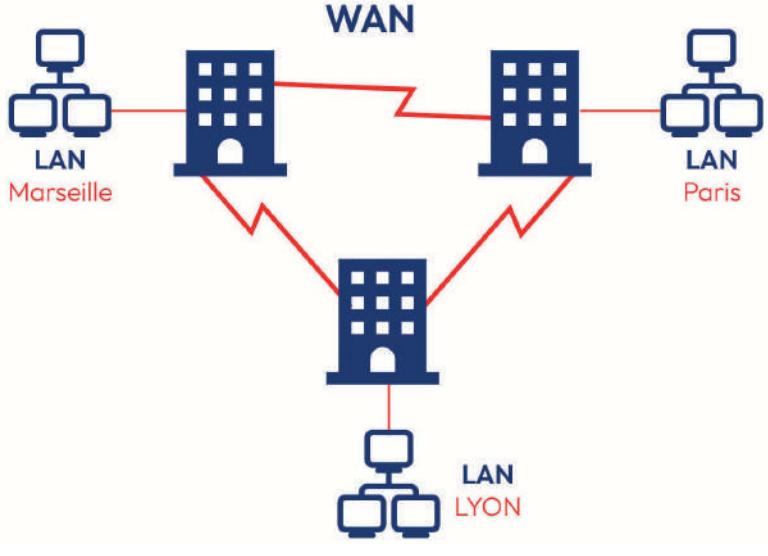
19

LES CONCEPTS DU WAN

19.1. Objectifs du WAN :

19.1.1. Introduction :

Le réseau étendu **WAN** (**W**ide **A**rea **N**etwork) est un réseau qui permet d'interconnecter des réseaux locaux distants.

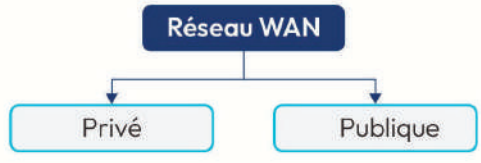


19.1.2. Comparaison entre un LAN et un WAN :

RÉSEAU LOCAL (LAN)	RÉSEAU ÉTENDU (WAN)
Le LAN offre les services réseau dans une petite zone géographique	Le WAN offre les services réseau dans de vastes zones géographiques
Le LAN est utilisé pour interconnecter les périphériques finaux (Ordinateurs, etc.)	Le WAN est utilisé pour interconnecter des utilisateurs distants, des réseaux et des sites.
Le LAN est géré par une seule entité	Le WAN est géré par le fournisseur des services WAN (Fournisseurs Internet, etc.)
Le client utilise le LAN gratuitement	Le client doit payer les services WAN
Le débit d'un LAN est très élevé	Le fournisseur WAN offre des débits faibles à élevés.

19.1.3. Types de WAN :

- Un réseau WAN privé est dédié à une organisation généralement pour interconnecter ses sites distants (Lignes louées, MPLS, Métro-Ethernet, etc.)
- Un réseau WAN public est disponible au grand public (Internet)

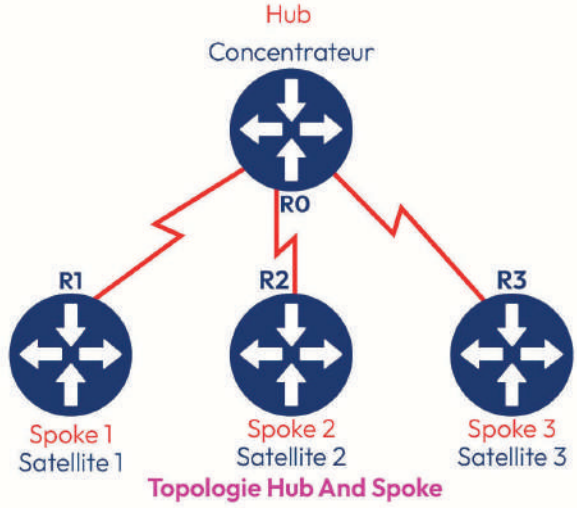


19.1.4. Topologies WAN :

TOPOLOGIE HUB AND SPOKE (EN ÉTOILE) :

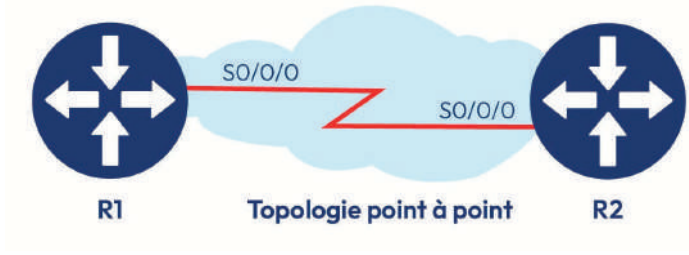
Une topologie Hub and Spoke (en étoile) est composée de deux types de routeurs :

- Un **concentrateur** (Hub) : Il permet d'interconnecter tous les sites de l'organisation.
- Des sites **satellites** (Spokes) : Ils peuvent communiquer en passant par le concentrateur.

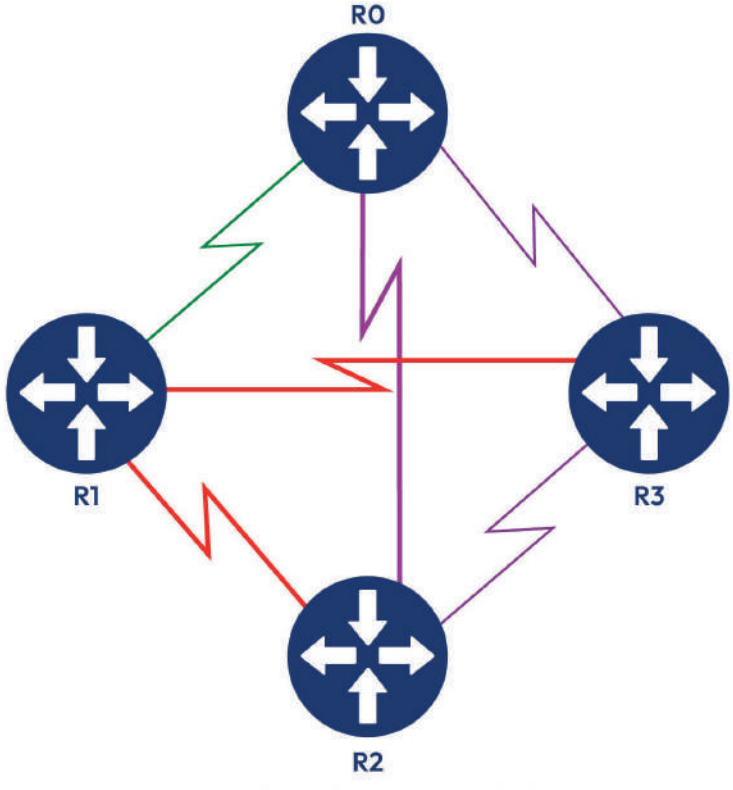


TOPOLOGIE POINT À POINT :

Dans une topologie point à point, les deux sites distants communiquent directement.



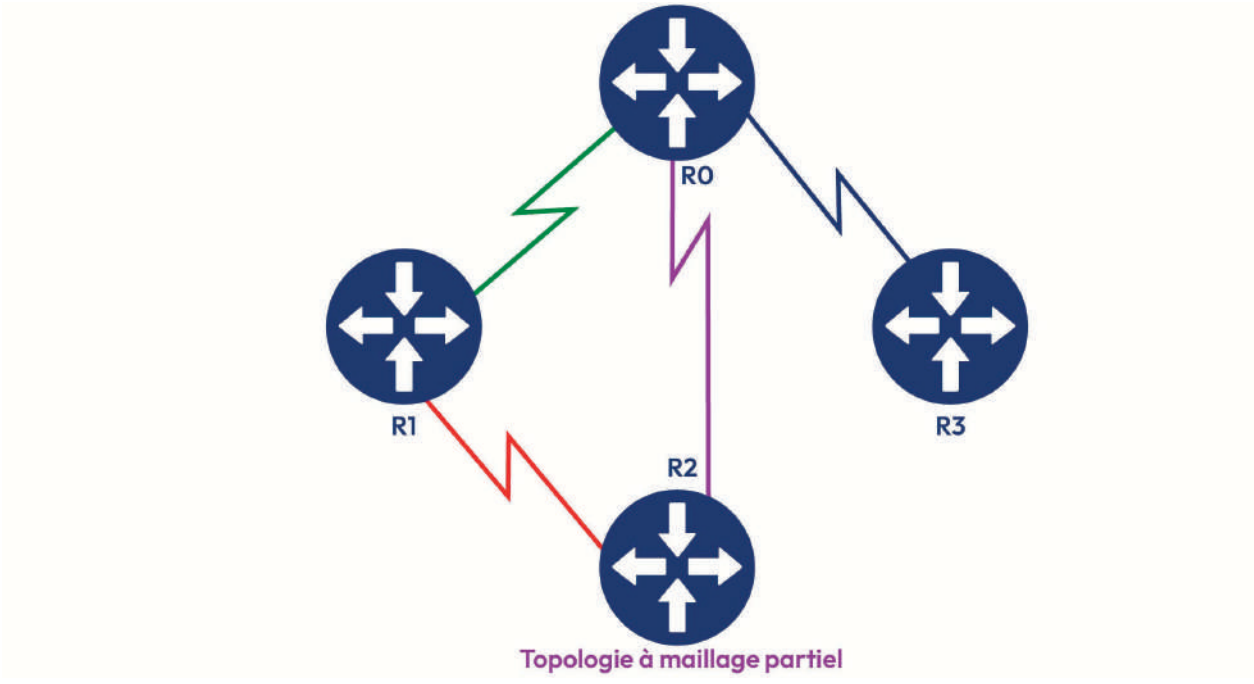
TOPOLOGIE À MAILLAGE GLOBAL :



Topologie à maillage global

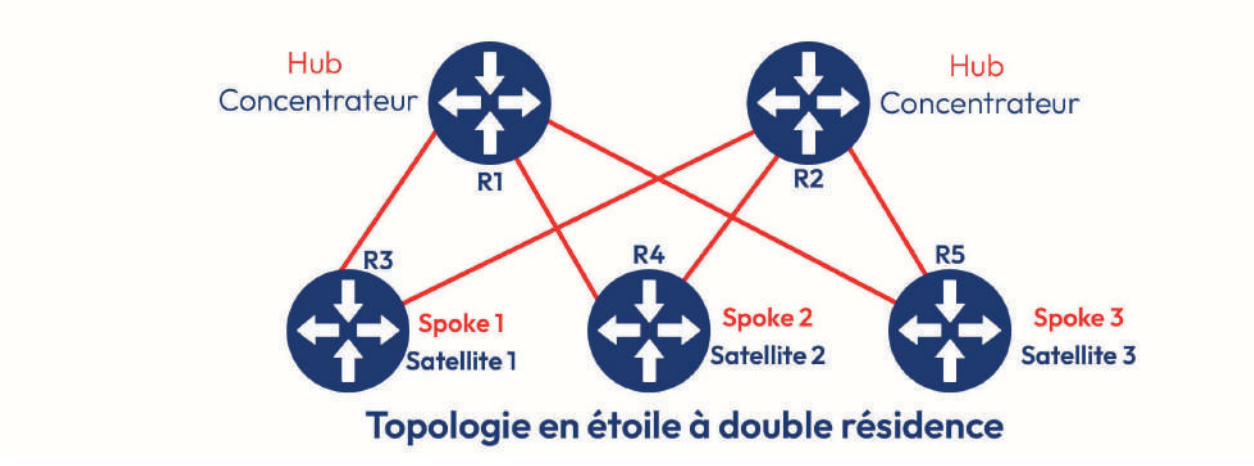
Dans une topologie à maillage global, chaque site est connecté à tous les autres.

TOPOLOGIE À MAILLAGE PARTIEL :



Dans une topologie à maillage partiel, il existe au moins deux sites qui ne sont pas interconnectés directement.

TOPOLOGIE À DOUBLE RÉSIDENCE :



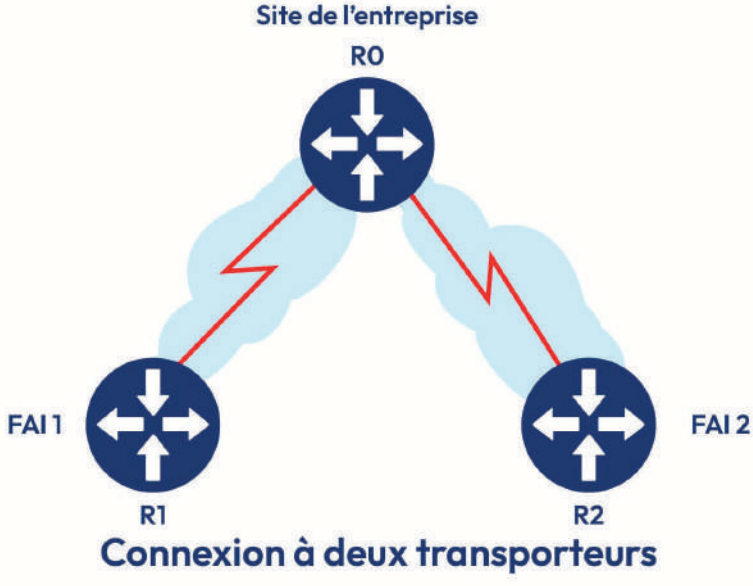
Une topologie à double résidence est une topologie qui offre une certaine redondance en utilisant deux concentrateurs.

19.1.5. Connexions de transporteurs :

CONNEXION À UN TRANSPORTEUR UNIQUE :

FAI : **F**ournisseur d'**a**ccès **I**nternet

CONNEXION À TRANSPORTEURS MULTIPLES :



19.2. Fonctionnement du WAN :

19.2.1. Normes WAN :

Les organisations qui gèrent les normes WAN sont :

- **TIA/EIA** : Association de l'industrie des télécommunications et Alliance des industries électroniques
- **ISO** : Organisation internationale de normalisation
- **IEEE** : Institut des ingénieurs en électricité et en électronique

19.2.2. WAN et le modèle OSI :

WAN (**W**ide **A**rea **N**etwork) est un terme utilisé pour décrire un réseau qui couvre une zone géographique étendue comme une ville, un pays ou même le monde.

Il permet de connecter des réseaux locaux (LAN) entre eux, en utilisant des technologies de communication telles que les lignes louées, les liaisons de satellite, les liaisons de câble et les connexions internet.

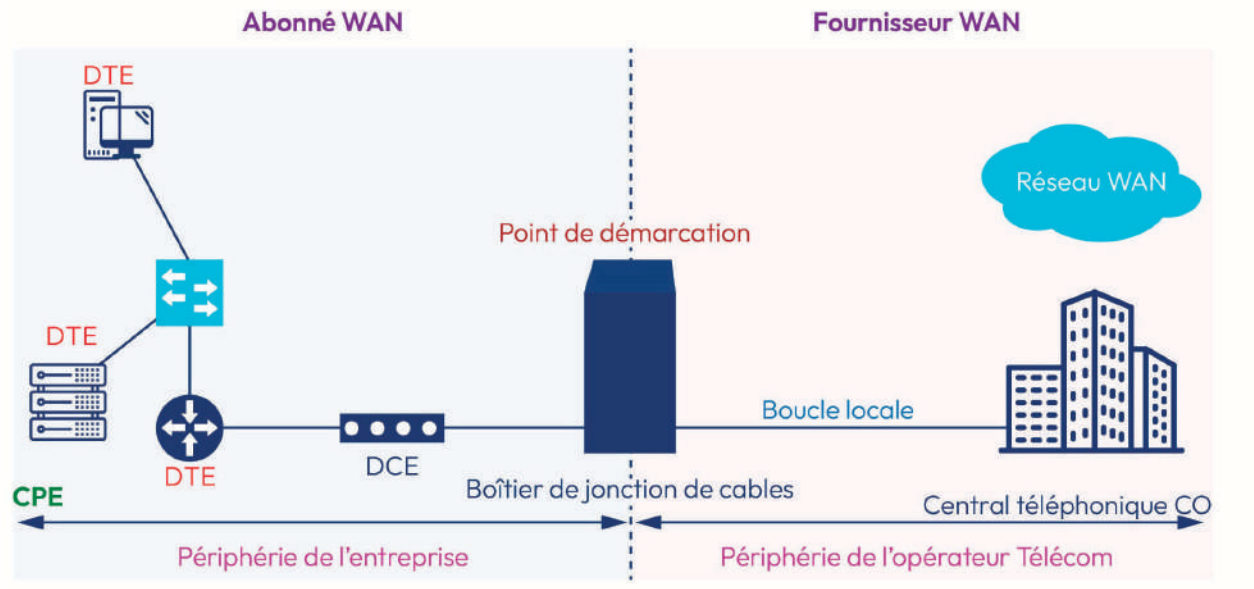
Quelques normes de la couche 1 :

- SDH (**S**ynchronous **D**igital **H**ierarchy)
- SONET (**S**ynchronous **O**ptical **Net**work)
- DWDM (**D**ense **W**avelength-**D**ivision **M**ultiplexing)

Quelques normes de la couche 2 :

- DSL (**D**igital **S**ubscriber **L**ine)
- WiMax (**W**orldwide **I**nteroperability for **M**icrowave **A**ccess)
- WAN Ethernet (Metro Ethernet)
- MPLS (**M**ulti **P**rotocol **L**abel **S**witching)
- PPP (**P**oint-to-**P**oint **P**rotocol)
- HDLC (**H**igh **L**evel Data **L**ink **C**ontrol)
- Frame Relay
- ATM (**A**synchronous **T**ransfer **M**ode)

19.2.3. Terminologie du WAN :

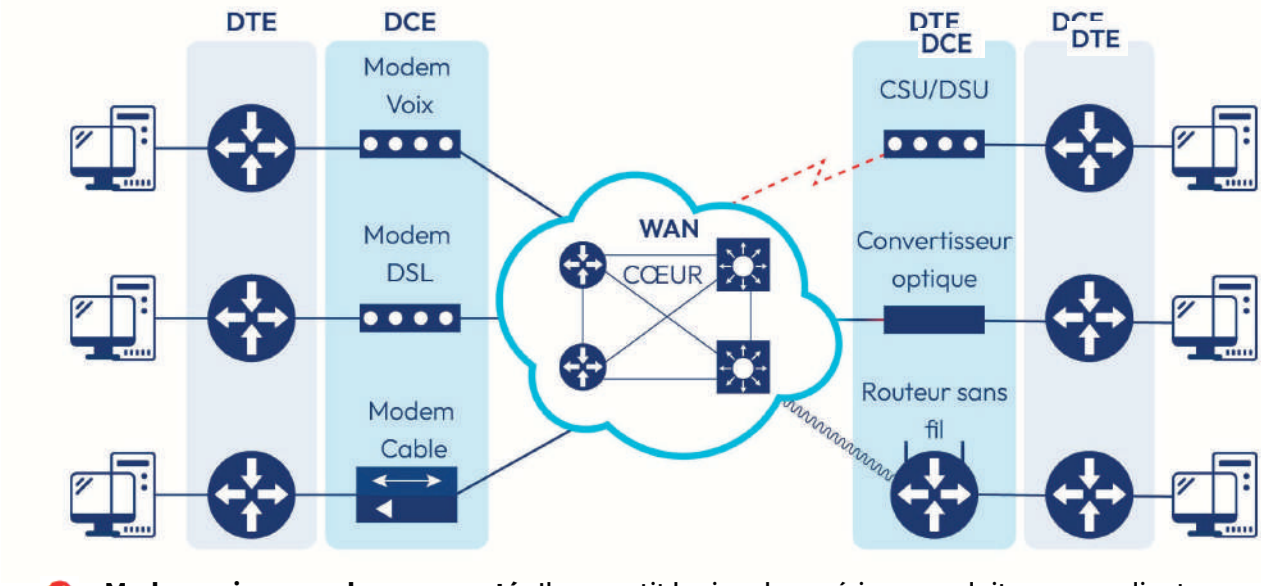


- Équipement terminal de données (**DTE**) : Il relie le LAN au dispositif du LAN (Routeur, Ordinateur, Serveur, etc.).
- Équipement communication de données (**DCE**) : C'est l'interface avec le réseau WAN du fournisseur.
- Point de démarcation : C'est le lieu où la responsabilité de l'exploitation du réseau passe de l'abonné au fournisseur de services WAN.
- **CPE** (**C**ustomer **P**remises **E**quipment) : Tout équipement installé dans les locaux de l'abonné.
- Central téléphonique **CO** : L'installation du fournisseur WAN qui connecte le CPE au réseau WAN.
- Boucle locale : C'est le câble qui relie le **CPE** au **CO**.
- Réseau à péage : Réseau du fournisseur WAN.

WAN (**W**ide **A**rea **N**etwork) est un terme utilisé pour décrire un réseau qui couvre une zone géographique étendue, comme une ville, un pays ou même le monde.

Il permet de connecter des réseaux locaux (LAN) entre eux, en utilisant des technologies de communication telles que les lignes louées, les liaisons de satellite, les liaisons de câble et les connexions internet.

19.2.4. Équipements du WAN :



- **Modem voix** ou **modem commuté** : Il convertit le signal numérique produit par un ordinateur en fréquences vocales.
- **Modem DSL** : Il se connecte au WAN à l'aide des lignes téléphoniques.
- **Modem câble** : Il se connecte au WAN à l'aide des lignes coaxiales.
- **Unité CSU/DSU** : Elle est utilisée avec les lignes louées pour convertir les trames LAN en LAN et vice versa.
- **Convertisseur optique** : Il est utilisé pour convertir les signaux optiques en signaux électriques et vice versa.

DTE (**D**ata **T**erminal **E**quipment) et DCE (**D**ata **C**ommunication **E**quipment) sont des termes utilisés pour décrire les différents types d'équipements utilisés dans une connexion de communication de données.

- **Un équipement DTE** est généralement un ordinateur ou un terminal qui génère ou bien utilise des données. En effet, il peut être connecté à un réseau ou à un autre équipement pour envoyer ou recevoir des données.
- **Un équipement DCE,** quant à lui, est généralement utilisé pour connecter des équipements DTE entre eux, en utilisant des technologies de communication telles que les lignes louées, les liaisons de satellite, les liaisons de câble et les connexions internet. Il peut également fournir des services tels que la conversion de protocoles et la modulation de signal. Les équipements DCE incluent généralement des modems, des routeurs et des commutateurs.

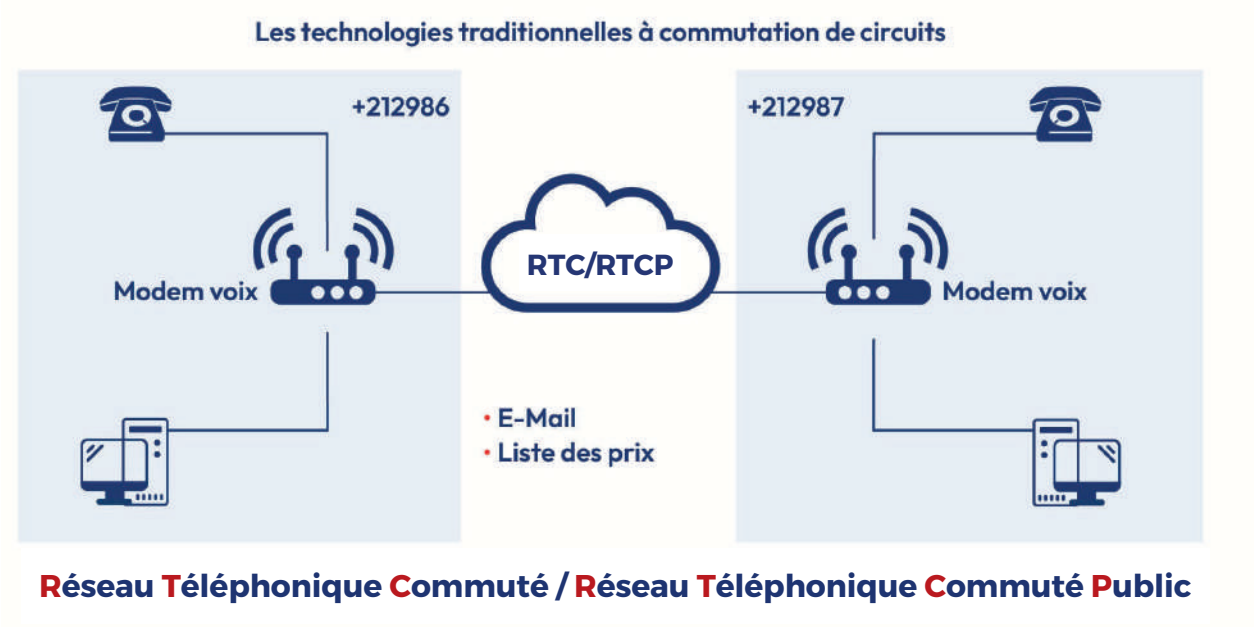
En résumé, un équipement DTE est un équipement qui génère ou utilise des données, et **un équipement DCE** est un équipement qui connecte les équipements DTE entre eux et fournit des services de communication de données.

19.3. Les technologies du WAN :

19.3.1. Les technologies traditionnelles :

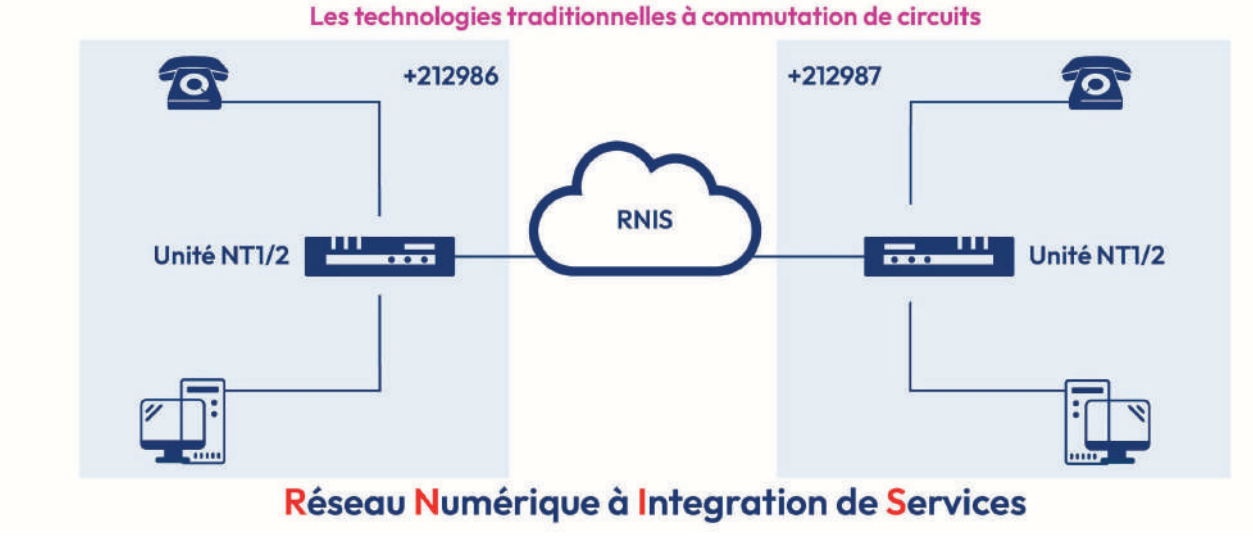
À COMMUTATION DE CIRCUITS :

RTC (PSTN en anglais) :



- L'équipement DCE est un modem commuté asynchrone.
- L'abonnée peut utiliser une seule communication par modem.
- Le débit est très faible : inférieur à 56 kbps.
- Le temps d'établissement d'une connexion est élevé.
- Le coût de la communication est élevé.
- La configuration est compliquée.
- Il est utilisé pour l'envoi des e-Mails, des listes des prix, etc.

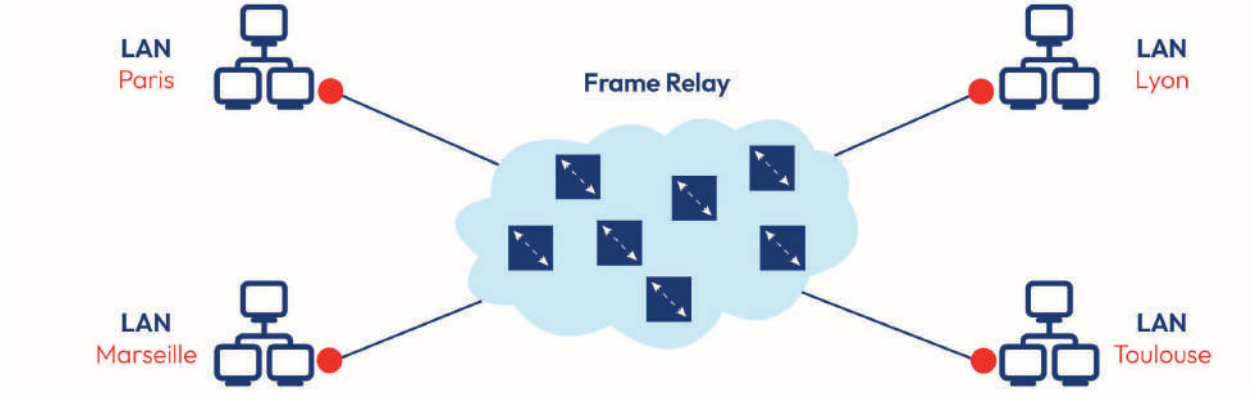
RNIS (ISDN en anglais) :



- L'équipement DCE est l'unité NT1/2.
- L'abonné peut effectuer plusieurs communications simultanément.
- Le débit est à partir de 45 kbps jusqu'à 2 Mb/s.
- Le coût d'une communication est établi en fonction du temps.

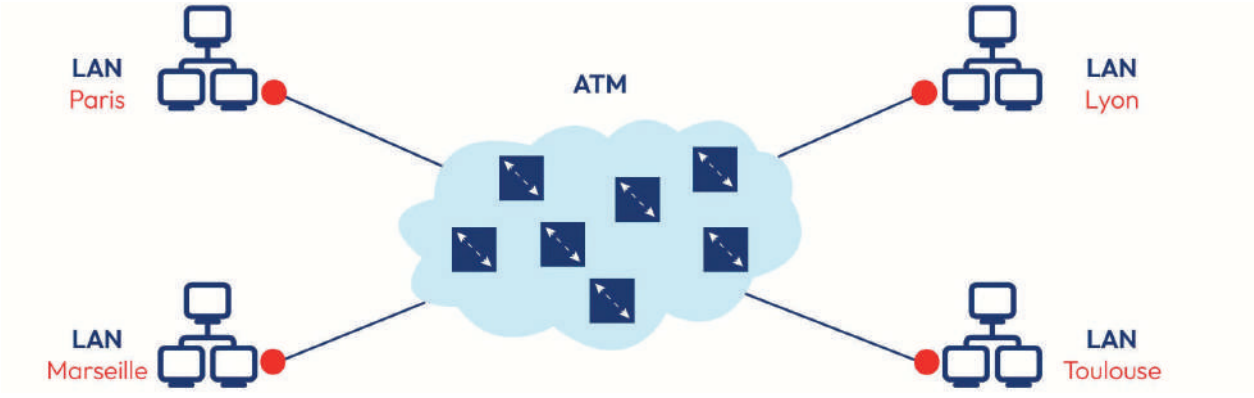
À COMMUTATION DE PAQUETS :

Relais de trames (Frame Relay) :



- Frame Relay est une technologie WAN à accès multiple sans diffusion (NBMA).
- Frame Relay peut interconnecter plusieurs LAN avec une seule interface physique.
- Frame Relay crée des circuits virtuels identifiés par des DLCI.

ATM :



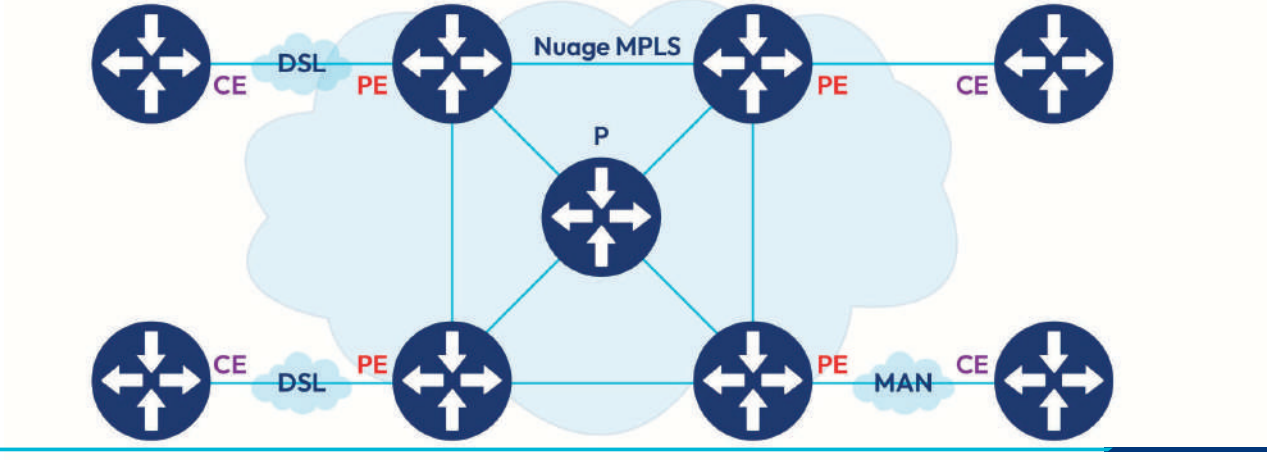
- ATM (**A**synchronous **T**ransfer **M**ode) est plus optimisée pour le transfert de la voix et de la vidéo.
- ATM utilise une architecture basée sur des cellules.
- La taille d'une cellule est toujours de 53 octets.
- Une ligne ATM type nécessite un débit supérieur de presque 20 % à celui Frame Relay.
- Les réseaux ATM ont été remplacés par des solutions Metro Ethernet et Internet.

19.3.2. Les technologies modernes :

À COMMUTATION DE PAQUETS :

MPLS :

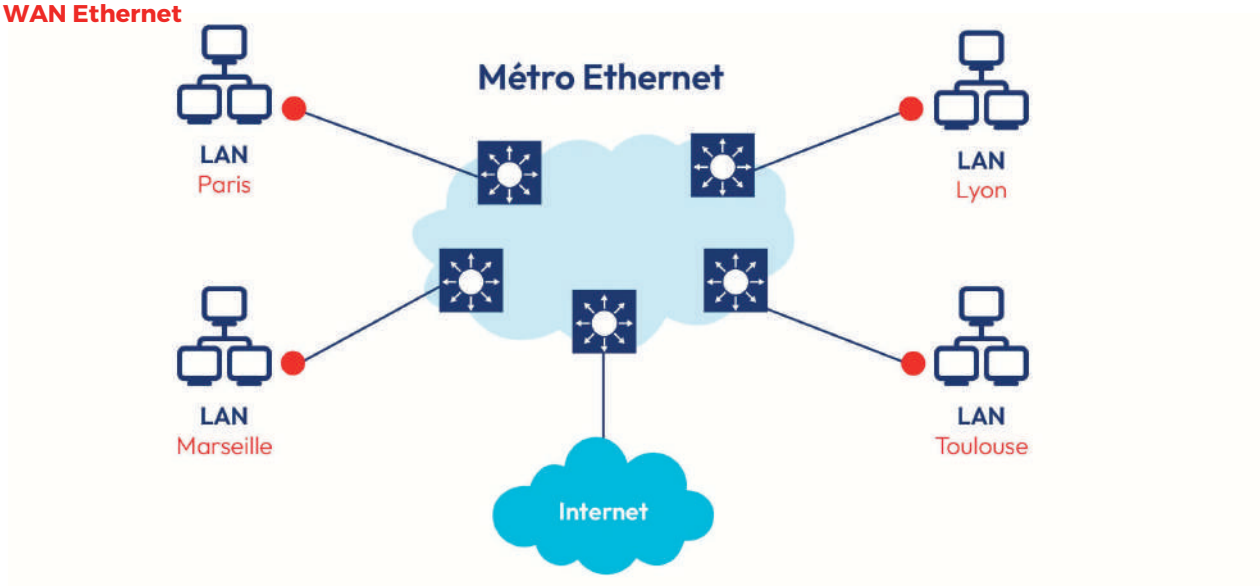
MPLS (**M**ulti**p**rotocol **L**abel **S**witching) est un protocole de commutation de données qui permet de créer des réseaux privés virtuels (VPN) sur des réseaux publics.
Il utilise des étiquettes pour identifier les paquets de données et les acheminer de manière efficace sur le réseau, ce qui permet de gérer la qualité de service (QoS) pour les différents types de trafic et de créer des réseaux privés virtuels (VPN) sur des réseaux publics.



- Un routeur MPLS peut être un routeur Edge client (CE), un routeur Edge fournisseur (PE) ou un routeur fournisseur interne (P).
- MPLS attache des étiquettes à des paquets pour transférer le trafic.
- MPLS fournit des services pour la prise en charge de la QoS, l'ingénierie du trafic, la redondance et les VPN.

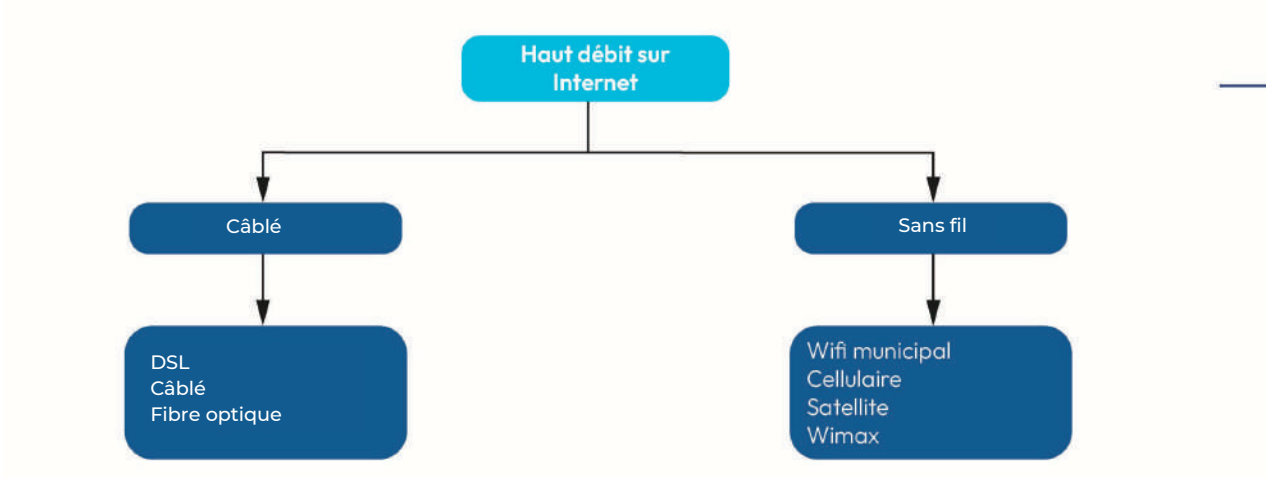
Un routeur CE (**C**ustomer **E**dge) est un routeur qui est connecté à un client et qui fait la transition entre le réseau du client et le réseau MPLS, tandis qu'un routeur PE (**P**rovider **E**dge) est un routeur qui est situé à la bordure du réseau MPLS du fournisseur de services et qui est utilisé pour connecter les réseaux locaux des clients au réseau MPLS.

WAN Ethernet

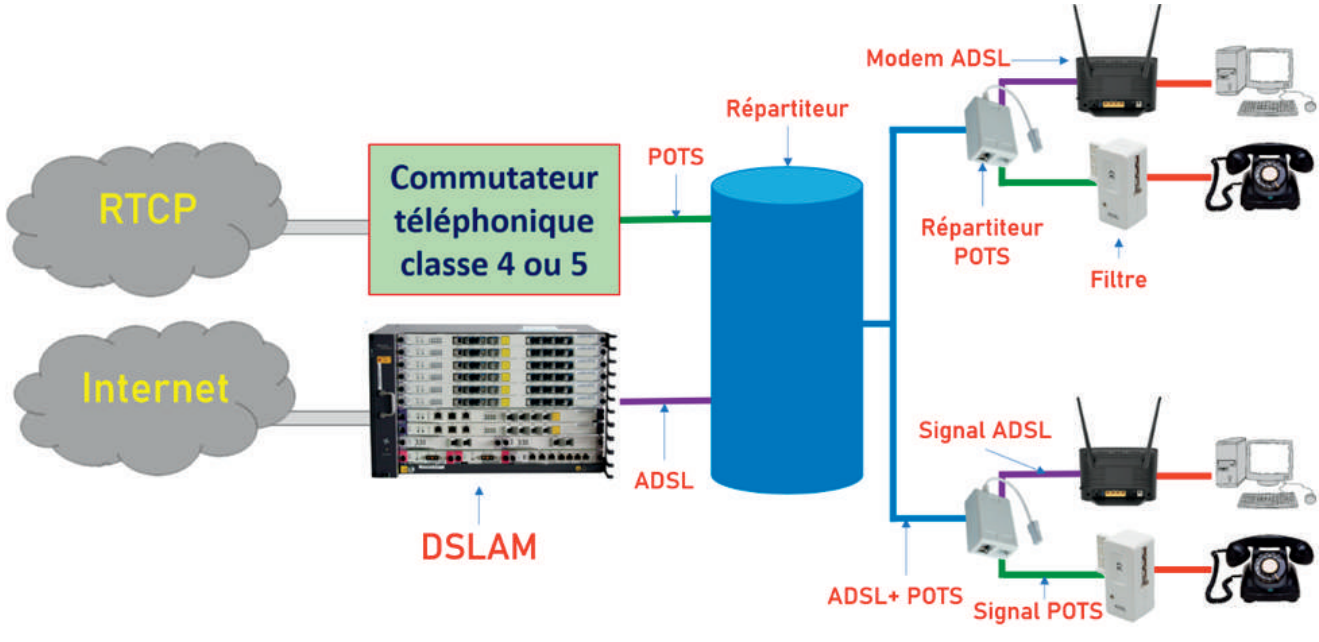


- Avec les nouveaux standards d'Ethernet relatifs à la fibre optique, il est possible de l'utiliser avec le WAN :
  - Les standards IEEE 1000BASE-LX : Les longueurs de câble jusqu'à 5 km.
  - Les standards IEEE 1000BASE-ZX : Les longueurs de câble jusqu'à 70 km.
- WAN par Ethernet peut prendre de nombreux noms :
  - Ethernet métropolitain (MetroE)
  - EoMPLS (Ethernet over MPLS)
  - Service LAN privé virtuel (VPLS)
- WAN Ethernet présente de nombreux avantages :
  - Réduction des dépenses et de l'administration
  - Intégration facile aux réseaux existants
  - Productivité accrue des entreprises

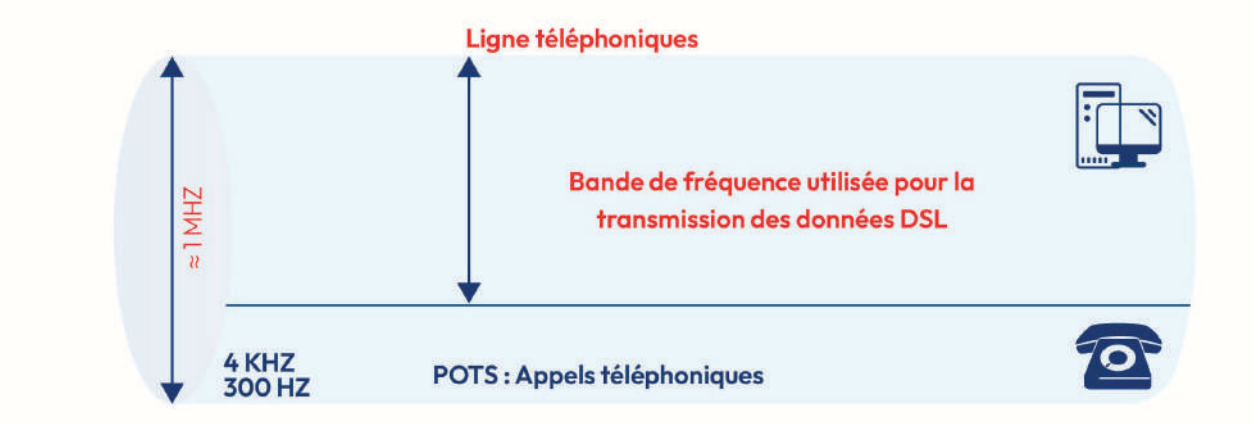
HAUT DÉBIT SUR INTERNET :



DSL :

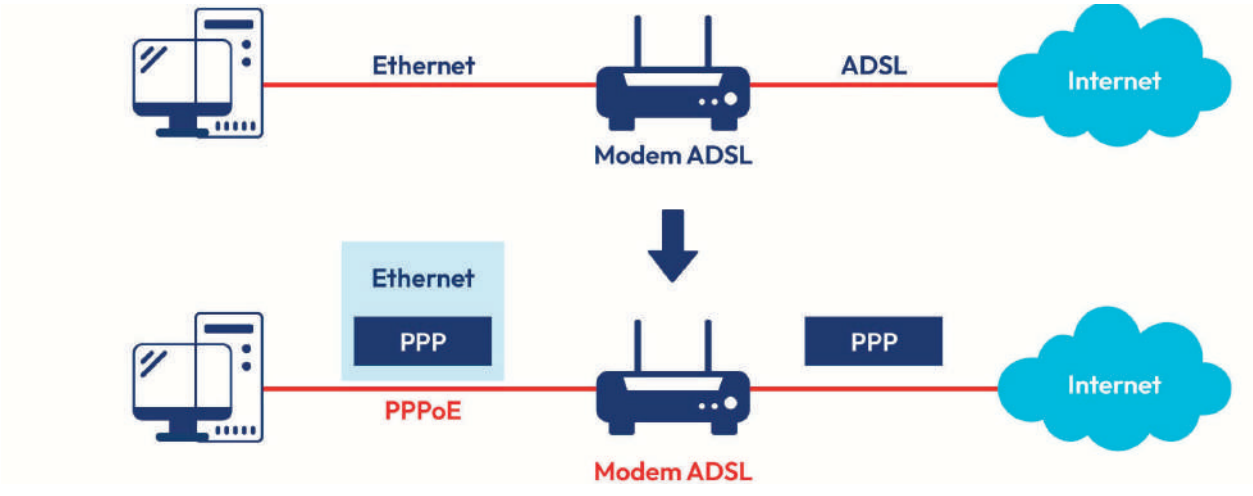


➲ Les lignes téléphoniques sont utilisées pour transmettre, en plus de la voix, les données Internet.



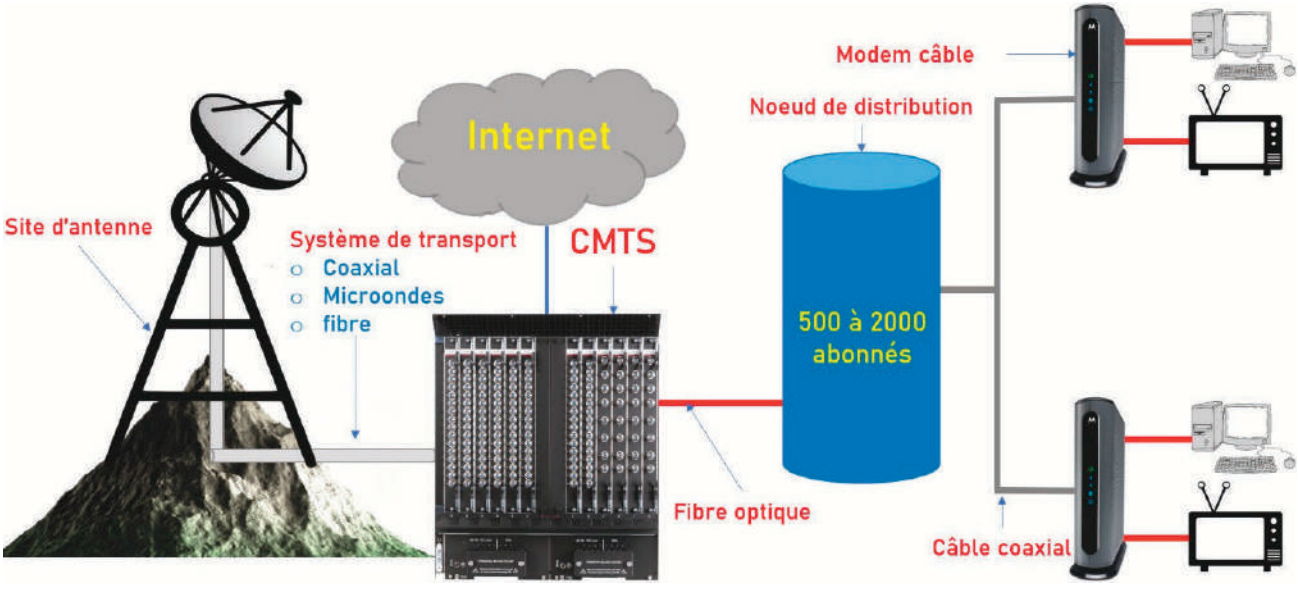
- Le modem DSL convertit les signaux Ethernet en un signal DSL.
- Le DSLAM est un multiplexeur DSL situé au central téléphonique CO pour concentrer les connexions de plusieurs abonnés.
- Chaque abonné a sa propre bande passante.

Le DSL et PPP :

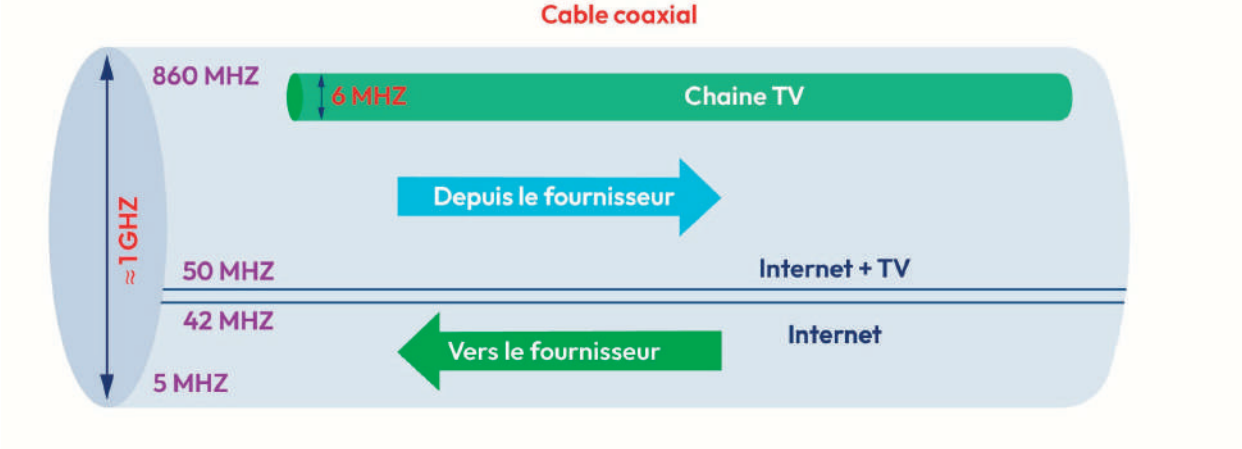


- Les clients apprécient Ethernet :
  - Simplicité
  - Disponibilité
- PPP est apprécié par le FAI:
  - Authentification
  - Gestion de comptes
  - Administration de la liaison

Câble :



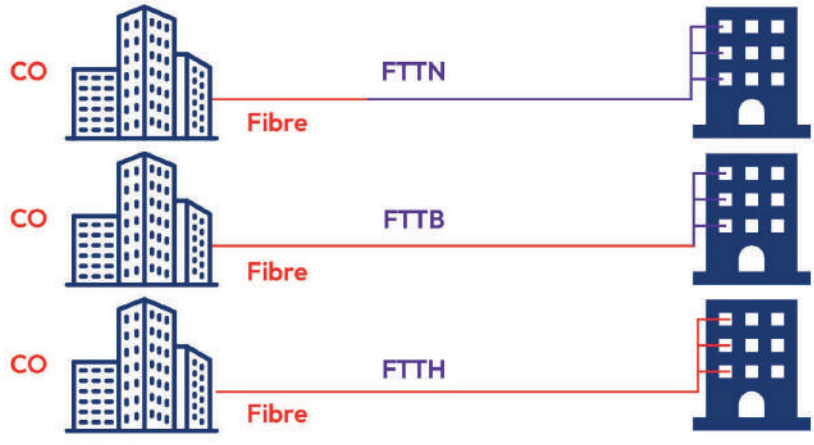
- L'internet par câble utilise les câbles coaxiaux pour le transfert des données Internet.



- Le modem câble permet de recevoir des données haut débit sur un câble coaxial.
- Le nœud de distribution optique permet de convertir les signaux RF en signaux optiques, et vice versa.
- Le CMTS permet d'échanger des signaux avec les modems câble des abonnés.
- La bande passante est partagée entre tous les abonnés.

Fibre optique :

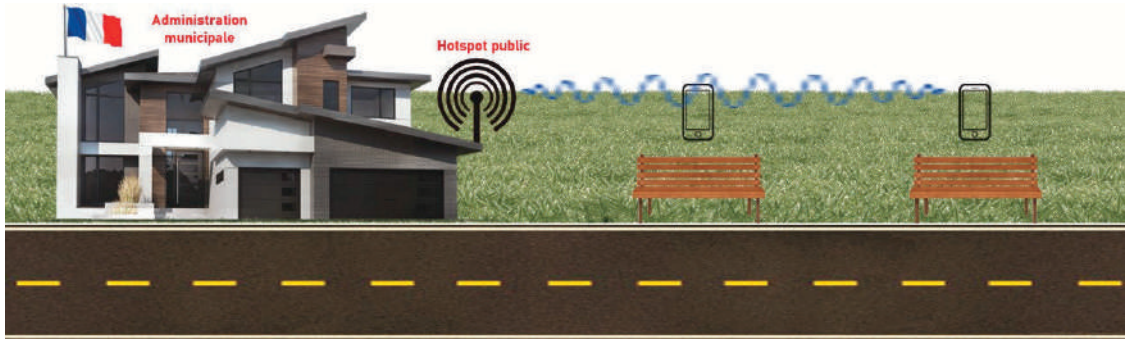
Il existe plusieurs normes :



- **FTTH** (**F**ibre **T**o **T**he **H**ome) : Fibre atteint la limite de la résidence.
- **FTTB** (**F**iber **T**o **T**he **B**uilding) : La fibre atteint la limite du bâtiment.
- **FTTN** (**F**ibre **T**o **T**he **N**ode/**N**eighborhood) : Le câblage optique atteint un nœud optique.

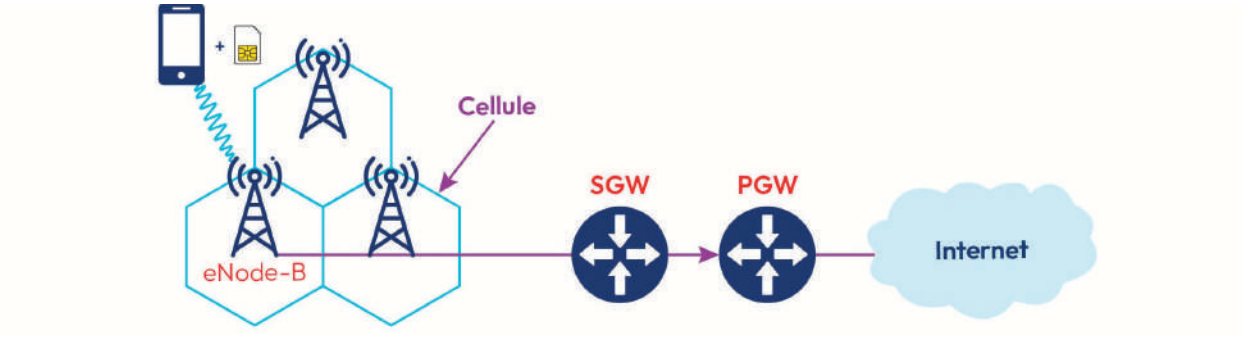
> FTTx peut fournir la bande passante la plus élevée de toutes les options haut débit.

Wifi municipal :



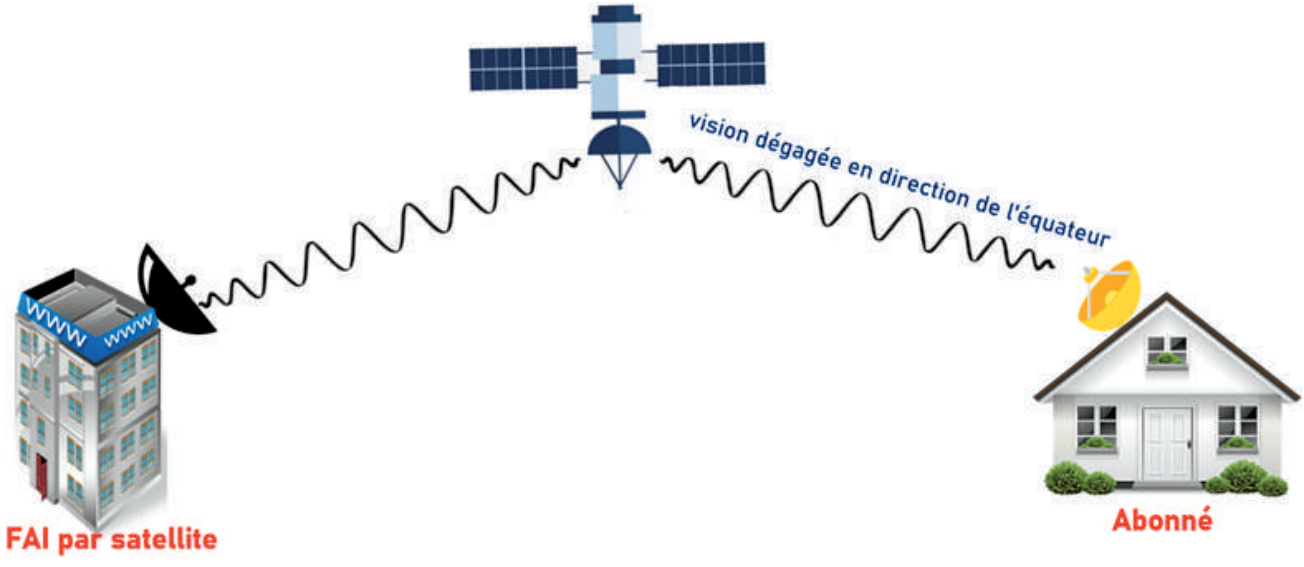
- Le Wifi municipal est destiné à l'usage des services de police, de pompier ou des employés municipaux.
- Le Wifi municipal utilise une topologie maillée.

Cellulaire :



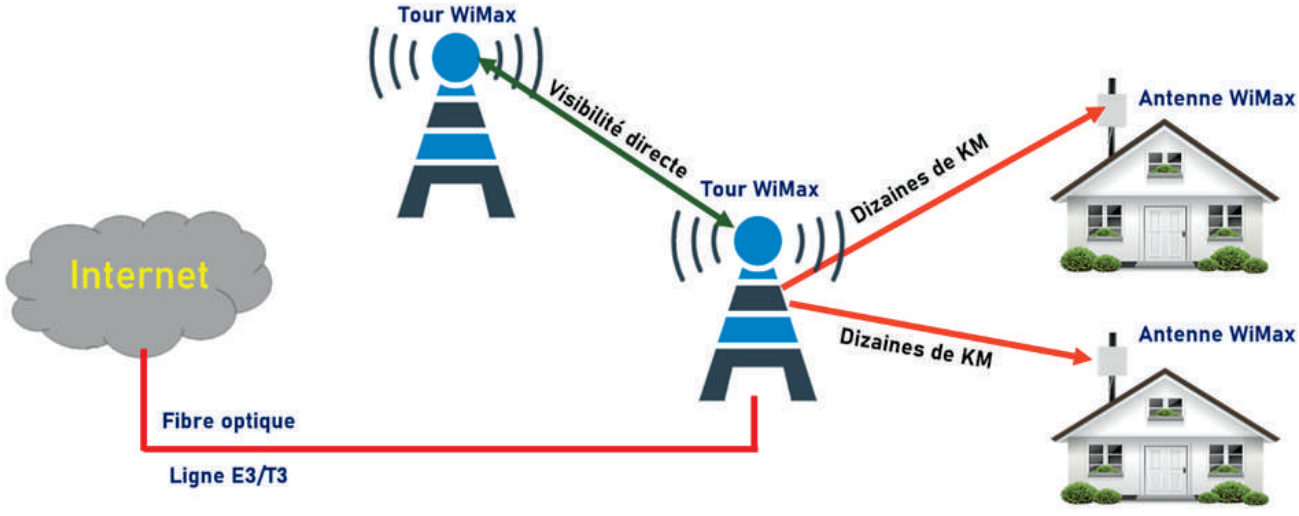
- Le réseau cellulaire est utilisé pour connecter au réseau Internet des téléphones mobiles ou tablettes munis de carte SIM.
- Il existe plusieurs normes cellulaires : 3G (UTMS), 4G (LTE) et 5G.

Internet par satellite :



- La technologie Internet satellite bidirectionnelle utilise la multidiffusion IP
- La technologie Satellite peut desservir simultanément jusqu'à 5.000 canaux de communication
- Vitesse d'UPLOAD= 1/10 de la vitesse de DOWNLOAD = 500 kbps

WiMax :



WiMax est encadrée par la norme IEEE 802.16

WiMax utilise une topologie point à multipoint

WiMax offre un débit allant jusqu'à 1 Gb/s

La zone de couverture d'une tour WiMax = 7500 km2

Le WiMax est largement remplacé par LTE, le câble ou le DSL.

19.3.3. Comparaison des technologies WAN :

Internet par Câble	Bande passante partagée
DSL	Bande passante limitée et sensible à la distance
Fiber to the Home	Installation nécessaire de la fibre à la maison
Cellulaire/mobile	La couverture présente souvent un problème et la bande passante n'est pas stable.
Wi-Fi municipal	La plupart des municipalités ne disposent pas d'un réseau Wi-Fi maillé.
Satellite	Technologie coûteuse et offre une capacité limitée par abonné. Généralement utilisé lorsqu'aucune autre option n'est disponible.

19.4. La technologie VPN :

19.4.1. Introduction aux réseaux privés virtuels :

LA SOLUTION WAN PUBLIQUE : INTERNET

- Solution à faible coût : on ne paie que la connexion Internet.
- Solution sécurisée.
- Solution évolutive.
- Solution compatible avec tous les équipements réseau et les technologies haut débit.
- L'inconvénient d'Internet, c'est que c'est une solution publique (moins sécurisée).

LES RÉSEAUX LOCAUX VIRTUELS VPN :

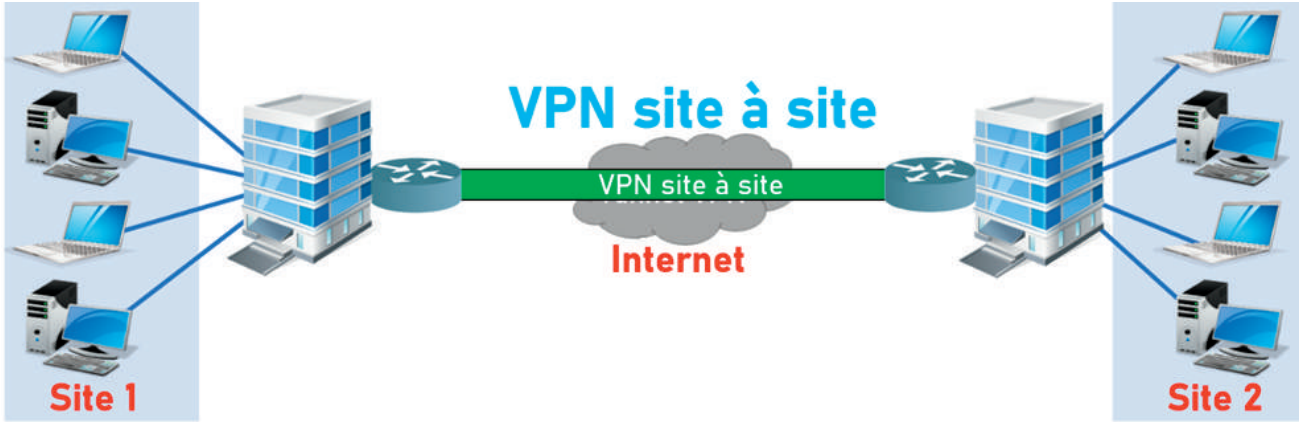
- Solution à faible coût : Elle est basée sur Internet.
- Solution évolutive : Elle est basée sur Internet.
- Solution compatible avec tous les équipements réseau et les technologies haut débit.
- Solution sécurisée : Elle offre des services de sécurité tels que la confidentialité et l'intégrité.

19.4.2. VPN site à site et VPN d'accès distant :

Il existe deux types de connectivité VPN :

- VPN site à site.
- VPN « Accès à distance ».

VPN SITE À SITE :



- Le VPN site à site est utilisé pour connecter d'une manière sécurisée deux sites d'une entreprise via Internet.
- Exemples : VPN IPSEC, GRE sur IPSEC, DMVPN, VTI (VPN de tunnel virtuel IPSEC)

VPN D'ACCÈS DISTANT :

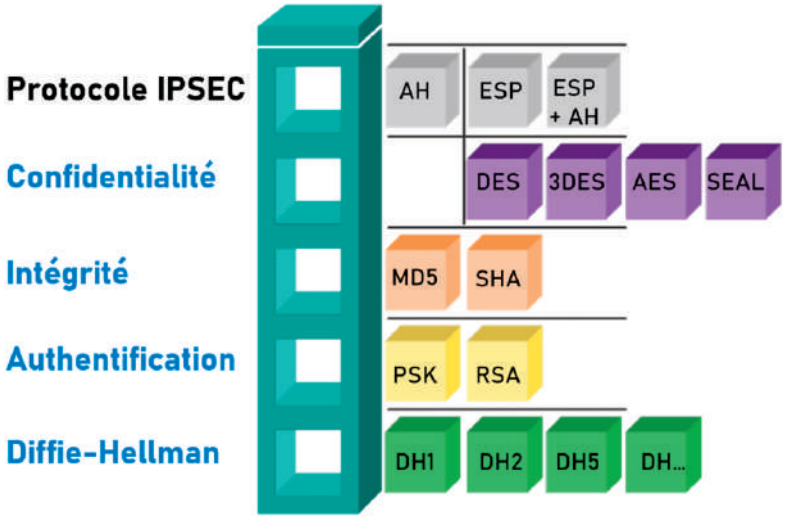
- Le VPN « Accès à distance » est utilisé pour connecter d'une manière sécurisée un hôte individuel au réseau de l'entreprise en utilisant une connexion Internet.
- Exemples : VPN IPSEC et VPN SSL

19.4.3. VPN IPSEC :

LES SERVICES DE SÉCURITÉ IPSEC :

VPN IPSEC est un cadre de normes ouvertes qui est indépendant des algorithmes existants pour mettre en œuvre des communications sécurisées.
IPSEC permet d'assurer la **confidentialité**, l'**intégrité**, l'**authentification** et l'**échange des clés DH**.

Les clés DH (Diffie-Hellman, en référence aux noms de ses inventeurs Whitfield Diffie et Martin Hellman) sont utilisées dans le cadre de la sécurité de l'information pour échanger des clés de chiffrement de manière sécurisée entre deux parties.
En effet, elles permettent aux parties de s'échanger une clé secrète sans qu'elle ne soit interceptée par un tiers, ce qui rend le chiffrement de leur communication plus sécurisé.



La confidentialité :

IPSEC utilise des algorithmes de chiffrement symétriques DES, 3DES, AES ou SEAL pour assurer la confidentialité des données.

ALGORITHME DE CHIFFREMENT SYMÉTRIQUE	LONGUEUR DE LA CLÉ
DES	56
3DES	56 (3 fois)
AES	128, 192, 256
SEAL	160

L'intégrité :

IPSEC utilise des fonctions de hachage telles que MD5 ou SHA, pour assurer l'intégrité des données.

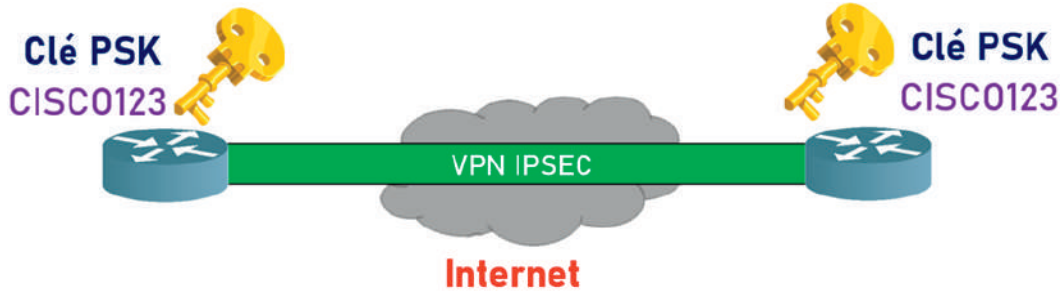
FONCTIONS DE HACHAGE	LONGUEUR DE L'EMPREINTE
HMAC-MD5	128
HMAC-SHA1	160

L'authentification d'origine :

IPSEC se base sur **IKE** pour l'authentification en utilisant l'une des méthodes suivantes :

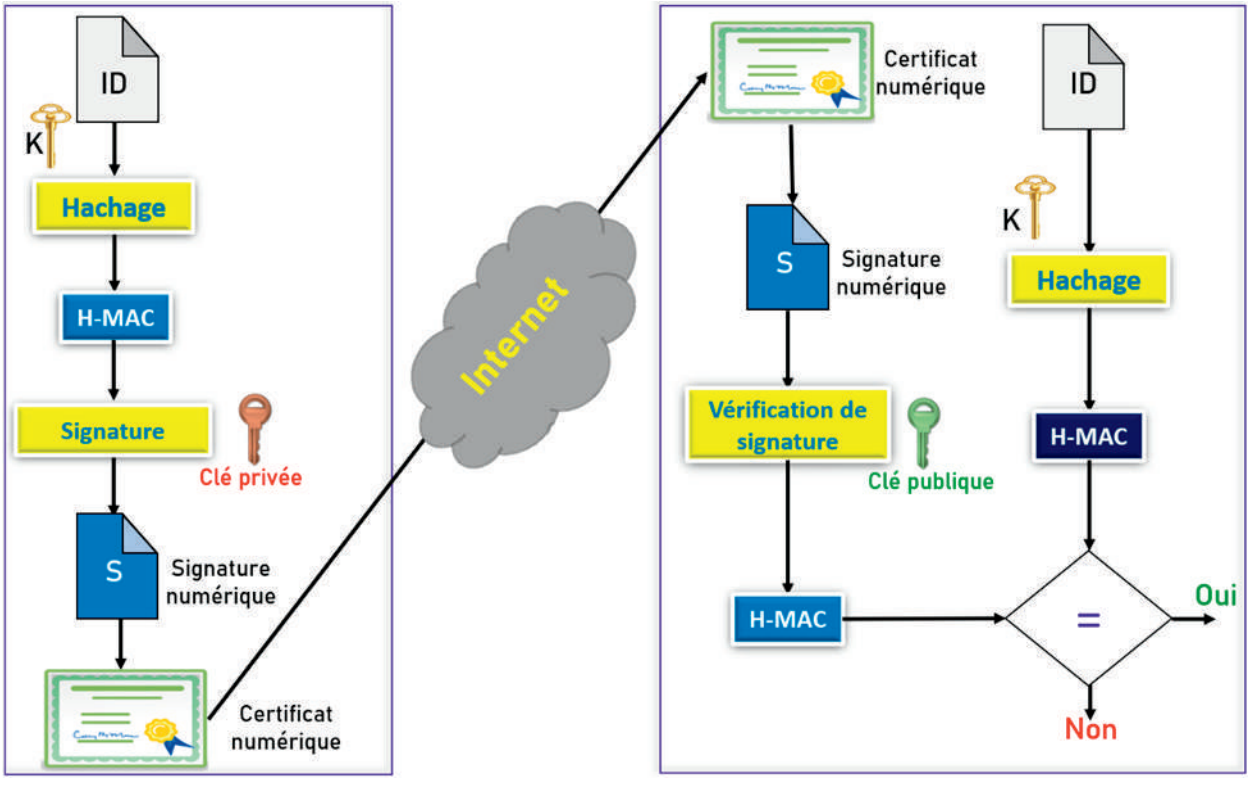
Authentification PSK :

Ce type d'authentification utilise une clé prépartagée (**PSK** : **P**re-**S**hared **K**ey) configurée au niveau de tous les homologues.



Authentification RSA :

Ce type d'authentification se base sur des certificats numériques utilisant l'algorithme de chiffrement asymétrique **RSA** (**R**ivest-**S**hamir-**A**dleman).



L'échange des clés :

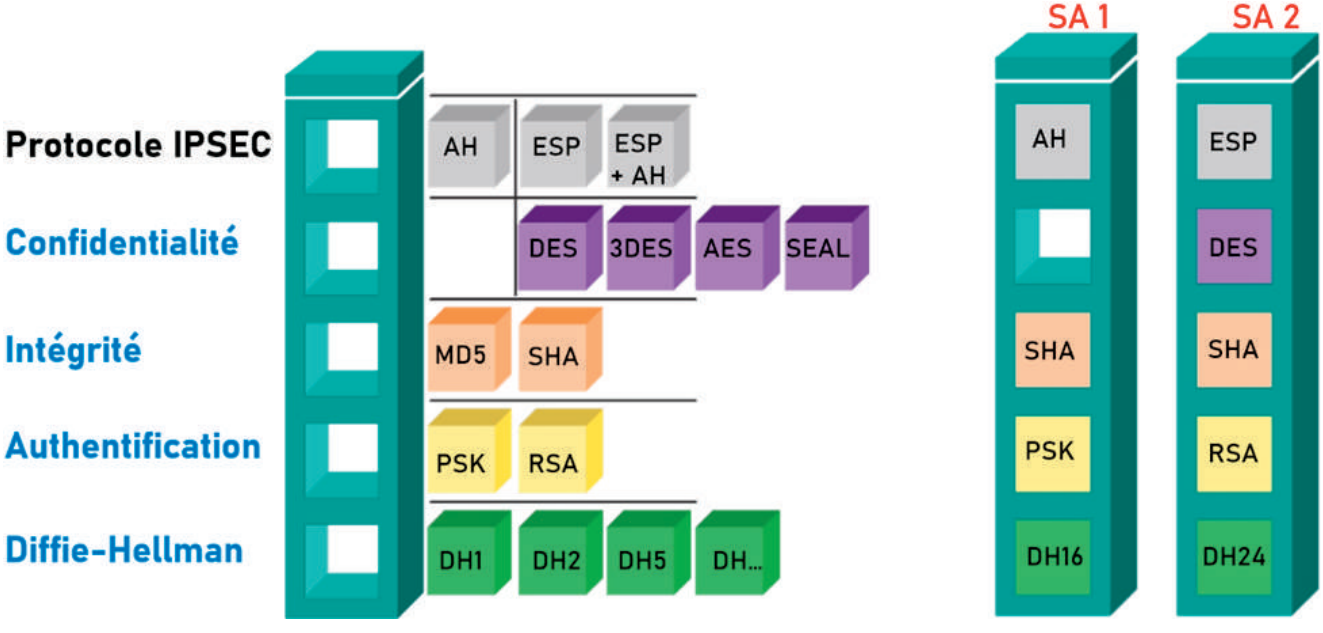
IPSEC utilise l'algorithme de **D**iffie-**H**ellman DH1, DH2, DH5 ou autre pour partager une clé secrète entre deux homologues de manière sécurisée.

ALGORITHMES DE DIFFIE-HELLMAN	LONGUEUR DE LA CLÉ
DH1	768
DH2	1024
DH5	1536
DH14	2048

ALGORITHMES DE DIFFIE-HELLMAN	LONGUEUR DE LA CLÉ
DH15	3072
DH16	4096
DH19	256 (cryptographie à courbe elliptique (ECC))
DH20	384 (cryptographie à courbe elliptique (ECC))
DH21	521 (cryptographie à courbe elliptique (ECC))
DH24	2048 (cryptographie à courbe elliptique (ECC))

LA STRUCTURE IPSEC ET LES ASSOCIATIONS DE SÉCURITÉ SA :

La structure IPSEC :

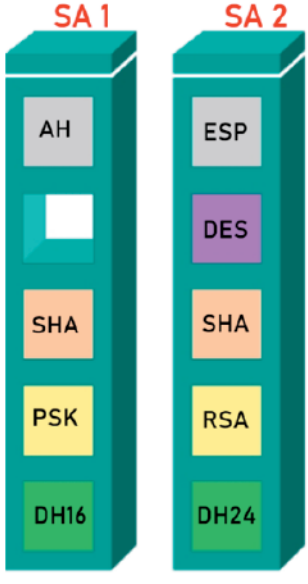


Il existe deux protocoles IPSEC :

- **AH** (**A**uthentication **H**eader) : Ne prend pas en charge la confidentialité des données.

- **ESP** (**E**ncapsulation **S**ecurity **P**ayload).

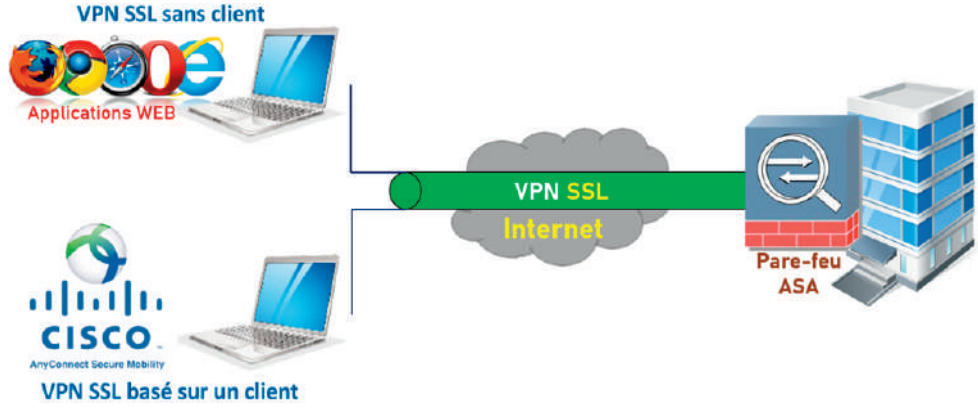
Les associations de sécurité IPSEC :



	Exemple SA 1	Exemple SA 2
Protocole IPSEC	AH	ESP
Confidentialité	AH n'assure pas la confidentialité	DES
Intégrité	SHA	SHA
Authentification	PSK	RSA
Echange des clés	DH16	DH24

> La combinaison ESP + AH est rarement utilisé, car elle ne peut pas traverser un périphérique NAT.

19.4.4. VPN SSL :

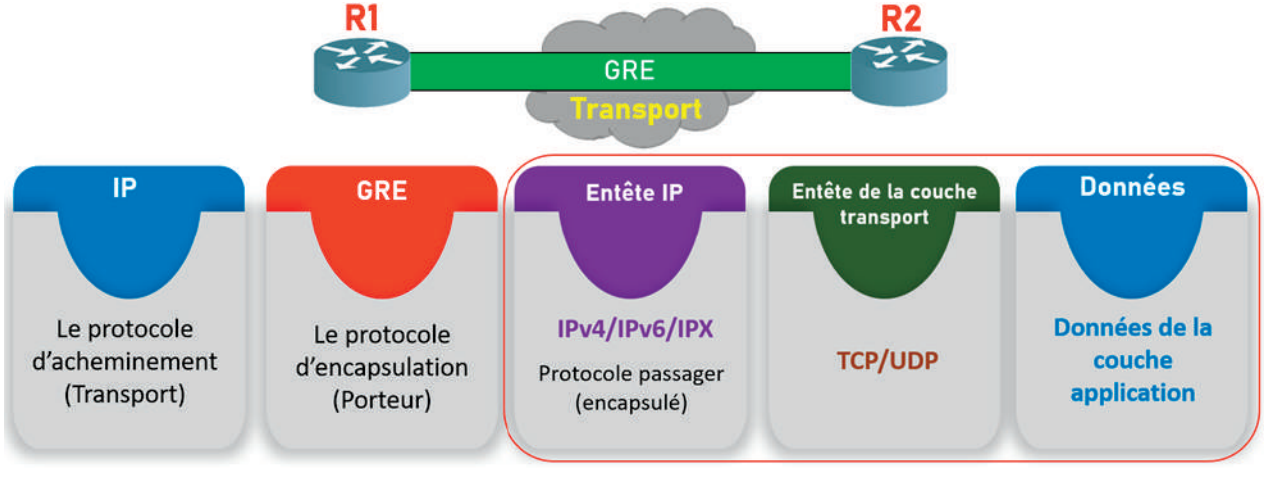


VPN sans client : L'utilisateur a un accès VPN en utilisant une connexion SSH par un navigateur Web.

VPN basé sur un client : L'utilisateur installe une application telle que Cisco AnyConnect Secure Mobilité de Cisco.

19.4.5. GRE sur IPSEC :

ENCAPSULATION GRE :

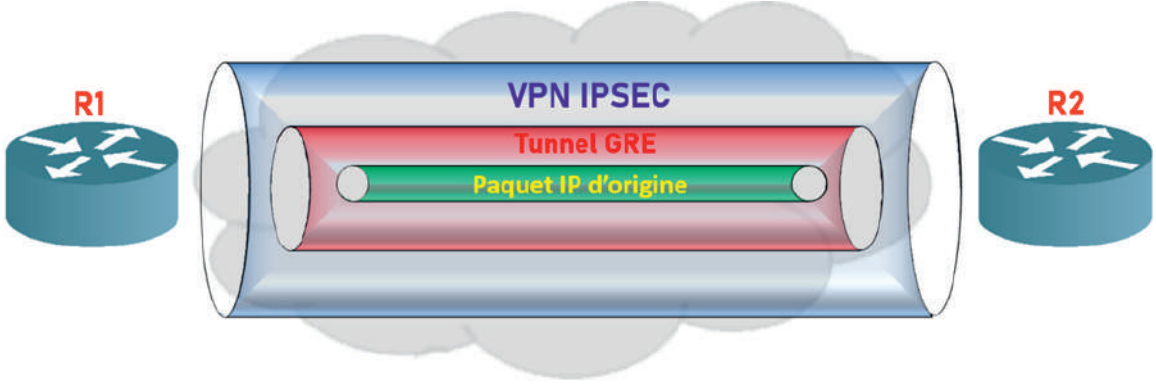


Le protocole passager : Le protocole d'origine qui doit être encapsulé (IPv4, IPv6, etc.).

Le protocole d'encapsulation (Porteur) : GRE qui encapsule le paquet d'origine.

Le protocole de transport : Le protocole utilisé pour transporter réellement le paquet (IPv4, IPv6, etc.).

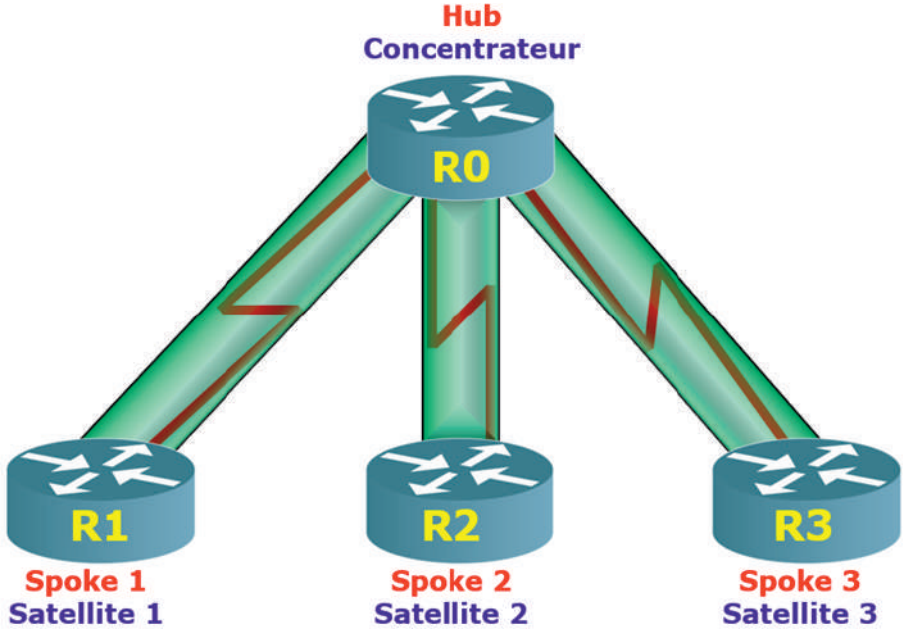
GRE SUR IPSEC :



19.4.6. DMVPN :

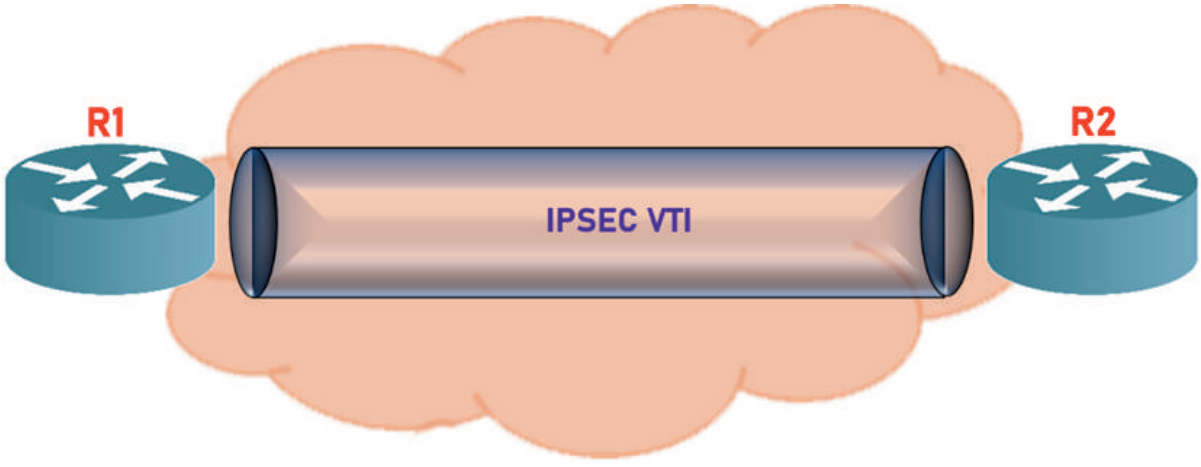
DMVPN (**D**ynamic **M**ultipoint **VPN**) est une solution logicielle de Cisco basée sur IPSEC qui permet de créer plusieurs VPN de façon simple, dynamique et évolutive.

- Chaque site est configuré en utilisant (mGRE).
- Lorsqu'un nouveau site nécessite une connexion sécurisée, la même configuration sur le HUB prend en charge le tunnel.



INTERFACE DE TUNNEL VIRTUEL IPSEC (IPSEC VTI) :

- IPSEC VTI simplifie le processus de configuration.
- La configuration IPSEC VTI utilise des interfaces virtuelles au lieu des interfaces physiques.
- IPSEC VTI supporte le trafic en multidiffusion (Trafic de routage, par exemple).
- IPSEC VTI peut être configuré entre les sites ou dans une topologie Hub-And-Spoke.

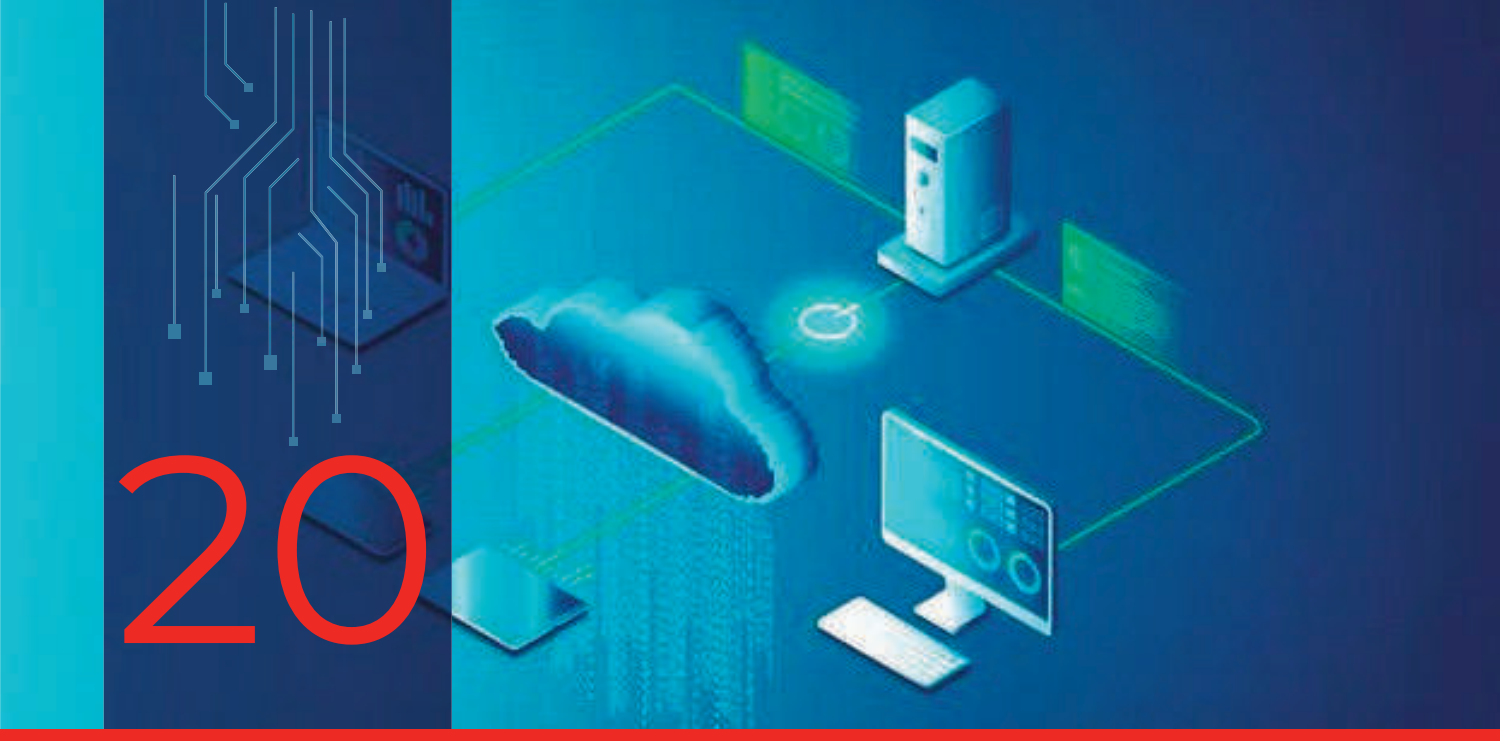


VPN MPLS :

Deux types de solutions VPN MPLS :

VPN MPLS de couche 3 : Le prestataire de service participe au routage client.

VPN MPLS de couche 2 : Le prestataire de services n'est pas impliqué dans le routage du client. (il déploie un service LAN privé virtuel (VPLS)).



20

LA VIRTUALISATION DU RÉSEAU

20.1. Le cloud computing

20.1.1. Notion du cloud :

Le cloud computing consiste à utiliser des serveurs distants par l'intermédiaire d'un réseau pour stocker des données ou les exploiter.

20.1.2. Services de cloud :

Il existe trois principaux services de cloud computing :

IAAS (INFRASTRUCTURE AS A SERVICE) :

- L'infrastructure en tant que service IAAS est un service de cloud qui permet d'utiliser un ordinateur virtuel complet avec toutes ses ressources.
- Le fournisseur du service IIAS gère la plateforme de l'hyperviseur.
- L'utilisateur du service IAAS gère l'ordinateur virtuel.

- Windows Azure est un exemple d'une infrastructure IAAS offerte par Microsoft.

PAAS (PLATFORM AS A SERVICE) :

- La plateforme en tant que service PAAS est un service de cloud qui permet d'utiliser une plateforme particulière et non pas un serveur complet.
- Le fournisseur du service IAAS fournit l'accès à la plateforme aux utilisateurs (généralement des développeurs).
- SQL Azure est un exemple de plateforme offerte par Microsoft.

SAAS (SOFTWARE AS A SERVICE) :

- Le logiciel en tant que service SAAS est un service de cloud dont le fournisseur du service héberge l'application de l'utilisateur et l'infrastructure entière qui prend en charge cette application.
- Office 365 est un exemple d'application SAAS qui offre la suite Office (Excel Word PowerPoint, etc.), ainsi que pour d'autres services tels que OneDrive, Skype, etc.

> ITAAS (IT As A Service) est un service qui fournit un support informatique pour chacun des services de cloud computing.

20.1.3. Modèles de cloud :

Il existe 4 modèles principaux de cloud :

- Cloud public
- Cloud privé
- Cloud hybride
- Cloud communautaire

CLOUD PUBLIC :

- Le cloud public fournit des services et des applications au grand public.
- Le cloud public peut héberger plusieurs locataires issus de plusieurs organisations.
- Les services peuvent être gratuits ou payants.
- Le cloud public est moins cher, car le coût est absorbé par les différents locataires.
- Le cloud public est moins sécurisé.

CLOUD PRIVÉ :

- Le cloud privé est dédié à une organisation unique.
- Le cloud privé est plus sécurisé.
- Le cloud privé est plus coûteux.

CLOUD HYBRIDE :

- Un cloud hybride est constitué de deux ou plusieurs clouds (exemple : partie privée, partie publique).
- Les clouds hybrides sont reliés par une architecture unique.
- Les utilisateurs d'un cloud hybride disposent de différentes autorisations d'accès aux divers services.

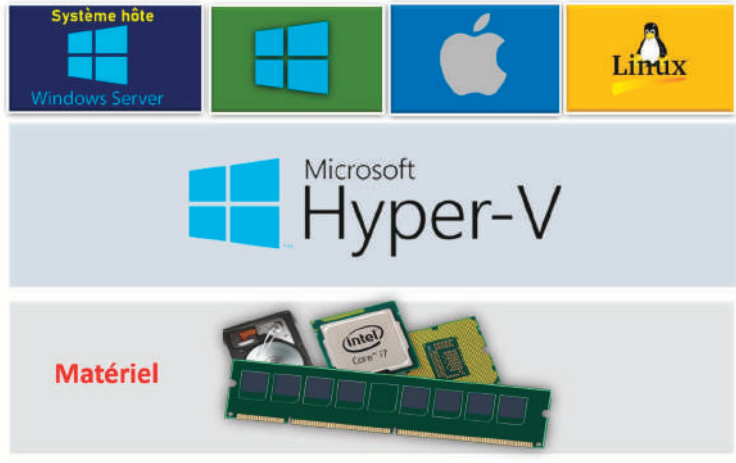
CLOUD COMMUNAUTAIRE :

- Un cloud communautaire est créé pour l'usage exclusif d'une communauté spécifique.
- Un cloud communautaire est utilisé par plusieurs organisations qui ont des besoins communs.

20.2. La virtualisation

20.2.1. Notion de la virtualisation :

La virtualisation est une technologie qui permet de créer plusieurs environnements simulés ou ressources dédiées à partir d'un seul système physique.



Il existe 3 éléments principaux :

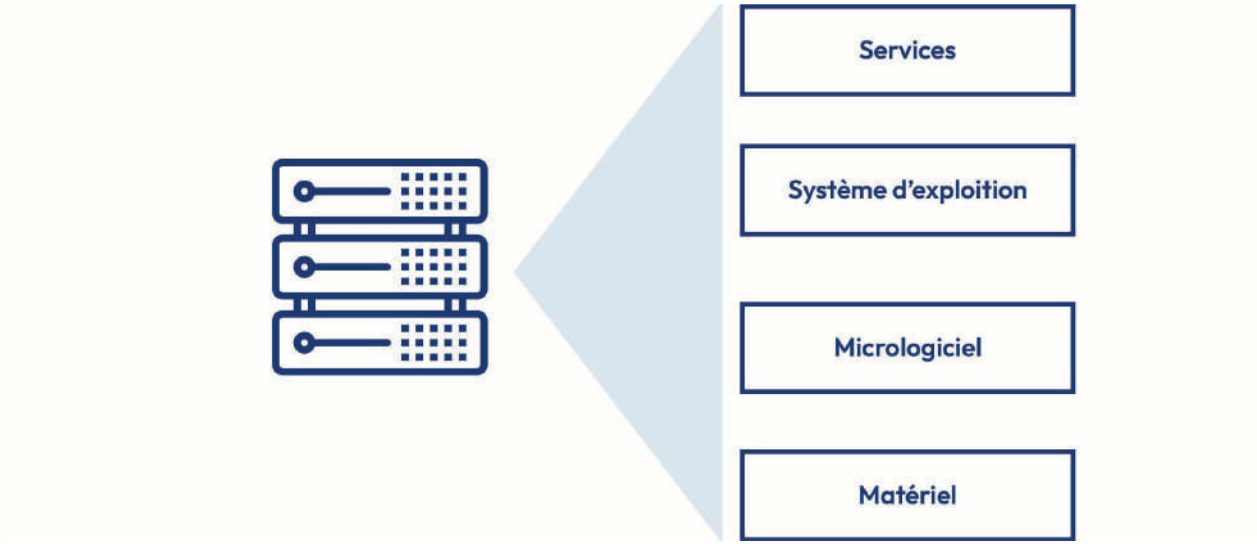
- **L'hyperviseur** : C'est le logiciel utilisé pour effectuer la virtualisation (Microsoft Hyper-V).
- **Le système hôte** : C'est le système installé sur la machine physique (Windows Server).
- **Les machines invitées** ou **les machines virtuelles** : Ce sont des environnements créés à l'aide de l'hyperviseur à partir de la machine physique (Windows 10, Mac, Linux, etc.).

20.2.2. Avantages de la virtualisation :

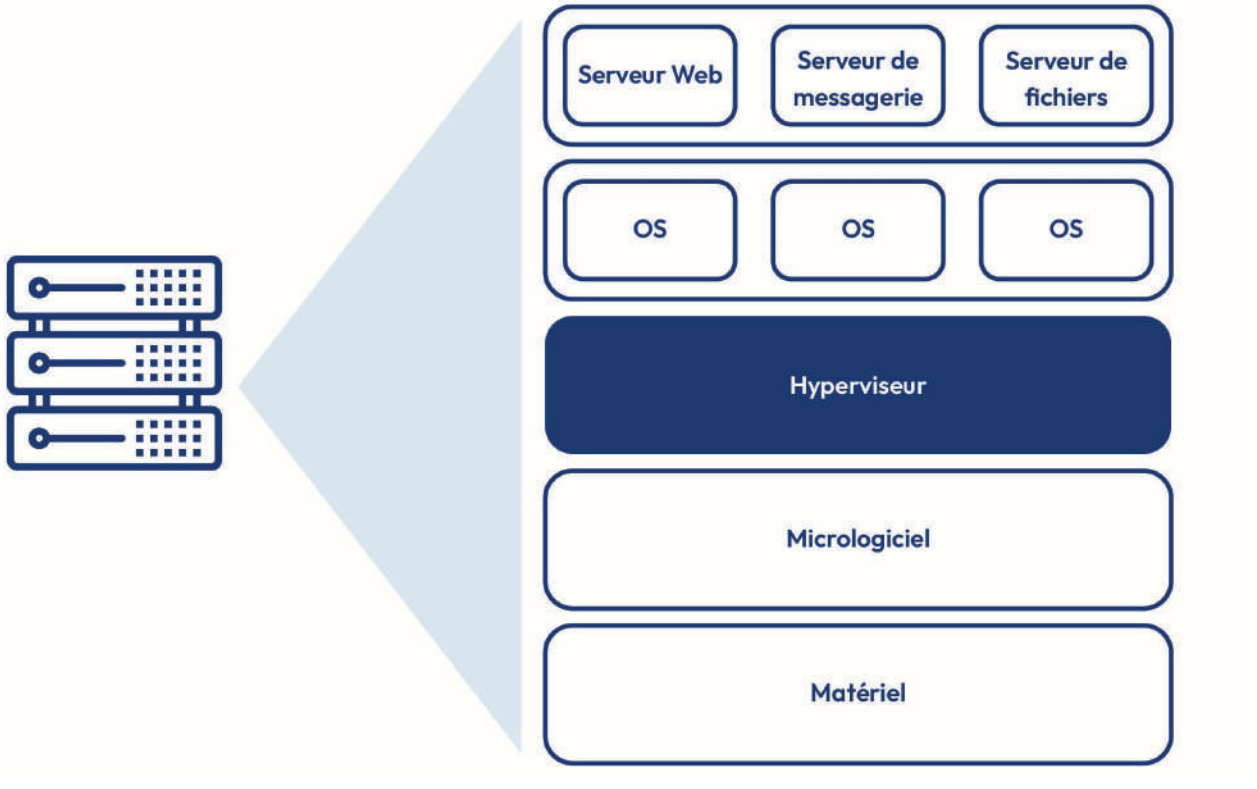
- Moins de matériel.
- Moins d'énergie.
- Moins d'espace.
- Prototypage plus facile.
- Provisionnement plus rapide des serveurs.
- Augmentation du temps de fonctionnement des serveurs.
- Amélioration de la reprise après désastre.

20.2.3. Couches d'abstraction :

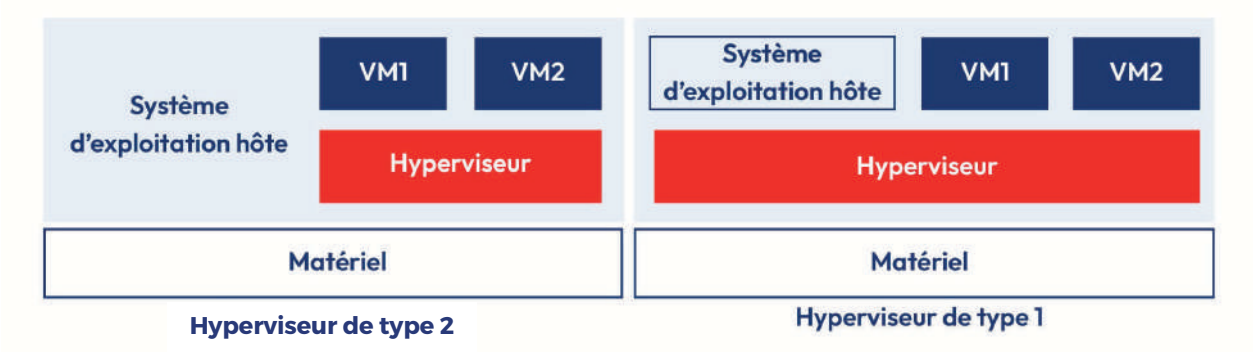
L'ARCHITECTURE SANS VIRTUALISATION :



L'ARCHITECTURE AVEC VIRTUALISATION :



20.2.4. Types d'hyperviseurs :

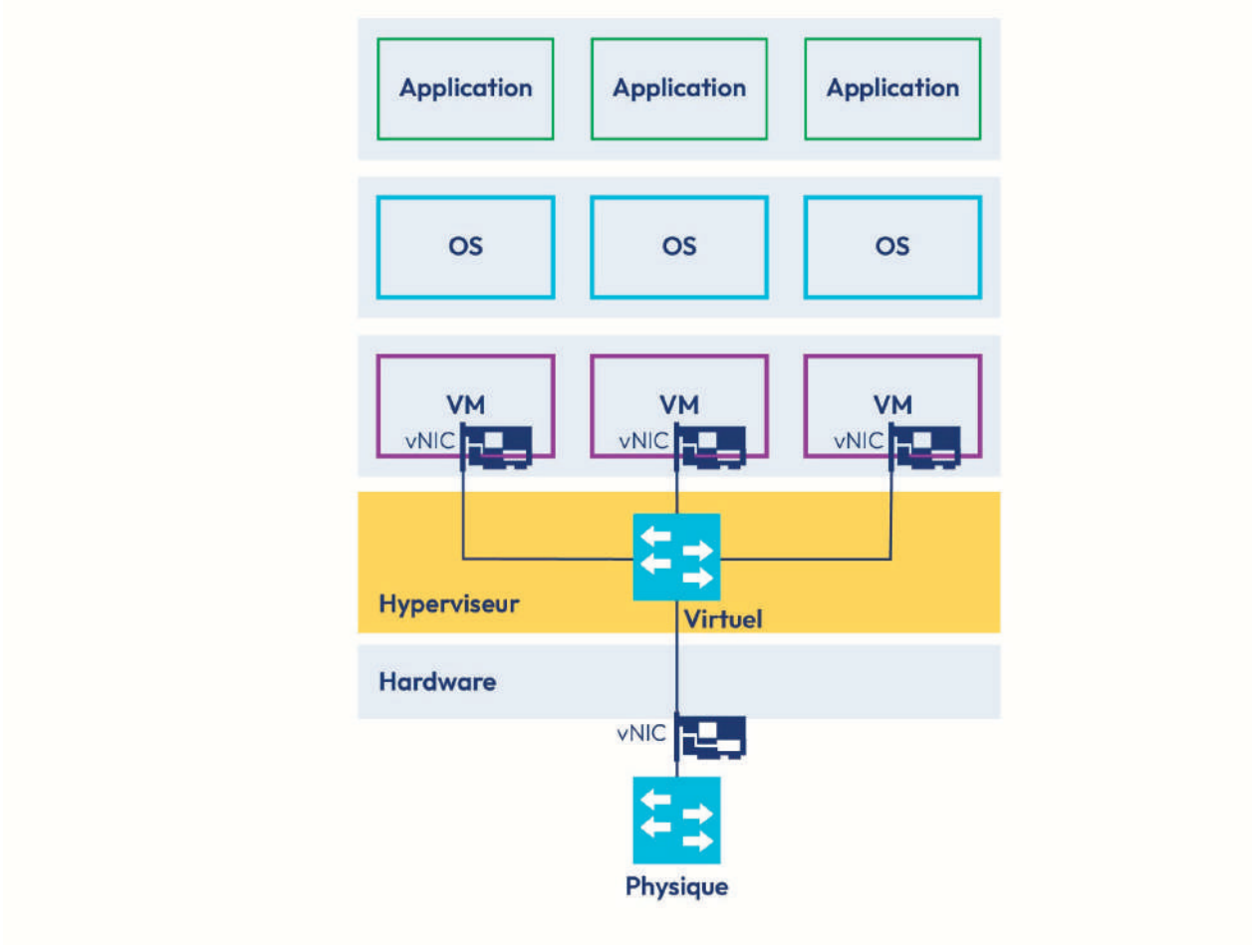


L'hyperviseur de type 1 : Les ressources matérielles sont gérées directement par l'hyperviseur.

L'hyperviseur de type 2 : L'hyperviseur est un logiciel qui s'installe en dessus du système d'exploitation. Ainsi, c'est le système d'exploitation qui gère les ressources matérielles et non pas l'hyperviseur.

20.2.5. Exemples d'hyperviseurs :

20.2.6. Carte d'interface réseau virtuelle :



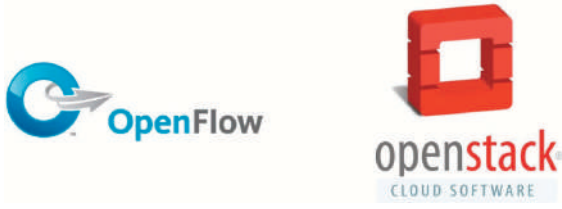
Chaque machine virtuelle possède une carte réseau virtuelle vNIC qui est connectée à un commutateur virtuel.

20.3. Réseaux SDN :

20.3.1. Technologies de virtualisation des réseaux :

SDN (SOFTWARE-DEFINED NETWORKING)

Composants SDN :



Types d'architectures SDN :

SDN basé sur les périphériques : Les périphériques sont programmables par des applications s'exécutant sur le périphérique lui-même (**Cisco OnePK**).

SDN basé sur les contrôleurs : Il utilise un contrôleur centralisé qui connaît tous les appareils du réseau. Les applications peuvent interagir avec le contrôleur qui est le responsable sur la gestion des périphériques réseau (**OpenDayLight**).

SDN basé sur les politiques : Il se base sur un contrôleur centralisé avec une couche stratégique supplémentaire. Il utilise des applications intégrées qui automatisent les tâches de configuration avancée des périphériques (**APIC-EM**).

ACI (CISCO APPLICATION CENTRIC INFRASTRUCTURE)