SUPPORT DE COURS : WAN ROUTEUR

GOUALO Mominé Elysée Angenor, Ingénieur
Sécurité et Réseau, certifié CCNA/CCNP/PCNSE

1. Introduction

Dans leur politique d'expansion vers de nouveaux marchés de production et de consommation ou de collaboration avec des partenaires, Les entreprises ont besoin de s'interconnecter avec leurs sites succursales et/ou les sites des partenaires afin d'échanger les informations(voix, données, vidéos), même si ces sites sont éloignés les uns des autres. Les réseaux étendus, ou WAN, sont utilisés pour relier les LANs du siège des entreprises aux LANs(réseaux informatiques locaux) des sites succursales et/ou partenaires distants. Un WAN(réseaux informatiques élargis ou Wide Area Network) peut couvrir une ville, un pays ou une région voire même des continents. Le WAN est la propriété du fournisseur de services publics ou privés, et les entreprises payent pour utiliser les services de réseau WAN du fournisseur.

2. Pourquoi un WAN ?

Le WAN a une portée qui va au-delà de l'étendue géographique du LAN. Les WAN sont utilisés pour interconnecter les sites de l'entreprise entre eux et à Internet et avec des partenaires.
Le WAN est la propriété du fournisseur de services. Cependant, certaines structures pour des raisons de sécurité construisent leur WAN de bout en bout afin d'interconnecter leurs différents sites sans se référer à un fournisseur. Ces cas où une organisation construitson propre WAN privé pour relier ses sites sont vraiment rares car la mise en place et la maintenance d'un WAN privé sont très coûteux. Pour minimiser les coûts, et les organisations payent pour utiliser les services de réseau du fournisseur pour connecter des sites distants. Les fournisseurs de services WAN comprennent les opérateurs de réseau téléphonique, de réseau câblé ou de service par satellite. Le fournisseur de services fournit les liens nécessaires à l'interconnexion des sites distants pour le transport de données, de voix et de vidéo.
À l'inverse, les LAN sont en général la propriété de l'organisation et servent à connecter les ordinateurs et les périphériques locaux, dans un bâtiment ou sur une zone géographique limitée.

2.1 Les WAN sont-ils nécessaires ?

Sans WAN, les LAN ne sont qu'un ensemble de réseaux isolés. Les LAN peuvent transmettre les données de façon rapide et efficace dans des zones géographiques restreintes. Toutefois, avec le développement des organisations, les entreprises doivent étendre les communications vers des sites éloignés du point de vue géographique. Voici quelques exemples :
Les bureaux régionaux ou les filiales d'une organisation doivent pouvoir se connecter aux applications métiers basées au siège pour leurs travaux quotidiens.
Les organisations ont besoin de partager les informations avec d'autres organisations. Par exemple, l'Université Polytechnique de Bingerville envoie les informations sur la performance de ses meilleurs étudiants aux Universités partenaires aux Canada pour les tests d'intégration dans ces Université Canadiennes ou des éditeurs de logiciels envoient régulièrement des informations sur les produits et les promotions aux distributeurs qui vendent les produits aux utilisateurs finaux.
Les employés effectuant souvent des voyages d'affaires doivent avoir accès aux informations qui se trouvent sur le réseau de leur entreprise.
Dans le cadre de leurs recherches, les étudiants accèdent à des catalogues et des publications de bibliothèques situées dans un lieu différent, dans le même pays ou à l'étranger.
Il n'est pas faisable de connecter des ordinateurs à l'échelle d'un pays, ou à l'échelle du monde, avec des câbles. Ainsi, différentes technologies sont apparues pour répondre au développement des communications. De plus en plus, Internet est utilisé comme une alternative bon marché aux WAN d'entreprise. Les entreprises ont à leur disposition de nouvelles technologies permettant d'assurer la sécurité et la confidentialité des communications et des transactions via Internet. Les WAN, utilisés seuls ou en conjonction avec Internet, offrent aux organisations et aux personnes la possibilité de communiquer sur de longues distances.

3. Fonctionnement WAN

3.1 WAN dans le modèle OSI

Le fonctionnement du WAN se fait principalement sur la couche physique (Couche OSI 1) et la couche de liaison de données (Couche OSI 2). Les normes d'accès au réseau étendu décrivent généralement les méthodes de livraison sur la couche physique et les caractéristiques requises pour la couche liaison de données, notamment l'adressage physique, le contrôle de flux et l'encapsulation.

Les normes d'accès aux WAN sont définies et gérées par un certain nombre d'autorités reconnues, dont :

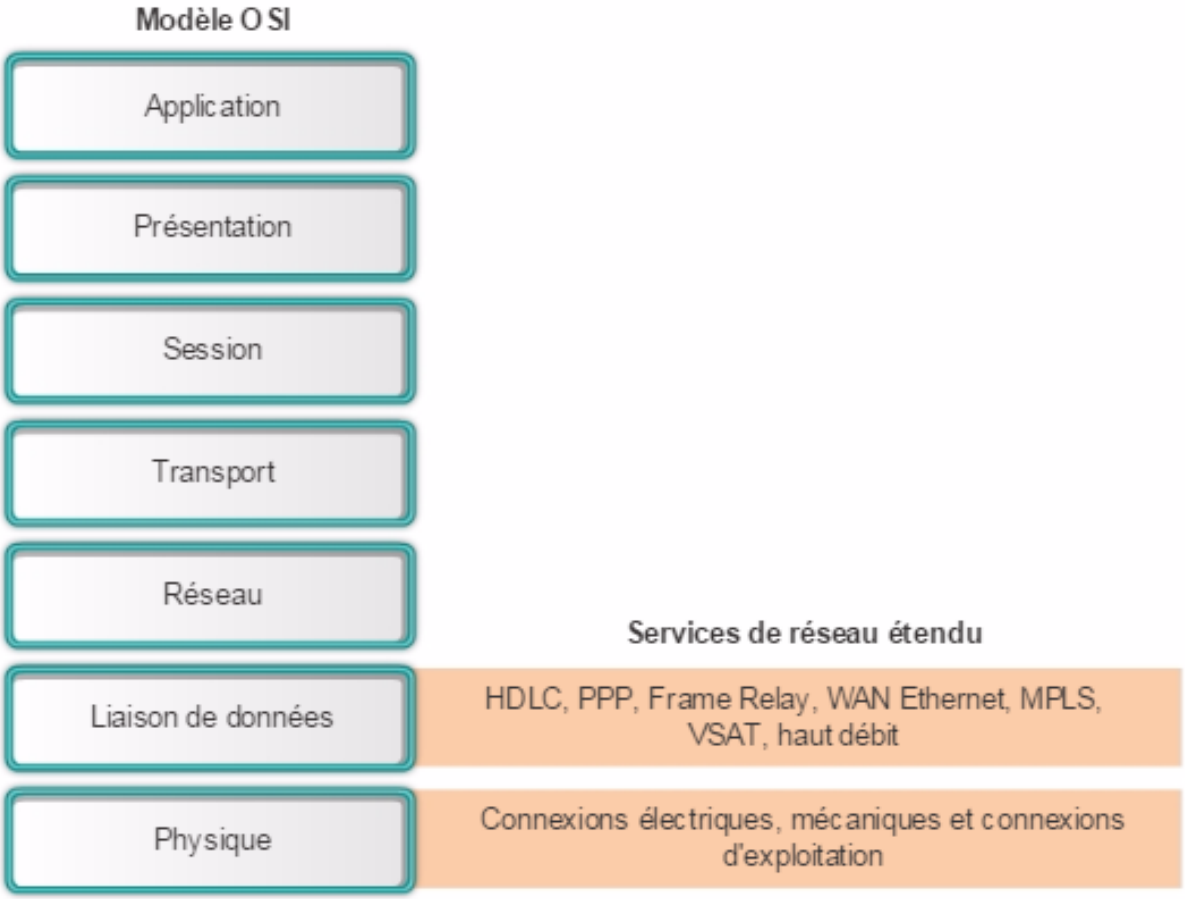
- **Telecommunication Industry Association et the Electronic Industries Alliance (TIA/EIA)**

- **ISO (International Standards Organization)**

- **Institute of Electrical and Electronics Engineers (IEEE)Les protocoles de la couche 1 décrivent comment fournir les connexions électriques, mécaniques, opérationnelles et fonctionnelles aux services du fournisseur de services de communication.**

Les protocoles de la couche 2 définissent comment les données sont encapsulées pour être transmises vers un emplacement distant, ainsi que les mécanismes de transfert des trames résultantes. Sont utilisées toute une série de technologies, par exemple le protocole PPP (Point-to-Point Protocol), le Frame Relay et ATM. Certains de ces protocoles utilisent les mêmes trames de base ou bien un sous-ensemble du mécanisme HDLC (High-Level Data Link Control).

La plupart des liaisons WAN sont point à point. Pour cette raison, le champ d'adresse dans la trame de couche 2 n'est généralement pas utilisé.



3.2 Terminologie WAN

La principale différence entre un WAN et un LAN et que la société, où l'organisation, doit s'abonner auprès d'un fournisseur de services WAN extérieurs afin d'utiliser les services du réseau de l'opérateur WAN. Le WAN utilise les liaisons de données fournies par les services de l'opérateur afin d'accéder à Internet et de connecter les différents emplacements de l'entreprise entre eux, à d'autres emplacements d'autres organisations, à des services externes, et enfin aux utilisateurs distants.

La couche physique du WAN correspond aux connexions physiques entre le réseau de la société et le réseau du fournisseur de services. La figure ci-dessous illustre la terminologie utilisée pour décrire les connexions WAN, par exemple :

- **Équipement d'abonné (CPE)** : périphériques et câblage interne qui se trouvent sur la périphérie d'entreprise et qui se connectent à une liaison

d'opérateur. L'abonné est propriétaire de l'équipement ou le loue à son fournisseur de services. L'abonné, dans ce contexte, est une société qui utilise les services WAN d'un fournisseur de services.

 Équipement de communication de données (DCE) : aussi appelé équipement de fin de circuit de données, le DCE comprend des périphériques qui placent des données sur la boucle locale. Le DCE fournit principalement une interface pour connecter les abonnés à une liaison de communication sur le cloud du WAN.

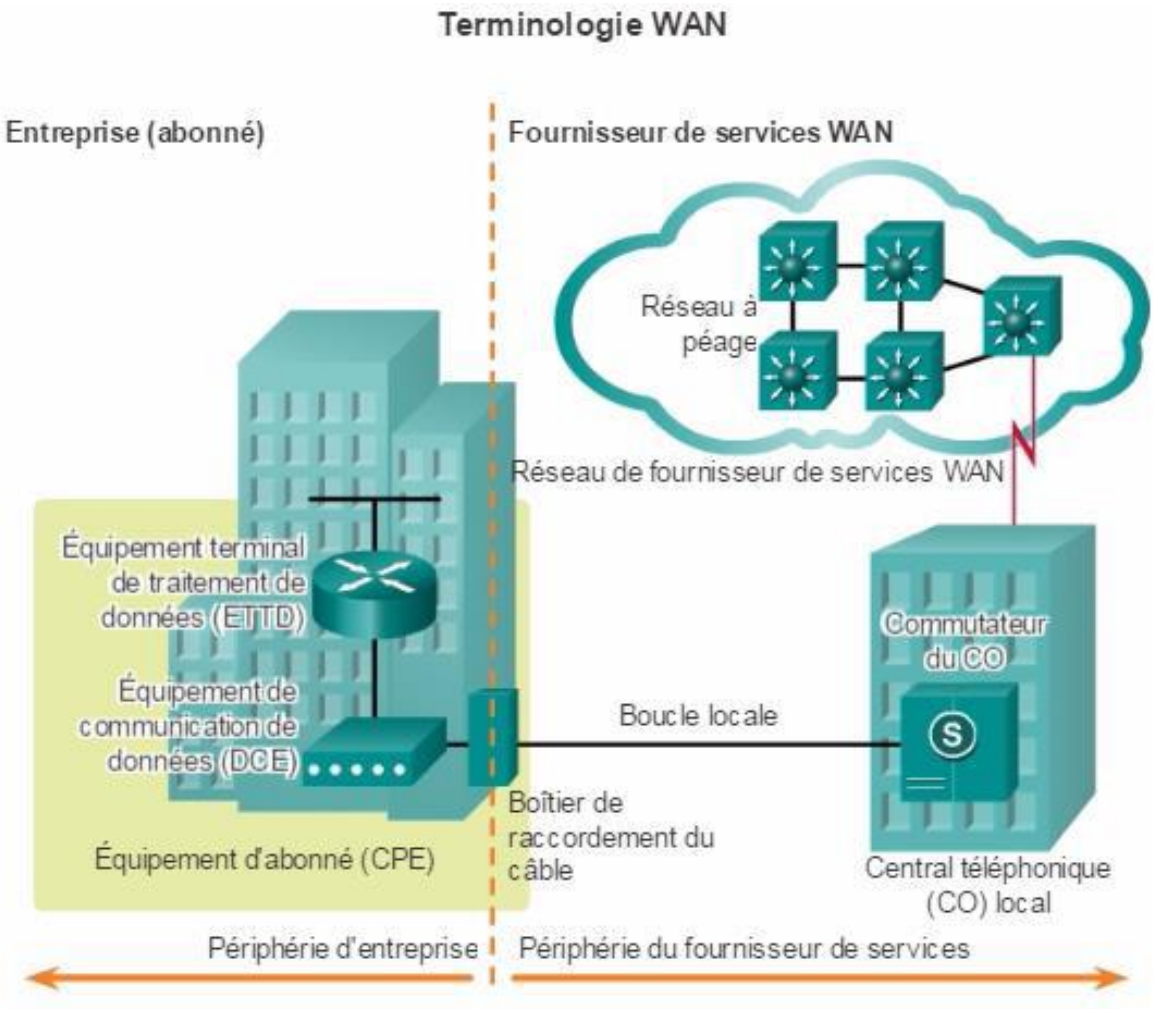
 Équipement terminal de traitement de données (ETTD) : les périphériques du client qui transmettent les données d'un réseau client ou d'un ordinateur hôte pour transmission sur le réseau étendu. L'équipement terminal de traitement de données se connecte à la boucle locale grâce à l'équipement de communication de données.

 Point de démarcation : point établi dans un bâtiment ou complexe afin de séparer les équipements du client des équipements du fournisseur de services. Physiquement, le point de démarcation est le boîtier de raccordement de câblage, situé chez le client, qui connecte les câbles de l'équipement d'abonné à la boucle locale. Il est généralement placé de façon à faciliter son accès par un technicien. Le point de démarcation physique est l'endroit où la responsabilité de la connexion passe de l'utilisateur au fournisseur de services. En cas de problème, il faut déterminer qui de l'utilisateur ou du fournisseur de services est responsable de la résolution du problème ou de la réparation.

 Boucle locale : le câble cuivre ou fibre qui connecte l'équipement de l'abonné au central téléphonique (CO) du fournisseur de services. Cette boucle locale est parfois aussi appelée le « dernier kilomètre ».

 Central téléphonique (CO) : installation ou bâtiment du fournisseur de services local qui relie l'équipement de l'abonné au réseau du fournisseur.

 Réseau à péage ou réseau cœur(backbone) : comprend les lignes en fibre optique de communication longue distance tout numérique, les commutateurs, les routeurs et tous les autres équipements dans le réseau du fournisseur WAN.



4 Infrastructures WAN privées

4.1 Lignes louées

Lorsque vous avez besoin de connexions permanentes dédiées, la liaison point à point permet de créer un chemin de communication WAN pré-établi depuis le bureau du client jusqu'au réseau du fournisseur. Les lignes point à point sont généralement louées auprès d'un fournisseur de services. Elles sont appelées lignes louées.

Ces lignes louées existent depuis le début des années 50, et portent différents noms, par exemple circuit loué, liaison série, ligne série, liaison point à point et ligne T1/E1 ou T3/E3. Le terme ligne louée fait référence au fait que

l'organisation paie tous les mois un certain montant à un fournisseur de services pour utiliser la ligne. Les lignes louées peuvent présenter des capacités variées et leur prix dépend généralement de la bande passante requise ainsi que de la distance entre les deux points de connexion.
En Amérique du Nord, les fournisseurs de services utilisent le système T-carrier pour définir les capacités de transmission numérique d'une liaison cuivre en série, alors qu'en Europe et Afrique, le système E-carrier est utilisé, comme illustré dans la figure ci-dessous. Par exemple, une liaison T1 prend en charge 1,544 Mbit/s, une liaison E1 2,048 Mbit/s, une liaison T3 43,7 Mbit/s et une connexion E3 34,368 Mbit/s. Le débit Optical Carrier est utilisé pour définir la capacité de transmission numérique d'un réseau fibre optique.
Les avantages des lignes louées sont les suivants :
 Simplicité : les liaisons de communication point à point ne nécessitent que peu d'expertise pour leur installation et leur maintenance.

 Qualité : les liaisons de communication point à point offrent habituellement une grande qualité de service, si la bande passante est adaptée. L'aspect dédié de la ligne permet d'éviter la latence ou la gigue entre les points d'extrémité.

 Disponibilité : la disponibilité constante est essentielle pour certaines applications, comme celles de commerce électronique. Les liaisons de communication point à point offrent une capacité permanente dédiée, nécessaire pour la voix ou la vidéo sur IP.

Les inconvénients des lignes louées sont les suivants :
 Coût : les liaisons point à point constituent généralement le type d'accès WAN le plus coûteux. Le coût des liaisons louées peut être important lorsqu'elles servent à connecter plusieurs sites répartis sur de grandes distances. De plus, chaque point d'extrémité nécessite une interface sur le routeur, ce qui augmente également le coût de l'équipement.

 Flexibilité limitée : le trafic WAN est souvent variable et les lignes louées possèdent une capacité fixe, de telle sorte que la bande passante de la ligne correspond rarement de manière exacte à ce qui est nécessaire. Toute modification de la ligne louée nécessite généralement une intervention sur site du personnel fournisseur d'accès Internet afin d'ajuster la capacité.

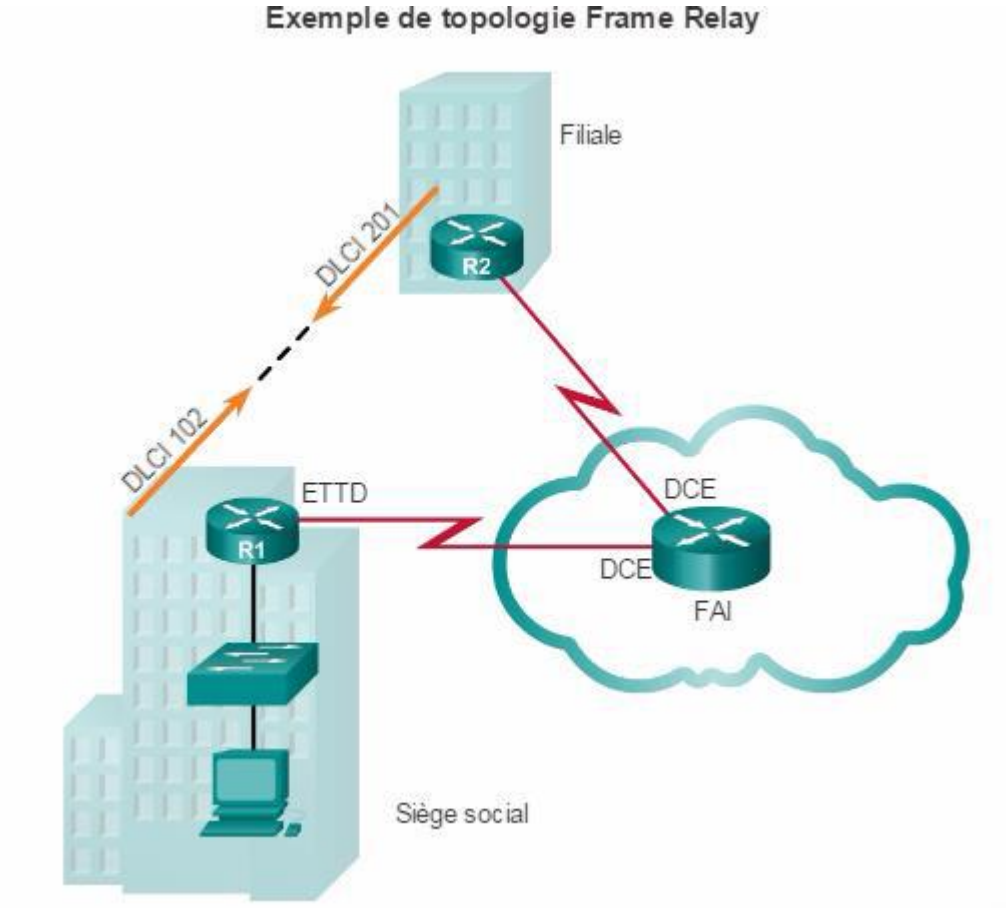
Le protocole de couche 2 est normalement le protocole HDLC ou le protocole PPP

Exemple de topologie de ligne louée

5. Frame Relay

Frame Relay est une technologie WAN simple de couche 2 d'accès multiple sans diffusion (NBMA) utilisée pour connecter des LAN d'entreprise. Il est possible de n'utiliser qu'une seule interface de routeur pour connecter plusieurs sites par des circuits virtuels permanents. Les circuits virtuels permanents sont utilisés pour transporter à la fois le trafic de voix et de données entre une source une destination. Ils assurent des taux jusqu'à 4 Mbit/s, certains fournisseurs proposant même des débits supérieurs.
Le routeur de périphérie n'a besoin que d'une seule interface, même lorsque plusieurs circuits virtuels sont utilisés. La petite ligne louée vers la périphérie de réseau du Frame Relay permet d'assurer des connexions bon marché entre plusieurs LAN éparpillés.
Frame Relay crée des circuits virtuels permanents identifiés grâce à un identifiant de connexion de liaison de données (DLCI). Les circuits virtuels permanents et les DLCI assurent la communication bidirectionnelle d'une

périphérique ETTD à un autre. Par exemple, dans l'illustration, R1 utilise le DLCI 102 pour atteindre R2, alors que R2 utilise le DLCI 201 pour atteindre R1



Quelques Avantages de frame relay :

- ✓ **Moins coûteux** : lorsque le client a déjà acheté une première liaison physique, alors pour les nouvelles interconnexions il réutilise la même liaison vue que Frame relay utilise les circuits logiques pour chaque interco.
- ✓ **Flexible** : peut s'adapter facilement à une augmentation du nombre des interconnexions.

Incnvénients :

- ✓ **Moins répandu dans le monde** : on trouve moins de fournisseur de frame relay dans le monde.
- ✓ **Pas de contrôle de flux ni de mécanisme de détection d'erreur**
- ✓ Débit limité à 44,375Mps.
- ✓ Il transporte les informations que sous forme de données

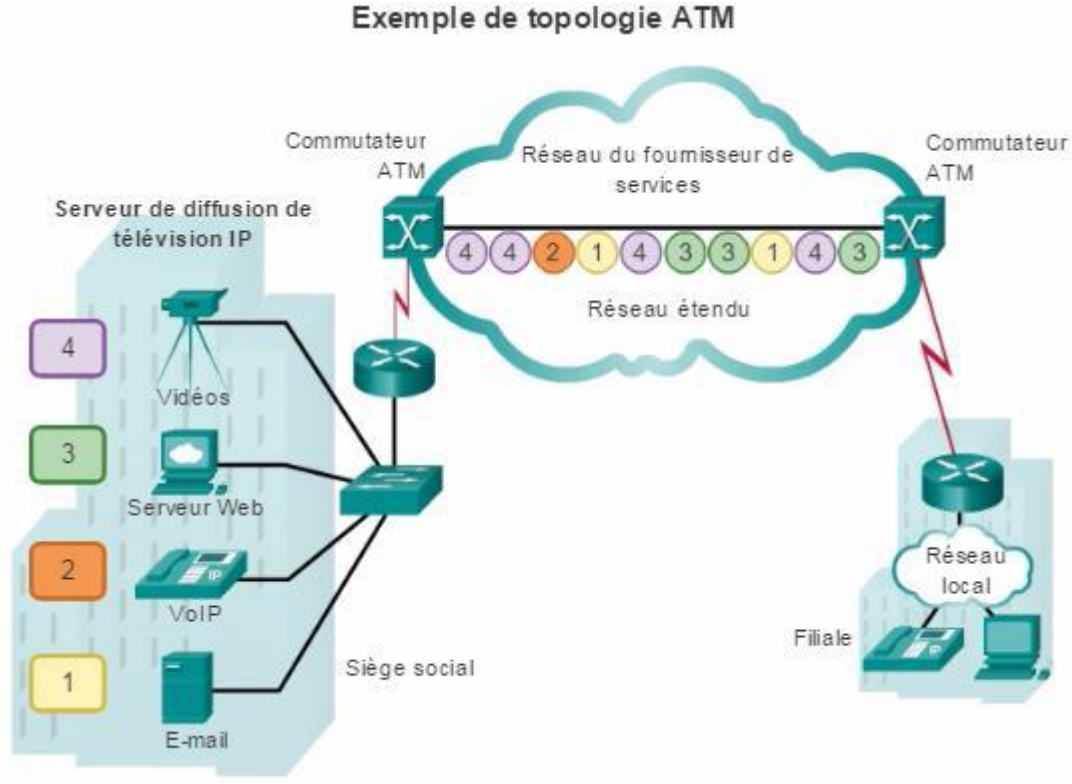
6. Technologie ATM

La technologie ATM (Asynchronous Transfer Mode) peut transférer de la voix, de la vidéo et des données sur des réseaux privés et publics. Elle s'appuie sur une architecture basée sur des cellules, plutôt que sur une architecture basée sur des trames. Les cellules ATM présentent toujours une longueur fixe de 53 octets. La cellule ATM de 53 octets contient un en-tête ATM de 5 octets, suivi de 48 octets de données utiles ATM. Les petites cellules de longueur fixe sont bien adaptées au transport du trafic vocal et vidéo, car ce trafic ne tolère pas les délais. En effet, le trafic vidéo et vocal n'a pas à attendre la fin de la transmission de paquets de données de plus grande taille.

La cellule ATM de 53 octets est moins efficace que les trames et paquets de plus grande taille de Frame Relay. Par ailleurs, la cellule ATM comporte au moins 5 octets de surcharge pour chaque ensemble de données utiles de 48 octets. Quand la cellule transporte des paquets de couche réseau segmentés, la surcharge est plus importante, car le commutateur ATM doit être en mesure de regrouper les paquets au niveau de la destination. Une ligne ATM type nécessite un débit supérieur de presque 20 % à celui de Frame Relay pour transporter le même volume de données de couche réseau.

La technologie ATM a été conçue pour faciliter l'extension et pour prendre en charge des vitesses de T1/E1 ou OC-12 (622 Mbit/s) et au-delà.

ATM propose à la fois des circuits virtuels permanents et des circuits virtuels commutés, même si les circuits virtuels permanents sont plus répandus avec les WAN. Comme pour d'autres technologies partagées, ATM autorise plusieurs circuits virtuels sur une seule connexion de ligne louée vers la périphérie de réseau.



Quelques raisons d'utiliser ATM :

- ✓ **S'intègre facilement avec les réseaux LAN.**
- ✓ **Transporte la voix, la donnée, la vidéo**
- ✓ **Débit élevé** de 155,5Mbps à 622Mps.
- ✓ Possède un mécanisme de contrôle de flux et détection d'erreur

Incnvénients :

- ✓ **Coûteux** par rapport à Frame Relay.
- ✓ **Mécanisme complexe de mise en place de la QoS**
- ✓ ATM est orienté connexion, le temps à établir la connexion est plus élevé que le temps mis pour l'utiliser.

7.WAN Ethernet

À l'origine, Ethernet a été développé comme technologie d'accès LAN. Cependant, au moment de son développement, Ethernet ne constituait pas une technologie d'accès WAN adaptée, car la longueur maximale de câble était d'environ un kilomètre. Cependant, de nouvelles normes Ethernet utilisant des câbles en fibre optique ont transformé Ethernet en une solution d'accès WAN applicable. Par exemple, la norme IEEE 1000BASE-LX autorise l'emploi de câbles en fibre optique de 5 km, alors que la norme IEEE 1000BASE-ZX prend en charge les câbles allant jusqu'à 70 km.

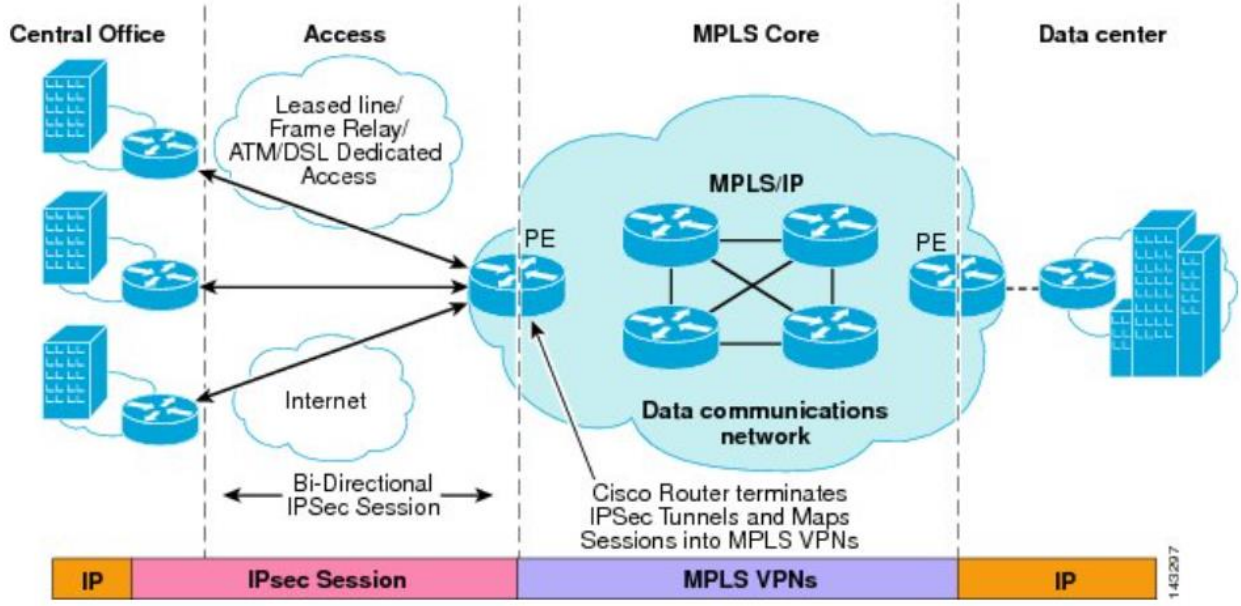
8. MPLS

MultiProtocol Label Switching (MPLS) est un mécanisme de transport de données basé sur la commutation d'étiquettes ou "labels", qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie. À l'origine, cette insertion s'opère entre la couche de liaison de données (niveau 2) et la couche réseau (niveau 3) afin de transporter des protocoles comme IP. C'est pourquoi de temps à autres **MPLS est qualifié de protocole de couche "2,5"**, entre la couche 2 (L2) du modèle OSI et la couche 3 (L3). Ce protocole a évolué pour fournir un service unifié de transport de données pour les clients en utilisant une technique de commutation de paquets.
La technologie MPLS présente plusieurs caractéristiques distinctes. Comme son sigle (MPLS) l'indique, ses caractéristiques sont :
Multiprotocol (multi-protocoles) : il est capable de transporter pratiquement tout type de trafic (voix, IPv4, IPv6, Ethernet, ATM, DSL et Frame Relay …) tout en respectant les contraintes de fonctionnement associées à chacun.

Label switching (commutation par étiquettes) : il se base sur une étiquette (en anglais : label) ou identifiant pour la commutation des paquets. Cette étiquette est attribuée aux paquets par l'équipement PE (Provider Edge) lors de leur entrée dans l'infrastructure MPLS

Le succès du IP/MPLS s'explique en grande partie par sa capacité à permettre au réseau de transporter tous les types de trafic, partant du trafic IP en passant par la VOIP jusqu'au trafic de niveau 2. MPLS est un moyen pour le réseau IP de consolider plusieurs réseaux en un seul. MPLS peut combiner les réseaux ATM, Frame Relay, voix, et d'autres réseaux IP en une seule infrastructure réseau unifiée, entrainant par conséquent une réduction considérable des coûts.

L'exemple de topologie de l'illustration présente l'utilisation de MPLS. Notez que les différents sites peuvent se connecter au cloud MPLS avec différentes technologies d'accès. Dans l'illustration, CE fait référence à la périphérie client, PE est le routeur de périphérie du fournisseur qui ajoute et supprime les étiquettes, et P est un routeur interne du fournisseur qui commute les paquets MPLS étiquetés.

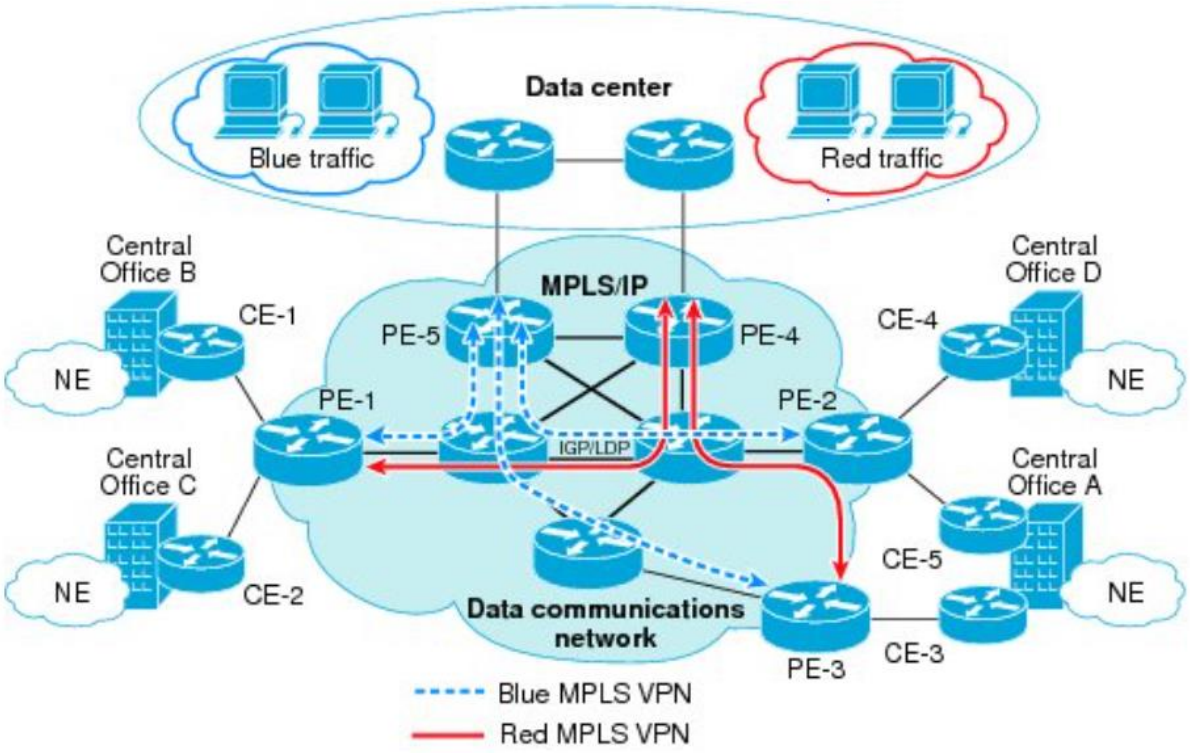


Architecture IP/MPLS

8.1 Terminologie IP MPLS

- **CE, Customer Edge** : Équipement du client situé chez le client qui n'a pas connaissance du IP/MPLS.
- **PE, Provider Edge** : équipement à l'entrée du nuage IP/MPLS, frontière entre le réseau IP pur et le réseau IP/MPLS.
- **P, Provider** : Equipement dans le nuage opérateur qui n'a pas d'interface avec le client.
- **LSP** : Label Switching Path, chemin suivi par un paquet dans le nuage IP/MPLS (voir lignes bleue et rouge sur le schéma ci-dessous)

- **LDP(Label Distribution Protocol)** : protocole de découverte de voisins et d'établissement de relation de voisinage entre les PE et P et entre P et P et de distribuer les Label dans MPLS
- **VRF(Virtual Routing and Forwading)** : permet d'avoir plusieurs tables de routage virtuelles sur un routeur MPLS permettant de résoudre le problème d'adresse IP dupliquée par différents clients du fournisseur MPLS.
- **MP-BGP** : MultiProtocol Border Gateway Protocol : utilisé pour faire passer les routes des clients dans le VPN MPLS
- **Route Distinguisher(RD)** : combinaison de chiffres sous forme XXX :YYY qui est utilisée par MP-BGP pour différencier les préfixes réseaux des différents client
- **Route Target Both(RT)** : combinaison de chiffres sous forme zzz :uuu qui est utilisée par MP-BGP pour l'échange de route(import-export) entre les VRFs
- **Redistribution de route** : permet l'échange d'information de routage entre différents protocoles de routage.



Topologie IP/MPLS avec LSP

8.2 QUELQUES AVANTAGES D'ADOPTER MPLS POUR LE FOURNISSEUR DE SERVICE :

- ❖ Avoir une infrastructure unifiée du réseau
- ❖ Avoir un cœur de réseau sans le protocole BGP
- ❖ Pouvoir facilement faire de l'ingénierie de traffic (traffic engineering, MPLS TE)
- ❖ Utilisation de label pour faire chemin vers le destinataire.

8.3 LES SERVICES OU APPLICATIONS MPLS

- ❖ MPLS VPN ou L3 MPLS VPN,, le plus populaire, utilisé généralement comme WAN par les entreprises pour interconnecter leurs sites.

- MPLS TE, adapté pour l'utilisation optimale automatique des liens.
- AToM, Any Transport over MPLS, service pour le transport des trafics de niveau 2 tels que Frame Relay, HDLC, ATM par MPLS.
- VPLS ou L2 MPLS VPN, permet d'établir le réseau ethernet sur le MPLS.

CAS PRATIQUE DE LA MISE EN PLACE D'UN NUAGE IP/MPLS ET D'INTERCONNEXION DE SITES D'ENTREPRISES : L'ENTREPRISE QUI SOUHAITE INTERCONNECTER SES DEUX SITES EST L'UNIVERSITE POLYTECHNIQUE DE BINGERVILLE.

OBJECTIF ATENDU LAB à la fin des 7 étapes: faire les ping avec succès entre les réseaux du client UPB connectés directement aux routeurs UPB AKANDJE et UPB YAMOUSSOUKRO .

NB : Les équipements du LAB sont du contructeur CISCO !!!

Ce travail se fera en sept étapes : A FAIRE EN LAB

1/ Mise en place du routage dans le nuage MPLS

Les types de protocoles à utiliser dans le Backbone IP/MPLS sont les protocoles à état de liens car ce sont ces derniers qui sont capables de faire de la commutation de labels. On a le choix entre les protocoles OSPF et IS-IS. Mais pour le cours, nous allons prendre OSPF

Router ospf 1

Net xx.xx.xx.0 0.0.0.255 area 0

saisir la commande précédente au tant de fois qu'il existe de réseau appartenant au domaine ospf y compris les réseaux de bouclage. A noter que tous les réseaux sont en /24 et que nous allons définir le backbone MPLS comme area 0

Sur chaque router backbone

Int loopback 0

Ip ospf network point-to-point

Vérification de OSPF : show ip protocole

2/ Mise en place du protocole de découverte de voisins

Sous chaque interface de routeurs appartenant au réseau cœur MPLS :

Interface fy/e

Mpls ip

Vérification : show mpls ldp neighbor

3/ Configuration de l'authentification des voisins(P ; PE)

Mpls ldp neigbhor @IP_du_voisin password UpbM1S@s2223

4/ Mise en place des VRFs et des interfaces

Ip vrf UPB

Rd 10 :1

Route-target both 10:1

Metrre les interfaces dans les vrf

Interface fj/u

Ip vrf forwarding UPB

Rajouter l'adresse ip de l'interface qui a sauté.

Vérification : show ip vrf

Ping vrf UPB @ip

5/Mise en place du protocole de routage entre CE-PE(au choix : RIP, OSPF, EIGRP, IS-IS, routage statique)

En utilisant RIP version 2

Configuration du protocole de routage Sur les CE

Router rip

Version 2

No auto-summary

Net @IP_réseau_loopbak_CE

Net @IP_réseau_vers_PE

Show ip protocole

PE

Router rip

Version 2

No auto-summary

Address-family ipv4 vrf UPB

Net @ip_réseau_versCE

Show ip route vrf UPB

6/ Mise en place du protocole MP-BGP

Sur les PE ayant les mêmes types de vrf uniquement

Router bgp 1

Neigbhor *router-id-du_PE_distant* remote 1

Neigbhor *router-id-du_PE_distant* update-source lo0

Mode config l3 vpn mpls :

Address-family vpnv4

Neigbhor ***router-id-du_PE_distant*** **activate**

Neigbhor ***router-id-du_PE_distant*** **send-community both**

Verification : show ip bgp neighbor, s'assurer que l'état de voisinage bgp est ESTABLISHED entre les PE concernés sinon veuillez revoir vos configs de l'étape 6/

7/ Redistribution de préfixes

Config à faire UNIQUEMENT sur les routeurs PE

a-Redistribuer les routes apprises par le protocole de routage RIP dans le protocole de routage MP-BGP :

Router bgp 1

Address-family ipv4 vrf UPB

Redistribute rip

b-Redistribuer les routes MP-BGP dans RIP :

Router rip

Address-family ipv4 vrf UPB

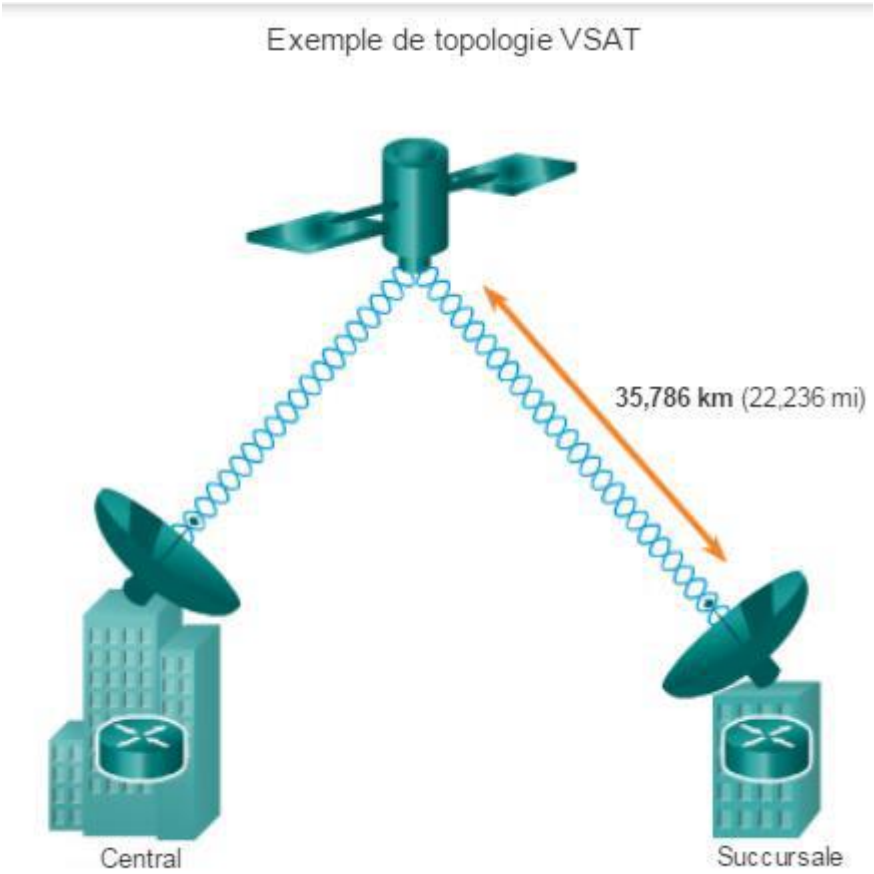
Redistribute bgp 1 metr trans

Vérification : Show ip bgp all

Aussi veuillez faire show ip route sur les routeurs CE et s'assurer que le routeur UPB_AKANDJE voit les réseaux locaux connecté directement au routeur UPB_YAMOUSSOUKRO et vice versa.

9. VSAT

Toutes les technologies WAN privées présentées jusqu'ici utilisent un support en cuivre ou en fibre optique. Comment faire dans le cas où une organisation a besoin d'une connexion dans un endroit isolé où aucun fournisseur de services ne propose de services WAN ?
La technologie VSAT (Very Small Aperture Terminal) est une solution qui utilise les communications satellite pour créer un WAN privé. Un VSAT est une petite antenne satellite similaire à celle utilisée pour Internet ou pour la télévision domestique. Les VSAT créent un WAN privé tout en offrant de la connectivité pour les emplacements distants.
Le routeur se connecte à une antenne satellite dirigée vers le satellite du fournisseur de services qui se trouve en orbite géostationnaire. Les signaux doivent couvrir une distance d'environ 35,786 kilomètres (22,236 miles) pour aller jusqu'au satellite et en revenir.
Dans l'exemple présenté dans la figure ci-dessous l'antenne VSAT sur le toit du bâtiment communique avec un satellite qui se trouve à plusieurs milliers de kilomètres dans l'espace.



10. Cellulaire 4G/5G

Avec la 4G, la connectivité WAN cellulaire a trouvé des applications très probantes en entreprise. Mais, à mesure que la 5G se déploie, cette connectivité sera encore plus attractive du fait de sa vitesse, de sa fiabilité et de son prix. La large disponibilité prochaine de la 5G va améliorer la connectivité WAN des entreprises étendues. Voici comment :

a. Mise en ligne rapide de nouveaux sites

Alors qu'il faut parfois trois mois ou plus pour tirer une connexion MPLS et des semaines pour activer une liaison Internet, le réseau étendu sans fil (Wireless WAN, WWAN) offre une solution très efficace pour mettre rapidement en route une succursale. Une entreprise de services professionnels a remarqué que dès que les employés disposaient de chaises et

de bureaux, le service IT pouvait leur fournir une connexion au WAN de l'entreprise via un tunnel IPsec site à site sur le réseau cellulaire 4G. Cette capacité de connectivité instantanée peut également servir à fournir un accès instantané aux employés relocalisés. Dès qu'il est mis sous tension, le routeur WWAN peut reconnecter un groupe de travail qui a été déplacé d'un immeuble de bureaux à un autre.

b. Le sans-fil, en renfort du filaire

C'est peut-être le cas d'usage le plus connu et la stratégie la plus largement adoptée pour utiliser un Wireless WAN. Les entreprises déplacées en périphérie des centres-villes, où le choix en matière de connectivité est plus réduit, ont adopté le WWAN pour parer aux pannes de connectivité filaire. Si la liaison filaire tombe en panne, la liaison sans fil est mise en service. Là encore, la mise en place reprend le modèle classique du tunnel de connexion vers le WAN. Cependant, la connectivité directe à Internet augmente à mesure de l'adoption du cloud. Plus de la moitié des charges de travail d'une entreprise moyenne sont exécutées dans un cloud ou un autre, au lieu du datacenter de l'entreprise.

c. Supplément de capacité potentielle

Comme pour la bande passante d'urgence, il en va de même pour la capacité supplémentaire. Dans ce scénario, le service cellulaire est établi mais n'est pratiquement pas utilisé, sauf en cas de besoin. Notamment quand des pointes de trafic soutenues entraînent une dégradation des performances de la connexion primaire ou dépassent tout simplement sa capacité..

d. Connexion primaire

Le sans-fil peut également servir de technologie unique pour la connectivité WAN, et remplacer totalement les liaisons câblées traditionnelles. En général, les entreprises ayant opté pour ce cas d'usage avec succès, avaient remplacé des installations en cuivre vieillissantes - lignes DSL, T1, T1

fractionnés, T1 jumelés - et se situaient souvent en dehors des centres urbains et des banlieues où la connectivité filaire est plus rare ou plus chère.

10.1 Avantages et inconvénients

Pour les entreprises qui souhaitent utiliser le WWAN en s'inspirant de l'un ou de plusieurs de ces quatre cas d'usage, les avantages sont clairs et cohérents :

- Disponibilité géographique quasi omniprésente de la 4G/5G, souvent auprès de plusieurs fournisseurs ;

- Accès instantané ;
- Des bandes passantes supérieures à celles de l'ancienne connectivité filaire bas de gamme ;

- Une fiabilité similaire ou supérieure pour les lieux desservis.

10.2 Les inconvénients étaient également cohérents :

- Disponibilité limitée d'un modèle de tarification filaire (un tarif mensuel fixe pour une vitesse déterminée, indépendamment du nombre de bits transmis) ;

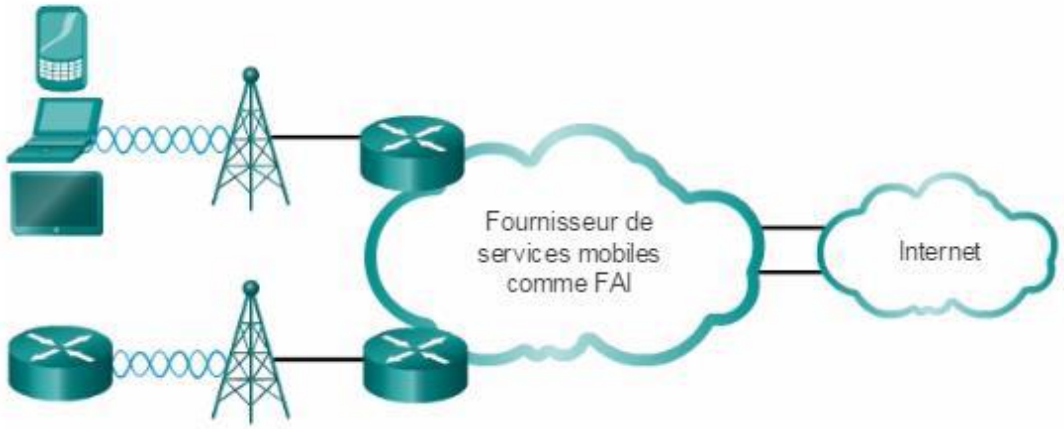
- Coût plus élevé que celui des services filaires remplacés (dans la plupart des cas, le prix par mégabit par seconde a baissé, mais le coût absolu a augmenté) ;

- Problèmes de placement de l'antenne dans certains endroits en raison des matériaux de construction et de l'emplacement des armoires électriques ;

- Nécessité d'éviter les plafonds d'usage et la limitation de vitesse.

10.3 Network slicing et généralisation tarifaire, avec la 5G

Au fur et à mesure de sa généralisation, la 5G apportera des améliorations bienvenues au monde du Wireless WAN. Notamment des vitesses plus élevées et une plus grande fiabilité. Mais une troisième amélioration importante concerne le network slicing ou découpage de réseau, lequel permet aux opérateurs de contrôler la consommation d'un client donné sur une station de base partagée. Avec le network slicing, les opérateurs pourront promettre des capacités aux entreprises clientes et s'y tenir. Au minimum, le découpage de réseau peut contribuer à un usage équitable, en empêchant qu'un client prive les autres clients connectés au même point d'accès. Il peut également séparer la capacité destinée aux entreprises sans fil fixes de la capacité destinée au grand public. Dans chacun des quatre cas d'usage décrits ci-dessus, des vitesses plus élevées, une meilleure fiabilité et des garanties de capacité significatives seront des améliorations bienvenues par rapport à l'état de l'art. Tout aussi important, le découpage du réseau sera essentiel pour généraliser les tarifs, à l'image de ce que font les opérateurs sur le réseau filaire grâce au niveau d'ingénierie du trafic requis pour y parvenir. Du fait d'une tarification équivalente à celle des réseaux câblés et de sa couverture géographique du même niveau que la 4G, le WWAN 5G va devenir une option accessible à la plupart des entreprises, en plus de la connectivité câblée, dans tous les cas d'usage mentionnés ci-dessus.



Architecture 4/5G

11. Solutions VPN

11.1. Définition d'un VPN

Un réseau privé virtuel virtual private network (VPN) étend un réseau privé à travers un réseau public comme l'Internet.

Il permet à un ordinateur d'envoyer et de recevoir des données à travers des réseaux partagés ou publics comme s'ils étaient directement connectés au réseau privé, tout en bénéficiant des fonctionnalités, de la sécurité et des politiques de gestion de ce réseau privé.

Une liaison VPN est créée en établissant une connexion virtuelle point à point sur de véritables connexions physiques par des protocoles de mise en tunnel et/ou de chiffrement du trafic.

Un VPN n'est pas nécessairement "sécurisé", on peut le considérer comme une facilité d'accès (*Virtual Network*) offrant le service d'une "ligne physique privée" (*Private*) (soit pas nécessairement confidentielle ou authentique).

11.2. Avantages

Les technologies VPN permettent de connecter des endroits à travers le monde de manière sécurisée et cohérente.

Aussi, les accès distants pour les utilisateurs mobiles connaissent son succès.

Enfin, les utilisateurs domestiques peuvent utiliser ces technologies pour cacher leur présence sur Internet.

11.3. Catégories

Les VPNs peuvent être dans des modèles :

- à accès distant (remote-access, road-warrior) connectant des individus à un réseau privé, établis à la demande
- site-à-site (site-to-site) connectant deux réseaux en leur bordure

Les systèmes VPN peuvent être classés selon :

- les protocoles utilisés pour la mise en tunnel du trafic
- le point de terminaison du tunnel
- la connectivité “site-to-site” ou “remote-access”
- le niveau de sécurité offert
- la couche OSI présente dans la connexion : des circuits de type L2 ou une connectivité réseau de type L3
- l’usage : WAN privé, WAN public

11.4. VPN non sécurisés

Toute encapsulation peut embarquer un paquet IP. En ce sens, tout protocole, quelle que soit sa couche pourrait servir de protocole de tunnel et servir de facilité VPN non sécurisé (ou sécurisé).

On connait des cas comme ip-in-ip, 6in4, et … GRE pour des protocoles de tunnels à usage en général légitime.

Il est trivial de placer du trafic IP dans des paquets ICMP, DNS ou TLS sur le port 443 qui sont difficilement ou négligemment filtrés par les pare-feu et les proxys en sortie.

11.5. VPN sécurisés

Les technologies VPN peuvent supporter des protocoles et des algorithmes de chiffrement, d'authentification et d'intégrité.

Un modèle de sécurité VPN assure :

- La confidentialité : même si le trafic est capturé, l'attaquant ne verra que du trafic chiffré
- L'authentification de l'émetteur pour empêcher des accès non autorisés
- L'intégrité des messages afin de détecter leur altération

11.6. VPN IPSEC Site-to-Site

Internet Protocol Security (IPsec) a été initialement développé par l'IETF pour IPv6 (quand celui-ci était obligatoire jusqu'au RFC 6434 qui se contente désormais de le recommander).

IPsec est un protocole standard de sécurité largement déployé avec IPv4 et L2TP. Attention, il s'agit d'un "framework" ouvert composé de plusieurs protocoles et supportant divers algorithmes.

Sa conception rencontre les objectifs principaux de la sécurité : authentification, intégrité et confidentialité. IPsec utilise le chiffrement en encapsulant les paquets IP dans un paquet IPsec. Il opère donc à la couche

3. La désencapsulation intervient en bout du tunnel pour rendre le paquet IP original.

11.7. VPN TLS (Remote Access)

Transport Layer Security (TLS) est un protocole de couche applicative qui peut mettre en tunnel le trafic entier d'un réseau ou des connexions individuelles.

On peut aussi lui trouver des fonctionnalités de type "WebVPN". Un grand nombre de fabricants propose des solutions d'accès distants par VPN toutes aussi incompatibles entre elles.

Enfin, un VPN TLS peut se connecter quasiment de n'importe quel endroit

11.8. Autres protocoles VPN sécurisés

- Datagram Transport Layer Security (DTLS) - utilisé par Cisco AnyConnect VPN et par OpenConnect VPN pour résoudre un problème TLS avec les tunnels sur UDP.
- Microsoft Point-to-Point Encryption (MPPE) fonctionnant avec Point-to-Point Tunneling Protocol et d'autres implémentations
- Multi Path Virtual Private Network (MPVPN).
- Secure Shell (SSH) VPN - OpenSSH
- PPTP/L2TP

12. SD-WAN

Historiquement, les applications étaient hébergées au siège de l'entreprise (SAP, email, …). Le WAN était essentiellement utilisé pour connecter les sites distants au siège. Internet était principalement utilisé pour le loisir (email personnel, navigation, …).

Ce modèle commence à évoluer dans les années 2005 – 2010 avec l'arrivée d'application disponibles directement sur Internet comme Salesforce, SAP,etc (« dans le **cloud** »). Les éditeurs de logiciel ont suivi, notamment Microsoft avec Office 365. Les applications ont donc quitté le siège des entreprises pour migrer dans des « Datacenters ». Ces centres de données regroupent des ressources informatiques (serveurs). Les applications sont ainsi accessibles directement depuis n'importe quelle connexion Internet.
La technologie MPLS créée pour répondre aux besoins initiaux (connecter des sites de l'entreprise de manière cloisonnée) n'est donc plus adaptée. Sa complexité dans la mise en place et dans l'utilisation n'arrangent rien. Nous assistons donc à une inéquation entre l'agilité et simplicité des applications dans le Cloud, disponibles facilement, et la rigidité et les limites de cette technologie.
Il existe un réel besoin d'un meilleur moyen d'envoyer le trafic directement sur Internet depuis les succursales vers des applications fiables, SaaS et basées dans le cloud, tout en maintenant la conformité avec les politiques de sécurité des entreprises.

12.1. Qu'est-ce que SD-WAN

SD-WAN, Software Defined WAN, est l'implémentation de SDN, Software Defined Network, dans le domaine des réseaux étendus (WAN).
SD-WAN relève le défis des WAN en étant à la hauteur des exigences des réseaux et des applications de nos jours en étant capable de donner une visibilité sur les applications et en permettant un management centralisé avec des fonctionnalités d'automatisation telles que PnP(Plug and Play) ou ZTP(Zero Touch Provisioning)

12.2. Pourquoi SD-WAN

Les temps changent et les entreprises passent au cloud et au logiciel as a service (SaaS). Si les utilisateurs se connectaient traditionnellement au datacenter de l'entreprise pour accéder aux applications stratégiques, ils bénéficient aujourd'hui d'une meilleure expérience en y accédant depuis le cloud.

Par conséquent, le WAN traditionnel n'est plus adapté, essentiellement à cause de la nécessité de réacheminer le trafic, y compris celui destiné au

cloud, des succursales aux sièges qui engendre des latences et freine les performances des applications et nuit à l'expérience utilisateur et à la productivité. Le SD-WAN simplifie le WAN, réduit les coûts, améliore l'efficacité de la bande passante et offre une bretelle d'accès fluide au cloud avec d'excellentes performances applicatives (surtout pour les applications stratégiques), sans pour autant sacrifier la sécurité et la confidentialité des données. Qui dit meilleures performances applicatives, dit meilleure productivité, meilleure satisfaction client et meilleure rentabilité à terme. En outre, une sécurité homogène limite les risques pour l'entreprise.

12.4. Ce qu'apporte la solution SD-WAN

- Utilisation optimale de la bande passante
- Un SD-WAN utilise une fonction de contrôle centralisée pour diriger le trafic de manière sûre et intelligente à travers le WAN et directement vers les fournisseurs SaaS et IaaS de confiance. Cela permet d'augmenter les performances des applications et d'offrir une expérience utilisateur de haute qualité, ce qui accroît la productivité et l'agilité de l'entreprise et réduit les coûts informatiques.
- Réduire les coûts d'exploitation et de management en passant à une gestion centralisée
- Réduire les coûts des solutions WAN en utilisant des solutions de connectivité Internet et 4G/5G moins chères comme alternative à MPLS
- Nouvelle approche des réseaux professionnels, multi-opérateurs, qui permet de souscrire à la meilleure offre Internet selon la localisation de l'entreprise, et d'en changer simplement. L'entreprise n'est donc plus captive à son opérateur historique, et peut donc faire jouer la concurrence pour optimiser ses coûts. Possibilité d'utiliser plusieurs liaisons pour potentialiser les débits.
- Un SD-WAN garantit des performances et une résilience constantes des applications, automatise l'orientation du trafic en fonction des caractéristiques des applications et des objectifs de l'entreprise, améliore la sécurité du réseau et simplifie l'architecture WAN.
- Contrairement à l'architecture WAN traditionnelle, axée sur le routeur, le modèle du SD-WAN est pensé pour prendre pleinement en charge les applications hébergées sur les datacenters sur site, dans les clouds publics ou privés et dans les services SaaS comme

Salesforce.com, Workday, Dropbox, Microsoft 365 et autres, tout en offrant les meilleurs niveaux de performances applicatives.