Chapitre 2 : Technologies Réseaux

Mots clés : réseaux, réseaux locaux (LAN), réseaux distants (WAN), réseaux sans fils (WIFI, WiMax, …) , Réseaux locaux virtuels (VLAN), Réseaux de stockage (SAN), Réseaux privés virtuels (VPN).

Objectifs de ce chapitre

- Définir les réseaux convergents et les différents défis s'y rapportant
- Décrire comment un modèle hiérarchique est utilisé pour concevoir des réseaux
- Expliquer la fonction des VLANs dans un réseau Local.
- Présenter les réseaux sans fils LAN, MAN et WAN.
- Découvrir les différents types de connexions WAN.
- Découvrir les technologies VPN.
- Comprendre les réseaux de stockage SAN.

Introduction

Un réseau informatique se compose de deux ordinateurs ou plus qui sont interconnectés les uns avec les autres et partagent des ressources telles que des imprimantes, des serveurs et du matériel et échangent les données sous la forme de fichiers, facilitant la communication électronique. Les ordinateurs sur un réseau peuvent être connectés par des câbles à paire torsadée, des lignes téléphoniques, des ondes radio, des satellites ou des câbles à fibres optiques. Le premier réseau informatique conçu était le «Réseau d'agence de projets de recherche avancée (ARPANET) par le Département de la défense des États-Unis. Depuis, plusieurs myriades de nouvelles technologies de réseau informatique ont été conçues.

2.1.Réseaux convergés

Notre monde numérique change. L'accès à Internet et au réseau d'entreprise n'est plus limité aux bureaux physiques, aux sites géographiques... Dans l'environnement de travail mondialisé d'aujourd'hui, les employés peuvent accéder à des ressources partout dans le monde et les informations doivent être disponibles à tout moment et sur tout périphérique ce qui nécessite l'élaboration de réseaux de nouvelle génération : sécurisés, fiables et hautement disponibles.

2.1.1.Principe

Les réseaux modernes évoluent constamment pour répondre aux demandes des utilisateurs. Les premiers réseaux de données se limitaient à échanger des informations basées sur les caractères entre les systèmes informatiques. Les réseaux traditionnels de téléphonie, de radio et de télévision ont été maintenus séparément des réseaux de données. Dans le passé, chacun de ces services nécessitait un réseau dédié, avec différents canaux de communication et différentes technologies pour transporter un signal de communication particulier. Chaque service avait son propre ensemble de règles et de normes pour assurer une communication réussie.

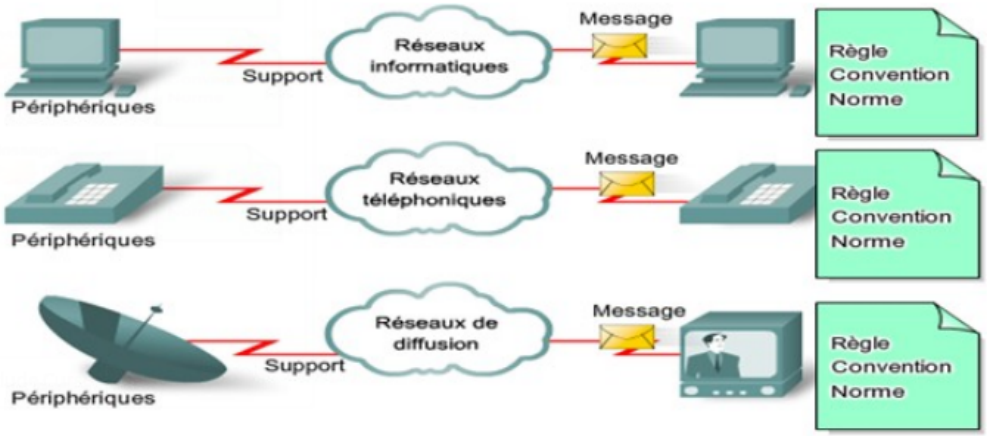

Figure 2.1. Réseaux multiples

Les progrès de la technologie permet de consolider ces différents types de réseaux sur une plate-forme appelée «**réseau convergé**». Contrairement aux réseaux dédiés, les réseaux convergents sont capables de fournir des flux vocaux, vidéo, textuels et graphiques entre différents types de dispositifs sur le même canal de communication et la structure du réseau, comme le montre la Figure 2.2.

Sur un réseau convergé, il existe de nombreux points de contact et de nombreux périphériques tels que les ordinateurs personnels, les téléphones, les téléviseurs et les tablettes, mais il existe une

infrastructure réseau commune. Cette infrastructure de réseau utilise le même ensemble de règles, d'accords et de normes de mise en œuvre.

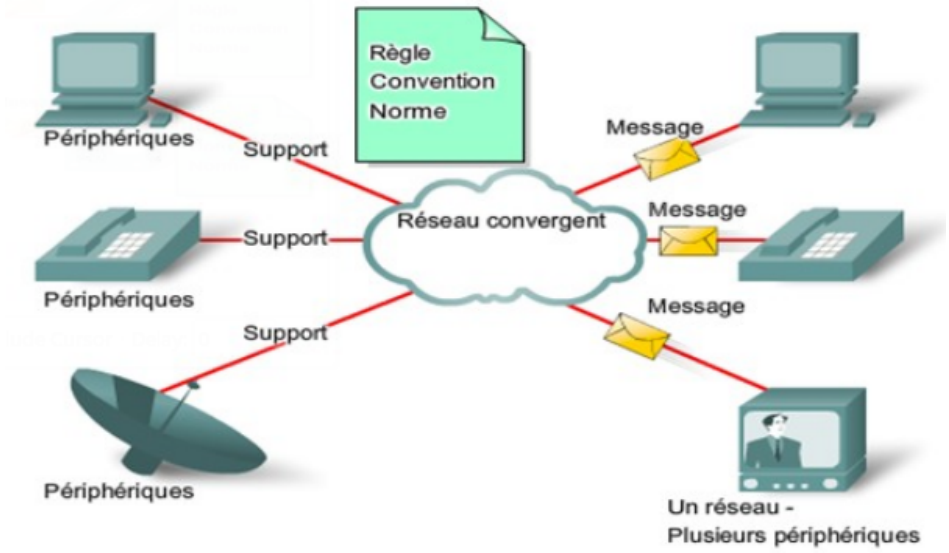

Figure 2.2.

Réseaux convergents

<u>Convergence du réseau</u> : est la coexistence efficace du téléphone, de la vidéo et de la communication de données dans un seul réseau afin d'offrir une meilleure flexibilité.

2.2.2. Challenges et défis des réseaux convergés

À mesure que la convergence des réseaux évolue, plusieurs défis et problèmes émergent :

- La demande de bande passante est le plus important défis des réseaux convergents car les applications et services exigent un réseau unique.
- Les réseaux convergents comprennent un mélange de plates-formes informatiques, de protocoles, de périphériques et de topologies de réseau. Ainsi différentes normes, types de communications, protocoles de système de fichiers et bus d'interface existent.
- Les problèmes liés aux partage du réseau. Dans un environnement convergé, le trafic de données, de voix, de vidéos et de stockage se combinera, ce qui va influencer sur les performances du réseau.
- La convergence du réseau va réduire la QoS (qualité de service) ce qui va réduire l'utilisation de la bande passante pour des applications en temps réel.
- Les réseaux de données utilisent traditionnellement le protocole Spanning Tree pour connecter les commutateurs, mais Spanning Tree ouvre trop de connexions dans un réseau convergé, ce qui va congestionner le réseau.

2.2.3. Composants d'un réseau

L'infrastructure réseau généralement comprend trois catégories de composant réseau :

2.2.3.1. Les périphériques

Les périphériques représentent les éléments physiques, ou le matériel, du réseau. Le matériel correspond souvent aux composants de la plateforme réseau, par exemple un ordinateur portable, un ordinateur de bureau, un commutateur, un routeur, un point d'accès sans fil ou le câblage qui sert à relier les périphériques. On retrouve principalement deux types de périphériques :

1) Périphériques finaux : les périphériques réseau auxquels les gens sont le plus habitués sont appelés périphériques finaux, ou hôtes. Ces périphériques forment l'interface entre les utilisateurs et le réseau de communication sous-jacent. Exemples : Ordinateurs (stations de travail, ordinateurs portables, serveurs de fichiers, serveurs Web), imprimantes réseau, caméras de surveillance, appareils mobiles, …

2) Périphériques de réseau intermédiaires : les périphériques intermédiaires relient des périphériques finaux. Ils offrent une connectivité et opèrent en arrière-plan pour s'assurer que les données sont transmises sur le réseau. Par exemple : périphériques d'accès au réseau (commutateurs et points d'accès sans fil), routeurs, pare-feu, …

2.2.3.2. Les supports de communication

La communication à travers un réseau s'effectue sur un support. Ce support fournit le canal via lequel les données sont envoyées de la source à la destination. Il existe principalement trois types de supports pour interconnecter des périphériques. Ce sont : fils métalliques dans des câbles (paires torsadées, câble coaxial), fibres de verre ou optiques, transmission sans fil.

2.2.3.3. Les services

Les composants réseau sont utilisés pour fournir des services et des processus. Les services et les processus sont les programmes de communication, qui sont exécutés sur les périphériques réseau. Un service réseau fournit des informations en réponse à une demande. Les services incluent de nombreuses applications réseau courantes utilisées quotidiennement, comme les services d'hébergement de messagerie et les services d'hébergement Web.

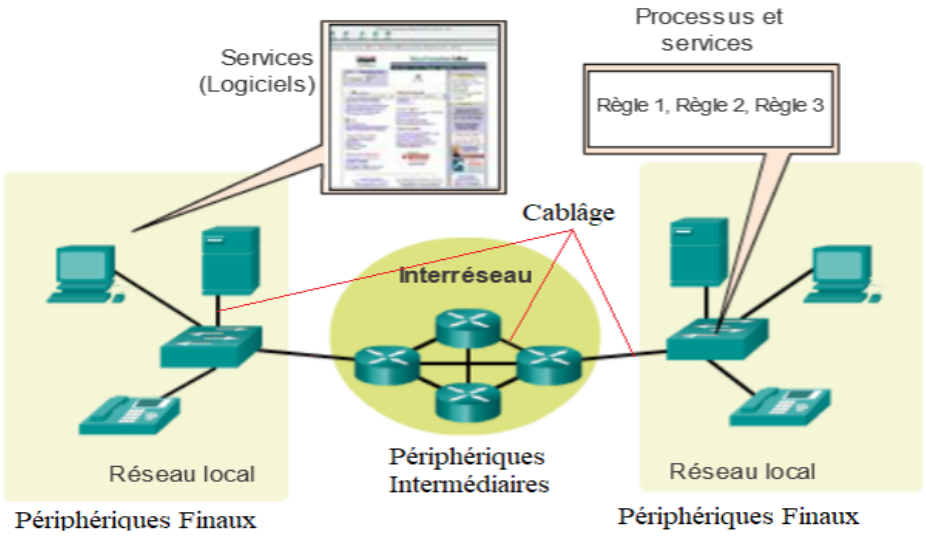

Figure 2.3. Composants d'un réseau

2.1.4. Caractéristiques des architectures réseau

1) Disponibilité

La disponibilité désigne la probabilité qu'un réseau soit en bon état de fonctionnement à un instant donné.

L'objectif pour qu'un réseau soit toujours disponible nécessite une architecture réseau conçue pour être tolérante aux pannes. Un réseau tolérant aux pannes est un réseau qui limite l'impact des pannes, de sorte que le plus petit nombre de périphériques possible soit affecté par ces dernières.

$$Disponibilité\,(\%) = \frac{Temps\ \ de\ \ disponibilité}{Temps\ \ de\ \ fontionnement\ \ total}$$

2) Fiabilité

La fiabilité fait référence à la probabilité générale d'une défaillance dans un système en cours d'exécution. Elle désigne la capacité du réseau soit en fonctionnement sur une période données (accomplir ses fonctions).

$$Fiabilité\,(heures) = \frac{Temps\ \ de\ \ disponibilité}{Nombre\ \ de\ \ défaillances}$$

3) Évolutivité (Scalabilité)

L'évolutivité désigne la capacité du réseau à évoluer afin de satisfaire les exigences de performances croissantes. Un réseau évolutif doit être en mesure de s'étendre rapidement afin de prendre en charge de nouveaux utilisateurs et applications sans que cela n'affecte les performances du service fourni aux utilisateurs existants.

4) Interopérabilité

L'interopérabilité est définie comme la capacité de différents types d'ordinateurs, de réseaux, de systèmes d'exploitation et d'applications à travailler ensemble efficacement, sans communication préalable, afin d'échanger des informations de manière utile et significative.

5) Qualité de service

La qualité de service (QS) est une exigence de plus en plus répandue qui repose sur les réseaux actuels. Elle correspond à la capacité du réeau à répondre aux différents besoins attendus. Les applications disponibles via des réseaux, telles que les applications de communication vocale et vidéo , entraînent des attentes plus poussées en termes de qualité des services fournis.

6) Sécurité

L'infrastructure réseau, les services et les données contenus dans les périphériques reliés au réseau sont des ressources personnelles et professionnelles essentielles. Compromettre l'intégrité de ces ressources pourrait avoir de graves conséquences. Pour cela deux aspects de la sécurité réseau doivent être pris en compte : la sécurité de l'infrastructure réseau et la protection des données.

2.1.5. Types de réseau

Les infrastructures réseau peuvent considérablement varier selon :

- la taille de la zone couverte ;
- le nombre d'utilisateurs connectés ;
- le nombre et les types de service disponibles.

Les types les plus courants d'infrastructure réseau sont :

- ***Réseau local (LAN) :*** infrastructure réseau permettant d'accéder aux périphériques finaux et aux utilisateurs sur une zone locale (limitée géographiquement).

- ***Réseau étendu (WAN) :*** infrastructure réseau permettant d'accéder à d'autres réseaux sur une vaste zone (étendue).
- ***Réseau métropolitain (MAN) :*** infrastructure réseau qui couvre une zone plus vaste qu'un LAN, mais moins étendue qu'un WAN (par exemple, une ville).
- ***LAN sans fil (WLAN) :*** infrastructure similaire à un réseau local, mais sans fil. Elle relie des utilisateurs et des terminaux situés dans une zone peu étendue.
- ***Réseau de stockage SAN :*** infrastructure réseau conçue pour prendre en charge des serveurs de fichiers et pour fournir des fonctionnalités de stockage, de récupération et de réplication de données. Cette infrastructure comprend des serveurs haut de gamme, plusieurs baies de disques et utilise la technologie d'interconnexion Fibre Channel.

2.2. Technologies filaires et sans fils LAN/MAN

2.2.1. Présentation des LAN et MAN

1) LAN

Un réseau local (LAN) est un réseau qui est limité à des zones géographiques petites, par exemple un bureau local, une école ou une maison. Environ tous les LAN actuels, qu'ils soient câblés ou sans fil, sont basés sur Ethernet. Les vitesses de transfert de données «réseau local» sont supérieures à WAN et à MAN qui peuvent s'étendre de 10,0 Mbps (réseau Ethernet) et à 10,0 Gbit / s (Gigabit Ethernet).

Les réseaux LAN peuvent être mis en œuvre de multiples façons, par exemple des câbles à paire torsadée et un Wi-Fi.

Les fonctionnalités offertes par les LAN sont :

- Les LAN relient des périphériques finaux dans une zone limitée telle qu'une maison, une école, un bureau ou un campus.
- En général, un réseau local est administré par une seule entreprise ou une seule personne.
- Le réseau local fournit une bande passante très élevée aux périphériques finaux et aux périphériques intermédiaires internes.

2) MAN

Un réseau de zone métropolitaine (MAN) est un réseau qui connecte plusieurs périphériques ou réseaux dans un seul réseau qui a une zone géographique plus grande que celle couverte par un «réseau local» mais plus petit que la région couverte par un « réseau étendu ».

Un réseau métropolitain regroupe un certain nombre de «réseaux locaux» avec des liaisons fibre optique qui servent de base et fournit des services similaires à ce que le fournisseur de services Internet (ISP) fournit aux réseaux étendus.

Les principales technologies utilisées dans les réseaux MAN sont «ATM», «FDDI» et «Switched Multi-megabit Data Service (SMDS». Dans la plupart des cas, ces technologies sont utilisées pour remplacer les simples connexions «Ethernet».

2.2.2. Architecture Hiérarchique LAN

2.2.2.1. Principes de conception

La création d'un réseau hiérarchique exige l'utilisation de principes de conception de réseaux robustes, pour assurer une disponibilité, une sécurité et une facilité de gestion. Le réseau doit pouvoir répondre aux besoins actuels et prendre en charge les services et technologies ultérieurement requis. Les directives de conception de réseaux reposent sur les principes suivants :

- ***Hiérarchie :*** faciliter la compréhension du rôle de chaque périphérique à chaque niveau, simplifier le déploiement, l'exploitation et la gestion, tout en réduisant les domaines défaillants à chaque niveau
- ***Modularité :*** permettre l'extension transparente du réseau et l'activation de services intégrés à la demande
- ***Résilience :*** assurer que le réseau reste toujours actif, pour répondre aux attentes des utilisateurs
- ***Flexibilité :*** utiliser toutes les ressources du réseau, afin de répartir avec intelligence la charge de trafic

2.2.2.2. Modèle à trois couches

La conception hiérarchisée d'un réseau représente une base sur laquelle repose les concepteurs réseaux pour représenter leurs réseaux. Un réseau hiérarchique se base sur la structure de niveaux. Chaque niveau hiérarchique permet d'assurer des fonctions et rôles spécifiques dans le réseau. Parmi ces modèles, on retrouve le modèle à trois couches.

Ce modèle est composé de trois niveaux principaux : accès, distribution, cœur de réseau.

1) Couche d'accès : elle constitue la périphérie du réseau, où le trafic entre dans le réseau et en sort. Généralement, un commutateur de couche d'accès a pour fonction principale de fournir à l'utilisateur un accès au réseau. Les commutateurs de couche d'accès se connectent aux commutateurs de la couche de distribution.

2) Couche de distribution : elle établit l'interface entre la couche d'accès et la couche cœur de réseau pour fournir de nombreuses fonctions, telles que : regroupement de réseaux, fonctions intelligentes de commutation, haute disponibilité à travers la redondance, ...

3) Couche cœur de réseau : elle sert de réseau fédérateur et connecte plusieurs couches du réseau. Elle a pour objectif principal d'assurer l'isolation des défaillances et la connectivité haut débit du réseau fédérateur.

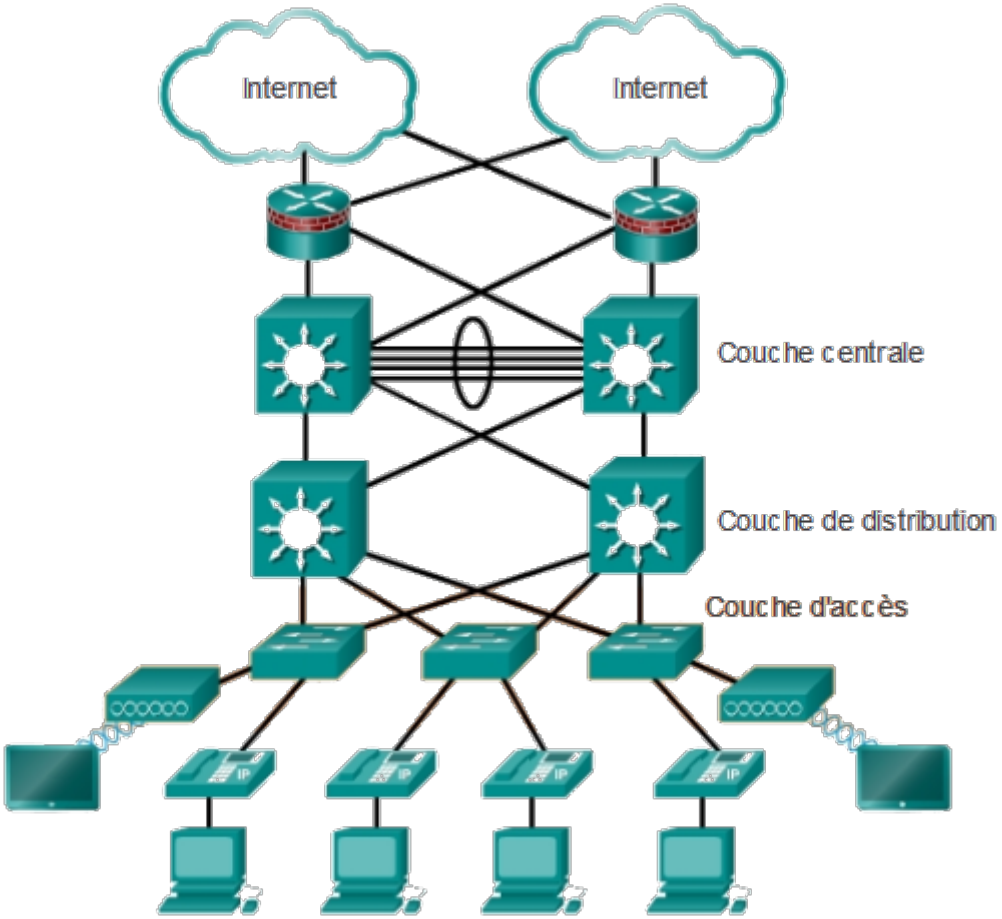

Figure 2.4. Modèle à trois niveaux

2.2.2.3. Modèle à deux couches

Dans le modèle à trois couches, les couches d'accès, de distribution et de cœur de réseau sont distinctes. Mais dans certains cas, en l'absence de restrictions physiques ou d'exigences d'évolutivité du réseau, il est inutile de séparer la couche de distribution et la couche cœur de réseau. Sur les sites comptant un seul bâtiment ou un nombre relativement réduit d'utilisateurs accédant au réseau, il n'est pas forcément nécessaire de séparer la couche cœur de réseau et la couche de distribution. Dans ce cas, on utilise un modèle à deux niveaux, également appelé conception réseau réduite.

La figure s suivante présente un exemple de conception d'un réseau LAN/MAN à deux niveaux, où les couches de distribution et cœur de réseau sont regroupées en une seule couche.

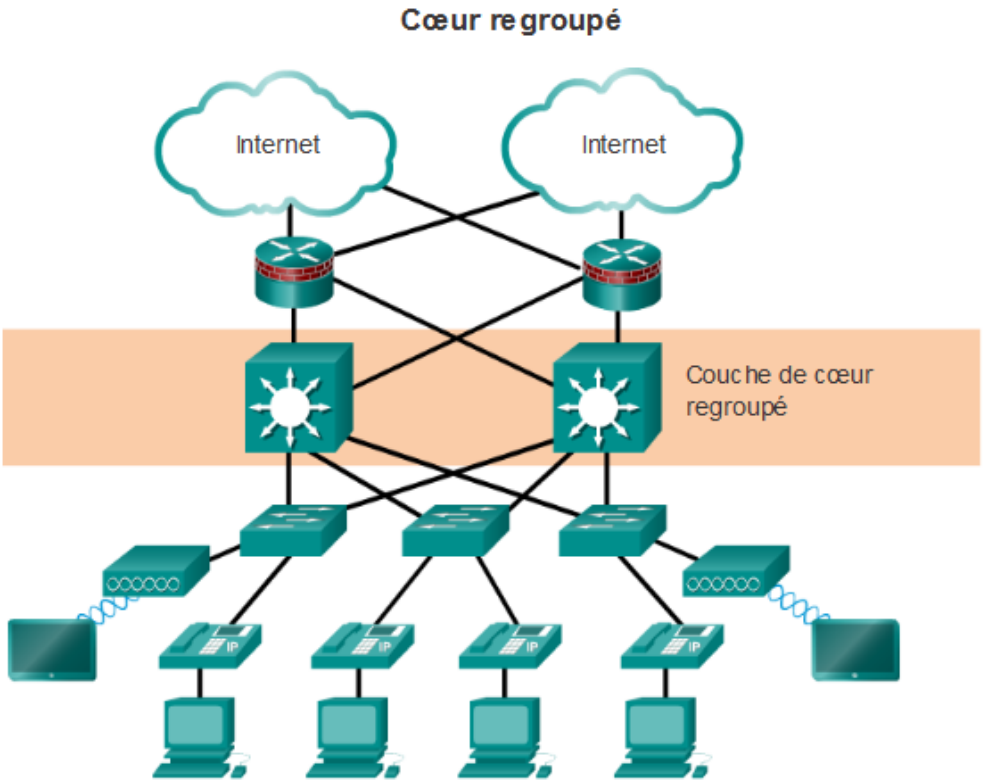

Figure 2.5. Modèle à deux niveau

2.2.3. Réseaux locaux virtuels (VLANs)

La performance réseau constitue un facteur important dans la productivité d'une entreprise. L'une des technologies permettant des les améliorer consiste à diviser de vastes domaines de diffusion en domaines plus petits. Par définition, les routeurs bloquent le trafic de diffusion à une interface. Cependant, ils possèdent en général un nombre restreint d'interfaces LAN. Le rôle principal d'un routeur est de déplacer les données entre les réseaux, pas de fournir l'accès réseau aux périphériques finaux.

La fourniture d'un accès au LAN est un rôle généralement réservé au commutateur de la couche d'accès. Un réseau local virtuel (VLAN) peut être créé sur un commutateur de couche 2 pour réduire la taille des domaines de diffusion, de sorte qu'elle soit équivalente à celle d'un périphérique de couche 3.

2.2.3.1. Principe

Les VLANs sont implémentés dans le niveau 2 du modèle OSI c'est à dire dans la couche liaison de données. Ils permettent de segmenter les réseaux en différent domaines de diffusion, et ainsi ils permettent de segmenter un support physique en segments logiques.

Les VLANs aident à organiser les réseaux selon :

- Localisation Physique (Exemple : Bâtiment)
- Organisation (Exemple : Dept. Marketing)
- Fonction (Exemple : Personnel)

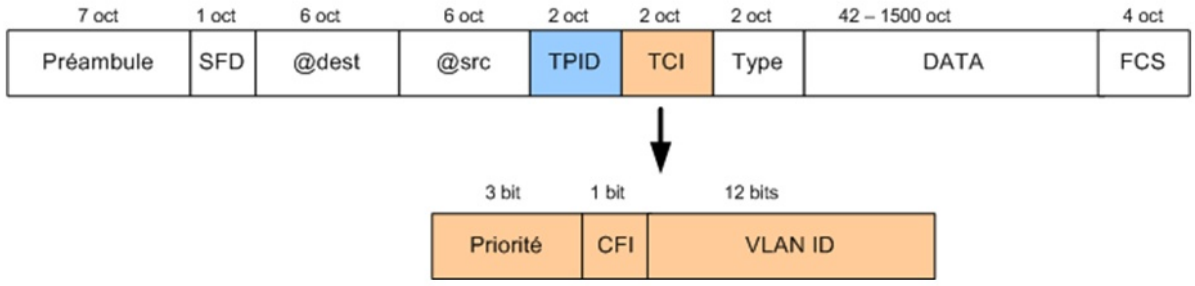

Figure 2.6. Trame Ethernet avec VLAN

2.2.3.2. Avantages

Les principaux avantages des VLAN sont les suivants :

- Sécurité.
- Réduction des coûts.
- Meilleures performances.
- Réduction des domaines de diffusion.
- Efficacité accrue du personnel informatique.
- Gestion simplifiée de projets et d'applications.

2.2.3.4. Méthodes d'implémentation

Il existe principalement deux méthodes d'implémentation des VLANs à savoir :

1) VLANs statiques : appelés aussi « port-bases »consiste à implémenter un VLAN de façon statique. Ce type de configuration nécessite une implémentation manuelle mais elle est facile à réaliser.

2) VLANs dynamiques : dans ce cas l'attribution d'un VLAN se fait dynamiquement sur la base d'une adresse physique (MAC), logique (IP) ou de crédits quelconques… Ce type d'implémentation est plus coûteuse

2.2.3.5. Types de VLANs

On peut trouver plusieurs types de VLANs. Ces types sont définis selon la méthode d'implémentation d'un VLAN, parmi ces types on peut citer :

1) VLAN par port : Chaque VLAN est implémenté sur un port différent. Ce type de VLAN est le plus simple à réaliser et s'implémente de façon statique.

2) VLAN par adresse MAC : dans ce type de VLAN, un VLAN est défini par un ensemble d'adresse MAC. Généralement ce type de VLAN est implémenté dynamiquement.

3) VLAN par adresse IP : pour ce type de VLAN, une plage d'adresses IP caractérise un VLAN. Généralement ce type de VLAN est implémenté dynamiquement.

4) VLAN par protocole de niveau 3 : dans ce type de VLAN, un VLAN est définit par un protocole de communication spécifique, et tous les clients qui utilisent le même protocole sont regroupés dans un même VLAN. La aussi l'implémentation du VLAN se fait dynamiquement.

2.2.4. Technologies LAN/MAN sans fils

Les réseaux sans fil apportent des modifications essentielles au réseau. Un réseau sans fil regroupe deux ou plus de deux ordinateurs au moyen d'une communication sans fils. Les réseaux sans fils offrent la possibilité à un utilisateur de se déplacer dans une vaste zone de couverture et toujours associé au réseau.

2.2.4.1. Types de réseaux sans fil

Il existe différents types de réseaux sans fil tels que le réseau étendu (WWAN), le réseau métropolitain (WMAN), le réseau local (WLAN) et le réseau de zones personnelles (WPAN).
WLAN (réseau local sans fil)

1) Le WLAN (Réseau local sans fils) : fournit une connexion réseau sans fil à l'aide du signal radio au lieu du câblage réseau traditionnel en passant par un périphérique appelé AP (Access Point – Point d'accs). Les WLAN ont plusieurs avantages telles que la couverture, le débit, l'interopérabilité avec l'infrastructure filaire, la simplicité et la facilité d'utilisation, le coût, l'évolutivité, ...

2) Le WMAN (Réseau métropolitain sans fil) : Les communications sans fils dans un réseau métropolitain s'appellent WMAN. Un WMAN est conçu pour une plus grande zone géographique qu'un LAN. Il est mis en place dans une ville entière ou une zone géographique pouvant atteindre jusqu'à 50 km.

2.2.4.2. Technologies WLAN/WMAN

Au fur et à mesure que diverses technologies de réseau sans fil ont avancé au fil du temps, plusieurs technologies WLAN et WMAN ont émergé, mais les principales technologies pour les réseaux locaux et métroplolitains sans fils est le WiFi et le WiMAX.

1) Wi-Fi pour les WLAN : qui signifie ***Wireless Fidelity*** est basé sur la famille de normes IEEE 802.11 et est principalement une technologie de réseau local (LAN) conçue pour fournir une couverture large bande.

Les systèmes WiFi actuels prennent en charge un taux de transmission de la couche physique maximale de 54 Mbps.

La norme 802.11 est définie par plusieurs spécifications de WLAN. Il existe plusieurs spécifications dans la famille 802.11 telles que :

- 802.11 : fournit une transmission de 1 ou 2 Mbps dans la bande de 2,4 GHz.
- 802.11a : Il s'agit d'une extension à 802.11 qui concerne les réseaux locaux sans fil et va jusqu'à 54 Mbps dans la bande de 5 GHz.
- 802.11b : Le WiFi à haut débit 802.11b est une extension à 802.11 qui se rapporte aux LAN sans fil et produit une connexion aussi rapide que la transmission 11 Mbps (avec un repli à 5.5, 2 et 1 Mbps en fonction de la puissance du signal) dans le 2.4- GHz.
- 802.11g : Cela concerne les réseaux locaux sans fil et fournit 20 + Mbps dans la bande 2,4 GHz.

On distingue 4 types de topologies WiFi :

- **Infrastructure (AP) :** ce type de topologie se base sur l'utilisation d'un point d'accès (AP) pour connecter le réseau. On retrouve deux types de topologies d'infrastructures :

  a) BSS (Basic Service Set) : qui utilise un seul AP.

  b) ESS (Extended Service Set) : qui utilise plusieurs APs.
- **Ad-hoc (P2P) :** ce type de topologies se base sur une connexion directe entre les périphériques sans fils sans l'utilisation d'un AP. Cette topologie est appelée ***IBSS (Independent BSS).***

- **Répéteur (repeater) :** ce base sur l'utilisation d'un AP qui regénère le signal à partir d'un autre point d'accès.
- **Pont (bridge) :** ce type de topologie consiste à étendre un réseau filaire par l'utilisation d'un AP.

Les problèmes et vulnérabilités qui existent pour la technologie Wi-Fi sont les suivants :

- Sécurité.
- Compatibilité et interopérabilité.
- Problèmes de facturation

2) WiMAX pour les WMAN : qui signifie ***Worldwide Interoperability for Microwave Access*** est une famille de normes de communication sans fil basées sur la norme IEEE 802.16.

Concrètement, le WiMAX fonctionne de manière similaire à WiFi, mais à des vitesses plus élevées, sur de plus grandes distances et pour un plus grand nombre d'utilisateurs. Un système WiMAX se compose de deux parties:

- Une tour WiMAX, de conception similaire à une tour de téléphone cellulaire - Une seule tour WiMAX peut fournir une couverture dans une très grande surface - jusqu'à 8 000 km carrés.
- Un récepteur WiMAX, le récepteur ou antenne WiMAX peut être une petite boîte ou une carte PCI ou peut être intégrés dans un ordinateur portable de la même façon du WiFi.

Les problèmes et défis qui existent pour la technologie WiMAX sont :

- Interférence et atténuation des fréquences radios.
- Conflit de l'opérateur pour le placement d'infrastructure pour maximiser les performances et la portée.
- Réglementation gouvernementale, gestion des licences spectrales et utilisation.
- Préoccupations concernant la croissance du marché de la station de base WiMax en raison de la partialité vers les réseaux vocaux

2.3. Technologies filaires et sans fils WAN

Un WAN est un réseau de communication de données qui couvre une zone géographique relativement large. Les technologies WAN fonctionnent généralement sur les trois couches inférieures du modèle de référence OSI : la couche physique, la couche de liaison de données et la couche réseau.

2.3.1. Types de connexions WAN

De nombreux réseaux WAN sont construits pour une organisation particulière et sont privées. D'autres, construits par des fournisseurs de services Internet, fournissent des connexions à Internet. Plusieurs options sont disponibles pour la connectivité WAN telles que les lignes louées, la commutation de circuit, la commutation de paquets, la commutation de cellule, l'ADSL, ...

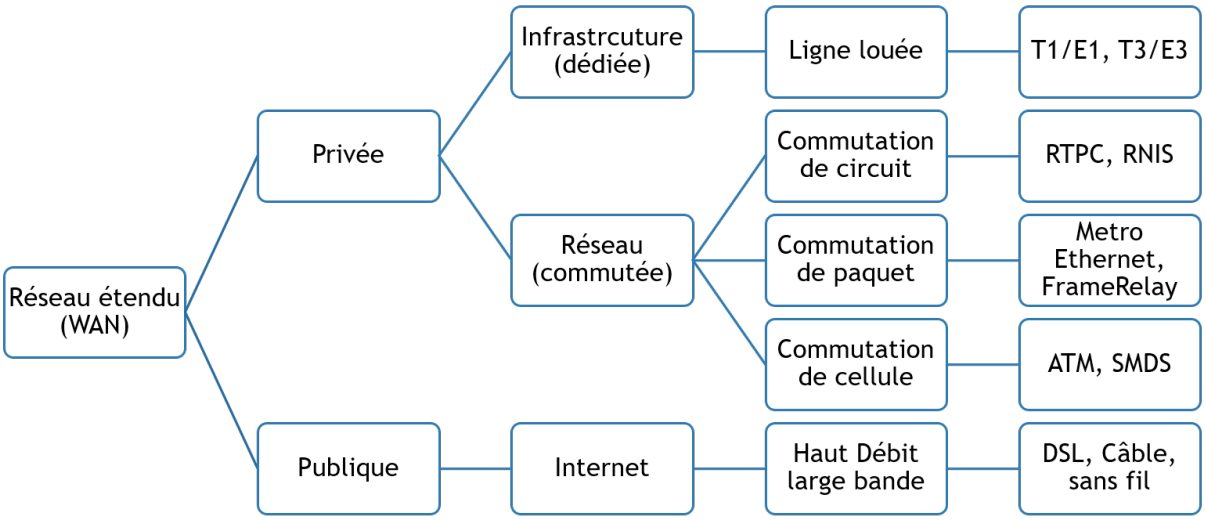

Figure 2.7. Types de connexions WAN

1) Ligne louée : Les WAN sont souvent construits à l'aide de lignes louées ou lignes spécialisées. Ces lignes louées impliquent une connexion directe point-à-point entre deux sites. Les lignes louées sont des lignes téléphoniques numériques qui permettent une transmission sécurisée et ininterrompue à des coûts fixes. À chaque extrémité de la ligne louée, un routeur se connecte au LAN d'un côté et à un hub dans le WAN de l'autre. Les lignes louées peuvent être très coûteuses à long terme.

2) Commutation de circuit : Au lieu d'utiliser des lignes louées, les WAN peuvent être construits à l'aide de la commutation de circuit. "Dans les télécommunications, un réseau de commutation de circuit établit un circuit (ou un canal) entre les nœuds et les terminaux avant que les utilisateurs ne puissent communiquer, comme si les nœuds étaient physiquement connectés avec un circuit électrique". Un exemple de commutation à circuit est le réseau RNIS.

3) Commutation de paquets : La commutation par paquets est une méthode qui regroupe toutes les données transmises ensemble de paquets. Les paquets sont ensuite transmis sur un réseau partagé. Similaire à la commutation de circuit, la commutation de paquets est relativement peu coûteuse.

4) Commutation de cellule : Le commutation de cellule est similaire à la commutation de paquets, mais utilise des cellules de longueur fixe au lieu de paquets de longueur variable. Les données sont divisées en ces cellules puis transportées sur des circuits virtuels. Cette méthode est la meilleure pour la voix et les données simultanées, mais peut causer des frais généraux considérables.

5) Haut débit large bande : représente les connexions publique généralement à travers Internet. Il existe plusieurs technologies pour ce types de WAN telles que : ADSL, le câble ou encore les connexions sans fils.

2.3.2. Facteurs à considérer lors de la sélection d'une connexion WAN

Il existe de nombreux facteurs importants à prendre en compte lors du choix d'une connexion WAN appropriée. Pour pouvoir décider quelle technologie WAN répond le mieux aux exigences de d'une activité spécifique, on doit considérer les facteurs suivants :

- L'objectif du réseau WAN.
- Portée et distance géographique (local, régional ou mondial).

- Transmission (type du trafic, volume du trafic, qualité de service).
- Sécurité.
- Type d'infrastructure (privée ou publique).
- Types de connexions disponibles.
- Coût.

2.3.3. Réseaux virtuels privés

Les entreprises ont besoin de moyens à la fois sécurisés, fiables et économiques permettant d'interconnecter plusieurs réseaux. Pour cela, les entreprises utilisent des technologies VPN pour créer une connexion sécurisée de bout en bout par réseau privé sur des réseaux tiers, comme Internet ou des extranets. Le tunnel supprime la barrière de distance et permet aux utilisateurs distants d'accéder aux ressources réseau du site central.

Un VPN est un réseau privé créé par tunneling sur un réseau public, généralement Internet. Les premiers VPN étaient exclusivement des tunnels IP qui n'incluaient ni l'authentification ni le chiffrement des données. Par exemple, le protocole GRE. À l'heure actuelle, l'implémentation sécurisée de VPN avec chiffrement, tels que des VPN Ipsec, Linux OpenVPN, … , est ce qu'on entend habituellement par une mise en réseau privé virtuel.
Les avantages d'un VPN sont les suivants :

- Réductions des coûts.
- Évolutivité.
- Compatibilité avec la technologie haut débit.
- Sécurité.

Il existe deux types de réseaux privés virtuels :

1) VPN de site à site : Un VPN de site à site est créé lorsque les périphériques situés des deux côtés de la connexion VPN connaissent par avance la configuration VPN. Le VPN reste statique et les hôtes internes ne savent pas qu'un VPN existe. Dans un VPN de site à site, les hôtes finaux envoient et reçoivent le trafic TCP/IP normal par l'intermédiaire d'une « passerelle » VPN. La passerelle VPN est responsable de l'encapsulation et du chiffrement de la totalité du trafic sortant issu d'un site spécifique.

2) VPN d'accès à distance : Un VPN d'accès à distance est créé lorsque les informations sur le VPN ne sont pas configurées de manière statique, mais de façon dynamique. Les VPN d'accès à distance prennent en charge une architecture client-serveur, dans laquelle le client VPN (hôte distant) obtient un accès sécurisé au réseau de l'entreprise par l'intermédiaire d'un périphérique de serveur VPN à la périphérie du réseau. Les VPN d'accès à distance sont utilisés pour la connexion d'hôtes individuels devant accéder en toute sécurité au réseau de leur entreprise via Internet.

2.3.4. Sécurité pour les réseaux étendus

Au cours des dernières années, les problèmes de sécurité sont devenues fréquents dans les réseaux étendus. On retrouve parmi les solutions de sécurité dans les réseaux WAN les technologies et les processus de sécurité suivants:

1) Défense en profondeur : un concept fondamental de la conception de la sécurité est une défense en profondeur dans laquelle de multiples couches de sécurité sont utilisées pour protéger les actifs. Si une couche de sécurité est compromise, d'autres sont encore en place pour fournir une protection. Ce principe est appliqué aux actifs physiques ainsi qu'aux ressources réseau et aux données.

2) Pare-feux (Firewalls) : Les pare-feu protègent le réseau d'entreprise et les ordinateurs individuels des attaques basées sur le réseau. Ils constituent la base de la technologie de sécurité réseau. Le pare-feu filtre les paquets de données qui se déplacent d'un réseau à l'autre selon des règles.

3) Systèmes de détection et de prévention des intrusions : un système de détection d'intrusion est semblable à un pare-feu car il surveille le trafic réseau. Il utilise des capteurs (qui peuvent être du matériel ou des logiciels) placés sur des ordinateurs ou à des emplacements clés sur le réseau pour détecter une activité non autorisée ou suspecte et alerter les administrateurs réseau en temps réel. Un système de prévention des intrusions est un système de détection d'intrusion qui peut également prendre des mesures pour arrêter le trafic malveillant ou la violation de sécurité au fur et à mesure qu'il se produit.

4) Logiciel antivirus : le logiciel Antivirus protège les données et les fichiers sur les ordinateurs et les serveurs en essayant de détecter, mettre en quarantaine et supprimer les logiciels malveillants. Il fonctionne en continu sur l'ordinateur et utilise des définitions de modèles de virus pour rechercher des signatures de virus dans les fichiers. Si une correspondance de signature de virus est trouvée, le logiciel met en quarantaine ou supprime le fichier, tente de supprimer le virus ou empêche le fichier d'être ouvert ou exécuté.

5) Chiffrement : le cryptage convertit l'information lisible en un format chiffré. Les données cryptées ne valent pas pour un attaquant si l'attaquant ne peut pas le déchiffrer. Les deux formes de cryptage basiques sont la cryptographie symétrique et asymétrique. Pour le cryptage symétrique, la même clé est utilisée pour crypter et décrypter les données, de sorte que la clé confidentielle doit être partagée en toute sécurité avec ceux qui ont besoin de décrypter les données. Le cryptage asymétrique, également appelé cryptage à clé publique, utilise différentes clés pour le cryptage et le décryptage. Le destinataire de données crée une clé privée, qui n'est pas partagée, et une clé publique. La clé publique (non confidentielle) est fournie aux expéditeurs de données pour chiffrer leurs informations. Le destinataire de données utilise la clé privée pour décrypter les informations.

2.3.5. Technologies WAN sans fils

2.3.5.1. WAN sans fil cellulaires

Un système cellulaire se compose de tours de cellules, de concentrateurs, de commutateurs vocaux et de passerelles de données. La tour de cellule reçoit des signaux provenant de périphériques utilisateurs et transmet les informations à l'utilisateur. Le commutateur vocal relie le périphérique utilisateur à un autre utilisateur sans fil via le système de distribution téléphonique. Il existe plusieurs générations de technologies WAN cellulaire à savoir :

	1G	2G	3G	4G	5G
Année	1970-1980	1990-2002	2001-2010	2010-2015	2015-2020
Standard	AMPS	GSM, GRPS, EDGE	UMTS	LTE	Standard unifié
Débit	2kbps	14,4-64 kbps	2 mbps	200 mpbs – 1 gbps	> 1 gbps
Service	Voix analogique sans transfert de données	Permet le transfert simultané de voix et de données numériques SMS, MMS	Permet le transfert simultané de voix et de données numériques à haut débit	Téléphonie IP TV mobile HD	Reste à implémenter

2.3.5.2. WAN sans fil spatiales

En plus des systèmes cellulaires terrestres, l'utilisation de systèmes spatiaux permet de mettre en réseau des utilisateurs sur de vastes zones. On retrouve deux technologies spatiales principales :

1) Satellites : L'utilisation de satellites pour la diffusion de la télévision et d'autres communications existe depuis plusieurs décennies. Jusqu'à récemment, les systèmes satellitaires fournissaient aux utilisateurs des connexions à Internet. Les taux de données sont appréciables, avec des téléchargements allant jusqu'à 1,5 Mbps.

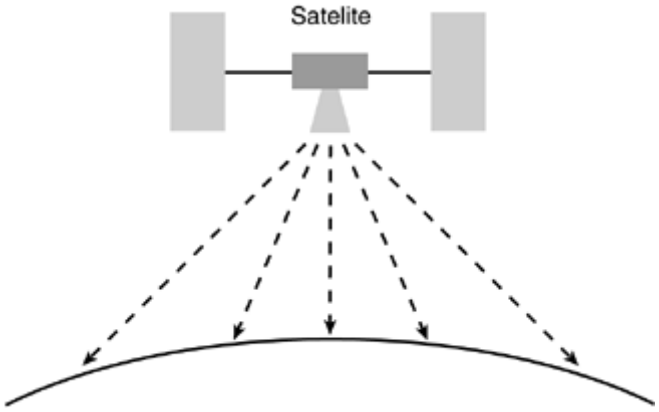

Figure 2.8. WAN sans fils à travers un système satellitaire

Certains systèmes satellitaires prennent en charge l'échange de données bidirectionnelles, permettant à un utilisateur d'envoyer des données vers le satellite (et vice versa). D'autres systèmes satellitaires, cependant, ne supportent qu'une liaison descendante.

2) Communications basées sur l'éclatement de météorites : des milliards de minuscules météorites microscopiques entrent dans l'atmosphère terrestre. En fait, les météores tombent souvent tout au long de la journée sur toutes les parties du monde. Comme ces météores pénètrent dans l'atmosphère, à haute altitude, ils se transforment en gaz. Connu comme le système satellites du pauvre, les communications par éclatement de météorite renvoient les signaux de radio-fréquence au large des sentiers météorologiques. Cela permet un lien de transmission de données sans fil longue distance (2.500 km) sans frais de lancement et de maintenance d'un satellite.

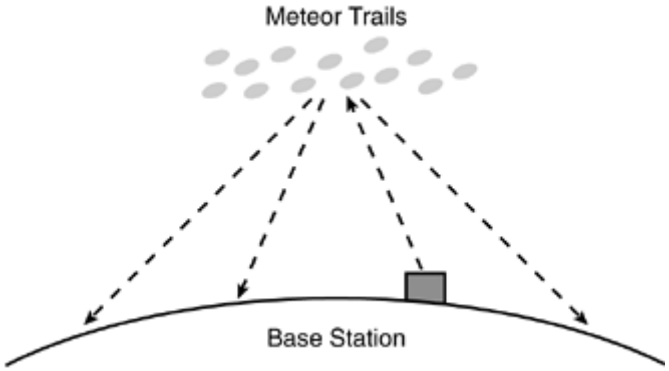

Figure 2.9. WAN sans fils à travers un système de météorites

2.4. Réseaux de stockage (SAN)

Un réseau de stockage est un type de réseau local (LAN) conçu pour gérer de gros transferts de données et le stockage en bloc d'informations numériques. Un SAN prend généralement en charge le stockage, la récupération et la réplication des données sur les réseaux commerciaux utilisant des serveurs haut de gamme, des blocs de disques multiples et une technologie d'interconnexion.

2.4.1. Storage Area Network (SAN)

Un SAN (Storage Area Network) est un terme qui définit toute l'infrastructure matérielle et logicielle qui permet à un ordinateur d'accéder au stockage qui n'est pas directement attaché à celui-ci. C'est un réseau à grande vitesse qui fournit un stockage au niveau du bloc pouvant être consulté par les applications exécutées sur n'importe quel serveur en réseau.

Les principales fonctions d'un réseau de stockage (SAN) comprennent les éléments suivants:

- Un réseau à grande vitesse de périphériques de stockage.
- Connecte les périphériques de stockage avec les serveurs.
- Peut être consulté par les applications sur les serveurs en réseau.
- Particulièrement utile pour la sauvegarde et la reprise après sinistre.
- Utilise des protocoles de réseau pour couvrir des distances plus longues géographiquement.
- Simplifie certaines tâches de gestion.
- Offre la flexibilité, disponibilité et performance.

2.4.2. Les technologies de communication pour réseau de stockage

Les deux technologies de communication dominantes pour les réseaux de stockage sont le canal de fibre (Fiber Channel) et le iSCSI (Internet Small Computer Systems Interface).

1) Canal de fibre (Fiber Channel – FC) : est le principal choix pour le réseau SAN. Les réseaux FC contiennent du matériel spécial appelé interrupteurs Fiber Channel qui relient la mémoire aux disques SAN. Les connexions FC fournissent des débits entre 1 Gbps et 16 Gbps.

2) iSCSI : a été créé comme une alternative moins coûteuse et moins performante à Fiber Channel. iSCSI fonctionne avec des commutateurs Ethernet au lieu d'utiliser du matériel spécialisé construit spécifiquement pour les charges de travail de stockage. Il fournit des débits de données de 10 Gbps ou plus. iSCSI est utilisé en particulier aux petites entreprises.

2.4.3. Les bénéfices du SAN

L'utilisation d'un SAN peut offrir les avantages suivants:

- Améliorations de la disponibilité des applications: le stockage est indépendant des applications et accessible via plusieurs voies de données pour une meilleure fiabilité, disponibilité et facilité d'utilisation.
- Performance supérieure de l'application: le traitement du stockage est déchargé des serveurs et déplacé sur un réseau distinct.
- Stockage centralisé et consolidé: une gestion, une évolutivité, une flexibilité et une disponibilité plus simples sont possibles.
- Transfert de données et saut à des sites distants: Une copie de données à distance est activée pour la protection contre les catastrophes et contre les attaques malveillantes.
- Gestion centralisée simplifiée: une seule image de support de stockage simplifie la gestion.

2.4.4. le virtuel SAN (VSAN)

Un réseau de stockage virtuel (VSAN) est une partition logique dans un réseau de stockage (SAN). Les VSAN permettent d'isoler le trafic dans des parties spécifiques d'un réseau de stockage. L'utilisation de plusieurs VSAN peut rendre un système plus facile à configurer et à étaler. Les VSAN offrent également la possibilité de redondance des données, ce qui minimise le risque de perte de données catastrophiques.

Pratiquement, Un réseau de stockage virtuel (VSAN) est une collection de ports à partir d'un ensemble de commutateurs Fiber Channel, qui forment un réseau de stockage virtuel. Les ports dans un seul commutateur peuvent être partitionnés en plusieurs VSAN, malgré le partage de ressources matérielles. À l'inverse, les commutateurs multiples peuvent joindre un certain nombre de ports pour former un seul VSAN.

L'utilisation de VSAN permet d'isoler le trafic dans des parties spécifiques du réseau. Si un problème se produit dans un VSAN, ce problème peut être traité avec un minimum de perturbation sur le reste du réseau. Les VSAN peuvent également être configurés séparément et indépendamment.