République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud Mammeri de Tizi-Ouzou

Faculté du Génie Electrique et d'Informatique
Département de Télécommunications

Mémoire de fin d'études de

MASTER ACADEMIQUE

Spécialité :

Réseaux & Télécommunications

Filière :

Télécommunications

Réalisé par

Assirem Azzouz

Thème

Conception d'un réseau campus sécurisé

Cas : Réseau informatique du campus Tamda UMMTO

Soutenu le : 26/06/2024

Devant le jury :

Présidente :	**BOUALLEG S.**	**MCB**
Promoteur :	**LAZRI M.**	**Professeur**
Co-promoteur :	**HAMEG S.**	**MCB**
Examinatrice :	**BECHA T.**	**MAB**
Directeur de stage :	**BELAID Ali**	**Ingénieur principal**

Année universitaire 2023-2024

Remerciements

En tout premier lieu, je tiens à remercier le bon Dieu de m'avoir donnée la force, la volonté et le courage pour réaliser ce travail.

Je tiens tout particulièrement à remercier M. Ali Belaid, pour ces judicieux conseils, sa disponibilité tout au long de ce mémoire, je le remercie d'avoir partagé avec moi ces connaissances, ce qui a contribué à alimenter ma réflexion.

Je tiens également à remercier mon encadrant M. Lazri et mon Co-encadrant M. Hameg, pour leur encouragement ainsi que pour leurs précieux conseils.

Je remercie également le personnel du Centre des Réseaux de l'Université Mouloud Mammeri de Tizi-Ouzou pour leur soutien.

Je tiens à remercier toutes les personnes qui, par leurs paroles, leurs écrits, leurs conseils et leurs critiques, ont contribué à la réussite de ce modeste travail, en particulier mes chers parents qui m'ont toujours soutenue et encouragée,

A tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude…

Dédicaces

Je dédie ce modeste travail :

A mes chers parents Said et Nadia à qui je dois tout, je les remercie pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes chères sœurs Hanane, Karima, Cylia, et mes adorables petites jumelles Lina et Milina pour leurs encouragements permanents, et leur soutien moral ainsi qu'à ma très chère cousine Ryma,

A toute ma famille pour leur soutien tout au long de mon parcours universitaire, ainsi qu'à ma belle-famille qui m'a toujours soutenue,

A mon encadrant Ali Belaid qui a cru en moi, pour son encouragement et sa disponibilité tout au long de ce mémoire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infaillible,

Merci d'être toujours là pour moi…

Table des matières

Liste des figures

Liste des abréviations, sigles et acronymes

PAN : personal Area Network
LAN : Local Area Network
MAN : Metropolitan Area Network
WAN : Wide Area Network
P2P: Peer to Peer
IEEE : Institute of Electrical and Electronics Engineers
CSMA/CD : Carrier Sense Multiple Access Collision Detection
CSMA/CA : Carrier Sense Multiple Access with Collision Avoidance
FDDI : Fiber Distributed Data Interface
Wi-Fi : Wireless Fidelity
MAC : Media Access Control
IP : Internet Protocol
VLAN : Virtual Local Area Networks
NAT : Network Address Translation
NIC : Network Interface Card
QoS : Quality Of Service
WPA : Wi-Fi Protected Access
WPA2 : Wi-Fi Protected Access 2
IPv4 : Internet Protocol Version 4
IPv6 : Internet Protocol Version 6
SSID : Service Set Identifier
UTP : Unshielded Twisted Pair
STP : Shielded Twisted Pair
FTP : Foiled Twisted Pair
SFTP : Shielded Foiled Twisted Pair
SMF : Fibre monomode
MMF : Fibre multimode
WDM : Wavelenghth Division Multiplexing
TCP : Transmission Control Protocol
UDP : User Datagram Protocol
OSI : Open Systems Interconnection
ISO : International Organization for Standardization
PPP : Point-to-Point
HTTP : Hypertext Transfer Protocol
HTTPS : Hypertext Transfer Protocol Secure
SMTP : Simple Mail Transfer Protocol
FTP : File Transfer Protocol
DNS : Domain name system
ICMP : Internet Control Message Protocol
IGMP : Internet Group Management Protocol
PDU : Protocol Data Unit
APDU : Application Protocol Data Unit
SPDU : Session Protocol Data Unit
ARPANET : Advanced Research Project Agency Network
FAI : les fournisseurs d'accès à Internet
FSI : les fournisseurs de services Internet
IANA : Internet Assigned Numbers Authority

VoIP : Voice Over Internet Protocol
AS : Autonomous Systems
IGP : Interior Gateway Protocol
OSPF: Open Shortest Path First
EIGRP Enhanced Interior Gateway Routing Protocol
IS-IS: Intermediate System to Intermediate System
EGP : Externe Gateway Protocol
BGP : Border Gateway Protocol
ARP : Address résolution Protocol
AP : Access point
WDS : Windows Deployement Service
VLSM : Variable Length Subnet Masking
SNMP : Simple Network Management Protocol
NPM : Network Performance Monitor
PRTG : Paessler Router Traffic Grapher
NTA : Network Traffic Analysis
SNPM : SolarWinds Network Performance Monitor
IoT : Internet of objet
IA : intelligence artificielle
DDoS : Les attaques par déni de service
SQL : Structured Querry language
NGFW : Next Generation FireWall
IDS : Les systèmes de détection d'intrusion
IPS : Les systèmes de prévention d'intrusion
RBAC : Role-Based Access Control
SSO : Single Sign-On
SAML : Security Assertion Markup Language
OAuth : Open Authorization
AD : Active Directory
SSL/TLS : Secure Sockets Layer/Transport Layer Security
SSH : Secure Shell
VPN : Virtual Private Network
DMZ : Demilitarized Zone
ACL : Access conrol list
CSRICTED : Centre des Systèmes et Réseaux d'Informations et de Communication, de Télé-enseignement et d'Enseignement à Distance

Introduction générale

De nos jours, la vie universitaire repose sur les réseaux informatiques, qui constituent le fondement technologique sur lequel reposent de nombreux aspects. Ils sont plus importants que la simple connexion Internet qui permet aux étudiants de se connecter à Internet ou de consulter leurs courriels. En effet, ces réseaux sont essentiels pour le fonctionnement et l'interaction des campus universitaires avec leur communauté.

Les réseaux informatiques rendent accessibles de nombreuses ressources éducatives en local, sans avoir besoin de connexion à Internet, telles que le catalogue de la bibliothèque et les plateformes d'enseignement en ligne. De cette manière, les étudiants ont la possibilité d'accéder à des cours, des articles de recherche, des vidéos pédagogiques et d'autres ressources éducatives depuis n'importe quel endroit sur le campus, ce qui encourage un apprentissage plus autonome et souple.

Grâce aux réseaux informatiques, les étudiants, les enseignants et le personnel peuvent communiquer et travailler de manière efficace, peu importe leur localisation géographique. La collaboration sur des projets de recherche, des exposés et d'autres activités pédagogiques est facilitée par les plateformes de messagerie professionnelle, les forums en ligne et les outils de visioconférence, qui permettent un échange d'idées fluide et constant.

Les activités pédagogiques et de recherche sur les campus universitaires sont soutenues par les réseaux informatiques. Des outils en ligne sont disponibles pour les enseignants afin de distribuer des cours et des examens en ligne, recueillir des travaux d'étudiants et donner des notes et des commentaires rapidement et efficacement. Les réseaux informatiques sont également utilisés par les chercheurs pour accéder à des bases de données, communiquer avec leurs collègues et partager leurs résultats de recherche.

L'importance des réseaux informatiques dans la gestion administrative des universités est également primordiale. Ils offrent à l'administration de l'université la possibilité de gérer de manière plus efficace et efficiente les inscriptions des bacheliers et étudiants, les calendriers académiques, les recrutements, les finances et d'autres processus administratifs.

Les réseaux informatiques sont des outils indispensables pour les campus universitaires, car ils permettent de faciliter l'accès à l'information, de favoriser la collaboration, de soutenir l'enseignement et la recherche, de simplifier la gestion administrative. Plus la technologie progresse, plus les universités doivent investir dans leurs infrastructures réseau afin de rester à la pointe de l'innovation et de continuer à offrir une expérience pédagogique de qualité à leurs étudiants et à leur personnel.

Le problème rencontré au niveau du campus Tamda, où se situe notre projet, est l'absence totale de réseau locale. Quelques lignes ADSL existent pour permettre à quelques services d'avoir accès à Internet.

La solution proposée et qui constitue notre projet est la conception puis la réalisation d'un réseau local de type réseau campus, qui permettra à tous les utilisateurs de se connecter à Internet à haut débit et de bénéficier des avantages d'un réseau local.

Pour ce faire, nous avons organisé notre travail en quatre chapitres :

Chapitre 1 : Généralités sur les réseaux informatiques, dans lequel nous allons aborder certaines notions de base d'un réseau informatique.

Chapitre 2 : Trafic des données sur un réseau, où nous allons explorer en détail la manière dont les données circulent sur notre réseau.

Chapitre 3 : Sécurité des réseaux informatiques, où nous allons identifier les concepts clés de cette discipline, les différentes failles et attaques les plus connues ainsi que les mécanismes que nous pouvons mettre en place pour protéger nos données.

Chapitre 4 : Partie pratique, dans laquelle nous allons présenter l'organisme d'accueil, identifier la problématique rencontrée ainsi que la solution proposée. Nous mettrons en évidence l'aspect technique de la solution choisie, l'architecture réseau, les équipements réseau et de sécurité déployés ainsi que le câblage.

Nous finirons notre étude par une simulation du réseau conçu au campus Tamda sur CISCO Packet Tracer où nous réaliserons plusieurs tests de PING au niveau du réseau local, du réseau local vers Internet, d'Internet vers un service Web hébergé au niveau du campus et enfin l'accès à des serveurs au niveau local.

Enfin, dans la conclusion générale, nous emmétrons des critiques et suggestions sur le projet réalisé et tenterons d'apporter des idées innovantes qui pourraient améliorer le réseau mis en place. Nous présenterons également les résultats des différents tests réalisés à l'issue de ce projet.

Chapitre I : Généralités sur les réseaux informatiques

I.1 Introduction

Dans cette partie, nous allons aborder le contexte et la justification de l'étude, qui sont des éléments fondamentaux pour comprendre l'importance de ce travail de recherche.

Il est crucial de souligner que nous vivons à l'ère de l'information et de la technologie, où les réseaux informatiques jouent un rôle central dans notre quotidien. Que ce soit dans le domaine des communications, des affaires, de l'éducation ou même du divertissement, les réseaux informatiques sont omniprésents et impactent notre manière de travailler, de communiquer et d'interagir avec le monde qui nous entoure.

I.2 Définition d'un réseau informatique

Il est important de comprendre ce qu'est un réseau informatique. En termes simples, Un réseau informatique peut être défini comme un ensemble d'appareils interconnectés qui partagent des ressources et des informations entre eux. Il s'agit d'une infrastructure essentielle dans le monde moderne, permettant la communication et l'échange de données à grande échelle, Ces appareils peuvent être situés dans une même pièce, dans un même bâtiment, voire à des milliers de kilomètres les uns des autres.

Un réseau informatique repose sur plusieurs éléments clés. Tout d'abord, il y a les dispositifs matériels appelés « nœuds ». Ce sont les équipements qui permettent la connexion entre les différents ordinateurs du réseau. Parmi ces dispositifs, on retrouve les routeurs, les commutateurs et les concentrateurs, qui jouent un rôle essentiel dans le transfert des données.

Ensuite, il y a les câbles qui relient les différents dispositifs entre eux, autrement dit Ces nœuds sont liés les uns aux autres par des moyens de connexion qui peuvent être physiques (filaires) et qui peuvent être de différents types, tels que les câbles Ethernet, les câbles à fibre optique ou encore les câbles coaxiaux ou sans fil tels que le Wi-Fi. Chaque type de câble a ses propres caractéristiques et capacités de transmission de données.

Les réseaux informatiques reposent sur des technologies et des protocoles spécifiques pour assurer la connectivité et la transmission des données. Ces technologies peuvent inclure des câbles Ethernet, des routeurs, des commutateurs, des antennes sans fil, des modems et bien d'autres encore. Les protocoles, quant à eux, régissent les règles et les normes de communication au sein du réseau.

Un réseau informatique peut avoir différentes topologies, c'est-à-dire la structure physique et logique des appareils interconnectés. Les topologies couramment utilisées sont l'étoile, le bus, l'anneau et le maillage. Chaque topologie a ses avantages et ses inconvénients, et peut être adaptée en fonction des besoins spécifiques d'un réseau.

Les réseaux informatiques peuvent également être classés en fonction de leur taille. On distingue généralement trois types de réseaux : les réseaux locaux (LAN - Local Area Network), les réseaux étendus (WAN - Wide Area Network) et les réseaux métropolitains (MAN - Metropolitan Area Network). Les LAN connectent des appareils au sein d'un espace géographique restreint, tels qu'un bureau ou un bâtiment, tandis que les WAN étendent la connectivité sur de plus grandes distances, souvent à l'échelle d'une ville, d'un pays ou même d'un continent. Les MAN, quant à eux, sont des réseaux qui couvrent une zone métropolitaine.

En conclusion, un réseau informatique joue un rôle essentiel dans le monde moderne, facilitant la collaboration, l'accès à l'information et l'échange de ressources. Que ce soit à petite ou grande échelle, les réseaux informatiques ont révolutionné notre façon de communiquer et de partager l'information.

I.2.1 Intérêts d'un réseau informatique

Les réseaux informatiques sont nés du besoin de communiquer des terminaux lointains. Cela met en évidence l'objectif fondamental des réseaux informatiques, qui est de permettre l'échange d'informations et de données entre des appareils situés dans des emplacements géographiques différents, tels que les ordinateurs, les téléphones, les tablettes et bien d'autres. Dans ce chapitre, nous allons explorer les intérêts d'un réseau informatique. Les réseaux informatiques jouent un rôle crucial dans notre société moderne, offrant de nombreux avantages et intérêts tant au niveau individuel que collectif.

Tout d'abord, l'un des principaux avantages d'un réseau informatique est la possibilité de partager et d'accéder aux ressources. Un réseau permet aux utilisateurs de partager des fichiers et des dossiers, de collaborer sur des projets et de faciliter le partage d'informations. Par exemple, dans un environnement éducatif, les enseignants et les étudiants peuvent partager des documents, des présentations et des recherches, ce qui favorise l'apprentissage collaboratif et la diffusion des connaissances.

Un autre intérêt majeur des réseaux est la communication. Les réseaux informatiques permettent des échanges rapides et efficaces d'informations entre les individus, peu importe leur emplacement géographique. Les e-mails, les chats et les appels vidéo sont autant d'outils qui facilitent la communication à distance. Cette connectivité renforce les relations personnelles et professionnelles, en favorisant les échanges, les collaborations et la résolution de problèmes en temps réel.

De plus, les réseaux informatiques offrent de nombreuses opportunités en termes de partage de ressources matérielles. Par exemple, grâce à la technologie de l'impression en réseau, plusieurs utilisateurs peuvent accéder à une imprimante partagée, ce qui permet d'économiser des coûts et de favoriser l'efficacité. De même, le partage de périphériques tels que les scanners, les projecteurs et les serveurs de stockage permet d'optimiser les ressources et d'améliorer la productivité.

Les réseaux informatiques favorisent également l'accès aux informations et aux services à distance. Grâce à Internet, les utilisateurs ont la possibilité de se connecter à des ressources en ligne telles que des bibliothèques numériques, des bases de données, des plateformes de formation en ligne, etc. Cela permet d'élargir les connaissances et de bénéficier de services et de contenus qui étaient auparavant inaccessibles.

Enfin, les réseaux informatiques contribuent à l'efficacité et à la flexibilité des processus de travail. Par exemple, les entreprises peuvent mettre en place des réseaux locaux (LAN) qui permettent aux employés de partager des informations, de travailler simultanément sur des projets et d'accéder aux bases de données de l'entreprise. De même, les réseaux étendus (WAN) permettent aux entreprises de se connecter à distance à leurs filiales ou partenaires, facilitant ainsi la coordination et la gestion des opérations.

En conclusion, les réseaux informatiques offrent de nombreux intérêts tant au niveau individuel que collectif. En favorisant le partage de ressources, la communication à distance, l'accès aux informations et aux services, ainsi que l'efficacité des processus de travail, les réseaux permettent d'améliorer la productivité, la collaboration et la connectivité.

I.3 Architecture des réseaux informatiques

L'architecture réseau est la représentation structurale et fonctionnelle d'un réseau, on distingue deux catégories, qui sont les suivantes :

I.3.1 Architecture réseau à serveur dédier : Clients/ server

Le concept de "Clients/Server" est fondamental dans l'architecture des réseaux informatiques. Il représente un modèle de communication dans lequel des dispositifs ou des applications appelés "clients" interagissent avec des dispositifs ou des applications appelés "serveurs" via un réseau. Ce modèle permet la distribution des tâches et des ressources, ce qui améliore considérablement l'efficacité des systèmes informatiques.
Dans ce modèle, les clients envoient des requêtes aux serveurs pour obtenir des informations ou des services spécifiques. Les serveurs, quant à eux, traitent ces requêtes et renvoient les résultats aux clients concernés. Cette interaction entre les clients et les serveurs peut être effectuée localement sur un réseau interne ou à distance via Internet.

L'architecture "Clients/Server" présente de nombreux avantages. Elle permet une centralisation des données et des processus, ce qui facilite la gestion et la maintenance des systèmes informatiques. De plus, ce modèle favorise la modularité et la scalabilité en permettant l'ajout de nouveaux clients ou serveurs sans perturber le fonctionnement global du réseau.

Un exemple concret de l'utilisation du modèle "Clients/Server" est le fonctionnement d'un site web. Lorsqu'un utilisateur accède à un site web, son navigateur agit en tant que client et envoie une requête au serveur hébergeant le site. Le serveur traite la requête, récupère les données demandées et les renvoie au navigateur client, qui les affiche alors à l'utilisateur.

Il est important de noter que le modèle "Clients/Server" n'est qu'un des nombreux modèles d'architecture de réseau disponibles, et il convient de choisir le modèle le plus approprié en fonction des besoins spécifiques de chaque système informatique.

En conclusion, le modèle "Clients/Server" est un élément essentiel de l'architecture des réseaux informatiques. Il facilite la communication et l'échange d'informations entre les clients et les serveurs, offrant ainsi une performance optimale et une gestion simplifiée des systèmes informatiques.

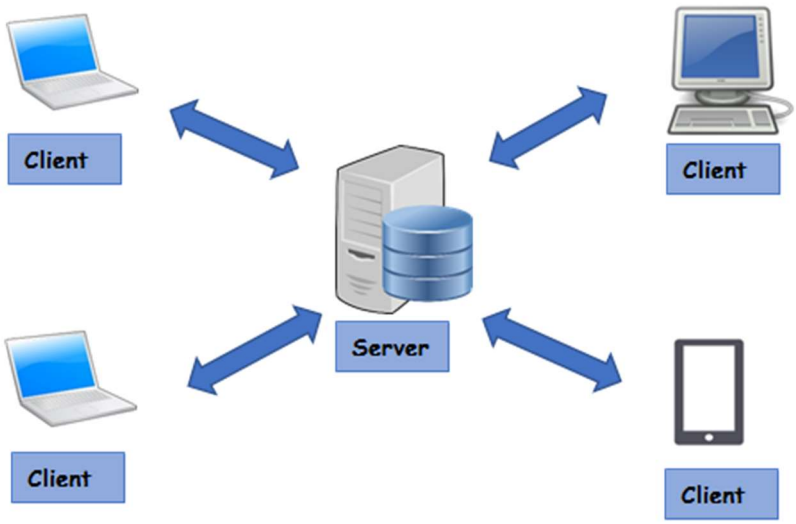


Figure I.1: réseau client/serveur. [1]

I.3.2 Architecture Peer to Peer (P2P):

Le concept fondamental du P2P repose sur le partage direct de ressources et d'informations entre les utilisateurs, sans passer par un serveur centralisé. Contrairement aux architectures client-serveur traditionnelles, le P2P permet une décentralisation complète du contrôle et de la distribution des données. Chaque nœud du réseau agit à la fois en tant que client et en tant que serveur, ce qui crée une interactivité directe et une redondance des données.
L'architecture P2P est connue pour sa résilience et sa tolérance aux pannes. En effet, en cas de défaillance d'un nœud, les autres nœuds peuvent continuer à fonctionner et fournir les ressources demandées. Cette redondance permet une meilleure disponibilité et une répartition de charge équilibrée sur le réseau, ce qui le rend plus rapidement réactif aux demandes des utilisateurs.

Un autre avantage majeur du P2P réside dans sa capacité à scaler horizontalement. En ajoutant simplement de nouveaux nœuds au réseau, celui-ci gagne en capacité de stockage et en puissance de calcul, ce qui permet de supporter une charge croissante d'utilisateurs et de données. Contrairement aux architectures client-serveur où l'ajout de serveurs peut être coûteux et complexe, le P2P offre une flexibilité et une évolutivité plus facilement réalisables.

Cependant, le P2P présente également certaines limites et défis. Tout d'abord, il est important de maintenir une bonne gestion du réseau pour assurer l'intégrité des données et prévenir les comportements malveillants ou indésirables tels que le téléchargement illégal de contenus protégés par le droit d'auteur. De plus, la sécurité des échanges et des données partagées constitue un enjeu majeur pour garantir la confidentialité et l'intégrité des informations.

En conclusion, l'architecture P2P offre de nombreux avantages pour les réseaux informatiques en permettant un partage direct des ressources entre les pairs connectés. Elle favorise la résilience, la tolérance aux pannes et l'évolutivité du réseau. Cependant, il est important de mettre en place des mécanismes de gestion et de sécurité adéquats pour en assurer le bon fonctionnement et la protection des données.

- Et bien sûr chaque modèle est adapté à des besoins spécifiques en fonction des exigences de performance, de sécurité et de gestion du réseau.

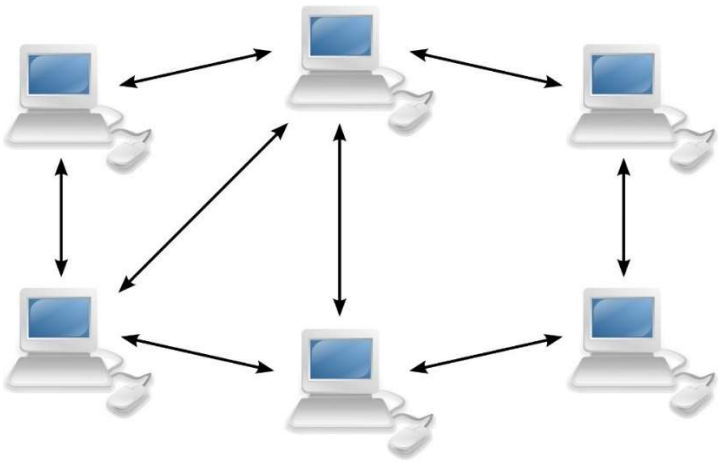


Figure I.2: réseau peer to peer. [2]

I.4 Classification des réseaux informatiques

La classification des réseaux informatiques consiste à regrouper les réseaux en différentes catégories (selon différentes perspectives) en fonction de critères spécifiques qui varies en fonction des aspects pris en compte tels que leur étendue géographique, leur topologie et leur performance.

I.4.1 Selon la topologie

La topologie décrit la manière dont les appareils sont connectés les uns aux autres, autrement dit un ensemble des méthodes physiques et standards qui oriente ou facilite la circulation des données entre les différents périphériques ou les différents nœuds associés à ce réseau, on distingue deux types de topologie à savoir ; la topologie physique et la topologie logique.

I.4.1.1 La topologie physique

La topologie physique définit la structure physique du réseau, c'est-à-dire la façon dont les dispositifs sont connectés et organisés sur le plan matériel comme les câbles et des appareils dans le réseau et des éléments matériels comme les cartes réseau, déterminant comment ces différents éléments du réseau sont connectés physiquement. Parmi les différentes topologies physiques, on retrouve :

I.4.1.1.1 La topologie en étoile

C'est l'une des plus répandues, notamment dans les réseaux locaux (LAN). Dans ce type de topologie, tous les périphériques du réseau sont connectés à un concentrateur central, également appelé commutateur. Cette configuration facilite la gestion du réseau et permet d'isoler les problèmes liés à un périphérique spécifique sans affecter l'ensemble du réseau. Cependant, la panne du concentrateur central peut entraîner une interruption de tout le réseau.

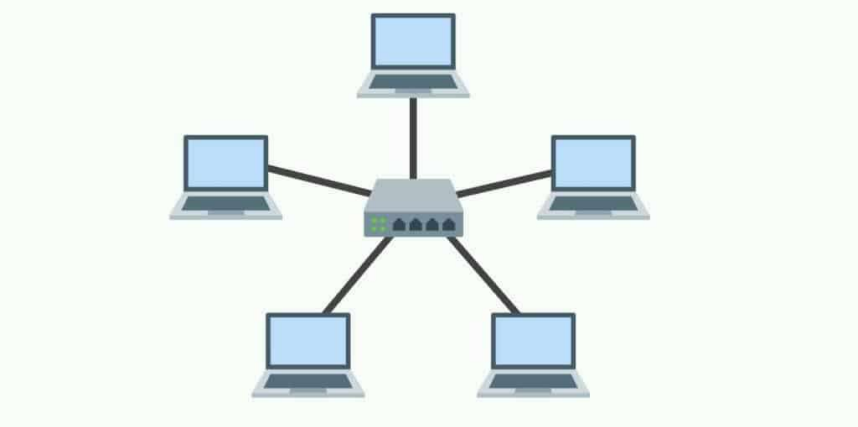


Figure I.3: Topologie en étoile. [3]

I.4.1.1.2 La topologie en bus

Il s'agit d'une autre topologie populaire, principalement utilisée dans les réseaux locaux. Dans ce type de configuration, tous les périphériques sont connectés à un seul câble principal, appelé bus. Les données sont transmises sur ce câble et sont reçues par tous les périphériques connectés. Bien que cette topologie soit simple et économique, elle présente un inconvénient majeur en termes de fiabilité. En effet, si le câble principal est endommagé, tout le réseau est affecté.

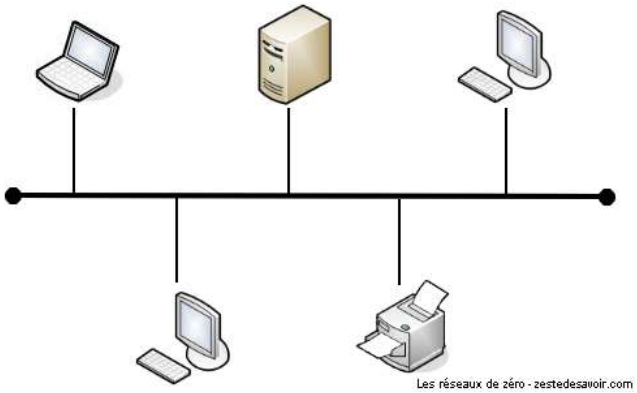


Figure I.4: topologie en bus [4]

I.4.1.1.3 La topologie en anneau

C'est une autre option couramment utilisée dans les réseaux locaux. Dans ce schéma, chaque périphérique est relié à deux autres périphériques formant un cercle, de sorte que les données circulent de périphérique en périphérique jusqu'à ce qu'elles atteignent leur destination. Cependant, si l'un des périphériques du réseau est défectueux, cela peut entraîner une interruption de la communication sur l'ensemble de l'anneau.

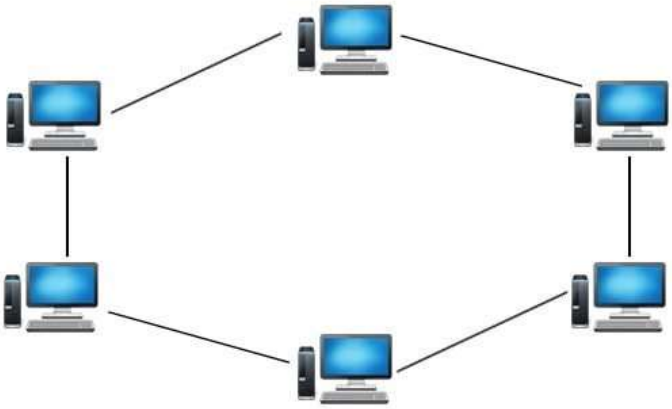


Figure I.5: Topologie en anneau. [5]

I.4.1.1.4 La topologie en arbre (hiérarchique)

La topologie hiérarchique est utilisée dans les grands réseaux, tels que les réseaux étendus (WAN). Elle combine les caractéristiques de la topologie en étoile et de la topologie en bus. Dans cette configuration, les commutateurs sont interconnectés pour former une structure semblable à un arbre. Cela permet de segmenter le réseau en sous-réseaux plus petits, ce qui facilite la gestion et l'organisation de l'ensemble du système. Cependant, la panne d'un concentrateur central peut entraîner l'effondrement de tout le sous-réseau qui lui est rattaché.

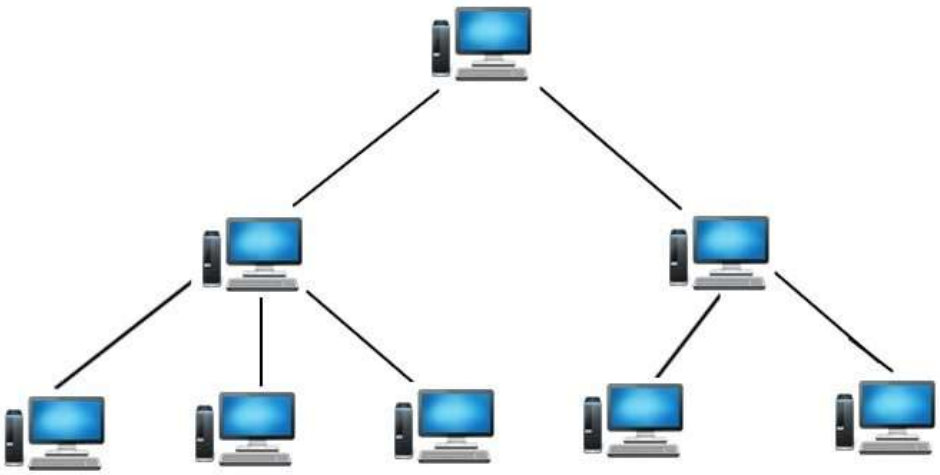


Figure I.6: Topologie hiérarchique [5]

I.4.1.1.5 La topologie maillée

C'est la plus complexe et la plus coûteuse, mais aussi la plus fiable. Dans cette configuration, chaque périphérique est connecté à tous les autres périphériques du réseau, formant ainsi un maillage complet. Cette redondance permet de garantir une très haute disponibilité et une tolérance aux pannes élevée. Cependant, cela nécessite un grand nombre de câbles et une configuration complexe, ce qui la rend moins courante dans les réseaux locaux.

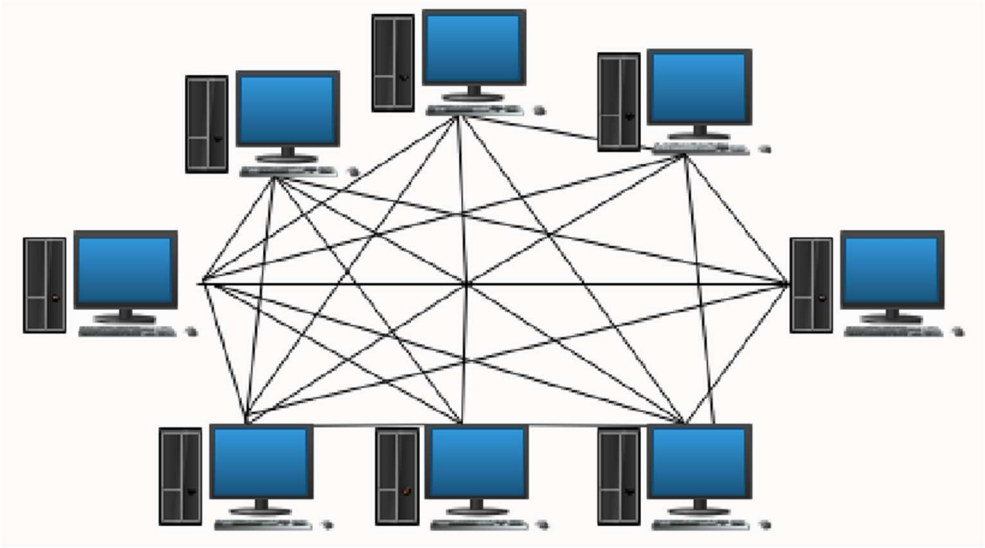


Figure I.7: Topologie en maille. [6]

En conclusion, la topologie physique d'un réseau informatique joue un rôle essentiel dans sa performance, sa fiabilité et son coût. Chaque topologie a ses propres caractéristiques et il est important de choisir celle qui convient le mieux aux besoins et aux contraintes spécifiques de chaque réseau. La classification des réseaux informatiques en fonction de leur topologie physique permet une meilleure compréhension et une gestion plus efficace de ces systèmes complexes.

I.4.1.2 La topologie logique

Par opposition à la topologie physique, ce type définit la manière et la façon dont les données sont transmises et traitées dans le réseau, on parle donc des méthodes d'accès au canal de transmission, c'est-à-dire la façon dont les données transitent dans les lignes de transmission. Parmi Les topologies logiques les plus courantes on trouve :

I.4.1.2.1 Topologie Ethernet

Une des topologies logiques les plus répandues, elle est basée sur la norme IEEE 802.3 qui est largement utilisée dans les réseaux locaux pour la transmission de données et les membres du réseau se retrouvent généralement sur un support de transmission commun (un câble)
En effet, dans un réseau Ethernet de type bus, le protocole CSMA/CD est utilisé pour régir la manière dont les postes accèdent au média de transmission
Imaginons un bureau équipé d'un réseau local Ethernet où plusieurs ordinateurs sont connectés à un commutateur central. Lorsqu'un ordinateur (A) souhaite envoyer des données à un autre ordinateur (B), il commence par écouter le canal de communication pour s'assurer qu'il est libre. Si le canal est occupé par un autre ordinateur qui transmet des données, l'ordinateur (A) attend que le canal soit libre avant d'envoyer ses propres données.
Si par malchance, deux ordinateurs (A et C) décident d'émettre des données en même temps et que leurs signaux se chevauchent, une collision se produit. Les ordinateurs (A) et (C) détectent cette collision grâce au protocole CSMA/CD et interrompent immédiatement leur transmission. Ensuite, ils attendent un bref délai aléatoire avant de réessayer d'envoyer leurs données pour éviter une nouvelle collision.

Cette méthode d'accès est utilisée pour assurer un accès équitable au média de transmission, entraînant ainsi les conflits qui pourraient survenir lors de l'accès compétitif au support de transmission dans ce type de réseau
Afin de comprendre comment fonctionne la procédure CSMA/CD, il est pertinent de décomposer les différents éléments du terme :

- Carrier Sense (CS) :

La détection de l'état de la porteuse veille à ce que tous les participants vérifient que le support est libre. Le protocole procède uniquement à la transmission des données lorsque cette étape a été effectuée.

- Multiple Access (MA) :

Plusieurs participants (ordinateurs connectés au réseau) se partagent un support de transmission.

- Collision Detection (CD) :

La détection des collisions est une extension du protocole initial et détermine comment agir en cas de collision de paquets de données.[1]

I.4.1.2.2 Topologie Token Ring (l'anneau à jetons)

C'est une méthode du passage du jeton c'est-à-dire elle fonctionne selon un principe de jetons qui circulent dans un anneau (en boucle), Les collisions sont proscrites et les appareils ne peuvent pas émettre simultanément ces données, chaque appareil dois attendre le jeton qui donne la permission de parler. Ce dernier passe d'un appareil à l'autre jusqu'à ce qu'il atteigne l'appareil qui a besoin de transmettre des données. Il y a des délais d'attente pour obtenir le jeton mais il n'y a pas de collision donc pas de délai de retransmission

I.4.1.2.3 Topologie FDDI (Fiber Distributed Data Interface)

La topologie logique FDDI repose sur l'utilisation de fibres optiques pour transmettre les données, et qui utilise un concept d'anneau double contre-rotatif pour assurer la transmission fiable et rapide des données sur de longues distances, ce qui en fait un choix idéal pour les réseaux nécessitant une bande passante élevée et une stabilité accrue comme les réseaux locaux tels que les réseaux campus et métropolitains ; le réseau est configuré en utilisant deux anneaux de transmission. L'anneau primaire est utilisé pour la transmission normale des données dans un sens, tandis que l'anneau secondaire sert de secours inactif dans l'autre sens et qui sert à rattraper les erreurs de l'anneau primaire (On note que le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs ; et c la que l'anneau secondaire prend son importance).
Les deux anneaux dans la topologie FDDI tournent dans des directions opposées, créant ainsi une redondance et une fiabilité accrue. Cette configuration permet d'assurer une continuité de la transmission des données même en cas de rupture ou de panne sur l'un des anneaux et donc le réseau FDDI se reconfigure automatiquement pour utiliser l'anneau secondaire comme voie de secours.

I.4.2 Selon l'Etendue géographique

L'extension géographique est un aspect essentiel lorsqu'il s'agit classer les réseaux informatiques. En effet, la taille et la portée géographique d'un réseau peuvent avoir des implications majeures sur sa conception, sa mise en œuvre et sa gestion.

Dans cette perspective, on distingue généralement quatre types principaux de réseaux informatiques en fonction de leur étendue géographique : les réseaux personnel (PAN), les réseaux locaux (LAN), les réseaux étendus (WAN) et les réseaux métropolitains (MAN).

I.4.2.1 Réseau personnel (PAN : personal Area Network)

C'est réseau conçu pour une seule personne (un même utilisateur) interconnecté sur quelque mètres ses appareils personnels tels que son ordinateur, son smartphone, sa tablette….

Figure I.8: Réseau PAN. [7]

I.4.2.2 Les réseaux locaux (LAN : local area network)

Souvent utilisés dans les environnements de taille réduite tels que les maisons, les bureaux ou les campus, ont une portée géographique limitée. Ils sont généralement composés de dispositifs reliés par des câbles Ethernet ou des connexions sans fil, et offrent des débits de transmission élevés. Les LAN permettent aux utilisateurs de partager des ressources telles que des fichiers, des imprimantes, des serveurs et de communiquer efficacement au sein d'un même réseau.

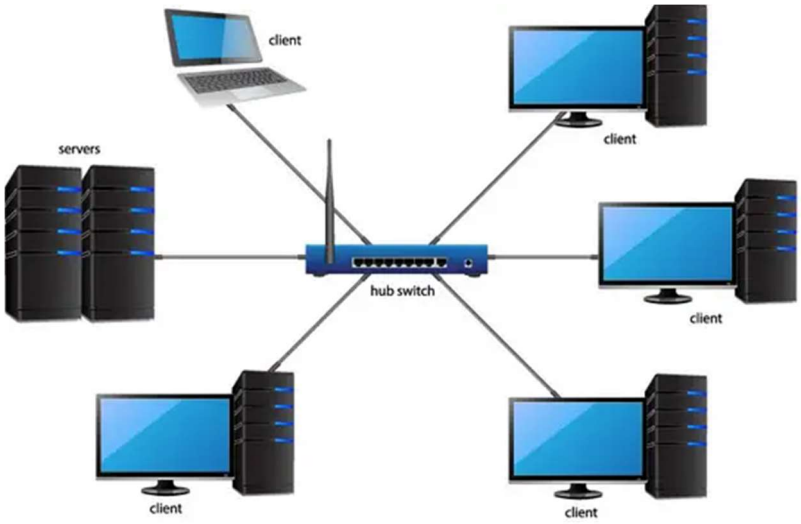


Figure I.9: Réseau LAN. [8]

I.4.2.3 Les réseaux métropolitains (MAN : métropolitain area network)

Se situent entre les réseaux locaux et les réseaux étendus en termes d'étendue géographique. Ils couvrent généralement une zone urbaine ou une région métropolitaine, interconnectant différents bâtiments ou sites situés à proximité les uns des autres. Ces réseaux fournissent des services de connectivité haut débit aux utilisateurs locaux et sont généralement gérés par des fournisseurs de services de télécommunication.

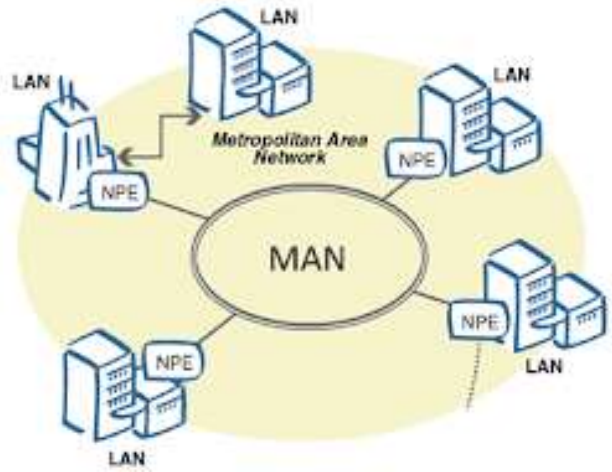


Figure I.10: Réseau MAN. [10]

I.4.2.5 Les réseaux étendus (WAN : wide area network)

Englobent de plus grandes distances géographiques, souvent à l'échelle d'une région, d'un pays, même à l'échelle mondiale. Ces réseaux sont constitués de multiples sites interconnectés, utilisant des technologies de télécommunication comme des liaisons privées dédiées, des réseaux virtuels privés (VPN) ou des connexions Internet. Les WAN permettent le partage de données et d'applications entre différents sites, ce qui en fait un choix optimal pour les entreprises à succursales multiples ou les organisations dispersées géographiquement.

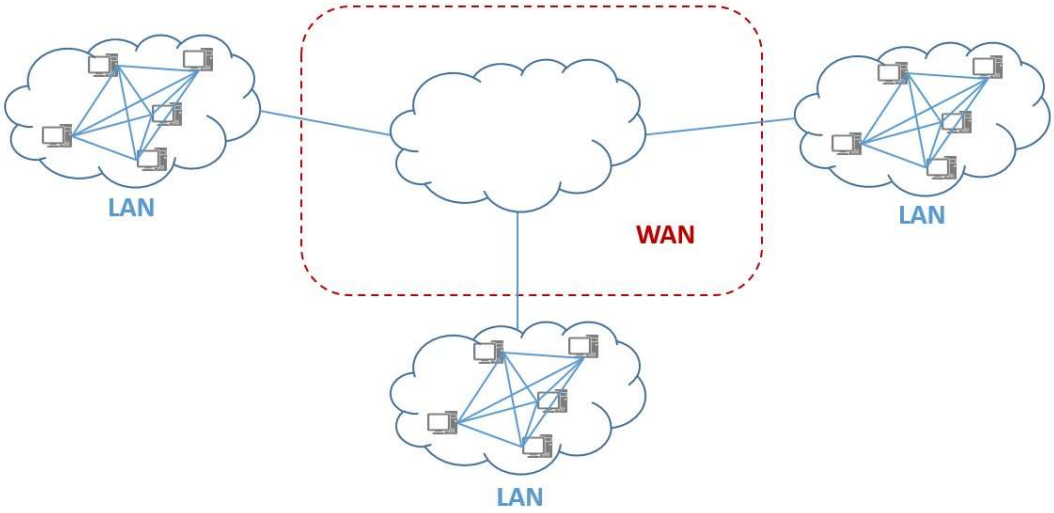


Figure I.11: Réseau WAN. [9]

Il est important de noter que l'étendue géographique d'un réseau peut avoir des implications sur les performances, la sécurité et la fiabilité de celui-ci. Plus la distance entre les sites est grande, plus les problèmes de latence, de perte de paquets ou d'interférences peuvent se poser. Les réseaux étendus nécessitent également une planification et une gestion plus complexes en termes de routage, de capacité et de sécurité.

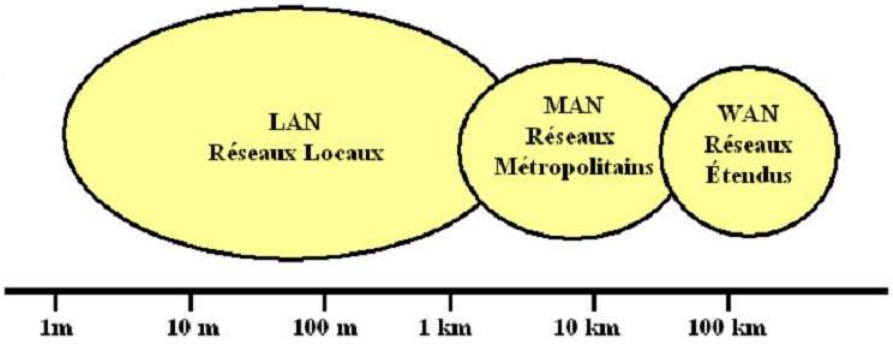


Figure I.12:l'etendu géographique en fonction de la distance.[11]

En conclusion, la classification des réseaux informatiques en fonction de leur étendue géographique est un aspect crucial pour comprendre les différentes architectures et technologies utilisées. Les réseaux locaux, étendus et métropolitains présentent des caractéristiques distinctes en termes de taille, de portée, de technologies utilisées et de services offerts. Il est donc essentiel de prendre en compte l'extension géographique lors de la conception et de la gestion d'un réseau informatique afin d'assurer une connectivité efficace et fiable pour les utilisateurs.

I.4.3 selon la Performance du réseau

La performance du réseau est un aspect important à prendre en compte lors de la classification des réseaux informatiques. En effet, la performance d'un réseau est déterminante pour garantir une connectivité fluide et efficace entre les différents dispositifs qui y sont connectés.

Lorsque l'on parle de performance du réseau, on fait référence à plusieurs critères tels que la vitesse de transmission des données, La latence qui représente le temps écoulé (le délais) entre l'envoi et la réception des données, La bande passante disponible, la gestion du trafic, la capacité de supporter un nombre élevé d'utilisateurs ainsi la capacité à maintenir une connexion stable et continue (la fiabilité), la résistance aux pannes et aux problèmes de congestion. Tous ces éléments contribuent à la qualité et à l'efficacité du réseau.

La performance d'un réseau peut être évaluée à l'aide de plusieurs indicateurs tels que le débit, qui mesure la quantité de données pouvant être transmise par unité de temps, mesuré en bits par seconde (bps), est un indicateur clé de la performance en termes de vitesse de transmission des données, et le temps de réponse, qui est le temps nécessaire pour qu'une requête traverse le réseau du point A au point B. Ces mesures permettent de quantifier la rapidité et l'efficacité du réseau.

Dans le cadre de la classification des réseaux informatiques, il est important de considérer la performance comme un critère de différenciation. On peut distinguer différents types de réseaux en fonction de leurs performances.

Par exemple, les réseaux locaux (LAN) offrent généralement une performance élevée, avec des débits élevés et une latence faible, ce qui les rend adaptés aux besoins des entreprises et des institutions nécessitant une connectivité rapide et fiable à l'échelle locale.
D'autre part, les réseaux étendus (WAN) sont conçus pour connecter des sites géographiquement dispersés et peuvent présenter des performances variables en fonction de la distance entre les sites.
Les réseaux métropolitains (MAN) quant à eux, offrent une performance intermédiaire entre les LAN et les WAN, et sont adaptés aux besoins des villes et des zones métropolitaines.

Enfin, les réseaux sans fil, tels que les réseaux Wi-Fi, peuvent présenter des performances variables en fonction de la distance entre le point d'accès et les dispositifs connectés, ainsi que des interférences provenant d'autres équipements électroniques. La performance du réseau sans fil peut également être affectée par le nombre d'utilisateurs simultanés et la qualité du signal.

Sans oublier de parler du critère de la Sécurité d'un réseau qui concerne la protection des données contre les accès non autorisés, les attaques malveillantes et les pertes d'informations sensibles.

En conclusion, la performance du réseau est un critère essentiel à prendre en compte lors de la classification des réseaux informatiques. Elle permet de déterminer la qualité, l'efficacité et la rapidité de la connectivité offerte par un réseau donné. En fonction de ses performances, un réseau peut être adapté à différents besoins, que ce soit à l'échelle locale, métropolitaine ou étendue.

I.5 Infrastructure d'un réseau informatique

Les réseaux informatiques constituent aujourd'hui un élément essentiel de notre monde interconnecté. Pour assurer la communication entre les différents appareils et permettre la transmission des données, il est nécessaire d'avoir une infrastructure solide et performante. Il est bien important de définir les composants ou les périphériques d’un réseau informatique dont on distingue 2 types d'équipements :

I.5.1 Les équipements d'interconnexion

Sont des composants clés des réseaux informatiques qui permettent de connecter différents segments de réseau et d'assurer la communication entre les appareils, on trouve :

I.5.1.1 Les commutateurs (switch)

Les commutateurs également connu sous le nom de switch en anglais. Les Switches sont connus comme étant des Hubs intelligents. La raison de cette dénomination est le fait qu'un Switch construit une table d'adresses MAC pour garder une trace des différentes adresses matérielles et des ports associés à ces adresses. Ils font partie composants clés qui permet de connecter différents dispositifs au sein d'un réseau local. Que ce soit au sein d'une entreprise, d'une institution éducative ou même d'un foyer, les commutateurs jouent un rôle fondamental dans le bon fonctionnement des réseaux.
Les switches sont des périphériques réseaux qui opèrent sur la couche 2 du modèle OSI, et qui peuvent éviter les boucles à travers l'utilisation du Spanning Tree Protocol.

Figure I.13: switch. [12]

I.5.1.1.1 Le fonctionnement d'un commutateur

Le fonctionnement d'un commutateur repose sur le principe de commutation de paquets. Lorsqu'un périphérique envoie des données vers un autre périphérique connecté au même commutateur, celui-ci analyse l'adresse de destination de chaque paquet et les transfère uniquement vers le port connecté à ce périphérique spécifique, minimisant ainsi les perturbations et optimisant les performances du réseau.
Le commutateur maintient une table de correspondance des adresses MAC, appelée table de commutation. Cette table enregistre l'adresse MAC de chaque périphérique connecté au commutateur et associe cette adresse à un port spécifique. Lorsqu'un paquet arrive au commutateur, il extrait l'adresse MAC de destination du paquet et recherche dans sa table de commutation pour déterminer vers quel port il doit être envoyé. Le paquet est ensuite transmis uniquement au port approprié, évitant ainsi les envois inutiles et les saturations du réseau.

Les commutateurs sont équipés de plusieurs ports qui permettent de connecter les différents dispositifs au réseau. Chaque port est capable de détecter automatiquement le type de connexion utilisé, que ce soit une connexion Ethernet, Wi-Fi ou même fibre optique. Cette polyvalence permet aux commutateurs de s'adapter aux différentes technologies utilisées par les appareils connectés.

L'un des avantages majeurs des commutateurs est leur capacité à gérer le trafic réseau de manière intelligente. Grâce à des algorithmes de commutation, les commutateurs peuvent déterminer la meilleure route à emprunter pour transmettre les paquets de données. Cela permet d'optimiser les performances du réseau, en évitant les congestions et en assurant une transmission fluide des données.

De plus, les commutateurs offrent également des fonctionnalités de gestion avancées. Ils permettent de segmenter le réseau en différentes Virtual Local Area Networks (VLANs), ce qui facilite la gestion des différents groupes d'appareils connectés. Ils offrent également des fonctionnalités de sécurité telles que l'authentification des utilisateurs, le contrôle d'accès et la surveillance du trafic réseau, garantissant ainsi la confidentialité et l'intégrité des données.

En conclusion, les commutateurs sont des outils indispensables dans la mise en place et la gestion des réseaux informatiques. Ils permettent de connecter efficacement les appareils au sein d'un réseau local, tout en assurant une transmission sécurisée des données. Grâce à leurs fonctionnalités avancées, les commutateurs facilitent la gestion et l'optimisation du trafic réseau, garantissant ainsi des performances optimales du réseau.

I.5.1.2 Les concentrateurs (hubs)

Un concentrateur est un appareil central qui permet de connecter plusieurs périphériques au sein d'un même réseau. Il agit comme un point de convergence où les données provenant des différents périphériques sont rassemblées et envoyées vers leur destination respective. En d'autres termes, il agit comme une plaque tournante des communications au sein du réseau.
Il agit au niveau 1 du modèle OSI (la couche physique), Les Hubs ne peuvent pas traiter la couche 2 ou la couche 3 du trafic. La couche 2 traite les adresses matérielles (MAC) et la couche 3 les adresses logiques (IP). Donc, les hubs ne peuvent pas traiter l'information basée sur les adresses MAC ou IP.

Concrètement, un concentrateur reçoit les signaux électriques émis par les périphériques connectés, les amplifie et les transmet à tous les autres périphériques du réseau. Cela permet à chaque appareil de recevoir les données transmises par les autres périphériques, favorisant ainsi la communication et les échanges d'informations.

L'avantage principal d'un concentrateur est sa capacité à permettre la connectivité entre plusieurs périphériques, sans qu'une configuration complexe soit nécessaire. En effet, il suffit de brancher les câbles des périphériques sur les ports du concentrateur pour établir la communication. De plus, les concentrateurs sont généralement peu coûteux, ce qui en fait des solutions abordables pour les petites entreprises et les réseaux domestiques.

Cependant, les concentrateurs présentent également quelques limitations. Tout d'abord, ils fonctionnent en mode half-duplex, ce qui signifie que les échanges de données ne peuvent se faire que dans un seul sens à la fois. Cela peut entraîner des ralentissements dans la transmission des données, notamment lorsque plusieurs appareils essaient de communiquer simultanément.

De plus, les concentrateurs diffusent les données à tous les périphériques connectés, indépendamment de leur destination. Par conséquent, les informations destinées à un périphérique spécifique doivent

être filtrées par le périphérique lui-même, ce qui peut entraîner une perte de bande passante et une augmentation du trafic réseau.

Pour pallier ces limitations, les concentrateurs ont été progressivement remplacés par des commutateurs Ethernet, qui offrent des fonctionnalités plus avancées et une meilleure efficacité de transmission des données. Néanmoins, dans les réseaux plus anciens ou pour des applications spécifiques, les concentrateurs restent encore utilisés.

Figure I.14: Hub [13]

En conclusion, les concentrateurs sont des composants importants dans la mise en place d'un réseau informatique, permettant la connectivité entre plusieurs périphériques. Bien qu'ils présentent certaines limitations en termes de vitesse de transmission et de gestion du trafic, ils restent une solution économique et simple à utiliser, notamment dans les petits réseaux ou les configurations moins complexes.

I.5.1.3 Les routeurs

Les routeurs, également appelés routeurs en français, est aussi l'un des composants de base d'un réseau informatique.

Un router est un dispositif matériel ou logiciel utilisé pour diriger le trafic réseau (diriger les paquets de données entre eux). Il agit comme un point de connexion centralisé qui permet de relier différents appareils au sein d'un réseau local (LAN) ou de connecter plusieurs réseaux entre eux, tels que des LAN, des réseaux étendus (WAN) ou encore l'Internet.
C'est un équipement qui qui fonctionnent sur la couche 3 du modèle OSI, On appelle parfois les routeurs des switches de niveau 3.

Figure I.15: router [14]

I.5.1.3.1 Fonctionnement d'un router

Techniquement, un router fonctionne en utilisant le protocole de routage ou tables de routage, qui contiennent des informations sur les différents réseaux connectés et les chemins pour les atteindre ; Ce protocole permet au router de déterminer le chemin optimal pour acheminer les données d'un point à un autre ; Lorsqu'un paquet de données est reçu par un routeur, celui-ci examine l'adresse de destination du paquet et consulte sa table de routage pour déterminer le prochain saut ou le prochain routeur à utiliser pour acheminer les données.

Et ce processus est répété à chaque saut jusqu'à ce que le paquet atteigne sa destination finale en analysant les adresses IP des appareils connectés.

En effet, chaque appareil dispose d'une adresse IP unique qui lui permet d'être identifié au sein du réseau. Le router utilise ces adresses IP pour décider par quel chemin les données doivent passer afin d'atteindre leur destination.

Un autre aspect important des routeurs est leur capacité à filtrer et à contrôler le trafic réseau. Grâce à des fonctionnalités de sécurité intégrées, les routeurs peuvent mettre en place des règles et des politiques de gestion du réseau, notamment en autorisant ou en refusant l'accès à certaines ressources ou en bloquant les attaques potentielles. Ces fonctionnalités de sécurité offrent une couche supplémentaire de protection pour les données et les appareils connectés.

En outre, les routeurs peuvent également fonctionner avec des fonctionnalités avancées telles que le Network Address Translation (NAT), qui permet de traduire les adresses IP privées des appareils du réseau local en une adresse IP publique unique pour accéder à Internet. Cette fonctionnalité permet de surmonter la limitation des adresses IP publiques et de garantir que tous les appareils connectés au réseau peuvent accéder à Internet de manière transparente.

En résumé, les routeurs sont des composants essentiels d'un réseau informatique en permettant la connexion, le routage et la sécurité des données transitant entre les appareils connectés. Ils jouent un rôle clé dans la gestion efficace et sécurisée des réseaux, tant au niveau local que global. Grâce à leur

capacité à diriger intelligemment le trafic, à filtrer les données et à protéger les appareils contre les menaces potentielles, les routeurs sont devenus des outils indispensables dans le monde d'informatique ou toute personne travaillant dans le domaine des réseaux.

I.5.1.3.2 Interconnexion des routeurs et des commutateurs

Afin de maintenir une communication flux et efficace au sein d'un réseau informatique, il est essentiel d'assurer une interconnexion robuste entre les routeurs et les commutateurs. L'interconnexion de ces équipements constitue le fondement de l'infrastructure réseau, permettant le transfert de données de manière efficace et fiable.

Tout d'abord, il convient de comprendre le rôle et les fonctionnalités des routeurs et des commutateurs. Les routeurs sont des dispositifs chargés de diriger le trafic des données entre différents réseaux. Ils utilisent des protocoles de routage pour déterminer le chemin optimal des paquets de données vers leur destination. Les commutateurs, quant à eux, sont responsables de l'acheminement des paquets de données au sein d'un réseau local (LAN). Ils utilisent des tables de commutation pour envoyer les données directement aux destinataires appropriés.

L'interconnexion des routeurs et des commutateurs permet de créer un réseau étendu (WAN) ou un réseau local (LAN) plus étendu et complexe. Elle offre la possibilité d'avoir plusieurs sous-réseaux interconnectés, permettant ainsi une meilleure gestion du trafic et une répartition de charge efficace. De plus, cela permet également de garantir la redondance des liens, réduisant ainsi les risques de pannes et assurant une continuité des services.

Pour réaliser cette interconnexion, plusieurs technologies peuvent être utilisées. L'une des méthodes couramment employées est l'utilisation de câbles réseau, tels que les câbles Ethernet, pour établir des connexions physiques entre les différentes interfaces des routeurs et des commutateurs. Ces câbles peuvent être en cuivre (comme les câbles RJ-45) ou en fibre optique, offrant des débits plus élevés et une plus grande capacité de transmission sur de longues distances.

Parallèlement aux câbles, les technologies sans fil, telles que le Wi-Fi, peuvent également être utilisées pour interconnecter les routeurs et les commutateurs. Ces technologies offrent une flexibilité accrue en permettant une connectivité sans fil entre les différents équipements, évitant ainsi le besoin de câblage physique dans certains cas spécifiques.

Une autre approche pour interconnecter les routeurs et les commutateurs consiste à utiliser des protocoles de routage et de commutation. Ces protocoles, tels que le protocole de routage OSPF (Open Shortest Path First) ou le protocole de commutation VLAN (Virtual Local Area Network), permettent aux équipements de se mettre automatiquement d'accord sur les routes à prendre et les chemins à emprunter pour transférer les paquets de données de manière optimale.

En conclusion, l'interconnexion des routeurs et des commutateurs est un élément essentiel dans la création et la gestion d'une infrastructure réseau solide et performante. Que ce soit par le biais de câbles, de technologies sans fil ou de protocoles de routage et de commutation, cette interconnexion permet de garantir une communication fluide et fiable au sein d'un réseau informatique, facilitant ainsi le transfert de données entre les différents équipements et utilisateurs.

I.5.1.4 Les cartes réseaux (NIC)

Les cartes réseaux sont l'un des composants essentiels d'un réseau informatique. Elles jouent un rôle très important dans la transmission des données entre les différents appareils connectés au réseau.

Une carte réseau, également appelée carte d'interface réseau ou NIC (Network Interface Card), est une carte d'extension qui se connecte à la carte mère d'un ordinateur. Elle permet à cet ordinateur de se connecter à d'autres appareils du réseau, qu'il s'agisse d'autres ordinateurs, de serveurs, d'imprimantes ou d'autres périphériques réseau.

Les cartes réseaux existent sous différentes formes, selon le type de réseau auquel elles sont destinées. Les deux principales catégories de cartes réseaux sont les cartes filaires et les cartes sans fil.

Figure I.16: NIC. [15]

Les cartes réseaux filaires, comme leur nom l'indique, se connectent au réseau à l'aide d'un câble Ethernet. Elles utilisent généralement des ports Ethernet RJ45 pour se connecter aux commutateurs ou routeurs du réseau. Ces cartes sont couramment utilisées dans les environnements professionnels où la vitesse et la stabilité de la connexion sont primordiales.

D'autre part, les cartes réseaux sans fil utilisent des technologies telles que le Wi-Fi pour établir une connexion avec le réseau. Elles sont plus courantes dans les environnements domestiques ou les petites entreprises, car elles offrent une plus grande flexibilité en permettant aux appareils de se connecter au réseau sans avoir besoin d'un câble physique. Les cartes réseaux sans fil sont également en constante évolution pour offrir des vitesses de connexion plus rapides et une meilleure couverture réseau.

En plus de fournir une connectivité au réseau, les cartes réseaux peuvent également être dotées de fonctionnalités supplémentaires, telles que l'accélération matérielle, la gestion de la qualité de service (QoS) ou encore la prise en charge du protocole de sécurité WPA/WPA2 pour les connexions sans fil. Ces fonctionnalités permettent d'améliorer les performances et la sécurité des connexions réseau.

Il est important de choisir la carte réseau appropriée en fonction des besoins spécifiques de l'environnement réseau. Les facteurs à prendre en compte comprennent la vitesse de connexion souhaitée (par exemple, 1 Gigabit ou 10 Gigabits), la compatibilité avec les protocoles réseau couramment utilisés (tels que IPv4 ou IPv6), ainsi que la compatibilité avec les systèmes d'exploitation pris en charge.

En conclusion, les cartes réseaux sont des composants essentiels d'un réseau informatique. Elles permettent de relier les différents appareils entre eux et d'assurer la transmission des données. Que ce soit via des connexions filaires ou sans fil, les cartes réseaux offrent des fonctionnalités avancées pour répondre aux besoins spécifiques de chaque environnement réseau. Il est donc crucial de choisir la carte réseau adaptée aux exigences techniques et aux contraintes du réseau auquel elle sera connectée.

I.5.1.5 Les ponts (Bridge)

Un pont est un équipement qui fonctionne au niveau liaison de données. Il interconnecte deux réseaux locaux de même type (par exemple deux réseaux Ethernet). Le principe général du pont c'est de décoder les adresses machine et qui peuvent donc décider de faire traverser au non les paquets ; il ne transmet les trames que si la station destinataire est sur l'autre réseau afin d'éviter du trafic inutile sur le réseau.

I.5.1.6 Les passerelles (Gateway)

Une passerelle est un équipement qui fonctionne au niveau de l'application. C'est un système informatique connecté à au moins deux réseaux utilisant des protocoles différents. Elle assure la conversion des formats de données et des protocoles entre ces réseaux. Les passerelles permettent d'interconnecter des réseaux hétérogènes.

I.5.1.7 Les points d'accès wifi

Dans le cadre du fonctionnement d'un réseau informatique, l'un des éléments essentiels est la présence de points d'accès WiFi. Ces derniers jouent un rôle primordial en permettant aux utilisateurs de se connecter et d'accéder aux ressources du réseau de manière sans fil. Dans cette partie, nous explorerons les différents aspects liés aux points d'accès WiFi, leurs fonctionnalités et leur importance au sein d'un réseau.

Tout d'abord, il convient de comprendre ce qu'est un point d'accès WiFi. Il s'agit d'un périphérique qui permet la connexion sans fil à un réseau, en utilisant les ondes radio. Les points d'accès WiFi sont souvent utilisés dans les environnements domestiques, les entreprises, les campus universitaires, les cafés ou les hôtels, permettant ainsi aux utilisateurs de se connecter à internet et d'accéder aux ressources partagées, telles que les serveurs, les imprimantes ou les fichiers partagés.

L'un des avantages majeurs des points d'accès WiFi est leur praticité et leur flexibilité. Contrairement aux connexions filaires, ils permettent aux utilisateurs de se connecter de n'importe où à l'intérieur de la portée du signal WiFi. Cela offre une grande liberté de mouvement et facilite la connectivité dans les zones où l'installation de câbles est difficile, voire impossible. Les utilisateurs peuvent ainsi se

déplacer librement avec leurs appareils (ordinateurs portables, smartphones, tablettes) tout en restant connectés au réseau.

Les points d'accès WiFi peuvent également être configurés pour offrir plusieurs réseaux virtuels, également connus sous le nom de SSID (Service Set Identifier). Cette fonctionnalité permet de segmenter le réseau en différents sous-réseaux, ce qui permet de séparer les différents groupes d'utilisateurs ou de créer des réseaux invités sécurisés.
Par exemple, dans un environnement d'entreprise, les employés peuvent se connecter à un réseau privé, tandis que les visiteurs peuvent accéder à un réseau invité avec des restrictions d'accès plus élevées.

La sécurité est un aspect essentiel lorsqu'il s'agit de points d'accès WiFi. Étant donné que le signal WiFi est diffusé dans l'air, il peut être capté par des tiers non autorisés. Ainsi, il est indispensable de mettre en place des mesures de sécurité appropriées pour protéger le réseau et les données qui y circulent. Parmi les méthodes de sécurité les plus couramment utilisées, on retrouve le chiffrement WPA2 (Wi-Fi Protected Access 2), qui permet de sécuriser les communications entre les points d'accès et les utilisateurs.

Enfin, il est essentiel de prendre en compte la portée des points d'accès WiFi. Cela dépendra du modèle et de la puissance du point d'accès utilisé. La portée peut varier en fonction des obstacles physiques présents dans l'environnement, tels que les murs ou les meubles. Il est donc important de planifier soigneusement le positionnement des points d'accès afin de couvrir efficacement la zone souhaitée.

Figure I.17: AP [16]

En conclusion, les points d'accès Wifi constituent une composante essentielle des réseaux informatiques modernes. Leur capacité à fournir une connectivité sans fil pratique et flexible fait d'eux une solution incontournable pour permettre aux utilisateurs de se connecter et de bénéficier des ressources du réseau. La sécurité et la portée sont également des éléments à prendre en compte lors de la mise en place de ces points d'accès afin d'assurer un fonctionnement optimal et sécurisé du réseau Wifi.

I.5.2 Les équipements finaux

Les équipements finaux d'un réseau informatique sont les appareils qui se connectent directement au réseau et qui utilisent les ressources du réseau pour communiquer entre eux. Ces équipements sont généralement des terminaux qui peuvent être des ordinateurs, des imprimantes, des tablettes, des smartphones, etc.

I.6 Les supports de transmission

Pour que les informations puissent circuler au sein d'un réseau informatique, il est nécessaire de relier les différents équipements à l'aide des supports de transmission qui transporte les données sous forme de signaux ; Les signaux électriques utilisent les supports à base de cuivre et les signaux lumineux utilisent les fibres optiques ou l'air.

Un support de transmission est un canal de liaison on distingue 2 catégories principales :
Liaison guidée : avec fils (les câbles) et liaison non guidée : sans fils

I.6.1 Les supports filaires

Les supports de transmission filaires utilisent des câbles physiques pour transmettre les données. Les principaux types de supports filaires sont :

I.6.1.1 Les câbles coaxiaux

Les câbles coaxiaux sont un type de câble électrique utilisé pour transmettre des signaux de haute fréquence. Composé d'un fil de cuivre central entouré d'un isolant et d'un blindage à vrai dire Ils se composent de quatre couches concentriques : une âme conductrice, une isolation interne, une tresse conductrice ou un blindage métallique, et une gaine externe protectrice. Ce type de câble est couramment utilisé dans les systèmes de télévision par câble, les réseaux informatiques, et pour les connexions d'antennes radio.

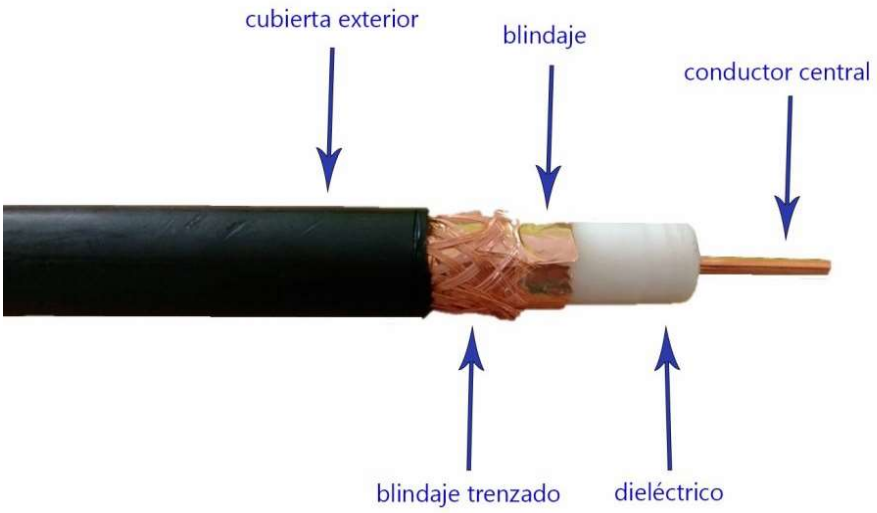


Figure I.18: câble coaxial. [17]

I.6.1.2 Les câbles pairs torsadés

Ce câble est composé de deux fils de cuivre isolés et torsadés, il se compose de plusieurs paires de fils de cuivre, chaque paire étant torsadée ensemble. Les câbles à paire torsadées sont divisés en plusieurs types, en fonction de la présence ou non de blindage métallique et de la qualité des matériaux utilisés, notamment :

UTP (Unshielded Twisted Pair) : Ces câbles n'ont pas de blindage supplémentaire. Ils sont moins coûteux et plus faciles à installer que les câbles blindés, mais ils offrent une protection moindre contre les interférences électromagnétiques.

STP (Shielded Twisted Pair) : Ces câbles ont un blindage autour de chaque paire de fils ou autour de l'ensemble des paires, offrant ainsi une meilleure protection contre les interférences électromagnétiques. Ils sont utilisés dans les environnements où il y a beaucoup d'interférences électromagnétiques, comme dans les usines ou les environnements industriels.

FTP (Foiled Twisted Pair) : Ces câbles sont un compromis entre UTP et STP. Ils ont un blindage global, généralement une feuille métallique, qui entoure toutes les paires de fils, mais pas de blindage individuel autour de chaque paire. Cela offre une protection contre les interférences électromagnétiques supérieure à celle des UTP mais inférieure à celle des STP.

SFTP (Shielded Foiled Twisted Pair) : Un câble SFTP possède un blindage réalisé avec une tresse métallique qui entoure les fils conducteurs. Ce type de blindage est similaire à celui des câbles coaxiaux. Pour un câble FTP, le blindage est réalisé avec une feuille de métal (généralement en l'aluminium).

Ainsi, il existe en plusieurs catégories (Cat5, Cat5e, Cat6, etc.) offrant des débits et des distances de transmission différents. C'est le support le plus utilisé pour les réseaux Ethernet

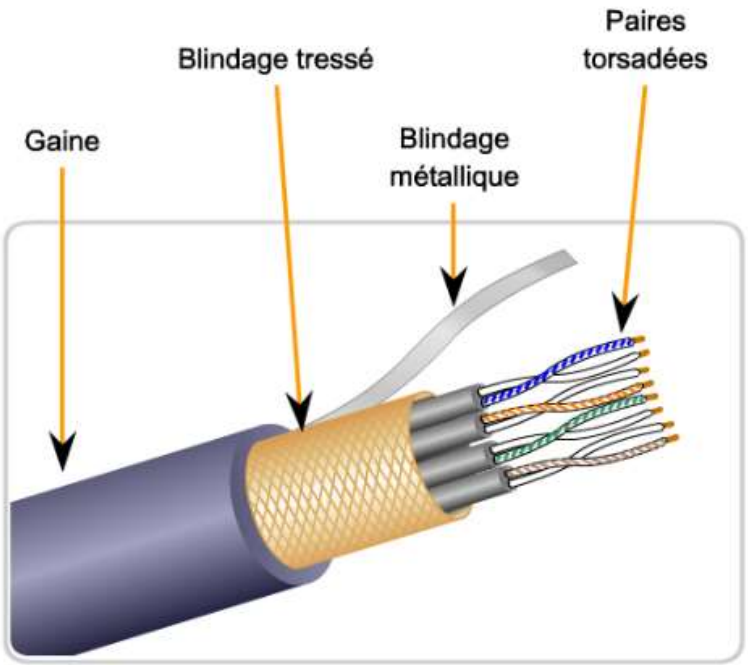


Figure I.19: pairs torsadés. [18]

I.6.1.3 Fibre optique

La fibre optique est un support de connexion fiable et performant. Dans le domaine des réseaux informatiques, la fibre optique occupe une place prépondérante en tant que support de connexion filaire. Elle présente de nombreux avantages par rapport aux câbles en cuivre traditionnels, notamment en termes de rapidité, de fiabilité et de capacité de transmission de données.

La fibre optique se compose d'un fin filament de verre ou de plastique, entouré d'une gaine protectrice. Grâce à l'utilisation de la lumière, elle permet de transmettre des informations sur de longues distances avec un taux de débit élevé. Contrairement aux câbles en cuivre, qui utilisent des signaux électriques et sont sensibles aux interférences électromagnétiques, la fibre optique offre une meilleure immunité aux perturbations extérieures, assurant ainsi une connexion plus stable et fiable.

Il existe deux types de fibre optique en fonction du diamètre de la fibre tel que :

Fibre monomode (SMF) : Possède un cœur très fin (environ 8 à 10 microns de diamètre) et permet la transmission d'un seul mode de lumière. Elle est utilisée pour les communications longue distance et les applications à haut débit, car elle offre une bande passante très élevée et une faible atténuation.
Fibre multimode (MMF) : Possède un cœur plus large (environ 50 à 62,5 microns de diamètre) et permet la transmission de plusieurs modes de lumière. Elle est généralement utilisée pour les communications à courte distance, comme dans les réseaux locaux (LAN), en raison de sa plus grande tolérance aux imperfections du câblage et de ses coûts moindres.

En termes de performance, la fibre optique offre des débits bien supérieurs à ceux des câbles en cuivre. Grâce à des technologies telles que le multiplexage en longueur d'ondes (WDM), la fibre optique permet de transmettre plusieurs flux de données simultanément sur une même fibre, augmentant ainsi la capacité de transmission. Cela en fait un choix privilégié dans les environnements où la bande passante est importante, tels que les entreprises, les centres de données ou les réseaux haut débit.

De plus, la fibre optique présente l'avantage d'être capable de transporter des signaux sur de très longues distances sans atténuation significative. Alors que les câbles en cuivre subissent une perte de signal à mesure que la distance augmente, la fibre optique conserve un signal fort et clair sur des distances pouvant atteindre plusieurs kilomètres. Cela en fait un choix idéal pour les réseaux étendus, les liaisons intercontinentales ou les opérateurs de télécommunication.

Enfin, la fibre optique offre également une sécurité accrue par rapport aux câbles en cuivre. Étant donné que le signal est transmis sous forme de lumière, il est moins susceptible d'être intercepté ou piraté. Cela en fait une solution privilégiée pour les communications sensibles ou confidentielles, et constitue un atout majeur dans le domaine de la sécurité des données.

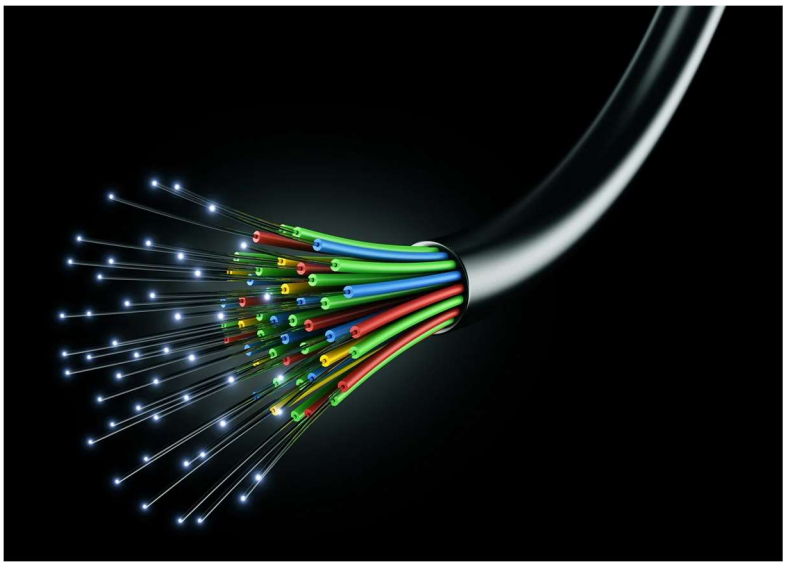


Figure I.20: fibre optique.[19]

En résumé, la fibre optique est devenue un support de connexion filaire incontournable dans le paysage des réseaux informatiques. Avec ses avantages en termes de rapidité, de fiabilité, de capacité de transmission et de sécurité, elle offre une solution performante pour répondre aux besoins croissants en bande passante et assurer des communications efficaces dans les environnements professionnels.

I.6.2 Les supports sans fils

Les supports de transmission sans fil utilisent des ondes électromagnétiques pour transmettre les données. On trouve :

I.6.2.1 La technologie Wifi

Dans la société actuelle, la connectivité sans fil est devenue essentielle. Grâce à l'évolution technologique, nous pouvons maintenant profiter du WiFi, une technologie qui permet de se connecter à Internet sans avoir à utiliser de câbles physiques. Le WiFi, également connu sous le nom de réseau local sans fil (WLAN), offre aux utilisateurs une liberté de mouvement et une accessibilité inégalée.

Les réseaux WiFi fonctionnent en utilisant des ondes radio pour transmettre des signaux entre un point d'accès sans fil et les dispositifs qui se connectent à ce réseau. Ces points d'accès sans fil sont généralement connectés à un réseau filaire, tel qu'un fournisseur d'accès Internet, qui permet aux utilisateurs de se connecter à Internet via le WiFi.

La technologie WiFi utilise différentes fréquences radio pour la transmission des données. Les fréquences les plus couramment utilisées sont de 2,4 GHz et 5 GHz. La fréquence de 2,4 GHz offre une plus grande portée, mais une vitesse de transfert de données plus lente, tandis que la fréquence de 5 GHz offre une plus grande vitesse mais une portée plus limitée. Certains routeurs WiFi modernes supportent également des fréquences supplémentaires, telles que 6 GHz, pour une connectivité améliorée.

Pour se connecter à un réseau WiFi, un dispositif doit être équipé d'une carte réseau sans fil (adaptateur WiFi) capable de recevoir et de transmettre les signaux WiFi. La plupart des smartphones, tablettes, ordinateurs portables et autres appareils électroniques sont maintenant dotés de cette fonctionnalité intégrée. Une fois que l'appareil est à portée d'un réseau WiFi, il peut se connecter en entrant un mot de passe, si le réseau est sécurisé, ou se connecter automatiquement si la sécurité est désactivée.

Les avantages du WiFi sont nombreux. Il permet aux utilisateurs de se connecter à Internet depuis n'importe quel endroit à portée d'un point d'accès sans fil, que ce soit à la maison, dans des lieux publics tels que les cafés, les aéroports, les hôtels, les bibliothèques, etc. Cela offre une grande flexibilité et la possibilité de travailler, étudier, socialiser ou se divertir en ligne où que l'on soit.

De plus, le WiFi facilite le partage de ressources et la mise en réseau de différents appareils. Par exemple, plusieurs utilisateurs peuvent partager une même connexion Internet à partir d'un seul point d'accès WiFi. En outre, il est possible de connecter des appareils intelligents tels que des téléviseurs, des enceintes, des thermostats, etc. à un réseau WiFi pour une gestion centralisée et un contrôle à distance.

Malgré ses nombreux avantages, le WiFi présente également quelques inconvénients. La portée limitée du signal peut poser problème dans de grands espaces ou des bâtiments avec des murs épais. De plus, étant donné que les signaux WiFi utilisent des ondes radio, ils peuvent être perturbés par d'autres dispositifs électriques, tels que les téléphones sans fil, les micro-ondes, les babyphones, etc. Cela peut entraîner des interférences et une dégradation de la qualité du signal.

En conclusion, le WiFi est devenu un élément essentiel de notre vie quotidienne, offrant une connectivité sans fil pratique et accessible. Que ce soit pour le travail, les études ou les loisirs, le WiFi nous permet de rester connectés et de profiter pleinement de l'univers numérique dans lequel nous vivons.

I.7 Conclusion

Les réseaux informatiques jouent un rôle central dans la connectivité et la communication modernes. Ils sont composés de divers éléments interconnectés tels que les routeurs, les commutateurs, les serveurs et les dispositifs finaux, chacun ayant une fonction spécifique dans la transmission et la gestion des données. La compréhension de ces structures et composants est fondamentale pour saisir comment les réseaux facilitent l'échange d'informations à travers le monde.

Cependant, au-delà de cette compréhension générale des réseaux, il est également crucial de se pencher sur la dynamique du trafic des données au sein de ces structures. Les données doivent naviguer efficacement à travers les différents composants du réseau, souvent en suivant des protocoles complexes et des chemins multiples.

Ainsi, une question essentielle se pose : comment ces données circulent-elles efficacement sur ce réseau et quels mécanismes assurent leur transit fluide et sécurisé ?

Chapitre II : Trafic des données sur un réseau informatique

II.1 Introduction

De nos jours, les réseaux informatiques constituent l'épine dorsale de notre monde numérique, facilitant la communication et le partage d'informations à une échelle sans précédent. Au cœur de cette connectivité se trouve le flux incessant de données, circulant à travers les câbles et les ondes radio, reliant des millions d'appareils à travers le globe. Ce flux constant d'informations, connu sous le nom de trafic de données, est non seulement vital pour le fonctionnement des réseaux informatiques, mais il est également le moteur qui propulse notre société vers de nouveaux sommets de connectivité et de collaboration.

L'un des principaux défis liés au trafic des données sur un réseau informatique réside dans la quantité énorme d'informations échangées chaque jour. Avec la prolifération des appareils connectés, des applications en ligne et des plateformes de partage de données, le volume de données échangées a explosé ces dernières années. Cependant, cette croissance exponentielle soulève également des questions quant à la sécurité et à la confidentialité des données.

L'un des aspects les plus préoccupants du trafic des données concerne la protection de la vie privée. En effet, les utilisateurs d'un réseau informatique peuvent être exposés à des risques tels que la collecte excessive de leurs données personnelles, la surveillance accrue par des tiers non autorisés et même le potentiel de piratage et de vol de données sensibles. Il est donc essentiel de comprendre les mécanismes et les outils de protection mis en place pour atténuer ces risques et assurer la confidentialité des utilisateurs.

En outre, l'optimisation du trafic des données est un enjeu primordial dans un réseau informatique. Le temps de latence, la bande passante et la qualité de service sont autant de paramètres importants qui doivent être pris en compte pour garantir des communications fluides et efficaces. Une gestion appropriée du trafic peut améliorer les performances du réseau et optimiser l'utilisation des ressources disponibles.

En conclusion, Le trafic de données sur un réseau informatique est bien plus qu'une simple transmission d'octets d'un point à un autre.

Dans cette partie, nous allons explorer en détail la manière dont les données circulent sur un réseau en mettant l'accent sur les aspects techniques, les défis actuels et les perspectives d'avenir.

II.2 Compréhension du Trafic des données sur un réseau informatique

La compréhension du trafic des données sur un réseau informatique est essentielle pour assurer son bon fonctionnement, sa sécurité et son efficacité. Le trafic de données fait référence au mouvement des informations à travers un réseau. Il est le reflet de nos interactions, de nos échanges, de nos transactions et de nos communications à travers le monde. Chaque courriel envoyé, chaque site Web visité, chaque vidéo diffusée, et chaque message partagé contribue à ce vaste océan de données qui alimente notre ère numérique.

II.2.1 Flux de données entre les différentes entités du réseau

Le flux de données entre les différentes entités d'un réseau informatique est le processus par lequel les informations sont transmises d'un point à un autre à travers le réseau. Ce flux de données implique plusieurs éléments clés et suit un acheminement défini par les protocoles de communication et les infrastructures réseau pour assurer la communication efficace et fiable entre les différents ordinateurs, serveurs, routeurs et autres périphériques connectés au réseau.

Le flux de données se matérialise par l'envoi et la réception d'informations, que ce soit des fichiers, des paquets de données ou des commandes, entre les différents acteurs du réseau.
Cette circulation des données peut prendre différentes formes selon la structure et la topologie du réseau par exemple dans un réseau local (LAN), les données sont généralement transmises via des câbles Ethernet, tandis que dans un réseau étendu (WAN), elles sont transmises à travers des liens de télécommunication tels que des connexions Internet ou des lignes louées.

L'acheminement des données d'une entité à une autre se fait grâce à des protocoles de communication qui définissent les règles et les formats d'échange. Parmi les protocoles les plus courants, on retrouve le protocole IP (Internet Protocol) qui permet l'adressage et le routage des paquets de données sur Internet, ainsi que le protocole TCP (Transmission Control Protocol) qui garantit la fiabilité de la transmission en mettant en place des mécanismes de vérification et de retransmission des données.

Le flux de données entre les différentes entités du réseau peut également être contrôlé par des dispositifs tels que les commutateurs réseau et les routeurs. Ces appareils jouent un rôle central dans la gestion du trafic en analysant les adresses des paquets de données et en déterminant le chemin optimal pour leur transmission. Ils sont capables de filtrer, rediriger ou regrouper les données en fonction de différents critères tels que les priorités, les politiques de sécurité ou la congestion du réseau.

En outre, il est important de prendre en compte la bande passante disponible sur le réseau pour assurer un flux de données optimal. En effet, une bande passante limitée peut entraîner des retards dans la transmission des données, ce qui peut avoir un impact négatif sur les performances et la réactivité du réseau. Il est donc essentiel de dimensionner correctement les ressources du réseau en fonction des besoins de trafic et de mettre en place des mécanismes de gestion de la congestion pour éviter les engorgements.

II.2.2 Types de trafic

Parmi les différents types de trafic que l'on peut rencontrer, on distingue notamment le trafic unicast, multicast et broadcast. Chacun de ces types de trafic présente des caractéristiques spécifiques, offrant ainsi des solutions adaptées à des besoins particuliers.

Le trafic unicast

Correspond à une transmission de données point à point, c'est-à-dire d'un émetteur vers un destinataire unique. Ce type de trafic est couramment utilisé dans les échanges de fichiers, les conversations en ligne ou encore l'accès aux sites web. L'émetteur envoie les données à une adresse IP spécifique et seul le destinataire associé à cette adresse recevra les informations transmises. Cela assure une communication efficace et privée entre les deux parties.

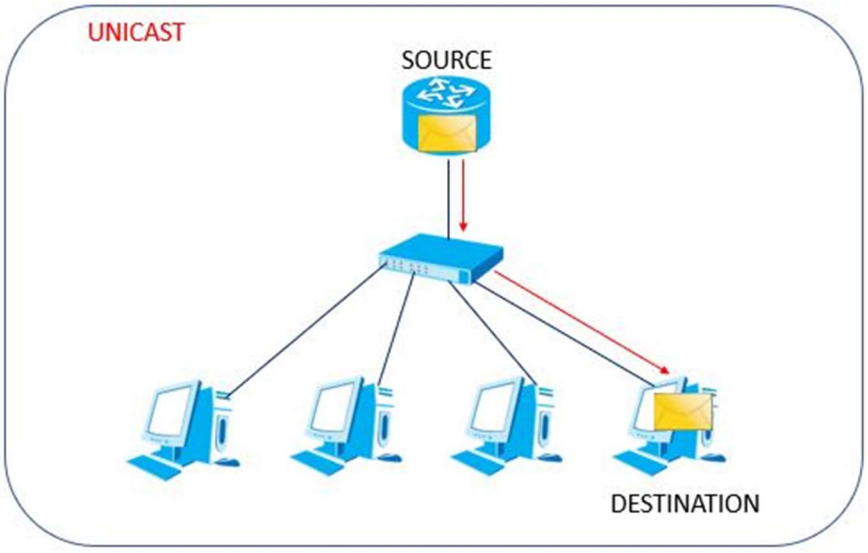


Figure II.21: Trafic unicast. [20]

Le trafic multicast

Il concerne la transmission de données d'un émetteur vers un groupe de destinataires. Contrairement au trafic unicast, les données envoyées en multicast sont dupliquées pour être reçues par plusieurs membres du groupe. Cela permet d'optimiser la bande passante du réseau en évitant une transmission individuelle de chaque paquet de données à chaque membre. Le trafic multicast est souvent utilisé pour la diffusion en direct de contenus vidéo ou audio, les visioconférences de groupe ou encore la distribution de mises à jour logicielles.

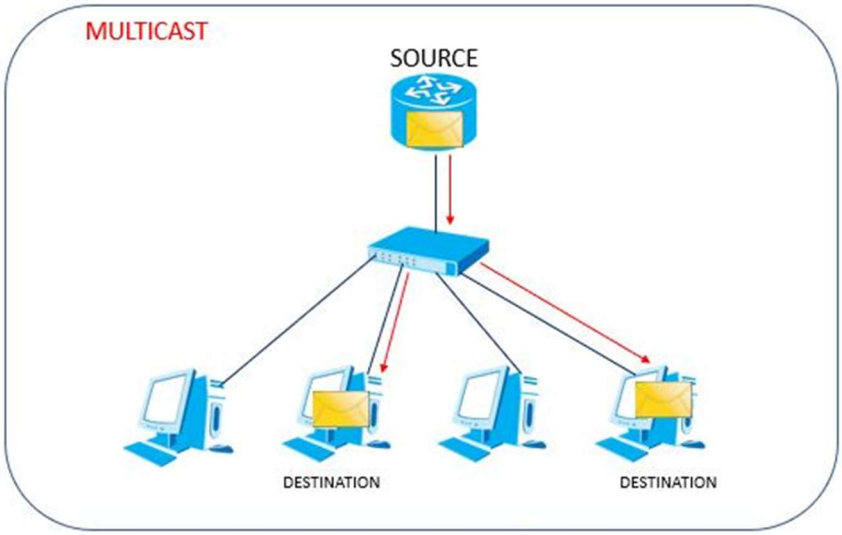


Figure II.22: le trafic multicast [22]

Le trafic broadcast

Correspond à une diffusion des données à tous les nœuds d'un réseau. Dans ce cas, l'émetteur envoie les données sans distinction à tous les membres du réseau, sans nécessiter une adresse IP spécifique. Ce type de trafic est utilisé, par exemple, pour les annonces de service, la découverte des périphériques ou encore la diffusion de messages d'urgence. Bien qu'il permette une diffusion rapide des informations, le trafic broadcast peut générer une charge réseau importante et peut nécessiter des mécanismes de contrôle afin d'éviter les boucles de diffusion.

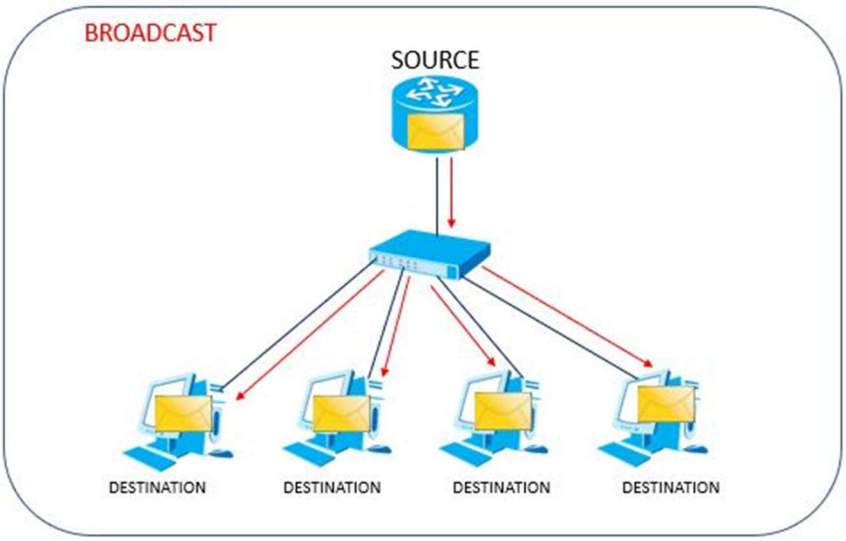


Figure II.23: le trafic de diffusion [20]

En conclusion, dans un réseau informatique, les différents types de trafic, tels que le unicast, le multicast et le broadcast, offrent des solutions variées pour répondre à différents besoins de transmission des données. Chaque type de trafic présente des avantages et des limitations qu'il convient de prendre en compte selon les contextes d'utilisation. Grâce à ces différentes approches, il est possible d'optimiser la communication et la diffusion des informations au sein d'un réseau.

II.3 Les Modèles de références

II.3.1 Modèle OSI

II.3.1.1 description

Le modèle OSI, acronyme pour "Open Systems Interconnection", est un modèle de référence largement utilisé dans le domaine des réseaux informatiques. Il a été créé par l'organisme de normalisation international, l'ISO (International Organization for Standardization), dans le but de fournir une structure claire et standardisée pour la conception, la mise en œuvre et la maintenance des réseaux de communication.

Le modèle OSI divise les tâches liées aux communications en réseaux en sept couches distinctes, allant de la couche physique à la couche d'application. Chaque couche est responsable de fonctions spécifiques, tout en interagissant avec les couches adjacentes pour permettre la transmission des données de manière fluide et ordonnée.

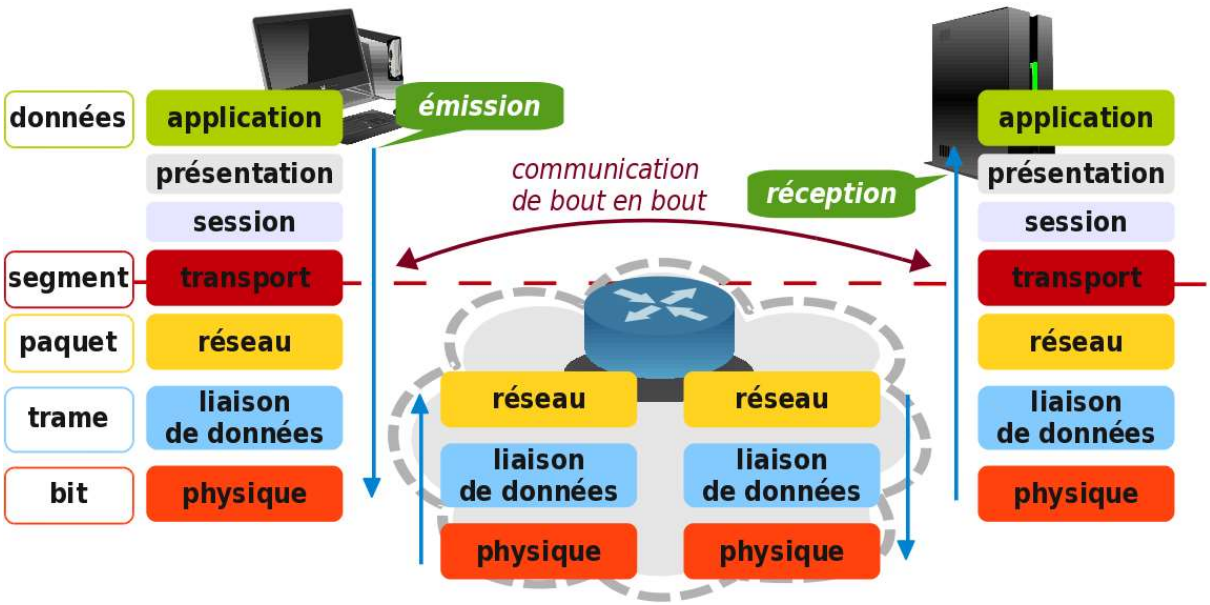


Figure II.24 : modélisation OSI [21]

II.3.1.2 les couches du modèle OSI

La couche physique

C'est La première couche, elle s'occupe de la transmission des données brutes sous forme de signaux électriques, optiques ou sans fil entre les dispositifs du réseau ; responsable de la transmission des bits à travers le média physique. Elle définit les caractéristiques physiques des supports de transmission, tels que les câbles Ethernet ou les ondes radios utilisées dans le Wifi.

La couche de liaison de données

C'est la deuxième couche, elle assure la fiabilité de la transmission des données sur un support physique spécifique. Elle effectue le découpage des données en trames, détecte les erreurs de

transmission et les corrige le cas échéant. Les protocoles couramment utilisés dans cette couche sont l'Ethernet et le protocole Point-to-Point (PPP).

La couche réseau

C'est la troisième couche, elle permet l'acheminement des données à travers différentes entités du réseau. Elle détermine le chemin optimal pour le transfert des données sous forme de paquets en utilisant des protocoles de routage, tels que le protocole IP (Internet Protocol).

La couche transport

C'est la quatrième couche, elle permet aux applications locales et distantes de communiquer, cette couche fournit des mécanismes de transport de bout en bout pour garantir une transmission fiable des données entre les applications source et de destination.

Elle gère la segmentation et le réassemblage des données, ainsi que la détection et la correction des erreurs.

Le protocole TCP (Transmission Control Protocol) est le protocole le plus couramment utilisé dans cette couche, c'est un protocole de contrôle de transmission, permet au niveau des applications de reconstituer les messages, de rassembler les segments dans l'ordre d'origine à l'aide d'un numéro d'ordre, de contrôler le flux de données, le protocole TCP utilise la taille de fenêtre pour identifier le nombre de segments qui sont envoyés par le périphérique final « émetteur » avant que le périphérique « récepteur » puisse envoyer une confirmation.

Le protocole UDP (User Datagram Protocol) c'est un protocole de couche transport, simple, sans connexion, il présente l'avantage d'imposer peu de surcharge pour l'acheminement de données, les blocs de communication utilisés dans le protocole UDP sont appelés des datagrammes, ce protocole utilisé par DNS, lecture vidéo en continu. [2]

La couche session

C'est la cinquième couche, elle établit, gère et termine les connexions entre les applications qui s'exécutent sur des ordinateurs différents. Elle permet également de synchroniser les échanges de données entre les applications, en fournissant des mécanismes d'ouverture, de fermeture et de maintien des sessions.

La couche présentation

C'est la sixième couche, elle assure la traduction et la conversion des données entre les différents formats utilisés par les applications. Elle fournit également des fonctionnalités de cryptage et de compression des données, afin de garantir leur confidentialité et leur efficacité lors des échanges.

La couche application

C'est la septième couche, elle permet aux applications de communiquer avec le réseau. Elle fournit des services tels que le courrier électronique, le transfert de fichiers et l'accès à des ressources distantes. Les protocoles les plus connus dans cette couche sont HTTP (Hypertext Transfer Protocol) pour le transfert de pages Web, SMTP (Simple Mail Transfer Protocol) pour l'envoi de courriels et FTP (File Transfer Protocol) pour le transfert de fichiers, ces protocoles définissent :

Les types de messages, la syntaxe des messages, la manière dont les messages sont envoyés et réponse attendue, l'interaction avec la couche inférieure suivante et la signification des champs d'information.

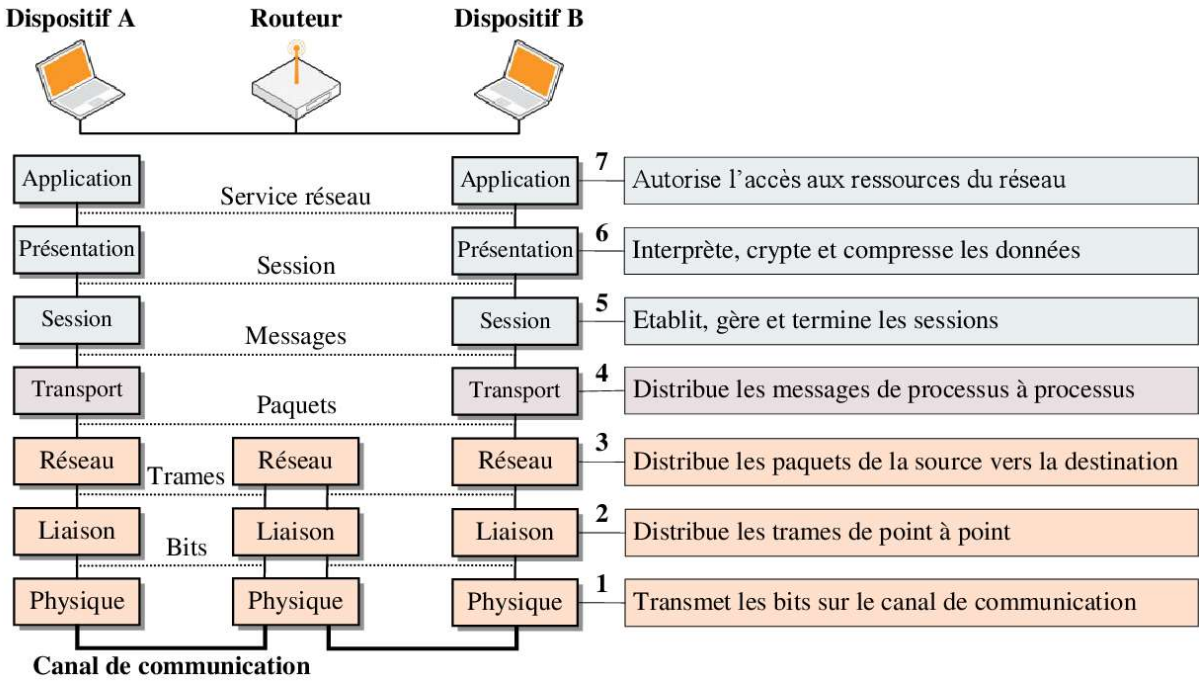


Figure II.25: fonctionnalités des couches du modèle OSI. [22]

En résumé, le modèle OSI fournit une structure logique et organisée pour la conception et la mise en œuvre des réseaux informatiques. Il permet d'assurer l'interopérabilité des différents systèmes, en décomposant les tâches liées aux communications en réseaux en sept couches distinctes. Ce modèle de référence est largement utilisé dans l'industrie des réseaux et constitue une base solide pour comprendre le fonctionnement des réseaux informatiques modernes.

II.3.1.3 La communication entre les couches

La communication entre les couches du modèle OSI est un processus complexe qui permet la transmission de données entre les systèmes de communication dont chaque couche N utilise la couche N-1 et fournit des services à la couche N+1
Voici une explication détaillée de ce processus :

Encapsulation des données
Nous avons vu que la couche en cours utilise les services de la couche au-dessous d'elle qui, à son tour, en offre pour la couche du dessous. Cette corrélation indique bien que certaines informations peuvent se retrouver d'une couche à une autre. Cela n'est possible que grâce au principe d'encapsulation. En d'autres termes, elle consiste à envelopper les données à chaque couche du modèle OSI.
Lorsqu'un système souhaite envoyer des données à un autre système, il commence par l'encapsulation des données à la couche application (couche 7). Les données sont empaquetées avec des en-têtes spécifiques à chaque couche ; L'en-tête contient des informations de contrôle et de gestion nécessaires à la communication, telles que les adresses source et de destination, les numéros de port, les informations de séquence, etc., créant ainsi un paquet de données. [3]

Transmission de données

Le paquet de données est ensuite transmis à la couche inférieure, la couche de présentation (couche 6), où il est compressé et chiffré si nécessaire. Le paquet est ensuite transmis à la couche session (couche 5), qui établit, gère et termine les connexions entre les applications

Coordination des transferts

Le paquet est ensuite transmis à la couche transport (couche 4), qui s'occupe de la coordination du transfert des données entre les systèmes. Elle garantit que les données seront fournies dans l'ordre correct et sans erreur

Acheminement des données

Le paquet est ensuite transmis à la couche réseau (couche 3), qui s'occupe de l'acheminement des données entre les réseaux. Elle détermine le chemin le plus efficace pour acheminer les données vers leur destination

Carrosserie de transmission (transmission physique)

Le paquet est ensuite transmis à la couche liaison de données (couche 2), qui s'occupe de la transmission des données entre les équipements de réseau voisins. Elle gère l'accès au média de transmission et la détection d'erreurs

Transmission sur les médias

Enfin, le paquet est transmis à la couche physique (couche 1), qui s'occupe de la transmission physique des données sur le média de transmission, comme un câble ou une onde radio.

Réception des données

Lorsque le colis arrive à destination, le processus est inversé. Les données sont dépaquetées à chaque couche, et les informations de contrôle et les en-têtes sont supprimées. Les données sont finalement remises à l'application destinataire, autrement dit dans la procédure de réception, chaque couche supprime son en-tête correspondant après l'avoir lu. Par exemple, l'en-tête NH (réseau) est supprimé dans la couche réseau de l'hôte récepteur après que ce dernier l'a lu.

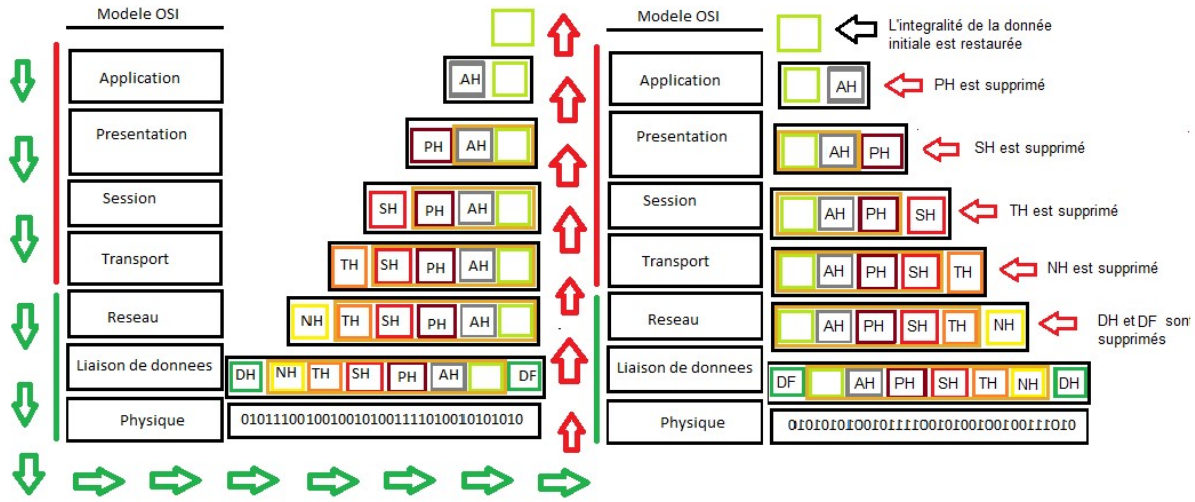


Figure II.26: principe d'encapsulation et de la communication entre les couches [23]

En résumé, la communication entre les couches du modèle OSI est un processus d'encapsulation et de transmission des données qui permet la communication entre les systèmes de communication. Chaque couche ajoute des informations de contrôle et des en-têtes spécifiques avant de transmettre le paquet à la couche inférieure, et inversement lors de la réception des données.

II.3.2 Modèle TCP/IP

II.3.2.1 description

Le modèle TCP/IP s'agit d'un ensemble de protocoles et de normes qui permettent la communication entre les différentes entités d'un réseau. Il réunit les protocoles de communication, notamment TCP et IP. Il décrit la manière dont les données sont transmises sur Internet.

II.3.2.2 les couches du modèle TCP/IP

Contrairement au modèle OSI qui comporte sept couches, le modèle TCP/IP se compose de quatre couches distinctes, chacune responsable d'un ensemble de fonctionnalités spécifiques.

La couche Application
C’est la couche la plus élevée, gère les applications et les services utilisés par les utilisateurs finaux, tels que le courrier électronique, le transfert de fichiers, la navigation web, etc. Les protocoles de cette couche incluent HTTP, FTP, SMTP, DNS, etc. Cette couche interagit avec les programmes réseau et les protocoles utilisés pour les communications.

La couche Transport
Qui est responsable de la gestion du transfert des données entre les différents systèmes. Assure la segmentation et le réassemblage des données, ainsi que la détection et la correction des erreurs. Le protocole principal utilisé à cette couche est le protocole de contrôle de transmission (TCP), qui garantit un transfert fiable des données en divisant les informations en segments, en assurant leur ordre d'arrivée et en gérant les erreurs de transmission et UDP (User Datagram Protocol).

La couche Internet
Qui est responsable de l'acheminement des paquets de données sur le réseau. Le protocole Internet (IP) est le protocole clé utilisé à cette couche pour l'adressage et le routage des paquets. Il définit des adresses IP uniques pour chaque appareil connecté au réseau, permettant ainsi leur identification et leur localisation ainsi les protocoles ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol).

La couche Accès au réseau
C’est la couche la plus basse et qui est responsable de l'accès physique au réseau. Cette couche implique les protocoles et les technologies spécifiques utilisées pour la transmission des données sur le support physique, tels que le câble Ethernet, les réseaux sans fil ou les lignes téléphoniques. L'un des avantages majeurs du modèle TCP/IP est sa flexibilité et sa compatibilité avec différents types de réseaux, qu'ils soient filaires ou sans fil. Il est également largement utilisé sur Internet pour permettre la communication entre les millions d'appareils connectés à travers le monde.

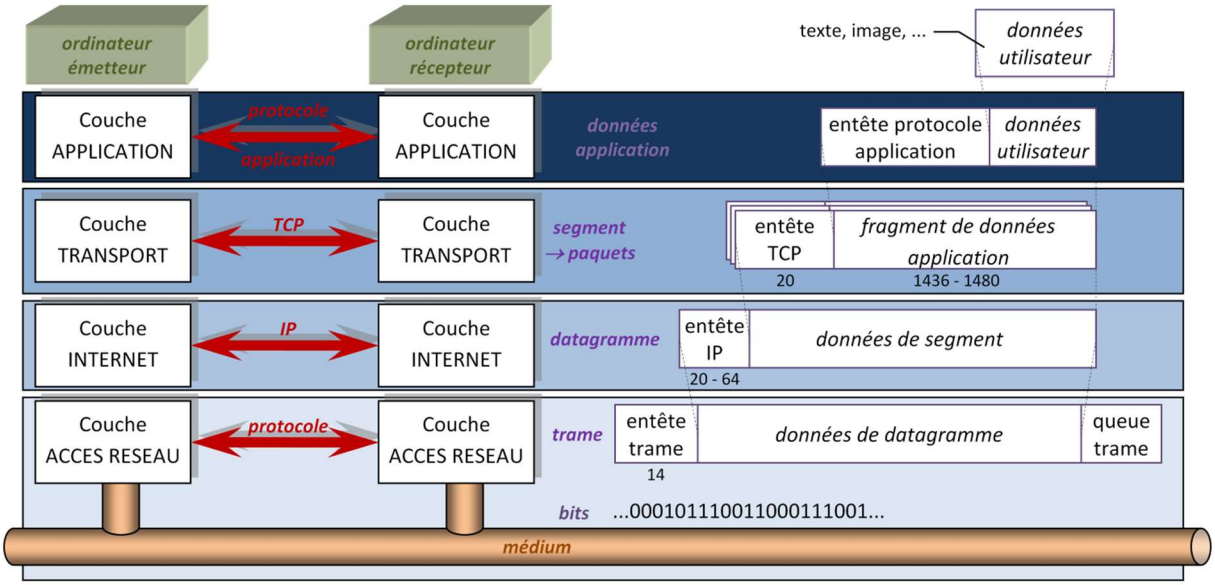


Figure II.27: le modèle TCP/IP [24]

En résumé, le modèle TCP/IP est un modèle de référence essentiel dans les réseaux informatiques. Il définit les protocoles et les normes nécessaires à la communication entre les différentes entités d'un réseau, en fournissant une structure hiérarchique et organisée. Cette organisation permet une communication fiable, sécurisée et efficace, ce qui en fait l'un des modèles les plus utilisés à travers le monde.

II.4 L'unité de donnée

Les données que vous transmettez sont tout simplement appelées unité de données (data unit en anglais). On les nomme parfois PDU (Protocol Data Unit : « unité de données de protocole ») ; dans ce cas, leur nom sera précédé de l'initiale de la couche dont ces données sont issues. Par exemple dans la couche applicative, elles prennent le nom d'APDU (Application Protocol Data Unit : « unité de données de protocole d'application »). Dans la couche de session, elles s'appelleront donc… SPDU (Session Protocol Data Unit : « unité de données de protocole de session »). Même principe pour la couche de présentation. Une fois dans la couche de transport, où elles sont segmentées, ces données deviennent logiquement des segments. (Nous les avons appelés séquences dans le chapitre précédent.)
Dans la couche réseau du modèle OSI, ces données prennent le nom de paquets ; dans les couches liaison et physique, respectivement ceux de frame (trame) et bit. [3]

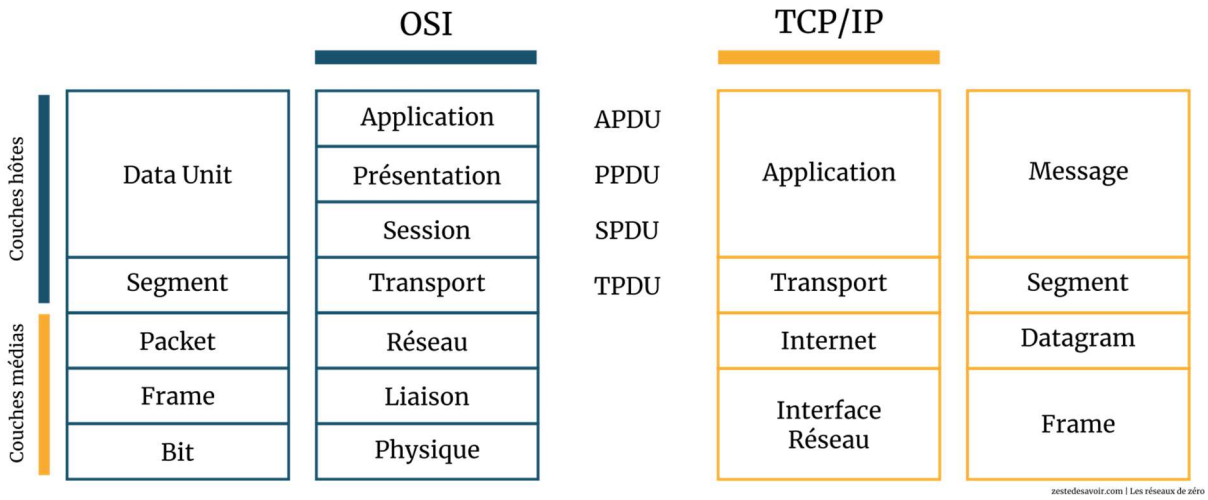


Figure II.28: Unités de données selon les modèles OSI et TCP/IP [25]

II.5 Comparaison entre les 2 modèles

Les deux modèles sont utilisés pour décrire la manière dont les données sont transmises sur les réseaux informatiques, La principale différence entre les deux modèles réside dans leur structure et leur approche de la communication en réseau.

Structure et nombre des canapés

Le modèle OSI est composé de 7 couches ce qui le rend plus détaillé et complexe : Application, Présentation, Session, Transport, Réseau, Liaison de données et Physique. Chaque couche a des fonctions spécifiques et communique avec les couches adjacentes pour transmettre les données de manière efficace.

En revanche, le modèle TCP/IP est plus simple, avec seulement 4 couches : Liaison, Internet, Transport et Application. Il regroupe certaines fonctions en une seule couche, ce qui le rend plus compact et adapté à l'environnement Internet.

Protocoles associés

Le modèle OSI est associé à des protocoles tels que HTTP, FTP, SMTP, etc., tandis que le modèle TCP/IP Réunis les 2 protocoles TCP et IP.

Origine et Utilisation

Le modèle OSI a été développé par l'ISO (International Organization for Standardization) dans le but de normaliser et comprendre les communications réseau, pour développer des protocoles et des technologies réseau, standardiser les routeurs, commutateurs, cartes mères, etc.

Le modèle TCP/IP est né de l'implémentation pratique des premiers réseaux Internet est développé par ARPANET (Advanced Research Project Agency Network), Spécialement conçu pour offrir un flux d'octets de bout en bout, Il est utilisé pour connecter des ordinateurs à Internet et à d'autres réseaux à grande échelle.

II.6 Adressage dans un réseau informatique

Pour comprendre le fonctionnement du trafic des données sur un réseau informatique, il est nécessaire de comprendre l'adressage réseau.

II.6.1 adressages MAC

Également appelée adresse de couche 2(liaison de données) ou appelée adresse physique, est une séquence composée de chiffres et de lettres codés sur 48 bits dans les 6 premiers chiffres permettent d'identifier le fabricant de l'appareil elle est couramment présentée au format hexadécimal, utilisé pour identifier d'une manière unique un périphérique réseau.

II.6.2 adressages IP

L'adressage IP dans un réseau informatique est un élément clé qui permet d'identifier de manière unique chaque équipement connecté au réseau. Les adresses IP sont utilisées pour permettre la communication entre les différents appareils sur le réseau, on distingue deux formats d'adressage, IPv4 et IPv6.

II.6.2.1 Principe et formats d'adressage IPv4

L'adressage IPv4 repose sur un système d'adresses numériques, composé de quatre octets, soit 32 bits. Chaque octet est représenté en décimal, allant de 0 à 255, et séparé par des points. Par exemple, une adresse IPv4 pourrait ressembler à ceci : 192.168.0.1. Cette adresse est utilisée pour identifier de manière unique un périphérique au sein d'un réseau.

Le premier octet d'une adresse IPv4 est réservé pour identifier la classe de réseau à laquelle l'adresse appartient.

II.6.2.1.1 les classes d'adresses

Il existe cinq classes d'adresses IPv4 :
La classe A qui commence de 0 à 12
La classes B qui commence de 128 à 191
La classes C qui commence de 192 à 223
La classe D qui commence de 224 à 239
La classe E qui commence de 240 à 255.
Les classes A, B et C sont utilisées pour les réseaux, tandis que les classes D et E sont réservées à un usage spécifique. Chaque classe d'adresse a une plage d'adresses prédéfinie, permettant ainsi de déterminer le nombre d'hôtes pouvant être connectés à un réseau donné.

Outre la classe de réseau, les octets restants de l'adresse IPv4 sont utilisés pour identifier de manière unique chaque périphérique au sein du réseau. La combinaison d'une adresse de réseau et d'une adresse d'hôte permet de déterminer l'emplacement exact d'un périphérique et de diriger correctement les paquets de données.

En plus de la représentation décimale, les adresses IPv4 peuvent également être converties en notation binaire ou hexadécimale, afin de faciliter les calculs et les opérations sur les adresses IP. La notation binaire représente chaque octet sous forme de 8 bits, tandis que la notation hexadécimale utilise les chiffres de 0 à 9 et les lettres de A à F pour représenter chaque octet.

L'adressage IPv4 est essentiel pour le routage des paquets de données sur un réseau. Chaque routeur utilise les informations d'adressage contenues dans les en-têtes des paquets pour déterminer la meilleure route à suivre afin d'acheminer les données vers leur destination.
Les adresses IP permettent également de définir des sous-réseaux, qui sont des portions d'un réseau plus grand, permettant ainsi une meilleure gestion des adresses et une optimisation du trafic des données.

II.6.2.2 Principe et formats d'adressage IPv6

Dans le contexte de la croissance constante d'Internet et de la nécessité d'avoir des adresses IP disponibles en quantité suffisante, l'IPv6, ou Internet Protocol version 6, a été créé pour succéder à l'IPv4. L'adressage IPv6 offre un espace d'adressage beaucoup plus vaste et des fonctionnalités améliorées par rapport à son prédécesseur. Dans cette partie, nous allons explorer les principes fondamentaux et les formats utilisés dans l'adressage IPv6.

Le principal avantage de l'IPv6 réside dans la taille de l'espace d'adressage disponible. Alors que l'IPv4 offre environ 4,3 milliards d'adresses uniques, l'IPv6 offre un nombre astronomique de 340 un décillions d'adresses (3,4 x 10^38). Cela permet d'alimenter la croissance exponentielle des appareils connectés à Internet, tels que les smartphones, les objets connectés et les véhicules autonomes.

Dans l'IPv6, une adresse est composée de huit groupes de quatre chiffres hexadécimaux séparés par des deux-points (:). Chaque groupe représente 16 bits, totalisant ainsi 128 bits pour une adresse IPv6 complète. Par exemple, une adresse IPv6 peut ressembler à ceci :
2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Les groupes de l'adresse IPv6 peuvent être simplifiés pour éviter les répétitions inutiles de zéros. Ainsi, l'adresse ci-dessus pourrait être simplifiée en utilisant l'écriture compacte :
2001:db8:85a3::8a2e:370:7334. Les groupes vides, représentés par deux points consécutifs, indiquent qu'ils sont remplacés par des zéros.

L'IPv6 propose également des formats spéciaux pour l'adresse de boucle locale, l'adresse unicast globale, l'adresse unicast lien-local, l'adresse unicast site-local et l'adresse multicast. L'adresse de boucle locale (::1) est utilisée pour communiquer avec le propre hôte
L’adresse unicast globale est destinée à être routée sur Internet.
Les adresses unicast lien-local sont utilisées pour les communications au sein d'un seul domaine de liaison.
Les adresses unicast site-local sont limitées à un seul site ou une organisation spécifique.
Les adresses multicast sont utilisées pour envoyer des paquets à plusieurs destinataires simultanément.

En conclusion, l'IPv6 offre des fonctionnalités avancées et un espace d'adressage considérablement étendu par rapport à l'IPv4. Son format d'adressage spécifique permet une identification unique et précise des appareils connectés à Internet. L'adoption de l'IPv6 est essentielle pour soutenir la croissance future d'Internet et garantir une connectivité continue pour les utilisateurs du monde entier.

II.6.3 Passage à IPv6 et enjeux associés

Avec l'épuisement des adresses IPv4, il est devenu impératif de migrer vers IPv6, qui offre un espace d'adressage considérablement plus vaste.

IPv6, également connu sous le nom d'Internet Protocol version 6, est le successeur d'IPv4 et présente de nombreuses améliorations par rapport à son prédécesseur. L'un des principaux avantages d'IPv6 est son espace d'adressage beaucoup plus large, permettant un nombre quasiment illimité d'adresses IP. Alors que IPv4 utilise des adresses composées de 32 bits, IPv6 utilise des adresses de 128 bits, offrant ainsi plus de 340 milliards de milliards de milliards de milliards d'adresses potentielles.

La transition vers IPv6 soulève toutefois de nombreux défis et enjeux auxquels il faut faire face. L'un des principaux défis est la compatibilité. Les infrastructures réseau existantes, notamment les routeurs, les pares-feux et les systèmes de gestion, doivent être mis à jour pour prendre en charge IPv6. Il est également nécessaire de former les professionnels de l'informatique à la nouvelle technologie pour assurer une transition fluide.

Un autre enjeu important de la migration vers IPv6 concerne la sécurité. Avec l'augmentation du nombre d'appareils connectés à Internet, il devient essentiel de mettre en place des mesures de sécurité robustes pour protéger les réseaux et les données. IPv6 offre de nouvelles fonctionnalités de sécurité, telles que l'authentification et le chiffrement intégrés, mais leur intégration correcte dans les infrastructures existantes nécessite une expertise approfondie.

De plus, la migration vers IPv6 nécessite une coordination et une collaboration étroites entre différents acteurs de l'industrie. Les fournisseurs d'accès à Internet, les fabricants d'équipements réseau, les entreprises et les institutions doivent travailler ensemble pour s'assurer que la transition se déroule de manière harmonieuse et sans perturbations majeures.

En conclusion, le passage à IPv6 présente de nombreux avantages, notamment un espace d'adressage beaucoup plus vaste et des fonctionnalités de sécurité améliorées. Cependant, cela soulève également des défis et des enjeux importants, tels que la compatibilité, la sécurité et la coordination. Les administrateurs et les utilisateurs des réseaux informatiques doivent donc être conscients de ces aspects et se préparer à faire face aux défis que le passage à IPv6 peut poser.
La transition vers IPv6 est inévitable et il est essentiel de saisir les opportunités qu'elle offre tout en minimisant les risques possibles.

II.6.4 types d'adresses IP

Les adresses IP peuvent être classées en deux catégories principales : les adresses IP publiques et les adresses IP privées. Chacune de ces catégories à un rôle spécifique dans le fonctionnement des réseaux informatiques.

II.6.4.1 Les adresses IP publiques

Les adresses IP publiques sont attribuées par les fournisseurs d'accès à Internet (FAI) aux appareils connectés à Internet et qui suivent des plages spécifiques définies par l'IANA (Internet Assigned Numbers Authority).
Elles sont visibles et accessibles depuis l'extérieur du réseau local et sont routables sur Internet, ce qui signifie qu'elles peuvent être utilisées pour communiquer avec des appareils situés n'importe où sur Internet.

II.6.4.2 Les adresses IP privé

Les adresses IP privées sont utilisées au sein de réseaux privés, c'est à dire permettent la communication entre les appareils à l'intérieur du réseau local comme les réseaux domestiques ou d'entreprise, utilisées pour les ordinateurs personnels, les imprimantes réseau, les téléphones IP, les caméras de sécurité, etc.
Elles ne sont pas accessibles depuis l'extérieur du réseau et ne sont pas routables sur Internet.

II.6.5 Le protocoles NAT (Network Address Translation)

Le NAT est utilisé pour permettre aux appareils avec des adresses IP privées d'accéder à Internet en traduisant leurs adresses en une adresse IP publique partagée, offrant ainsi une couche de sécurité supplémentaire et notamment le besoin en adresses IP publiques.
Le NAT est généralement implémenté sur des routeurs ou des pares-feux, qui font office de passerelle entre le réseau local et Internet. Lorsqu'un appareil du réseau local envoie une requête vers Internet, le routeur traduit l'adresse IP source privée en une adresse IP publique, et inversement pour les réponses.
Bien que le NAT offre de nombreux avantages, il peut également poser certains problèmes, comme la complexité de la configuration, la difficulté de mettre en place certains services (comme le VoIP) et la perte d'informations sur l'adresse IP d'origine lors de la traduction.

II.7 Mécanismes de routage et de commutation

Les mécanismes de routage et de commutation dans les réseaux informatiques font référence aux différentes façons dont les paquets de données sont acheminés et transférés entre les équipements réseau.

II.7.1 le routage

Le routage est le processus par lequel les paquets de données sont acheminés d'un réseau à un autre, en utilisant des équipements appelés routeurs. Les routeurs utilisent des tables de routage pour déterminer le meilleur chemin pour acheminer les paquets vers leur destination finale

II.7.1.1 Gestion de la table de routage

La gestion de la table de routage est un élément essentiel dans le domaine des réseaux informatiques, en particulier dans le contexte de l'adressage IP. En effet, l'adressage IP permet d'attribuer une adresse unique à chaque périphérique connecté à un réseau, ce qui permet d'acheminer les données de manière efficace.

La table de routage, quant à elle, constitue une base de données utilisée par les routeurs pour déterminer le chemin optimal à emprunter afin de transmettre les paquets de données vers leur destination. Elle contient des informations sur les réseaux voisins et les routes disponibles, ainsi que des métriques permettant d'évaluer la qualité des chemins possibles et les ports associés, ainsi les protocoles utilisés.

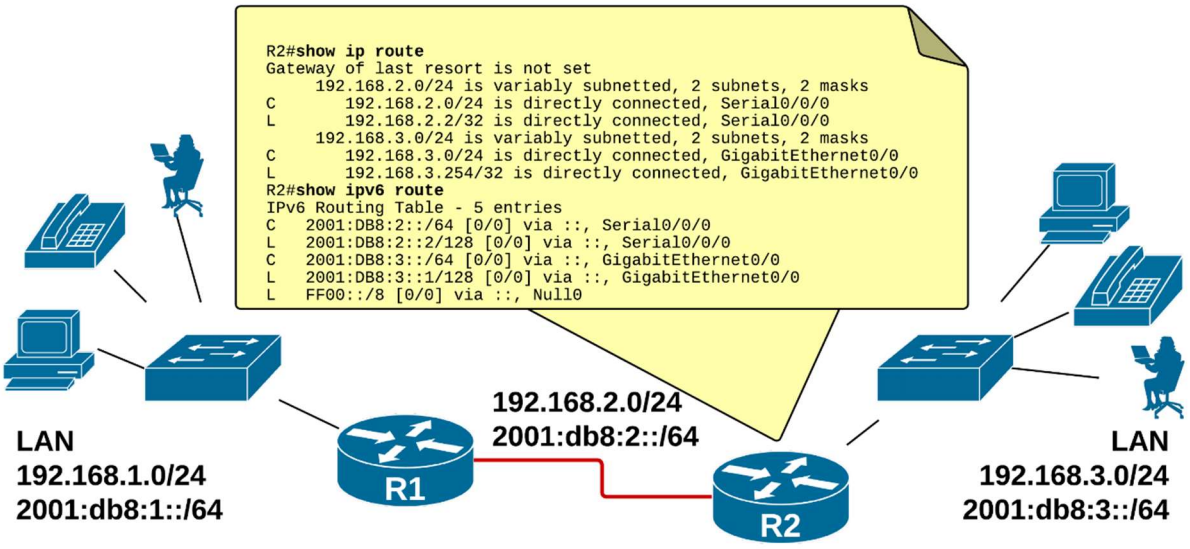


Figure II.29: exemple de table de routage [26]

L'une des fonctions principales de la gestion de la table de routage est de mettre à jour et maintenir les entrées de cette table de manière dynamique. En effet, les réseaux évoluent en permanence, de nouveaux périphériques peuvent être ajoutés, des pannes peuvent se produire ou des chemins plus efficaces peuvent apparaître. Ainsi, il est important de prendre en compte ces changements et de les refléter dans la table de routage.

La gestion de la table de routage implique également la résolution des conflits potentiels entre les routes disponibles. Par exemple, si deux routes mènent à la même destination, le routeur doit sélectionner celle qui présente la métrique la plus faible, c'est-à-dire le chemin le plus court ou le plus rapide. Dans certains cas, des techniques avancées telles que le routage dynamique peut être utilisées pour prendre des décisions de routage automatisées et optimisées.

Une autre facette importante de la gestion de la table de routage est la sécurité. Les routeurs doivent être capables de filtrer et d'évaluer les paquets de données entrants afin de détecter d'éventuelles menaces ou attaques. Ils peuvent ainsi appliquer des filtres pour bloquer certains types de trafic indésirable ou mettre en place des listes de contrôle d'accès pour restreindre l'accès à certaines ressources sensibles.

En conclusion, la gestion de la table de routage joue un rôle central dans l'acheminement des données sur un réseau informatique. Elle permet d'optimiser la transmission des paquets, de prendre en compte les changements dans le réseau et de garantir la sécurité des communications.
Une bonne maîtrise de ces aspects est essentielle pour assurer le bon fonctionnement et la performance des réseaux modernes.

II.7.1.2 Les types de routage

Il existe deux principaux types de routage dans les réseaux informatiques :

II.7.1.2.1 Routage statique

Consiste à définir manuellement les routes dans les tables de routage des routeurs. Les routes sont configurées par l'administrateur réseau et ne changent pas automatiquement, c'est-à-dire des routes fixes.
Le routage statique convient pour les petits réseaux avec un seul chemin vers l'extérieur. Il est simple à mettre en place mais nécessite une intervention manuelle en cas de changement de topologie.

II.7.1.2.2 Routage dynamique

Permet aux routeurs de mettre à jour automatiquement leurs tables de routage en utilisant des protocoles de routage. Les routeurs échangent des informations sur la topologie du réseau et calculent les meilleures routes.
Le routage dynamique s'adapte automatiquement aux changements de topologie et convient aux réseaux de taille moyenne à grande.

Les protocoles de routage dynamique peuvent être classés en deux catégories :

- **Protocoles à vecteur de distance**

Chaque routeur diffuse périodiquement sa table de routage aux routeurs voisins, c'est-à-dire dans ce type de protocole, chaque routeur transmet ses informations de routage à ses voisins en spécifiant la distance jusqu'à la destination. Les voisins mettent ensuite à jour leurs tables de routage en fonction des informations reçues, et transmettent ces informations à leurs propres voisins. Ce processus se répète jusqu'à ce que tous les routeurs du réseau aient connaissance des différentes routes disponibles, ce qu'on appelle la convergence.

- **Protocoles à état de liens**

Chaque routeur envoie des messages courts indiquant l'état de ses liens avec les autres routeurs. Dans ce type de protocole, chaque routeur échange des informations sur l'état de ses liens avec les autres routeurs du réseau. Ces informations incluent la bande passante, la latence et la fiabilité de chaque lien. Les routeurs utilisent ensuite ces informations pour construire une carte topologique du réseau, qui leur permet de calculer les chemins les plus courts vers chaque destination.

En résumé, le routage statique est manuel et convient aux petits réseaux, tandis que le routage dynamique est automatique et s'adapte mieux aux grands réseaux. Le choix entre les deux dépend de la taille et de la complexité du réseau.

II.7.1.3 Les différents protocoles de routage

Les protocoles de routage sont essentiels pour le fonctionnement des réseaux, en particulier pour déterminer comment les données sont acheminées d'un point à un autre.
Les protocoles de routage peuvent être classés en deux catégories principales : les protocoles de routage intra-domaine (interne) et les protocoles de routage inter-domaine. Les protocoles de routage intra-domaine sont utilisés à l'intérieur d'un réseau localisé, comme une entreprise ou une université, pour acheminer le trafic entre différents sous-réseaux. Ils se concentrent sur l'efficacité et la rapidité de l'acheminement des données à l'intérieur du réseau.

Les protocoles de routage inter-domaine (externe) sont utilisés pour acheminer le trafic entre différents réseaux, tels que des réseaux d'opérateurs Internet ou des réseaux de fournisseurs de services. Ces protocoles doivent prendre en compte des aspects tels que les politiques de routage, la qualité de service et la garantie de la confidentialité et de la sécurité des données transitant entre les différents domaines.

- **Un système autonome (AS)**

Est un ensemble de réseaux sous la même autorité administrative (autorité de gestion). Au sein d'un système autonome, les routes sont générées par des protocoles de routage intérieurs comme RIP, EIGRP, OSPF ou ISIS, cependant les protocoles de routage qui permettent de connecter les systèmes autonomes entre eux sont des protocoles de routage extérieurs comme BGP. [4]

II.7.1.3.1 les protocoles de routage interne (IGP)

IGP (interior gateway protocol) : Est un protocole de routage dynamique au sein d'un système autonome (SA).

Il permet aux routeurs d'échanger des informations de routage à l'intérieur du même système autonome. Et donc acheminer le trafic à l'intérieur d'un réseau local. Parmi les protocoles de routage interne les plus couramment utilisés, on retrouve :
Le protocole RIP (Routing Information Protocol), l'OSPF (Open Shortest Path First), le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) et le protocole IS-IS (Intermediate System to Intermediate System). Chacun de ces protocoles présente ses propres particularités et fonctionnalités, adaptées à des besoins spécifiques.

Le protocole RIP est un protocole de routage à vecteur de distance qui utilise l'algorithme de Bellman-Ford pour déterminer les routes optimales. Il est principalement utilisé dans les petits réseaux où la topologie est relativement simple.
Le protocole RIP Utilise le nombre de sauts (hops) comme métrique de routage. La limite maximale de sauts est de 15, ce qui limite sa portée aux petits réseaux.

Les mises à jour de routage sont envoyées toutes les 30 secondes, ce qui peut entraîner une convergence lente.
Ce protocole Utilise des messages de diffusion (broadcast) pour envoyer des mises à jour de routage. En revanche, sa convergence lente et ses limitations en termes de scalabilité en font un choix moins adapté pour les réseaux de grande envergure malgré ça Simplicité de configuration et de mise en œuvre.

L'OSPF, quant à lui, est un protocole de routage à état de lien qui utilise l'algorithme de Dijkstra pour calculer les chemins les plus courts entre les différents nœuds du réseau. Il est largement utilisé dans les réseaux d'entreprise en raison de sa capacité à prendre en charge des topologies complexes et à fournir une redondance de liens. Ce protocole Divise le réseau en zones hiérarchiques, avec une zone principale (backbone) et des zones de transit.
Les mises à jour de routage sont envoyées uniquement lorsqu'il y a des changements dans la topologie, ce qui améliore l'efficacité.
De plus, l'OSPF offre une convergence rapide et une grande scalabilité malgré qu'il soit compliquer à configurer et à gérer en comparent avec le RIP.

Le protocole EIGRP est un protocole de routage avancé développé par Cisco. Il combine les avantages des protocoles à vecteur de distance et des protocoles à état de lien, en utilisant la diffusion périodique des mises à jour de routage ainsi que des mises à jour partielles lorsqu'un changement de topologie se produit ce qui améliore la convergence
Ce protocole utilise une métrique composite basée sur la bande passante, la latence, la charge, la fiabilité et la taille des paquets, particulièrement adapté aux réseaux de taille moyenne et offre des fonctionnalités de redondance de liens et de tolérance aux pannes.

Le protocole IS-IS est un protocole de routage de type état de lien, utilisé principalement dans les réseaux de fournisseurs de services et les grandes entreprises. Divise le réseau en domaines hiérarchiques avec des niveaux ; Les routeurs de niveau 1 connaissent les routes à l'intérieur de leur propre domaine (ou aire) mais ne savent pas comment atteindre d'autres domaines, ils utilisent d'autres routeurs appelés routeurs de niveau 2 pour communiquer avec des routeurs dans d'autres domaines et ils sont responsables que de la communication inter-domaines.

II.7.1.3.2 les protocoles de routage externe (EGP)

Les protocoles de routage externe sont utilisés pour échanger des informations de routage entre différents systèmes autonomes (AS - Autonomous Systems). Le protocole de routage externe le plus important et le plus largement utilisé est :

Le protocole BGP (Border Gateway Protocol) qui est utilisé pour interconnecter différents systèmes autonomes sur Internet. Il est responsable de l'acheminement des paquets de données à travers les réseaux Internet et utilise des critères tels que la politique de routage et la qualité du lien pour prendre des décisions d'acheminement. BGP est un protocole complexe et exigeant, utilisé principalement par les fournisseurs de services Internet et les grands opérateurs de réseau.

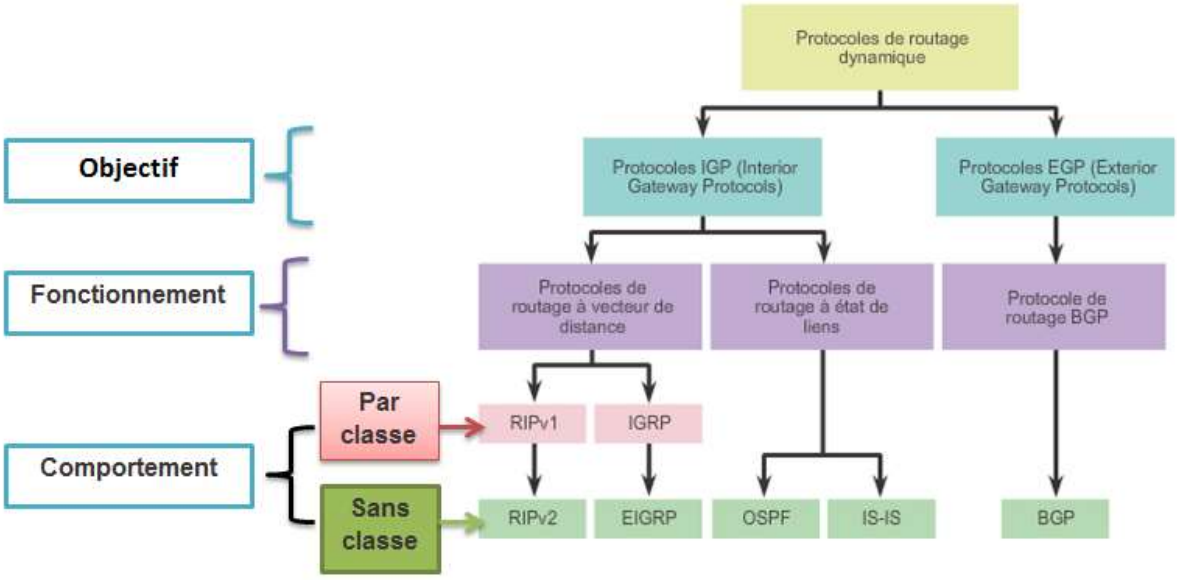


Figure II.30:classification des protocoles de routage [27]

En conclusion, Chacun de ces protocoles présente des fonctionnalités et des avantages spécifiques, adaptés aux besoins et à la taille du réseau. Il est donc essentiel de choisir le protocole de routage approprié en fonction des exigences du réseau afin de garantir un acheminement efficace des paquets de données.

II.7.2 la commutation

La commutation est le processus par lequel les paquets de données sont transférés entre les ports d'un commutateur (switch) au sein d'un même réseau local (LAN). Les commutateurs utilisent des tables d'adresses MAC pour déterminer vers quel port transmettre les paquets.
Il existe deux principaux mécanismes de commutation :
Commutation par processus : Le commutateur transfère les paquets en mode logiciel, ce qui est plus lent mais permet plus de fonctionnalités.
Commutation rapide : Le commutateur transfère les paquets en mode matériel, ce qui est plus rapide mais offre moins de fonctionnalités.

En résumé, le routage permet d'acheminer les paquets entre différents réseaux en utilisant des routeurs, tandis que la commutation permet de transférer les paquets entre les ports d'un même réseau local en utilisant des commutateurs. Le choix entre routage et commutation dépend de la topologie du réseau et des besoins en termes de performances et de fonctionnalités.

II.8 Communication entre les dispositifs réseau

La communication entre les dispositifs réseau repose sur des principes et des protocoles standardisés qui permettent l'échange de données de manière fiable et efficace.

II.8.1 Le protocole ARP et la résolution d'adresses MAC

Le protocole ARP (Address Protocol) est un protocole essentiel dans les réseaux informatiques pour permettre la résolution d'adresses MAC. Il joue un rôle très important dans la communication entre les dispositifs réseau en établissant la correspondance entre les adresses IP et les adresses MAC.

Lorsqu'un dispositif souhaite envoyer des données vers une autre machine sur le réseau local, il a besoin de connaître l'adresse MAC de cette dernière afin de pouvoir acheminer le paquet de données de manière efficace. C'est ici que le protocole ARP intervient en résolvant la question de la correspondance entre l'adresse IP et l'adresse MAC.

Dans un réseau, chaque dispositif possède une adresse IP qui lui est attribuée, mais également une adresse MAC qui est associée à sa carte réseau. L'adresse IP est utilisée pour acheminer les paquets de données au bon destinataire, tandis que l'adresse MAC est utilisée pour la transmission des données au niveau local, c'est-à-dire au sein du réseau local.

Lorsqu'un dispositif souhaite envoyer des données à une autre machine dont il connaît l'adresse IP, il utilise une requête ARP pour trouver l'adresse MAC correspondante. Le dispositif émet alors une requête ARP de type "Who has" en broadcast sur le réseau local, demandant qui possède l'adresse IP recherchée. Tous les dispositifs du réseau reçoivent cette requête et la machine concernée répond avec son adresse MAC. Ainsi, le dispositif émetteur peut mettre à jour sa table ARP en associant l'adresse IP à l'adresse MAC.

La résolution d'adresses MAC effectuée par le protocole ARP permet donc d'établir une correspondance entre les adresses IP et les adresses MAC, facilitant ainsi la communication entre les dispositifs sur un réseau local. Cette résolution d'adresses est dynamique, c'est-à-dire qu'elle est mise à jour lorsque les adresses IP ou les adresses MAC changent.

Il est à noter que le protocole ARP fonctionne au niveau de la couche réseau du modèle OSI, ce qui signifie qu'il est indépendant du type de réseau sous-jacent, qu'il s'agisse d'un réseau local Ethernet, d'un réseau sans fil ou d'un réseau étendu. Il permet ainsi aux dispositifs de communiquer efficacement, peu importe le type de réseau utilisé.

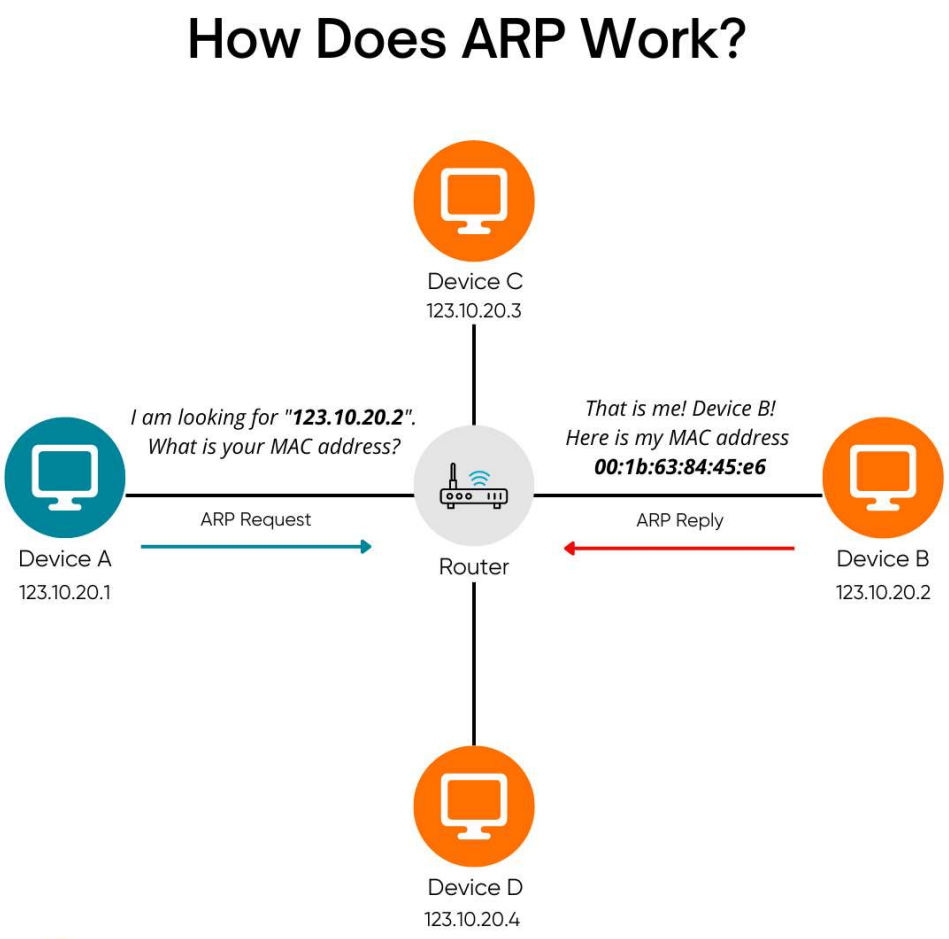


Figure II.31: principe de fonctionnement de l'ARP [28]

En conclusion, le protocole ARP et la résolution d'adresses MAC sont essentiels dans un réseau informatique pour permettre la communication entre les dispositifs. Grâce à ce protocole, les adresses IP peuvent être associées aux adresses MAC, ce qui facilite l'acheminement des données au sein du réseau local. La mise à jour dynamique de la table ARP permet une adaptation aux changements d'adresses IP et MAC, assurant ainsi une communication fluide et efficace entre les dispositifs.

II.9 Le trafic des donnés filaire et sans fils sur un réseau informatique

Le trafic des données dans un réseau informatique peut se faire de manière filaire qui utilise des câbles physiques pour transmettre les données entre les dispositifs réseau, ou sans fil qui utilise des ondes radio pour transmettre les données entre les dispositifs réseau.
Pour encapsuler les données transmises via le trafic filaire on utilise ce qu'on appelle les trames Ethernet, en revanche Des trames spécifiques au Wi-Fi sont utilisées pour encapsuler les données transmises via le trafic sans fil.

II.9.1 Le rôle des trames dans la communication des données

Dans le domaine des réseaux informatiques, la communication entre les dispositifs est essentielle pour assurer la transmission efficace et fiable des données. Parmi les technologies utilisées pour faciliter cette communication, les trames Ethernet qui jouent un rôle fondamental.
Les paquets IP ne peuvent pas transiter sur un réseau tel quel, ils vont eux aussi être encapsulé avant de pouvoir « voyager » sur le réseau. L'encapsulation des paquets IP produit ce que l'on appelle une trame.

II.9.1.1 Les trames Ethernet

Sont des unités de données qui encapsulent les informations à transmettre sur un réseau Ethernet. Elles sont constituées d'un en-tête, d'un corps et d'une séquence de contrôle. L'en-tête de la trame contient des informations telles que l'adresse MAC de l'émetteur et du destinataire, le type de protocole utilisé, ainsi que des informations de contrôle pour permettre la détection des erreurs.
Les trames ont une taille spécifique qui peut varier en fonction du type de réseau et des protocoles utilisés. Par exemple, sur un réseau Ethernet, la taille d'une trame est généralement comprise entre 64 et 1518 octets.

Lorsqu'un dispositif émet des données (par exemple un paquet du protocole IP) sur le réseau, il les encapsule dans une trame Ethernet avant de les envoyer. Cette trame est ensuite transmise à travers le réseau, en passant par les commutateurs et les routeurs, jusqu'à ce qu'elle atteigne le dispositif destinataire. À chaque saut, les commutateurs analysent l'adresse MAC de la trame pour déterminer le chemin optimal vers le dispositif destinataire.

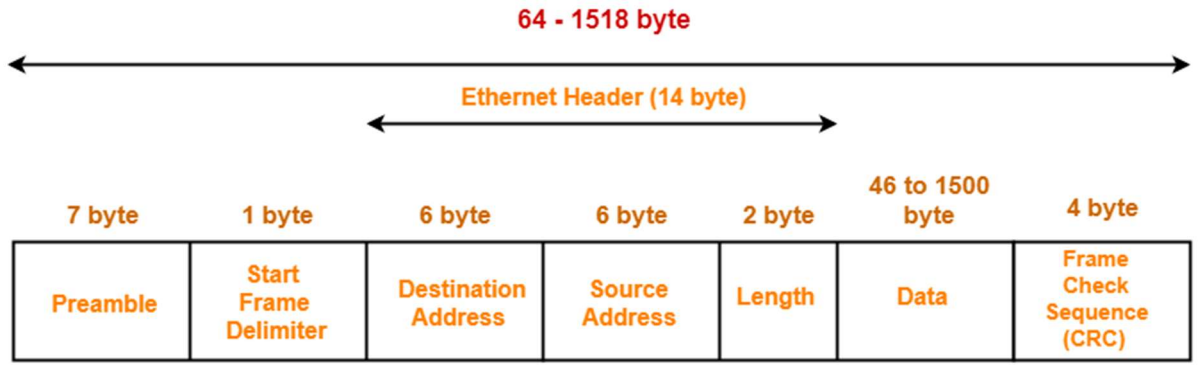


Figure II.32: Structure d'une trame Ethernet [29]

Les trames Ethernet, grâce à leur structure bien définie, permettent une communication efficace et fiable des données. Elles garantissent également la sécurité des informations en fournissant des mécanismes de détection et de correction d'erreurs, ainsi que des fonctionnalités de contrôle d'accès.

II.9.2 Le trafic dans point d'accès wifi

Le trafic dans un point d'accès Wi-Fi (Wireless Access Point, ou AP) implique la transmission et la gestion des données entre les dispositifs sans fil (comme les smartphones, les ordinateurs portables, et les tablettes) et le réseau local filaire (LAN).
Un point d'accès Wi-Fi sert de pont entre les dispositifs sans fil et le réseau filaire. Il reçoit les signaux sans fil des dispositifs, les convertit en signaux filaires, et vice-versa. Les AP modernes utilisent plusieurs technologies et protocoles pour gérer efficacement le trafic réseau tel que la technologie WDS, qui connecte au routeur de point d'accès sans utiliser de câbles.

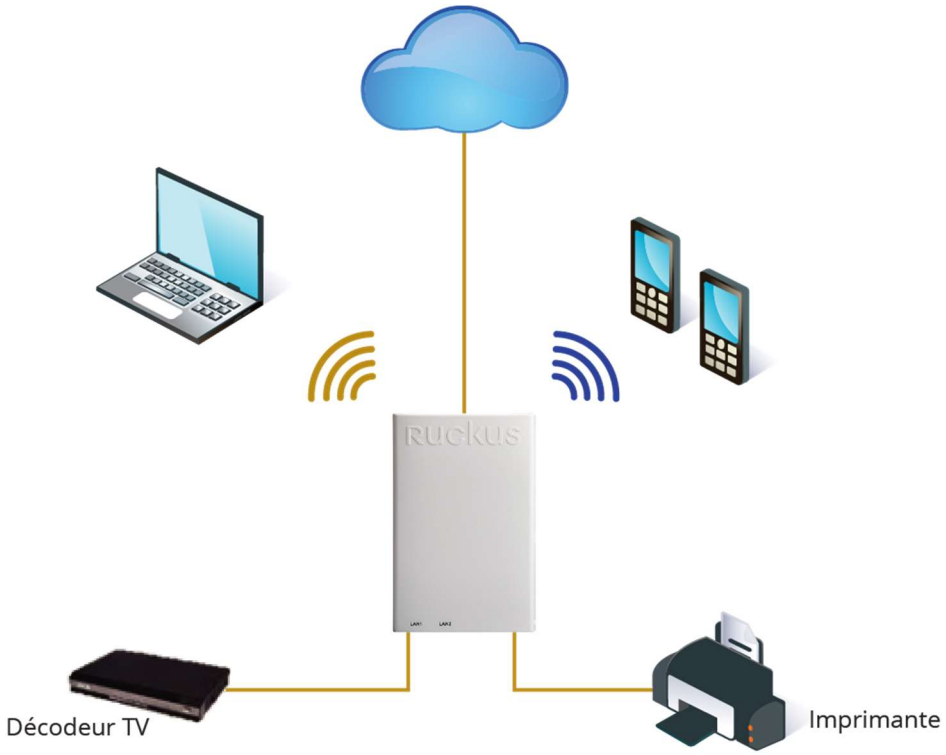


Figure II.33: Point d'accès WIFI [30]

II.9.2.1 Processus de Communication

- **Association** :

Un dispositif sans fil envoie une demande d'association au point d'accès.
Le point d'accès vérifie les informations d'identification (SSID, mot de passe) et accepte ou rejette la demande.
Une fois accepté, le dispositif est associé et peut commencer à échanger des données.

- **Transmission de Données**

Les données sont envoyées en paquets entre le dispositif et l'AP.
Les paquets peuvent contenir des données utilisateur, des requêtes de contrôle, ou des messages de gestion.

- **Accès au Média**

Utilise des mécanismes comme CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) pour gérer l'accès au canal sans fil et éviter les collisions.

- **Encapsulation et Décapsulation**

Les données sont encapsulées en trames Wi-Fi pour la transmission sans fil.
Le point d'accès décapsule les trames Wi-Fi et les encapsule en trames Ethernet pour les transmettre sur le réseau filaire.

II.10 Optimisation du trafic sur un réseau informatique

II.10.1 La gestion du trafic (bande passante, QoS, VLAN)

L'optimisation du trafic sur un réseau informatique est un enjeu majeur pour assurer des performances optimales et une qualité de service (QoS) satisfaisante pour les utilisateurs.

La QoS est un ensemble de techniques et de protocoles qui permettent de hiérarchiser le trafic, en attribuant des priorités aux différents types de données selon leurs besoins en termes de délai, de bande passante et de fiabilité. En utilisant des mécanismes de contrôle de congestion, tels que les files d'attente pondérées, la QoS permet de prévenir les problèmes de latence et de perte de paquets, assurant ainsi une transmission de données plus efficiente. Par exemple, les données en temps réel, comme la voix sur IP ou la vidéoconférence, peuvent être priorisées par rapport aux téléchargements de fichiers moins sensibles à la latence.

Au cœur de cette optimisation se trouve la gestion de la bande passante, qui vise à répartir efficacement les ressources afin de garantir une utilisation fluide du réseau.

La bande passante désigne la capacité d'un réseau à transmettre des données sur une période donnée. Elle représente la quantité d'informations pouvant être transmise en un laps de temps déterminé. Une gestion efficace de la bande passante permet d'éviter des congestions, des retards et des ralentissements sur le réseau.

Pour optimiser le trafic, il est essentiel de définir des mécanismes de QoS appropriés. La QoS consiste à hiérarchiser les flux de données en fonction de leur importance ou de leur sensibilité aux retards ou aux pertes. Cela permet de garantir des niveaux de service différenciés en fonction des besoins des utilisateurs et des applications.

Dans ce contexte, différentes techniques peuvent être mises en place pour gérer la bande passante et assurer une QoS optimale. Parmi ces techniques, on retrouve le traffic shaping, qui consiste à contrôler le débit des flux de données en les façonnant de manière à éviter les pics de trafic et à maintenir une utilisation équilibrée des ressources.

Le traffic shaping s'appuie sur des règles de priorité et de gestion du trafic, permettant ainsi de traiter les flux les plus critiques en priorité, tout en limitant le débit des flux moins prioritaires. Cela permet de prévenir les problèmes de latence et d'engorgements du réseau.

Par ailleurs, la mise en place de file d'attente (ou queues) peut également contribuer à une gestion efficace de la bande passante. Les paquets de données sont placés en file d'attente et sont traités selon des règles de priorité, permettant d'optimiser leur flux et de garantir une expérience utilisateur fluide.

Enfin, l'utilisation de protocoles de routage adaptatifs, tels que le routage basé sur l'état des liens (link-state routing) ou le routage à états de lien avec QoS (link-state routing with QoS), peut également contribuer à l'optimisation du trafic sur un réseau informatique. Ces protocoles permettent de prendre en compte les contraintes de bande passante et de QoS lors du calcul des meilleures routes pour la transmission des données.

D'un autre côté, parmi les mécanismes qui permettent d'optimiser la performance et de garantir une expérience fluide pour les utilisateurs, on trouve les VLANs.
Les VLANs est un moyen de segmenter un réseau physique en plusieurs réseaux virtuels indépendants. Cette segmentation permet d'isoler le trafic et d'améliorer la sécurité, notamment en évitant les collisions de paquets entre différents groupes d'utilisateurs sur un même réseau.
Les VLANs peuvent être mis en place en configurant des commutateurs réseau pour attribuer différents ports à différents groupes de machines. Ainsi, par exemple, les étudiants peuvent être regroupés dans un VLAN distinct de celui du personnel administratif, assurant ainsi une meilleure gestion du trafic et une sécurité renforcée.

En combinant la QoS et les VLAN, il est possible de créer un réseau informatique performant et adapté aux besoins spécifiques d'une organisation ou d'une institution académique.
La QoS permet de garantir la qualité de service pour les différents types de données, tandis que les VLAN assurent une segmentation et une isolation efficaces du trafic. Ensemble, ces mécanismes permettent d'optimiser les performances du réseau et d'offrir une expérience utilisateur de haute qualité.

Cependant, il convient de souligner que la mise en place de ces mécanismes de contrôle de trafic nécessite une planification minutieuse, une configuration appropriée et une surveillance constante. Des connaissances approfondies en matière de réseaux informatiques et de protocoles sont nécessaires pour mettre en œuvre ces mécanismes de manière efficace.
En outre, l'évolution constante des technologies de réseau rend important la mise à jour régulière des dispositifs et des politiques de contrôle de trafic pour suivre les nouvelles tendances et garantir des performances optimales.

En conclusion, la gestion du trafic, en particulier de la bande passante et de la QoS, les VLANs, ou bien en combinant ces deux derniers, est un aspect crucial pour garantir des performances optimales et une expérience utilisateur satisfaisante sur un réseau informatique. Différentes techniques peuvent être mises en œuvre pour optimiser le trafic, telles que le traffic shaping, la gestion des files d'attente et l'utilisation de protocoles de routage adaptatifs. Une gestion efficace du trafic permet d'éviter les congestions, de maintenir des débits stables et d'assurer une QoS adaptée aux besoins des utilisateurs et des applications.

II.10.2 L'utilisation de la technologie VLSM pour optimiser l'adressage IP

L'utilisation de la technologie VLSM (Variable Length Subnet Masking) constitue une méthode efficace pour optimiser l'adressage IP sur un réseau informatique. L'adressage IP est essentiel dans un réseau, car il permet l'identification des différents appareils connectés ainsi que leur communication. Cependant, une mauvaise gestion de l'adressage IP peut entraîner des problèmes tels que la surutilisation des adresses IP, des problèmes de routage et une perte de performances.

VLSM offre une solution en divisant un réseau en sous-réseaux de différentes tailles, ce qui permet une utilisation plus efficace des adresses IP disponibles. Au lieu d'attribuer un masque de sous-réseau fixe pour tous les sous-réseaux d'un réseau, VLSM permet d'utiliser des masques de sous-réseau variables en fonction des besoins spécifiques de chaque sous-réseau. Par conséquent, des réseaux de différentes tailles peuvent coexister, ce qui réduit le gaspillage des adresses IP.

L'optimisation de l'adressage IP grâce à VLSM offre plusieurs avantages. Tout d'abord, cela permet une utilisation plus efficace des adresses IP, ce qui est particulièrement bénéfique dans les situations où les adresses IP sont limitées, par exemple dans les réseaux d'entreprises ou les réseaux publics. En utilisant des masques de sous-réseau variables, on peut allouer les adresses IP de manière plus précise, en attribuant un nombre d'adresses adapté à la taille de chaque sous-réseau. Cela permet de réduire le gaspillage des adresses IP et de maximiser leur utilisation.

De plus, l'utilisation de VLSM permet de faciliter la gestion du réseau. En divisant le réseau en sous-réseaux de différentes tailles, il est possible de mieux organiser les adresses IP et d'améliorer la granularité du routage. Les routes peuvent être plus spécifiques pour atteindre les sous-réseaux, ce qui rend le routage plus efficace et évite les congestions inutiles.

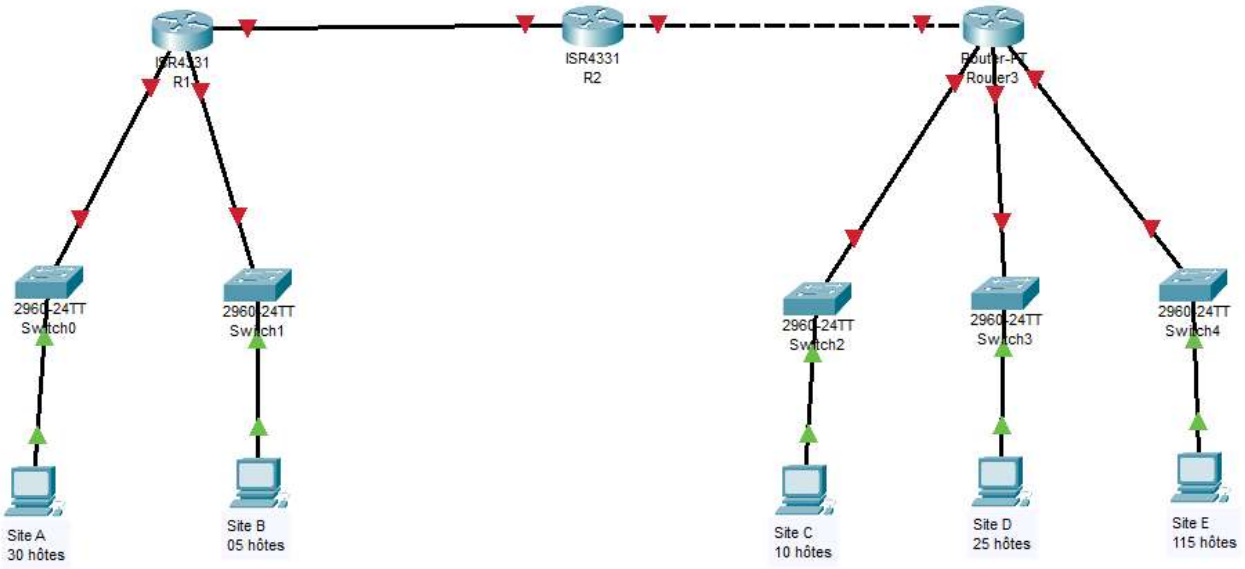
En outre, l'utilisation de VLSM offre une plus grande flexibilité dans la conception du réseau. Elle permet de mieux adapter l'adressage IP aux besoins spécifiques de chaque sous-réseau, en attribuant un nombre d'adresses suffisant pour accueillir le nombre d'appareils connectés. Cela facilite l'expansion du réseau et permet d'ajouter de nouveaux sous-réseaux sans perturber le fonctionnement global.

Cependant, il est important de souligner que la mise en place de VLSM nécessite une planification préalable minutieuse et une bonne compréhension des principes de base de l'adressage IP. Une mauvaise configuration peut entraîner des problèmes de routage, de la confusion dans la gestion des adresses IP et des erreurs de configuration. Il est donc essentiel de prendre en compte tous les aspects lors de la mise en œuvre de VLSM afin d'optimiser réellement l'adressage IP sur un réseau.

En conclusion, l'utilisation de la technologie VLSM constitue une méthode efficace pour optimiser l'adressage IP sur un réseau informatique. Elle permet une utilisation plus efficace des adresses IP, facilite la gestion du réseau et offre une plus grande flexibilité dans la conception. Cependant, une planification préalable minutieuse et une bonne compréhension des principes de base de l'adressage IP sont nécessaires pour une mise en œuvre réussie. En utilisant VLSM de manière appropriée, il est possible d'améliorer les performances du réseau et d'optimiser l'utilisation des ressources d'adressage IP disponibles.

II.10.2.1 Exemple d'utilisation de VLSM

Soit le réseau suivant avec une adresse réseau 202.160.22.0/24



En utilisant la technique du VLSM, on obtient un plan d'adressage détaillé dans ce tableau [5] :

Site	Adresse sous-réseau	Masque sous-réseau	Adresse diffusion	Intervalle des adresses valides
Site E	202.160.22.0/25	255.255.255.128	202.160.22.127	202.160.22.1-126
Site A	202.160.22.128/27	255.255.255.224	202.160.22.159	202.160.22.129-158
Site D	202.160.22.160/27	255.255.255.224	202.160.22.191	202.160.22.161-190
Site C	202.160.22.192/28	255.255.255.240	202.160.22.207	202.160.22.193-206
Site B	202.160.22.208/29	255.255.255.248	202.160.22.215	202.160.22.209-214
WAN R1-R2	202.160.22.216/30	255.255.255.252	202.160.22.219	202.160.22.217-218
WAN R2-R3	202.160.22.220/30	255.255.255.252	202.160.22.223	202.160.22.221-222

II.11 Outils et Méthodes pour l'Analyse du Trafic Réseau

II.11.1 méthodes pour l'analyse du trafic réseau

Les méthodes pour l'analyse de trafic réseau sont aussi des techniques et des approches systématiques utilisées pour examiner et comprendre le comportement du trafic de données sur un réseau informatique, parmi ces méthodes on trouve :

Analyse de Paquets (Packet Analysis)
L'analyse de paquets consiste à capturer et examiner les paquets individuels de données qui transitent sur un réseau, parmi les outils utilisés on trouve le Wireshark, tcpdump.
Parmi les utilisations principales de cette méthode :

- Dépannage des problèmes réseau.
- Détection des intrusions et des anomalies.
- Vérification des configurations de protocoles.

Analyse des Flux (Flow Analysis)

L'analyse des flux consiste à examiner les flux de données entre les dispositifs sur le réseau. Un flux est une séquence de paquets ayant des propriétés communes (par exemple, même source, destination, protocole), parmi les outils utilisés on trouve le NetFlow, sFlow et IPFIX permet de collecter des informations sur les flux de trafic sans avoir à analyser le contenu des paquets. Cela offre une meilleure évolutivité.

Parmi les utilisations principales de cette méthode :

- Surveillance de l'utilisation de la bande passante.
- Planification de la capacité.
- Détection des comportements anormaux et des anomalies de trafic.

Surveillance SNMP (Simple Network Management Protocol)

La surveillance SNMP utilise le protocole SNMP pour collecter des informations sur les dispositifs réseau (comme les routeurs, les commutateurs, les serveurs) et surveiller leur performance et leur état, parmi les outils utilisés on trouve SolarWinds Network Performance Monitor (NPM) et PRTG Network Monitor.

Parmi les utilisations principales de cette méthode :

- Surveillance de la santé des dispositifs réseau.
- Gestion des configurations.
- Collecte de statistiques de performance.

Monitoring (surveillance) en Temps Réel

Le monitoring en temps réel implique la surveillance continue du trafic réseau pour détecter immédiatement les anomalies et les problèmes, parmi les Outils Utilisés on trouve le Nagios**,** Zabbix et Cacti

Parmi les utilisations principales de cette méthode :

Surveillance proactive du réseau.

- Détection immédiate des problèmes de performance.
- Gestion et prévention des incidents.

Analyse Comportementale (Behavioral Analysis)

L'analyse comportementale utilise des techniques avancées pour surveiller et analyser le comportement des utilisateurs et des dispositifs sur le réseau afin de détecter des activités inhabituelles ou suspectes et cela permet d'identifier les menaces avancées, parmi les Outils Utilisés on trouve Darktrace, Vectra AI.

Parmi les utilisations principales de cette méthode :

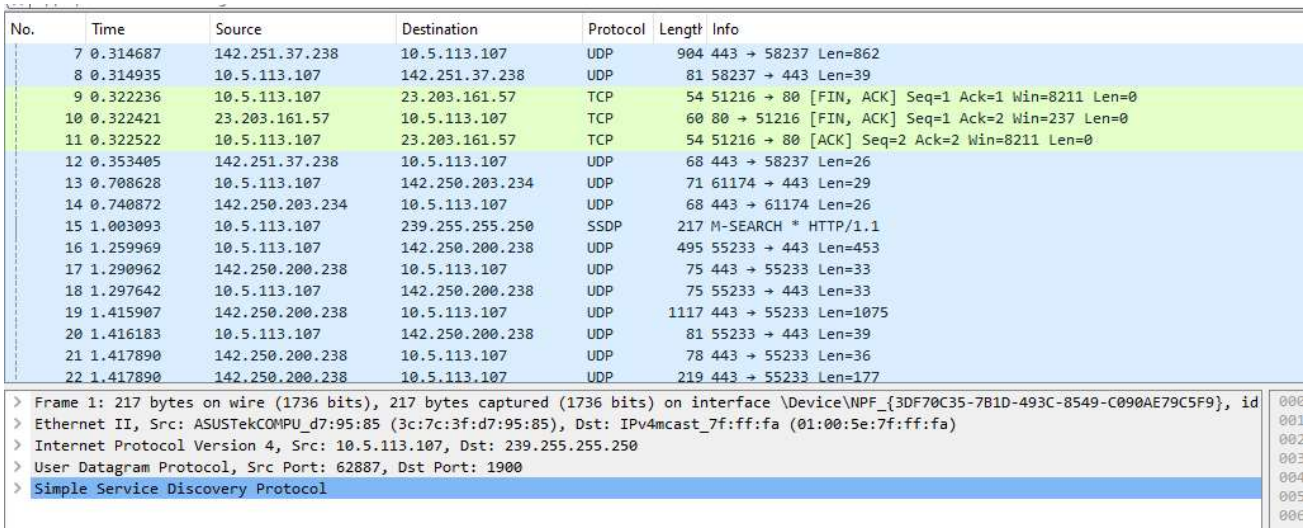
- Détection des menaces internes.
- Analyse des anomalies comportementales.
- Amélioration de la sécurité réseau.

II.11.2 outils d'analyse du trafic réseau (Network Traffic Analysis - NTA)

Les outils d'analyse de trafic réseau sont des logiciels ou des dispositifs utilisés pour surveiller, capturer, analyser et gérer le trafic de données qui circule sur un réseau informatique. Leur objectif est d'aider les administrateurs réseau à comprendre et à optimiser la performance du réseau, à identifier et résoudre les problèmes, et à garantir la sécurité des données, parmi les principaux outils d'analyse du trafic réseau on trouve :

Wireshark
Outil d'analyse de protocoles réseau qui permet de capturer et d'examiner les paquets en temps réel.
Utilisé pour le dépannage des problèmes réseau, l'analyse de la sécurité, et la vérification de la conformité aux normes.

Extrait d'une analyse de paquets réalisée sur le réseau de l'université :



tcpdump
Outil en ligne de commande pour capturer les paquets réseau, principalement utilisé sur les systèmes Unix/Linux. Utile pour une analyse rapide et automatisée des paquets.

NetFlow analyzer
Technologie de Cisco pour la collecte d'informations sur les flux de trafic réseau.
Utilisé pour la surveillance de la performance, la planification de la capacité, et la détection d'anomalies.

SolarWinds Network Performance Monitor (SNPM)
Outil complet de surveillance réseau utilisant SNMP, NetFlow, et d'autres protocoles.
Fournit des visualisations de la topologie réseau, des alertes et des rapports personnalisables.

PRTG Network Monitor
Outil polyvalent de surveillance réseau utilisant SNMP, NetFlow, sFlow, et d'autres technologies.
Offre une surveillance en temps réel de la bande passante et de la performance, avec des alertes et des rapports détaillés.

II.12 Conclusion

Il est essentiel de comprendre comment les données circulent sur un réseau informatique, comment les paquets se transmise, pour améliorer leur gestion et leur protection. Les données transitent à travers divers nœuds et dispositifs, empruntant des chemins complexes avant d'atteindre leur destination. Ce processus implique plusieurs protocoles et mécanismes de transmission qui garantissent la fluidité et l'efficacité du trafic.

Cependant, au-delà de la simple compréhension de ces mécanismes, il devient crucial d'examiner les vulnérabilités potentielles qui pourraient mettre en péril l'intégrité et la confidentialité des informations échangées. En effet, même avec une connaissance approfondie du fonctionnement du réseau, il reste indispensable de penser aux mesures de protection adéquates pour sécuriser ce flux d'informations.

Ainsi, en fin de compte, une question fondamentale se pose : pour bien appréhender la manière dont les données circulent sur un réseau, comment pouvons-nous les protéger efficacement contre les menaces potentielles tout en assurant une transmission fluide et sécurisée ?

Chapitre III : La sécurité des réseaux informatiques

III.1 Introduction

La sécurité des réseaux informatiques comprend un ensemble de mesures, de protocoles et de pratiques visant à protéger les systèmes, les données et les communications contre les menaces et les attaques potentielles. Elle repose sur plusieurs concepts clés qui sont indispensables à connaître pour saisir les fondements de la sécurité des réseaux informatiques.
Dans cette partie, nous allons nous concentrer sur la définition de la sécurité des réseaux informatiques, en expliquant les principes et les objectifs clés de cette discipline.

Le premier concept clé est celui de la confidentialité. La confidentialité fait référence à la protection des informations et des données confidentielles contre des accès non autorisés. Elle vise à garantir que seules les personnes autorisées puissent accéder aux informations sensibles et les utiliser de manière appropriée. Pour atteindre cet objectif, plusieurs mécanismes de sécurité peuvent être mis en place, tels que le chiffrement des données, l'authentification des utilisateurs et le contrôle d'accès aux ressources du réseau.

Un autre concept fondamental est l'intégrité, qui se réfère à la fiabilité et à la précision des informations. L'intégrité des données assure qu'elles ne sont pas modifiées, altérées ou corrompues de manière non autorisée ou accidentelle. Pour protéger l'intégrité des données, des mécanismes de vérification et de contrôle sont mis en place, tels que les codes de hachage, les signatures électroniques et les journaux d'audit.

La disponibilité des services et des ressources réseau est un autre objectif fondamental et également un concept clé de la sécurité des réseaux informatiques. Il s'agit de garantir que les utilisateurs autorisés ont accès aux informations et aux services dont ils ont besoin, sans interruption ni perturbation. Des mesures de redondance, de sauvegarde et de planification des capacités sont mises en place pour assurer la disponibilité des ressources informatiques.

L'authentification joue un rôle aussi important dans la sécurité des réseaux informatiques. L'authentification consiste à vérifier l'identité d'un utilisateur, d'un périphérique ou d'un système. Elle est réalisée à l'aide de mécanismes tels que les mots de passe, les cartes d'identité électroniques ou les certificats numériques.

Le contrôle d'accès est un autre concept essentiel. Il vise à limiter l'accès aux ressources informatiques aux seules personnes autorisées. Le contrôle d'accès peut être mis en œuvre à plusieurs niveaux, allant de l'identification et de l'authentification à l'utilisation de listes de contrôle d'accès pour définir les droits et les permissions des utilisateurs.

Enfin, la traçabilité est un concept important dans la sécurité des réseaux informatiques. La traçabilité permet de suivre et d'enregistrer les activités des utilisateurs, des systèmes et des réseaux afin de détecter les comportements suspects ou les violations de sécurité. Les logs, les journaux d'activité et les outils de surveillance sont utilisés pour assurer la traçabilité des événements.

La compréhension de ces concepts clés est essentielle pour appréhender la problématique de la sécurité des réseaux informatiques de manière approfondie. Chacun de ces concepts contribue à la mise en place de stratégies et de mesures de sécurité qui permettent de protéger les systèmes, les données et les réseaux contre les menaces et les attaques. En connaissant et en maîtrisant ces concepts, il devient possible de développer des politiques de sécurité solides et de mettre en place des mécanismes de défense efficaces pour faire face aux défis actuels et futurs de la sécurité des réseaux informatiques.

III.2 Introduction à la sécurité des réseaux informatiques

III.2.1 L'importance croissante des réseaux informatiques

L'importance croissante des réseaux informatiques a transformé la façon dont les organisations fonctionnent et interagissent. Les réseaux informatiques permettent la transmission et le partage rapide de l'information, facilitant ainsi la prise de décision, la collaboration et l'innovation. Dans le contexte de la sécurité des réseaux informatiques, cette évolution représente à la fois un défi et une opportunité. Il est essentiel de comprendre les différentes dimensions de l'importance croissante des réseaux informatiques pour garantir la protection des données et des systèmes contre les menaces et les attaques potentielles.
La première dimension de l'importance des réseaux informatiques réside dans leur rôle central au sein des organisations. Les réseaux informatiques relient les différents départements, bureaux et sites d'une organisation, permettant une communication et une coordination efficaces. Les applications et les services basés sur les réseaux sont devenus indispensables pour les activités quotidiennes des entreprises, que ce soit pour la communication interne, la gestion des ressources ou le partage des informations sensibles. Ainsi, la disponibilité et l'intégrité du réseau informatique sont cruciales pour garantir le bon fonctionnement de l'organisation.

La deuxième dimension de l'importance croissante des réseaux informatiques réside dans leur rôle dans la connectivité mondiale. Les réseaux informatiques permettent la communication et l'échange d'informations à l'échelle mondiale, facilitant ainsi les échanges commerciaux, la collaboration internationale et la mobilité des individus. Avec la mondialisation croissante, les entreprises ont de plus en plus besoin de se connecter et d'interagir avec des partenaires, des clients et des fournisseurs situés dans différentes parties du monde. Cela implique un niveau élevé de sécurité des réseaux pour protéger les données confidentielles et les informations commerciales sensibles contre les fuites ou les attaques malveillantes.

La troisième dimension de l'importance des réseaux informatiques réside dans leur rôle dans la transformation numérique. Les réseaux informatiques sont le fondement de la numérisation des processus et des opérations commerciales. Les entreprises adoptent de plus en plus de technologies telles que l'Internet des objets (IoT), l'intelligence artificielle (IA) et le cloud computing, qui reposent sur des infrastructures réseau robustes et sécurisées. La transformation numérique permet

d'automatiser les tâches, d'améliorer l'efficacité opérationnelle et d'offrir de nouveaux produits et services aux clients. Cependant, cela augmente également la surface d'attaque potentielle, nécessitant une attention accrue à la sécurité des réseaux informatiques.

De plus, avec l'évolution constante des menaces et des attaques informatiques, la sécurité des réseaux informatiques est un enjeu en constante évolution. Les professionnels de la sécurité informatique doivent rester à jour sur les nouvelles techniques d'attaque et les meilleures pratiques de défense pour garantir la protection optimale des réseaux. La collaboration et le partage d'informations entre les entités gouvernementales, les organisations privées et les institutions académiques sont essentiels pour renforcer la sécurité des réseaux informatiques à l'échelle mondiale.

En résumé, Ces dimensions soulignent l'importance de la sécurité des réseaux informatiques pour protéger les données, les systèmes et les processus contre les menaces et les attaques. La compréhension de ces dimensions permet de justifier la nécessité d'une étude approfondie de la sécurité des réseaux informatiques et de développer des stratégies et des mesures de sécurité appropriées pour faire face aux défis et aux risques associés. Avec l'importance croissante des réseaux informatiques, la protection de la sécurité des réseaux est devenue une priorité absolue pour toutes les organisations qui veulent garantir une gestion efficace et sécurisée de leurs ressources et de leurs données.

III.2.2 Définition de la sécurité des réseaux informatiques

La sécurité des réseaux informatiques est un sujet primordial dans le domaine de l'informatique et des technologies de l'information. Avec l'évolution constante des technologies et l'augmentation des cyberattaques, la sécurité des réseaux informatiques est devenue une nécessité absolue pour assurer la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques.

La sécurité des réseaux informatiques est le processus de protection des réseaux, des données et des systèmes contre les menaces potentielles et les attaques malveillantes. Il vise à prévenir les intrusions, à détecter les activités suspectes, à réagir aux incidents de sécurité et à en limiter l'impact.

La sécurité des réseaux informatiques s'appuie sur plusieurs principes clés pour atteindre ses objectifs. Tout d'abord, le principe de défense en profondeur repose sur le fait de mettre en place plusieurs couches de sécurité, de la périphérie du réseau jusqu'à ses composants internes, afin de renforcer la résistance aux attaques. Ensuite, le principe du moindre privilège consiste à donner aux utilisateurs uniquement les droits nécessaires pour effectuer leur travail, afin de minimiser les risques d'abus ou de compromission.

En outre, la sécurité des réseaux informatiques repose sur le principe de la gestion des identités et des accès, qui consiste à gérer de manière centralisée les comptes et les autorisations des utilisateurs, afin de garantir des accès appropriés et de prévenir les intrusions ou les utilisations abusives. Le principe de la détection et de la réponse aux incidents de sécurité est également essentiel, en mettant en place des systèmes de surveillance et de détection des activités suspectes, et en réagissant de manière appropriée en cas d'incident.

Figure III.34: sécurité des réseaux informatique [31]

En conclusion, la sécurité des réseaux informatiques est une discipline clé dans le domaine de l'informatique et des technologies de l'information. Elle vise à protéger les réseaux, les données et les systèmes contre les menaces et les attaques malveillantes, en assurant la confidentialité, l'intégrité et la disponibilité des informations. Grâce à des principes et à des mesures de sécurité appropriés, la sécurité des réseaux informatiques permet de renforcer la confiance des utilisateurs et de garantir le bon fonctionnement des systèmes informatiques.

III.3 Enjeux et risques associés à la sécurité des réseaux informatique

Les enjeux et risques associés à la sécurité des réseaux informatiques sont nombreux et nécessitent une attention constante de la part des entreprises et des professionnels de la sécurité informatique. Comprendre ces enjeux et risques est essentiel pour mettre en place des mesures adéquates de protection des réseaux et des données.

1. L'un des principaux enjeux de la sécurité des réseaux informatiques est la protection des données sensibles. Les entreprises stockent une grande quantité de données confidentielles, telles que des informations clients, des données financières, des propriétés intellectuelles, etc. La fuite ou la compromission de ces données peut entraîner des conséquences financières désastreuses, mais également nuire à la réputation et à la confiance des clients. Les professionnels de la sécurité des réseaux doivent donc mettre en œuvre des stratégies de protection des données, telles que le chiffrement des données, l'accès restreint aux informations sensibles et la surveillance continue des activités suspectes.

2. Un autre enjeu important est la protection contre les cyberattaques. Les réseaux informatiques sont constamment la cible d'attaques par des pirates informatiques qui cherchent à voler des données, à perturber les systèmes ou à obtenir un avantage financier. Pour faire face à ces menaces, les professionnels de la sécurité des réseaux doivent mettre en place des mesures de prévention, de

détection et de réponse aux attaques, en utilisant des pares-feux, des antivirus, des systèmes de détection d'intrusion, etc.

3. La sécurisation des communications est également un enjeu crucial dans la sécurité des réseaux informatiques, notamment avec le développement du travail à distance et des échanges entre partenaires externes. Il est essentiel que les communications entre les différents acteurs du réseau soient chiffrées et sécurisées pour protéger les informations échangées des interceptions ou des altérations. Cela comprend l'utilisation de protocoles de chiffrement robustes, de certificats numériques et de systèmes d'authentification solides pour garantir l'intégrité, la confidentialité et l'authenticité des communications.

4. En outre, les aspects juridiques et réglementaires sont également des enjeux importants dans le domaine de la sécurité des réseaux informatiques. Les entreprises et les organisations doivent se conformer à des réglementations en matière de protection des données personnelles, de confidentialité des communications, de sûreté des systèmes d'information, etc. La non-conformité à ces réglementations peut entraîner des sanctions financières, des poursuites judiciaires ou des dommages réputationnels importants.

5. Enfin, un autre enjeu clé est la sensibilisation des utilisateurs aux bonnes pratiques en matière de sécurité informatique. Les erreurs humaines, telles que l'utilisation de mots de passe faibles, le téléchargement de logiciels malveillants ou la divulgation d'informations sensibles, constituent souvent une porte d'entrée pour les attaquants. Il est donc essentiel de former les utilisateurs aux bonnes pratiques en matière de sécurité, tels que l'utilisation de mots de passe forts, la mise à jour régulière des logiciels, la reconnaissance des tentatives de phishing, etc.

La prise en compte de ces différents enjeux et risques associés à la sécurité des réseaux informatiques permet aux entreprises de mettre en place des mesures de sécurité adéquates pour protéger leurs réseaux et leurs données. En comprenant les menaces et en évaluant les vulnérabilités, les entreprises peuvent développer des stratégies de sécurité robustes et réactives pour prévenir les incidents de sécurité et minimiser les conséquences en cas d'attaque. La sécurité des réseaux informatiques est un processus continu qui nécessite une vigilance constante et une adaptation aux évolutions des menaces, afin de garantir la protection des données et la continuité des activités.

III.4 Menaces, attaques d’un réseau informatique

Les menaces et attaques sont des risques majeurs pour la sécurité des réseaux informatiques. Avec la prolifération des technologies de l'information et de la communication, les réseaux informatiques sont devenus des cibles de choix pour les cybercriminels, les espions nationaux et les hackers malveillants. Les attaques peuvent prendre différentes formes, allant des attaques par déni de service aux ransomwares en passant par l'ingénierie sociale. Il est essentiel de comprendre ces menaces et attaques afin de pouvoir mettre en place des mesures de protection adéquates.

III.4.1 Les types de menaces et d'attaques

Les attaques par déni de service (DDoS)

Les attaques par déni de service (DDoS) sont l'une des principales menaces auxquelles les réseaux informatiques sont confrontés. Ces attaques visent à saturer les ressources d'un système cible, telles que la bande passante, les processeurs ou la mémoire, afin de submerger les ressources réseau et rendre les applications et services inaccessibles aux utilisateurs légitimes. Les attaquants utilisent souvent des botnets, qui sont des réseaux d'ordinateurs compromis et contrôlés à distance, Ces ordinateurs infectés, appelés "zombies", sont utilisés pour générer et relayer un trafic malveillant vers la cible. L'utilisation de botnets permet aux attaquants de masquer leur identité et de coordonner des attaques à grande échelle, rendant difficile la défense contre les attaques DDoS.

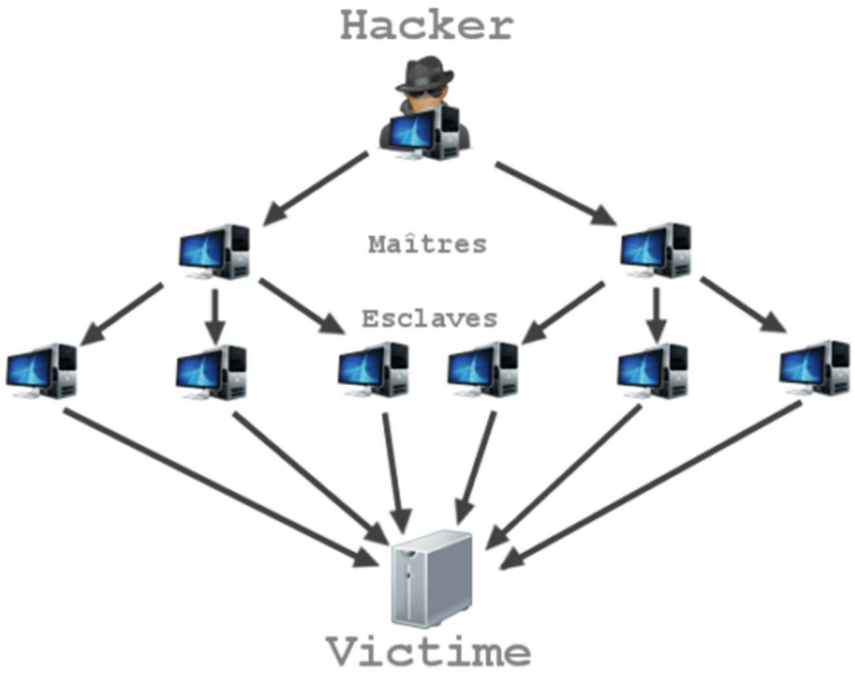


Figure III.35: attaque DDOS [32]

Les attaques DDoS représentent une menace persistante pour la sécurité des réseaux informatiques. Elles peuvent causer des perturbations majeures, entraînant des pertes financières, une perte de productivité et une atteinte à la réputation. Pour se protéger contre les attaques DDoS, les organisations doivent mettre en place des stratégies de défense adaptées.

Ces stratégies de défense peuvent inclure la mise en place de systèmes de détection et de prévention des intrusions (IDS/IPS) pour identifier et bloquer les flux de trafic malveillants, l'utilisation de pares-feux à état pour limiter l'accès non autorisé aux ressources réseau, et la mise en place de plans de continuité des activités pour faire face aux attaques DDoS et minimiser leur impact.

En outre, les fournisseurs de services Internet (FSI) jouent un rôle crucial dans la protection contre les attaques DDoS. Ils peuvent utiliser des systèmes de détection avancés sur leur infrastructure pour bloquer le trafic malveillant en amont et prévenir les attaques avant qu'elles n'atteignent les systèmes

cibles. Ils peuvent également proposer des services de mitigation des attaques DDoS, qui consistent à rediriger le trafic malveillant vers des centres de nettoyage pour l'analyser et le filtrer avant de le renvoyer au système cible.

Les attaques par injection de codes malveillants (malwares)

Les attaques par injection de codes malveillants, également connues sous le nom de malwares, sont l'une des principales menaces auxquelles les réseaux informatiques sont confrontés. Les malwares sont des programmes malveillants conçus pour infiltrer, perturber et compromettre les systèmes informatiques. Ces attaques peuvent prendre différentes formes, telles que les virus, les vers, les chevaux de Troie, les ransomwares, et bien d'autres.

Figure III.36: attaque par injection de codes malveillants [33]

Les malwares sont généralement introduits dans un système par le biais de techniques d'injection de codes dans les fichiers exécutables, les scripts, les bases de données, ou même les commandes envoyées aux serveurs.

Les attaques par injection de codes malveillants peuvent entraîner des conséquences graves pour les réseaux informatiques. Elles peuvent permettre aux attaquants de voler des informations confidentielles, d'accéder aux ressources du système, de bloquer l'accès aux utilisateurs légitimes, de modifier ou de supprimer des données de la base de données ou même de prendre le contrôle total d'un système. Ces attaques peuvent causer des dommages financiers importants, des violations de la vie privée, ainsi que des perturbations opérationnelles pour les organisations ciblées.

- **Chevaux de Troie (trojan)**

Les chevaux de Troie sont l'une principales menaces auxquelles sont confrontés les réseaux informatiques. Un cheval de Troie, également connu sous le nom de trojan, est un type de logiciel malveillant qui se cache à l'intérieur d'un programme légitime et qui s'exécute à l'u de l'utilisateur. Tire son nom de légende grecque cheval de Troie, où les Grecque ont dissimulé des soldats à l'intérieur d'un immense cheval en bois pour infiltrer la cité de Troie.

Figure III.37: l'attaque par les chevaux de Troie [34]

Les chevaux de Troie peuvent prendre de nombreuses formes et sont souvent camouflés en logiciels apparemment inoffensifs, tels que des jeux, des utilitaires ou des applications téléchargeables. Les utilisateurs sont amenés à télécharger et à exécuter ces programmes malveillants, sans se douter des conséquences. Une fois installés, les chevaux de Troie permettent aux pirates informatiques d'accéder aux systèmes, de voler des données confidentielles, de détourner des comptes bancaires, d'installer d'autres logiciels malveillants ou de prendre le contrôle à distance des ordinateurs infectés.

Leur capacité à se cacher et à se propager silencieusement dans les systèmes en font des outils dangereux entre les mains des pirates informatiques. Les chevaux de Troie peuvent être transmis par différents moyens, tels que des pièces jointes infectées dans des e-mails, des sites web compromis ou des clés USB infectées. Une fois qu'un utilisateur a exécuté le programme infecté, le cheval de Troie se cache dans le système et peut avoir des effets dévastateurs. Certains chevaux de Troie sont conçus pour voler des informations sensibles, tels que des identifiants de connexion, des numéros de carte de crédit, des coordonnées bancaires ou des informations personnelles. D'autres peuvent endommager le système en supprimant, modifiant ou corrompant des fichiers importants.

La lutte contre les chevaux de Troie et la protection des réseaux informatiques contre ces menaces sont des défis majeurs pour les professionnels de la sécurité informatique. Il existe plusieurs mesures de prévention et de détection qui peuvent être mises en place pour réduire les risques liés aux chevaux de Troie. Tout d'abord, il est essentiel de maintenir à jour les systèmes d'exploitation et les logiciels afin de corriger les vulnérabilités connues. De plus, l'utilisation d'un logiciel antivirus et d'un pare-feu fiable peut aider à détecter et à bloquer les chevaux de Troie avant qu'ils ne puissent causer des dommages ainsi de la sensibilisation des utilisateurs est également cruciale dans la lutte contre les chevaux de Troie.

- **Ransomware**

Un ransomware est une forme de logiciel malveillant (malware) qui restreint l'accès à un système informatique ou à des données en les chiffrant, puis demande aux victimes de payer une rançon pour en récupérer l'accès. Ce type d'attaque est devenu de plus en plus courant et constitue une menace majeure pour la sécurité des réseaux informatiques. Les ransomwares peuvent causer des perturbations importantes, tant au niveau des particuliers que des organisations, en entraînant des pertes financières, une paralysie des activités et une violation de la confidentialité des données.

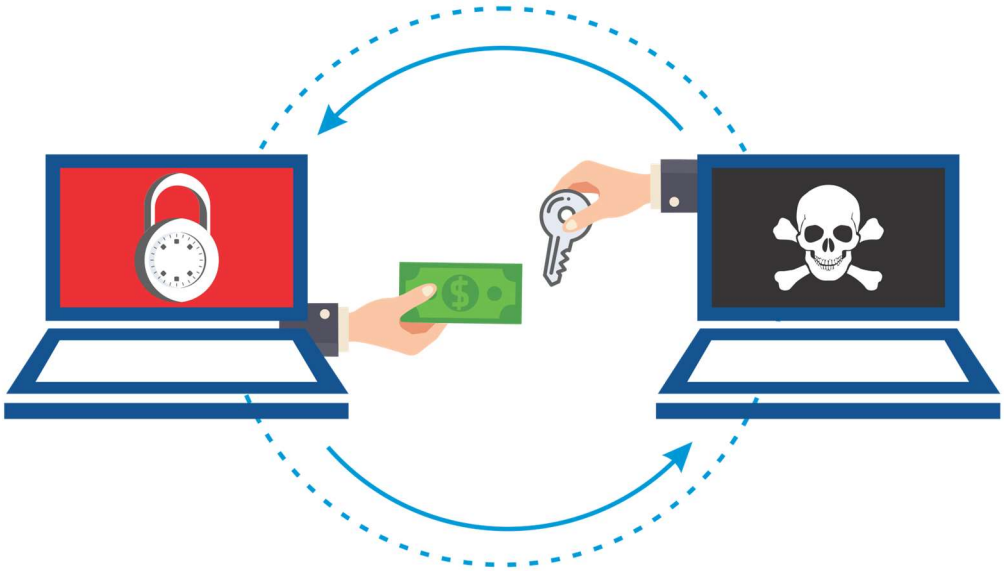


Figure III.38: Ransomwares [35]

Les ransomwares se propagent généralement par le biais de pièces jointes d'e-mails malveillants, de liens infectés ou de téléchargements frauduleux. Une fois qu'ils ont infiltré un système, ils utilisent des techniques de chiffrement avancées pour bloquer l'accès aux fichiers et aux données. Les victimes sont ensuite confrontées à une demande de rançon, généralement en cryptomonnaie, pour récupérer leurs données. Il est important de noter que même si les victimes paient la rançon, il n'y a aucune garantie que les cybercriminels honoreront leur promesse de déchiffrer les données.

Outre les pertes financières potentielles, les ransomwares peuvent également entraîner d'autres conséquences néfastes. Par exemple, une entreprise peut subir une perte de productivité importante si ses systèmes informatiques sont paralysés. De plus, les données sensibles ou confidentielles peuvent être compromises, ce qui peut avoir un impact sur la réputation de l'entreprise et la confiance de ses clients. Enfin, le coût de la remédiation et du renforcement des mesures de sécurité informatique peut être considérable.

Pour faire face aux ransomwares, il est essentiel de mettre en place des mesures de prévention et de réponse appropriées. Une sauvegarde régulière des données importantes et leur stockage hors ligne constitue une mesure clé pour minimiser les pertes de données en cas d'attaque de ransomware. De plus, une sensibilisation des utilisateurs aux risques de téléchargements ou de pièces jointes suspects peut aider à prévenir les infections par ransomware.

Phishing (hameçonnage)

Le phishing, également connu sous le nom d'hameçonnage, est une méthode d'attaque couramment utilisée par les cybercriminels pour tromper les utilisateurs et leur soutirer des informations confidentielles, telles que des identifiants de connexion, des informations bancaires ou des données personnelles. Cette technique repose sur la création de faux sites web ou de fausses communications de manière à sembler légitimes, en utilisant des logos, des polices ou des contenus qui imitent ceux de l'organisation ciblée, pour inciter les utilisateurs à divulguer leurs informations sensibles Les attaques de phishing reposent généralement sur des techniques de tromperie et d'ingénierie sociale pour inciter les utilisateurs à agir de manière non méfiante. Les hackers peuvent envoyer des e-mails frauduleux, des messages instantanés ou des SMS contenant des liens vers de faux sites web ou des pièces jointes malveillantes. Ces communications sont conçues.

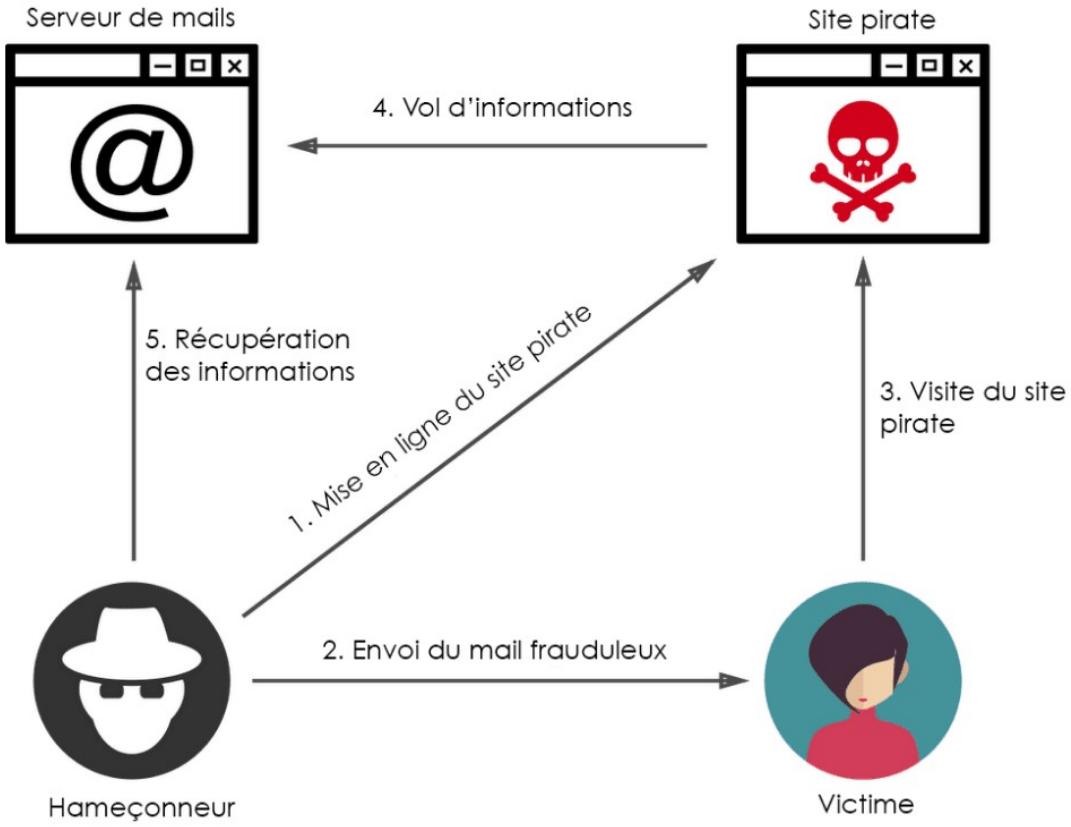


Figure III.39:L'hameçonnage [36]

Lorsqu'un utilisateur tombe dans le piège du phishing et divulgue ses informations sensibles, les conséquences peuvent être graves. Les hackers peuvent accéder à des comptes en ligne, effectuer des transactions frauduleuses, voler des identités ou accéder à d'autres informations confidentielles. Pour se protéger contre les attaques de phishing, il est essentiel d'adopter des bonnes pratiques de sécurité informatique. Les utilisateurs doivent être constamment vigilants et méfiants lorsqu'ils reçoivent des e-mails, des messages ou des appels suspects, et doivent toujours vérifier l'authenticité des sources avant de divulguer des informations sensibles.

Il est important de reconnaître les signes d'une attaque de phishing et de ne jamais divulguer d'informations confidentielles sans vérifier l'authenticité de la source. En sensibilisant les utilisateurs et en mettant en place des mesures de sécurité adéquates, il est possible de réduire les risques liés au phishing et de protéger la sécurité des réseaux informatiques.

Man in the middle

Le terme « man the middle » désigne une attaque laquelle un individu malveillant s'insère entre deux parties qui communiquent, en écoutant et en interceptant les échanges de données. Cette attaque est particulièrement dangereuse car elle permet à l'attaquant d'intercepter, de modifier et de réacheminer les informations échangées entre les deux parties, sans que celles-ci ne se rendent compte de la présence de l'intermédiaire. Cette technique est couramment utilisée dans les attaques visant à voler des informations sensibles telles que des identifiants de connexion, des mots de passe ou des données financières.

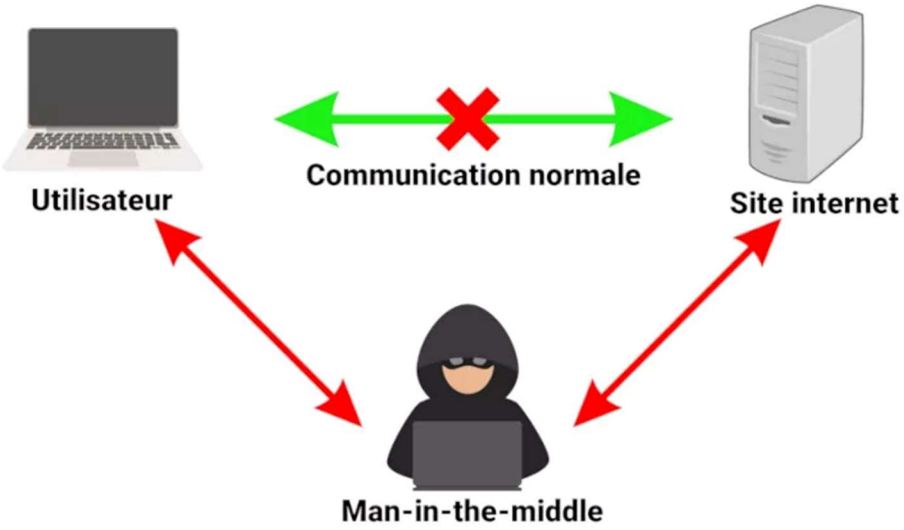


Figure III.40: Attaque par Man in the middle [37]

Lors d'une attaque "man in the middle", l'attaquant crée un point d'accès malveillant entre les deux parties légitimes. Cela peut être réalisé en utilisant des techniques telles que l'usurpation d'adresse IP, le détournement de routeurs ou l'utilisation d'un réseau Wi-Fi public non sécurisé. Une fois qu'il a accès aux données échangées, l'attaquant peut les utiliser à des fins malveillantes. Par exemple, il peut voler des informations d'identification pour accéder à des comptes en ligne, récupérer des données financières pour effectuer des transactions frauduleuses ou même modifier les informations en transit pour tromper les parties légitimes. De plus, l'attaquant peut également rediriger le trafic vers des serveurs malveillants, permettant ainsi de collecter encore plus d'informations confidentielles.

Pour mener à bien une attaque "man in the middle", l'attaquant peut utiliser différentes méthodes, notamment l'ARP poisoning (empoisonnement ARP) qui consiste à envoyer de fausses adresses MAC dans le réseau local, permettant ainsi à l'attaquant de rediriger le trafic vers lui-même, le DNS spoofing (usurpation DNS) ou l'utilisation de certificats falsifiés.

Pour contrer l'attaque "man in the middle", il est essentiel de mettre en place des mesures de sécurité appropriées. Tout d'abord, l'utilisation d'un réseau Wi-Fi sûr et sécurisé est recommandée pour éviter toute interception des données en transit. De plus, l'implémentation de protocoles de cryptage forts tels que le SSL/TLS est essentielle pour sécuriser les communications en ligne. La vérification des certificats SSL/TLS est également cruciale pour s'assurer de l'authenticité des sites Web visités et éviter toute redirection vers des sites malveillants.

- **Usurpation de DNS (DNS spoofing)**

L'usurpation de DNS est l'une des menaces majeures auxquelles les réseaux informatiques sont confrontés. Cette attaque consiste à falsifier les enregistrements DNS (Domain Name System) afin de rediriger le trafic vers des serveurs malveillants. Le DNS est responsable de la traduction des noms de domaine en adresses IP, et toute altération de ces enregistrements peut entraîner des conséquences graves sur la sécurité et l'intégrité des communications en ligne. Il est donc essentiel de comprendre en détail cette menace et les mécanismes qui la sous-tendent afin de pouvoir la prévenir et la contrer efficacement.

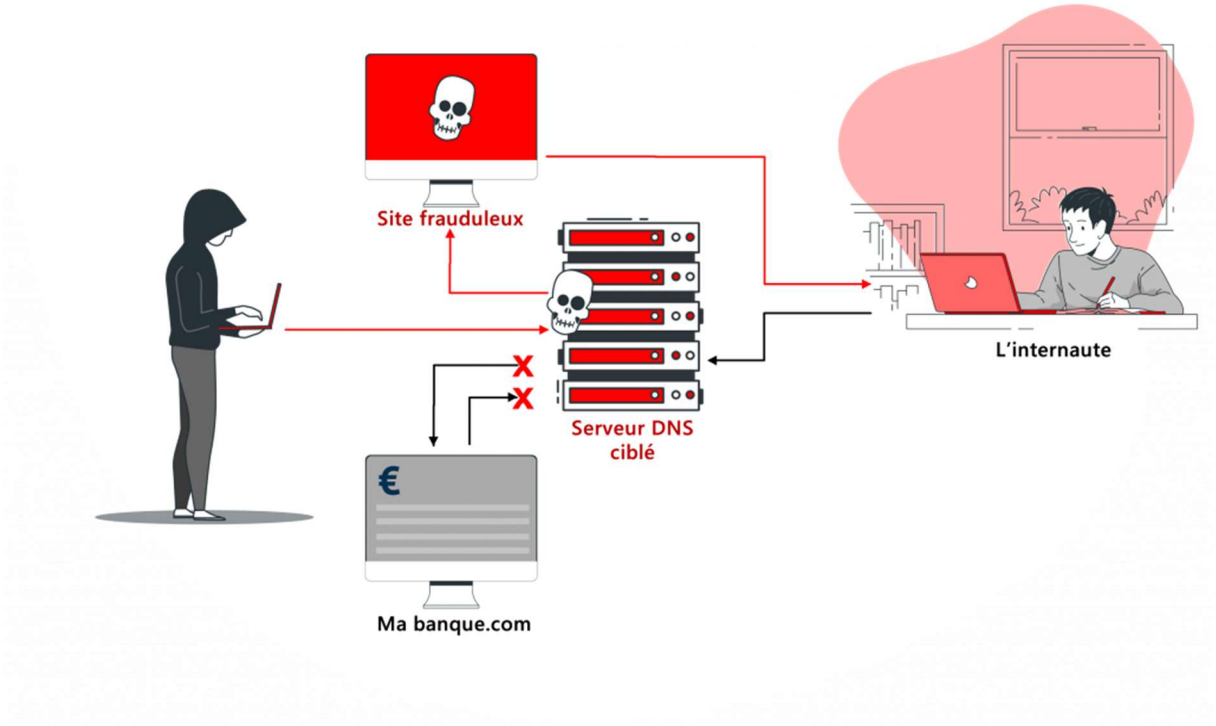


Figure III.41: DNS spoofing [38]

L'usurpation de DNS peut être réalisée de différentes manières, dont les principales sont le DNS cache poisoning et le DNS spoofing.
Le DNS cache poisoning consiste à corrompre les caches DNS sur les serveurs ou sur les clients afin de leur faire croire que des enregistrements DNS sont associés à de mauvaises adresses IP. Cela peut être réalisé en exploitant des vulnérabilités dans les protocoles DNS ou en menant des attaques de type man-in-the-middle pour intercepter et altérer les requêtes DNS.
Le DNS spoofing, quant à lui, consiste à falsifier les réponses DNS envoyées aux clients en se faisant passer pour un serveur DNS légitime. Cette technique peut être utilisée pour rediriger le trafic vers des sites malveillants et permettre des attaques de phishing ou d'injection de code malveillant.

La prévention et la détection de l'usurpation de DNS reposent sur plusieurs mesures de sécurité. Tout d'abord, il est essentiel de maintenir les logiciels et les systèmes à jour pour éviter les vulnérabilités connues qui pourraient être exploitées par les attaquants. De plus, la mise en place de pare-feu et de systèmes de filtrage du trafic peut aider à bloquer les requêtes DNS malveillantes et à détecter les tentatives d'usurpation ainsi la mise en œuvre de technologies de chiffrement et la surveillance constante des enregistrements DNS.

- **Usurpation d'identité**

L'usurpation d'identité consiste à se faire passer pour une autre personne en utilisant ses informations personnelles et confidentielles, telles que son nom, son adresse, son numéro de sécurité sociale ou ses identifiants de connexion. L'objectif de cette attaque est généralement de voler des informations sensibles, de commettre des fraudes financières ou de compromettre la réputation de la victime. Comprendre les mécanismes de l'usurpation d'identité, les techniques utilisées par les attaquants et les conséquences potentielles de cette menace est nécessaire pour garantir la sécurité des réseaux informatiques.

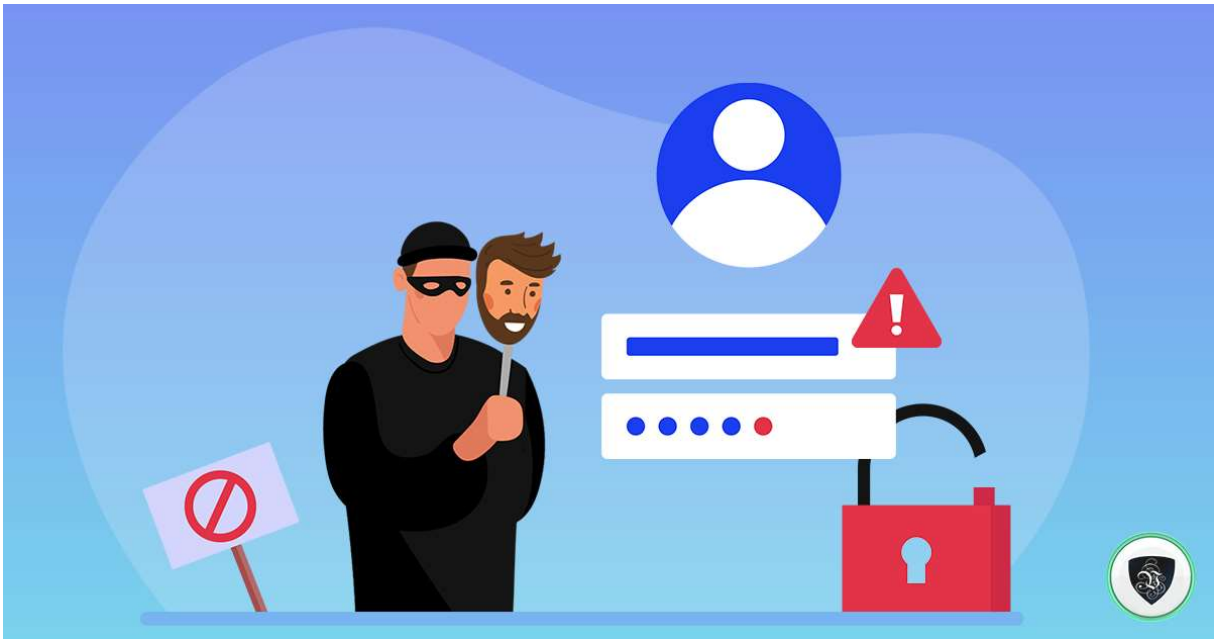


Figure III. 42: Usurpation d'identité [39]

L'usurpation d'identité peut prendre différentes formes, telles que le phishing, le spoofing qui consiste à falsifier des adresses IP ou des adresses e-mail pour se faire passer pour quelqu'un d'autre, trompant ainsi les victimes et leur faisant croire que les communications proviennent de sources fiables ou le keylogging qui est une technique utilisée pour enregistrer les frappes clavier des victimes et collecter ainsi leurs identifiants de connexion ou d'autres informations confidentielles.

Pour prévenir l'usurpation d'identité, il est essentiel de mettre en œuvre des mesures de sécurité appropriées. Cela inclut l'utilisation de méthodes d'authentification robustes, telles que la vérification en deux étapes et l'utilisation de mots de passe forts. La sensibilisation des utilisateurs aux techniques d'usurpation d'identité et la formation à la détection des e-mails ou des messages suspects sont également importantes pour réduire les risques.

Les attaques d'ingénierie sociale

Qui exploitent la confiance et la manipulation psychologique pour obtenir des informations confidentielles ou pour inciter les utilisateurs à effectuer des actions compromettantes. [6]

III.5 Les vulnérabilités et les failles de sécurité

III.5.1 Les failles de protocoles

Les failles de protocoles sont des vulnérabilités dans les protocoles de communication utilisés pour établir et maintenir des connexions au sein des réseaux informatiques. Les protocoles de communication, tels que TCP/IP, HTTP, FTP, sont des ensembles de règles et de procédures qui régissent l'échange d'informations entre les différents équipements du réseau. Cependant, ces protocoles peuvent présenter des failles de conception ou d'implémentation qui peuvent être exploitées par des attaquants pour compromettre la sécurité du réseau.

Les failles de protocoles peuvent se manifester de plusieurs manières, notamment par des problèmes d'authentification, des erreurs de validation, des faiblesses cryptographiques et des défauts de conception. Par exemple, une faille d'authentification peut permettre à un attaquant de contourner les mécanismes de sécurité et d'accéder illégalement à un système ou à des données sensibles. Une faille de validation peut permettre à un attaquant de manipuler les données échangées entre les équipements du réseau et d'introduire des informations malveillantes.

Les faiblesses cryptographiques dans les protocoles de communication peuvent également être exploitées par des attaquants pour compromettre la confidentialité et l'intégrité des données échangées. Par exemple, si un protocole utilise un algorithme de chiffrement faible ou s'il n'utilise pas de certificats numériques pour vérifier l'authenticité des parties communicantes, il devient vulnérable aux attaques telles que l'interception de données ou l'usurpation d'identité.

Les défauts de conception des protocoles peuvent également être des failles de sécurité potentielles. Par exemple, certains protocoles peuvent autoriser des transactions non sécurisées ou permettre des opérations sans vérification adéquate, créant ainsi des opportunités pour des attaques telles que l'injection de code ou la manipulation de données.

Pour exploiter les failles de protocoles, les attaquants peuvent utiliser différentes techniques, telles que l'ingénierie sociale, l'exploitation de logiciels malveillants, l'usurpation d'identité ou l'utilisation d'outils automatisés pour scanner et analyser le réseau à la recherche de vulnérabilités. Une fois qu'une faille de protocole est exploitée, un attaquant peut accéder à des informations confidentielles, compromettre le fonctionnement du réseau ou même prendre le contrôle des équipements.

La prise de conscience des failles de protocoles et la mise en place de mesures de sécurité appropriées sont essentielles pour protéger les réseaux informatiques contre les attaques. Cela peut inclure l'utilisation de versions mises à jour des protocoles, la configuration appropriée des paramètres de sécurité, le monitoring régulier des vulnérabilités et l'utilisation de mécanismes de détection d'intrusion pour détecter et prévenir les attaques en temps réel.

III.5.2 Les failles de logiciels

Les failles de logiciels peuvent être exploitées par des attaquants pour accéder illégalement à des systèmes, voler des informations sensibles ou causer des dommages aux infrastructures informatiques.

L'une des vulnérabilités les plus courantes des logiciels est la faille de programmation. Les erreurs de programmation, telles que les erreurs de mémoire, les erreurs de validation des entrées ou les conditions de concurrence mal gérées, peuvent donner aux attaquants la possibilité d'exécuter du code malveillant sur le système cible. Ces erreurs peuvent survenir à toutes les étapes du processus de développement logiciel, de la conception à l'implémentation, et peuvent être le résultat d'une mauvaise gestion des ressources, d'une compréhension insuffisante des spécifications de sécurité ou simplement d'une négligence du programmeur. Les attaquants peuvent exploiter ces failles pour prendre le contrôle de l'ordinateur ou pour voler des informations sensibles.

Une autre catégorie de failles de logiciels réside dans les failles de configuration. Les applications et les systèmes informatiques sont souvent configurés avec des paramètres par défaut peu sécurisés, qui peuvent être exploités par des cybercriminels. Par exemple, un administrateur système peut omettre de modifier les mots de passe par défaut ou de désactiver les fonctionnalités inutiles, laissant ainsi des points d'entrée faciles pour les attaquants. De plus, les mises à jour de sécurité peuvent être négligées ou retardées, laissant les systèmes exposés à des vulnérabilités connues. La mauvaise configuration des pares-feux, des serveurs web ou des bases de données peut également rendre les systèmes vulnérables à des attaques.

Enfin, les failles de logiciels peuvent également être introduites intentionnellement par des développeurs malveillants ou des attaquants internes. Ces attaques dites "backdoors" ou portes dérobées peuvent permettre à un acteur mal intentionné d'accéder et de contrôler un système distant discrètement. Les portes dérobées peuvent être insérées dans le code source d'un programme de manière à contourner les mesures de sécurité et à permettre l'accès illégal, souvent à des fins de surveillance, d'espionnage ou de sabotage. La détection de ces portes dérobées nécessite une analyse minutieuse du code source et une veille constante sur les menaces émergentes.

III.5.3 Les failles liées aux utilisateurs

Les failles liées aux utilisateurs représentent l'une principales vulnérabilités dans la sécurité des réseaux informatiques. Malgré les mesures de sécurité mises en place, les erreurs humaines, les comportements négligents et les attaques de phishing continuent de compromettre la sécurité des réseaux. Comprendre les différentes failles liées aux utilisateurs permet de mieux les prévenir et de renforcer la sécurité des infrastructures informatiques.

Les erreurs humaines sont l'une des principales sources de failles dans les réseaux informatiques qui peuvent inclure des erreurs de configuration, des erreurs de câblage, des erreurs d'installation ou des erreurs de maintenance. Un simple clic sur un lien malveillant, un mot de passe faible ou partagé, ou encore une mauvaise configuration des paramètres de sécurité peut ouvrir la porte à des attaques. Les utilisateurs peuvent être mal informés, manquer de formation ou être tout simplement négligents dans leurs pratiques de sécurité informatique. La gestion insuffisante des identifiants et des mots de passe, par exemple, peut permettre à des cybercriminels d'accéder facilement à des données confidentielles.

Les comportements négligents des utilisateurs peuvent également compromettre la sécurité des réseaux informatiques. L'ouverture de pièces jointes provenant de sources inconnues, le téléchargement de logiciels piratés ou l'utilisation d'appareils non sécurisés sont autant de comportements à risque pouvant entraîner des infections par des malwares ou des attaques de

phishing. De plus, l'utilisation d'informations personnelles sur les réseaux sociaux peut être exploitée par des cybercriminels pour mener des attaques ciblées.

Les attaques de phishing représentent une menace majeure pour la sécurité des réseaux informatiques. Les cybercriminels utilisent des techniques sophistiquées pour manipuler les utilisateurs et les inciter à divulguer des informations sensibles telles que des identifiants, des mots de passe ou des informations financières. Les e-mails de phishing, les faux sites Web et les appels téléphoniques frauduleux sont autant de moyens utilisés pour tromper les utilisateurs et obtenir leur confiance. Les attaques de phishing sont particulièrement dangereuses car elles exploitent la faiblesse humaine et contournent souvent les mesures de sécurité technologiques.

Les utilisateurs doivent être informés des risques liés aux comportements négligents, des techniques utilisées dans les attaques de phishing et des précautions à prendre pour prévenir les infections. De plus, les politiques de sécurité des entreprises doivent intégrer des mesures visant à minimiser les erreurs humaines, telles que la mise en place d'exigences de mots de passe complexes, la restriction des privilèges d'accès aux données.

III.5.4 Les failles physiques

Alors que la sécurité des réseaux informatiques est souvent associée aux mesures de protection numériques, il est important de noter que les attaques physiques peuvent également compromettre gravement la sécurité d'un système. Les failles physiques font référence à toutes les vulnérabilités qui peuvent être exploitées physiquement, que ce soit par des intrus malveillants ou par des accidents involontaires. Il est essentiel de comprendre ces failles et d'adopter des mesures appropriées pour les prévenir et les contrôler afin de garantir la sécurité globale du réseau informatique.

Les failles physiques peuvent prendre différentes formes et être causées par divers facteurs. L'une des failles physiques les plus courantes est l'accès physique non autorisé aux composants du réseau. Cela peut inclure des intrusions dans les locaux où les serveurs et les équipements réseau sont hébergés, permettant ainsi un accès direct aux systèmes. Les attaquants peuvent profiter de l'absence de mesures de sécurité physiques adéquates, telles que des systèmes de verrouillage et de surveillance ou des contrôles d'accès, pour pénétrer dans les installations et accéder aux infrastructures du réseau.

Les infrastructures des centres de données, où sont hébergés les serveurs et les systèmes de stockage qui constituent le réseau informatique, sont également susceptibles de présenter des failles physiques. Un accès physique non autorisé à ces centres de données peut permettre à un attaquant de manipuler directement les serveurs ou les systèmes de stockage, de voler des informations ou de les endommager intentionnellement. Il est donc essentiel de mettre en place des mesures de sécurité physiques, telles que des systèmes de surveillance vidéo, des contrôles d'accès et des politiques strictes pour l'accès aux infrastructures sensibles.

III.5.5 Les failles de configuration

Une fail de configuration se produit lorsqu'une configuration du réseau ou d'un système est incorrecte, incomplète ou non sécurisée, ce qui permet à des attaquants de compromettre l'intégrité, la confidentialité ou la disponibilité des données. Il est essentiel de comprendre les différentes failles de

configuration afin de les prévenir, de les détecter et de les corriger pour garantir un niveau de sécurité optimal des réseaux informatiques.

Les failles de configuration peuvent se produire à différents niveaux, tels que la configuration des équipements réseau (routeurs, switches), des serveurs, des pares-feux, des services ou des applications. Une mauvaise configuration des équipements réseau peut permettre aux attaquants d'accéder à des portes dérobées, de détourner le trafic, de masquer leur présence ou d'intercepter des données en transit. Les pares-feux, s'ils sont mal configurés, peuvent laisser passer des paquets indésirables ou bloquer des connexions légitimes. Enfin, les failles de configuration des services ou des applications peuvent permettre des attaques par injection de code, des fuites d'informations sensibles ou des erreurs de contrôle d'accès.

Plusieurs types de failles de configuration peuvent être identifiés et qui peuvent être liées à des erreurs humaines ou à un manque de connaissances Tout d'abord, les configurations par défaut ou les configurations non sécurisées sont courantes. Les administrateurs réseau peuvent négliger de changer les mots de passe par défaut, de désactiver les services inutiles ou de limiter les accès aux ressources. Les attaquants peuvent ainsi profiter de ces configurations par défaut pour accéder facilement aux systèmes et aux données sensibles.
Les failles de configuration peuvent résulter de l'utilisation de protocoles de communication non sécurisés ou obsolètes qui peut exposer le trafic réseau à des attaques de type "interception" ou "replay". Il est essentiel de mettre en œuvre des protocoles de communication sécurisés et de maintenir les équipements et les logiciels à jour pour prévenir ce type de faille de configuration.

Les failles de configuration peuvent avoir de graves conséquences sur la sécurité des réseaux informatiques, telles que la fuite d'informations sensibles, la perte de données, les attaques de déni de service ou le compromis des systèmes. Il est donc essentiel de mettre en place des politiques et des procédures de sécurité solides pour prévenir, détecter et corriger les failles de configuration. Cela inclut l'établissement de bonnes pratiques de configuration, la mise en œuvre de technologies de détection des failles, l'utilisation de scans de sécurité réguliers et l'éducation des utilisateurs finaux sur les bonnes pratiques en matière de sécurité informatique.

III.5.6 Les failles matérielles

Ces failles se réfèrent aux points faibles et aux défauts dans l'infrastructure matérielle des systèmes informatiques, tels que les serveurs, les ordinateurs, les routeurs, les commutateurs, les câbles et autres composants physiques. Les failles matérielles peuvent être exploitées par des attaquants pour compromettre la sécurité des réseaux, accéder à des données sensibles, perturber les services et causer des dommages importants. Comprendre les différents types et les causes des failles matérielles est essentiel pour renforcer la sécurité des réseaux informatiques.

Il existe plusieurs types de failles matérielles couramment rencontrées dans les réseaux informatiques. L'une des plus fréquentes est la défaillance matérielle, qui peut être causée par des erreurs de conception, des problèmes de fabrication ou une utilisation prolongée. Les pannes matérielles, telles que les défaillances des disques durs, des cartes réseau ou des systèmes de refroidissement, peuvent entraîner des interruptions de service ou des pertes de données ou des comportements inattendus des dispositifs, tandis qu'un routeur défaillant peut provoquer des pannes du réseau.

Par ailleurs, les failles matérielles peuvent également être le résultat de problèmes de gestion des actifs informatiques. Souvent, les organisations ne suivent pas correctement leurs actifs matériels, ce qui peut entraîner des appareils obsolètes, non patchés ou non mis à jour. Ces dispositifs obsolètes peuvent contenir des vulnérabilités connues qui peuvent être exploitées par des attaquants pour compromettre la sécurité des réseaux.

En investissant dans la sécurité matérielle, les organisations peuvent mieux protéger leurs réseaux contre les attaques et assurer l'intégrité et la confidentialité de leurs informations sensibles. [7]

III.6 Mécanisme de sécurité réseau

III.6.1 Equipement : Les pare-feu (firewalls)

Figure III.43: Exemple de matériel pare-feu [40]

III.6.1.1 Description

Les pares-feux, également connus sous le nom de firewalls, sont des éléments essentiels pour assurer la sécurité des réseaux informatiques. Ils agissent comme une barrière de protection entre le réseau interne et les menaces provenant de l'extérieur. Les pares-feux jouent un rôle crucial dans le filtrage du trafic réseau, la prévention des intrusions et la surveillance des activités suspectes. Dans cette sous partie, nous nous concentrerons sur la description des pares-feux ainsi que sur les différents types de pare-feu utilisés dans les réseaux informatiques.

Figure 44: protection pare-feu [41]

Les pares-feux sont des dispositifs matériels ou logiciels qui examinent et filtrent le trafic réseau en fonction de règles prédéfinies. Leur objectif principal est de contrôler les flux de données entrants et sortants, en autorisant uniquement les connexions valides et sécurisées. Les pares-feux fonctionnent

en analysant les en-têtes de paquets, qui contiennent des informations telles que l'adresse IP source et de destination, le port de communication, le protocole utilisé, etc. Grâce à cette analyse, les pares-feux peuvent prendre des décisions quant à l'acceptation ou au rejet des paquets.

III.6.1.2 types de pare-feu

Il existe plusieurs types de pare-feu, chacun offrant des fonctionnalités et des avantages spécifiques pour la sécurité du réseau.

- **Le pare-feu stateful ou pare-feu d'État**

Est l'un des types les plus couramment utilisés. Ce pare-feu analyse non seulement les en-têtes de paquets, mais maintient également un suivi de l'état de chaque connexion réseau établie. Ainsi, il peut autoriser les paquets entrants qui appartiennent à une connexion déjà établie et bloquer les tentatives de connexion non autorisées. Ce type de pare-feu est efficace pour protéger contre les attaques par déni de service (DoS) et les tentatives d'usurpation d'identité.

- **Le pare-feu de niveau application**

Un autre type de pare-feu largement utilisé, contrairement au pare-feu stateful, qui se concentre principalement sur les informations de niveau réseau, le pare-feu de niveau application inspecte les données à un niveau plus profond, jusqu'aux informations de la couche application du modèle OSI. Cela permet de détecter et de bloquer les attaques spécifiques aux applications, telles que les injections SQL ou les attaques de contournement d'authentification. Les pares-feux de niveau application sont particulièrement importants pour protéger les serveurs d'applications et les sites web contre les vulnérabilités connues.

En plus de ces types classiques de pare-feu, il existe également des solutions de pare-feu de nouvelle génération (NGFW) qui combinent les fonctionnalités de filtrage de paquets traditionnelles avec des capacités plus avancées, telles que l'inspection SSL/TLS, la prévention des intrusions (IPS), la détection des logiciels malveillants et la sécurité avancée des applications. Les NGFW sont conçus pour offrir une protection plus complète et adaptée aux besoins des réseaux d'aujourd'hui, qui sont de plus en plus complexes et exposés à des attaques sophistiquées.

III.6.1.3 Principe de fonctionnement

Les pares-feux jouent un rôle crucial dans le maintien de l'intégrité, de la confidentialité et de la disponibilité des informations en contrôlant le trafic réseau entrant et sortant. Le principe de fonctionnement des pares-feux repose sur plusieurs aspects clés : la politique de sécurité, les règles de filtrage, les zones de confiance et les techniques d'inspection du trafic.

La politique de sécurité est l'ensemble des règles et des procédures qui définissent les objectifs de sécurité d'un réseau et les mesures mises en place pour les atteindre. Elle peut inclure des politiques de contrôle d'accès, de confidentialité des données et de gestion des vulnérabilités. La politique de sécurité est le fondement même de la configuration des pares-feux, car elle détermine les règles qui régissent le filtrage du trafic réseau.

Les règles de filtrage sont les instructions spécifiques qui dictent le comportement d'un pare-feu lorsqu'il traite les paquets de données qui traversent le réseau. Elles peuvent être basées sur différents critères, tels que les adresses IP, les ports de communication, les protocoles de réseau ou même le contenu des paquets. Les règles peuvent être configurées pour autoriser, bloquer ou rediriger le trafic en fonction des critères spécifiés. Par exemple, une règle peut être mise en place pour autoriser uniquement le trafic HTTP provenant des adresses IP approuvées.

Les pares-feux peuvent également diviser le réseau en différentes zones de confiance, également appelées segments de réseau. Chaque zone de confiance correspond à un niveau de fiabilité et de sécurité différent. Par exemple, une entreprise peut avoir une zone de confiance interne pour les employés et une zone de confiance externe pour les invités. Les pares-feux peuvent être configurés pour réguler strictement le trafic entre ces zones, en s'assurant que seuls les flux de données autorisés peuvent passer d'une zone à l'autre.

Pour inspecter le trafic réseau, les pares-feux utilisent différentes techniques, telles que l'inspection de paquets, l'inspection d'état et l'inspection d'application. L'inspection de paquets consiste à analyser les en-têtes des paquets de données pour vérifier qu'ils sont conformes aux règles de filtrage. L'inspection d'état examine l'état des connexions réseau, en vérifiant si une communication a été établie de manière légitime et en autorisant uniquement les paquets pertinents pour cette connexion. L'inspection d'application est utilisée pour analyser le contenu des paquets, en recherchant des signatures d'attaques connues ou en détectant des anomalies dans les comportements du trafic.

L'ensemble de ces éléments permet aux pares-feux de fonctionner de manière cohérente et efficace pour protéger les réseaux informatiques. Les politiques de sécurité définies guident les décisions de filtrage, en s'assurant que seuls les flux de données autorisés peuvent traverser le pare-feu. Les règles de filtrage spécifiques régulent le trafic réseau, en autorisant, bloquant ou redirigeant les paquets en fonction des critères définis. Les zones de confiance et les techniques d'inspection du trafic ajoutent des couches de sécurité supplémentaires, en limitant l'accès aux différentes parties du réseau et en détectant les anomalies potentielles. [7]

III.6.2 Les systèmes de détection et prévention d'intrusion IDS et IPS

Les systèmes de détection et prévention d'intrusion, plus communément appelés IDS et IPS, jouent un rôle essentiel dans la sécurité des réseaux informatiques. Ces outils sont conçus pour identifier et atténuer les menaces et les incidents de sécurité en surveillant en permanence le trafic réseau et en détectant les comportements suspects ou malveillants.

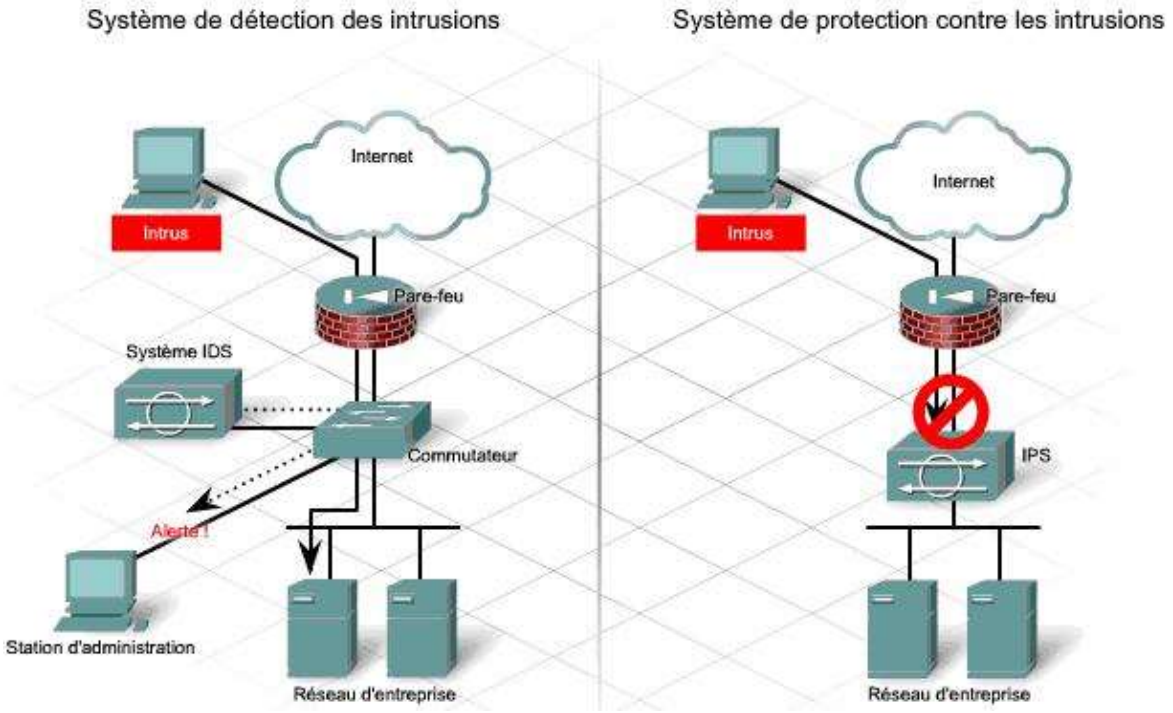


Figure III.45: l'IDS et l'IPS [42]

III.6.2.1 Principes de fonctionnement de l'IDS

Les principes de fonctionnement des IDS sont basés sur plusieurs concepts clés qui permettent leur efficacité et leur adaptabilité dans un environnement en constante évolution.

Tout d'abord, les IDS se basent sur la collecte de données et l'analyse du trafic réseau pour détecter les intrusions. Ils surveillent le flux de données en temps réel, en analysant les paquets entrants et sortants à la recherche de schémas ou d'anomalies qui pourraient indiquer une activité malveillante. Cette analyse peut être réalisée à différents niveaux, tels que la couche réseau, la couche transport ou la couche application, afin de détecter une variété d'attaques.

Ensuite, les IDS utilisent des bases de données de signatures pour identifier les modèles d'attaques connues. Ces signatures, également appelées règles, sont des modèles de comportement ou de code malveillant déjà identifiés. Lorsque le système de détection repère une correspondance entre le trafic en cours d'analyse et une signature connue, il déclenche une alerte pour indiquer une possible intrusion. Cependant, les IDS ne se limitent pas uniquement à la détection d'attaques connues, ils peuvent également utiliser des méthodes d'apprentissage automatique pour identifier les anomalies dans le trafic réseau, permettant ainsi la détection d'attaques inconnues.

Les IDS peuvent être déployés selon deux principales architectures : l'IDS centralisé et l'IDS distribué. Dans une architecture centralisée, toutes les données du réseau sont collectées et analysées à partir d'un point central. Cette approche permet une gestion plus centralisée et une analyse approfondie, mais peut également entraîner un goulot d'étranglement du flux de données et une vulnérabilité en cas de défaillance du point central. Dans une architecture distribuée, les capteurs de détection sont répartis sur différents points du réseau, ce qui permet une surveillance plus étendue et une résilience accrue en cas de problèmes au niveau d'un ou plusieurs capteurs.

Enfin, les IDS nécessitent une maintenance régulière pour rester efficaces dans un environnement en constante évolution. Les bases de données de signatures doivent être mises à jour régulièrement pour inclure les dernières menaces connues. De plus, les règles de détection peuvent nécessiter des ajustements pour s'adapter aux spécificités du réseau et aux nouveaux types d'attaques émergents.

III.6.2.2 Principes de fonctionnement de l'IPS

L'IPS, ou système de prévention d'intrusion, est une évolution de l'IDS qui a des fonctionnalités supplémentaires pour détecter, bloquer et prévenir les attaques dans les réseaux. Les principes de fonctionnement de l'IPS reposent sur des mécanismes avancés de surveillance, d'analyse du trafic et de prise de décision automatisée pour garantir la sécurité des données et des systèmes.

L'un des principes de fonctionnement de l'IPS est l'inspection en profondeur du contenu du trafic réseau. L'IPS analyse le flux de données qui traverse le réseau pour identifier les activités suspectes ou malveillantes. Il examine les paquets de données en temps réel pour détecter les signatures d'attaques connues, les comportements anormaux, les tentatives de contournement ou les vulnérabilités exploitables. L'inspection en profondeur permet à l'IPS d'identifier et de bloquer rapidement les menaces, en réagissant de manière proactive pour protéger le réseau et les systèmes contre les attaques.

Un autre principe clé de l'IPS est la mise en œuvre de règles et de politiques de sécurité. Les IPS sont configurés pour appliquer des politiques de sécurité spécifiques aux réseaux ou aux systèmes protégés. Ces politiques comprennent des règles de filtrage qui déterminent l'autorisation ou le blocage du trafic en fonction de critères prédéfinis tels que les adresses IP source et destination, les ports de service, les protocoles, les signatures d'attaque, etc. Les règles peuvent être définies de manière granulaire, permettant ainsi de personnaliser les niveaux de sécurité et de contrôle en fonction des besoins spécifiques du réseau.

L'utilisation de modèles comportementaux est également un principe fondamental de l'IPS. Les IPS sont conçus pour apprendre et comprendre les modèles de trafic normaux dans le réseau, afin de détecter les anomalies ou les activités suspectes. En analysant les schémas de trafic, les IPS peuvent repérer les comportements aberrants tels que les tentatives d'intrusion, les attaques de déni de service, les scans de ports ou les activités malveillantes. Ces modèles comportementaux permettent à l'IPS de distinguer les activités légitimes des activités nuisibles, en fournissant une défense proactive contre les nouvelles menaces et les techniques d'évasion.

Un autre aspect important du fonctionnement de l'IPS est la réaction automatisée aux menaces détectées. L'IPS est capable de prendre des mesures immédiates pour bloquer le trafic malveillant ou déclencher des alarmes pour alerter les administrateurs du réseau. Cela peut inclure le blocage d'adresses IP, la mise en quarantaine de systèmes infectés, l'arrêt de connexions suspectes ou la génération de rapports détaillés sur les événements de sécurité. La réaction automatisée permet de garantir une réponse rapide et efficace aux attaques, minimisant ainsi les dommages et réduisant les délais de récupération.

III.6.3 La gestion des identités et des accès

III.6.3.1 La gestion des droits d'accès avec (RBAC)

La gestion des droits d'accès (RBAC) est un élément essentiel de la sécurité des réseaux informatiques. RBAC, ou Role-Based Access Control (contrôle d'accès basé sur les rôles), est une méthode qui permet de contrôler les autorisations d'accès aux ressources informatiques en fonction des rôles que les utilisateurs occupent au sein de l'organisation. Avec RBAC, les droits d'accès sont attribués aux rôles plutôt qu'aux individus, ce qui facilite la gestion des autorisations et réduit les risques de mauvaise gestion des accès.

Dans le cadre de la gestion des droits d'accès avec RBAC, plusieurs éléments clés peuvent être identifiés. Tout d'abord, la définition des rôles est un aspect essentiel. Les rôles représentent les différents niveaux d'autorisation au sein d'une organisation et sont définis en fonction des responsabilités et des tâches spécifiques. Par exemple, un rôle peut être créé pour les administrateurs système, un autre pour les utilisateurs finaux et un autre encore pour les responsables de la sécurité. Chaque rôle est associé à un ensemble de droits d'accès prédéfinis, qui déterminent les actions que les utilisateurs peuvent effectuer sur les ressources du réseau.

La gestion des droits d'accès avec RBAC comprend également la délégation des autorisations. Grâce au RBAC, les administrateurs peuvent déléguer des droits d'accès spécifiques à certains utilisateurs en leur attribuant des rôles supplémentaires. Cela permet de répartir la responsabilité de la gestion des accès entre différents acteurs tout en maintenant un niveau élevé de contrôle. Par exemple, un responsable de projet peut se voir attribuer des droits spécifiques pour gérer les ressources liées à son projet, sans pour autant avoir un accès complet aux ressources de l'organisation.
Enfin, le RBAC nécessite également une approche de suivi et de gestion des droits d'accès. Il est important de disposer d'outils et de mécanismes de surveillance pour évaluer et ajuster les droits d'accès des utilisateurs au fil du temps. Cela peut être réalisé en effectuant régulièrement des audits de sécurité, en examinant les autorisations actuelles, en vérifiant leur pertinence et en procédant aux ajustements nécessaires.

La gestion des droits d'accès avec RBAC présente de nombreux avantages. Tout d'abord, elle permet une gestion plus efficace et simplifiée des autorisations d'accès en se basant sur des rôles prédéfinis plutôt que sur des autorisations individuelles. Cela réduit les risques d'erreurs humaines et facilite les processus de création, de modification et de suppression des utilisateurs. De plus, le RBAC offre une plus grande granularité de contrôle, car il permet d'attribuer des droits d'accès spécifiques en fonction des rôles. Il s'agit donc d'un système plus flexible et évolutif pour gérer les droits d'accès dans les réseaux informatiques.

III.6.3.2 Les systèmes de gestion d'authentification (SSO)

Les systèmes de gestion d'authentification, connus sous le terme de Single Sign-On (SSO), sont outils essentiels dans la gestion des identités et des accès dans les réseaux informatiques. Ils permettent aux utilisateurs de s'authentifier une seule fois pour accéder à plusieurs applications et ressources, sans avoir à saisir à chaque fois leurs identifiants. Les systèmes de SSO offrent ainsi plus de commodité pour les utilisateurs tout en renforçant la sécurité des réseaux informatiques.

Le fonctionnement des systèmes de gestion d'authentification repose sur des protocoles d'authentification fiables et sécurisés, tels que SAML (Security Assertion Markup Language) ou OAuth (Open Authorization). Ces protocoles permettent d'établir une relation de confiance entre l'utilisateur, l'application et le fournisseur de services d'authentification, en utilisant des échanges de jetons d'authentification. L'utilisateur s'authentifie une seule fois auprès du fournisseur de services d'authentification, qui génère un jeton autonome, valide pour une durée déterminée. Ce jeton est ensuite utilisé pour accéder aux applications et ressources autorisées, sans avoir à fournir à nouveau les identifiants.

Les systèmes de gestion d'authentification SSO offrent plusieurs avantages. Tout d'abord, ils améliorent l'expérience utilisateur en permettant un accès transparent aux différentes applications. Les utilisateurs n'ont plus besoin de retenir de multiples identifiants et de les saisir à chaque fois qu'ils veulent accéder à une application spécifique. Cela réduit la charge cognitive et facilite l'utilisation des ressources informatiques.

De plus, les systèmes de SSO renforcent la sécurité des réseaux informatiques en réduisant les risques associés aux mots de passe faibles ou réutilisés. En utilisant un seul identifiant fort pour accéder à diverses applications, les utilisateurs sont plus enclins à choisir des mots de passe complexes et à les mettre à jour régulièrement. Les systèmes de SSO peuvent également mettre en place des mécanismes de contrôle d'accès plus avancés, tels que la vérification en deux étapes, pour renforcer davantage la sécurité.

Un autre avantage des systèmes de gestion d'authentification SSO réside dans leur capacité à faciliter la gestion des droits d'accès. En centralisant les autorisations et les rôles d'utilisateur au niveau du fournisseur de services d'authentification, les administrateurs peuvent plus facilement gérer les droits d'accès des utilisateurs à différentes applications et ressources. Cela permet de simplifier les processus de provisionnement et de provisionnement des utilisateurs, et d'améliorer la conformité aux politiques de sécurité et de confidentialité.

Bien que les systèmes de gestion d'authentification SSO offrent de nombreux avantages, ils ne sont pas sans limites. Par exemple, en utilisant un identifiant unique pour accéder à différentes applications, si cet identifiant est compromis, toutes les applications associées peuvent être exposées à des risques de sécurité. Il est donc essentiel de mettre en place des mesures de protection robustes pour sécuriser l'authentification, telles que l'utilisation de certificats numériques ou de solutions de gestion des identités et des accès avancés.

III.6.4 Rôle de l'Active Directory dans la sécurité (AD)

L'Active Directory, également connu sous le sigle AD, est un service de gestion des identités et des accès développés par Microsoft pour les environnements Windows. Il joue un rôle essentiel dans la sécurité des réseaux informatiques, offrant un contrôle centralisé sur les utilisateurs, les groupes, les ressources et les politiques de sécurité. L'Active Directory permet une gestion sécurisée des identités, une authentification et une autorisation précises, ainsi que des fonctionnalités avancées de gestion des certificats. Son utilisation généralisée en entreprise en fait une composante clé de la stratégie de sécurité informatique.

L'Active Directory offre plusieurs fonctionnalités qui renforcent la sécurité des réseaux informatiques. Tout d'abord, il permet la gestion centralisée des identités, ce qui facilite la création, la gestion et la suppression des comptes utilisateurs. Grâce à l'Active Directory, les administrateurs peuvent attribuer des rôles, des privilèges et des droits d'accès spécifiques à chaque utilisateur, en fonction de ses besoins et de ses responsabilités. Cela permet de garantir que seules les personnes autorisées aient accès aux ressources sensibles, réduisant ainsi les risques d'accès non autorisés ou d'utilisations malveillantes.

En outre, l'Active Directory offre des fonctionnalités avancées de gestion des politiques de sécurité. Les administrateurs peuvent mettre en place des politiques de mots de passe complexes, imposer des exigences de verrouillage de compte et de réinitialisation de mot de passe régulière, et définir des règles de sécurité pour les ressources du réseau. Ces mesures renforcent la sécurité des identités et des accès en obligeant les utilisateurs à respecter des normes de sécurité strictes et en limitant les risques liés à l'utilisation de mots de passe faibles ou compromis.

Un autre avantage de l'Active Directory est sa compatibilité avec les certificats numériques. Grâce à son intégration avec des services de gestion des certificats, il facilite la gestion et le déploiement des certificats pour l'authentification forte, le chiffrement des communications et la signature numérique. L'utilisation de certificats numériques renforce la sécurité des échanges de données sensibles en garantissant l'authentification des utilisateurs et en assurant l'intégrité des informations échangées.

L'Active Directory est également équipé de fonctionnalités de suivi et d'audit, qui permettent de surveiller l'activité des utilisateurs et de détecter les comportements suspects ou les tentatives d'accès non autorisées. Les journaux d'audit stockent les informations relatives aux connexions, aux modifications d'autorisations et aux tentatives d'accès infructueuses, offrant aux administrateurs une visibilité sur les activités de sécurité du réseau. Cela permet de réagir rapidement en cas d'incident de sécurité et de prendre les mesures nécessaires pour protéger les ressources informatiques.

En conclusion, l'Active Directory joue un rôle crucial dans la sécurité des réseaux informatiques grâce à ses fonctionnalités de gestion des identités et des accès. En fournissant un contrôle centralisé sur les utilisateurs, les groupes, les ressources et les politiques de sécurité, il permet une gestion sécurisée des identités, une authentification précise, une autorisation granulaire et des fonctionnalités avancées de gestion des certificats. En combinant ces fonctionnalités, l'Active Directory renforce la sécurité des réseaux informatiques en limitant les risques d'accès non autorisés, en imposant des normes de sécurité strictes et en facilitant la surveillance et la réponse aux incidents de sécurité.

III.7 les protocoles de sécurité

III.7.1 Les protocoles HTTP et HTTPS

Les protocoles HTTP (Hypertext Transfer Protocol) et HTTPS (HTTP Secure) sont largement utilisés pour la communication et l'échange d'informations sur les réseaux informatiques. Ils permettent aux utilisateurs d'accéder et de visualiser des sites Web, et jouent un rôle essentiel dans la transmission des données sur Internet.

III.7.1.1 Principes de fonctionnement

Pour assurer la sécurité de ces protocoles, certains principes de fonctionnement sont mis en place. Tout d'abord, le protocole HTTP est un protocole qui fonctionne sur la couche application du modèle OSI (Open Systems Interconnection). Il définit les règles et les procédures pour l'échange de données entre un client (par exemple, un navigateur web) et un serveur. Ce protocole est basé sur un modèle de requête-réponse, où le client envoie une demande (requête) au serveur, qui renvoie ensuite une réponse. Cependant, le principal inconvénient du protocole HTTP est que les données sont transmises en clair, c'est-à-dire sans chiffrement, ce qui les rend vulnérables à l'interception et à la manipulation par des attaquants. Pour remédier à cette vulnérabilité, le protocole HTTPS est introduit.

Parmi les principaux principes de fonctionnement du protocole HTTPS, on retrouve l'utilisation des certificats SSL/TLS, des techniques de chiffrement pour sécuriser les données échangées entre le client et le serveur qu'il prétend être. Le chiffrement asymétrique est utilisé pour établir une clé de session partagée entre le client et le serveur, Une fois que la clé de session est établie, les données sont chiffrées à l'aide de cette clé avant d'être envoyées sur le réseau, Cette clé de session est générée de manière aléatoire pour chaque connexion, ce qui améliore la sécurité du protocole.

En mettant en place ces principes de fonctionnement, le protocole HTTPS garantit une sécurité accrue lors de la transmission des données sur Internet. Il permet de protéger la confidentialité des échanges, de garantir l'authenticité des serveurs et de prévenir les attaques de type man-in-the-middle. En utilisant des certificats SSL/TLS, des mécanismes de chiffrement solides et des techniques d'intégrité des données, le protocole HTTPS assure une communication sécurisée entre les clients et les serveurs.

III.7.2 Les certificats SSL/TLS

Les certificats SSL/TLS qui veut dire (Secure Sockets Layer/Transport Layer Security) sont des outils essentiels pour sécuriser les protocoles HTTP et HTTPS utilisés dans les réseaux informatiques. Un certificat SSL/TLS est une clé électronique qui permet d'établir une connexion sécurisée entre un serveur web et un navigateur. Il garantit que les données échangées entre les deux parties sont chiffrées et donc protégées contre les interceptions et les utilisations malveillantes. Les certificats SSL/TLS jouent un rôle crucial dans la protection de la confidentialité et de l'intégrité des données transmises sur les réseaux informatiques.

Le processus de mise en place d'un certificat SSL/TLS comprend plusieurs étapes. Tout d'abord, l'administrateur du serveur web génère une paire de clés asymétriques composée d'une clé privée et d'une clé publique. La clé privée est gardée secrète et utilisée pour chiffrer et déchiffrer les données, tandis que la clé publique est partagée avec les utilisateurs du service. Ensuite, un organisme de certification vérifie l'identité du propriétaire du certificat et signe numériquement la clé publique avec sa propre clé privée. Cette signature garantit l'authenticité et l'intégrité du certificat.

Lorsqu'un utilisateur accède à un site web sécurisé, un processus de poignée de main SSL/TLS est initié. Le navigateur du client demande au serveur de lui prouver son identité en lui envoyant son certificat SSL/TLS signé. Le navigateur du client vérifie alors la légitimité du certificat en vérifiant la signature avec la clé publique de l'organisme de certification. Si la vérification est réussie, le navigateur du client envoie une clé de session au serveur, qui l'utilise pour chiffrer les données échangées entre les deux parties.

Les certificats SSL/TLS offrent plusieurs avantages en termes de sécurité des réseaux informatiques. Tout d'abord, ils garantissent la confidentialité des données en chiffrant les informations sensibles qui sont transmises sur les réseaux. Cela signifie que même si un tiers intercepte les données, il ne pourra pas les lire sans la clé de déchiffrement appropriée. De plus, les certificats SSL/TLS assurent l'intégrité des données. Grâce à la signature numérique, il est possible de vérifier que les données n'ont pas été modifiées lors de leur transmission. Enfin, les certificats SSL/TLS permettent d'authentifier l'identité du serveur web, offrant ainsi une protection contre les attaques de type "man-in-the-middle".

Pour garantir la sécurité des réseaux informatiques, il est important de prendre en compte certains aspects liés aux certificats SSL/TLS. Tout d'abord, il est important de s'assurer de la validité du certificat en vérifiant sa date d'expiration et l'entité qui l'a émis. Ensuite, il est recommandé de choisir des certificats émis par des organismes de certification fiables, qui utilisent des pratiques de vérification rigoureuses. De plus, il est essentiel de mettre à jour régulièrement les certificats afin de toujours bénéficier des dernières mesures de sécurité. [8]

III.7.3 Sécurité des protocoles de connexion à distance

III.7.3.1 Le protocole SSH

Le protocole SSH (Secure Shell) est un protocole de communication sécurisé utilisé pour établir une connexion cryptée entre un client et un serveur distant. Il assure la confidentialité et l'intégrité des données échangées, ainsi que l'authentification des utilisateurs. Le protocole SSH est largement utilisé dans le domaine de la sécurité des réseaux informatiques pour sécuriser les connexions à distance et les transferts de fichiers.

Le protocole SSH fonctionne en utilisant une paire de clés, une clé privée et une clé publique. La clé publique est stockée sur le serveur distant, tandis que la clé privée est conservée par l'utilisateur. Lorsque l'utilisateur souhaite se connecter au serveur distant, il utilise sa clé privée pour prouver son identité. Le serveur distant vérifie ensuite cette identité en utilisant la clé publique correspondante.

La sécurisation des connexions à distance est essentielle pour protéger les données sensibles échangées entre les clients et les serveurs. Sans un protocole de sécurité comme SSH, les connexions à distance sont exposées à des risques de sniffing, d'interception et de modifications non autorisées des données. Le protocole SSH utilise des techniques de chiffrement et de mutualisation de clés pour garantir que les données transmises sur le réseau sont protégées contre les attaques.

En utilisant le protocole SSH, les administrateurs système peuvent administrer à distance leurs serveurs sans compromettre la sécurité des informations sensibles, telles que les mots de passe et les données confidentielles. Les connexions SSH peuvent également être utilisées pour exécuter des commandes à distance, transférer des fichiers de manière sécurisée et configurer des tunnels VPN pour sécuriser les communications entre des réseaux distants.

L'un des avantages du protocole SSH est sa facilité à mettre en place. Il est livré avec la plupart des systèmes d'exploitation modernes et est largement pris en charge par les serveurs et les clients SSH.

De plus, l'utilisation des clés publiques et privées facilite l'authentification et élimine le besoin de saisir des mots de passe lors des connexions.

Cependant, malgré les nombreuses fonctionnalités de sécurité offertes par le protocole SSH, il n'est pas complètement exempt de vulnérabilités. Les attaques par force brute, les attaques par dictionnaire et les attaques par usurpation d'identité sont encore possibles si des mesures de sécurité supplémentaires ne sont pas mises en place. Les administrateurs doivent mettre en œuvre des politiques rigoureuses en matière de clés, de mots de passe, de verrouillage des connexions inactives et de journalisation pour garantir la sécurité des connexions SSH.

III.7.3.2 Les protocoles Telnet et VPN

Les protocoles Telnet et VPN jouent un rôle essentiel dans la sécurisation de connexions à distance au sein d'un réseau informatique.

Telnet est un protocole qui permet une connexion à distance non sécurisée, ce qui signifie que les données échangées via Telnet sont vulnérables aux interceptions et aux attaques par des tiers. Les informations sensibles telles que les noms d'utilisateur et les mots de passe sont transmises en clair, ce qui les rend facilement accessibles aux attaquants. En outre, Telnet ne supporte pas le chiffrement des données, ce qui expose les flux de données à des risques de manipulation ou de falsification.

Le VPN (Virtual Private Network, en revanche, offre une solution de sécurité plus avancée pour les connexions à distance. Un VPN crée un réseau virtuel privé en utilisant des protocoles de cryptage pour sécuriser les données transitant entre les points du réseau. Il permet aux utilisateurs d'accéder de manière sécurisée à des ressources situées dans un réseau privé à partir d'un emplacement distant. Le VPN utilise des techniques de chiffrement avancées pour rendre les données illisibles pour les tiers, assurant ainsi la confidentialité des informations échangées. Il offre également des mécanismes d'authentification et d'intégrité des données pour garantir l'identité des utilisateurs et la validité des données transmises.

Un VPN peut être mis en œuvre de différentes manières, que ce soit en utilisant des logiciels VPN sur les ordinateurs et les appareils mobiles, ou en configurant des routeurs VPN au niveau du réseau. Les VPN peuvent être utilisés pour sécuriser les connexions à distance des employés travaillant à distance, pour permettre l'accès sécurisé aux applications et aux ressources du réseau d'entreprise, ou pour connecter des réseaux distribués sur plusieurs sites géographiques.

L'utilisation d'un VPN présente plusieurs avantages en matière de sécurité des réseaux informatiques. Tout d'abord, le chiffrement des données garantit que seules les personnes autorisées peuvent accéder aux informations échangées, en rendant les données incompréhensibles pour les personnes non autorisées. Deuxièmement, l'authentification des utilisateurs permet de s'assurer de l'identité de chaque utilisateur qui tente de se connecter au réseau, renforçant ainsi la sécurité du système. Enfin, l'utilisation d'un VPN permet de garantir l'intégrité des données en s'assurant qu'elles n'ont pas été altérées ou modifiées au cours de la transmission. [7], [9]

III.8 Isolation des réseaux dans une DMZ

Une DMZ, ou Demilitarized Zone (zone démilitarisée), est un segment de réseau distinct qui est placé entre une organisation interne et Internet. Son objectif principal est de fournir une couche supplémentaire de sécurité en isolant les réseaux internes sensibles des menaces provenant d'Internet. Elle agit comme une barrière de sécurité supplémentaire en isolant les serveurs et les services accessibles depuis Internet du réseau interne. La création d'une DMZ repose sur un certain nombre de principes et d'architectures spécifiques qui garantissent son efficacité et sa fonctionnalité.

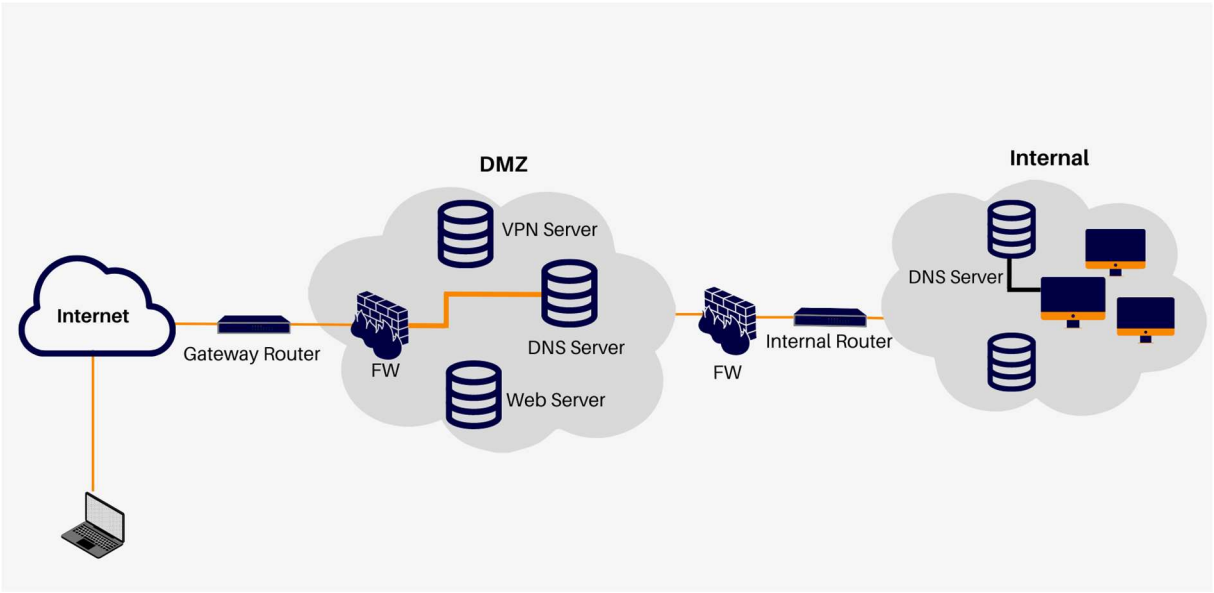


Figure III.46: la zone démilitarisée [43]

III.8.1 Architecture et principes de mise en place d'une DMZ :

L'architecture d'une DMZ est composée de plusieurs éléments clés. Le premier élément est le pare-feu, qui est utilisé pour protéger la DMZ et filtrer le trafic entre Internet et les réseaux internes. Le pare-feu est configuré avec des règles spécifiques qui déterminent quelles connexions sont autorisées ou bloquées. Il permet également de surveiller et de détecter les tentatives d'intrusion provenant de l'extérieur.

Un autre élément clé de l'architecture d'une DMZ est le serveur frontal, également appelé serveur hébergeant les services publics. Ce serveur est situé dans la DMZ et joue le rôle d'interface entre Internet et les réseaux internes. Il héberge des services qui sont destinés à être accessibles depuis Internet, tels que les sites web, les serveurs de messagerie ou les serveurs VPN. En étant situé dans la DMZ, le serveur frontal limite les risques d'exposition directe des réseaux internes aux attaques provenant d'Internet.

Un troisième élément important de l'architecture d'une DMZ est le serveur d'application, qui est également situé dans la DMZ mais uniquement accessible depuis les réseaux internes. Ce serveur héberge des applications internes qui nécessitent une interaction avec Internet, telles que les services cloud ou les applications mobiles. Le serveur d'application est protégé par le pare-feu de la DMZ et peut communiquer avec le serveur frontal pour établir des connexions avec Internet de manière sécurisée.

En complément de ces éléments, une DMZ peut également inclure un serveur de base de données, protégé et isolé du reste du réseau interne par des règles de pare-feu strictes. Les bases de données contiennent souvent des informations sensibles, telles que des données clients ou des données de l'entreprise, et leur protection est donc important pour éviter des fuites d'informations.

L'architecture d'une DMZ repose sur le principe de segmentation du réseau. En séparant les réseaux internes sensibles de la zone Internet non fiable, les risques de compromission des données sensibles sont réduits. Les connexions entre la DMZ et les réseaux internes sont strictement contrôlés et limités aux seules communications nécessaires pour le bon fonctionnement des services. De plus, l'utilisation de pares-feux, de règles de filtrage et de cryptage des données assure un niveau de sécurité supplémentaire.

III.8.2 Avantages et limites d'une DMZ

La mise en place d'une DMZ présente plusieurs avantages en termes de sécurité, mais comporte également certaines limites qu'il est important de prendre en compte.

Les avantages d'une DMZ sont nombreux. Premièrement, elle permet de protéger le réseau interne des attaques provenant d'Internet en isolant les serveurs exposés. En plaçant ces serveurs dans la DMZ, il est possible de restreindre les accès depuis Internet et d'appliquer des règles de sécurité strictes pour filtrer les connexions entrantes. Cette isolation réduit considérablement la surface d'attaque et limite les risques de compromission du réseau interne.

Deuxièmement, une DMZ permet de mieux contrôler les flux de données entre le réseau interne et Internet et donc contrôler de manière plus précise le trafic réseau, en utilisant des règles strictes de filtrage et de pare-feu pour autoriser ou bloquer les connexions.
Les règles de filtrage appliquées au niveau de la DMZ peuvent être plus restrictives pour les connexions entrantes, en limitant les ports et les services disponibles pour les utilisateurs externes. De plus, les connexions sortantes depuis la DMZ peuvent également être filtrées et surveillées de manière plus stricte, ce qui renforce la sécurité du réseau interne.

Troisièmement, la mise en place d'une DMZ facilite la gestion des services accessibles depuis Internet. Les serveurs exposés peuvent être regroupés dans une infrastructure spécifique, disposant d'une configuration et de paramètres de sécurité adaptés à leur rôle. Cela simplifie la gestion des accès, des correctifs de sécurité et des mises à jour des serveurs. De plus, en cas d'attaque ou de compromission d'un serveur dans la DMZ, l'impact sur le réseau interne est réduit, car les connexions entre la DMZ et le réseau interne sont limitées.

Cependant, malgré les avantages qu'elle offre, une DMZ présente également certaines limites. Premièrement, la configuration et la gestion d'une DMZ nécessitent des compétences en matière de sécurité informatique. Une mauvaise configuration de la DMZ peut entraîner des conséquences graves en termes de sécurité, en exposant le réseau interne à des risques non négligeables. Il est donc essentiel d'avoir des experts en sécurité pour mettre en place et maintenir une DMZ de manière efficace.

Deuxièmement, même si une DMZ permet de réduire la surface d'attaque, elle n'élimine pas complètement les risques de compromission des serveurs exposés. Les attaquants peuvent toujours tenter d'exploiter les vulnérabilités des serveurs dans la DMZ. Il est donc nécessaire de maintenir une vigilance constante et de mettre à jour régulièrement les serveurs de la DMZ avec les derniers correctifs de sécurité.

Enfin, la DMZ ne doit pas être considérée comme une solution unique pour tous les problèmes de sécurité. Elle doit être combinée à d'autres mesures de sécurité, telles que l'utilisation de pare-feu, d'antivirus et de systèmes de détection des intrusions, pour offrir une protection globale du réseau informatique.

III.9 Sécurité des équipements réseaux

La configuration sécurisée des routeurs et commutateurs est un aspect essentiel de la sécurité des réseaux informatiques. Les routeurs et les commutateurs sont des équipements clés dans l'infrastructure réseau, responsables du transfert et de la gestion du trafic entre les différents appareils connectés. Une configuration sécurisée permet de réduire les risques et les vulnérabilités associés à ces équipements, en garantissant que seules les communications autorisées sont permises et en protégeant le réseau contre les intrusions et les attaques.

III.9.1 Configuration sécurisée des routeurs et des commutateurs (ACL)

La configuration sécurisée des routeurs et des commutateurs comprend plusieurs mesures de sécurité, telles que la mise en place de mots de passe solides, la désactivation des services inutiles, la mise à jour régulière du firewire, l'utilisation de listes de contrôle d'accès (ACL) et la configuration de fonctionnalités de sécurité avancées telles que le VPN (Virtual Private Network).

La première étape pour configurer de manière sécurisée les routeurs et les commutateurs consiste à définir des mots de passe solides pour les interfaces d'administration. Ces mots de passe doivent être complexes et uniques, et il est préférable d'utiliser une combinaison de lettres, de chiffres et de caractères spéciaux. De plus, l'utilisation de la fonctionnalité de chiffrement des mots de passe est essentielle pour empêcher leur lecture en cas d'accès physique aux équipements.

Ensuite, il est important de désactiver tous les services inutiles qui sont activés par défaut sur les routeurs et les commutateurs. Les services tels que Telnet doivent être désactivés au profit de protocoles plus sécurisés tels que SSH (Secure Shell). De plus, les ports d'administration doivent être restreints aux adresses IP spécifiques des administrateurs afin de limiter l'accès aux équipements.

La mise à jour régulière du firewall est une autre mesure nécessaire pour la configuration sécurisée des routeurs et des commutateurs. Les fabricants publient régulièrement des correctifs de sécurité pour remédier aux vulnérabilités découvertes dans le firewall. Il est donc essentiel de maintenir à jour les équipements avec les dernières versions du firewall pour garantir une protection optimale contre les attaques.

- **Les listes de contrôle d'accès (ACL)**

Sont des mécanismes utilisés dans les réseaux informatiques pour contrôler et filtrer le trafic réseau, également utilisées pour définir des règles de filtrage configurées sur les équipements réseau, comme les routeurs, pour déterminer si les paquets de données doivent être acheminés ou rejetés ainsi permettant de contrôler le flux du trafic réseau. Les ACL permettent de spécifier quels types de communications sont autorisés ou refusés en fonction de critères tels que les adresses IP source et destination, les ports de protocole et les autres paramètres de niveau supérieur. Grâce aux ACL, il est possible de limiter l'accès aux services et aux ressources sensibles du réseau, renforçant ainsi la sécurité globale du système.

Enfin, la configuration de fonctionnalités de sécurité avancées telles que le VPN est une étape importante pour protéger les communications et les données sensibles circulant à travers les routeurs et les commutateurs. Les VPN permettent de créer des connexions sécurisées et chiffrées entre différents sites ou utilisateurs distants, garantissant ainsi la confidentialité et l'intégrité des données.

En adoptant une approche proactive et en appliquant ces bonnes pratiques, il est possible de renforcer la sécurité des infrastructures réseau et de prévenir les incidents de sécurité potentiellement coûteux et dommageables.

III.9.2 Exemples de commandes de configuration CISCO

CISCO est l'un des principaux fournisseurs d'équipements réseau et propose une gamme de commandes spécifiques pour configurer et gérer la sécurité des différents composants du réseau. Ces commandes permettent d'appliquer des politiques de sécurité, de contrôler les accès aux ressources réseau, de détecter et de prévenir les attaques, et bien plus encore.

Les commandes de configuration CISCO peuvent être utilisées pour plusieurs aspects de la sécurité des réseaux. Parmi ces aspects, on retrouve la sécurisation des accès, la mise en place de pare-feu, la sécurisation des protocoles, la détection d'intrusions et la gestion des journaux.

Pour sécuriser les accès, il est possible d'utiliser des commandes telles que "access-class" qui permettent de configurer les listes de contrôle d'accès (ACL) pour limiter les connexions entrantes à certains services ou adresses IP spécifiques. Il est également possible d'utiliser des commandes d'authentification comme "login authentication" pour renforcer l'authentification des utilisateurs et empêcher les accès non autorisés.

La mise en place de pare-feu est également un aspect important de la sécurité des réseaux. CISCO propose des commandes telles que "ip inspect" qui permettent de configurer le firewall intégré dans les équipements CISCO pour filtrer les paquets en fonction de critères prédéfinis. Ces commandes permettent de bloquer le trafic non désiré et de protéger les ressources réseau contre les attaques externes.

La sécurisation des protocoles est une autre préoccupation majeure en matière de sécurité des réseaux. Les commandes CISCO, telles que "crypto isakmp" ou "crypto ipsec", permettent de configurer des tunnels VPN (Virtual Private Network) pour sécuriser les communications à travers un réseau non

sécurisé, comme Internet. Ces commandes permettent de fournir une confidentialité et une intégrité des données, ainsi qu'une authentification des participants au réseau VPN.

La détection d'intrusions est un élément essentiel pour protéger les équipements réseaux contre les attaques. CISCO propose des commandes telles que "ip source-route" qui permettent de bloquer les paquets IP avec des adresses sources falsifiées, "ip unreachables" pour contrôler les messages ICMP (Internet Control Message Protocol) et "ip access-list logging interval" pour spécifier l'intervalle de journalisation des événements de correspondance dans les ACLs. Ces commandes permettent de détecter et de prévenir les tentatives d'intrusion et les attaques de déni de service (DDoS).

La gestion des journaux est également une composante essentielle de la sécurité des réseaux. Les commandes CISCO, telles que "logging buffered" qui spécifie le mode de journalisation en tampon, "logging host" pour configurer un serveur de journalisation distant, ou encore "show logging" pour afficher les journaux système, permettent de surveiller les activités du réseau, de détecter les incidents de sécurité et de mener des enquêtes en cas d'incident.

Ces commandes offrent des fonctionnalités avancées pour assurer la confidentialité, l'intégrité et la disponibilité du réseau. En comprenant et en maîtrisant ces commandes, les administrateurs réseau peuvent mettre en place des dispositifs de sécurité solides et efficaces, améliorant ainsi la résilience et la fiabilité des réseaux informatiques.

III.9.3 Les mécanismes de protection des réseaux sans fil

Les réseaux sans fil sont devenus omniprésents dans notre quotidien, que ce soit à la maison, au travail ou dans les lieux publics. Cependant, la sécurité des réseaux sans fil est une préoccupation majeure, car ces réseaux sont souvent vulnérables aux attaques et aux intrusions. Les mécanismes de protection des réseaux sans fil sont donc essentiels pour garantir la confidentialité, l'intégrité et la disponibilité des données échangées via ces réseaux.

Les mécanismes de protection des réseaux sans fil peuvent être regroupés en plusieurs catégories, notamment l'authentification et l'identification des utilisateurs, le chiffrement des données, le contrôle d'accès et la détection des intrusions.

L'authentification et l'identification des utilisateurs sont des mécanismes qui permettent de s'assurer de l'identité des personnes ou des appareils qui se connectent au réseau sans fil. L'utilisation de mots de passe, de certificats numériques ou de systèmes de reconnaissance biométrique sont autant de solutions permettant d'authentifier les utilisateurs et de prévenir les accès non autorisés.
Le chiffrement des données est également une composante essentielle de la sécurité des réseaux sans fil. Il permet de protéger les informations échangées contre les interceptions et les écoutes malveillantes. Les protocoles de chiffrement, tels que le WPA2 (Wi-Fi Protected Access 2) ou le WPA3, offrent des mécanismes de cryptage robustes pour sécuriser les données transitant sur le réseau. Le chiffrement des données est d'autant plus important lorsque des informations sensibles, telles que des données personnelles ou des transactions bancaires, sont échangées.

Le contrôle d'accès est un autre moyen de garantir la sécurité des réseaux sans fil en limitant l'accès aux seules personnes autorisées. Les pares-feux, les systèmes de détection d'intrusion (IDS) qui

permettent de surveiller en temps réel le trafic réseau, d'analyser les modèles de comportement et de détecter les activités suspectes. En cas de détection d'une intrusion ou d'une activité malveillante, ces systèmes peuvent déclencher des alertes et prendre des mesures pour arrêter l'intrusion et protéger le réseau.

Les systèmes de prévention des intrusions (IPS) sont utilisés pour détecter et bloquer les tentatives d'accès non autorisées ou les activités suspectes sur le réseau.

Ces mécanismes de contrôle d'accès peuvent être configurés pour bloquer automatiquement les adresses IP suspectes, les tentatives de connexion infructueuses ou les comportements anormaux.

En adoptant et en mettant en œuvre ces mécanismes de protection, les organisations peuvent réduire les risques de compromission de leurs réseaux sans fil et préserver la confiance de leurs utilisateurs dans leurs systèmes informatiques. [10]

III.10 Perspectives d'évolution de la sécurité des réseaux informatiques

III.10.1 Les objets connectés IoT

Les objets connectés IoT (Internet of objet) ont pris une de plus en plus importante dans notre quotidien. Ces dispositifs interconnectés, tels que les montres intelligentes, les thermostats connectés ou encore les capteurs de surveillance, offrent une multitude de fonctionnalités et de facilités d'utilisation. Cependant, leur utilisation massive et leur connexion aux réseaux informatiques posent des défis majeurs en matière de sécurité. Il est donc essentiel de comprendre les enjeux et les risques liés aux objets connectés IoT afin de garantir la sécurité des réseaux informatiques.

Figure III.47: IOT [44]

Les objets connectés IoT peuvent présenter différents risques en matière de sécurité. Tout d'abord, en raison de leur nombre croissant et de leur diversité, il devient difficile de gérer et de protéger tous ces dispositifs de manière adéquate. De plus, la plupart des objets connectés sont dotés de fonctionnalités de collecte et de traitement de données, ce qui peut entraîner des problèmes liés à la confidentialité et

à la protection des informations personnelles. En outre, la robustesse et la sûreté des objets connectés IoT varient considérablement, ce qui les rend plus vulnérables aux attaques et aux violations de sécurité.

Un autre défi majeur lié à la sécurité des objets connectés IoT est l'absence de normes et de protocoles de sécurité uniformes. Les objets connectés sont souvent développés par différents fabricants, utilisant diverses technologies et implémentant des mesures de sécurité différentes, voire inexistantes. Cette hétérogénéité rend le processus de sécurisation des réseaux informatiques complexe, avec des dispositifs pouvant être vulnérables à des attaques et des piratages.

Les objets connectés IoT sont également vulnérables aux attaques de type "botnet". Ces cyberattaques exploitent les failles de sécurité des objets connectés pour les infecter et les utiliser comme des "robots" pour lancer des attaques en masse. Les attaques par déni de service distribué (DDoS) peuvent ainsi être amplifiées et causer d'importants dommages aux infrastructures et réseaux informatiques.

III.10.2 La sécurisation des objets connectés

Avec la prolifération des objets connectés tels que les smartphones, les montres intelligentes, les thermostats ou même les réfrigérateurs connectés, de plus en plus de dispositifs sont susceptibles d'être vulnérables aux cyberattaques. La sécurisation de ces objets connectés est essentielle pour protéger la vie privée des utilisateurs, prévenir les intrusions malveillantes et garantir la stabilité des réseaux et pour atténuer les risques liés aux objets connectés IoT, plusieurs mesures peuvent être mises en place.
La sécurisation des objets connectés repose sur plusieurs éléments clés. Tout d'abord, il est essentiel de mettre en place des protocoles de communication sécurisés. Cela implique l'utilisation de méthodes d'authentification robustes, de cryptage des données et de mécanismes de gestion des clés. Les protocoles de communication sécurisés garantissent que seules les personnes autorisées peuvent se connecter aux objets connectés et interagir avec eux de manière sécurisée.

Ensuite, la sécurité physique des objets connectés est tout aussi importante. Il est essentiel d'empêcher l'accès physique non autorisé aux dispositifs connectés, car cela pourrait permettre à des attaquants de manipuler ou de compromettre leurs fonctionnalités. Des mesures telles que des procédures de contrôle d'accès, des dispositifs d'authentification physique et des protections anti-manipulation peuvent être mises en place pour renforcer la sécurité physique des objets connectés.

Un autre aspect clé de la sécurisation des objets connectés est la gestion des vulnérabilités. Comme tout autre système informatique, les objets connectés peuvent présenter des vulnérabilités qui pourraient être exploitées par des attaquants. Il est donc important de mettre en place des mécanismes de détection et de correction des vulnérabilités, tels que des mises à jour régulières du firewire, des audits de sécurité et des tests de pénétration. De plus, il est essentiel de mettre à jour régulièrement les logiciels et les micrologiciels des objets connectés afin de corriger les failles de sécurité connues. Une gestion efficace des vulnérabilités permet de garantir que les objets connectés restent protégés contre les dernières menaces.

Enfin, la sensibilisation et l'éducation, les utilisateurs doivent être conscients des risques liés à l'utilisation des objets connectés et être informés des bonnes pratiques de sécurité, comme la gestion

des mots de passe forts, la vérification des sources avant de télécharger des applications et la limitation des informations personnelles partagées avec les objets connectés. La sensibilisation et la formation permettent de réduire le risque d'erreurs humaines qui pourraient compromettre la sécurité des objets connectés.

La sécurisation des objets connectés contribue à renforcer l'ensemble de la sécurité des réseaux informatiques. En garantissant la sécurité des objets connectés, on garantit également la sécurité des données échangées entre ces objets et les serveurs auxquels ils sont connectés. De plus, la sécurisation des objets connectés offre une meilleure protection contre les attaques par déni de service distribué (DDoS) et entraînant une interruption des services. En sécurisant les objets connectés, on minimiserait le risque de compromettre la stabilité des réseaux dans leur ensemble.

III.10.3 Les enjeux et défis

Les enjeux et défis de sécurité des réseaux informatiques sont nombreux et complexes. Avec l'évolution technologique rapide et la multiplication des menaces cybernétiques, il est essentiel de comprendre les enjeux actuels et les défis auxquels sont confrontés les systèmes informatiques en matière de sécurité.

Les enjeux de la sécurité des réseaux informatiques se manifestent à différents niveaux. Tout d'abord, la protection des données et des informations sensibles est un enjeu majeur. Les réseaux informatiques sont utilisés pour stocker et échanger des données précieuses, telles que des informations personnelles, des secrets industriels ou des données financières. La compromission de ces données peut entraîner des conséquences graves, tant sur le plan financier que sur la réputation des organisations concernées. Les organismes gouvernementaux, les entreprises et même les particuliers doivent s'efforcer de protéger leurs données contre les attaques malveillantes et les fuites accidentelles.

Un autre enjeu majeur de la sécurité des réseaux informatiques concerne la disponibilité des systèmes. Les attaques par déni de service (DDoS) visent à perturber l'accès aux ressources informatiques en inondant les serveurs de requêtes. Ces attaques peuvent paralyser les activités d'une organisation, empêchant l'accès aux services en ligne et perturbant gravement les opérations. Assurer une disponibilité constante des réseaux informatiques est donc un défi important pour garantir la continuité des activités et la satisfaction des utilisateurs.

La confidentialité des données est un autre enjeu majeur. Les réseaux informatiques peuvent être vulnérables à des attaques visant à intercepter et à accéder aux informations confidentielles, telles que des communications sensibles ou des données stratégiques. Les organisations doivent mettre en place des mesures de sécurité adéquates, telles que le chiffrement des données et l'authentification à deux facteurs, pour protéger la confidentialité des informations échangées sur les réseaux.

La complexité croissante des infrastructures informatiques est également un enjeu de sécurité. Avec l'avènement de la virtualisation, du cloud computing et de l'Internet des objets, les réseaux informatiques sont devenus de plus en plus interconnectés et hétérogènes. Cette complexité accrue rend la gestion et la protection des réseaux plus difficiles. Les entreprises doivent s'assurer d'avoir

une visibilité complète de leurs infrastructures et des mécanismes de surveillance en place pour détecter les anomalies et les comportements suspects.

En outre, les défis de la sécurité des réseaux informatiques sont continuellement amplifiés par l'évolution des techniques d'attaques. Les cybercriminels utilisent des méthodes sophistiquées, telles que l'ingénierie sociale, le phishing ou le ransomware, pour contourner les mesures de sécurité traditionnelles. Ces attaques sont de plus en plus ciblées, adaptatives et difficilement détectables. Les organisations doivent constamment mettre à jour leurs défenses et adopter des stratégies de sécurité proactives pour contrer ces menaces.

Dans l'ensemble, les enjeux et défis de la sécurité des réseaux informatiques sont nombreux et complexes, nécessitant une attention continue et des investissements stratégiques. Les organisations doivent adopter une approche holistique de la sécurité, en intégrant des solutions technologiques, des méthodologies de gestion des risques et des pratiques de sensibilisation et de formation des utilisateurs. Comprendre les enjeux actuels et les défis permet de renforcer la sécurité des réseaux et de prévenir les pertes financières et de réputation associées aux cyberattaques. [11]

III.11 Conclusion

La sécurité des réseaux informatiques est devenue une préoccupation centrale dans le monde numérique d'aujourd'hui. Avec l'avènement du tout numérique et l'intégration croissante des technologies de l'information dans tous les aspects de la vie quotidienne et professionnelle, assurer l'intégrité, la disponibilité et la confidentialité des données est crucial. Les menaces pesant sur la sécurité des réseaux sont diverses et en constante évolution, nécessitant des mesures de protection sophistiquées et adaptatives.

Pour les professionnels, en particulier dans des domaines traitant d'informations sensibles telles que le secteur juridique, la mise en place d'audits informatiques réguliers est indispensable. Ces audits permettent d'identifier les vulnérabilités potentielles et de mettre en œuvre des solutions pour pallier ces failles avant qu'elles ne soient exploitées par des acteurs malveillants. Les fournisseurs de solutions de sécurité, tels que mentionnés dans les analyses de Bitdefender, jouent également un rôle crucial dans la protection des réseaux, offrant des outils avancés pour détecter et contrer les menaces.

À l'ère du numérique, la sécurité des réseaux informatiques n'est pas seulement une question technique, mais aussi une responsabilité collective. Il est impératif pour chaque utilisateur, chaque entreprise et chaque institution de prendre au sérieux leur rôle dans la protection de leurs infrastructures numériques. En mettant en place des politiques de sécurité robustes, en restant informés sur les dernières menaces, et en intégrant des solutions de sécurité efficaces, afin de pouvoir viser à créer un environnement numérique plus sûr pour tous.

Dans un monde où les données sont le nouveau pétrole et où l'information est un pouvoir, assurer la sécurité des réseaux informatiques est devenu non seulement un impératif technique mais aussi une nécessité sociétale. En prenant les mesures appropriées, nous pouvons aspire à un avenir numérique plus résilient face aux menaces, où la confiance numérique facilite le progrès et l'innovation.

Chapitre IV : PARTIE PRATIQUE

Cas : Réalisation du réseau Internet / Intranet du campus Tamda À L'université Mouloud Mammeri de Tizi-Ouzou

IV.1 Introduction

Dans le cadre de la réalisation de la partie pratique de mon mémoire, j'ai intégré l'équipe du centre des systèmes et réseaux d'information et de communication, de télé-enseignement et d'enseignement à distance de l'université Mouloud Mammeri de Tizi-Ouzou.
Ce centre est chargé de l'étude technique du projet de réalisation du réseau Internet / Intranet du campus Tamda. Mon mémoire porte d'ailleurs sur ce projet.

IV.2 Présentation de l'organisme d'accueil

L'université de Tizi-Ouzou est créée en 1977 (décret no 77-93 du 20 juin 1977, JORADP n. 51 du 26.06.1977) sous forme de Centre universitaire rattaché à l'université d'Alger.

En 1989, le Centre universitaire de Tizi-Ouzou devient une université à part entière (décret no 89-139 du 1er août 1989, modifié et complété).

En 1984, le Centre universitaire de Tizi-Ouzou éclate en 9 instituts :

INES des Sciences Juridiques et Administratives (présentement Faculté de droit et des sciences politiques, FDSP)
INES d'Agronomie
INES de Biologie
INES des Lettres et littérature arabes
INES de Génie Civil
INES des Sciences Économiques
INES des Sciences Médicales
INES d'Électronique et Informatique
En 1989, cinq nouveaux départements y sont créés :

Département d'Architecture.
Département d'Électronique.
Département des Langues Étrangères
Département des Sciences Exactes
Département de Génie Mécanique
En 1991, les quatre premiers départements cités deviennent des instituts. Quant au cinquième, il n'est érigé en institut qu'en 1995.

En 1990, le département des Langues et Culture Amazigh a vu le jour par arrêté ministériel.

L'université compte actuellement 9 facultés réparties sur plusieurs sites notamment Boukhalfa (faculté de Droit et Sciences politiques, et Résidences), Hasnaoua, Bastos (Technologies), Tamda (Sciences Humaines, Annexes facultés de sciences, génie électrique et informatique, de Médecine…)
L'Université Mouloud Mammeri de Tizi-Ouzou compte désormais plus de 50.000 étudiants, plus de 2.000 enseignants-chercheurs et près de 1.700 fonctionnaires administratifs, technique et de service. [12]
En plus des neuf facultés de l'université, la direction de l'UMMTO se fait au niveau du rectorat et de ses services communs. Parmi ces services, nous citerons la bibliothèque universitaire, le Centre

d'enseignement intensif des langues, les sous-directions (moyens, finances, personnels et activités culturelles et sportives), le centre d'impression et de l'audiovisuel, mais surtout le Centre des Systèmes et Réseaux d'information et de communication, de télé-enseignement et d'enseignement à distance, dans lequel j'ai effectué mon stage pratique.

Le Centre des Systèmes et Réseaux CSRICTED a été créé par l'arrêté interministériel du 24 août 2004 fixant l'organisation administrative du rectorat, de la faculté, de l'institut, de l'annexe de l'université et de ses services communs.
Il est composé de trois services :

- Service des réseaux informatiques
- Service des Systèmes informatiques
- Service du Télé-enseignement

Les missions principales de ce centre sont :

- L'exploitation, l'administration et la gestion des infrastructures des réseaux ;
- L'exploitation et le développement des applications informatiques de gestion de la pédagogie ;
- Le suivi et l'exécution des projets de télé-enseignement et d'enseignement à distance ;
- Assurer l'appui technique à la conception et la production de cours en ligne ;
- La formation et l'encadrement des intervenants dans l'enseignement à distance ;
- La conception et le développement de tous les sites et plateformes web de l'université.

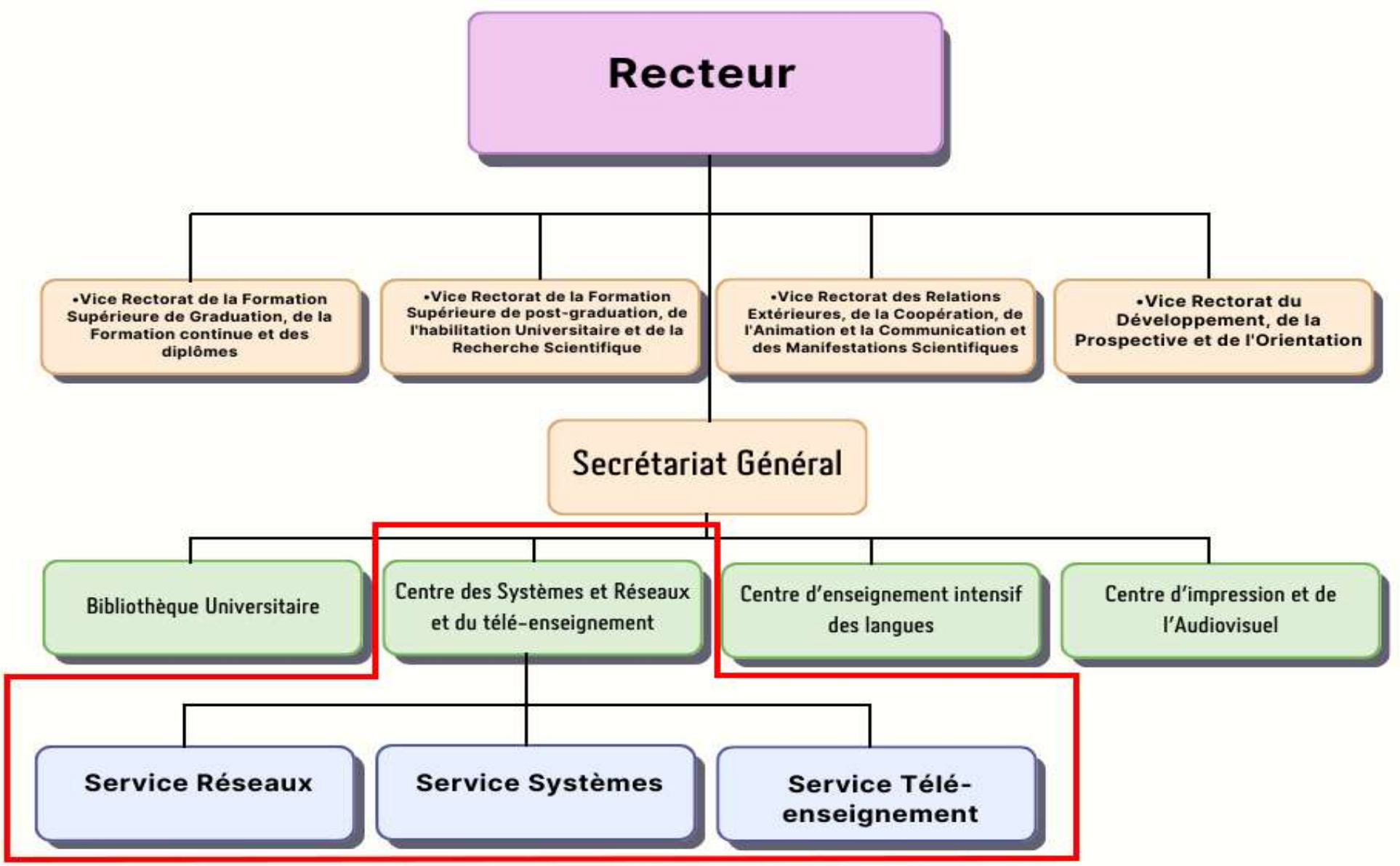


Figure *IV*.48: Organigramme du Rectorat de l'UMMTO

IV.3 Contexte du projet

Le campus Tamda est désormais le plus important pôle de l'université Mouloud Mammeri de Tizi-Ouzou. On y trouve la faculté des sciences humaines et sociales, un auditorium, une bibliothèque, en plus de plusieurs départements de presque toutes les facultés.
Il est officieusement découpé en deux campus Tamda 1 et Tamda 2. Il faut également signaler que 10.000 nouvelles places pédagogiques seront bientôt livrées à Tamda (Tamda 3).
Le campus Tamda 1 de 8000 places pédagogiques (4000 + 4000) et Tamda 2 de 7000 places pédagogiques (4000 + 3000) ne sont à ce jour pas connectés au réseau malgré la nécessité et le besoin de la pédagogie en matière de connexion Internet, notamment en ce qui concerne les spécialités implantées à Tamda (Sciences et technologies, mathématique et informatique, médecine…).

Le projet de réalisation du réseau Internet / Intranet du campus Tamda vise à connecter l'ensemble des immeubles avec une connexion à haut débit.

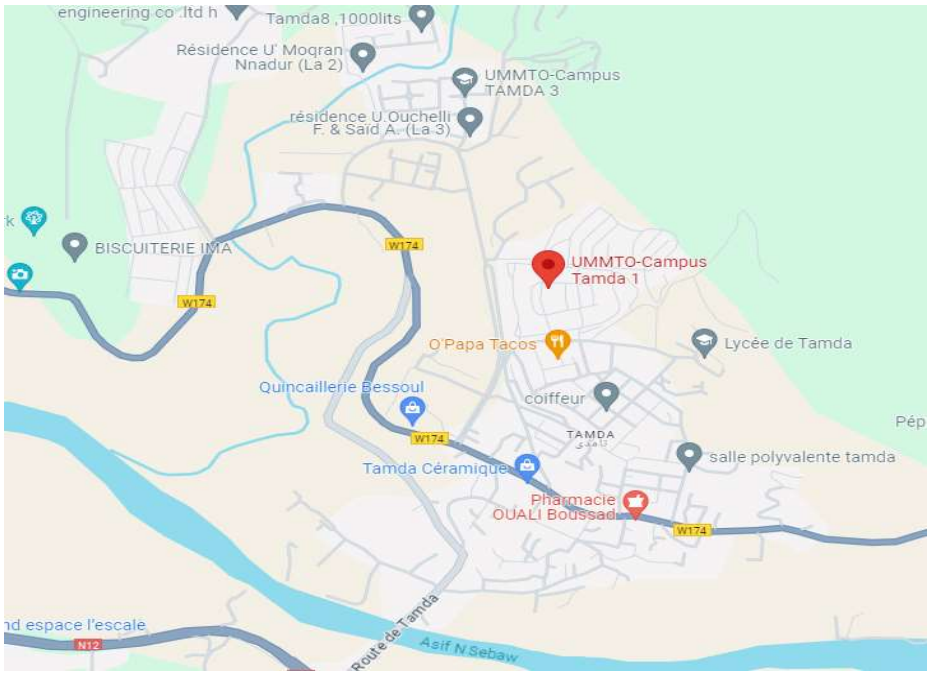


Figure IV.49: Localisation du projet

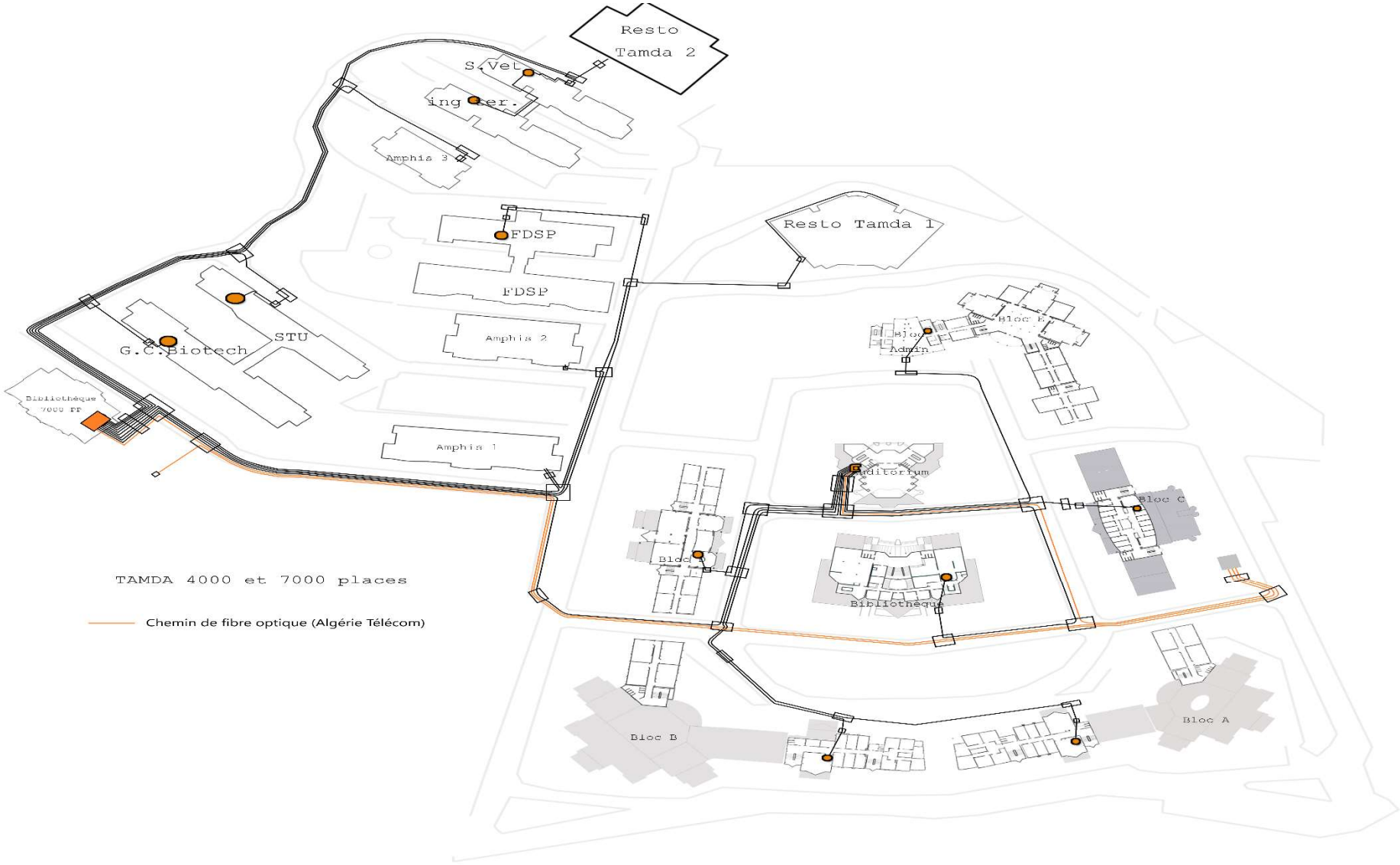


Figure IV. 50: Interconnexion des immeubles en Fibre Optique Monomode du Campus Tamda / Source : Centre des réseaux

IV.4 Description technique du projet

IV.4.1 Interconnexion des immeubles

L'ensemble des immeubles du campus Tamda devront être reliés avec des liaisons en fibre optique monomode. Les colonnes montantes à l'intérieur des immeubles devront quant à elles être réalisées en fibre optique multimode.

Les câbles de fibre optique monomode devront être protégés dans des fourreaux en PVC 40mm conformément aux normes en la matière.

Des chambres de tirage renforcées en bétons armé seront également réalisées.

IV.4.2 Réseaux locaux à l'intérieur des immeubles

A part les colonnes montantes entre les étages qui seront réalisées en fibre optique multimode, les liaisons horizontales seront réalisées en cuivre FTP catégorie 6, dans des goulottes en PVC, entre les switches d'accès et les terminaux.

IV.4.3 Partie active

Pour la partie active, les commutateurs utilisés sont tous de niveau 3 et de la marque reconnue CISCO.

Deux backbones seront réalisées. Le premier au niveau de l'auditorium pour alimenter tout le campus Tamda 1 et le second au niveau de la Bibliothèque pour alimenter Tamda 2.

Ces commutateurs sont des CISCO 9400 avec deux cartes de supervision.

Ils seront reliés en fibre optique monomode directement au niveau de chaque immeuble à des switches de distribution du modèle CISCO 9300 avec 24 ports SFP.

Chaque commutateur CISCO 9300 sera relié en fibre optique multimode à des switches d'accès du modèle CISCO 1000 au niveau de chaque étage de l'immeuble.

Les commutateurs CISCO 1000 desserviront à leur tour les terminaux de l'étage concerné en cuivre SFTP catégorie 6.

Il est également prévu 40 points d'accès wifi CISCO.

IV.5 Réalisation du projet

Le projet a pour but de fournir, d'installer et de mettre en service un réseau informatique connecté à Internet en haut débit pour l'ensemble des blocs des campus.

Etant donné l'importance du projet, il sera divisé en deux parties :

- Partie 1 : Réalisation du réseau local à l'intérieur des blocs des deux campus :
- Partie 2 : Réalisation de l'infrastructure d'accueil, pose et raccordement en fibre optique entre tous les blocs des deux campus.

Partie 1 : Réalisation du réseau local à l'intérieur des blocs des deux campus Tamda 1 et Tamda 2

Cette partie comprend la réalisation et la mise en service du réseau local à l'intérieur des blocs à savoir :

- Plans de chemin de câble (goulotte)
- Plans pose de câble cuivre SFTP et fibre optique multimode.
- Plans des colonnes montantes pour les interconnexions entres les étages.
- Plans de pose des armoires et fixation des équipements passifs et actifs (fixation des panneaux de brassages, tiroirs optiques, commutateurs, bandeaux d'alimentation, onduleurs, ventilateurs, passes-câbles, guides-câbles, cordons de brassage, jarretières, ….)
- Réalisation des terminaisons de la partie passive : raccordement des noyaux et prises RJ45, soudure de tous les brins de fibres optiques multimode et monomode.
- Test et mise en service du réseau LAN

Le réseau installé doit supporter un débit d'un 1 Gigabit/s au minimum. Tous les composants installés (câbles, support, équipements,) devront supporter ce débit.

Le système de câblage posé doit avoir une architecture en étoile : l'ensemble des câbles reliant les équipements actifs (répartiteurs d'étage et répartiteurs des blocs) converge vers une baie de brassage d'un répartiteur principal.

Des répartiteurs techniques doivent être prévus au niveau de chaque bloc répartis comme suit :

- Un répartiteur principal par campus situé au niveau de l'Auditorium pour le campus Tamda 1 et la bibliothèque du campus Tamda 2.
- Un répartiteur de distribution par bloc
- Un ou plusieurs répartiteurs par étage en fonction du nombre des prises Ethernet et l'étendue de l'étage.
- Une ou plusieurs colonnes montantes doivent être créées au niveau de chaque bloc.
- Les répartiteurs doivent être situés à proximité des colonnes montantes, et le plus près possible du centre de la zone à distribuer, et doivent être éloignés de toute source de perturbation (cages d'ascenseur, sanitaires, répartiteurs de courants forts, ...).

Le réseau de distribution à l'intérieur des blocs sera réalisé en fibre optique multimode :

- Prévoir deux paires de brins de fibre en réserve pour toutes les interconnexions en fibre entre les équipements actifs (chaque commutateur doit avoir 3 paires de fibre : une active et deux de secours)
- Les extrémités des brins de câble en fibre optique doivent être soudés avec des pigtails ayant des connecteurs de type LC et fixés sur des tiroirs optiques de format 19''.

Le câblage reliant les équipements actifs jusqu'aux prises terminales (postes de travail) sera réalisé en câble cuivre SFTP :

- Câble en cuivre de type SFTP 4 paires torsadées catégorie 6.
- Les chemins de câbles de distribution verticale ou horizontale doivent avoir une capacité permettant d'augmenter la quantité de câbles de 25% au minimum.

- La convention de câblage (EIA/TIA 568) doit être la même sur l'ensemble de l'installation.
- Les cordons de poste et de brassage doivent être testés aux usines du constructeur, portant le marquage indiquant les références concordantes avec le catalogue du constructeur.

IV.6 Description technique du matériel et accessoires utilisés pour l'installation du réseau LAN

IV.A Partie passive

1. Prises Ethernet RJ45

Prise RJ45 catégorie 6 SFTP mosaïque 2 modules :

- SFTP - 2 module (45x45 mm)
- Blindage métal
- Prise avec connecteur à connexion rapide sans outil et permettant un re-câblage en cas d'erreur
- Repérage T568A et B avec codes couleurs

2. Cable en cuivre FTP Cat6

Câble catégorie 6 SFTP 4 paires torsadées 4*2*23awg 100 Ω

- Gaine LSOH : sans halogène
- Code couleur EIA/TIA
- Performance 300 MHz
- Débit supporté 1Gbps pour 100 mètres

3. Panneau de brassage Cat 6

Panneau de brassage Catégorie 6 équipé de 24 connecteurs RJ 45

- Montage universel sur toutes les baies de brassage
- Le panneau assure une reprise de masse automatique de chaque connecteur.
- Équipé de guide-câbles à l'arrière pour maintien du câble lors de la maintenance.
- Équipé de 4 cassettes de 6 connecteurs RJ 45 cat. 6, FTP à connexion rapide sans outils et permettant un re-câblage en cas d'erreur, pré-montés, dotés de bouchons de protection anti-poussière
- Repérage T568A et B avec codes couleurs
- Livré avec étiquettes de couleur
- Panneau 19" - 1 U
- Extraction automatique des cassettes par simple pression. Possibilité d'extraire chaque connecteur individuellement
- Panneau FTP - Blindage métal

4. Cordon de brassage longueur 1ml / 2ml

- Cordon RJ 45 Catégorie 6 FTP 4 paires torsadées 4*2*24awg
- RJ 45/RJ 45 droit
- Avec plug spécial "préhension aisée"
- SFTP blindés impédance 100 Ω

- Longueur 1 mètre, 2 mètres.
- Cordons testés en usine individuellement
- Gaine LSOH

5. Cordon de poste 3ml cat 6

- Cordon RJ 45 Catégorie 6 FTP 4 paires torsadées 4*2*24awg
- RJ45 / RJ45 droit
- Avec plug spécial "préhension aisée"
- SFTP blindé impédance 100 Ω
- Cordons testés en usine individuellement
- Longueur 3 mètres
- Gaine LSOH

6. Cable Fibre optique multimode

Le réseau optique à l'intérieur des blocs sera réalisé en fibre optique multimode 12 brins au minimum, armés fibre de verre, protection anti-rongeurs.

- Insensibles aux courbures "Bend insensitive"
- Pour installations multimodes 50/125 µm, type OM4
- Conviennent au réseau 1 Gigabit Ethernet
- Intérieur/extérieur
- 36 brins de fibre au minimum

7. Jarretière multimode

Jarretière LC/LC duplex multimodes 50/125 µm, type OM4

- Équipés à chaque extrémité de 2 connecteurs à férule en céramique
- Conviennent au réseau 1Gigabit Ethernet
- Pertes optiques maxi/Master : 0,25 dB
- Gaine Zipcord LSZH
- Longueur : 2 mètres

8. Tiroir optique équipé

Tiroir optique coulissant 19 pouces, 12 LC duplex multimode/monomode, 2 entrées de câbles, avec couvercle et kit de visserie

- Hauteur 1 U
- Repérage du panneau et des ports optiques sur zone de marquage dédiée
- 24 pigtails
- 12 traversées duplex LC avec obturateurs
- Boucles de lovage rotatif

9. Modules Fibre optique SFP

Module SFP multimode

- Module émetteur/récepteur optique enfichable
- Type de fibre optique : Multimode
- Type de connecteur : Duplex LC

- Vitesse de transfert de données : 1 Gbps
- Compatible avec la fibre et les ports SFP des équipements actifs (commutateurs) installés.

Module SFP monomode

- Module émetteur/récepteur optique enfichable
- Type de fibre optique : Monomode
- Type de connecteur : Duplex LC
- Vitesse de transfert de données : 1 Gbps
- Compatible avec la fibre et les ports SFP des équipements actifs (commutateurs) installés : les modules doivent être du même fabriquant que celui des équipements actifs.

10. Goulotte 105*50 clippage direct

Goulotte à 1 compartiment à clippage direct 50 x105mm mosaïque

- Comprends :
  - 1 corps (profilé)
  - 1 couvercle souple largeur 45 mm
- Accepte tous les appareillages mosaïques
- Découpe à l'aide d'une scie (type scie à métaux ou taille moulures pour découper les couvercles)
- Réponds aux exigences de fiabilité, de sécurité et de performance technique (Conforme à la norme NF EN 50085-2-1)

10.1 Accessoires de finition et de cheminement

- Angles 90° plats
- Angles intérieurs 80 à 100°
- Angles extérieurs
- Embouts
- Dérivations planes vers goulottes de même largeur de profilé.
- Chevilles et vis pour la mise en place de tous les profilés

11. Armoire de brassages

11.1 Baie de brassage 12U 600*600

- Capacité : 12 U
- Hauteur : 740 mm
- Largeur : 600 mm
- Profondeur : 600 mm
- Porte avant réversible, galbée en verre de sécurité sérigraphié
- Porte arrière réversible en métal
- Panneaux latéraux et arrière démontables avec liaison équipotentielle automatique
- Condamnation des 4 faces par serrure à clé 2433A
- Entrées de câbles hautes et basses prédécoupées au format 19" pouvant recevoir des plaques 19" avec balai, ventilateurs…
- Kit de roulettes et pieds de nivellement réglables de l'intérieur
- Baies entièrement démontables en cas d'accès difficile
- Charge admissible : 150 kg

11.2 Baie de brassage 24U 600*800

- Capacité : 24 U
- Hauteur : 1226 mm
- Largeur : 600 mm
- Profondeur : 800 mm
- Porte avant réversible, galbée en verre de sécurité sérigraphié
- Porte arrière réversible en métal
- Panneaux latéraux et arrière démontables avec liaison équipotentielle automatique
- Condamnation des 4 faces par serrure à clé 2433A
- Entrées de câbles hautes et basses prédécoupées au format 19" pouvant recevoir des plaques 19" avec balai, ventilateurs…
- Kit de roulettes et pieds de nivellement réglables de l'intérieur
- Baies entièrement démontables en cas d'accès difficile
- Charge admissible : 400 kg

11.3 Baie de brassage 42U 600*800

- Capacité : 42 U
- Hauteur : 2 026 mm
- Largeur : 600 mm
- Profondeur : 800 mm
- Porte avant réversible, galbée en verre de sécurité sérigraphié
- Porte arrière réversible en métal
- Panneaux latéraux démontables avec liaison équipotentielle automatique
- Condamnation des 4 faces par serrure à clé 2433A
- Entrées de câbles hautes et basses prédécoupées au format 19" pouvant recevoir des plaques 19" avec balai, ventilateurs…
- Kit de roulettes et pieds de nivellement réglables de l'intérieur
- Baies entièrement démontables en cas d'accès difficile
- Charge admissible : 420 kg

12. Bandeau d'alimentation de prises électrique (PDU)

- Protège contre les surtensions réseau tout en conservant les prises sous tension
- Cuve aluminium hauteur 1 U
- Alimentation 220/230 V - 50/60 Hz
- Nombre de prises : 6 prises 2P+T inclinées à 55° avec éclipse de protection
- Module parasurtenseur et interrupteur débordant pour éviter les coupures accidentelles
- Avec témoins lumineux :
    - 1 LED (blanc) pour la présence tension
    - 1 LED (vert) pour l'indication d'état du module parasurtenseur
- Cordon d'alimentation 3 m avec fiche 2P+T 16 A
- Montage sur racks 19" Haute Densité uniquement avec visserie
- Guidage du cordon intégré

13. Tiroir de ventilation 1U format 19

- Interrupteur ON/OFF lumineux
- 4 ventilateurs
- Fixation sur 2 montants 19" par vis M6 imperdables et écrou-cages à picots 9,5 mm (livrés)
- Tiroir en acier
- Alimentation 220/230 V

IV.B Partie active

Les équipements actifs doivent avoir une version OS la plus complète, la plus récente et la plus stable à la date de mise en marche.

1. **Commutateur d'accès administrable de couche 3 avec : 24 ports 10/100/1000 base-T RJ-45 + 4 ports SFP 1 Gbps Modèle choisi « CISCO Catalyst 1000 »**

- Montable sur rack 1U
- Interfaces :
  - 24 × 10/100/1000Base-T RJ-45
  - 1 x USB Type A
  - 1 x série (console) RJ-45 gestion
  - 1 x gestion (Gigabit LAN) RJ-45 gestion
  - 1 x gestion (mini-USB) Type B gestion
  - 4 × 1GBase-X SFP liaison montante
- RAM : 512 Mo
- Mémoire flash : 256 Mo
- Protocole de Routage : IGMP
- Protocole de gestion à distance : SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, SSH, CLI
- Méthode d'authentification : Kerberos, Secure Shell (SSH), RADIUS, TACACS+
- Périphérique d'alimentation :
  - Alimentation électrique interne - enfichable à chaud
  - Nombre installé : 1 (installé) / 2 (maximum)
  - Tension requise : CA 120/230 V (50/60 Hz)

2. **Points d'accès Wifi**

- Nombre de Connexions simultanées : minimum 32 connexions.
- Nombre d'antennes : deux antennes omnidirectionnelles intégrées.
- Interface Ethernet : 10/100 Base T RJ45, raccordement sans outil.
- Interface WiFi : le point d'accès permet un fonctionnement en simultané en 802.11b/g/n 2,4 GHz ou en 802.11a/n 5GHz.
- Envoi des logs via le réseau « Syslog »
- Débit de transfert de données supérieur ou égal à 300 Mbits/s
- Interface web d'administration (en HTTP, HTTPS)
- Adressage IP statique ou dynamique (DHCP).

- Authentication: 802.1x (EAP TLS, EAP TTLS, PEAP).
- Cryptage :
  - WEP-802.1x(WEP dynamique avec Radius)
  - WPA-PSK cryptage TKIP
  - WPA-802.1x cryptage TKIP avec Radius
  - WPA2-PSK cryptage AES
  - WPA2-802.1x cryptage AES avec Radius
- Support VLAN trunking 802.1q sur le câble Ethernet
- Support de fixation

3. Commutateur de distribution administrable de couche 3 avec 24 ports SFP Modèle choisi « CISCO Catalyst 9300 »

- Montable sur rack 1U format 19 pouces
- Interfaces :
  - 24 Ports 1Gps SFP
  - 1 x USB Type A
  - 1 x série (console) RJ-45 gestion
  - 1 x gestion (Gigabit LAN) RJ-45 gestion
  - 1 x gestion (mini-USB) Type B gestion

- Capacité de commutation : 68 Gbps (92 Gbps pour 24 ports SFP)
- Taille de la table d'adresses MAC : 32 000 entrées
- 4 Go RAM
- 2 Go Mémoire Flash
- Protocole de Routage supportant IPV4 et IPV6 : Routage IP statique, EIGRP, OSPF, routage à base de règles (PBR) RIP-2, IGMPv2, IGMP, PIM-SM, PIM-DM, IGMPv3, OSPFv3, BGPv4
- Protocole de gestion à distance : SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, SSH, CLI
- Méthode d'authentification : Kerberos, Secure Shell (SSH), RADIUS, TACACS+
- Périphérique d'alimentation :
  - Alimentation électrique interne - enfichable à chaud
  - Nombre installé : 1 (installé) / 2 (maximum)
  - Tension requise : CA 120/230 V (50/60 Hz)

4. Commutateur Core administrable de couche 3 avec double carte de supervision Modèle choisi « CISCO Catalyst 9400 »

4.1 Châssis

- Équipé de quatre logements horizontaux, numérotés de 1 à 4 (de haut en bas).
- Montable sur rack : 6 U
- Baie de ventilation : réparable et remplaçable à chaud.
- Connecteurs dédiés pour les cartes de ligne (modules de commutation) : 2
- Connecteurs dédiés pour les moteurs de supervision : 2
- PoE supporté par le châssis : ~2880 W PoE par connecteur de ligne.
- Alimentation redondante enfichable à chaud

- Fond de panier : 120 Gbit/s de bande passante de fond de panier pour chaque connecteur de module de charge utile, avec les modules de supervision.
- Emplacement du montage en rack 19 pouces : Avant

4.2 Modules de supervision : deux cartes de supervision en redondance

- Processeurs installés : Intel 2.4 GHz
- RAM : 16 Go
- Mémoire flash : 10 Go
- Disque dur : SSD 960 Go
- Format : Module enfichable forme 1U pour châssis 4U
- Technologie de connectivité : Filaire
- Protocole de liaison de données : Gigabit Ethernet
- Bande passante : 120 Gbit/s par connecteur de carte de ligne
- Capacité :
  - Adresses MAC : 64000
  - Routes IPv4 : 112000
  - ID de VLAN : 4096
  - Interfaces virtuelles commutées (SVI) : 4000
  - Taille de cadre large : 9198 octets
  - Entrées de table de routage IPv4 : 112000
  - Entrées de table de routage IPv6 : 56000
  - Routes de multidiffusion : 16000
  - Entrées de matériel QoS : 18000
  - Entrées matérielles ACL de sécurité : 18000

4.3 Modules de commutation 24 ports 1Gbps SFP format LC

- Module enfichable forme 1U pour châssis 4U
- Interfaces : 24 Ports 1Gbps SFP
- Niveau de commutation : L2/L3

4.4 Module de commutation 48 ports 100/1000 Mbps RJ45

- Module enfichable forme 1U pour châssis 4U
- Interfaces : 48 Ports 100/1000 Mbps RJ45 POE
- Niveau de commutation : L2/L3

5. Onduleur monophasé PDU 1U : on line double conversion

- Format rack 19"
- Hauteur : 1 U
- Régulation automatique de la tension
- Protège contre les surtensions et les pics causés par le tonnerre et la foudre
- Écran LCD multifonction
- Puissance nominale : 1 KVA
- Puissance active : 670 W
- Batterie remplaçable à chaud
- Autonomie : supérieur à 15 minutes

6. Onduleur monophasé PDU 2U : online double conversion

- Format rack 19"
- Hauteur : 2U
- Régulation automatique de la tension
- Protège contre les surtensions et les pics causés par le tonnerre et la foudre
- Écran LCD multifonction
- Puissance nominale : 2KVA
- Puissance active : 1800 W
- Batteries remplaçables à chaud
- Autonomie : supérieur à 15 minutes
- Type de prise d'entrée : IEC C14
- Prises ondulées et para-surtensées : 8 × IEC C13

Partie 2 : Réalisation de l'infrastructure d'accueil, pose et raccordement en fibre optique entre tous les blocs des deux campus Tamda1 et Tamda2

L'infrastructure passive permet le raccordement en fibre optique Monomode des répartiteurs de distribution, situés au niveau de chaque bloc, aux répartiteurs principaux du campus.
Elle comprend :

- Plan d'installation des chambres de tirage de type renforcé
- Plan de pose de fourreaux PEHD dans des tranchées
- Plan de pose de câble fibre optique Monomode à partir des répartiteurs principaux des campus jusqu'aux répartiteurs de distribution des blocs
- Test et mise en service de l'infrastructure installée.

Le réseau optique, de débit minimum d'1 Gbps, sera réalisé en fibre optique monomode, avec protection anti-rongeurs et doit respecter les normes d'installation, de sécurité, et de déploiement des réseaux locaux fibre optique :

- Les câbles en fibre optique doivent être protégés dans des fourreaux PEHD.
- Les fourreaux PEHD doivent être enfouis dans des tranchées comportant un grillage avertisseur ayant la largeur de la tranchée.
- Le raccordement des fourreaux entre eux doit être étanche.
- Dans le cas de la dérivation d'un ou plusieurs câbles en fibre optique provenant d'un fourreau vers un autre, au niveau des chambres, les dérivations doivent être protégées au moyen d'un boîtier ou accessoire assurant la protection et l'étanchéité.
- Toutes les terminaisons des brins de câble en fibre optique doivent être soudées avec des pigtails ayant des connecteurs de type LC et fixés sur des tiroirs optiques de format 19''.

IV.7 Architecture du réseau sur les deux campus

La conception du réseau informatique du campus universitaire de Tamda a été réalisée de telle sorte à répondre au besoin des étudiants, enseignants-chercheurs ainsi que de l'administration en question d'accès au réseau local et à Internet tout en garantissant une bande passante stable et de qualité.
L'étude prévoit des prises réseaux dans tous les bureaux, salles et laboratoires. Le nombre de prises dans chaque local est défini selon le nombre d'occupants.
Nous nous sommes basés sur un nombre de prises qui dépasse le nombre d'utilisateurs actuels afin d'éviter toute extension de réseau pour les besoins futurs.
L'architecture réseau sera hiérarchique et composée de trois couches.

IV.7.1 Concept du réseau hiérarchique

La conception de réseau hiérarchique est une approche d'architecture de réseau permettant de créer des systèmes de réseau informatique fiables, évolutifs et efficaces. La méthodologie de conception permet d'améliorer la gestion, les performances et la sécurité en divisant le réseau en différentes couches, chacune avec des fonctions et des responsabilités spécifiques. Initialement introduite par Cisco en 2002, la conception de réseau hiérarchique est devenue une pratique standard dans de nombreuses conceptions de réseaux.
Dans les conceptions traditionnelles de réseaux plats, les réseaux sont connectés à l'aide de hubs et de commutateurs, qui deviennent difficiles à gérer et à entretenir à mesure qu'ils évoluent. L'introduction d'une conception de réseau hiérarchique répond à ces défis en divisant le réseau en

différentes couches pour mieux contrôler le trafic, améliorer les temps de réponse et optimiser les performances du réseau.

Le réseau hiérarchique est composé de trois couches principales :

a- Couche Cœur de réseau

La couche centrale constitue l'épine dorsale du réseau et est responsable de la transmission de données et de l'échange de trafic à haut débit. Il connecte les différentes couches d'agrégation et offre une disponibilité et une redondance élevées du réseau. La couche centrale doit être caractérisée par une bande passante élevée, une faible latence et une haute disponibilité. [13]

La couche cœur de réseau sera composée des deux switches Core CISCO 9400. Le premier sera installé au niveau du local technique situé à l'Auditorium du campus Tamda 1 et le second au local technique situé à la nouvelle bibliothèque de Tamda 2.

Ils seront reliés, en fibre optique monomode, d'une part aux équipements d'Algérie Télécom et d'autre part aux switches de distribution.

b- Couche Distribution

La couche de distribution est située entre la couche d'accès et la couche cœur de réseau et est responsable de la connexion des différents sous-réseaux de la couche d'accès. Au niveau de la couche de distribution, le trafic est agrégé et filtré, ainsi que séparé entre les secteurs (via la technologie LAN virtuel ou VLAN). [13]

La couche de distribution sera composée de douze switches CISCO 9300 avec 24 ports SFP. Chaque immeuble du campus sera équipé d'un switch de distribution.

Ceux-ci seront reliés d'un côté au switch Core en fibre optique monomode et de l'autre côté en fibre optique multimode aux switches d'accès.

c- Couche Accès

Il s'agit du point d'entrée permettant aux appareils des utilisateurs (par exemple, les ordinateurs, les imprimantes, etc.) d'accéder au réseau. La couche d'accès est chargée de fournir l'accès des utilisateurs, l'authentification, les politiques de sécurité et d'autres fonctions, mais effectue également le traitement du trafic local. Les commutateurs jouent un rôle clé dans cette couche, connectant les appareils des utilisateurs au réseau. [13]

La couche d'accès sera composée des switches CISCO 1000 dotés de 24 ports RJ45 et quatre ports SFP. Ils seront reliés d'un côté en fibre optique multimode aux switches de distribution et de l'autre côté en câble SFTP catégorie 6 aux terminaux (PC, imprimantes…)

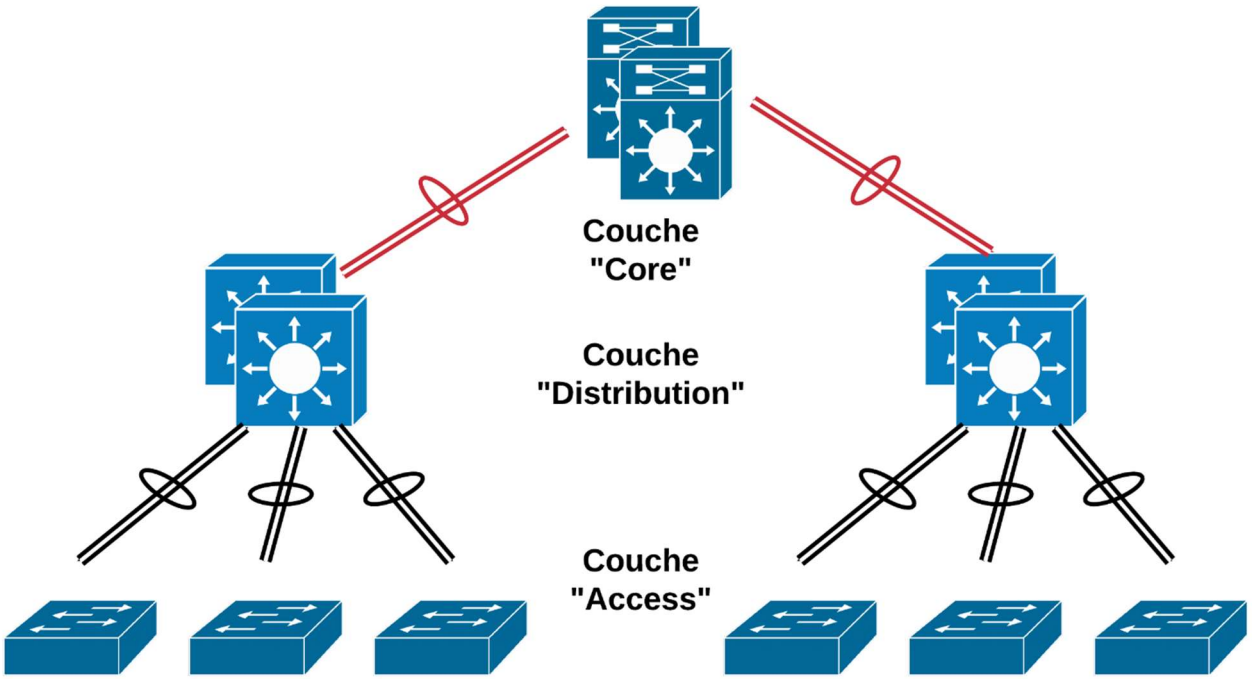


Figure IV.51: Modèle hiérarchique

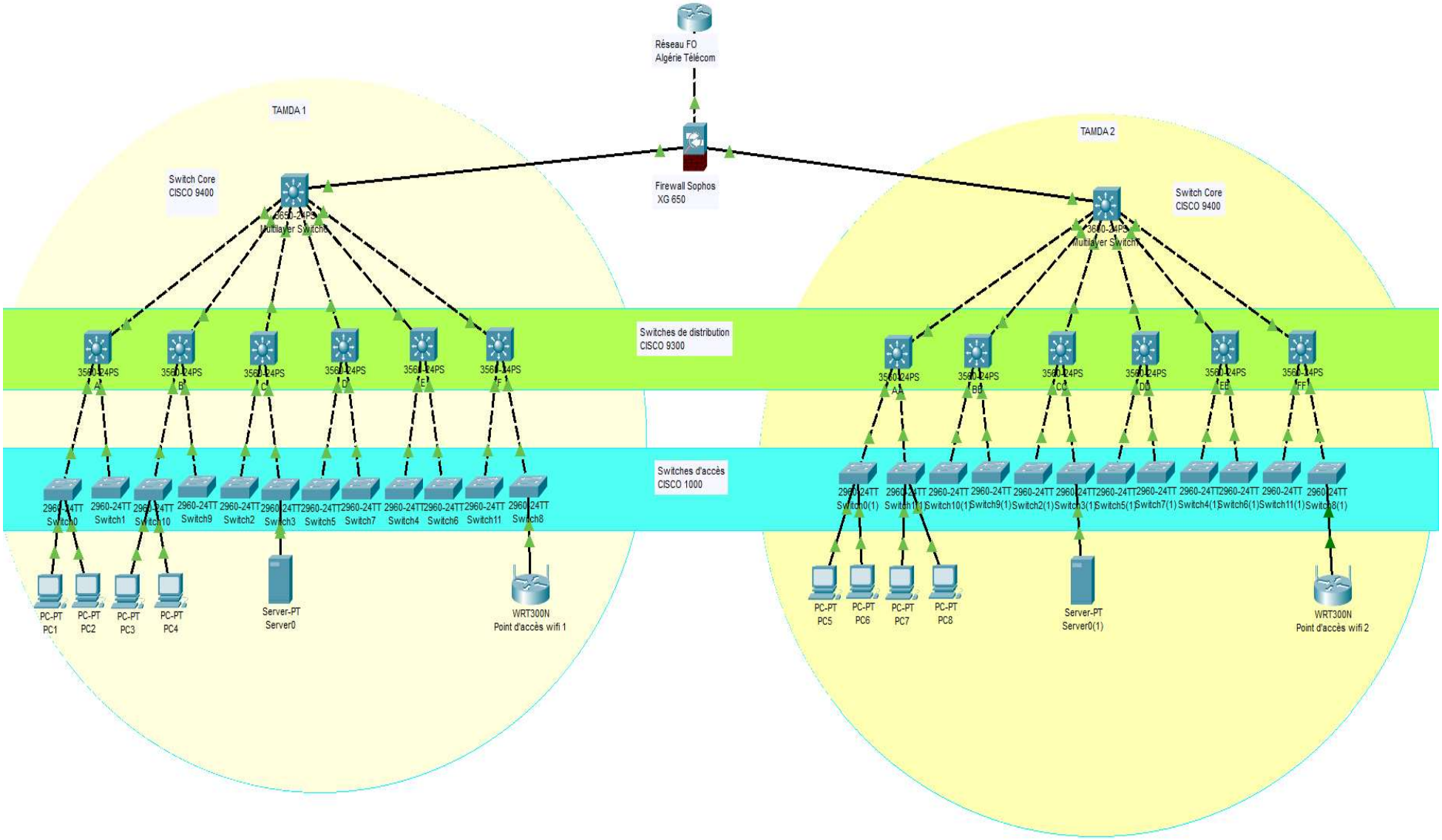


Figure IV.52: Architecture réseau réalisé au campus Tamda

IV.8 Répartition des prises par locaux au campus Tamda 1

BLOC A

Bloc	Etage	Local	Prise RJ45 +noyau	Câble SFTP cat 6	Local technique et armoire
BLOC A	RDC	Amphis A1-09	2	70	Source des prises 1er étage
		Amphis A1-11	2	60	
		Amphis A1-13	2	50	
		Total	**6**	**180**	
	1er étage	Salle de lecture A1-13	2	60	
		Banque de prêt A1-12	6	100	Armoire 12U
		Vidéothèque A1-11	4	100	
		Salle de tirage	2	50	Source des prises 2ème étage
		Bureau en face de la salle e tirage	2	50	
		Total	**16**	**360**	
	2ème étage	Laboratoire A2-17	2	60	Armoire 12U
		Laboratoire A2-16	2	70	
		Laboratoire A2-15	2	40	
		Laboratoire A2-14	2	50	
		Vidéothèque A2-11	4	230	
		Salle TP internet	40	960	Armoire 42U arrivée FO SM
		Salle machine Etudiants	22	660	
		Bureau du comité	2	40	
		Bureau Examen	4	90	Armoire 12U
		Bureau Enseignement	4	80	
		Bureau 02	4	40	
		Bureau 04	4	60	
		Total	**92**	**2380**	
	3ème étage	Bureau 01	3	120	Armoire 24U
		Bureau 02	3	120	
		Bureau 03	4	120	
		Bureau 04	4	90	
		Bureau 05	4	80	
		Bureau 06	4	100	
		Bureau 07	4	140	
		Bureau 08	4	120	
		Bureau 09	4	110	
		Bureau 10	4	90	
		Bureau 11	4	80	
		Bureau 12	4	60	Armoire 24U

		Salle réunion	18	200	
		Salle internet enseignants	8	200	
		Total	**72**	**1630**	
	4ème étage	Bureau 01	3	120	Armoire 12U
		Bureau 02	3	120	
		Bureau 03	4	100	
		Bureau 04	4	80	
		Bureau 05	4	80	
		Bureau 06	4	100	
		Total	**22**	**600**	
		Total	**208**	**5150**	

BLOC B

Bloc	Etage	Local	Prise RJ45 +noyau	Câble SFTP cat 6	Local technique et armoire
BLOC B	**RDC**	Amphi Lani	2	90	Armoire 12U
		Amphi Matoub	2	120	
		Amphi Kateb Yacine	2	170	
		Laboratoire B01	2	60	
		Laboratoire B02	2	40	
		Laboratoire B03	2	60	
		Laboratoire B04	2	70	
		Total	**14**	**610**	
	1er étage	B1-01	2	60	Armoire 12U / Armoire 24U
		B1-02	2	60	
		B1-03	2	70	
		B1-04	2	80	
		Grande salle B2	2	20	
		Bibliothèque Fonds docs	6	100	
		Vidéothèque B2-11	4	100	
		Labo biologie végétale 01	2	70	
		Labo biologie végétale 02	2	90	
		Labo biologie animale3	2	80	
		Labo bio 4	4	100	
		Labo géophysique	4	80	
		Labo gitologie	2	40	
		Labo biologie végétale 02	2	60	

		Labo biologie végétale 03	2	50	
		En face bureau DLEP	4	120	
		Bureau DLEP	4	120	
		Total	**48**	**1300**	
	2ème étage	B2-12	10	200	Armoire 12U
		Vidéothèque B2-11	4	160	
		B2-10	3	100	
		Salle lecture biblio	3	120	
		Salle machine étudiant	24	500	Armoire 42U arrivée FO SM
		Bureau Enseignant 01	4	80	
		Bureau Enseignant 02	4	90	Armoire 12U
		Bureau Enseignant 03	4	100	
		Bureau Enseignant 04	4	120	
		Total	**60**	**1470**	
	3ème étage	Bureau Moyens-G	2	50	Armoire 24U
		Bureau enseignant	2	50	
		Salle internet enseignants	20	500	
		Bureau Comité	4	120	
		Bureau enseignant	4	160	
		Bureau UGTA	4	200	
		Bureau enseignant	4	80	
		Bureau Associ.	4	120	
		Bureau Moyens-G	4	160	
		Chef Dép Géolo.	4	100	
		Scolarité	4	120	Armoire 12U
		Secrétariat	4	80	
		Chef de filière	4	90	
		Bureau enseignant	4	100	
		Bureau admin	4	120	
		Total	**72**	**2050**	
	4ème étage	Bureau 01	4	80	Armoire 12U
		Bureau 02	4	90	
		Bureau 03	4	100	
		Bureau 04	4	120	
		Bureau 05	4	120	
		Bureau 06	4	100	
		Total	**24**	**610**	
		Total	**218**	**6040**	

BLOC C

Bloc	Etage	Local	Prise RJ45 +noyau	Câble SFTP cat 6	Local technique et armoire
BLOC C	Sous-Sol	Bureau Moyens-G	2	150	Source des prises 2ème étage
		Total	**2**	**150**	
	RDC	Bureau Moyens-G	4	200	Source des prises 2ème étage
		Salle de tirage	4	300	
		Total	**8**	**500**	
	1er étage	Vidéothèque	4	220	Source des prises 2ème étage
		Bureau comité	2	120	
		Total	**6**	**340**	
	2ème étage	Salle lecture 1	2	100	Armoire 42U
		Salle lecture 2	2	100	
		Salle internet étudiant 1	24	720	
		Salle internet étudiant 2	24	1200	
		Total	**52**	**2120**	
	3ème étage	Bureau 01	4	120	Armoire 42U arrivée FO SM
		Bureau 02	4	100	
		Bureau 03	4	80	
		Bureau 04	4	100	
		Bureau 05	4	120	
		Bureau 06	4	140	
		Bureau 07	4	160	
		Salle internet enseignants	24	720	
		Salle internet Post-Graduation	24	720	Armoire 12U Armoire 12U
		Salle réunion (coté escalier)	4	200	
		Magasin informatique	4	200	
		Total	**84**	**2660**	
	4ème étage	Bureau 01	4	120	Armoire 24U
		Bureau 02	4	100	
		Bureau 03	4	80	
		Bureau 04	4	100	
		Bureau 05	4	120	
		Bureau 06	4	160	
		Bureau 07	4	180	
		Bureau 08	6	240	
		Bureau 09	4	160	

		Bureau 10	4	120	
		Bureau 11	6	180	
		Total	**48**	**1560**	
		Total	**200**	**7330**	

BLOC D

Bloc	Etage	Local	Prise RJ45 + noyau	Câble SFTP cat 6	Local technique et armoire
BLOC D	Sous-Sol	Bureau 01	2	150	Source des prises RDC
		Bureau 02	2	150	
		Bureau 03	2	130	
		Bureau 04	2	130	
		Bureau 05	2	100	
		Bureau 06	2	100	
		Total	**12**	**760**	
	RDC	Bureau 01	2	140	Armoire 24U
		Bureau 02	2	140	
		Bureau 03	2	120	
		Bureau 04	2	120	
		Bureau 05	2	90	
		Bureau 06	2	90	
		Bureau 07	2	40	
		Bureau 08	2	100	
		Amphis 1	2	100	
		Amphis 2	2	120	
		Total	**20**	**1060**	
	1er étage	Amphis 1	2	130	Source des prises RDC
		Amphis 2	2	140	
		Bureau 09	2	110	
		Bureau 10	2	110	
		Bureau 11	2	120	
		Bureau 12	2	120	
		Bureau 13	2	140	
		Bureau 14	2	140	
		Total	**16**	**1010**	
	2ème étage	Salle internet	22	900	Armoire 24U
		Salle informatique	24	720	
		Total	**46**	**1620**	
	3ème étage	Bureau 01	6	240	
		Bureau 02	4	160	
		Bureau 03	4	180	
		Bureau 04	4	200	
		Bureau 05	4	220	
		Bureau 06	4	260	
		Bureau 07	4	280	

		Bureau 08	6	420	2Armoires 42U arrivée FO SM
		Bureau 09	10	450	
		Bureau 10	4	160	
		Bureau 11	4	140	
		Bureau 12	4	120	
		Bureau 13	4	90	
		Bureau 14	6	150	
		Total	**68**	**3070**	
	4ème étage	Bureau 01	10	550	Armoire 24U
		Bureau 02	4	200	
		Bureau 03	4	180	
		Bureau 04	4	160	
		Bureau 05	4	140	
		Bureau 06	4	120	
		Bureau 07	4	90	
		Bureau 08	6	120	
		Bureau 09	6	210	
		Bureau 10	6	270	
		Bureau 11	6	330	
		Bureau 12	4	180	
		Bureau 13	4	200	
		Bureau 14	4	220	
		Bureau 15	4	240	
		Bureau 16	6	360	
		Bureau 17	6	390	
		Bureau 18	6	420	
		Total	**92**	**4380**	
		Total	**254**	**11900**	

BLOC E – Partie pédagogue

Bloc	Etage	Local	Prise RJ45 +noyau	Câble SFTP cat 6	Local techniques et armoire
BLOC E Partie pédagogique	**Sous-Sol**	Scolarité License	8	240	Armoire 12U
		Scolarité Master	8	200	
		Chef service Scolarité	4	160	
		Bureau en face du chef de service	4	120	
		Total	**24**	**720**	
	RDC	Amphi 1	2	100	Source des prises 2ème étage
		Amphi 2	2	120	
		Amphi 3	2	160	
		Total	**6**	**380**	
	1er étage	Amphi 4	2	150	Source des prises 2ème étage

		Total	**2**	**150**	
	2ème étage	Salle Internet	25	750	1 Armoire 42U arrivée FO SM
		Salle de lecture	2	100	
		Salle des enseignants	13	720	
		Total	**40**	**1570**	
		Total	**72**	**2820**	

BLOC E – Partie administrative

Bloc	Etage	Local	Prise RJ45 +noyau	Câble SFTP cat 6	Local technique et armoire
BLOC E Partie administrative	**RDC**	Secrétariat	3	200	Source des prises 1er étage droite
		Magasin	0	0	
		Chef de section	2	90	
		Chef de section S4	3	120	
		Bureau 1	3	200	Source des prises 1er étage gauche
		Bureau 2	2	110	
		Bureau 3	2	80	
		Bureau 4	3	120	
		Total	**18**	**920**	
	1er étage	Bureau S. Sociale	3	170	Armoire 12U Armoire 12U
		Bureau S. Humaines	3	140	
		Bureau secrétariat	3	60	
		Bureau Sociologie	3	90	
		Bureau Post Grad.	3	140	
		Bureau 1	3	170	
		Bureau 2	3	140	
		Bureau 3	3	60	
		Bureau 4	3	90	
		Bureau 5	3	140	
		Total	**30**	**1200**	
	2ème étage	Bureau 1 droite	4	140	Armoire 42U et 24U Arrivée FO SM
		Bureau 2 droite	4	100	
		Bureau 3 droite Dép SH	4	100	
		Bureau 4 droite secrétariat	4	120	
		Bureau 5 droite	4	140	
		Bureau 6 droite	4	180	
		Bureau 7 droite	4	220	
		Sce enseignement	4	100	
		Chef Dép Sce Humaines	4	140	
		Bureau 1 gauche	4	140	

	Bureau 2 gauche	4	100	Armoire 24U
	Bureau 4 gauche	4	100	
	Bureau 5 gauche	4	120	
	Bureau 6 gauche spéc. Psycho	4	140	
	Bureau 7 gauche SC Dép Psycho	4	180	
	Bureau 8 gauche	4	220	
	Adjoint Chef Dép Psycho	4	100	
	Chef Dép Psycho	4	140	
	Total	**72**	**2480**	
3ème étage	Bureau 4	4	140	Armoire 42U
	Service E	4	100	
	Secrétariat Chef Section	4	100	
	Responsable Spécialité	4	120	
	Bureau 16	4	140	
	Bureau 15	4	180	
	Bureau 14	4	220	
	Section info et Comm	4	100	
	Sce enseignement	4	140	
	Salle PG	10	400	
	Salle réunion	10	500	
	Secrétariat Vice doyen	4	140	Armoire 24U
	Bureau 6	4	100	
	Bureau 7	4	100	
	Secrétariat Chef Section	4	120	
	Bureau 11	4	140	
	Section Orthophonie	4	180	
	Adjoint Chef Section Orth	4	220	
	V Doyen pédagogie	4	100	
	Bureau 9	4	140	
	Total	**92**	**3380**	
4ème étage	Bureau 4	4	140	
	Bureau 3	4	100	
	Bureau 2	4	100	
	Bureau 18	4	120	
	Bureau 17	4	140	
	Bureau 16	4	180	

		Bureau 15	4	220	Armoire 24U
		Bureau 1	4	100	
		Bureau Rédaction	4	140	
		Bureau 6	4	140	
		Bureau 7	4	100	
		Secrétariat	4	100	
		Espace chercheurs	4	120	
		Bureau 12	4	140	
		Ecole doctorale	4	180	
		Bureau 14	4	220	Armoire 24U
		Bureau des directeur LSET	4	100	
		Espace doctorant	4	140	
		Total	**72**	**2480**	
		Total	**284**	**10460**	

Bibliothèque

Bloc	Etage	Local	Prise RJ45 + noyau	Câble SFTP cat 6	Local technique et armoire
Bibliothèque	**Sous-Sol**	Salle de lecture	6	510	Source des prises 1er étage
		Banque de prêt (coté salle lecture)	2	170	
		Banque de prêt (coté salle stockage)	6	400	
		Total	**14**	**1080**	
	RDC	Salle de lecture	2	170	Source des prises 1er étage
		Banque de prêt	4	160	
		Salle de lecture	2	120	
		Salle stockage	6	200	
		Total	**14**	**650**	
	1er étage	Salle revue	2	160	Armoire 42U arrivée FO SM
		Salle informatique	2	80	
		Banque de prêt	6	180	
		Salle de stockage	4	80	
		Total	**14**	**500**	
	2ème étage	Salle lecture	2	140	
		Bureau 6	4	240	
		Bureau 1	4	240	
		Bureau 2	4	220	
		Secrétariat	4	200	
		Bureau 3	4	180	
		Bureau 4	4	160	
		Bureau 5	4	140	

		Salle réunion	4	100	Armoire 24U
		Banque de prêt	6	200	
		Stockage	4	160	
		Total	**44**	**1980**	
		Total	**86**	**4210**	

Auditorium

Bloc	Etage	Local	Prise RJ45 +noyau	Câble SFTP cat 6	Local techniques et armoire
Auditorium	S Sol	Bureau	4	260	Source des prises RDC
		Scène	5	300	
		Arrière Scène	4	260	
		Total	**13**	**820**	
	RDC	Espace Multimédia	6	500	
		Salle stockage	18	1080	
		Salle projection	2	100	
		Salle blanche	20	100	1 Armoire 42U 1 Armoire 24U Arrivée des FO SM **Switch Core n°1**
		Total	**46**	**1780**	
	1er étage	Espace Multimédia	4	300	Source des prises RDC
		Scène	5	350	
		Total	**9**	**650**	
		Total	**68**	**3250**	

IV.9 Répartition des prises par locaux au campus Tamda 2

BLOC I

Bloc	Etage	Local	Prise RJ45 + noyau	Câble SFTP cat 6	Local technique et armoire
BLOC I	S Sol	Magasin 01	4	120	Armoire 12U
		Magasin 02	4	80	
		Salle de soutenance	4	200	
		Total	**12**	**400**	
	RDC	Bureau 23,10	4	100	2Armoire 42U arrivée FO SM Armoire 42U Armoire 24U
		Bureau 24,25	4	120	
		Bureau 12,80	4	160	
		Bureau 20,10	4	180	
		Salle archives	6	240	
		Bureau 22,45	4	120	
		Bureau 23,15	4	100	
		Conseil scientifique	6	120	
		Salle informatique 1	24	1100	
		Salle informatique 2	24	850	
		Laboratoire 1	4	250	
		Laboratoire 2	4	250	
		Laboratoire 3	4	160	
		Laboratoire 4	4	180	
		Total	**100**	**3930**	
	1er étage	Bureau 23,30	4	100	Armoire 42U Armoire 42U Armoire 24U
		Bureau 17,90	4	120	
		Bureau 15,50	4	140	
		Bureau 19,87	4	160	
		Bureau 23,55	4	180	
		Bureau 19,95	4	180	
		Bureau 16,87	4	160	
		Bureau 15,50	4	140	
		Bureau 17,90	4	120	
		Bureau 19,87	4	100	
		Bureau 21,65	4	80	
		Salle informatique 3	24	960	
		Salle informatique 4	26	960	
		Salle lecture 02	2	100	
		Laboratoire 5	4	250	
		Laboratoire 6	4	250	
		Laboratoire 7	4	160	
		Laboratoire 8	4	180	

		Total	**112**	**4340**	
	2ème étage	Bureau 23,30	4	100	Armoire 42U Armoire 24U
		Bureau 17,90	4	120	
		Bureau 15,50	4	140	
		Bureau 19,87	4	160	
		Bureau 23,55	4	180	
		Bureau 19,95	4	180	
		Bureau 16,87	4	160	
		Bureau 15,50	4	140	
		Bureau 17,90	4	120	
		Bureau 19,87	4	100	
		Bureau 21,65	4	80	
		Laboratoire 9	4	250	
		Laboratoire 10	4	250	
		Laboratoire 11	4	160	
		Laboratoire 12	4	180	
		Total	**60**	**2320**	
	3ème étage	Laboratoire 13	4	250	Armoire 24U
		Laboratoire 14	4	250	
		Laboratoire 15	4	160	
		Laboratoire 16	4	180	
		Total	**16**	**840**	
	4ème étage	Laboratoire 17	4	250	Armoire 24U
		Laboratoire 18	4	250	
		Laboratoire 19	4	160	
		Laboratoire 20	4	180	
		Total	**16**	**840**	
		Total	**316**	**12670**	

BLOC H

Bloc	Etage	Local	Prise RJ45 + noyau	Câble SFTP cat 6	Local technique et armoire
BLOC H	**S Sol**	Magasin 01	2	100	Armoire 12U
		Magasin 02	2	80	
		Salle internet	4	100	
		Salle de soutenance	4	160	
		Total	**12**	**440**	
	RDC	Bureau 23,10	4	100	
		Bureau 24,25	4	120	
		Bureau 12,80	4	160	
		Bureau 20,10	4	180	2Armoire 42U arrivée FO SM
		Salle archives	6	240	
		Bureau paysage 22,45	4	120	
		Bureau paysage 23,15	4	100	

	Conseil scientifique	6	120	Armoire 42U
	Salle informatique 1	24	1100	
	Salle informatique 2	24	850	Armoire 24U
	Salle internet 2	32	1400	
	Laboratoire 1	4	250	
	Laboratoire 2	4	250	
	Laboratoire 3	4	160	
	Laboratoire 4	4	180	
	Total	**132**	**5330**	
1er étage	Bureau 23,30	4	100	
	Bureau 17,90	4	120	
	Bureau 15,50	4	140	
	Bureau 19,87	4	160	
	Bureau 23,55	4	180	
	Bureau 19,95	4	180	
	Bureau 16,87	4	160	
	Bureau 15,50	4	140	
	Bureau 17,90	4	120	
	Bureau 19,87	4	100	
	Bureau 21,65	4	80	Armoire 42U
	Salle lecture 1	2	160	
	Salle lecture 2	2	160	
	Laboratoire 5	4	250	
	Laboratoire 6	4	250	
	Laboratoire 7	4	160	Armoire 24U
	Laboratoire 8	4	180	
	Total	**64**	**2640**	
2ème étage	Bureau 23,30	4	100	
	Bureau 17,90	4	120	
	Bureau 15,50	4	140	
	Bureau 19,87	4	160	
	Bureau 23,55	4	180	
	Bureau 19,95	4	180	
	Bureau 16,87	4	160	
	Bureau 15,50	4	140	
	Bureau 17,90	4	120	
	Bureau 19,87	4	100	
	Bureau 21,65	4	80	Armoire 42U
	Laboratoire 9	4	250	
	Laboratoire 10	4	250	
	Laboratoire 11	4	160	Armoire 24U
	Laboratoire 12	4	180	
	Total	**60**	**2320**	
3ème étage	Laboratoire 13	4	250	
	Laboratoire 14	4	250	Armoire 24U

		Laboratoire 15	4	160	
		Laboratoire 16	4	180	
		Total	**16**	**840**	
	4ème étage	Laboratoire 17	4	250	Armoire 24U
		Laboratoire 18	4	250	
		Laboratoire 19	4	160	
		Laboratoire 20	4	180	
		Total	**16**	**840**	
		Total	**300**	**12410**	

Bloc Médecine

Bloc	Etage	Local	Prise RJ45 + noyau	Câble SFTP cat 6	Local technique et armoire
Bloc Médecine	**S Sol**	Bureau côté Magasin 02	4	240	Source des prises RDC
		Salle de soutenance	4	320	
		Total	**8**	**560**	
	RDC	Bureau 1	4	180	2 Armoires 42U arrivée FO SM
		Bureau 2	4	200	
		Bureau 3	4	210	
		Bureau 4	6	360	
		Bureau 5	6	200	
		Bureau 6	6	100	
		Bureau 7	4	120	
		Total	**34**	**1370**	
	1er étage	Bureau 8	4	80	Armoire 24U
		Bureau 9	4	100	
		Bureau 10	4	120	
		Bureau 11	6	300	
		Bureau 12	4	130	
		Bureau 13	4	170	
		Bureau 14	4	210	
		Bureau 15	4	240	
		Bureau 16	4	270	
		Total	**38**	**1620**	
	2ème étage	Bureau 17	4	80	Armoire 24U
		Bureau 18	4	100	
		Salle archives 1	6	250	
		Salle archives 2	6	300	
		Bureau 19	6	300	
		Salle Conseil Scientifique	10	500	
		Bureau 20	4	120	Armoire 12U
		Bureau 21	4	100	
		Bureau 22	4	80	
		Bureau 23	4	120	

		Bureau 24	4	180	
		Bureau 25	4	160	
		Total	**60**	**2290**	
	3ème étage	Salle informatique 1	24	600	Armoire 24U Armoire 24U
		Salle informatique 2	24	720	
		Salle informatique 3	24	600	
		Salle informatique 4	24	720	
		Total	**96**	**2640**	
	4ème étage	Salle lecture 1	2	120	Source des prises 3ème étage
		Salle lecture 2	2	160	
		Total	**4**	**280**	
		Total	**240**	**8760**	

Bloc Médecine 2ème partie

Bloc	Etage	Local	Prise RJ45 + noyau	Câble SFTP cat 6	Local technique et armoire
BLOC Médecine 2ème partie	**S Sol**	Laboratoire 1	4	300	Source des prises RDC
		Laboratoire 2	4	280	
		Salle de soutenance	4	280	
		Magazin01	2	140	
		Magazin02	2	160	
		Total	**16**	**1160**	
	RDC	Laboratoire 3	4	250	Armoire 24U 2 Armoires 42U arrivée FO SM
		Laboratoire 4	4	250	
		Laboratoire 5	4	180	
		Laboratoire 6	4	160	
		Bureau 1	4	180	
		Bureau 2	4	200	
		Bureau 3	4	210	
		Bureau 4	6	360	
		Bureau 5	6	200	
		Bureau 6	6	100	
		Bureau 7	4	120	
		Total	**50**	**2210**	
	1er étage	Laboratoire 7	4	250	Armoire 24U Armoire 24U
		Laboratoire 8	4	250	
		Laboratoire 9	4	180	
		Laboratoire 10	4	160	
		Bureau 8	4	80	
		Bureau 9	4	100	
		Bureau 10	4	120	
		Bureau 11	6	300	

		Bureau 12	4	130	
		Bureau 13	4	170	
		Bureau 14	4	210	
		Bureau 15	4	240	
		Bureau 16	4	270	
		Bureau 17	4	180	
		Bureau 18	4	200	
		Total	**62**	**2840**	
	2ème étage	Laboratoire 11	4	250	Armoire 24U
		Laboratoire 12	4	250	
		Laboratoire 13	4	180	
		Laboratoire 14	4	160	
		Salle Conseil Scientifique	10	500	
		Bureau 19	6	300	Armoire 24U
		Bureau 20	4	80	
		Bureau 21	4	100	
		Bureau 22	4	120	
		Bureau 23	4	160	
		Salle archives 1	6	300	
		Total	**54**	**2400**	
	3ème étage	Laboratoire 15	2	140	Source des prises 2ème étage
		Salle préparation	2	140	
		Salle lecture 1	2	120	
		Salle lecture 2	2	160	
		Total	**8**	**560**	
	4ème étage	Salle informatique 1	24	720	2Armoire 42U
		Salle informatique 2	24	600	
		Salle informatique 3	24	720	
		Salle informatique 4	24	1080	
		Total	**96**	**3120**	
		Total	**286**	**12290**	

BLOC ST

Bloc	Etage	Local	Prise RJ45 + noyau	Câble SFTP cat 6	Local technique et armoire
BLOC ST	**Sous-Sol supérieur**	Salle de soutenance	4	280	Source des prises RDC
		Total	**4**	**280**	
	RDC	Bureau 4	4	160	Armoire 24U
		Bureau 5	4	140	
		Bureau 6	4	120	
		Bureau 7	4	100	

	Bureau 8	4	120	Armoire 24U
	Bureau 9	4	140	
	Bureau 10	4	160	
	Bureau 11	4	160	
	Bureau 12	4	140	
	Bureau 13	4	120	
	Bureau 14	4	100	
	Salle de cours 1	2	100	
	Salle de séminaire 1	6	360	
	Salle de séminaire 2	6	200	Armoire 24U
	Total	**58**	**2120**	
1er étage	Salle archives 1	8	520	2 Armoires 42U arrivée FO SM
	Bureau 15	4	220	
	Bureau 16	4	200	
	Bureau 17	4	180	
	Bureau 18	4	160	
	Bureau 19	4	140	
	Bureau 20	4	120	
	Bureau 21	4	160	
	Bureau 22	4	140	
	Bureau 23	4	120	
	Bureau 24	4	100	
	Salle de cours 3	10	500	
	Salle de cours 4	32	1400	
	Salle Conseil Scientifique	6	180	Armoire 42U
	Total	**96**	**4140**	
2ème étage	Salle archives 2	6	240	Armoire 42U
	Bureau 25	4	140	
	Bureau 26	4	120	
	Bureau 27	4	100	
	Bureau 28	4	120	
	Bureau 29	4	140	
	Bureau 30	4	160	
	Bureau 31	4	120	
	Bureau 32	4	120	
	Bureau 33	4	140	
	Bureau 34	4	160	
	Secrétariat	4	200	
	Bureau Doyen	4	240	
	Bureau 35	4	160	
	Bureau 36	4	140	
	Bureau 37	4	120	
	Bureau 38	4	100	Armoire 42U
	Bureau 39	4	120	

		Bureau 40	4	140	
		Bureau 41	4	180	
		Bureau 42	4	160	
		Bureau 43	4	160	
		Bureau 44	4	140	
		Bureau 45	4	160	
		Bureau 46	4	180	
		Bureau 47	4	260	
		Bureau 48	4	240	
		Total	**110**	**4260**	
	Sous-Sol inférieur	Salle informatique 1	4	260	Armoire 24U
		Salle informatique 2	4	100	
		Salle informatique 3	4	240	
		Salle informatique 4	4	300	
		Total	**16**	**900**	
		Total	**284**	**11700**	

Nouvelle Bibliothèque

Bloc	Etage	Local	Prise RJ45 + noyau	Câble SFTP cat 6	Local technique et armoire
Nouvelle Bibliothèque	**Sous-Sol**	Local service téléphonie	4	320	Armoire 24U
		Atelier maintenance des équipements	6	420	
		Service Thèses	6	420	
		Office Publication Universitaire	6	200	
		Restauration et entretien des livres	4	280	
		Dépôt arrivée des livres	6	200	
		Service entretien	4	140	
		Bureau chef de service traitement	4	100	
		Bureau service traitement	4	100	
		Bureau du service acquisition	4	160	
		Total	**48**	**2340**	
	RDC	Salle des catalogues et	20	700	

		fichiers informatisés			Armoire 42U arrivée FO SM **Switch Core n°2**
		Archive	4	100	
		Atelier photocopie et reliure	6	240	Armoire 12U
		Salle de prêt et de retour	4	200	
		Stockage et rayonnage des livres	4	180	
		Bureau 1	4	120	
		Atelier de maintenance informatique	6	120	
		Total	**48**	**1660**	
	1er étage	Salle périodiques	6	400	Armoire 42U Armoire 24U
		Bureau pour bibliothécaires	6	360	
		Salle de lecture	4	200	
		Salle informatique	48	1500	
		Salle internet	30	900	
		Bureau sécurité et surveillance	4	200	
		Total	**98**	**3560**	
	2ème étage	Salle lecture enseignants	2	140	Armoire 42U
		Bureau chef de service bibliothèque	4	240	
		Bureau 2	4	280	
		Bureau du service prêt entre bibliothèques	6	420	
		Salle lecture	2	120	
		Salle internet enseignants	30	1100	
		Salle réunion	10	500	
		Bureau 3	4	200	
		Secrétariat	4	260	
		Bureau Directeur	4	280	
		Total	**70**	**3540**	
		Total	**264**	**11100**	

IV.10 Plan d'adressage

Une fois l'ensemble du matériel en place et la répartition par bloc et étages réalisée, nous devons nous intéresser à l'adressage IP.
Pour avoir un bon plan d'adressage au campus Tamda, nous avons choisi de découper le réseau en utilisant l'adresse de classe A.

Dans le tableau ci-dessous, nous avons représenté l'emplacement et les caractéristiques des équipements ainsi que les adresses IP utilisées.

Equipements	Nombre de switches	Localisation	Adresses IP
TAMDA 01 / BLOC A			
CISCO Catalyst 9300	**01**	BLOC A **ETAGE 02** TAMDA 01	**10.10.100.1**
CISCO Catalyst 1000	**01**	BLOC A ETAGE RDC TAMDA 01	**10.10.100.10**
CISCO Catalyst 1000	**03**	BLOC A ETAGE 01 TAMDA 01	**10.10.100.11** **10.10.100.12** **10.10.100.13**
CISCO Catalyst 1000	**03**	BLOC A ETAGE 02 TAMDA 01	**10.10.100.20** **10.10.100.21** **10.10.100.22**
CISCO Catalyst 1000	**03**	BLOC A ETAGE 03 TAMDA 01	**10.10.100.30** **10.10.100.31** **10.10.100.33**
CISCO Catalyst 1000	**01**	BLOC A ETAGE 04 TAMDA 01	**10.10.100.40**

Equipements	Nombre de switches	Localisation	Adresses IP
TAMDA 01 / BLOC B			
CISCO Catalyst 9300	**01**	BLOC B **ETAGE 02** TAMDA 01	**10.10.100.2**
CISCO Catalyst 1000	**01**	BLOC B ETAGE 01 TAMDA 01	**10.10.100.50**
CISCO Catalyst 1000	**05**	BLOC B ETAGE 02 TAMDA 01	**10.10.100.60** **10.10.100.61** **10.10.100.62** **10.10.100.63** **10.10.100.64**
CISCO Catalyst 1000	**04**	BLOC B ETAGE 03 TAMDA 01	**10.10.100.70** **10.10.100.71** **10.10.100.72** **10.10.100.73**
CISCO Catalyst 1000	**01**	BLOC B ETAGE 04 TAMDA 01	**10.10.100.80**

Equipements	Nombre de switches	Localisation	Adresses IP
TAMDA 01 / BLOC C			
CISCO Catalyst 9300	**01**	BLOC C **ETAGE 03** TAMDA 01	**10.10.100.3**
CISCO Catalyst 1000	**01**	BLOC C ETAGE RDC TAMDA 01	**10.10.100.90**
CISCO Catalyst 1000	**03**	BLOC C ETAGE 02 TAMDA 01	**10.10.100.100** **10.10.100.101** **10.10.100.102**
CISCO Catalyst 1000	**04**	BLOC C ETAGE 03 TAMDA 01	**10.10.100.110** **10.10.100.111** **10.10.100.112** **10.10.100.113**

Equipements	Nombre de switches	Localisation	Adresses IP
TAMDA 01 / BLOC D			
CISCO Catalyst 9300	**01**	BLOC D **ETAGE 03** TAMDA 01	**10.10.100.4**
CISCO Catalyst 1000	**01**	BLOC D ETAGE RDC TAMDA01	**10.10.100.130**
CISCO Catalyst 1000	**02**	BLOC D ETAGE 02 TAMDA 01	**10.10.100.140** **10.10.100.141**
CISCO Catalyst 1000	**03**	BLOC D ETAGE 03 TAMDA 01	**10.10.100.150** **10.10.100.151** **10.10.100.152**
CISCO Catalyst 1000	**04**	BLOC D ETAGE 04 TAMDA 01	**10.10.100.160** **10.10.100.161** **10.10.100.162** **10.10.100.161**

Equipements	Nombre de switches	Localisation	Adresses IP
TAMDA 01 / BLOC E PATIE PEDAGOGIQUE			
CISCO Catalyst 9300	**01**	BLOC E **ETAGE 02** TAMDA 01	**10.10.100.5**
CISCO Catalyst 1000	**01**	BLOC E ETAGE SOU-SOL TAMDA 01	**10.10.100.170**
CISCO Catalyst 1000	**02**	BLOC E ETAGE 02 TAMDA01	**10.10.100.171** **10.10.100.172**

Equipements	Nombre de switches	Localisation	Adresses IP
TAMDA 01 / BLOC E PARTIE ADMINISTRATIVE			
CISCO Catalyst 9300	**01**	BLOC E - 2 **ETAGE 02** TAMDA 01	**10.10.100.6**
CISCO Catalyst 1000	**02**	BLOC E – 2 ETAGE 01 TAMDA 01	**10.10.100.180** **10.10.100.181**
CISCO Catalyst 1000	**04**	BLOC E - 2 ETAGE 02 TAMDA 01	**10.10.100.190** **10.10.100.191** **10.10.100.192** **10.10.100.193**
CISCO Catalyst 1000	**05**	BLOC Administratif- ETAGE 03 TAMDA01	**10.10.100.200** **10.10.100.201** **10.10.100.202** **10.10.100.203** **10.10.100.204**
CISCO Catalyst 1000	**04**	BLOC Administratif- ETAGE 04 TAMDA01	**10.10.100.210** **10.10.100.211** **10.10.100.212** **10.10.100.213**

Equipements	Nombre de switches	Localisation	Adresses IP
TAMDA 01 / BIBLIOTHEQUE			
CISCO Catalyst 9300	**01**	Bibliothèque **ETAGE 01** TAMDA 01	**10.10.100.7**
CISCO Catalyst 1000	**02**	Bibliothèque ETAGE 01 TAMDA 01	**10.10.100.220** **10.10.100.221**
CISCO Catalyst 1000	**02**	Bibliothèque ETAGE 02 TAMDA 01	**10.10.100.230** **10.10.100.231**

Equipements	Nombre de switches	Localisation	Adresses IP
TAMDA 01 / AUDITORIUM			
CISCO Catalyst 9400 Switch Core	**01**	Auditorium **ETAGE RDC** TAMDA 01	
CISCO Catalyst 1000	**02**	Auditorium ETAGE RDC TAMDA 01	**10.10.100.240** **10.10.100.241**

IV.11 La réalisation des VLANs

La création de réseaux locaux virtuels permettra de créer sur le même commutateur plusieurs réseaux indépendants, ne pouvant pas communiquer, par défaut, entre eux.

Ci-dessous le tableau des Vlan définis, il s'agit principalement d'une segmentation du réseau en plusieurs domaine de broadcast en utilisant la technologie des Vlans.

Vlan de gestion	10.10.100.0/24 Le rang 10.10.100.1-9 réservé pour les Switch de distribution) Le reste pour les Switch d'accès (un rang de 10 adresses par étage)
Résumé de route	10.10.0.0/16
ID VLAN	CAMPUS+BLOC+ETAGE Exemple : - CAMPUS 1 BLOC B ETAGE 1 ID VLAN : 121
Switch hostname	CAMPUS+BLOC+ETAGE+ARMOIRE+NUMERO SEQUENTIEL Exemple : - CAMPUS 1 BLOC A ETAGE 3 ARMOIRE 2 SWITCH 4 Hostname : T1BAE3AR2S4

CAMPUS TAMDA 1			
BLOC	**ETAGE**	**ID VLAN**	**IP VLAN**
bloc a (bloc 01) 10.10.8.0/22	RDC	111	10.10.8.0/24
	1		
	2	112	10.10.9.0/24
	3	113	10.10.10.0/24
	4	114	10.10.11.0/24
bloc b (bloc 02) 10.10.12.0/22	1	121	10.10.12.0/24
	2	122	10.10.13.0/24
	3	123	10.10.14.0/24
	4	124	10.10.15.0/24
bloc c (bloc 03) 10.10.16.0/22	RDC	131	10.10.16.0/24
	2	132	10.10.17.0/24
	3	133	10.10.18.0/24
	4	134	10.10.19.0/24

CAMPUS TAMDA 1			
BLOC	**ETAGE**	**ID VLAN**	**IP VLAN**
bloc d (bloc 04) 10.10.20.0/22	RDC	141	10.10.20.0/24
	2	142	10.10.21.0/24
	3	143	10.10.22.0/24
	4	144	10.10.23.0/24
bloc e (bloc 05) 10.10.24.0/22	SOU-SOL	151	10.10.24.0/24
	2	152	10.10.25.0/24
bloc administratif (bloc 06) 10.10.28.0/22	1	161	10.10.28.0/24
	2	162	10.10.29.0/24
	3	163	10.10.30.0/24
	4	164	10.10.31.0/24
bibliothèque (bloc 07) 10.10.32.0/22	1	171	10.10.32.0/24
	2	172	10.10.33.0/24
auditorium (bloc 08) 10.10.36.0/22	RDC	181	10.10.36.0/24

La même politique de nommage et plan d'adressage ont été utilisés pour le campus Tamda 2

IV.12 Configuration des équipements

IV.12.1 Mode Trunk

Un port trunk sur un switch, est un port qui permet le passage de flux Ethernet taggués avec des IDs VLAN qu'on veut laisser passer sur ce port.
Tous les ports à connecter aux switches accès(L2), seront mis en mode Trunk.

```
SWITCH# configure terminal
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# Switchport mode trunk
```

Pour limiter les VLAN autorisés à communiquer sur un port Trunk :

```
SWITCH# configure terminal
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# Switchport trunk allowed vlan 10-12
```

IV.12.2 Accès à distance aux équipements

Afin de permettre l'accès à distance aux équipements, le protocole SSH sera configuré sur tous les équipements de réseau.
Le tableau suivant définit les informations concernant la partie accès sur les équipements :

Enable Secret	*******	
User	**password**	**privilège**
Xxxxx	******	15

Ci-dessous un exemple de configuration SSHv2

```
SWITCH# configure terminal
SWITCH(config)# Enable secret xxxxx
SWITCH(config)# Hostname xxxx
SWITCH(config)# ip domain-name xxxx.xx
SWITCH(config)# username xxxx password ******* privilege 15
SWITCH(config)# crypto key generate rsa
1024
SWITCH(config)# ip ssh version 2
!
SWITCH(config)# line vty 0 15
SWITCH(config-line)# transport input ssh
SWITCH(config-line)# exec-timeout 5 0
```

```
!
```

IV.12.3 Message Banner

Le message BANNER est un message présenté à un utilisateur qui tente de se connecte sur un SWITCH Cisco. La plupart des administrateurs de réseau l'utilisent pour afficher des avis légaux concernant l'accès au commutateur, comme l'accès non autorisé à ce périphérique est interdit et les contrevenants seront poursuivis en justice.

Ci-dessous un exemple de configuration d'une bannière

```
SWITCH# configure terminal
SWITCH(config)#
banner motd ^
        ********************************************************************
        ********************************************************************
                                Cet équipement est la propriété
                                de Université de TIZI OUZOU
                                Toute Tentative d'accès sans autorisation
                                sur cet équipement
                                est strictement interdite

        ********************************************************************
        ********************************************************************
^
```

IV.12.4 Configuration complète du switch de distribution CISCO 9300 T1B2E2AR1SD

```
conf t
hostname T1B2E2AR1SD

enable secret UMMTO@2024

interface Vlan1
 no ip address
 shutdown
exit

interface Vlan100
ip address 10.10.100.2 255.255.255.0
no shut

exit

ip default-gateway 10.10.100.254

vlan 100
 name Management

vlan 121
 name vlan_121

vlan 122
 name vlan_122

vlan 123
```

```
 name vlan_123

vlan 124
 name vlan_124

exit

no ip domain lookup

ip domain name TIZI.com

crypto key generate rsa

username admin privilege 15  password UMMTO@2024

Line vty 0 4
 Transport input ssh
 login local
exit


banner motd ^
**************************************************************
**************************************************************
     Toute Tentative d'accès sans autorisation
     Sur cet équipement est strictement interdite

**************************************************************
**************************************************************
^

interface GigabitEthernet1/0/24
switchport mode trunk
switchport trunk allowed vlan add 100

exit

interface range GigabitEthernet1/0/1-23
switchport mode trunk
switchport trunk allowed vlan add 100,121-124

exit

Interface vlan 121
Ip address 10.10.12.254 255.255.255.0
No shut

Interface vlan 122
Ip address 10.10.13.254 255.255.255.0
No shut
```

```
Interface vlan 123
Ip address 10.10.14.254 255.255.255.0
No shut

Interface vlan 124
Ip address 10.10.15.254 255.255.255.0
No shut

ip dhcp excluded-address 10.10.12.1 10.10.12.20

ip dhcp pool VLAN121
 network 10.10.12.0 255.255.255.0
 default-router 10.10.12.254
 dns-server 8.8.8.8 4.2.2.2

ip dhcp excluded-address 10.10.13.1 10.10.13.20

ip dhcp pool VLAN122
 network 10.10.13.0 255.255.255.0
 default-router 10.10.13.254
 dns-server 8.8.8.8 4.2.2.2

ip dhcp excluded-address 10.10.14.1 10.10.14.20

ip dhcp pool VLAN123
 network 10.10.14.0 255.255.255.0
 default-router 10.10.14.254
 dns-server 8.8.8.8 4.2.2.2

ip dhcp excluded-address 10.10.15.1 10.10.15.20

ip dhcp pool VLAN124
 network 10.10.15.0 255.255.255.0
 default-router 10.10.15.254
 dns-server 8.8.8.8 4.2.2.2

exit
!
do wr
```

IV.12.5 Configuration complète du switch d'accès CISCO 1000 T1B2E3AR2S1

```
conf t
hostname T1B2E3AR2S1

enable secret UMMTO@2024

interface Vlan1
 no ip address
 shutdown
exit

interface Vlan100
ip address 10.10.100.71 255.255.255.0
no shut

exit

ip default-gateway 10.10.100.254

vlan 100
 name Management

vlan 123
name vlan_123

no ip domain lookup

ip domain name TIZI.com

crypto key generate rsa

username admin privilege 15  password UMMTO@2024

Line vty 0 4
 Transport input ssh
 login local
exit


banner motd ^
**********************************************************************
**********************************************************************
     Toute Tentative d'accès sans autorisation
     Sur cet équipement est strictement interdite
**********************************************************************
**********************************************************************
^

Interface range GigabitEthernet1/0/25-28
```

```
switchport mode trunk
switchport trunk allowed vlan add 100,123

exit

interface range GigabitEthernet1/0/1-24
switchport  access vlan 123

exit

do wr
```

IV.13 Prévisions et suggestions futures

Campus Tamda de 10.000 places pédagogiques

Il est à signaler qu'un nouveau campus de 10.000 places pédagogiques sera bientôt réceptionné par notre université à Tamda. A cet effet, nous avons prévu un câble de fibre optique monomode qui reliera les équipements d'Algérie Télécom à ce nouveau campus en passant par le Firewall Sophos XG650.

Téléphonie IP

Le réseau informatique du campus Tamda sera réalisé en respectant les normes en la matière. Il serait dommage de ne pas y inclure la téléphonie IP.
En effet, puisque ce réseau couvre l'ensemble des locaux du campus, il suffirait d'acquérir un IPBX et les terminaux pour bénéficier des avantages de la téléphonie IP.

Points d'accès Wifi Outdoor

Compte tenu du fait que les campus Tamda 1 et 2 occupent une superficie très importante et qu'avec la réception des 10
.000 nouvelles places pédagogiques ça sera encore plus vaste avec beaucoup d'espaces où les étudiants pourront réviser ou tout simplement prendre une pause détente, il serait intéressant d'acquérir des points d'accès extérieurs (Outdoor) pour leur permettre d'avoir accès au réseau et à Internet même depuis l'extérieur.

Centralisation de la gestion des points d'accès Wifi

Il n'est pas évident de gérer les quarante points d'accès Wifi déjà prévus (nombre qui pourrait évoluer). La gestion centralisée des points d'accès Wifi à partir d'une même interface simplifierait les tâches telles que la configuration des paramètres du réseau, le déploiement des mises à jour logicielles et la surveillance des performances du réseau.

Solution Active Directory

Il existe plusieurs avantages à la mise en place d'Active Directory. En centralisant les données des utilisateurs et des différents équipements informatiques, ce service contribue à sécuriser le réseau. Les administrateurs peuvent définir les autorisations d'accès des utilisateurs ou groupes

d'utilisateurs aux différentes ressources et logiciels. Active Directory offre également des fonctionnalités permettant de gérer plus facilement les installations de logiciels et leurs mises à jour sur l'ensemble du réseau. [14]

Réseau de caméras IP

Le réseau conçu au campus Tamda couvre l'ensemble des blocs et des espaces administratifs et pédagogiques. Il serait très intéressant d'y intégrer un réseau de caméras IP qui seront directement reliées aux switches PoE sans avoir besoin de les relier au réseau électrique. On aura ainsi un centre de contrôle centralisé ou on pourra accéder aux différentes caméras à partir d'un seul terminal.

IV.14 Conclusion

Des tests de connexion sont faits au niveau des équipements :

- Les soudures des bruns de fibre optique ont été testées et contrôlées ;
- Des tests de Ping ont été effectués entre les blocs et entre les étages de chaque bloc ;
- Des tests de débit ont été effectués :

La réalisation du réseau informatique au campus Tamda permettra aux 25.000 étudiants qui fréquentent ce campus ainsi qu'à leurs enseignants et à l'administration d'avoir accès à Internet à haut débit. Ceci permettra d'apporter un plus considérable à la pédagogie notamment au niveau des laboratoires et salles informatique pour les étudiants des spécialités techniques.

La répartition des prises au niveau de tous les locaux du campus permettra également à l'administration de travailler dans de meilleures conditions, notamment à l'ère de l'administration numérique.

Les points d'accès Wifi installés pour la plupart au niveau des bibliothèques et salles de lecture offriront plus de confort aux étudiants qui souhaitent se connecter avec leur laptop, tablette ou smartphone.

L'interconnexion des blocs en fibre optique monomode ainsi que les colonnes montantes réalisées en fibre optique multimode permettra d'avoir un trafic fluide et surtout d'éviter les perturbations, notamment au niveau des laboratoires techniques équipés d'appareils électroniques et de moteurs qui causent d'importantes interférences avec les câbles en cuivre.

Conclusion générale :

La conception d'un réseau campus sécurisé constitue un élément crucial dans le paysage technologique actuel, où les universités doivent faire face aux défis grandissants en matière de sécurité des données et des systèmes. Dans cette étude, nous avons examiné les divers aspects de cette conception, en soulignant les éléments clés et les méthodes les plus efficaces pour garantir un environnement réseau sécurisé et fiable.

Les tests effectués lors des simulations Packet Tracer et sur terrain montrent la fluidité du trafic dans le réseau déployé à travers les différents équipements actifs. Les 23 ligne FTTH de 100Mbps chacune permettent d'avoir une bande passante de 2,3 Gbps au niveau des deux switches Core.

L'infrastructure réseau réalisée en fibre optique permet également d'avoir une meilleure qualité ainsi qu'un trafic fiable qui ne peut être perturbé par les interférences des nombreux appareils, moteurs et bobines qui se trouvent notamment au niveau des laboratoires.

Il a été observé que la sécurité d'un réseau campus ne se résume pas uniquement à l'installation de pare-feu et de systèmes de détection des intrusions, mais qu'elle inclut également une approche globale, comprenant des éléments tels que la segmentation du réseau, la gestion des identités et des accès, ainsi que la surveillance continue.

Les universités peuvent renforcer la sécurité de leur réseau campus en adoptant une approche proactive et en anticipant les menaces potentielles, ce qui permet de diminuer les risques de violations de données et de perturbations des opérations.

Néanmoins, il est primordial de prendre conscience que la sécurité est un processus continu et évolutif. Les risques sont en constante évolution, ce qui nécessite une adaptation des stratégies de sécurité en conséquence. Ainsi, les universités et leurs services IT doivent rester attentives, rester à jour sur les tendances et les technologies les plus récentes en matière de sécurité, et investir dans la formation et le développement des compétences de leur personnel.

En résumé, la conception d'un réseau campus sécurisé est un élément fondamental pour garantir la confidentialité, l'intégrité et la disponibilité des données et des systèmes au sein de l'université. En instaurant des politiques et des technologies adéquates, et en adoptant une approche proactive, les services IT peuvent renforcer le niveau de sécurité de leur établissement et se prémunir de manière plus efficace contre les nouvelles menaces.

Références bibliographiques

[1] « IONOS | Hébergeur Web » Domaines, mails et sites Web ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.ionos.fr/
[2] « ELITE TRI ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://elitetri.blogspot.com/
[3] « Enssib | École nationale supérieure des sciences de l'information et des bibliothèques ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.enssib.fr/
[4] « cisco.goffinet.org ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://cisco.goffinet.org/
[5] Pr. DAOUI Mehammed, « Examen professionnel », 2020.
[6] « Les causeries d'Au Poste | Au Poste média libre & indépendant ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.auposte.fr/
[7] « Le Monde Informatique : actualités, dossiers et tendances IT ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.lemondeinformatique.fr/
[8] « Particulier | CNIL ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.cnil.fr/fr
[9] « TLS vs SSL : Comprendre les Différences et l'Importance de la Sécurité des Protocoles de Communication Web ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.leptidigital.fr/securite-informatique/tls-vs-ssl-44867/
[10] « Les outils de sécurisation d'applications web dans l'informatique en nuage (cloud) | CNIL ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.cnil.fr/fr/les-outils-de-securisation-dapplications-web-dans-linformatique-en-nuage-cloud
[11] « L'évolution du rôle du RSSI en 2024 ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.journaldunet.com/cybersecurite/1527527-l-evolution-du-role-du-rssi-en-2024/
[12] « Université de Tizi Ouzou — Wikipédia ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://fr.wikipedia.org/wiki/Universit%C3%A9_de_Tizi_Ouzou
[13] « One-stop Optical Network Solution Provider | FiberMall ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.fibermall.com/
[14] « Active Directory : définition, avantages et différence avec le LDAP ». Consulté le: 7 juin 2024. [En ligne]. Disponible sur: https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203425-active-directory-definition-avantages/

[1] https://damsak.medium.com/evolution-of-client-server-architecture-and-web-servers-cd58f60436f7
[2] https://www.cyberagentsinc.com/2018/09/14/peer-to-peer-networks/
[3] https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/
[4] https://zestedesavoir.com/tutoriels/2789/les-reseaux-de-zero/le-concept-et-les-bases/les-topologies/
[5] https://jharaphula.com/types-of-network-topology-diagram/
[6] https://www.researchgate.net/figure/Topologie-maillee-Topologie-arborescente-offre-des-liens-dedies-qui-permettent-de_fig6_350340759
[7] https://www.vedantu.com/coding-for-kids/types-of-networks
[8] https://www.informatique-mania.com/linternet/red-lan/
[9] https://forum.huawei.com/enterprise/en/wan-basics-introduction-of-the-wan-network/thread/667246517406285824-667213852955258880
[10] https://muhamadridwan-jarkom.blogspot.com/2020/03/tugas-kuliah-jaringan-komputer.html

[11] https://mrproof.blogspot.com/2010/10/les-reseaux-informatiques-introduction.html
[12] https://www.amazon.ca/Sg102-24-Compact-24port-Gigabit-Switch/dp/B007I59CN6
[13] https://www.minitool.com/lib/ethernet-hub.html
[14] https://www.amazon.co.uk/CISCO-SYSTEMS-RV340-K9-G5-RV340-ROUTER/dp/B06XSDWGVJ
[15] https://www.darty.com/nav/achat/informatique/reseau/carte_reseau/d-link_carte_pci_ethernet_dfe-528tx.html
[16] https://www.uniformatic.fr/point-d-acces-wifi-interieur-poe-300-mbps-24ghz-2x3dbi-c2x29822817
[17] https://www.guiahardware.es/cable-coaxial-que-es-como-funciona/
[18] https://tpemlpjvdp.weebly.com/quels-supports-de-transmission-pour-transfeacuterer-mes-donneacutees.html
[19] https://www.m2optics.com/blog/what-is-optical-fiber
[20] https://forum.huawei.com/enterprise/en/differences-between-unicast-multicast-and-broadcast/thread/667243781264654336-667213852955258880
[21] https://elitetri.blogspot.com/2012/06/les-7-couches-osi.html
[22] https://which-cameratobuy.blogspot.com/2017/04/7-couches-osi.html
[23] https://eventus-networks.blogspot.com/2013/11/lencapsulation.html
[24] https://si.blaisepascal.fr/1t-tcp-ip/
[25] https://zestedesavoir.com/tutoriels/2789/les-reseaux-de-zero/un-modele-qui-en-tient-une-couche/ils-en-tiennent-une-couche-osi-et-tcp-ip/
[26] https://cisco.goffinet.org
[27] https://www.kolmaa3rif.com/2019/10/protocoles-routage-dynamique.html#google_vignette
[28] https://www.cloudns.net/blog/arp-address-resolution-protocol-why-is-it-important/
[29] https://www.ques10.com/p/37853/draw-and-discuss-the-ethernet-frame-format-1/#google_vignette
[30] https://webresources.ruckuswireless.com/datasheets/h320/ds-ruckus-h320-fr.html
[31] https://mapetiteentreprise.net/comment-assurer-la-securite-de-vos-reseaux-en-entreprise/
[32] https://special-it.fr/attaque-par-deni-service-dos-ddos/#google_vignette
[33] https://simplycit.ch/post/code-malveillant-distribue-via-les-certificats-d-link
[34] https://trungtambaohanh.com/products/trojan-la-gi-cach-phong-tranh-virus-trojan-xam-nhap-may-tinh-hieu-qua
[35] https://hanatech.ca/news/what-are-ransomwares/
[36] https://visionarymarketing.com/fr/2023/05/08/phishing-comment-proteger-son-entreprise-du-hameconnage/
[37] https://www.hsc.fr/attaque-man-in-the-middle/
[38] https://www.nameshield.com/ressources/lexique/spoofing/
[39] https://www.le-vpn.com/fr/quest-ce-usurpation-didentite/
[40] https://vpnactu.fr/securite-informatique-le-pare-feu-integre-suffit-il-reellement/
[41] https://www.edox.com
[42] https://the-networking-space.blogspot.com/2011/07/ids-ips.html
[43] https://www.zenarmor.com/docs/network-security-tutorials/what-is-dmz
[44] https://www.technomedia.org/2019/07/quelle-technologie-choisir-pour.html

Mots clés

Informatique, Réseaux, Télécommunications, Commutateurs, Switches, Cybersécurité, Hack, Failles, Firewall, Pare-feu, LAN, VLAN, CISCO, Fibre optique, Configuration, Trafic, Données, ACL, Sécurité, TCP/IP, OSI.

Résumé

Les réseaux informatiques jouent un rôle crucial dans la connectivité et la communication modernes, notamment dans le domaine de l'éducation, de l'enseignement et de la recherche scientifique. L'efficacité et la performance des réseaux sont des éléments clés pour assurer un fonctionnement optimal des systèmes informatiques. Dans ce mémoire, nous allons nous intéresser à l'étude et la conception d'un réseau informatique sécurisé au sein d'un campus universitaire, en l'occurrence, le campus Tamda de l'Université de Tizi-Ouzou.

Dans un contexte de numérisation des administrations en général et des universités en particulier, le besoin de réseaux rapides et fiables est en constante augmentation. Les universités font face à des défis significatifs pour maintenir des performances élevées tout en gérant la charge croissante des utilisateurs et des applications. Cette étude se concentre sur l'identification de la problématique au niveau du campus et sur la proposition de solutions pour surmonter ces obstacles.

L'objectif principal de ce mémoire est de concevoir un réseau informatique de type réseau campus au niveau de Tamda, de réaliser des interconnexions en fibre optique entre les blocs pédagogiques et de mettre en place une architecture réseau qui puisse répondre au besoin exprimé. Il faudra aussi que la solution proposée permette aux utilisateurs d'avoir accès à Internet en haut débit et de bénéficier des avantages d'un réseau local.

Pour atteindre ces objectifs, un plan fibre optique représentant l'interconnexion des blocs sera mis en place, ainsi que des colonnes montantes à l'intérieur des immeubles. Une répartition équitable et selon les besoins sera réalisée en ce qui concerne la mise en place des équipements actifs.

Nous soulignerons également dans ce mémoire le coté sécurité des réseaux et nous adopterons une solution permettant de garantir la disponibilité, la confidentialité et l'intégrité des données des utilisateurs. Dans cette partie, nous allons nous intéresser particulièrement à la configuration des commutateurs CISCO, à la mise en place de VLANs, des ACL ainsi que de l'activation de l'accès à distance sécurisé SSHv2.

Enfin, une simulation sera réalisée sur CISCO Packet Tracer en mettant en place le modèle réseau adopté. Plusieurs accès seront réalisés, notamment d'un terminal à un autre au niveau du campus, du réseau local vers Internet, d'Internet vers un service web hébergé à l'intérieur du campus et enfin les tests des différents VLANs.

En conclusion, ce mémoire a mis en lumière l'importance critique de la configuration et de l'optimisation des réseaux informatiques pour répondre aux exigences croissantes de performances et de fiabilité. Nous soulèverons plusieurs suggestions, telles que l'intégration de la téléphonie IP et les caméras de surveillance IP au réseau réalisé. Les recommandations formulées peuvent servir de guide pratique pour les administrateurs réseau et les décideurs cherchant à améliorer l'efficacité opérationnelle et à optimiser les investissements en infrastructure informatique.

Abstract

Computer networks play a crucial role in modern connectivity and communication, especially in education, teaching and scientific research. Network efficiency and performance are key elements to ensure optimal functioning of IT systems. In this dissertation, we will focus on the study and design of a secure computer network within a university campus, in this case, the Tamda campus of the University of Tizi-Ouzou.

In a context of digitalization of administrations in general and universities in particular, the need for fast and reliable networks is constantly increasing. Universities face significant challenges in maintaining high performance while managing increasing user and application load. This study focuses on identifying the problem at the campus and proposing solutions to overcome these obstacles.

The main objective of this dissertation is to design a campus network type computer network at Tamda, to create optical fiber interconnections between the educational blocks and to set up a network architecture that can meet the expressed need. The proposed solution will also need to allow users to have high-speed Internet access and benefit from the advantages of a local network.

To achieve these objectives, a fiber optic plan representing the interconnection of the blocks will be put in place, as well as riser columns inside the buildings. An equitable distribution according to needs will be carried out with regard to the installation of active equipment.

We will also highlight in this report the security side of networks and we will adopt a solution to guarantee the availability, confidentiality and integrity of user data. In this part, we will focus particularly on the configuration of CISCO switches, the establishment of VLANs, ACLs as well as the activation of SSHv2 secure remote access.

Finally, a simulation will be carried out on CISCO Packet Tracer by implementing the adopted network model. Several accesses will be made, in particular from one terminal to another at the campus level, from the local network to the Internet, from the Internet to a web service hosted inside the campus and finally the tests of the different VLANs.

In conclusion, this dissertation has highlighted the critical importance of configuring and optimizing computer networks to meet increasing performance and reliability requirements. We will raise several suggestions, such as integrating IP telephony and IP surveillance cameras into the network. The recommendations provided can serve as a practical guide for network administrators and decision-makers seeking to improve operational efficiency and optimize IT infrastructure investments.

Outils et logiciels utilisés

Plusieurs outils ont été utilisés pour la réalisation de ce mémoire y compris le stage pratique. Les plus importants sont listés ci-dessous :