vidéo en direct, créent des attentes plus élevées quant à la qualité des services fournis. Avez -vous déjà tenté de visionner une vidéo saccadée ? Tandis que les données, les communications voix et le contenu vidéo convergent sur le même réseau, la QoS constitue un mécanisme essentiel pour gérer l'encombrement et assurer une fourniture fiable des contenus à l'ensemble des utilisateurs.

Un encombrement survient lorsqu'une demande excessive de bande passante dépasse les capacités disponibles. La bande passante réseau est mesurée en fonction du nombre de bits pouvant être transmis en une seconde, soit en « bits par seconde » (bit/s). Lorsque plusieurs communications sont initiées simultanément sur le réseau, la demande de bande passante peut excéder la quantité disponible, créant ainsi un encombrement du réseau.

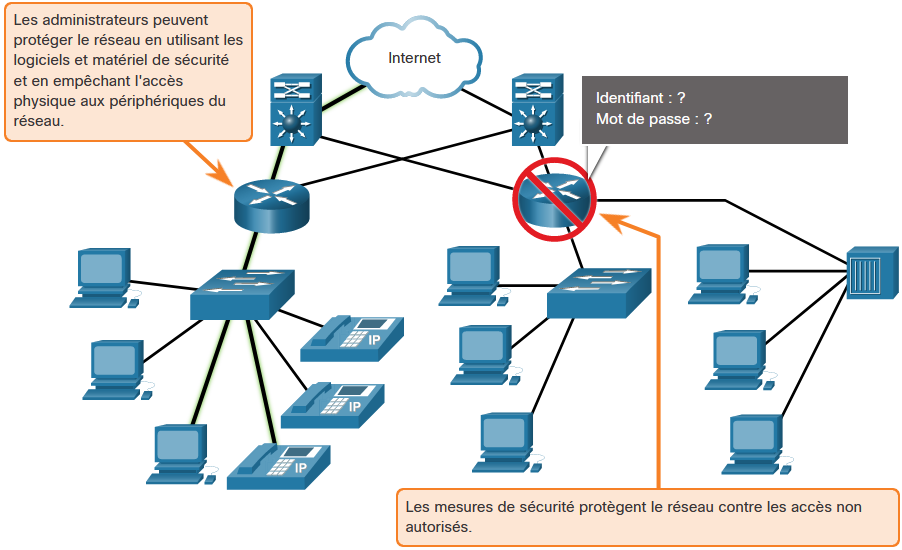
Lorsque le volume du trafic est supérieur à ce qui peut être transporté sur le réseau, les appareils gardent les paquets en mémoire jusqu'à ce que des ressources soient disponibles pour les transmettre. Dans la figure, un utilisateur demande une page web, et un autre est au téléphone. Lorsqu'une politique de Qualité de service (QoS) est mise en œuvre, le routeur peut gérer le flux de données et le trafic voix en donnant la priorité aux communications voix en cas de congestion du réseau.



Sécurité du Réseau

L'infrastructure réseau, les services et les données stockées sur les périphériques reliés au réseau sont des actifs personnels et professionnels essentiels. Les administrateurs de réseau doivent répondre à deux types de préoccupations en matière de sécurité des réseaux : la sécurité des infrastructures de réseau et la sécurité des informations.

La sécurisation de l'infrastructure du réseau comprend la sécurisation physique des dispositifs qui assurent la connectivité du réseau et la prévention de l'accès non autorisé aux logiciels de gestion qui y résident, comme le montre la figure.



Les administrateurs de réseau doivent également protéger les informations contenues dans les paquets transmis sur le réseau, ainsi que les informations stockées sur les périphériques connectés au réseau. Pour atteindre les objectifs de la sécurité des réseaux, il y a trois exigences principales.

* **Confidentialité** - La confidentialité des données signifie que seuls les destinataires prévus et autorisés peuvent accéder aux données et les lire.
* **Intégrité** - L'intégrité des données garantit aux utilisateurs que les informations n'ont pas été altérées lors de leur transmission, de l'origine à la destination.
* **Disponibilité** -La disponibilité des données garantit aux utilisateurs un accès rapide et fiable aux services de données pour les utilisateurs autorisés.

## Vérifiez votre compréhension - Réseaux fiables

## 

Tendance des réseaux

Tendances récentes

Vous en savez beaucoup sur les réseaux aujourd'hui, sur ce dont ils sont faits, sur la façon dont ils nous connectent et sur ce qui est nécessaire pour qu'ils restent fiables. Mais les réseaux, comme tout le reste, continuent de changer. Il y a quelques tendances en matière de réseautage que vous, en tant qu'étudiant NetaCAD, devriez connaître.

Avec l'arrivée de nouvelles technologies et de nouveaux appareils sur le marché, les entreprises et les consommateurs doivent en permanence s'adapter à un environnement en constante évolution. Il existe plusieurs nouvelles tendances relatives au réseau qui vont affecter les entreprises et les consommateurs:

* BYOD
* Collaboration en ligne
* Communications vidéo
* Cloud computing

BYOD

Le concept de tout appareil, pour tout contenu, de quelque manière que ce soit, est une tendance mondiale majeure qui exige des changements importants dans la manière dont nous utilisons les appareils et les connectons en toute sécurité aux réseaux. C'est ce que l'on appelle "Bring Your Own Device" (**BYOD**).

BYOD donne aux utilisateurs finaux la liberté d'utiliser des outils personnels pour accéder aux informations et communiquer à travers un réseau d'entreprise ou de campus. Avec la croissance des appareils grand public et la baisse des coûts qui en découle, les employés et les étudiants peuvent disposer d'appareils informatiques et de réseaux avancés pour leur usage personnel. Il s'agit notamment des ordinateurs portables, des blocs-notes, des tablettes, des téléphones intelligents et des lecteurs électroniques. Ils peuvent être achetés par l'entreprise ou l'école, achetés par le particulier, ou les deux.

Le BYOD, c'est pour tout type d'appareil, quel que soit son propriétaire, et partout.

Collaboration en ligne

Les utilisateurs individuels souhaitent se connecter au réseau pour accéder aux applications de données, mais aussi pour collaborer les uns avec les autres. La collaboration est définie comme « le fait de travailler avec une ou plusieurs autres personnes sur un projet commun ». Les outils de collaboration, comme Cisco WebEx, illustrés dans la figure, donnent aux employés, aux étudiants, aux enseignants, aux clients et aux partenaires un moyen de se connecter, d'interagir et d'atteindre leurs objectifs instantanément.

La collaboration est une priorité critique et stratégique que les organisations utilisent pour rester compétitives. La collaboration est également une priorité dans le domaine de la formation. Les étudiants doivent collaborer pour s'entraider dans l'apprentissage, pour développer les compétences d'équipe utilisées dans la vie professionnelle et pour travailler ensemble sur des projets en équipe.

Cisco Webex Teams est un outil de collaboration multifonctionnel qui vous permet d'envoyer des messages instantanés à une ou plusieurs personnes, de publier des images, des vidéos et des liens. Chaque équipe "espace" conserve un historique de tout ce qui y est affiché.

Communications vidéo

Une autre facette de la mise en réseau qui est essentielle à l'effort de communication et de collaboration est la vidéo. La vidéo est utilisée pour les communications, la collaboration et le divertissement. Les appels vidéo sont effectués vers et depuis toute personne disposant d'une connexion Internet, quel que soit l'endroit où elle se trouve.

La vidéo conférence est un outil puissant pour communiquer avec d'autres utilisateurs à distance, tant au niveau régional qu'international. La vidéo devient une condition essentielle pour collaborer efficacement à mesure que les entreprises se développent au-delà des frontières géographiques et culturelles.

Cloud computing

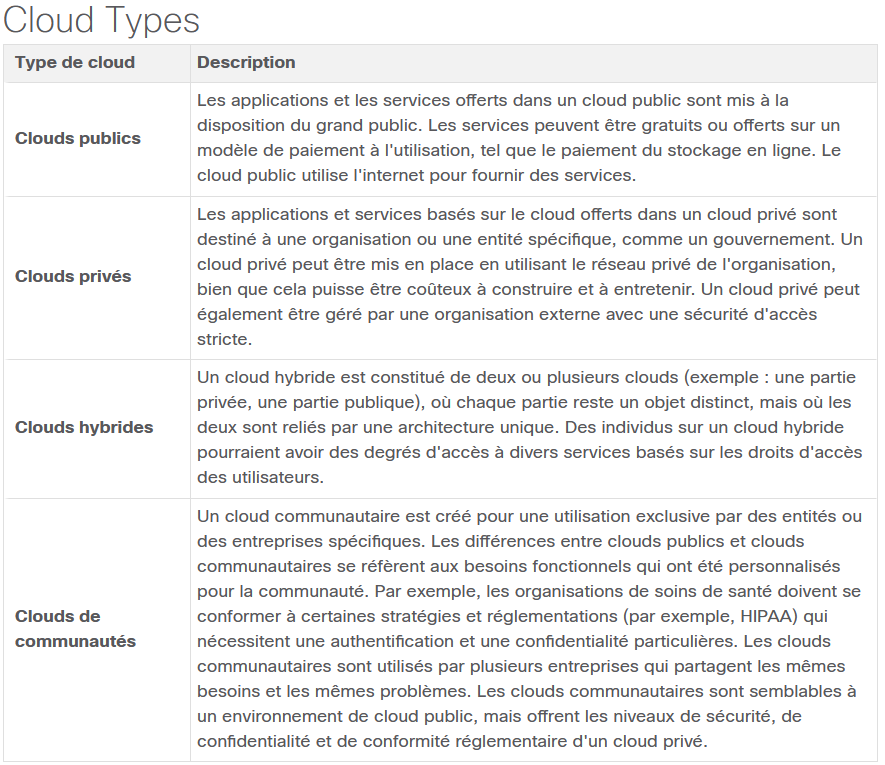
L'informatique en cloud est l'un des moyens d'accéder aux données et de les stocker. Le **cloud computing** nous permet de stocker des fichiers personnels, et même de sauvegarder un disque entier sur des serveurs via l'internet. Des applications telles que le traitement de texte et l'édition de photos sont accessibles via le cloud.

Pour les entreprises, le **cloud computing** offre de nouvelles fonctionnalités sans devoir investir dans une nouvelle infrastructure, former de nouveau le personnel, ni acheter de nouveaux logiciels sous licence. Ces services sont disponibles à la demande et sont fournis de manière économique à tout appareil se trouvant n'importe où dans le monde sans compromettre la sécurité ou le fonctionnement.

Le **cloud computing** fonctionne grâce aux centres de données. Les centres de données sont des installations utilisées pour héberger les systèmes informatiques et les composants associés. Un centre de données peut occuper une pièce d'un bâtiment, un ou plusieurs étages, ou un bâtiment entier de la taille d'un entrepôt. La construction et l'entretien des centres de données sont en général très coûteux. C'est pour cela que les grandes entreprises utilisent des centres de données privés pour stocker leurs données et fournir des services aux utilisateurs. Les entreprises de plus petite taille qui n'ont pas le budget suffisant pour gérer leur propre data center privé peuvent réduire le coût total de possession (TCO) en louant des services de serveur et de stockage à un centre de données de plus grande envergure hébergé dans le cloud.

Pour des raisons de sécurité, de fiabilité et de tolérance aux pannes, les fournisseurs de cloud computing stockent souvent les données dans des centres de données distribués. Au lieu de stocker toutes les données d'une personne ou d'une organisation dans un centre de données, elles sont stockées dans plusieurs centres de données situés à différents emplacements.

Il existe quatre principaux types de clouds: Les clouds publics, les clouds privés, les clouds hybrides et les clouds communautaires, comme indiqué dans le tableau.



Tendances technologiques domestiques

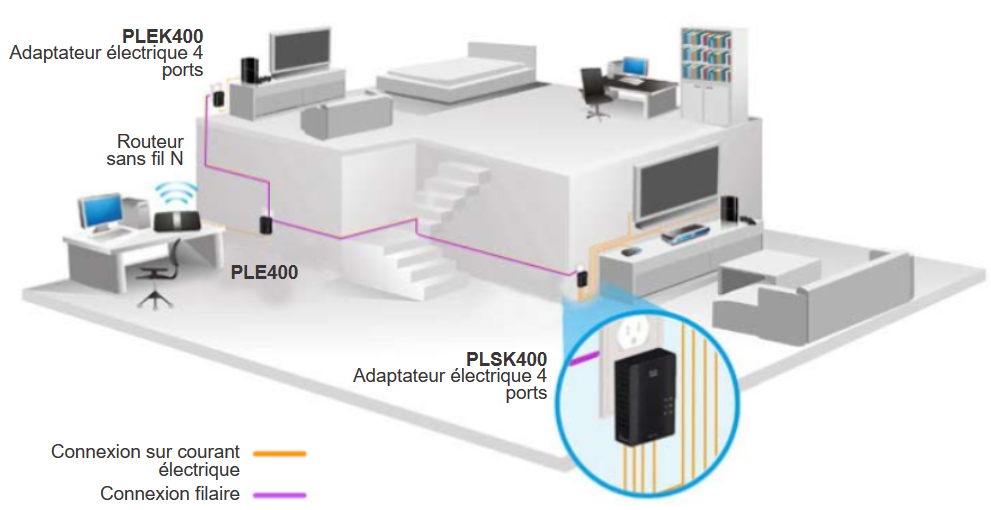
Les tendances à la mise en réseau n'affectent pas seulement la façon dont nous communiquons au travail et à l'école, mais elles modifient également de nombreux aspects de la maison. Les dernières tendances pour la maison incluent les « technologies domestiques intelligentes ».

La technologie de la maison intelligente s'intègre dans les appareils ménagers quotidiens, qui peuvent ensuite se connecter à d'autres appareils pour les rendre plus "intelligents" ou automatisés. Par exemple, vous pourriez préparer des aliments et les placer dans le four pour les faire cuire avant de quitter la maison pour la journée. Vous programmez votre four intelligent pour la nourriture que vous voulez qu'il cuisine. Il serait également relié à votre "calendrier des événements" afin de déterminer l'heure à laquelle vous devriez être disponible pour manger et d'ajuster les heures de début et la durée de la cuisson en conséquence. Il peut même régler les heures et les températures de cuisson en fonction des changements apportés à votre calendrier. En outre, un téléphone intelligent ou une tablette de connexion vous permet de vous connecter directement au four, pour effectuer les réglages souhaités. Lorsque la nourriture est prête, le four vous envoie un message d'alerte (ou quelqu'un que vous spécifiez) que la nourriture est faite et réchauffée.

Les technologies domestiques intelligentes sont en cours de développement et s'intègreront bientôt à toutes les pièces de la maison. La technologie des maisons intelligentes deviendra de plus en plus courante à mesure que les réseaux domestiques et la technologie de l'internet à haut débit se développeront.

Réseau sur courant électrique

La mise en réseau par courant électrique pour les réseaux domestiques utilise le câblage électrique existant pour connecter les appareils, comme le montre la figure.



À l'aide d'un adaptateur secteur standard, les périphériques peuvent se connecter au LAN en utilisant n'importe quelle prise de courant. Aucun câble de données n'a besoin d'être installé, et il y a peu ou pas d'électricité supplémentaire utilisée. Grâce au câblage électrique existant, le réseau sur courant porteur transmet des informations en envoyant les données sur des fréquences spécifiques.

La mise en réseau par courant électrique est particulièrement utile lorsque les points d'accès sans fil ne peuvent pas atteindre tous les appareils de la maison. Le réseau électrique n'est pas un substitut au câblage dédié dans les réseaux de données. Toutefois, elle constitue une alternative lorsque les câbles de réseau de données ou les communications sans fil ne sont pas possibles ou efficaces.

Haut débit sans fil

Dans de nombreux endroits où le câble et le DSL ne sont pas disponibles, le sans fil peut être utilisé pour se connecter à Internet.

**Fournisseur de services Internet sans fil**

Un fournisseur de services internet sans fil (WISP) est un fournisseur d'accès internet qui connecte les abonnés à un point d'accès ou à un point d'échange désigné en utilisant des technologies sans fil similaires à celles que l'on trouve dans les réseaux locaux sans fil (WLAN) des foyers. Les fournisseurs d'accès Internet sans fil opèrent généralement dans les régions rurales où la technologie DSL et les services par câble ne sont pas disponibles.

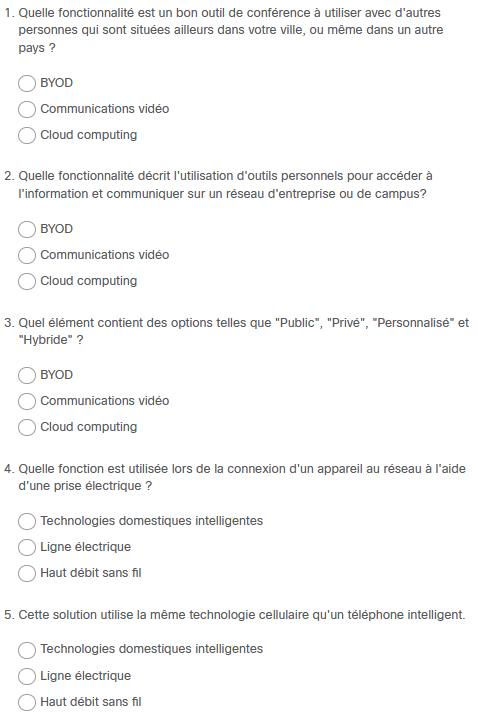
Bien qu'une tour de transmission séparée puisse être installée pour l'antenne, celle-ci est généralement fixée à une structure surélevée existante, telle qu'un château d'eau ou un pylône radio. Une petite parabole ou antenne est installée sur le toit de la maison de l'abonné, à portée de l'émetteur du fournisseur d'accès Internet sans fil. L'unité d'accès de l'abonné est connectée au réseau câblé à l'intérieur de la maison. Pour l'utilisateur à domicile, cette configuration n'est pas très différente de la technologie DSL ou du câble. La principale différence est en fait la connexion entre la maison et l'ISP: celle-ci se fait sans fil et n'utilise pas de câble.

**Service à large bande sans file**

Le haut débit sans fil est une autre solution pour disposer d'une connexion sans fil chez soi et dans les petites entreprises, comme indiqué dans la figure ci-contre.

Cette solution utilise la même technologie cellulaire qu'un téléphone intelligent. Une antenne est installée à l'extérieur de la maison pour offrir une connectivité avec ou sans fil aux périphériques du domicile. Dans de nombreuses régions, le haut débit sans fil domestique est en concurrence directe avec la technologie DSL et le câble.

**Vérifiez votre compréhension - Tendances du réseau**



Sécurité du réseau

Menace de sécurité

Vous avez, sans aucun doute, entendu ou lu des nouvelles sur un réseau d'entreprise violé, donnant aux acteurs de menace l'accès aux informations personnelles de milliers de clients. Pour cette raison, la sécurité réseau sera toujours une priorité absolue des administrateurs.

La sécurité des réseaux fait partie intégrante des réseaux informatiques, que le réseau se trouve dans un foyer avec une seule connexion à l'internet ou qu'il s'agisse d'une entreprise comptant des milliers d'utilisateurs. La sécurité du réseau mise en œuvre doit tenir compte de l'environnement, ainsi que des outils et des besoins du réseau. Le réseau doit être capable de sécuriser les données, tout en garantissant en permanence la qualité de service attendue.

La sécurisation d'un réseau implique des protocoles, des technologies, des dispositifs, des outils et des techniques afin de protéger les données et d'atténuer les menaces. Ces risques ou menaces peuvent être externes ou internes. De nos jours, de nombreuses menaces externes pour la sécurité des réseaux proviennent de l'internet.

Il existe plusieurs menaces externes courantes pour les réseaux :

* **Virus, vers, et chevaux de Trois** - logiciels malveillants et code arbitraire s'exécutant sur un périphérique utilisateur.
* **Spyware et adware** - Ce sont des types de logiciels qui sont installés sur l'appareil d'un utilisateur. Le logiciel recueille alors secrètement des informations sur l'utilisateur.
* **Attaques du jour zéro** - Appelées aussi attaques de l'heure zéro, elles se produisent le premier jour où une vulnérabilité est connue.
* **Attaques des acteurs de menace** - Une personne malveillante attaque les appareils des utilisateurs ou les ressources du réseau.
* **Attaques par déni de service** - Ces attaques ralentissent ou bloquent les applications et les processus sur un périphérique réseau.
* **Interception et vol de données** - Cette attaque permet de capturer des informations privées sur le réseau d'une organisation.
* **Usurpation d'identité** - Cette attaque consiste à voler les identifiants de connexion d'un utilisateur afin d'accéder à des données privées.

Il est également important de prendre en compte les menaces internes. De nombreuses études démontrent que la plupart des violations de données se produisent par la faute des utilisateurs internes du réseau. Ces violations peuvent découler d'une perte ou d'un vol de périphériques, de la mauvaise utilisation d'un périphérique par un employé ou, dans un contexte professionnel, d'un employé malveillant. En raison du développement des stratégies BYOD, les données d'entreprise sont beaucoup plus vulnérables. Par conséquent, lors de l'élaboration d'une politique de sécurité, il est important d'aborder les menaces de sécurité tant externes qu'internes, comme le montre la figure.

Solution de sécurité

Il n'existe pas de solution unique capable de protéger le réseau contre toutes les menaces existantes. Pour cette raison, la sécurité doit être implémentée en plusieurs couches et faire appel à plusieurs solutions de sécurité. Si un élément de sécurité ne parvient pas à identifier et à protéger le réseau, d'autres peuvent réussir.

La mise en œuvre de la sécurité du réseau domestique est habituellement plutôt simple. Généralement, vous l'implémentez sur les appareils terminaux, ainsi qu'au point de connexion à l'internet, et vous pouvez même compter sur les services contractuels d'ISP.

Ce sont les éléments de base de la sécurité d'un réseau domestique ou d'un petit bureau :

* **Antivirus et antispyware** - Ces applications aident à protéger les terminaux contre l'infection par des logiciels malveillants.
* **Filtrage par pare-feu** - Le filtrage par pare-feu bloque les accès non autorisés à l'entrée et à la sortie du réseau. Il peut s'agir d'un système de pare-feu basé sur l'hôte qui empêche tout accès non autorisé au dispositif final, ou d'un service de filtrage de base sur le routeur domestique pour empêcher tout accès non autorisé du monde extérieur au réseau.

En revanche, la mise en œuvre de la sécurité du réseau d'une entreprise implique généralement de nombreux composants intégrés dans le réseau afin de contrôler et de filtrer le trafic. L'idéal est que tous les composants fonctionnent ensemble, ce qui réduit les opérations de maintenance et renforce la sécurité. Les réseaux plus grands et les réseaux d'entreprise utilisent un antivirus, un antispyware et un filtrage de pare-feu, mais ils ont également d'autres exigences de sécurité:

* **Systèmes de pare-feu dédiés** - Ils offrent des capacités de pare-feu plus avancées qui peuvent filtrer de grandes quantités de trafic avec une plus grande granularité.
* **Listes de contrôle d'accès (ACL)** - Elles permettent de filtrer davantage l'accès et l'acheminement du trafic en fonction des adresses IP et des applications.
* **Systèmes de prévention des intrusions (IPS)** - Ils identifient les menaces qui se répandent rapidement, comme les attaques de type "zéro jour" ou "zéro heure".
* **Réseaux privés virtuels (VPN)** - Ils fournissent un accès sécurisé à une organisation pour les travailleurs à distance.

Les exigences de sécurité du réseau doivent prendre en compte l'environnement réseau, ainsi que les différentes applications et les exigences informatiques. Les réseaux domestiques et professionnels doivent pouvoir sécuriser leurs données tout en garantissant en permanence la qualité de service attendue de chaque technologie. En outre, la solution de sécurité mise en œuvre doit être capable de s'adapter aux nouvelles tendances et à l'évolution du réseau.

L'étude des menaces pour la sécurité du réseau et des techniques permettant de limiter les risques nécessite tout d'abord une parfaite compréhension de l'infrastructure de routage et de commutation sous-jacente, qui permet d'organiser les services réseau.

## Vérifiez votre compréhension - Sécurité des réseaux

## 

Professionnel de l’IT

CCNA

En tant qu'étudiant NetaCAD, vous avez peut-être déjà une carrière en informatique, ou vous êtes encore en train de vous former pour vous préparer à votre carrière. Dans les deux cas, il est bon de connaître les compétences nécessaires pour correspondre aux types d'emplois disponibles en informatique.

Le rôle et les compétences des ingénieurs réseau évoluent constamment et sont plus indispensables que jamais. La certification Cisco Certified Network Associate (CCNA) démontre que vous avez une connaissance des technologies de base et vous assure de rester pertinent avec les compétences nécessaires à l'adoption des technologies de nouvelle génération.

Un CCNA consolidé et mis à jour pour les ingénieurs réseau est composé de trois cours et d'un examen qui couvre les sujets fondamentaux pour toutes les technologies réseau. La nouvelle CCNA se concentre sur les fondements de l'IP et les questions de sécurité, ainsi que sur le sans-fil, la virtualisation, l'automatisation et la programmabilité des réseaux.

Il existe de nouvelles certifications DevNet aux niveaux associé, spécialiste et professionnel, pour valider vos compétences en matière de développement de logiciels.

Il existe des options de certification spécialisée pour valider vos compétences en fonction de votre rôle et de vos intérêts professionnels. Cela inclut la certification Cisco Enterprise Advanced Infrastructure Specialist.

Vous pouvez commencer où vous voulez. Il n'y a pas de conditions préalables pour commencer à obtenir votre certification de niveau associé, spécialiste, professionnel ou expert. Des crédits de formation continue pour la recertification et le développement continu sont désormais disponibles pour la CCNA.

## Module Questionnaire - Mise en réseau aujourd'hui

## 

