Cisco (RESIR2) - Lucky Summary

Sm!le42

22 mars 2021

Table des matières

1 Composants réseaux

1.1 Network

Un réseau est un **ensemble inter-connecté**, fait de composants autorisant la **circulation de flux** ou d'éléments finis.

(Ensemble de relations)

1.2 Rôle d'hôte

1.2.1 Hôtes ou périphériques finaux

Parfois appelés **clients**, ce sont des **ordinateurs connectés** à un réseau et qui participent directement aux communications transmises sur le réseau.

(Ex : Ordinateur, téléphone, tablette, imprimante...)

1.2.2 Adresse IP

Numéro qui **identifie** l'hôte et le réseau auquel l'hôte est connecté.

1. **IPv4 :** *Adresses IP* codées sur **32 bits**. Au maximum 2^{32} adresses *(soit 4 294 967 296)* peuvent donc être attribuées simultanément en théorie (en pratique, un certain nombre ne sont pas utilisables).
   Une *adresse IPv4* est représentée sous la forme de **quatre nombres entiers** séparés par des points. (Ex : 193.43.55.67)
   Chacun des nombres représente **un octet**. La plage d'attribution s'étend de *0.0.0.0* à *255.255.255.255*, sachant qu'il existe des contraintes empêchant l'utilisation de certaines adresses (réservée, masque, broadcast...).
2. **IPv6 :** Grâce à des adresses de **128 bits** *(au lieu de 32 bits en IPv4)*, on dispose d'un espace d'adressage bien plus important qu'IPv4 *(plus de 340 sextillions, ou* $\boldsymbol{340*10^{36}}$ *adresse différentes)*.
   Cette quantité d'adresses considérable permet une plus grande **flexibilité** dans l'attribution des adresses et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire.
   Le **déploiement** d'IPv6 sur Internet est **compliqué** en raison de l'**incompatibilité** des adresses IPv4 et IPv6. Les traducteurs d'adresses automatiques se heurtent à des problèmes pratiques importants. Pendant une **phase de transition** où coexistent IPv6 et IPv4, les hôtes disposent d'une **double pile**, c'est-à-dire qu'ils disposent à la fois d'adresses IPv6 et IPv4, et des tunnels permettent de traverser les groupes de routeurs qui ne prennent pas encore en charge IPv6.

1.2.3 Serveur

Ordinateur équipé de logiciels lui permettant de **fournir des informations**, *comme des messages électroniques ou des pages web*, à d'autres périphériques finaux sur le réseau.

CLIENT——-INTERNET——-SERVEUR

> **Notes :** Chaque service nécessite un **logiciel serveur distinct**. Un seul ordinateur peut exécuter différents types de logiciel client.
>
> (Ex : Logiciel de serveur web pour offrir des services web. Un utilisateur peut vérifier son courrier électronique et consulter une page web tout en utilisant une messagerie instantanée et en écoutant un flux audio.)

1.3 Peer-To-Peer

Lorsqu'un **ordinateur** fait à la fois office de **serveur** et de **client** sur le réseau.

(Ex : Réseaux particuliers, petites entreprises...)

> **Avantages :**
> — Facile à configurer
> — Moins complexe
> — Coût réduit car appareils réseau et serveurs dédiés pas toujours nécessaires
> — Peut-être utilisé pour des tâches simples
> **Inconvénients :**
> — Pas d'administration centralisée
> — Peu sécurisé
> — Non évolutif
> — Tous les périphériques peuvent servir à la fois de client et de serveur, ce qui peut ralentir les performances.

1.4 Équipements actifs

1.4.1 Périphérique intermédiaire

Périphérique **reliant** différents dispositifs finaux au réseau, et **fournissant la connectivité** en s'assurant que les données sont **transmises** sur le réseau.

(Ex : Routeur, routeur sans fil, pare-feu, commutateur LAN, commutateur multicouche...)

> **Rôles :**
> — Régénérer et retransmettre les signaux de communications.
> — Gérer des informations indiquant les chemins qui existent à travers le réseau et l'inter-réseau.
> — Indiquer aux autres périphériques les erreurs et les échecs de communication.
> — Diriger des données vers d'autres chemins en cas d'échec de liaison.
> — Classifier et diriger des messages en fonction des priorités.
> — Autoriser ou refuser le flux des données, selon des paramètres de sécurité.

Notes : Tous les dispositifs intermédiaires remplissent la fonction de répéteur. Les dispositifs intermédiaires peuvent connecter plusieurs réseaux individuels pour former un inter-réseau.

1.4.2 Répéteur

Dispositif qui **régénère et retransmet** les signaux de communication.

1.5 Support réseau

Canal via lequel le **message se déplace** de la source à la destination.

Les plus connus sont :
— Le cuivre
— La fibre optique
— Les ondes électromagnétiques

> Critères à prendre en compte :
> — Distance maximale des supports
> — Environnement
> — Quantité de donnée et vitesse de transmission
> — Coût des supports et de l'installation

1.6 Data center (Centre de données)

Installation utilisée pour **héberger** les systèmes informatiques et les composants associés.

> Un data center peut occuper une pièce d'un bâtiment, un ou plusieurs étages, voire même un bâtiment entier de la taille d'un entrepôt.
>
> Sa construction et son entretien sont en général très coûteux, ainsi, les grandes entreprises utilisent des centres de données privés, alors que les entreprises de plus petite taille, qui n'ont pas le budget suffisant pour gérer leur propre data center privé, vont plutôt en louer.

2 Topologies et représentations du réseau

2.1 Représentation du réseau

2.1.1 Diagramme de topologie

Représentation visuelle des connexions d'un réseau, permettant de comprendre facilement comment les appareils sont connectés dans ce réseau.

2.1.2 Carte d'interface (NIC)

Relie physiquement le dispositif terminal au réseau.

2.1.3 Port physique

Connecteur ou prise sur un dispositif de réseau où le support se connecte à un dispositif terminal ou à un autre dispositif de réseau.

2.1.4 Interface

Ports spécialisés sur un dispositif de réseau qui se connecte à des réseaux individuels.

> Comme les routeurs connectent les réseaux, les ports des routeurs sont appelés *interfaces réseaux*.
>
> Les termes port et interface sont souvent utilisés l'un pour l'autre.

3 Types courants de réseaux

3.1 Réseaux de tailles diverses

3.1.1 Petit réseau domestique

Relie **quelques ordinateurs** entre eux et à Internet.

(Ex : Réseau classique familial)

3.1.2 Réseau de petit bureau et de bureau à domicile (SOHO)

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.

(Ex : Très petites entreprises)

3.1.3 Moyen et grand réseaux

Possibilité d'avoir de **nombreux emplacements** avec des centaines ou des milliers d'hôtes inter-connectés.

(Ex : Entreprises, écoles...)

3.1.4 Réseau mondial

Connexion de **centaines de millions** d'ordinateurs dans le **monde entier**.

(Ex : Internet)

3.2 LAN et WAN

3.2.1 LAN (Local Area Network)

Un réseau local est une **infrastructure de réseau** qui fournit un accès aux utilisateurs et aux dispositifs finaux dans une **petite zone géographique**.

(Ex : Maison, école, immeuble, campus...)

Caractéristiques :
- Zone limitée
- Administré par une seule personne
- Bande passante à haut débit pour les périphériques terminaux internes et intermédiaires

3.2.2 WLAN (Wireless Local Area Network)

Un WLAN est un LAN utilisant la technologie sans fil.

3.2.3 WAN (World Area Network)

Un réseau mondial 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 télécommunication.

Caractéristiques :
- Vaste zone géographique (Villes, états, provinces, pays, continents...)
- Administré par plusieurs prestataires de services
- Liaisons à plus bas débit entre les réseaux locaux

3.3 Internet

Ensemble **mondial** de réseaux privés et publics inter-connectés. (Réseau de réseaux)

3.4 Intranet et extranet

3.4.1 Intranet

Connexion **privée** de LAN et de WAN qui appartiennent 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.

3.4.2 Extranet

Accès sûr et sécurisé pour aux personnes qui travaillent pour une organisation différente, mais qui ont besoin d'accéder aux données de l'organisation.

Exemples :
- Entreprise qui donne accès aux fournisseurs et entrepreneurs de l'extérieur
- Hôpital qui fournit un système de réservation aux médecins afin qu'ils puissent prendre des rendez-vous pour leurs patients
- Bureau local de l'éducation qui fournit des informations sur le budget et le personnel aux écoles de son district

INTERNET——-(EXTRANET)——-((INTRANET))

Pas d'accès———(Accès restreint)——((Accès complet))

4 Connexions Internet

4.1 Technologie d'accès à Internet

4.1.1 ISP (Internet Service Provider)

Fournisseur d'accès à Internet. (Ex : Proximus, Orange...)

4.1.2 WISP (Wireless Internet Service Provider)

Un WISP *(Wireless Internet Services Provider)* 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 des foyers.

Cette configuration n'est pas très différente de la technologie DSL ou du câble. La **principale différence** est la connexion entre le maison et l'ISP : Celle-ci se fait sans fil et n'utilise pas de câble.

4.2 Connexions Internet des bureaux à domicile et des petits bureaux

4.2.1 Câble

Utilisation du même câble que celui qui achemine la **télévision** par câble.

Avantages :
— Large bande passante
— Connexion permanente à l'Internet

4.2.2 DSL (Digital Subscriber Line)

Utilisation d'une **ligne téléphonique**.

Avantages :
— Large bande passante
— Connexion permanente à l'Internet
— Grande disponibilité

1. **ADSL :** *Asymmetric Digital Subscriber Line*
   Vitesse descendante **supérieure** à la vitesse ascendante.
2. **SDSL :** *Symmetric Digital Subscriber Line*
   Vitesse descendante et ascendante **identiques** et élevées.
3. **VDSL :** *Very high-speed rate Digital Subscriber Line*
   Vitesse de transmissoin **très élevée**. (Symmetric ou Asymmetric)

4.2.3 Cellulaire

Utilisation d'un réseau de téléphonie **mobile**.

Avantage :
Permet une connexion dans une région qui, autrement, n'aurait aucune connectivité Internet.
Inconvénient :
Les antennes paraboliques nécessitent une ligne de vue claire vers le satellite.

4.2.4 Ligne commutée

Utilisation d'une **ligne téléphonique** et d'un **modem**.

Avantages :
— Peu coûteux
— Utile lors de déplacements
Inconvénient :
Faible bande passante, insuffisante pour les transferts de données importantes

4.3 Connexion Internet d'entreprise

4.3.1 Ligne louées dédiée

Circuit **réservé** au sein du réseau du fournisseur de service, qui relie des bureaux géographiquement séparés par un réseau privé de voix et/ou de données. (Généralement loué sur une base mensuelle ou annuelle)

4.3.2 Ethernet (ou Ethernet WAN)

Étend la technologie d'accès LAN au WAN.

4.3.3 Business DSL

Souvent SDSL.

4.3.4 Satellite

Lorsqu'une solution câblée n'est pas disponible, on peut avoir recours à des satellites en orbite autour de la Terre, qui fournissent une connexion Internet sans fil.

4.4 Réseau convergent

4.4.1 Réseaux séparés traditionnels

Réseaux utilisant des **technologies différentes** pour le transport du signal de communication, et ne **pouvant donc pas communiquer entre eux**.

Chaque réseau a son propre ensemble de règles et de normes pour garantir le bon fonctionnement des communications.

(Ex : Les ordinateurs, téléphones, services de diffusion, ne peuvent pas communiquer entre eux. On ne peut donc pas voir un appel téléphonique sur un ordinateur)

4.4.2 Réseaux convergents

Réseaux **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* mis en oeuvre.

(Ex : Les ordinateurs, téléphones, services de diffusion, peuvent communiquer entre eux grâce à une règle de contrat standard commune)

5 Réseaux fiables

5.1 Architecture réseau

Technologies qui soutiennent l'infrastructure et les services programmés et les règles, ou protocoles, qui font circuler les données sur le réseau.

5.2 Tolérance aux pannes

Limitation du nombre de dispositifs affectés lors d'une panne. Conception de façon à permettre une récupération rapide en cas de panne. Utilisation de la redondance.

5.2.1 Redondance

Utilisation de plusieurs chemins entre la source et la destination d'un message. Ainsi, si un chemin échoue, les messages sont instantanément envoyés sur un autre lien.

5.2.2 Commutation par paquets

Fractionnement du trafic en *paquets* qui sont acheminés sur un réseau partagé. Ainsi, un message unique (tel qu'un e-mail ou un flux vidéo) est fractionné en de nombreux blocs de messages appelés *paquets*, qui contiennent chacun 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, ce qui signifie que **tous les paquets d'un même message peuvent emprunter des chemins très différents pour atteindre la même destination** car le routeur modifie dynamiquement l'itinéraire lorsqu'une connexion est défaillante (–> Redondance).

5.3 Évolutivité

5.3.1 Réseau évolutif

Un réseau évolutif se **développe rapidement** pour prendre en charge les nouveaux utilisateurs et applications, et ceci **sans dégrader les performances** des services auxquels les utilisateurs existant accèdent. 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 logiciels 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 s'assurer leur fonctionnement dans le réseau.

(Ex : Il est posible de connecter des utilisateurs supplémentaires, et même des réseaux entiers, à Internet, sans que les performances soient dégradés au niveau de l'utilisateur)

5.4 Qualité de service (QoS)

Mécanisme essentiel pour **gérer l'encombrement** et assurer une fourniture fiable des contenus à l'ensemble des utilisateurs. 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.

(Ex : Si un utilisateur demande une page web, et un autre est au téléphone, lorsqu'une politique de QoS est mise en oeuvre, le routeur peut gérer le flux de données et le trafic voix en donnant la priorité aux communcations voix en cas de congestion du réseau)

Note : Les pages web se voient généralement affecter une priorité moins élevée. Un appel de voix sur IP (VoIP) devra être prioritaire pour maintenir une expérience utilisateur fluide et ininterrompue.

5.4.1 Encombrement

Lorsque la demande de bande passante excède la quantité disponible.

5.4.2 Bande passante

Nombre de bits pouvant être transmis par seconde. (bit/s)

5.5 Sécurité du réseau

Les administrateurs de réseaux doivent répondre à deux types de préoccupations en matière de sécurité des réseaux :

- La sécurité des infrastructures de réseau (Sécurité physique)
- La sécurité des informations (Sécurité virtuelle)

Il y a 3 exigences principales :

1. **Confidentialité :** Seuls les destinataires prévus et autorisés peuvent accéder aux données et les lire.
2. **Intégrité :** Garantir aux utilisateurs que les informations n'ont pas été altérées lors de leur transmission, de l'origine à la destination.
3. **Disponibilité :** Garantir aux utilisateurs un accès rapide et fiable aux services de données.

6 Tendances des réseaux

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.

6.1 BYOD (Bring Your Own Device)

Le 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. C'est ce qu'on appelle le "Bring Your Own Device". (–> "Apporte Ton Propre Appareil")

6.2 Collaboration en ligne

C'est le fait de travailler avec une ou plusieurs autres personnes sur un projet commun. Ceci offre un moyen de se connecter, d'interagir et d'atteindre des objectifs instantanément.

6.3 Communication vidéo

Outil puissant pour communiquer avec d'autres utilisateurs à distance, tant u 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.

6.4 Cloud computing

Le cloud computing nous permet de stocker des fichiers personnels, et même de sauvegarder un disque entier sur des serveurs via l'Internet, grâce aux centres de données.

Il existe 4 principaux types de clouds :

1. **Cloud public**
   Services mis à la disposition du grand public via Internet, pouvant être gratuits ou payants.

2. **Cloud privé**
   Services destinés à une organisation ou une entité spécifique.
3. **Cloud hybride**
   Constitué de deux ou plusieurs clouds, où chaque partie reste un objet distinct, mais où les deux sont reliés par une architecture unique. (Ex : Une partie privée, et une partie publique)
4. **Cloud de communautés**
   Créé pour une utilisation exclusive par des entités ou des entreprises spécifiques, semblable à un environnement de cloud public, mais offrant les niveaux de sécurité, de confidentialité et de conformité réglementaire d'un cloud privé.

6.5 Tendances technologiques domestiques

Celles-ci 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 intelligents*.

Technologies domestiques intelligentes : Celles-ci s'intègrent dans les appareils ménagers quotidiens, qui peuvent ensuite se connecter à d'autres appareils pour les rendre plus *"intelligents"* ou *automatisés*.

Les technologies domestiques intelligents sont en cours de développement et s'intègreront bientôt à toutes les pièces de la maison.

La technologie domestique intelligente deviendra de plus en plus courant à mesure que les réseaux domestiques et la technologie de l'Internet à haut débit se développeront.

(Ex : Four programmable afin de déterminer certaines heures et températures en fonction de vos disponibilités et des aliments utilisés, avec possibilité de recevoir une notification sur un autre appareil lorsque le repas est prêt.

6.6 Réseau sur courant électrique

Utilisation du **câblage électrique** existant pour connecter les appareils. Le réseau sur courant porteur transmet des informations en envoyant les données sur des **fréquences spécifiques**. Ainsi, 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.

La mise en réseau par courant 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.

6.7 Haut débit sans fil

Celle-ci 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 à domicile.

Dans de nombreuses régions, le haut débit sans fil domestique est en concurrence avec la technologie DSL et le câble.

7 Sécurité du réseau

7.1 Menaces de sécurité

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 millions d'utilisateurs.

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**.

7.1.1 Menaces internes

Violations par la faute d'utilisateurs **internes du réseau**.

En raison du développement des stratégies BYOD, les données d'entreprises sont beaucoup plus vulnérables.

Exemples :
— Perte ou vol d'un périphérique
— Mauvaise utilisation d'un périphérique
— Employé malveillant

7.1.2 Menaces externes

Violations par la faute d'utilisateur **externes au réseau** (venant Internet).

1. **Virus, vers et chevaux de Troie :** Logiciels malveillants et code arbitraire s'exécutant sur un périphérique utilisateur.
2. **Spyware et adware :** Types de logiciels installés sur l'appareil d'un utilisateur. Ce logiciel **recueille** alors secrètement des **informations** sur l'utilisateur.
3. **Attaques du jour zéro :** Appelées aussi *attaques de l'heure zéro*, elles se produisent le **premier jour** où une vulnérabilité est connue.
4. **Attaques des acteurs de menace :** Une personne malveillante attaque les **appareils** des utilisateurs ou les **ressources** du réseau.
5. **DoS (Denial of Service attack) :** Ces *attaques par déni de service* **ralentissent** ou **bloquent** les applications et les processus sur un périphérique réseau.
6. **Interception et vol de données :** Cette attaque permet de **capturer des informations privées** sur le réseau d'une organisation.
7. **Usurpation d'identité :** Cette attaque consiste à **voler les identifiants** de connexion d'un utilisateur afin d'accéder à des données privées.

7.2 Solutions 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.

7.2.1 Sécurité d'un réseau domestique

La mise en place de la *sécurité d'un réseau domestique* est habituellement plutôt simple.

Généralement elle est implémentée sur les **appareils terminaux**, ainsi qu'au **point de connexion à l'Internet**, et on peut même compter sur les services contractuels d'ISP.

1. **Antivirus et antispyware :** Ces applications aident à protéger les terminaux contre l'infection par des logiciels malveillants.
2. **Filtrage par pare-feu :** Blocage des 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 vers le réseau.

7.2.2 Sécurité d'un réseau d'entreprise

La mise en place de la *sécurité d'un réseau d'entreprise* implique généralement de **nombreux composants intégrés** dans le réseau afin de contrôler et de filtrer le trafic.

Les réseaux d'entreprises utilisent un antivirus, un antispyware et un filtrage de pare-feu, mais ils ont également d'autres exigences de sécurité :

1. **Systèmes de pare-feu dédiés :** Ceux-ci offrent des capacités de pare-feu plus avancées qui peuvent filtrer de **grandes quantités de trafic** avec une plus grande granularité.
2. **ACL (Access Control List) :** Les listes de contrôle d'accès permettent de filtrer d'avantage l'accès et l'acheminement du trafic en fonction des adresses IP et des applications.
3. **IPS (Intrusion Prevention System) :** Les *systèmes de prévention d'intrusion* identifient les menaces qui se répandent rapidement, comme les attaques de type jour zéro.
4. **VPN :** Les VPN fournissent un accès sécurisé à une organisation pour les travailleurs à distance.

8 OS (Operating System)

Un *système d'exploitation* est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs.

Le système d'exploitation est le logiciel :
- Principal car il permet à l'ordinateur et aux programmes de fonctionner
- Qui se lance en second après le firmware (*programme d'amorçage* ou *bootloader*) exécuté lors de la mise en marche de l'ordinateur.

Tous les **périphériques finaux** et **réseau** requièrent un *système d'exploitation*.

8.1 Objectifs d'un OS

Les OS réseau sont similaires aux OS d'un ordinateur classique.

Grâce à un GUI, l'**OS d'un PC** permet à l'utilisateur de procéder aux opérations suivantes :
- Utiliser une souris pour faire des sélections ou exécuter des programmes
- Entrer des commandes textuelles
- Afficher des images sur un écran

Un **OS réseau** utilisant un CLI permet à un technicien réseau d'effectuer les opérations suivantes :
- Utiliser un clavier pour exécuter des programmes réseau basés sur **CLI**
- Utiliser un clavier pour entrer des commandes textuelles
- Afficher des images sur un écran

8.2 Kernel

Le *noyau* d'un OS est sa partie qui assure la **communication** entre le **matériel** informatique et les **logiciels**, et qui gère le mode d'utilisation des ressources matérielles pour satisfaire la configuration logicielle.

8.3 Interpréteur de commandes

L'*interpréteur de commandes* d'un OS est un interface qui permet aux utilisateurs de demander des tâches spécifiques à partir de l'ordinateur. Ces requêtes peuvent être effectuées via l'interface **CLI** *(Command Line Interface)* ou **GUI** *(Graphical User Interface)*.

Les **GUI** ne disposent pas toujours de toutes les fonctionnalités disponibles dans le **CLI**, et elles peuvent également tomber en panne ou simplement ne pas fonctionner correctement. C'est pourquoi l'accès aux périphériques réseau se fait habituellement vie le **CLI**.

9 UI (User Interface)

9.1 CLI (Command Line Interface)

L'*interface en ligne de commande* est le moyen **textuel** utilisé par les utilisateurs afin d'accéder à l'**interpréteur de commandes**.

> Nécessite très **peu de ressources** pour fonctionner et offre une grande **stabilité** par rapport au **GUI**, cependant, l'utilisateur doit connaître la structure de commandes sous-jacente qui contrôle le système.

9.2 GUI (Graphical User Interface)

L'*interface graphique* permet aux utilisateurs d'interagir avec le système à l'aide d'un environnement utilisant des **éléments graphiques** *(icônes, menus, fenêtres. . .)*. (Ex : Windows, MacOS, KDE...)

> Plus convivial que le **CLI** et ne nécessite pas de connaître la structure de commandes sous-jacente qui contrôle le système. En revanche, le **GUI** est moins fiable et plus lent que le **CLI**.

10 Méthodes d'accès

Un commutateur transmet le trafic par défaut et n'a **pas besoin** d'être explicitement configuré pour fonctionner.

(Ex : Deux hôtes configurés connectés au même nouveau commutateur seraient en mesure de communiquer)

Quel que soit le comportement par défaut d'un nouveau commutateur, **tous** les commutateurs doivent être **configurés** et **sécurisés**.

10.1 Console

Port de gestion permettant un accès **hors réseau** à un périphérique. L'accès hors bande désigne l'accès via un canal de gestion dédié qui est utilisé uniquement pour la maintenance des périphériques.

Avantage : Le périphériques est accessible même si aucun service réseau n'a été configuré.

10.2 SSH (Secure Shell)

Moyen d'établir **à distance** une connexion CLI **sécurisée** via une interface virtuelle sur un réseau. Les connexions SSH requièrent des **services réseau actifs** sur le périphériques, notamment une interface active possédant une adresse.

10.3 Telnet

Moyen **non sécurisé** d'établir une connexion CLI à distance via une interface virtuelle sur un réseau. Contrairement à *SSH*, *Telnet* fournit une connexion qui n'est **pas sécurisée ni cryptée**, et ne doit donc être utilisé que dans un environnement de travaux pratiques.

Les informations d'authentification des utilisateurs, les mots de passe et les commandes sont envoyés sur le réseau **en clair**.

10.4 Programmes d'émulation de terminal

Programme permettant de se **connecter** à un périphérique réseau via une connexion série sur un port de console ou via une connexion SSH ou Telnet.

(Ex : PuTTY, Tera Term, SecureCRT...)

Ceux-ci permettent d'**améliorer la productivité** grâce à différentes fonctionnalités comme la **personnalisation** de la taille des fenêtres, de la taille des polices ou des jeux de couleurs.

11 Utilisation de l'IOS de Cisco via le CLI

11.1 Mode privilégié

Par mesure de sécurité, le logiciel Cisco IOS sépare l'accès à la gestion en deux modes de commande :
- Mode d'exécution **utilisateur** avec **accès limité** aux commandes (Symbole '>')
- Mode d'exécution **privilégié** avec **accès complet** aux commandes (Symbole '#')

Commande pour entrer en mode privilégié : `enable`.
Commande pour revenir en mode utilisateur : `disable`.

11.2 Mode de configuration globale

Pour **configurer** un périphérique, l'utilisateur doit passer en mode de **configuration globale**. Celui-ci affecte le fonctionnement du périphérique dans son ensemble. Ce mode se reconnaît à l'invite de commande se terminant par **(config)#** après le nom de l'appareil. (Ex : Switch(config)#)

Une fois le mode de configuration globale activé, l'utilisateur a accès à des **sous-modes** de configuration. Les deux sous-modes de configuration les plus courants sont ceux-ci :
- Mode de configuration **en ligne** (Via Console, SSH, Telnet ou AUX)
- Mode de configuration d'**interface** (Configuration de l'interface réseau d'un port de Switch ou routeur)

Lors de l'utilisation d'un CLI, le mode actif est reconnaissable à son invite de commandes unique.

```
Périphérique (mode-mode) mode
```

Exemples :
- **Switch(config-line)#** = *Configuration **en ligne** de **Switch** en mode **privilégié***
- **Foo(config-if)#** = *Configuration **interface** de **Foo** en mode **privilégié***

Commande pour entrer en mode de configuration globale : `configure terminal`.
Commande pour sortir d'un mode de configuration : `exit`.
Commande pour quitter tous les modes de configuration : `end` *ou* `Ctrl+Z`.

Exemple :
```
— Switch>
— Switch> enable
— Switch#
— Switch# configure terminal
— Switch(config)#
— Switch(config)# line console 0
— Switch(config-line)#
— Switch(config-line)# exit
— Switch(config)#
— Switch(config)# interface vlan 1
— Switch(config-if)#
— Switch(config-if)# end ( ou CTRL+Z )
— Switch#
— Switch# disable
— Switch>
```

11.3 Structure des commandes IOS de base

Les commandes de base sont formées ainsi :

Invite + Commande + 'espace' + Mot-clé ou argument

Exemples :
- Switch> show ip protocol
- Switch# ping 192.168.10.5

Un **mot-clé** est un paramètre **spécifique** défini dans l'OS. (Ex : ip protocol)

Un **argument** n'est pas défini dans l'OS, c'est une valeur ou variable définie par l'utilisateur. (Ex : 192.168.10.5)

11.4 Conventions pour la configuration des noms d'hôte

Par convention, un nom d'hôte doit respecter les règles suivantes :
- Débuter par une lettre
- Ne pas contenir d'espaces
- Se terminer par une lettre ou un chiffre
- Ne comporter que des lettres, des chiffres et des tirets
- Comporter moins de 64 caractères

Exemple : (attribution du nom "`Sw-Floor-1`" au périphérique `Switch`)
- `Switch\# configure terminal`
- `Switch(config)\#`
- `Switch(config)\# hostname Sw-Floor-1`
- `Sw-Floor_1\#`

11.5 Configurer les mots de passe

Pour **sécuriser** l'accès en mode d'exécution **utilisateur**, il faut utiliser les commandes suivantes :
- `configure terminal` (Entrer dans le mode de configuration globale)
- `line console 0` (Accéder à la première interface de la console de ligne, souvent la seule disponible)
- `password azerty` (Configurer le mot de passe "azerty")
- `login` (Activer l'accès d'exécution utilisateur)
- `end` (Quitter tous les modes de configuration)

La console d'accès requiert à présent le mot de passe `azerty` avant d'accéder au mode d'exécution utilisateur.

Pour **sécuriser** l'accès en mode **privilégié**, il faut utiliser les commandes suivantes :
- `configure terminal` (Entrer dans le mode de configuration globale)
- `enable secret azerty` (Configurer le mot de passe "azerty")
- `exit` (Quitter le mode de configuration)

Les lignes **VTY** (virtual terminal) activent l'accès **à distance** au périphérique en utilisant SSH ou Telnet.

Pour sécuriser les lignes **VTY**,il faut utiliser les commandes suivantes :
- `configure terminal` (Entrer dans le mode de configuration globale)
- `line vty 0 15` (Entrer dans le mode de configuration de VTY ligne)
- `password azerty` (Configurer le mot de passe "azerty")
- `login` (Activer l'accès VTY)
- `end` (Quitter tous les modes de configuration)

11.6 Chiffrer les mots de passe

Pour **chiffrer** tous les mots de passe en texte clair, il faut utiliser les commandes suivantes :
- `configure terminal` (Entrer dans le mode de configuration globale)
- `service password-encryption` (Activer le chiffrement des mots de passe non chiffrés)
- `end` (Quitter le mode de configuration globale)
- `show running-config` (Vérifier que les mots de passe sont maintenant chiffrés)

11.7 Fichiers de configuration

Deux fichiers système stockent la **configuration** des périphériques :
- `startup config` (Fichier stocké dans la mémoire non volatile, et donc, disponibles lors du démarrage de la machine)
- `running-config` (Fichier stocké dans la mémoire RAM, et donc, perdue lors de l'extinction de la machine)

En cas de redémarrage ou de panne de courant, toutes les modifications de la configuration non enregistrées seront **perdues**.

Pour enregistrer les configurations dans le fichier "startup-config", il faut utiliser la commande suivant :

```
copy running-config startup-config
```

Pour restaurer l'appareil dans sa configuration précédente (startup-config), il faut utiliser la commande suivante :

```
reload
```

(Cette commande impliquera une brève interruption du réseau)

Pour supprimer toutes les configurations, il faut utiliser les commandes suivantes :
- `erase startup-config` (Supprimer le fichier "startup-config")
- `reload` (Supprimer le fichier "running-config" et charger la configuration initiale d'origine)

11.8 Enregistrer une configuration dans un fichier texte

Pour **enregistrer** une configuration dans un **fichier texte**, il faut utiliser un logiciel d'émulation de terminal (Ex : PuTTY) connecté à un Switch.
- **Ouvrir** le logiciel d'émulation de terminal
- **Activer l'enregistrement** dans le logiciel d'émulation, et choisir un emplacement de fichier de sortie
- **Exécuter** la commande "`show running-config`" ou "`show startup-config`" dans l'invité de commande d'exécution privilégiée (Le texte affiché dans la fenêtre du terminal est alors placé dans le fichier configuré à la deuxième étape)
- **Désactiver l'enregistrement** dans le logiciel d'émulation

Pour **restaurer** un fichier de configuration sur un périphérique :
- Passer en mode de **configuration globale** sur le périphérique
- **Copier-Coller** le fichier texte dans la fenêtre du terminal connecté

(Le texte contenu dans le fichier est appliqué sous forme de commandes dans l'environnement CLI et devient la configuration en cours du périphérique)

11.9 Configuration de l'interface de commutateur virtuelle

Pour accéder à distance au commutateur, une adresse IP et un masque de sous-réseau doivent être configurés.

- `configure terminal` (Accéder au mode de configuration global)
- `interface vlan1` (Accéder au mode de configuration interface de vlan1)
- `ip address 192.168.1.20 255.255.255.0` (Ex : Attribuer l'adresse IP en fonction du masque)
- `no shutdown` (Activer l'interface virtuelle)
- `exit` (Quitter le mode de config interface)
- `ip default-gateway 192.168.1.1` (Attribuer l'adresse IP à la passerelle par défaut)

12 Exigences relatives au Protocole de Réseau

Les protocoles informatiques communs comprennent le exigences suivantes :
- Codages des messages
- Format et encapsulation des messages
- Taille des messages
- Synchronisation des messages
- Options de remise des messages

12.1 Codages des messages

Il faut que l'expéditeur et la destination utilisent le même système de *codage* et de *décodage*.

(Ex : Si on veut dire quelque chose à quelqu'un, il vaut mieux utiliser une langue qu'il comprend)

12.2 Format et encapsulation des messages

Lorsqu'un message est envoyé de la source à la destination, il doit suivre un *format* ou un *structure* spécifique. Celui-ci dépend du type de message et du type de canal utilisé.

(Ex : Si on veut envoyer un message à quelq'un, on peut l'envoyer via une lettre par la poste. Celle-ci devra comporter l'adresse du destinataire placée au bon endroit, sans quoi la lettre ne sera pas transmise)

12.3 Taille des messages

13 TODO Suite en cours de création…

14 Vocabulaire de base

14.1 OSI Model (Open Systems Interconnection)

Le modèle OSI est une **norme de communication**, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation internationale de normalisation) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

Modèle OSI

	PDU	Couche		Fonction
Couches hautes	Donnée	7	Application	Point d'accès aux services réseau
		6	Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine
		5	Session	Communication Interhost, gère les sessions entre les différentes applications
	Segment (en) / Datagramme	4	Transport	Connexion de bout en bout, connectabilité et contrôle de flux ; notion de port (TCP et UDP)
Couches matérielles	Paquet	3	Réseau	Détermine le parcours des données et l'adressage logique (adresse IP)
	Trame	2	Liaison	Adressage physique (adresse MAC)
	Bit	1	Physique	Transmission des signaux sous forme numérique ou analogique

FIGURE 1 – Modèle OSI (Wikipédia)

14.2 Protocol

Ensemble de **règles** qui régissent les **échanges de données** ou le comportement collectif de processus ou d'ordinateurs en réseaux ou d'objets connectés.

Exemple de protocole si on veut discuter avec quelqu'un :
- On l'appelle pour savoir s'il est attentif et prêt à discuter
- On attend sa réponse pour savoir si on peut commencer la discussion
- On parle, en se répondant mutuellement à chaque phrase
- En cas de non réponse à une phrase, on peut lui demander s'il est attentif
- On précise que l'on va devoir mettre fin à la discussion
- On lui dit au revoir en partant, pour mettre fin la discussion

14.3 Téléchargement ascendant/descendant

1. **Ascendant :** Envoi de données. (Upload)
2. **Descendant :** Réception de données. (Download)

14.4 Sender (Expéditeur)

Source de l'information. Celui qui envoie le message.

14.5 Destination

Celui qui reçoit le message et l'interprète.

14.6 Canal

Support qui assure le cheminement du message de la source à la destination.

14.7 Packet

Afin de transmettre un message d'une machine à une autre sur un réseau, celui-ci est **découpé** en plusieurs paquets transmis séparément.

Un paquet inclut un en-tête (en anglais, header), comprenant les informations nécessaires pour acheminer et reconstituer le message, et encapsule une partie des données. (Ex : Le paquet IP)

Le paquet ne doit pas être confondu avec la trame, correspondant à la couche liaison (couche 2 du modèle OSI). (Ex : la trame Ethernet)

14.8 Frame

Dans les réseaux informatiques, une *trame* est la **structure de base** d'un ensemble de données encadré par des bits de début *(drapeau)* et des bits de fin *(fanion)*.

Une trame est composée

- D'un **header** *(en-tête)*
- Des **données** que l'on veut transmettre
- D'un **trailer** *(postambule)*. Un paquet (dans le cas d'IP par exemple) ne peut transiter directement sur un réseau : il est **encapsulé** comme données à l'intérieur d'une *trame* qui elle-même finit en un **enchaînement de bits** qui circule sur le support physique

Il existe trois versions différentes (dont une qui a été abandonnée) :

1. ~~Ethernet Type I (créée par Xerox) abandonnée à l'heure actuelle~~
2. Ethernet Type II (propriétaire Intel, Digital, Xerox)
3. IEEE 802.3.

14.9 MAC (Media Access Control)

Une *adresse MAC*, parfois nommée **adresse physique**, est un **identifiant physique** et **unique au monde**, stocké dans une **carte réseau** ou une interface réseau similaire.

Toutes les cartes réseau ont une adresse MAC, même celles contenues dans les PC et autres appareils connectés. (Ex : Tablette tactile, smartphone, consoles de jeux, réfrigérateurs, montres ...)

Une **adresse MAC-48** est constituée de **48 bits** *(6 octets)* et est généralement représentée sous la forme **hexadécimale** en séparant les octets par un double point. (Ex : 5E :FF :56 :A2 :AF :15)

Ces 48 bits sont répartis de la façon suivante :

- **1 bit** I/G : indique si l'adresse est individuelle, auquel cas le bit sera à 0 (pour une machine unique, unicast) ou de groupe (multicast ou broadcast), en passant le bit à 1
- **1 bit** U/L : 0 indique si l'adresse est universelle (conforme au format de l'IEEE) ou locale, 1 pour une adresse administrée localement
- **22 bits** réservés : tous les bits sont à zéro pour une adresse locale, sinon ils contiennent l'adresse du constructeur
- **24 bits** : adresse unique (pour différencier les différentes cartes réseaux d'un même constructeur)

Les concepteurs d'Ethernet ayant utilisé un adressage de 48 bits, il existe potentiellement 2^{48} d'adresses MAC possibles *(environ 281 000 milliards)*. L'IEEE donne des préfixes de 24 bits (appelés Organizationally Unique Identifier - OUI) aux fabricants, ce qui offre 2^{24} d'adresses MAC disponibles par préfixe *(environ 16 millions)*.

14.10 Subnet mask

Le *masque de sous réseau* est le masque distinguant les **bits** d'une adresse IPv4 utilisés pour identifier le **sous-réseau** de ceux utilisés pour identifier l'hôte. L'adresse du **sous-réseau** est obtenue en appliquant l'**opérateur** `ET` binaire entre l'adresse IPv4 et le *masque de sous-réseau*. L'adresse de l'hôte à l'intérieur du sous-réseau est quant à elle obtenue en appliquant l'**opérateur** `ET` entre l'adresse IPv4 et le **complément à un** du masque.

Un masque de sous réseau ne pourra donc **jamais** être composé d'un `0` suivi d'un `1`. Uniquement une suite de `1` suivie d'une suite de `0`.

(~~`0.250.250.250`~~ n'est **pas** un masque de sous réseau valide, par contre `250.250.250.0` est valide)

Exemple :

Adresse IPv4	`192.168.1.2`	`192.168.1.2`	*Adresse IPv4*
&	*&*	*&*	*&*
Masque de sous réseau	`255.255.255.0`	`0.0.0.255`	*Complément à 1 du masque de sous réseau*
=	=	=	=
Adresse de sous réseau	`192.168.1.0`	`0.0.0.2`	*Adresse de l'hôte dans le sous réseau*

Soit en binaire :

`11000000.10101000.00000001.00000010`	`11000000.10101000.00000001.00000010`
&	&
`11111111.11111111.11111111.00000000`	`00000000.00000000.00000000.11111111`
=	=
`11000000.10101000.00000001.00000000`	`00000000.00000000.00000000.00000010`

14.11 Routing

Le *routage* est le **mécanisme** par lequel des **chemins** sont **sélectionnés** dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. Le *routage* est une tâche exécutée dans de nombreux réseaux, tels que le réseau téléphonique, les réseaux de données électroniques comme Internet, et les réseaux de transports. Sa performance est importante dans les réseaux décentralisés, c'est-à-dire où l'information n'est pas distribuée par une seule source, mais échangée entre des agents indépendants. C'est grâce à ça que par exemple les mails sont envoyés aux bons destinataires.

14.11.1 Unicast

Il n'existe qu'**une association** entre une adresse réseau et le **point d'arrivée final** : chaque adresse de destination identifie de manière unique **un seul receveur final**.

14.11.2 Anycast

Technique d'adressage et de routage permettant de rediriger les données vers le serveur informatique le « **plus proche** » ou le « **plus efficace** » selon la politique de routage.

14.11.3 Multicast

Forme de diffusion d'un émetteur (source unique) vers un **groupe de récepteurs**. Les termes *diffusion multipoint* ou *diffusion de groupe* sont également employés.

Les récepteurs intéressés par les messages adressés à ce groupe doivent s'inscrire à ce groupe. Ces abonnements permettent aux switchs et routeurs intermédiaires d'établir une route depuis le ou les émetteurs de ce groupe vers les récepteurs de ce groupe.

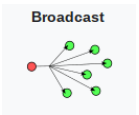
Avantages :

- Plus efficace que l'unicast pour diffuser des contenus simultanément vers une large audience. En streaming unicast, on enverrait l'information autant de fois qu'il y a de connexions, d'où gaspillage de temps, de ressources du serveur et surtout de bande passante. Au contraire, en multicast, chaque paquet n'est émis qu'une seule fois et sera routé vers toutes les machines du groupe de diffusion sans que le contenu ne soit dupliqué sur une quelconque ligne physique
- Le multicast permet de développer des applications interactives de groupe, comme la visioconférence, le partage de tableau…

Inconvénients :

- Ne permet pas le contrôle de la participation au groupe par la source : la source ne peut déterminer ni qui participe, ni qui peut participer ou non au groupe
- L'identification et l'authentification des participants doivent être prises en charge au niveau applicatif si elles sont souhaitées

14.11.4 Broadcast



Technique d'adressage et de routage permettant de rediriger les données vers **toutes** les machines connectées au réseau.

14.12 Firewall

Un pare-feu est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).

14.13 Gateway

Une *passerelle* est le nom générique d'un dispositif permettant de **relier** deux réseaux informatiques de types différents. (Ex : Un réseau local et le réseau Internet)

14.14 HUB

Un *concentrateur Ethernet* est un appareil informatique permettant de **concentrer** les transmissions Ethernet de plusieurs équipements sur un même support dans un réseau informatique local.

Ce dispositif est un **répéteur de données** ne permettant **pas de protection** particulière des données et transmettant les trames à toutes les machines connectées (par opposition au commutateur réseau qui dirige les données uniquement vers la machine destinataire). Ceci le rend **vulnérable aux attaques** par Analyseur de paquets. Il permet également d'étendre un réseau local mais ne permet pas de le transformer en un réseau étendu.

Le *HUB* possède deux types de ports :

— Les ports pour la connexion des machines
— Le port pour extension du réseau auquel se connecte un autre concentrateur (il n'y en a généralement qu'un seul par concentrateur). Ce type de port est identique au précédent à l'exception du câblage qui est inversé (on peut aussi utiliser un câble à connecteur RJ45 croisé pour y connecter un ordinateur supplémentaire).

14.15 Switch

Un *commutateur réseau* est un équipement qui **relie** plusieurs segments (câbles ou fibres) dans un **réseau** informatique et de télécommunication et qui permet de créer des **circuits virtuels**.

La *commutation* est un des deux modes de transport de trame au sein des réseaux informatiques et de communication, l'autre étant le **routage**. Dans les réseaux locaux, il s'agit le plus souvent d'un boîtier disposant de plusieurs ports RJ45 (entre 4 et plusieurs centaines), il a donc la même apparence qu'un concentrateur.

Contrairement à un concentrateur, un *commutateur* ne reproduit pas sur tous les ports chaque trame qu'il reçoit : il sait **déterminer sur quel port** il doit envoyer une trame, en fonction de l'**adresse de destination** de cette **trame**. Les commutateurs sont souvent utilisés pour remplacer des concentrateurs car **ils encombrent moins le réseau**.

> **Fonctionnement :**
> Le *commutateur* établit et met à jour une **table**, dans le cas du *commutateur* pour un réseau Ethernet il s'agit de la **table d'adresses MAC**, qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC source des trames reçues sur chaque port. Le commutateur **construit** donc dynamiquement une **table** qui associe numéro de port et adresses MAC.

14.16 DDoS (Distributed Denial of Service attack)

Une *attaque par déni de service* (DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de **plusieurs sources**, on parle alors d'**attaque par déni de service distribuée (DDoS)**.

Il peut s'agir de :

— L'inondation d'un réseau afin d'empêcher son fonctionnement
— La perturbation des connexions entre deux machines, empêchant l'accès à un service particulier
— L'obstruction d'accès à un service pour une personne en particulier
— Le fait d'envoyer des milliards d'octets à une box internet

L'*attaque par déni de service* peut ainsi **bloquer un serveur** de fichiers, rendre impossible l'accès à un serveur web ou empêcher la distribution de courriel dans une entreprise.

14.17 VPN (Virtual Private Network)

Le *réseau privé virtuel* est un système permettant de créer un **lien direct** entre des ordinateurs distants, qui **isole** leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

1. Un VPN permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local. Il permet d'avoir un **accès au réseau interne** (réseau d'entreprise, par exemple) ou de créer un **réseau de pairs**.
2. Un VPN dispose généralement aussi d'une passerelle permettant d'accéder à l'extérieur, ce qui permet de **changer l'adresse IP source** apparente de ses connexions. Cela rend plus difficile l'identification et la localisation approximative de l'ordinateur émetteur par le fournisseur de service. Cela permet aussi de contourner les restrictions géographiques de certains services proposés sur Internet. L'utilisation des VPN n'est généralement pas légalement restreinte (sauf en Chine).
   Cependant, l'infrastructure de VPN (généralement un serveur) dispose des informations permettant d'identifier l'utilisateur. (Ex : Les sociétés proposant des VPN gratuits ou payants peuvent récolter les données de navigation de leurs clients, ce qui relativise l'anonymat de ces services)
3. Le VPN permet également de construire des **réseaux overlay**, en construisant un **réseau logique** sur un **réseau sous-jacent**, faisant ainsi abstraction de la topologie de ce dernier.