République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira - Béjaïa

Faculté des Sciences Exactes
Département d'Informatique

Projet de Fin d'Études

Pour l'obtention du diplôme de Master en Informatique

Spécialités : Administration et Sécurité des Réseaux & Réseaux et Sécurité

Thème

Analyse et Optimisation des Performances du Réseau LAN Cas d'étude Cevital

Préparé par :
HOCINI Ilyas
IDRISSOU Ayoub

Encadré par :
Dr. Bachiri Lina

Coencadrant industriel :
M. Slimani Mennad (Cevital)

Membres du jury :

Mme. Aloui Soraya ..	**MCA** (Présidente)
Mme. Zamouche Djamila	**MCB** (Examinatrice)
Mme. Yaici Malika ...	**MCB** (Examinatrice)
Mme. Mameri Souhila .	**MCB** (Examinatrice)

Année universitaire : 2024 – 2025

Remerciements

Au terme de ce travail, nous tenons à exprimer nos sincères remerciements à toutes les personnes qui nous ont accompagnés et soutenus tout au long de notre parcours universitaire, ainsi que durant la réalisation de ce mémoire.

Nous remercions particulièrement Madame **Bachiri Lina**, notre encadrante de mémoire, pour son suivi rigoureux, sa disponibilité constante et ses conseils méthodiques qui ont grandement contribué à la qualité de ce travail. Son encadrement précis et bienveillant a été un véritable atout tout au long de ce projet.

Nos remerciements vont également à Monsieur **Mennad Slimani**, notre encadrant de stage au sein de l'entreprise **Cevital**, pour son accueil chaleureux, son accompagnement professionnel, ainsi que la richesse de ses conseils techniques et pratiques, qui ont permis de donner une dimension concrète et opérationnelle à notre étude.

Nous tenons aussi à exprimer toute notre gratitude à Madame **Hamza Lamia**, notre enseignante et encadrante pédagogique tout au long de notre parcours de licence et de notre projet de fin de cycle (PFC). Son implication dans notre formation, son soutien constant, ainsi que son accompagnement dans notre projet de startup ont été une source d'inspiration précieuse.

Nous remercions chaleureusement l'ensemble des enseignants du département d'informatique de l'Université Abderrahmane Mira de Béjaïa, pour la qualité de l'enseignement qu'ils nous ont transmis avec engagement, sérieux et générosité.

Enfin, nous exprimons notre profonde reconnaissance à nos familles pour leur soutien moral, leur patience et leurs encouragements constants, ainsi qu'à nos amis et toutes les personnes qui, de près ou de loin, nous ont aidés, motivés ou accompagnés durant ce parcours.

Ce mémoire est le fruit d'un travail de binôme, nourri par un encadrement de qualité et des échanges humains enrichissants.

Résumé

Ce mémoire présente le travail que nous avons réalisé dans le cadre de notre projet de fin d'études, portant sur l'analyse, la refonte et la sécurisation de l'infrastructure réseau de l'entreprise **Cevital**. À la suite d'un audit complet de la topologie existante, plusieurs faiblesses ont été relevées, notamment en matière de disponibilité, de performance, de supervision, de résilience et de sécurité.

À partir de ces constats, nous avons conçu une nouvelle architecture hiérarchique et tolérante aux pannes, intégrant des standards et protocoles professionnels tels que **Virtual Local Area Network (VLAN)**, **VLAN Trunking Protocol (VTP)**, **Hot Standby Router Protocol (HSRP)**, **Spanning Tree Protocol (STP)**, **Port-Security**, **SSH**, **DHCP**, et le **trunking** 802.1Q. Le tout repose sur une infrastructure modernisée en étoile, fondée sur deux commutateurs de niveau 3 redondants et des liens Gigabit Ethernet, garantissant performance, évolutivité et sécurité.

Les différentes configurations ont été testées et validées via des simulations dans l'environnement **Cisco Packet Tracer**, permettant d'évaluer précisément les gains en termes de latence, de disponibilité, de charge réseau, et de fiabilité. Ce travail démontre que des choix technologiques pertinents, appliqués de manière structurée, peuvent transformer une infrastructure limitée en un socle stratégique robuste et évolutif.

Mots-clés : Réseau d'entreprise, Infrastructure Local Area Network (LAN), VLAN, VTP, HSRP, Cisco, Optimisation réseau, Sécurité réseau, Routage inter-VLAN, Supervision, Port-Security, STP, SSH, DHCP, Disponibilité, Redondance, Trunking, Résilience, Cevital.

Abstract

This thesis presents the work carried out as part of our final-year project, focused on analyzing, redesigning, and securing the network infrastructure of the company **Cevital**. A full audit of the existing topology highlighted several weaknesses in terms of availability, performance, supervision, scalability, and network security.

In response, we designed a new hierarchical and resilient architecture that incorporates modern standards and protocols such as **VLAN**, **VTP**, **HSRP**, **STP**, **Port-Security**, **SSH**, **DHCP**, and 802.1Q trunking. The new structure is based on two redundant Layer 3 switches, connected to access switches via Gigabit Ethernet, ensuring performance, scalability, and high availability.

The configurations were tested and validated through simulations using **Cisco Packet Tracer**, showing clear improvements in latency, fault tolerance, manageability, and service continuity. This project demonstrates how thoughtful network engineering decisions can significantly enhance the reliability and efficiency of enterprise network infrastructures in industrial environments.

Keywords : Enterprise Network, LAN Infrastructure, VLAN, VTP, HSRP, Cisco, Network Optimization, Network Security, Inter-VLAN Routing, Port-Security, STP, SSH, DHCP, Availability, Redundancy, Trunking, Supervision, Cevital.

Table des matières

Table des figures

Liste des tableaux

Liste des Abréviations

ADSL Asymmetric Digital Subscriber Line. 21

ARP Address Resolution Protocol. 35

BPDU Bridge Protocol Data Unit. 24, 63, 64

CPL Courant Porteur en Ligne. 22

DHCP Dynamic Host Configuration Protocol. 24, 35, 63

DNS Domain Name System. 19, 24

FTP File Transfer Protocol. 18, 19

GNS3 Graphical Network Simulator 3. 35

HSRP Hot Standby Router Protocol. 2, 5, 25, 53, 55, 62, 63, 65, 68

HTTP Hypertext Transfer Protocol. 18, 19, 24

HTTPS Hypertext Transfer Protocol Secure. 24

ICMP Internet Control Message Protocol. 24

IEEE Institute of Electrical and Electronics Engineers. 21

IMAP Internet Message Access Protocol. 24

IoT Internet des Objets. 23

IP Internet Protocol. 8, 18–21, 23–25, 27, 28, 33, 35, 43, 51, 54, 55, 57, 63

IR Infrarouge. 23

ISO International Organization for Standardization. 18

LAN Local Area Network. 2–4, 12, 13, 17, 21, 23, 25, 27–29, 34–51, 53, 62

MAC Media Access Control. 21, 28, 48

MAN Metropolitan Area Network. 15, 17

MPLS Multiprotocol Label Switching. 21

MTTR Temps moyen de réparation. 34, 54, 55

NAT Network address translation. 21

NMS Network management station. 35

OSI Open Systems Interconnection. 8, 18–21, 33

OSPF Open Shortest Path First. 25, 35

PAN Personal Area Network. 17

POP Point of Presence. 24

QoS Quality of Service. 33

RF Ondes radio. 23

RSA Rivest–Shamir–Adleman. 45

SDN Software-Defined Networking). 28

SFTP Secure File Transfer Protocol. 24

SLA Service Level Agreement. 34

SMTP Simple Mail Transfer Protocol. 18, 24

SNMP Simple Network Management Protocol. 27, 35

SPOF Point de défaillance unique. 48, 54

SSH Secure Shell. 24, 43, 45, 48, 63

SSL Secure Sockets Layer. 24

STP Spanning Tree Protocol. 2, 24, 35, 62, 64

TCP Transmission Control Protocol. 8, 18–21, 23, 35

TLS Transport Layer Security. 24

UDP User Datagram Protocol. 18, 19, 35

VLAN Virtual Local Area Network. 2, 4, 5, 24, 27, 28, 33, 34, 43, 44, 47, 48, 53–55, 57, 62–64

VoIP Voice over IP. 20, 34, 54, 55

VTP VLAN Trunking Protocol. 2, 5, 24, 27, 43, 44, 63, 64

WAN Wide Area Network. 15, 17

WLAN Wireless LAN. 21

Introduction Générale

Introduction Générale

Dans un monde où les communications numériques occupent une place centrale dans le fonctionnement des entreprises, les réseaux locaux, ou LAN (Local Area Network), constituent une infrastructure essentielle pour assurer la connectivité, l'échange de données et l'accès aux ressources informatiques. Ils permettent de relier efficacement les ordinateurs, serveurs, imprimantes et autres équipements nécessaires à l'activité quotidienne d'une organisation. La fiabilité de ces réseaux influence directement la productivité, la sécurité des données, et la fluidité des opérations internes.

Avec l'augmentation constante du nombre d'appareils connectés, les besoins croissants en bande passante, et les enjeux de cybersécurité de plus en plus complexes, la performance d'un réseau LAN devient un facteur stratégique. Une infrastructure mal conçue ou insuffisamment optimisée peut entraîner des problèmes de congestion, des interruptions de service ou une latence accrue, impactant directement le rendement des équipes et générant des coûts supplémentaires. Dans cette optique, la capacité d'une entreprise à maîtriser son réseau local est aujourd'hui un critère déterminant de compétitivité.

L'entreprise Cevital, en tant que groupe industriel de premier plan, s'appuie fortement sur son réseau LAN pour garantir la fluidité des échanges d'information entre ses différents services. Toutefois, comme toute grande organisation, elle peut être confrontée à des défaillances structurelles ou fonctionnelles de son réseau, compromettant la qualité du service informatique fourni aux utilisateurs internes. Ces difficultés soulèvent une interrogation centrale : comment analyser et optimiser les performances du réseau LAN de Cevital afin d'en améliorer l'efficacité, la sécurité et la fiabilité ?

Le présent mémoire s'inscrit dans cette problématique. Il vise à comprendre en profondeur le fonctionnement du réseau local de l'entreprise, à identifier les éléments susceptibles de limiter ses performances, et à proposer des solutions concrètes et adaptées aux besoins spécifiques de Cevital. L'étude s'appuiera d'une part sur un socle théorique solide portant sur les principes fondamentaux des réseaux LAN et les critères d'évaluation de leur performance, et d'autre part sur une analyse technique du réseau existant, basée sur l'observation, la mesure et l'interprétation des données collectées sur le terrain.

L'objectif est de formuler des recommandations techniques pertinentes et réalistes, susceptibles d'apporter une réelle amélioration de la qualité du service réseau. Ces propositions seront étudiées à la lumière de leur faisabilité, de leur coût, mais aussi de leurs retombées positives sur les processus métier de l'entreprise. À travers cette démarche, ce mémoire entend contribuer à la modernisation et à l'optimisation des infrastructures LAN dans un environnement professionnel exigeant, à la croisée des enjeux techniques et stratégiques.

Organisation du Mémoire

Ce mémoire est structuré en quatre chapitres principaux :

— **Chapitre 1 : Généralités sur les réseaux informatiques**
Présentation des notions fondamentales des réseaux, leur classification, leurs composants, ainsi que les principaux protocoles de communication.

— **Chapitre 2 : Introduction aux réseaux LAN**
Étude des caractéristiques des réseaux locaux (LAN), de leur architecture typique, des technologies utilisées, ainsi que des enjeux liés à la sécurité, à la performance et à l'évolutivité.

— **Chapitre 3 : Analyse des performances du réseau LAN de Cevital**
Analyse de l'infrastructure réseau existante de l'entreprise Cevital, identification des limites techniques et évaluation des performances.

— **Chapitre 4 : Optimisation et validation – approches et recommandations**
Proposition d'une topologie optimisée avec justification des choix techniques, en mettant l'accent sur la fiabilité, la sécurité et l'amélioration des performances du réseau.

Chapitre 1
Généralités sur les Réseaux Informatique

Chapitre 1

Généralités sur les Réseaux Informatique

1.1 Introduction

Avant d'aborder la configuration d'un réseau local comme celui de l'entreprise Cevital, il est important d'en comprendre les bases théoriques. Dans ce chapitre, nous allons poser les fondements des réseaux informatiques, en définissant leurs objectifs, leurs types, leurs architectures, les équipements qu'ils utilisent, ainsi que les protocoles essentiels à leur fonctionnement. Ces notions constituent le socle sur lequel s'appuie toute analyse ou optimisation d'un système .

1.2 Définitions générales des réseaux

Un réseau informatique est un ensemble d'équipements interconnectés qui permettent l'échange d'informations, le partage de ressources et la communication entre utilisateurs. Ces systèmes peuvent être locaux ou étendus, filaires ou sans fil, simples ou complexes, mais partagent des objectifs communs. [1]

1.2.1 Objectifs d'un Réseau Informatique

La mise en place d'un réseau informatique répond à plusieurs objectifs fondamentaux dans une organisation moderne. Il s'agit avant tout de faciliter la communication interne et externe, de partager efficacement les ressources, et de centraliser les services afin de rationaliser les opérations. Par ailleurs, un réseau bien conçu contribue à renforcer la sécurité des données, à améliorer la disponibilité des services numériques et à simplifier la gestion des équipements. [1]

Ces objectifs s'appliquent à tous les types de réseaux, qu'ils soient étendus Wide Area Network (WAN), Metropolitan Area Network (MAN) ou locaux (LAN). Dans les chapitres suivants, nous approfondirons ces notions dans le cadre spécifique des réseaux locaux, qui constituent l'ossature de nombreuses infrastructures informatiques d'entreprise.

1.2.2 Avantages et Limites des Réseaux Informatiques

Les réseaux informatiques ont profondément transformé les méthodes de travail des entreprises et des institutions. Ils permettent une collaboration plus fluide, un accès rapide aux données, et une meilleure productivité. Cependant, comme toute technologie, leur mise en œuvre s'accompagne de défis à relever, notamment en matière de sécurité et de maintenance.

Avantages

- **Gain de temps et de productivité** : le partage d'informations en temps réel et l'accès centralisé aux données optimisent les processus de travail.
- **Partage simplifié des ressources** : les utilisateurs peuvent accéder à des imprimantes, fichiers, bases de données ou applications à travers une infrastructure commune, ce qui réduit les coûts matériels.
- **Communication instantanée et centralisée** : les technologies réseau (emails, visioconférences, messageries internes) facilitent les échanges, même entre sites éloignés.
- **Sécurité et gestion centralisée** : les politiques de sécurité, l'authentification des utilisateurs, la surveillance et la sauvegarde des données peuvent être administrées de manière centralisée.
- **Automatisation des tâches d'administration** : la gestion à distance des postes, les mises à jour logicielles ou les déploiements peuvent être automatisés, augmentant la fiabilité du système.

Limites

- **Vulnérabilités en cybersécurité** : sans protection adéquate, les réseaux peuvent être exposés à des menaces comme les virus, les ransomwares ou les attaques par phishing.
- **Complexité de la gestion** : les réseaux nécessitent une supervision constante, des compétences spécialisées, et une veille technologique continue.
- **Dépendance au fonctionnement du réseau** : une panne réseau ou une coupure Internet peut interrompre totalement l'activité de l'entreprise.
- **Coût d'implémentation et d'évolution** : le déploiement initial (câblage, équipements, logiciels) et les mises à niveau régulières peuvent représenter des investissements importants.

1.3 Classification des Réseaux

Les réseaux informatiques peuvent être classés selon plusieurs critères permettant de mieux comprendre leur portée, leur structure organisationnelle et leur fonctionnement. Les deux critères les plus couramment utilisés sont l'étendue géographique et l'architecture.

1.3.1 Par étendue géographique

La classification par étendue géographique distingue les réseaux en fonction de leur couverture spatiale, c'est-à-dire la distance qu'ils couvrent et les zones qu'ils desservent.

— **Personal Area Network (PAN)** :
Un PAN est un réseau personnel à très courte portée, destiné à interconnecter des appareils individuels autour d'un utilisateur. Il couvre typiquement quelques mètres et utilise des technologies sans fil comme le Bluetooth, le Wi-Fi Direct ou l'infrarouge. Il permet, par exemple, de relier un smartphone à une montre connectée, à des écouteurs sans fil ou à un ordinateur portable. Les PAN sont simples à mettre en œuvre, consomment peu d'énergie, mais offrent un débit limité et une portée réduite. [2]

— **Local Area Network (LAN)** :
Un LAN est un réseau local couvrant une zone géographique restreinte comme une maison, un bureau, une école ou un campus universitaire. Il permet de connecter un nombre limité de dispositifs (ordinateurs, imprimantes, serveurs) afin de partager des fichiers, des applications ou des connexions Internet. Les LAN sont généralement rapides, peu coûteux à mettre en œuvre, et faciles à administrer. L'architecture Ethernet est la plus fréquemment utilisée dans les LAN. [2]

— **Metropolitan Area Network (MAN)** :
Un MAN couvre une zone urbaine plus vaste que le LAN, comme une ville ou une agglomération. Il relie plusieurs LAN entre eux à travers des infrastructures de communication publiques ou privées (comme la fibre optique). Les MAN sont souvent utilisés par les institutions gouvernementales, les grandes entreprises ou les fournisseurs de services Internet pour interconnecter plusieurs bâtiments répartis sur une même ville. [2]

— **Wide Area Network (WAN)** :
Un WAN est un réseau étendu couvrant de grandes distances, allant de plusieurs centaines à des milliers de kilomètres. L'exemple le plus connu de WAN est l'Internet. Ce type de réseau utilise des technologies variées (liaisons satellitaires, fibres optiques, liaisons MPLS, etc.) et permet la communication entre des réseaux locaux situés dans différents pays, voire sur différents continents. [2]

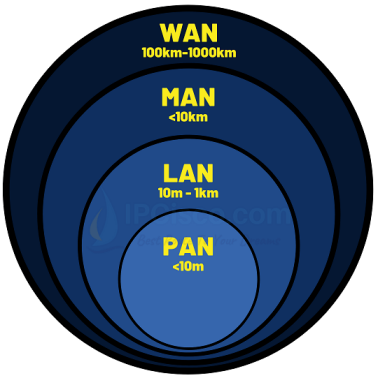

FIGURE 1.1 – Classification des réseaux par étendue géographique [W1]

1.3.2 Par architecture

La classification selon l'architecture décrit la manière dont les différents dispositifs du réseau interagissent entre eux. [2]

— **Client-serveur** :
Dans une architecture client-serveur, les ordinateurs appelés clients font des requêtes à un serveur centralisé, qui fournit des services ou des ressources spécifiques (fichiers, bases de données, applications, etc.). Cette architecture est largement utilisée dans les entreprises pour des raisons de sécurité, de gestion centralisée et d'efficacité.

— **Pair-à-pair (P2P)** :
Dans une architecture pair-à-pair, tous les nœuds du réseau jouent un rôle équivalent. Chaque poste peut agir à la fois comme client et comme serveur, partageant directement ses ressources avec les autres nœuds. Ce modèle est souvent utilisé pour le partage de fichiers (ex. : BitTorrent) et dans certaines applications décentralisées comme les réseaux blockchain.

1.4 Architecture OSI et modèles de communication

Pour concevoir, comprendre et diagnostiquer les réseaux informatiques, il est indispensable de s'appuyer sur des modèles de référence. Parmi les plus utilisés figurent le modèle OSI, proposé par l'ISO, et le modèle TCP/IP, qui constitue la base des communications sur Internet. Ces modèles fournissent une structure logique qui permet de décomposer le processus de communication en couches fonctionnelles bien définies.

Modèle OSI

Le modèle OSI, défini par International Organization for Standardization (ISO), est une architecture en sept couches qui permet de structurer la communication entre deux systèmes informatiques. Chaque couche a une fonction spécifique et interagit directement avec les couches qui lui sont adjacentes.

— **Couche 7 – Application** : Fournit des services aux applications de l'utilisateur (navigateur web, messagerie, etc.). Exemples de protocoles : Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP).
— **Couche 6 – Présentation** : Gère la représentation des données (encodage, chiffrement, compression). Elle s'assure que les données soient interprétables par le récepteur.
— **Couche 5 – Session** : Établit, maintient et termine les sessions de communication. Elle assure la synchronisation des échanges entre applications.
— **Couche 4 – Transport** : Assure le transport fiable (ou non) des données. Contrôle de flux, gestion des erreurs. Protocoles associés : TCP, User Datagram Protocol (UDP).
— **Couche 3 – Réseau** : Permet l'acheminement des paquets entre réseaux. Elle gère le routage et les adresses IP.
— **Couche 2 – Liaison de données** : Encapsule les données en trames et contrôle leur transfert sur le support. Technologies courantes : Ethernet, Wi-Fi.

— **Couche 1 – Physique** : Transmet les bits bruts sur le support physique (câble cuivre, fibre optique, ondes radio). Elle définit les normes électriques et mécaniques. [3]

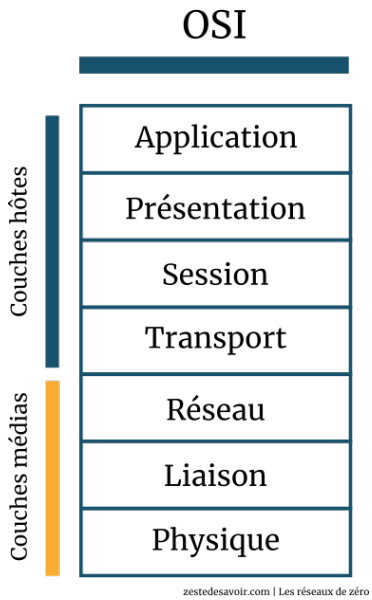

FIGURE 1.2 – Le modèle OSI [W2]

Modèle TCP / IP

Le modèle TCP / IP, développé par le département de la Défense des États-Unis, est plus proche des implémentations réelles. Il repose sur quatre couches principales et constitue la base des communications sur Internet.

— **Couche 4 – Application** : Combine les couches Application, Présentation et Session du modèle OSI. Elle fournit les services de communication aux applications utilisateurs (ex. : HTTP, FTP, Domain Name System (DNS)).

— **Couche 3 – Transport** : Assure la fiabilité des échanges entre hôtes (via TCP ou UDP), tout comme dans le modèle OSI.

— **Couche 2 – Internet** : Correspond à la couche Réseau du modèle OSI. Elle s'occupe de l'adressage IP et du routage des paquets.

— **Couche 1 – Accès réseau** : Regroupe les fonctions des couches Liaison de données et Physique du modèle OSI. Elle gère la transmission des données sur le support physique. [3]

Modèle OSI (7 couches)	Modèle TCP / IP (4 couches)
Application	**Application**
Présentation	
Session	
Transport	**Transport**
Réseau	**Internet**
Liaison de données	**Accès Réseau (Link)**
Physique	

TABLE 1.1 – Correspondance entre les couches du modèle OSI et du modèleTCP / IP

1.5 Équipements réseau

Un réseau informatique est constitué de plusieurs éléments essentiels qui permettent la communication, la transmission des données et la sécurité des échanges. Ces composants se répartissent en trois grandes catégories : les équipements terminaux, les équipements d'interconnexion et les supports de transmission.

1.5.1 Équipements terminaux

Les équipements terminaux, aussi appelés hôtes, sont les dispositifs utilisés directement par les utilisateurs finaux pour accéder aux services du réseau ou pour y contribuer. Ils peuvent être fixes ou mobiles, et remplissent différents rôles selon leur fonction. [4]

Exemples courants :

— **Ordinateurs de bureau et portables** : utilisés pour la navigation, le travail collaboratif, ou l'accès à des services réseau.

— **Imprimantes réseau** : permettent l'impression partagée entre plusieurs utilisateurs du réseau.

— **Téléphones IP (Voice over IP (VoIP))** : permettent les communications vocales via le protocole Internet.

— **Terminaux mobiles (smartphones, tablettes)** : accèdent au réseau via Wi-Fi ou réseau cellulaire.

FIGURE 1.3 – Terminaux

1.5.2 Équipements d'interconnexion

Ces équipements permettent de relier les équipements terminaux entre eux et d'assurer la communication entre différents segments de réseau. Ils sont essentiels pour la structuration logique et physique du réseau. [4]

— **Commutateurs (Switches)** : dispositifs qui relient les équipements à l'intérieur d'un même réseau local (LAN). Ils fonctionnent généralement au niveau 2 du modèle OSI (liaison de données) et permettent la transmission efficace des trames en tenant compte des adresses Media Access Control (MAC). Certains commutateurs dits « de niveau 3 » intègrent des fonctions de routage.

— **Routeurs** : utilisés pour interconnecter plusieurs réseaux différents. Ils opèrent au niveau 3 du modèle OSI (réseau) et déterminent le meilleur chemin pour acheminer les paquets IP. Ils assurent également la traduction d'adresses (Network address translation (NAT)) et peuvent inclure des fonctionnalités de sécurité.

— **Points d'accès (Access Points)** : servent de relais entre les appareils sans fil (comme les smartphones ou ordinateurs portables) et le réseau câblé. Ils permettent la création de réseaux locaux sans fil (Wireless LAN (WLAN)) et prennent en charge des protocoles comme Institute of Electrical and Electronics Engineers (IEEE) 802.11.

— **Pare-feux (Firewalls)** : dispositifs matériels ou logiciels chargés de contrôler le trafic réseau en appliquant des règles de sécurité. Ils filtrent les données entrantes et sortantes afin de protéger le réseau contre les accès non autorisés.

— **Concentrateurs (Hubs)** : dispositifs simples qui diffusent les données reçues à tous les ports sans distinction. Utilisés dans les anciens réseaux Ethernet, ils sont désormais obsolètes et remplacés par les switches.

— **Ponts (Bridges)** : utilisés pour diviser un réseau en segments afin de réduire le trafic. Ils analysent les adresses MAC pour décider si une trame doit être transmise ou non. Peu utilisés aujourd'hui car remplacés par les switches.

— **Passerelles (Gateways)** : équipements permettant la communication entre des réseaux utilisant des protocoles différents (ex : TCP/IP , AppleTalk). Elles opèrent aux couches supérieures du modèle OSI (couches 5 à 7).

— **Contrôleurs sans fil (Wireless LAN Controllers)** : gèrent et supervisent plusieurs points d'accès sans fil. Ils centralisent la configuration, l'authentification et la gestion du réseau WLAN.

— **Modems** : permettent la connexion à Internet via les lignes téléphoniques, Asymmetric Digital Subscriber Line (ADSL), câble ou fibre optique. Ils modulent et démodulent les signaux analogiques et numériques.

— **Équipements Multiprotocol Label Switching (MPLS) (Label Switch Routers)** : utilisés dans les réseaux d'opérateurs pour gérer le routage via des labels plutôt que par adresse IP, améliorant la performance du réseau.

— **Boîtiers Courant Porteur en Ligne (CPL)** : permettent de faire transiter le réseau informatique via les prises électriques. Ils sont utiles dans les environnements où les câbles Ethernet ou le Wi-Fi sont difficiles à déployer.

FIGURE 1.4 – Équipements d'interconnexion

1.5.3 Supports de transmission

Les supports de transmission constituent le canal par lequel les données circulent dans le réseau. Ils peuvent être **filaires** ou **sans fil**, chacun ayant ses avantages en termes de vitesse, de distance, de coût et de fiabilité. [4]

Supports filaires :

— **Câblage cuivre (Ethernet)** : le plus répandu dans les réseaux locaux. Les câbles RJ45 de catégorie 5e, 6 ou 7 permettent une transmission stable et fiable à courte ou moyenne distance. Ils sont sensibles aux interférences électromagnétiques.

— **Câble coaxial** : utilisé historiquement pour les réseaux Ethernet 10Base2 et 10Base5. Il est encore présent dans certaines infrastructures de télévision câblée et Internet.

— **Fibre optique** : utilisée pour les liaisons longue distance et les besoins en très haut débit. Elle offre une bande passante élevée, une faible atténuation et une excellente immunité aux interférences électromagnétiques. Deux types existent : monomode (longue distance) et multimode (distance moyenne).

— **Courant porteur en ligne (CPL)** : permet de transmettre les données numériques via le réseau électrique existant. Idéal dans les bâtiments où il est difficile de tirer des câbles Ethernet.

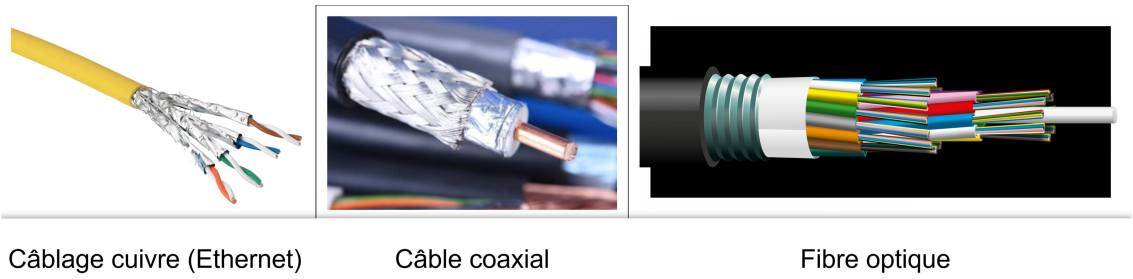

FIGURE 1.5 – Supports de transmission

Supports sans fil :

— **Wi-Fi (IEEE 802.11)** : Technologie sans fil largement utilisée dans les réseaux locaux (LAN). Elle offre une mobilité aux utilisateurs tout en assurant un débit élevé, bien qu'elle soit sensible aux interférences et nécessite une sécurisation adaptée.

— **Bluetooth** : Protocole de communication sans fil à courte portée (jusqu'à 10 mètres), utilisé principalement pour connecter des périphériques personnels comme des écouteurs, claviers ou imprimantes.

— **Infrarouge (IR)** : Technologie de transmission optique à très courte portée nécessitant une ligne de visée directe. Jadis répandue, elle est aujourd'hui largement remplacée par des alternatives plus efficaces.

— **Réseaux cellulaires (3G, 4G, 5G)** : Réseaux mobiles permettant un accès à Internet à grande échelle via les antennes relais. Ils offrent des débits croissants selon la génération, avec une très large couverture géographique.

— **Ondes radio (RF)** : Ondes électromagnétiques utilisées pour transmettre des données sur de longues distances avec une faible consommation. Elles sont exploitées dans des technologies comme LoRa, Sigfox ou Zigbee, principalement pour l'Internet des Objets (IoT).

— **Satellite** : Solution de communication par liaison directe avec des satellites. Utilisée dans les zones rurales ou isolées, elle offre un bon débit mais présente une latence relativement élevée.

— **Micro-ondes terrestres** : Technologie de transmission point à point utilisant des faisceaux hertziens, souvent pour relier deux bâtiments distants. Elle est adaptée aux environnements complexes (zones montagneuses ou étendues rurales).

1.6 Protocoles réseaux essentiels

Les protocoles de communication sont des ensembles de règles permettant aux équipements informatiques de dialoguer de manière fiable, sécurisée et standardisée. [5]

— **Internet Protocol (IP)** : Ce protocole travaille au niveau de la couche réseau. Il se charge de l'adressage logique et du routage des paquets à travers différents réseaux, permettant ainsi leur acheminement d'un point d'origine à une destination, même si celle-ci se trouve sur un autre réseau. Il ne garantit toutefois pas la fiabilité de la transmission.

— **Transmission Control Protocol (TCP)** : Fonctionnant au niveau de la couche transport, TCP établit une connexion fiable entre deux hôtes. Il assure l'intégrité des données transmises à travers un mécanisme de numérotation des segments, d'accusés de réception et de retransmission en cas de perte, garantissant ainsi une communication ordonnée et fiable.

— **Hypertext Transfer Protocol (HTTP)** : Protocoles utilisés pour l'échange de contenus web. *Hypertext Transfer Protocol Secure (HTTPS)* ajoute un chiffrement Secure Sockets Layer (SSL)/Transport Layer Security (TLS), garantissant la confidentialité des données.

— **Secure File Transfer Protocol (SFTP)** : Protocoles dédiés au transfert de fichiers. *SFTP*, basé sur SSH, permet un transfert sécurisé.

— **Simple Mail Transfer Protocol (SMTP) / Point of Presence (POP) / Internet Message Access Protocol (IMAP)** : Protocoles de messagerie électronique. *SMTP* sert à envoyer les e-mails, *POP* à les récupérer localement, et *IMAP* à les gérer directement sur le serveur.

— **Dynamic Host Configuration Protocol (DHCP) (Dynamic Host Configuration Protocol)** : Assure l'attribution automatique des adresses IP et des paramètres réseau aux hôtes.

— **Domain Name System (DNS)** : Traduit les noms de domaine (ex : `www.example.com`) en adresses IP.

— **Internet Control Message Protocol (ICMP)** : Utilisé pour les messages de diagnostic et d'erreur, comme les réponses à la commande `ping`.

— **Virtual LAN (VLAN)** : permet de segmenter logiquement un réseau physique pour isoler les flux ou sécuriser des sous-réseaux. Nous approfondirons ce point dans la section suivante.

— **VLAN Trunking Protocol (VTP)** : Protocole Cisco facilitant la gestion centralisée des VLANs. Les informations sont propagées automatiquement depuis un switch *serveur* vers les *clients*.

— **802.1Q (Encapsulation Dot1Q)** : Permet le transport simultané de plusieurs VLANs sur un même lien trunk grâce à l'encapsulation des trames.

— **Spanning Tree Protocol (STP)** : Protocole de niveau 2 permettant d'éviter les boucles de commutation en construisant une topologie logique sans boucle, grâce à la désactivation temporaire de certains liens redondants tout en assurant une reconvergence en cas de défaillance.

— **PortFast** : Fonctionnalité STP qui permet à un port access de basculer directement à l'état *forwarding*, réduisant ainsi le temps de démarrage des terminaux.

— **Port Security** : Limite l'accès physique aux ports en autorisant un nombre restreint d'adresses MAC et en détectant les anomalies (ex : MAC flooding).

— **Bridge Protocol Data Unit (BPDU) Guard** : Protège les ports utilisateurs contre l'injection de trames STP en désactivant automatiquement le port en cas de détection.

— **Secure Shell (SSH)** : Assure une connexion distante sécurisée aux équipements réseau (authentification chiffrée).

— **Hot Standby Router Protocol (HSRP)** : Protocole de redondance pour les passerelles. Il fournit une adresse IP virtuelle et garantit la continuité d'accès réseau en cas de panne d'un routeur.

— **Open Shortest Path First (OSPF)** : Protocole de routage dynamique interne à état de lien. Il est utilisé pour l'échange de routes entre routeurs au sein d'une même zone logique.

1.7 Conclusion

Ce premier chapitre nous a permis d'établir les fondements nécessaires à toute démarche de conception, d'analyse ou d'optimisation d'un réseau. En comprenant les objectifs, classifications, modèles de communication et protocoles fondamentaux, nous serons mieux préparés à étudier plus concrètement les réseaux LAN, qui feront l'objet du chapitre suivant.

Chapitre 2
Introduction aux Réseaux LAN

Chapitre 2

Introduction aux Réseaux LAN

2.1 Introduction

Dans ce chapitre, nous allons approfondir l'étude des réseaux locaux (LAN), dont les principes généraux ont été abordés précédemment. Un LAN désigne une infrastructure réseau déployée sur une zone géographique restreinte (comme un bâtiment, un service ou un campus) permettant le partage de ressources, une communication rapide et une administration centralisée. Nous présenterons ses caractéristiques techniques, les topologies couramment utilisées, les protocoles qui en assurent le fonctionnement, ainsi que les indicateurs de performance. Cette analyse théorique sera enrichie par notre propre expérience d'observation et d'audit du réseau de l'entreprise Cevital.

2.2 Caractéristiques d'un Réseau Local (LAN)

Les réseaux locaux (LAN), déjà évoqués dans le chapitre précédent, présentent des caractéristiques techniques spécifiques qui les rendent particulièrement adaptés aux environnements professionnels et industriels.

2.2.1 Fonctions et finalités d'un LAN

Au-delà de leurs propriétés techniques, les réseaux locaux sont conçus pour répondre à des besoins fonctionnels précis [1] :

- **Connectivité locale optimisée** : connexion fiable des équipements critiques comme les postes clients, serveurs, imprimantes, téléphones IP, caméras de surveillance ou objets connectés.
- **Partage centralisé** : accès partagé aux ressources (fichiers, logiciels métiers, bases de données), avec contrôle des droits utilisateur.
- **Administration simplifiée** : supervision centralisée via des équipements managés, VLANs, et protocoles tels que VTP ou Simple Network Management Protocol (SNMP).

— **Sécurité réseau** : segmentation logique via VLANs, filtrage d'accès (MAC/IP), authentification et surveillance active.
— **Évolutivité** : ajout de nouveaux équipements ou extensions réseau sans impact significatif sur les performances existantes.

2.2.2 Architecture typique d'un LAN

Un réseau local (LAN) moderne est généralement structuré selon une architecture hiérarchique en trois couches, afin d'assurer performance, évolutivité, sécurité et facilité de gestion. [6]

1. **Couche d'accès (Access Layer)** :
   Elle regroupe les équipements terminaux (postes de travail, imprimantes, caméras IP, points d'accès Wi-Fi) via des commutateurs d'accès. C'est à ce niveau que sont appliquées les premières politiques de sécurité et de segmentation réseau (VLAN).
2. **Couche de distribution (Distribution Layer)** :
   Elle relie les commutateurs d'accès aux équipements du cœur de réseau. Elle centralise la gestion du trafic local, applique des règles de routage ou de contrôle d'accès, et assure la redondance pour éviter les points de défaillance.
3. **Couche cœur de réseau (Core Layer)** :
   Cette couche assure l'interconnexion rapide et hautement disponible entre les différents segments du réseau et les services critiques (serveurs, Internet, data centers). Elle est conçue pour des performances maximales et une faible latence.

2.2.3 Évolutions des LAN

Avec les exigences croissantes en matière de performance, de sécurité et de flexibilité, les réseaux locaux connaissent des évolutions majeures. Les principales tendances actuelles incluent [7] :

— **La virtualisation du réseau (Software-Defined Networking) (SDN)** :
Permet une gestion centralisée, dynamique et programmable de l'infrastructure réseau, facilitant la création de réseaux virtuels et l'application rapide de politiques de sécurité.
— **La haute disponibilité** :
Mise en place de redondances matérielles (switchs, liens, alimentations) pour garantir la continuité de service en cas de défaillance.
— **L'automatisation de la configuration (Zero Touch Provisioning)** :
Simplifie le déploiement initial et les mises à jour du réseau sans intervention manuelle, réduisant les erreurs humaines et le temps d'installation.
— **L'intégration massive de l'IoT** :
Les LAN doivent désormais supporter des milliers de capteurs, objets connectés et équipements intelligents tout en maintenant des performances et une sécurité élevées.
— **La cybersécurité avancée intégrée** :
Les LAN modernes intègrent des fonctionnalités comme le contrôle d'accès granulaire, la micro-segmentation et la détection des menaces en temps réel.

— **L'évolutivité** :
Les architectures LAN sont pensées pour accompagner la croissance des entreprises, avec des capacités de montée en débit et d'extension sans refonte complète.

2.3 Topologies physiques et logiques

2.3.1 Topologies physiques

La topologie physique d'un réseau désigne la manière dont les équipements (ordinateurs, imprimantes, routeurs, commutateurs, etc.) sont physiquement interconnectés au sein de l'infrastructure. Elle représente la structure réelle du câblage et des connexions entre les dispositifs. [8]

Le choix de la topologie a un impact direct sur les performances du réseau, sa facilité de maintenance, son coût de déploiement, ainsi que sa capacité à tolérer les pannes. Il existe plusieurs types de topologies, chacun présentant des avantages et des inconvénients selon le contexte d'usage.

Topologie en bus

Dans une topologie en bus, tous les nœuds du réseau sont connectés à un seul câble principal (appelé backbone), qui transporte les données. Lorsqu'un nœud envoie un message, celui-ci est visible par tous les autres. Toutefois, seul le destinataire l'accepte. [9]

Avantages :
— Faible coût de mise en œuvre.
— Facilité d'installation pour les petits réseaux.
Inconvénients :
— Les collisions de données sont fréquentes si plusieurs nœuds communiquent simultanément.
— Une panne du câble principal affecte tout le réseau.
— Difficile à diagnostiquer et à étendre.

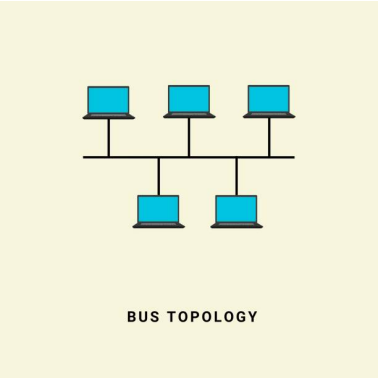

FIGURE 2.1 – Topologie en bus [W3]

Topologie en étoile

Dans cette topologie, chaque nœud est connecté individuellement à un dispositif central (hub, switch ou routeur). Toutes les communications passent par ce nœud central. [9]

Avantages :
— Facilité de gestion et d'ajout de nouveaux nœuds.
— Moins de collisions comparé à la topologie en bus.
— Une panne sur un câble n'affecte pas les autres connexions.
Inconvénients :
— Le dispositif central constitue un point de défaillance unique.
— Le coût est plus élevé à cause du matériel nécessaire.

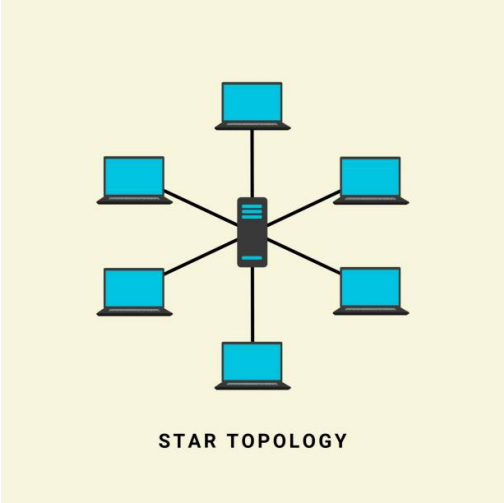

FIGURE 2.2 – Topologie en étoile [W4]

Topologie en anneau

Dans une topologie en anneau, chaque nœud est connecté au suivant et le dernier au premier, formant une boucle fermée. Les données circulent dans un seul sens ou dans les deux, selon les variantes. [9]

Avantages :
— Contrôle de flux amélioré, peu de collisions.
— Performances stables avec un trafic modéré.
Inconvénients :
— Une panne sur un nœud ou un câble peut interrompre tout le réseau.
— Maintenance plus complexe.

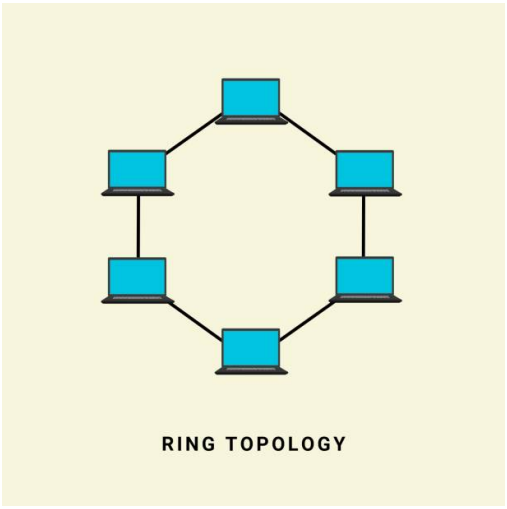

FIGURE 2.3 – Topologie en anneau [W5]

Topologie maillée

Dans une topologie maillée, chaque nœud est connecté à tous les autres. Cela permet une redondance élevée et une excellente tolérance aux pannes. [9]

Avantages :
— Très fiable : une panne ne perturbe pas la communication entre d'autres nœuds.
— Performances optimales grâce à des connexions directes.
Inconvénients :
— Coût élevé en termes de câblage et de configuration.
— Complexité importante pour la maintenance.

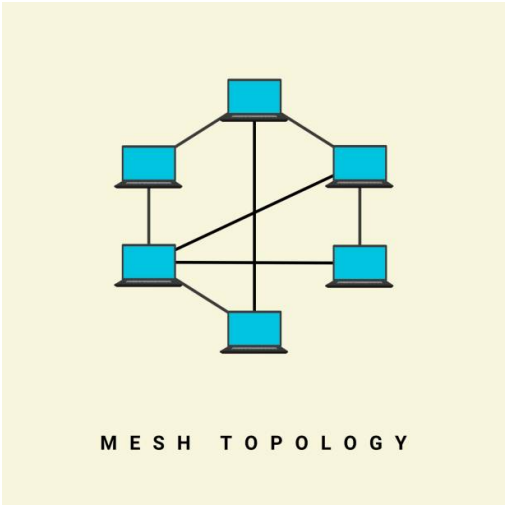

FIGURE 2.4 – Topologie en maillée [W6]

Topologie hybride

La topologie hybride combine deux ou plusieurs types de topologies de base (étoile, bus, anneau, etc.) afin d'optimiser les avantages de chacune et de pallier leurs inconvénients. Par

exemple, une entreprise peut adopter une structure en étoile pour ses bureaux internes, reliés ensuite entre eux par une topologie en bus. [9]

Avantages :
— Flexible et évolutive.
— Peut être conçue selon les besoins spécifiques de l'organisation.
Inconvénients :
— Coût et complexité potentiellement élevés.
— Difficulté de gestion et de dépannage.

2.3.2 Topologies logiques

La topologie logique décrit la manière dont les données circulent entre les dispositifs au sein du réseau, indépendamment de la disposition physique du câblage. Elle représente le schéma de communication réel entre les équipements connectés. [8]

Ainsi, un réseau physiquement en étoile peut adopter une logique de communication en bus, en anneau ou en commutation. Cette distinction est essentielle pour comprendre le comportement du réseau en matière de routage, de diffusion ou de collision des données.

Il existe principalement deux grandes topologies logiques [10] :

Topologie logique en bus

Dans une topologie logique en bus, toutes les stations partagent un même canal de communication. Lorsqu'un périphérique envoie une donnée, celle-ci est diffusée à tous les autres. Un seul appareil peut transmettre à la fois, ce qui peut générer des collisions si plusieurs essaient simultanément.

Exemples : Réseaux Ethernet anciens basés sur le câble coaxial (10BASE-2, 10BASE-5).

Caractéristiques :
— Communication unidirectionnelle.
— Les données circulent sur un canal commun.
— Risque élevé de collisions si non maîtrisé (sans commutation).

Topologie logique en commutation

Dans ce modèle, chaque appareil communique avec les autres à travers un switch qui gère les flux de données de manière intelligente. Les données sont transmises uniquement entre l'émetteur et le destinataire.

Exemples : Réseaux modernes basés sur des switches Ethernet.

Caractéristiques :
— Communication point à point.
— Réduction des collisions grâce à la commutation.
— Performances optimisées pour les réseaux actuels.

Remarque : Dans les réseaux actuels, la plupart des architectures utilisent une topologie physique en étoile combinée à une topologie logique commutée, ce qui permet de tirer parti à la fois de la simplicité de câblage et des performances élevées.

2.4 Segmentation logique par VLANs

Les **VLANs (Virtual Local Area Networks)** ne constituent pas à proprement parler une topologie logique comme la diffusion ou la commutation. Il s'agit plutôt d'un mécanisme de **segmentation logique** permettant de créer plusieurs sous-réseaux isolés au sein d'un même réseau physique.

Un VLAN regroupe des équipements réseau (ordinateurs, imprimantes, caméras IP, etc.) comme s'ils faisaient partie d'un même domaine de diffusion, indépendamment de leur emplacement physique. Cette approche permet une séparation logique du trafic et une gestion plus fine des flux réseau. [11]

Pourquoi parle-t-on de segmentation logique et non de topologie logique ?

— Les VLANs **n'altèrent pas la structure logique de transmission** (comme l'Ethernet commuté), mais ajoutent une couche d'organisation au niveau 2 du modèle OSI.
— Leur objectif principal est de **limiter les domaines de broadcast**, renforcer la sécurité, améliorer Quality of Service (QoS), et faciliter l'administration réseau.
— Ils sont **indépendants de la topologie physique** : on peut créer un VLAN unique pour plusieurs postes répartis sur différents switches tant qu'ils sont connectés à un réseau compatible VLAN. [11]

Avantages des VLANs :

— **Isolation du trafic** : chaque département de l'entreprise peut disposer de son propre réseau logique, ce qui réduit les risques d'écoute ou d'interférences.
— **Sécurité renforcée** : un utilisateur d'un VLAN ne peut pas accéder aux ressources d'un autre VLAN sans autorisation explicite (via routage inter-VLAN).
— **Réduction du trafic de broadcast** : seuls les équipements d'un même VLAN reçoivent les paquets de diffusion.
— **Flexibilité et évolutivité** : il est possible de modifier la structure logique du réseau sans changer le câblage physique.

Exemple de mise en œuvre dans le cas de Cevital : Dans notre étude du réseau de l'entreprise Cevital, les VLANs ont été utilisés pour structurer logiquement les services fonctionnels :

— **VLAN 2** : IT
— **VLAN 3** : DFC
— **VLAN 4** : DRH
— **VLAN 5** : Logistique
— **VLAN 6** : Réseaux & Sécurité
— **VLAN 7** : Ressources Humaines
— **VLAN 8** : Imprimantes
— **VLAN 9** : Serveurs
— **VLAN 10** : Appro / Achats
— **VLAN 11** : HSE
— **VLAN 12** : Téléphonie IP
— **VLAN 15** : Management

Cette segmentation permet une meilleure organisation du réseau, une sécurisation des échanges entre services, et un contrôle plus fin de la bande passante et des priorités de trafic.

Remarque : pour permettre la communication entre ces VLANs, on utilise un dispositif de niveau 3 (un routeur ou un switch multilayer) chargé du *routage inter-VLAN*. Ce mécanisme permet de définir des règles de communication entre VLANs tout en conservant l'isolation par défaut.

2.5 Critères d'évaluation des performances d'un LAN

L'évaluation des performances d'un réseau local (LAN) repose sur plusieurs indicateurs techniques permettant d'identifier les points forts et les éventuels goulots d'étranglement. Ces critères sont essentiels pour garantir la fluidité des échanges, la stabilité des services et l'adaptation du réseau aux besoins de l'entreprise.

Principaux critères à considérer Philippe Atelin et José Dordoigne (2006) [1] et William Stallings (2013) [12] :

- **Débit (Throughput)** : Il s'agit du volume réel de données transférées par seconde sur le réseau, exprimé en Mbps ou Gbps. Un débit élevé est crucial pour les applications exigeantes comme la visioconférence, les transferts de fichiers volumineux ou les systèmes ERP.
- **Latence** : Temps nécessaire à un paquet pour aller de la source à la destination. Elle est mesurée en millisecondes (ms). Une faible latence est indispensable pour les services en temps réel (VoIP, vidéoconférence, jeux en réseau).
- **Taux de perte de paquets** : Pourcentage de paquets envoyés qui n'arrivent jamais à destination. Un taux élevé peut engendrer des coupures audio/vidéo, une lenteur dans les applications ou des retransmissions inutiles.
- **Gigue (Jitter)** : Variation de la latence dans le temps. La gigue est particulièrement critique dans les flux multimédia (VoIP) où elle peut provoquer des interruptions ou de la distorsion.
- **Disponibilité** : Pourcentage de temps pendant lequel le réseau est opérationnel. Exprimée en *Service Level Agreement (SLA)*, elle est souvent visée à 99,9
- **Utilisation des ressources** : Taux d'occupation des liens, des ports, de la bande passante et des équipements réseau (CPU, RAM). Une surcharge constante peut entraîner des baisses de performances et des risques de panne.
- **Erreurs de transmission** : Ce sont les anomalies survenues lors du transfert de données à travers le réseau, telles que les collisions, les trames corrompues ou les erreurs de contrôle de redondance cyclique (CRC). Leur présence fréquente traduit généralement des défaillances au niveau physique (câbles défectueux, interférences électromagnétiques) ou des erreurs de configuration des équipements réseau.
- **Temps moyen de réparation (MTTR)** : Délai nécessaire pour rétablir le service après une panne. Un MTTR faible traduit une bonne résilience du réseau et une efficacité de l'équipe IT.

— **Capacité d'extension (scalabilité)** : Aptitude du LAN à évoluer sans impact significatif sur la performance. Cela concerne l'ajout d'utilisateurs, d'équipements, ou de services (téléphonie IP, caméras, etc.).

2.5.1 Présentation des outils utilisés

Afin de mener à bien nos simulations, mesures et rédaction, nous avons utilisé un ensemble d'outils professionnels et open source. Voici un aperçu des principaux outils employés dans ce projet :

— `iperf3` : Utilisé pour tester le débit réseau (bande passante) entre deux machines, en mode TCP ou UDP. Il permet de mesurer le taux de transfert, la perte de paquets et la stabilité de la connexion. [W7]
— `ping` : Commande de base pour vérifier la connectivité entre deux hôtes et mesurer la latence moyenne. Elle est utile pour détecter les pertes de paquets ou les interruptions de liaison. [W8]
— `traceroute` : Permet d'identifier les routeurs intermédiaires (hops) empruntés par les paquets pour atteindre leur destination. Utile pour analyser les retards ou goulots d'étranglement. [W9]
— `Wireshark` : Analyseur de trames réseau puissant utilisé pour capturer, décoder et analyser les paquets. Il permet d'étudier le comportement des protocoles comme DHCP, Address Resolution Protocol (ARP), STP, OSPF, etc. [W10]
— `top` / `htop` : Outils de surveillance système pour Linux. Ils permettent de visualiser en temps réel l'usage du processeur, de la mémoire RAM, et de détecter les processus gourmands. [W11]
— `free` : Affiche l'état de la mémoire vive. Complémentaire à `htop`, il est utile pour évaluer la consommation mémoire lors des tests de charge réseau. [W12]
— **Cisco Packet Tracer** : Logiciel de simulation réseau développé par Cisco. Il a été utilisé pour concevoir et tester les topologies, configurer les VLANs, le routage inter-VLAN, HSRP et les mécanismes de sécurité. [W13]
— **Graphical Network Simulator 3 (GNS3)** : Simulateur avancé permettant l'intégration de véritables images IOS Cisco. Utilisé pour les tests approfondis de protocoles dynamiques (comme OSPF), dans des conditions proches du réel. [W14]

Outils de mesure courants :

— *ping, traceroute, iperf, Wireshark* : pour tester la connectivité, la latence et la bande passante.
— *SNMP, NetFlow, Network management station (NMS)* : pour la supervision continue du trafic et l'analyse des performances réseau.

Critère	Outil recommandé	Explication
Débit (Bandwidth)	`iperf3`	Mesure la capacité de transmission entre deux hôtes (en Mbps ou Gbps).
Latence	`ping`, `traceroute`	Temps moyen de réponse entre deux équipements (en millisecondes).
Perte de paquets	`ping`, `iperf3 -u`	Taux de paquets perdus durant une communication, important pour la qualité de service.
Temps de convergence	`Wireshark` + chronomètre	Temps pris par les protocoles comme STP ou OSPF pour se stabiliser après une panne.
Utilisation CPU/-RAM	`top`, `htop`, `free`	Mesure la charge système sur les équipements réseau ou VMs.
Nombre de sauts (hops)	`traceroute`	Nombre de nœuds intermédiaires entre deux hôtes, utile pour le diagnostic de chemin.
Résilience / Tolérance	Coupure manuelle de lien	Permet d'observer le comportement du réseau en cas de défaillance d'un lien.

TABLE 2.1 – Outils d'évaluation des performances d'un réseau local (LAN)

2.6 Conclusion

Ce chapitre nous a permis d'examiner en détail les spécificités des réseaux LAN, aussi bien sur le plan architectural que technologique. Ces connaissances théoriques serviront de base pour l'analyse concrète du réseau LAN de l'entreprise Cevital dans le chapitre suivant.

Chapitre 3
Analyse des Performances du Réseau LAN de Cevital

Chapitre 3

Analyse des Performances du Réseau LAN de Cevital

3.1 Introduction

Dans ce mémoire, nous avons choisi d'étudier le réseau local (LAN) de l'entreprise **Cevital**, en raison de la complexité de son infrastructure et de son importance stratégique dans les activités industrielles, logistiques et commerciales du groupe.

Ce travail a été réalisé dans le cadre de notre stage de fin d'études, effectué au sein de l'entreprise du **02 mars 2025** au **30 mai 2025**. Cette immersion en environnement professionnel nous a permis d'observer de près les problématiques réelles liées à la gestion d'un réseau d'entreprise à grande échelle.

Ce choix s'explique par l'envergure multisite de Cevital et les défis que cela représente en termes de performance, de sécurité et de gestion. Nous avons analysé la topologie existante, identifié ses limites, et proposé une architecture optimisée, plus fiable, évolutive et adaptée aux exigences professionnelles de l'entreprise.

3.2 Présentation de l'entreprise Cevital

Cevital est une société par actions de droit privé, créée en mai 1998, avec un capital de 68,76 milliards de dinars. Implantée à l'est du port de Béjaïa, elle est devenue l'un des leaders de l'industrie agroalimentaire en Algérie. Grâce à des unités de production modernes et une politique d'investissement ambitieuse, Cevital s'est imposée comme un acteur stratégique dans l'économie nationale, avec une forte contribution à la création d'emplois. À titre d'exemple, le nombre de salariés de Cevital Food est passé de 500 en 1999 à près de 4 000 en 2008.

3.2.1 Historique

Le groupe a été fondé par Issad Rebrab, pionnier du secteur privé industriel en Algérie. Depuis les années 1970, il a développé plusieurs entreprises dans la construction métallique, la sidérurgie, les TIC, et l'importation automobile. En 1998, il lance Cevital dans l'agroalimentaire, avant d'élargir ses activités à la grande distribution, l'électroménager, le verre plat, le transport et la logistique.

3.2.2 Étapes clés

— **1971–1986** : Création et acquisition d'entreprises industrielles (SOCOMEG, PROFILOR, SACM...).
— **1988** : Création de METAL SIDER (sidérurgie).
— **1991** : Reprise des activités IBM Algérie, lancement du journal *Liberté*.
— **1997–1998** : Création de Hyundai Motors Algérie, puis de Cevital SPA.
— **2006–2009** : Déploiement dans la grande distribution (Numidis), le verre (MFG), et la logistique (Numilog).
— **2013–2014** : Internationalisation avec l'acquisition d'Oxxo, Brandt, et d'Aferpi en Europe.

3.2.3 Activités

Cevital opère dans plusieurs secteurs :
— Agroalimentaire
— Distribution
— Électroménager
— Sidérurgie
— Verre
— Logistique et transport
— Immobilier et services [13]

3.2.4 Organisation et filiales

Le groupe Cevital est structuré autour de plusieurs pôles d'activité majeurs :
— **Agroalimentaire** : à travers Cevital Agro-industrie, le groupe est leader dans la production de sucre, d'huiles végétales, de margarines, de boissons et de conditionnements alimentaires. Il dispose des plus grandes capacités de production et de stockage en Afrique.
— **Industrie** : via des filiales comme *Sider El Hadjar* et *Cevital Industrial*, le groupe intervient dans la sidérurgie, l'aluminium, la fabrication de verre plat et les matériaux de construction.
— **Électroménager** : avec *Brandt Algérie*, Cevital conçoit et fabrique des appareils électroménagers de qualité destinés aussi bien au marché national qu'à l'exportation.

— **Distribution et logistique** : à travers *Numidis* (enseignes Uno et Samha), le groupe déploie un réseau de grande distribution moderne. Il possède également une plateforme logistique avancée pour le transport de marchandises.
— **Automobile et services** : le groupe s'est récemment lancé dans l'importation et l'assemblage de véhicules, tout en développant des services annexes dans les domaines de la finance, des télécoms et de l'immobilier.

3.2.5 Implantation géographique

Cevital possède des unités de production et des plateformes logistiques réparties sur l'ensemble du territoire algérien, avec des pôles industriels majeurs à Béjaïa, Sétif, Oran, Tizi Ouzou et Alger. Il est également présent à l'international, notamment en Europe (France, Espagne, Italie), au Moyen-Orient et en Afrique de l'Ouest, ce qui confère au groupe une forte dimension exportatrice.

3.2.6 Organisation générale des composantes et missions des directions

L'entreprise Cevital est structurée autour de plusieurs directions spécialisées qui assurent la gestion fonctionnelle, opérationnelle, industrielle et commerciale de l'ensemble des activités. Chaque direction a des missions précises, contribuant collectivement à l'atteinte des objectifs du groupe.

— **Direction Marketing** : pilote les marques et gammes de produits à travers une connaissance approfondie des consommateurs, de leurs besoins et usages. Elle assure une veille sur les marchés et la concurrence, propose des recommandations d'innovation, de rénovation et de communication, mises en œuvre via des groupes de projets pluridisciplinaires.
— **Direction des Ventes & Commerciale** : en charge de la commercialisation de toutes les gammes de produits et du développement du fichier clients. Elle détecte et promeut des projets à base de hautes technologies et entretient une relation directe avec les prospects et clients.
— **Direction Système d'Informations** : assure la mise en place des technologies de l'information nécessaires à la stratégie et à la performance de l'entreprise. Elle garantit la cohérence, la mise à jour, la sécurité et la disponibilité des systèmes informatiques et de communication.
— **Direction des Finances et Comptabilité** : responsable de la préparation des budgets, de la tenue de la comptabilité selon les normes, du contrôle de gestion et du reporting périodique.
— **Direction Industrielle** : définit avec la direction générale les objectifs et budgets des sites de production, analyse les dysfonctionnements, supervise les besoins en matériel et veille à la politique environnement et sécurité.

- **Direction des Ressources Humaines** : propose les principes de gestion RH en cohérence avec les objectifs du business et la politique RH du groupe. Elle assure le recrutement, la formation, la gestion des carrières, la performance, les rémunérations, le support administratif, et accompagne la direction dans les actions disciplinaires et la communication interne.
- **Direction Approvisionnements** : met en place les mécanismes d'approvisionnement en matières et services dans les meilleurs délais, au meilleur coût et avec la meilleure qualité pour soutenir la production et les ventes.
- **Direction Logistique** : gère l'expédition des produits finis, le transport (interne, affrété ou client), l'alimentation en matières premières et le stockage dans les dépôts locaux et régionaux.
- **Direction des Silos** : décharge les matières premières en vrac, les stocke dans des conditions optimales, assure leur transfert vers les unités utilisatrices et entretient les installations.
- **Direction des Boissons** : comprend trois unités industrielles (LLK, unité plastique et COJEK) spécialisées dans la production d'eau minérale, de boissons, d'emballages et de jus à partir de fruits et légumes.
- **Direction Corps Gras** : regroupe les unités de raffinerie et de conditionnement d'huiles, margarine et les unités en chantier à El Kseur. Elle a pour mission la production d'huiles végétales, margarines et beurres pour la consommation locale et l'export.
- **Direction Pôle Sucre** : comprend plusieurs unités (raffineries de sucre solide, unité de sucre liquide, conditionnement) et produit du sucre en respectant les normes de qualité, de sécurité et d'environnement, à destination des industriels et des particuliers.

Cette organisation permet à Cevital de gérer efficacement ses ressources, de répondre aux exigences du marché et d'assurer un haut niveau de performance industrielle et commerciale. [13]

3.2.7 Vision et engagement

Cevital se donne pour mission de participer activement au développement économique de l'Algérie en créant de la richesse et de l'emploi durable. Le groupe s'engage dans des projets structurants et durables, en misant sur la qualité, l'innovation, la performance, et le respect des normes internationales en matière d'environnement et de responsabilité sociétale.

3.3 Organisation générale du réseau dans l'entreprise

L'entreprise Cevital est structurée en de nombreux départements fonctionnels, chacun ayant des besoins spécifiques en matière d'accès réseau, de sécurité, de disponibilité et de bande passante. L'organigramme présenté en figure 3.1 illustre la complexité organisationnelle de l'entreprise, répartie en pôles industriels, direction générale, services supports, et unités de production.

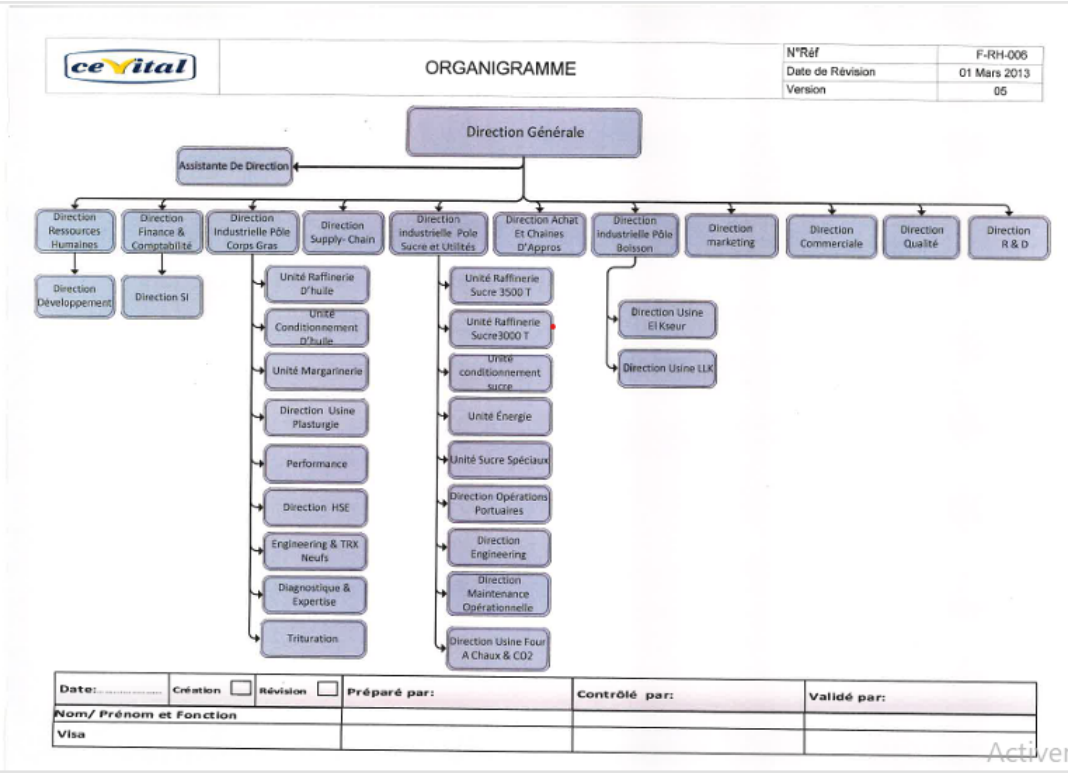

FIGURE 3.1 – Organigramme fonctionnel de l'entreprise Cevital [13]

Cette diversité fonctionnelle implique une infrastructure réseau segmentée logiquement à travers des VLANs dédiés, et une architecture hiérarchisée en couches (accès, distribution, cœur), afin d'assurer la performance, la sécurité et la gestion centralisée du système d'information de l'entreprise.

La section suivante détaillera l'état initial de l'infrastructure réseau mise en place, avant optimisation.

3.4 Présentation de la topologie actuelle (initiale)

L'entreprise Cevital disposait d'une infrastructure centralisée, globalement fonctionnelle, reposant sur une configuration manuelle des équipements. Cependant, cette architecture présentait plusieurs limites en termes de performance, de résilience et d'évolutivité. La présente section détaille l'organisation du réseau local (LAN) avant la refonte, ainsi que les constats issus de l'audit technique initial.

3.4.1 Architecture générale

La topologie déployée reposait sur un **commutateur de niveau 3 (L3)** central, chargé à la fois du routage inter-VLAN et de la distribution du trafic vers les commutateurs de niveau 2 (L2) connectés en cascade. Ces derniers desservaient les différents services et départements de l'entreprise (Direction, Ressources Humaines, IT, Logistique, etc.).

Principales caractéristiques identifiées :

- **Commutation hiérarchique en cascade** : Jusqu'à quatre niveaux de commutateurs L2 connectés en série, ce qui augmentait la latence et créait une forte dépendance à un chemin unique.
- **Routage centralisé** : Le switch L3 principal assurait le routage entre les VLANs, sans mécanisme de redondance ni basculement automatique en cas de panne.
- **Technologie de câblage** : Utilisation de câbles en cuivre (CAT5e), limités à un débit de 100 Mbps (Fast Ethernet), insuffisant face aux besoins croissants de l'entreprise.
- **Segmentation logique** : Une organisation par VLANs était mise en place afin de séparer les différents services.
- **VTP activé** : Le protocole **VLAN Trunking Protocol** était configuré pour faciliter la propagation automatique des VLANs entre les équipements.
- **Sécurisation des accès** : L'accès distant aux équipements était protégé par le protocole `SSH`, garantissant la confidentialité des sessions d'administration.

3.4.2 Organisation des VLANs

Afin d'optimiser la gestion, la sécurité et les performances du réseau, une segmentation logique a été mise en œuvre à l'aide de la technologie **VLAN (Virtual Local Area Network)**. Celle-ci permet d'isoler les flux de données entre services, de limiter la diffusion des trames broadcast, et d'appliquer des politiques spécifiques à chaque domaine fonctionnel.

Un total de **treize LANs** a été configuré, chacun correspondant à un service ou un usage spécifique. Cette structuration facilite le déploiement de règles de sécurité, le contrôle du trafic et garantit une qualité de service adaptée, notamment pour des usages sensibles comme la téléphonie IP.

VLAN	Nom / Service	Adresse Réseau	Masque de sous-réseau
20	IT (Informatique)	10.80.2.0	255.255.255.0
30	DFC (Direction Financière et Comptable)	10.80.3.0	255.255.255.0
40	DRH (Direction des Ressources Humaines)	10.80.4.0	255.255.255.0
50	Logistique	10.80.5.0	255.255.255.0
60	Réseaux & Sécurité (RS)	10.80.6.0	255.255.255.0
70	Ressources Humaines (RH)	10.80.7.0	255.255.255.0
80	Imprimantes	10.80.8.0	255.255.255.0
10	Serveurs	10.80.9.0	255.255.255.0
100	Approvisionnement / Achats	10.80.10.0	255.255.255.0
110	HSE (Hygiène, Sécurité, Environnement)	10.80.11.0	255.255.255.0
12	Téléphonie IP	10.80.12.0	255.255.255.0
15	Management (Administration Réseau)	10.80.15.0	255.255.255.0

TABLE 3.1 – Plan d'adressage IP et segmentation logique par VLANs

Pour centraliser et automatiser la gestion de cette segmentation, le protocole **VTP (VLAN Trunking Protocol)** a été déployé. Le commutateur principal était configuré en *mode serveur*, autorisant la création, la modification et la suppression de VLANs. Les commutateurs secondaires, configurés en *mode client*, recevaient automatiquement ces informations, assurant la cohérence des configurations à travers l'infrastructure.

Chaque VLAN était associé à une interface virtuelle (SVI) sur le commutateur L3, permettant d'assurer le routage inter-VLAN. Ce mécanisme garantissait la communication entre les services tout en maintenant l'isolation logique du trafic, essentielle à la sécurité et à la performance globale du réseau.

3.4.3 Fonctionnement global

Chaque service disposait de son propre VLAN, défini sur le switch L3 et distribué via VTP. Le routage inter-VLAN s'effectuait localement sur le commutateur principal. Les liens trunk entre les équipements véhiculaient l'ensemble des VLANs configurés, sans mise en œuvre de segmentation topologique avancée.

L'absence de liens redondants ou de mécanismes de basculement signifiait qu'une défaillance du switch principal entraînait l'interruption de toutes les communications inter-départements, voire une panne réseau généralisée.

3.5 Configuration réseau

3.5.1 Configuration de base

Hostname et domaine

Avant toute autre configuration, on définit l'identité et on prépare le switch au SSH :

```
hostname Direction-IT
ip domain-name cevital.com
service password-encryption
```

Explication détaillée :

- `hostname Direction-IT` : nomme l'équipement « Direction-IT » dans l'IOS.
- `ip domain-name cevital.com` : nécessaire pour la génération des clés Rivest–Shamir–Adleman (RSA) SSH.
- `service password-encryption` : chiffre les mots de passe en clair dans la config.

Accès SSH

On remplace Telnet par SSH et on crée un admin local :

```
username admin privilege 15 secret Str0ngP@ss
crypto key generate rsa modulus 2048
ip ssh version 2

line vty 0 4
  transport input ssh
  login local
```

Explication :

- Création d'un user 'admin' en privilege 15.
- Clés RSA 2048 bits pour SSH v2.
- Limitation des lignes VTY à SSH et authent local.

3.5.2 VLANs et VTP

Définition des VLANs

```
vlan 2
  name Direction-IT
vlan 70
  name Ressources-Humaines

vlan 80
  name Imprimantes
```

Pourquoi ? Segmentation logique par service, isolation de broadcast et sécurité.

Propagation des VLANs (VTP)

Sur le switch L3 (serveur VTP) :

```
vtp mode server
vtp domain cevital.com
```

Sur tous les L2 (clients VTP) :

```
vtp mode client
vtp domain cevital.com
```

Attribution des ports

```
interface FastEthernet0/1
  switchport mode access
  switchport access vlan 10

interface GigabitEthernet1/0/1
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,40
```

Résumé : – Ports utilisateurs en mode access dans le VLAN approprié. – Uplinks en trunks 802.1Q autorisant les VLANs.

3.5.3 DHCP

```
ip dhcp excluded-address 10.80.10.1 10.80.10.20

ip dhcp pool VLAN10
  network 10.80.10.0 255.255.255.0
  default-router 10.80.10.1
  dns-server 8.8.8.8
```

Notes : – Exclusion des adresses statiques → éviter conflits. – Pool par VLAN pour automatiser le provisioning.

3.5.4 Routage inter-VLAN

```
interface Vlan10
  ip address 10.80.10.1 255.255.255.0
interface Vlan20
  ip address 10.80.20.1 255.255.255.0
interface Vlan30
  ip address 10.80.30.1 255.255.255.0
ip routing
```

But : donner aux L3 la fonction de router les VLANs entre eux.

3.6 Schéma de la topologie initiale

Voici ci-dessous la topologie initiale du réseau de Cevital, modélisée à l'aide du simulateur Cisco Packet Tracer.

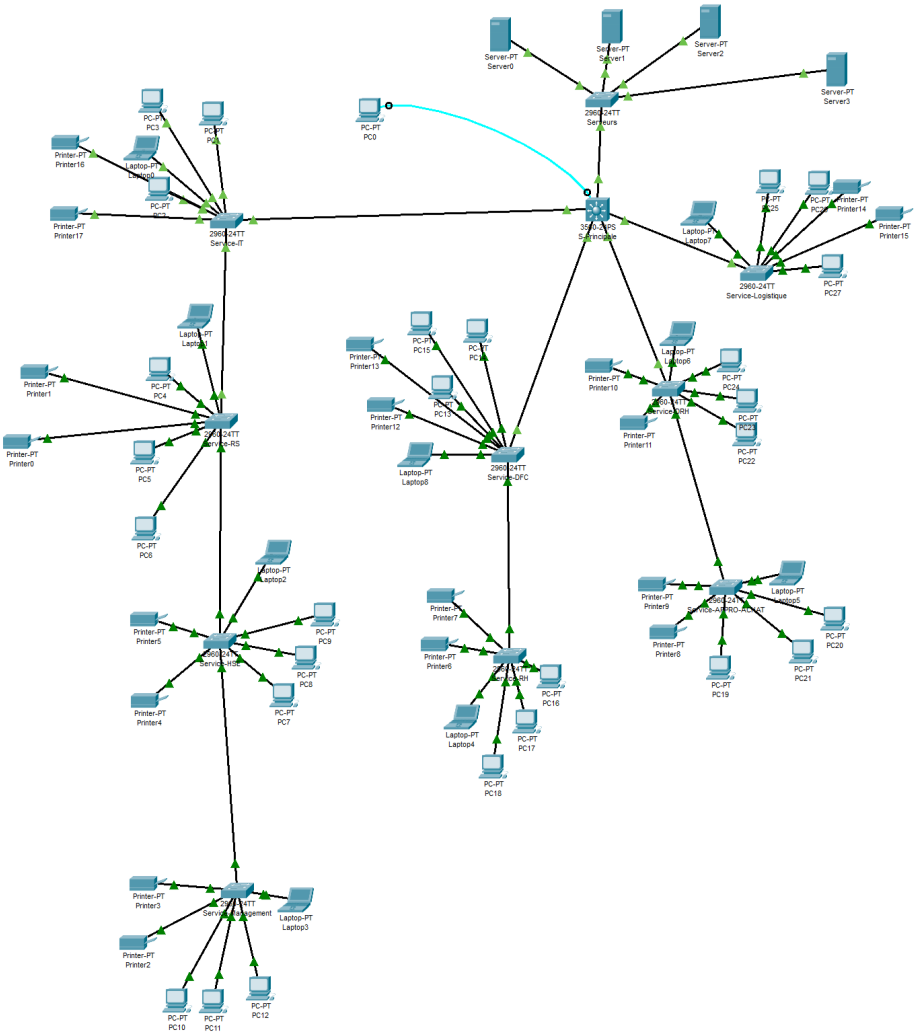

FIGURE 3.2 – Topologie initiale du réseau de Cevital (architecture en cascade)

Cette topologie initiale du réseau de Cevital, présente une architecture hiérarchique centrée autour d'un commutateur de couche 3 (L3) agissant comme le cœur ou la couche de distribution. Ce commutateur L3 est responsable du routage inter-VLAN et de la connectivité principale, reliant plusieurs serveurs et se connectant à son tour à une série de commutateurs de couche 2 (L2). Ces commutateurs L2 forment la couche d'accès, à partir de laquelle se ramifient de multiples appareils d'extrémité tels que des PCs, des ordinateurs portables et des imprimantes. La particularité de cette topologie réside dans les cascades de commutateurs L2, où certains commutateurs de couche 2 sont connectés à d'autres commutateurs de couche 2, étendant ainsi la connectivité aux groupes de périphériques d'extrémité dans différentes sections du réseau.

3.7 Problèmes identifiés et limites observées

L'analyse de l'architecture réseau existante chez Cevital a permis de mettre en évidence plusieurs limites techniques et organisationnelles freinant la performance, la sécurité et la résilience globale du système. Ces constats ont motivé la mise en place d'une nouvelle topologie plus robuste.

— **Latence excessive et performances dégradées**
La structure en cascade, avec plusieurs niveaux de commutateurs L2 connectés successivement, provoquait une augmentation significative de la latence réseau. Des pics de 18 à 20 ms ont été observés, affectant directement les performances des applications critiques (ERP, VoIP, supervision industrielle).

— **Point de défaillance unique (SPOF)**
Le switch de niveau 3, assurant à la fois la commutation centrale et le routage inter-VLAN, constituait un point de concentration unique. Lors d'un incident électrique, une interruption de 25 minutes a été enregistrée, paralysant l'ensemble des services de l'entreprise, faute de redondance ou de mécanisme de basculement.

— **Débit insuffisant sur les liens principaux**
Le câblage cuivre en Fast Ethernet (100 Mbps) était inadapté aux volumes de données échangés, en particulier pour :
  — les communications VoIP sensibles à la latence et à la gigue,
  — les transferts entre serveurs de fichiers, postes de supervision et équipements industriels.

  Cette limitation entraînait des saturations ponctuelles et des lenteurs constatées par les utilisateurs finaux.

— **Sécurité perfectible malgré la présence de SSH**
Bien que l'accès distant soit sécurisé via le protocole SSH, plusieurs failles subsistaient :
  — Absence de filtrage par adresse MAC sur les ports d'accès,
  — Aucune politique de journalisation centralisée (logs d'accès, alertes, etc.),
  — VLANs actifs, mais non cloisonnés par des ACL ou politiques de sécurité fines.

— **Évolutivité limitée et gestion complexe**
L'ajout progressif de commutateurs en cascade compliquait la maintenance et augmentait les risques de boucle réseau. Ce mode d'expansion rendait la topologie difficilement scalable et source d'erreurs lors de la configuration manuelle.

Ces constats ont mis en évidence la nécessité d'une refonte complète de l'infrastructure réseau, visant à améliorer la tolérance aux pannes, les performances, la sécurité, ainsi que la flexibilité de gestion à long terme.

3.8 Bilan de performance du réseau existant

La topologie initiale adoptée par Cevital repose sur une structure en cascade : les commutateurs de niveau 2 (L2) sont connectés les uns aux autres en série, avec un seul commutateur de niveau 3 (L3) au centre du réseau. Cette structure, bien qu'économique à déployer, présente plusieurs limites en termes de performance, comme nous le montrons dans les sous-sections suivantes.

3.8.1 Latence cumulée

Chaque commutateur (switch) introduit un petit délai de traitement et de transmission des données. Dans une architecture en cascade, ces délais s'additionnent à chaque saut. La latence cumulée peut être exprimée par la formule suivante [12] :

$$L_{\text{totale}} = n \cdot (L_t + L_p + L_{\text{traitement}})$$

— n : le nombre de sauts, c'est-à-dire le nombre de commutateurs traversés par le paquet.
— L_t : le temps de transmission, soit le temps nécessaire pour placer tous les bits du paquet sur le lien (en fonction du débit).
— L_p : le temps de propagation, soit le délai que met le signal à voyager physiquement à travers le câble.
— $L_{\text{traitement}}$: le temps de traitement, soit le délai introduit par le switch pour analyser le paquet et décider de sa redirection.

Cette formule permet d'estimer précisément la latence induite par l'architecture réseau, notamment dans les topologies linéaires ou en cascade où le nombre de sauts est important.

Exemple réel : Supposons que le paquet de données doive traverser 5 commutateurs pour aller d'un ordinateur A à un ordinateur B (ce qui est courant dans un réseau en cascade).

— Taille d'un paquet standard : 1500 octets = 12000 bits
— Débit des liaisons FastEthernet : 100 Mbps
— Latence de transmission par saut :

$$L_t = \frac{12000}{100 \times 10^6} = 120\ \mu s$$

— Temps de traitement par switch : environ 10 μs

Donc, pour 5 sauts :

$$L_{\text{total}} = 5 \times (120 + 10) = 650\ \mu s$$

Interprétation : une simple requête ping entre deux hôtes peut prendre près de 0.65 millisecondes, ce qui est acceptable pour la bureautique mais trop élevé pour de la téléphonie IP ou de la vidéosurveillance.

3.8.2 Débit et Bande Passante

Dans cette architecture, tous les liens sont en **FastEthernet (100 Mbps)**. Lorsqu'un même lien est partagé entre plusieurs utilisateurs, la bande passante disponible est divisée entre eux.

Exemple : Si 10 ordinateurs utilisent simultanément un lien FastEthernet, chaque poste ne dispose en moyenne que de :

$$\frac{100 \text{ Mbps}}{10} = 10 \text{ Mbps}$$

Conséquence sur un transfert de fichier : Pour envoyer un fichier de 100 Mo (800 Mbits) :

$$T = \frac{800 \times 10^6}{10 \times 10^6} = 80 \text{ secondes}$$

Cela signifie qu'un simple fichier de 100 Mo peut prendre plus d'une minute vingt secondes à transférer, ce qui est inacceptable dans un contexte industriel.

3.8.3 Goulots d'étranglement et congestion

Dans une topologie en cascade :
— Tous les flux inter-VLAN doivent passer par le même switch N3.
— Plusieurs utilisateurs partagent les mêmes liens descendants.

Exemple : Trois services (RH, Production, Sécurité) situés sur des VLAN différents veulent accéder simultanément au serveur ERP. Le trafic de tous ces services converge vers le même lien FastEthernet entre un switch N2 et le switch N3.

Résultat : ce lien devient un goulot d'étranglement, ce qui ralentit toutes les communications critiques.

3.8.4 Faible tolérance aux pannes

Défaut majeur : l'absence de redondance.

Exemple : Si un switch intermédiaire (N2) tombe ou est débranché, tous les périphériques connectés après ce point sont complètement isolés du réseau. Cela peut bloquer des lignes de production, l'accès aux bases de données ou à Internet pour plusieurs utilisateurs.

3.8.5 Impact global sur les services Cevital

— **ERP / Gestion commerciale** : ralentissements lors des consultations des stocks, retards dans la validation des bons de commande.
— **Contrôle industriel** : délai dans la remontée des alarmes ou des capteurs critiques.
— **Téléphonie IP / Visio** : coupures, gigue audio et vidéo.
— **Sauvegardes réseau** : durées excessives, surcharge nocturne.

Conclusion du Bilan

Le réseau initial, bien qu'opérationnel, présente les limites suivantes :
— **Latence cumulative élevée**, causée par la cascade de commutateurs.
— **Bande passante insuffisante** en période de charge.
— **Absence totale de redondance**, ce qui rend le système fragile.
— **Congestion autour du switch central**.

Ces éléments justifient pleinement une refonte de l'architecture réseau vers une structure optimisée, adaptée aux exigences modernes de performance, de sécurité et de disponibilité.

3.9 Conclusion

L'analyse du réseau LAN de l'entreprise Cevital a mis en évidence plusieurs limites structurelles affectant la performance, la disponibilité et la sécurité globale de l'infrastructure. La topologie en cascade, bien que fonctionnelle, engendre des délais de transmission élevés, une faible tolérance aux pannes, ainsi qu'un risque accru de congestion réseau.

Ces constats justifient la nécessité de repenser l'architecture existante afin de répondre aux exigences croissantes de l'entreprise, tant en matière de rapidité que de fiabilité. C'est dans cette optique que nous présentons, dans le chapitre suivant, une proposition d'optimisation complète du réseau accompagnée d'une validation argumentée sur les plans théorique et technique.

Chapitre 4

Optimisation et Validation : Approches et Recommandations

Chapitre 4

Optimisation et Validation : Approches et Recommandations

4.1 Introduction

Après avoir relevé les nombreuses limitations de l'infrastructure LAN existante (cascade profonde, goulot unique, sécurité minimale, latence et bande passante insuffisantes), nous proposons une nouvelle architecture répondant aux exigences actuelles de performance, de résilience, de sécurité et de gestion. Cette refonte s'appuie sur les bonnes pratiques issues des modèles hiérarchiques préconisés par Cisco, et intègre des mécanismes avancés de redondance (HSRP), de segmentation (VLANs), et de supervision.

Ce chapitre présente de manière structurée les différentes optimisations apportées, accompagnées d'exemples concrets de configurations Cisco IOS permettant leur mise en œuvre. Pour une vue d'ensemble complète et fonctionnelle, une configuration intégrale de l'infrastructure optimisée est également fournie en annexe.

4.2 Présentation de la nouvelle architecture proposée

4.2.1 Objectifs poursuivis

La refonte de l'infrastructure réseau répond à une volonté d'alignement avec les exigences modernes de performance, de sécurité et de résilience. Les objectifs visés sont les suivants :

— **Améliorer la disponibilité du réseau**
Réduire le risque d'interruption de service en assurant la continuité des opérations même en cas de panne ou d'incident matériel critique.

— **Équilibrer la charge réseau**
Répartir intelligemment le trafic entre les équipements cœur (switchs L3) afin d'éviter les congestions et d'optimiser l'utilisation des ressources.

— **Optimiser les performances**
Accroître la capacité de transport des données et limiter les délais de transmission, notamment pour les flux sensibles ou temps réel.

— **Réduire la latence entre les équipements**
Diminuer le nombre de sauts et raccourcir les chemins entre les différents segments du réseau afin d'offrir une meilleure réactivité des applications.
— **Accroître la sécurité des accès réseau**
Prévenir les intrusions, restreindre les accès non autorisés, et protéger les communications internes contre les risques de compromission.
— **Faciliter l'administration et la supervision**
Permettre une gestion plus cohérente, centralisée et évolutive des équipements réseau, tout en réduisant la charge opérationnelle.
— **Préparer l'évolutivité de l'infrastructure**
Garantir la capacité du réseau à absorber de nouvelles charges, intégrer de nouveaux services ou équipements, sans compromettre sa stabilité ni sa sécurité.

4.3 Implémentation des solutions pour l'atteinte des objectifs

4.3.1 Amélioration de la disponibilité du réseau

L'un des axes critiques de l'optimisation de l'infrastructure réseau repose sur le renforcement de la **disponibilité des services**, enjeu fondamental pour toute entreprise moderne. Dans la topologie initiale, la présence d'un unique switch de niveau 3, à la fois routeur et passerelle par défaut, constituait un *point de défaillance unique* (SPOF). Sa panne ou son redémarrage entraînait une coupure totale des communications inter-VLAN, affectant l'ensemble des utilisateurs.

Constat initial et limites techniques

— Le cœur de réseau était centralisé sur un seul switch de niveau 3.
— Aucun mécanisme de redondance ou de basculement n'était mis en œuvre.
— Toute défaillance du switch L3 entraînait une interruption complète du trafic.
— Le rétablissement du service dépendait d'une intervention manuelle, augmentant considérablement le temps d'arrêt ($MTTR$).

Impact sur les services métier

Dans un contexte d'entreprise comme Cevital, l'indisponibilité du réseau, même temporaire, perturbe :
— L'accès aux outils de gestion (ERP, messagerie, base de données),
— La téléphonie sur IP (VoIP), très sensible aux coupures de liaison,
— Les échanges entre départements via le réseau local,
— Le fonctionnement normal des serveurs et imprimantes réseau.

Solution d'optimisation : double cœur de réseau et passerelle virtuelle HSRP

Pour résoudre cette faiblesse majeure, la nouvelle architecture repose désormais sur :

— **Deux switchs de niveau 3**, déployés en parallèle au niveau du cœur du réseau, assurant une double redondance matérielle et fonctionnelle.

— La mise en œuvre du protocole **HSRP (Hot Standby Router Protocol)**, qui permet la création d'une **passerelle IP virtuelle redondante** assurée conjointement par les deux équipements.

Grâce à cette approche, l'un des switchs cœur agit comme **actif principal**, tandis que l'autre reste en veille. En cas de défaillance de l'équipement principal, le second prend automatiquement le relais, sans interruption de service pour les utilisateurs.

Extrait de configuration HSRP :

```
! Switch Principal
interface Vlan10
  standby 10 ip 10.80.10.254
  standby 10 priority 110
  standby 10 preempt

! Switch Secondaire
interface Vlan10
  standby 10 ip 10.80.10.254
  standby 10 priority 90
  standby 10 preempt
```

Explication des paramètres :

— `standby 10 ip 10.80.10.254` : définit l'adresse IP virtuelle utilisée comme passerelle par tous les clients du VLAN.

— `priority` : la priorité plus élevée désigne le switch actif par défaut.

— `preempt` : permet au switch principal de redevenir actif automatiquement après son rétablissement.

Bénéfices obtenus

La mise en œuvre de cette double stratégie (double switch + HSRP) permet :

— **Tolérance aux pannes renforcée** : aucune interruption de service en cas de panne d'un switch cœur.

— **Continuité transparente** : aucun changement de configuration pour les postes clients.

— **Meilleurs indicateurs de disponibilité** :

  — Taux de disponibilité global supérieur à **99,9 %**.

  — Réduction significative du *MTTR* (Mean Time To Recovery).

  — Préservation de la qualité de service pour les flux critiques (VoIP, applicatif).

4.3.2 Répartition équilibrée de la charge réseau

En plus de garantir la disponibilité, une infrastructure réseau moderne doit assurer une utilisation optimale de ses ressources pour éviter les saturations localisées. Dans la topologie initiale, tout le trafic réseau transitait par un unique commutateur de niveau 3, entraînant une surcharge inévitable de cet équipement.

Constat initial et limites techniques

- Le cœur de réseau reposait exclusivement sur un seul switch de niveau 3.
- L'ensemble des VLANs étaient routés par cet unique équipement, générant un déséquilibre de charge.
- L'absence de répartition dynamique provoquait une sollicitation excessive du processeur réseau et des files d'attente.
- Les performances se dégradaient notablement lors des périodes de forte activité.

Conséquences sur l'infrastructure

Cette surcharge impactait :

- Les temps de réponse des applications critiques (ERP, supervision),
- La qualité des flux temps réel (VoIP, visioconférence),
- La stabilité du routage inter-VLAN sous forte charge,
- La durée de traitement des requêtes réseau.

Solution d'optimisation : équilibrage par distribution des VLANs et priorités *STP*

La nouvelle architecture intègre deux switchs de niveau 3 configurés pour partager la charge selon la logique suivante :

- Chaque switch devient routeur par défaut pour un sous-ensemble distinct des VLANs,
- Les priorités STP sont configurées de manière asymétrique pour répartir la charge de pont racine par VLAN,
- Les liens montants sont répartis uniformément pour éviter les goulots d'étranglement.

Cette méthode permet une distribution intelligente des traitements réseau entre les deux équipements de cœur, assurant ainsi une meilleure efficacité globale.

Extrait de configuration Spanning Tree :

```
! Sur Switch 1 (prioritaire pour VLANs 2-6)
spanning-tree vlan 2-6 priority 4096
spanning-tree vlan 7-11 priority 8192

! Sur Switch 2 (prioritaire pour VLANs 7-11)
spanning-tree vlan 2-6 priority 8192
spanning-tree vlan 7-11 priority 4096
```

Explication :
— Le switch ayant la priorité la plus faible devient pont racine pour le VLAN concerné.
— Cette répartition logique permet d'équilibrer les flux montants, assurant une charge réseau mieux répartie.

Bénéfices obtenus

L'application de cette stratégie permet :
— **Réduction de la charge sur chaque switch** grâce à une répartition symétrique,
— **Amélioration des performances inter-VLAN** grâce à un routage réparti,
— **Prévention des congestions** sur les liens montants,
— **Meilleure stabilité du réseau** durant les pics d'activité.

4.3.3 Augmentation de la capacité d'interconnexion du réseau

Un facteur clé dans l'amélioration des performances globales du réseau réside dans la capacité de transport des données entre les différents équipements. L'ancienne infrastructure, reposant encore sur des liaisons Fast Ethernet (**100 Mbps**), s'est révélée rapidement insuffisante face aux exigences croissantes des applications modernes, comme les systèmes ERP, la téléphonie IP, ou les solutions de vidéosurveillance haute définition.

Constat initial et limites techniques

— **Bande passante limitée** à 100 Mbps sur les liens montants entre commutateurs.
— **Congestion régulière** du trafic réseau, notamment inter-VLAN.
— **Incapacité à supporter** simultanément les services critiques (sauvegardes, appels VoIP, transferts volumineux).
— **Saturation des trunks** entre les switches, causant pertes de paquets et lenteurs.

Impact sur la qualité de service

Cette contrainte technique entraînait :
— Un allongement des temps de réponse pour les utilisateurs.
— Une instabilité des applications temps réel (visioconférence, VoIP).
— Des ralentissements observés lors des synchronisations serveurs et sauvegardes.

Stratégie d'optimisation : adoption du Gigabit Ethernet

La nouvelle architecture intègre une montée en capacité avec :
— Le remplacement de tous les liens critiques par des **connexions Gigabit Ethernet (1 Gbps)**.
— L'utilisation d'interfaces **GigabitEthernet (Gig0/x)** pour tous les trunks.
— Une préparation à l'évolution vers le **10 Gbps** (via modules SFP+ ou agrégation LACP).

Exemple de configuration d'un lien trunk Gigabit :

```
interface GigabitEthernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,40
```

Explication des commandes :

- `switchport trunk encapsulation dot1q` : active le balisage VLAN selon le standard IEEE.
- `switchport mode trunk` : permet le transport de plusieurs VLANs sur une même interface.
- `trunk allowed vlan` : filtre les VLANs autorisés à circuler pour limiter la saturation.

Bénéfices obtenus

- **Bande passante multipliée par 10**, assurant une fluidité pour les flux critiques.
- **Réduction significative des congestions** sur les trunks inter-switch.
- **Stabilité améliorée** des services temps réel (VoIP, ERP, supervision).
- **Infrastructure évolutive**, compatible avec les exigences futures (vidéosurveillance HD, IoT industriel).

4.3.4 Réduction de la latence réseau

La latence, c'est-à-dire le temps nécessaire au transit d'un paquet de données entre deux équipements, est un critère déterminant pour les performances perçues par les utilisateurs. L'ancienne architecture en cascade introduisait une latence excessive, incompatible avec les exigences d'applications modernes comme la VoIP, les ERP ou les outils collaboratifs.

Constat initial et limitations techniques

- Les switches d'accès (niveau 2) étaient connectés en chaîne avant de rejoindre le cœur de réseau (L3).
- Chaque paquet pouvait traverser jusqu'à 3 ou 4 équipements intermédiaires avant d'atteindre sa destination.
- **Latence moyenne observée :** ~20 ms, avec pics en cas de charge élevée.
- La convergence de STP en cas de panne était lente, accentuant les délais de reprise.
- Une défaillance sur un switch intermédiaire pouvait impacter toute une branche d'utilisateurs.

Nouveau modèle topologique : étoile redondante

La nouvelle architecture repose sur un schéma en étoile entièrement refondu, intégrant :

- **Deux commutateurs cœur de niveau 3** (redondants) interconnectés directement avec tous les switches d'accès.
- Des **liaisons ascendantes doubles** (uplinks) par switch d'accès, assurant la redondance physique et logique.

— Des **connexions Gigabit Ethernet** remplaçant les anciens liens Fast Ethernet.

Résultats techniques obtenus

— **Latence moyenne réduite à ~5 ms**, même sous charge réseau soutenue.
— Moins de sauts intermédiaires (*hops*) → communications plus rapides.
— **Amélioration immédiate des performances** pour les flux sensibles au délai : VoIP, bases SQL, visioconférences.
— Topologie plus simple à documenter, auditer et superviser.

Impacts stratégiques pour l'entreprise

— Réactivité accrue du système d'information.
— Réduction des interruptions liées aux lenteurs ou congestions.
— Amélioration de l'expérience utilisateur et du confort de travail numérique.
— Infrastructure prête à accueillir de nouvelles charges sans dégradation perceptible des délais de réponse.

4.3.5 Renforcement de la sécurité d'accès aux équipements

Dans toute infrastructure critique, la sécurité des accès physiques et logiques constitue un pilier incontournable de la stratégie réseau. L'ancienne topologie, bien que fonctionnelle, manquait de mécanismes de contrôle aux points de terminaison. Dans la nouvelle architecture, un ensemble cohérent de mesures a été déployé pour verrouiller les connexions physiques et prévenir les comportements malveillants ou accidentels.

Failles constatées dans l'ancienne architecture

— **Ports non filtrés** : Acceptation implicite de tout périphérique physique connecté à un port libre.
— **Absence de limitation MAC** : Risque de surcharge des tables de commutation via attaque de type *MAC flooding*.
— **Aucune défense contre les boucles STP** : Les ports utilisateurs n'étaient pas protégés contre l'introduction de commutateurs non autorisés.

Dispositifs de sécurisation déployés

La nouvelle infrastructure intègre les protections suivantes :
— **Accès sécurisé en SSH** : L'administration distante des équipements ne peut se faire qu'à travers une session chiffrée SSH, excluant tout usage de Telnet.
— **Port-Security** : Contrôle des adresses MAC autorisées par port, avec limitation stricte du nombre de dispositifs et apprentissage automatique (`sticky`).
— **PortFast** : Activation sur les ports utilisateurs pour éviter les délais d'initialisation STP.
— **BPDU Guard** : Blocage automatique des ports recevant des trames BPDU, empêchant toute tentative d'introduction d'un switch non autorisé.

Exemple de configuration appliquée :

```
interface range fastEthernet 0/1 - 24
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Analyse des paramètres :

- `port-security maximum 1` : un seul périphérique autorisé par port.
- `violation restrict` : le trafic est bloqué, mais le port reste actif, ce qui facilite le diagnostic.
- `mac-address sticky` : les adresses MAC sont mémorisées automatiquement.
- `portfast + bpduguard` : les ports utilisateurs se connectent immédiatement tout en restant protégés.

Effets attendus et bénéfices techniques

- **Réduction significative des risques internes** : connexions non autorisées détectées et bloquées.
- **Prévention proactive des incidents réseau** : protection contre les erreurs humaines (insertion de switch) ou attaques.
- **Visibilité accrue** : journalisation possible des violations et supervision simplifiée.

4.3.6 Préparation à l'évolutivité de l'infrastructure

Dans un contexte industriel en perpétuelle évolution, une architecture réseau performante doit non seulement répondre aux besoins actuels, mais aussi être en mesure d'absorber les futures extensions fonctionnelles et structurelles de l'entreprise. La nouvelle topologie a ainsi été pensée pour offrir une base solide, évolutive et durable.

Limites observées dans l'ancienne infrastructure

- **Topologie rigide et non modulaire** : le rajout de nouveaux équipements nécessitait des manipulations complexes et risquées (physiques ou logicielles).
- **Cascade excessive** : l'extension du réseau alourdissait l'architecture existante, augmentant la latence et le risque de boucles STP.
- **Liaisons Fast Ethernet (100 Mbps)** : rapidement saturées en cas d'augmentation du trafic ou d'ajout de services.
- **Gestion manuelle des VLANs** : chaque ajout imposait une configuration locale, lente et sujette aux erreurs.

Objectif technique

Permettre une extension fluide et maîtrisée du réseau, sans impact négatif sur la stabilité, les performances ou la sécurité de l'infrastructure :

— **Accepter l'ajout de nouveaux équipements sans révision du cœur de réseau**.
— **Supporter la montée en charge** (trafic applicatif, voix, vidéo, IoT...).
— **Rendre l'administration agile** : centralisation, supervision, configuration automatisée.

Mesures d'optimisation adoptées

— **Topologie en étoile directe** : chaque nouveau switch peut être relié directement à l'un des deux cœurs L3, sans impact sur les autres équipements.
— **Liens montants en Gigabit Ethernet** : assurent une capacité suffisante pour les extensions futures.
— **Propagation automatique des VLANs via VTP** : configuration centralisée assurant cohérence et gain de temps.
— **Routage dynamique OSPF** : permet d'étendre l'interconnexion vers d'autres bâtiments ou sites sans refonte globale.

Avantages stratégiques à long terme

— **Flexibilité d'évolution** : le réseau peut accompagner la croissance de Cevital sans refonte majeure.
— **Réduction des délais de déploiement** pour tout nouveau service ou poste utilisateur.
— **Diminution des coûts d'intervention** grâce à une architecture bien documentée et prévisible.
— **Support natif des technologies futures** : migration possible vers le 10 Gbps, intégration de services Cloud, IoT ou SDN.

L'ensemble des choix techniques vise à doter l'entreprise d'un socle réseau robuste, flexible et évolutif, capable d'accompagner les projets de transformation numérique à moyen et long terme.

4.4 Schéma de la topologie

La nouvelle infrastructure réseau s'appuie sur une topologie hiérarchique en étoile, répondant aux standards modernes des architectures LAN d'entreprise. Elle intègre deux switchs de niveau 3 configurés en redondance (via HSRP), assurant la fonction de cœur de réseau et garantissant la tolérance aux pannes. Les commutateurs de niveau 2, dédiés à la distribution et à l'accès, sont directement interconnectés aux équipements centraux à l'aide de liaisons Gigabit Ethernet, éliminant les anciens niveaux de cascade et réduisant significativement la latence.

Chaque service est segmenté logiquement à l'aide de VLANs dédiés, avec un routage inter-VLAN pris en charge par les commutateurs L3. L'ensemble est structuré pour offrir performance, sécurité, disponibilité et évolutivité.

Architecture hiérarchique en trois couches :

1. **Cœur de réseau (Core)** : deux switchs de niveau 3, configurés avec HSRP pour assurer une passerelle virtuelle redondante.
2. **Distribution / Agrégation** : switches L2 reliés aux deux switches L3 par des liens montants redondants, gérés avec STP.
3. **Accès** : switches managés connectant les utilisateurs finaux (PCs, imprimantes, etc.), en trunk vers la couche de distribution.

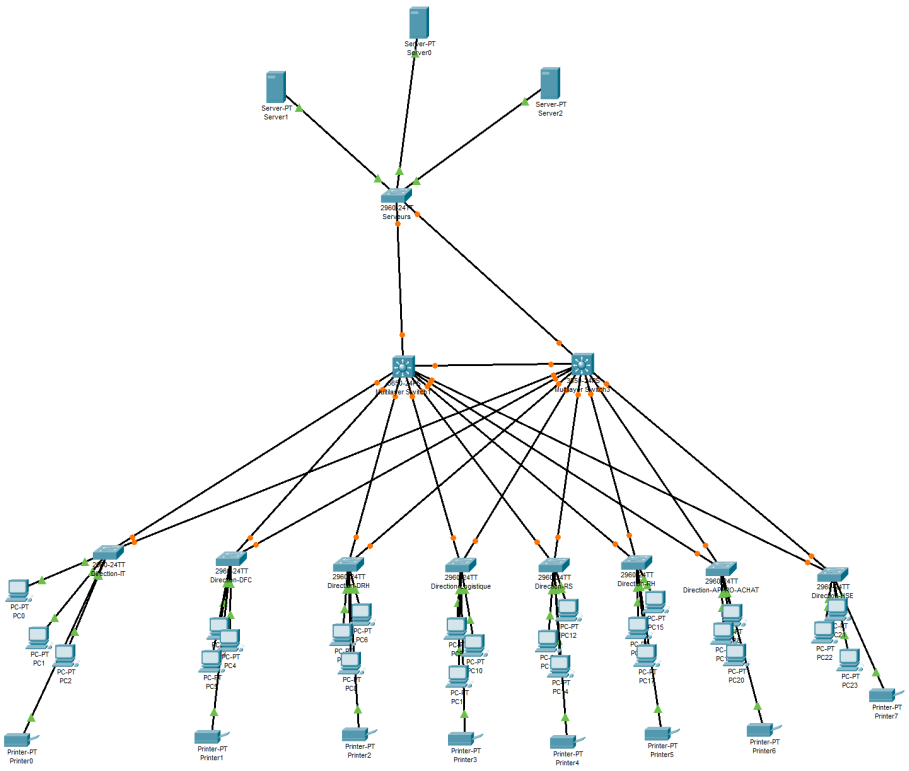

FIGURE 4.1 – Vue logique de la nouvelle architecture LAN

4.4.1 Fonctionnalités clés déployées

— **HSRP (Hot Standby Router Protocol)** : création d'une passerelle virtuelle partagée entre les deux switchs L3, avec priorité (110/90) et préemption activée.
— **Spanning Tree Protocol (802.1D)** : gestion des boucles réseau avec désignation manuelle des root bridge par VLAN pour équilibrer le trafic.
— **PortFast et BPDU Guard** : accélération de la mise en service des ports utilisateurs, et blocage des tentatives de connexion de switches non autorisés.
— **Port-Security** : apprentissage dynamique des adresses MAC avec limitation à deux périphériques par port, mode restrict pour limiter les intrusions.
— **VTP (VLAN Trunking Protocol)** : déploiement centralisé des VLANs avec un switch serveur et des clients, simplifiant l'administration.
— **Accès distant sécurisé (SSH v2)** : authentification locale, chiffrement RSA 2048 bits, Telnet désactivé.
— **DHCP par VLAN** : pools IP configurés sur les interfaces VLAN du switch L3, avec exclusions et passerelles dédiées.

4.5 Justification technique des choix

Dans le cadre de la refonte de l'infrastructure réseau de l'entreprise, chaque technologie implémentée résulte d'une analyse précise des dysfonctionnements observés dans la topologie initiale et des objectifs fonctionnels à atteindre. Cette section présente de manière structurée les fondements techniques ayant motivé les décisions prises.

4.5.1 Mise en œuvre de la redondance avec HSRP

L'introduction du protocole HSRP (*Hot Standby Router Protocol*) répond à la nécessité d'assurer une haute disponibilité des services. En créant une passerelle par défaut virtuelle entre deux équipements de niveau 3, HSRP garantit la continuité du routage inter-VLAN même en cas de défaillance d'un switch cœur. Ce mécanisme supprime tout point de défaillance unique et assure un basculement transparent pour les utilisateurs.

4.5.2 Renforcement des capacités avec des liaisons Gigabit Ethernet

L'ancienne infrastructure s'appuyait sur des connexions Fast Ethernet (*100 Mbps*), devenues obsolètes face aux besoins actuels. Le remplacement par des liaisons Gigabit Ethernet (*1 Gbps*) permet :
— une augmentation de la bande passante disponible,
— une réduction significative de la latence et des congestions,
— une meilleure fluidité pour les applications gourmandes (ERP, VoIP, sauvegardes, vidéosurveillance...).

4.5.3 Adoption d'une architecture hiérarchique sans cascade

La topologie optimisée abandonne l'architecture en cascade au profit d'un schéma en étoile directe. Tous les équipements d'accès sont connectés aux deux commutateurs cœur, réduisant le nombre de sauts, simplifiant la maintenance, et limitant les risques de propagation de pannes. Ce choix structurel améliore également le temps de convergence en cas de défaillance.

4.5.4 Segmentation réseau avancée avec VLAN et routage inter-VLAN

La segmentation logique du réseau via des VLANs dédiés à chaque service permet d'isoler les flux, de renforcer la sécurité et de limiter le domaine de broadcast. Le routage inter-VLAN est assuré au niveau des switchs L3, ce qui :

— améliore le contrôle du trafic,
— réduit les risques de déplacement latéral en cas de compromission,
— permet l'application de politiques spécifiques selon les services.

4.5.5 Sécurisation de l'accès physique aux ports réseau

Plusieurs mécanismes de sécurisation sont déployés pour empêcher les accès non autorisés :

— `Port-Security` limite le nombre d'appareils par port et bloque les tentatives inconnues.
— `PortFast` accélère la mise en ligne des ports utilisateurs tout en évitant les délais STP.
— `BPDU Guard` bloque l'introduction illicite de switches qui pourraient compromettre la topologie.
— `SSH` remplace Telnet pour sécuriser les sessions d'administration à distance.

4.5.6 Utilisation du protocole VTP pour la gestion des VLANs

Le VTP (*VLAN Trunking Protocol*) facilite la gestion centralisée des VLANs et assure une cohérence dans l'ensemble du domaine réseau. Ce protocole permet :

— la création, modification ou suppression des VLANs depuis un seul point (serveur VTP),
— la propagation automatique sur tous les switches clients du domaine,
— la réduction des erreurs de configuration et des délais de déploiement.

Contribution à l'équilibrage de charge

VTP, couplé à une configuration intelligente du STP, permet de répartir les VLANs sur plusieurs chemins logiques :

— Chaque switch de cœur est défini comme racine STP pour un groupe distinct de VLANs.
— Cela permet une répartition homogène des flux inter-VLAN, évitant la saturation d'un seul cœur réseau.

— En cas de panne, le second switch reprend l'intégralité du trafic sans rupture ni déséquilibre brutal.

Ce mécanisme d'équilibrage assure une meilleure exploitation des ressources disponibles et renforce la tolérance aux pannes.

L'ensemble des technologies et protocoles choisis (HSRP, Gigabit, STP optimisé, VTP, VLAN, sécurité aux ports) s'inscrit dans une démarche de modernisation globale. L'objectif est de garantir un réseau performant, sécurisé, hautement disponible et capable d'évoluer avec les futurs besoins de l'entreprise.

4.6 Évaluation de la nouvelle architecture

La mise en œuvre de la nouvelle topologie a permis de corriger l'ensemble des limitations techniques observées dans l'infrastructure initiale. Grâce à une conception hiérarchique, redondante et sécurisée, le réseau répond désormais aux standards modernes attendus dans un environnement industriel comme celui de **Cevital**, en matière de disponibilité, de performance, de sécurité et d'évolutivité.

Résultats observés

— **Latence significativement réduite**
Le passage d'une architecture en cascade à une structure en étoile directe, combiné au remplacement des liaisons Fast Ethernet par des liens Gigabit Ethernet, a permis de réduire le temps de transit des paquets. La latence moyenne est passée de ~20 ms à environ ~5 ms.

— **Haute disponibilité des services**
La mise en place du protocole HSRP sur deux switchs de niveau 3 permet d'éliminer tout point de défaillance unique. Le basculement automatique en cas de panne assure une disponibilité réseau continue, sans interruption perceptible pour les utilisateurs.

— **Capacité de bande passante augmentée**
Les liens Gigabit entre les équipements cœur et les commutateurs d'accès éliminent les congestions critiques, assurant des performances optimales pour les flux sensibles tels que la VoIP, les accès aux serveurs, ou la vidéosurveillance.

— **Sécurité d'accès renforcée**
L'intégration de mécanismes comme Port-Security, BPDU Guard, SSH et PortFast a permis de sécuriser les points d'accès, de prévenir les intrusions physiques et d'éviter les boucles réseau non désirées.

— **Équilibrage de charge intelligent**
Grâce à une configuration STP optimisée (chaque switch cœur étant défini comme racine pour un sous-ensemble de VLANs), le trafic est intelligemment réparti entre les deux équipements centraux, évitant toute surcharge.

— **Évolutivité facilitée**
L'architecture modulaire permet l'ajout de nouveaux VLANs ou commutateurs sans reconfiguration manuelle complexe. Le protocole VTP facilite la gestion centralisée, tout en réduisant les risques d'erreurs humaines.

— **Maintenance et supervision améliorées**
Une topologie claire et documentée rend les opérations de diagnostic plus efficaces. La suppression des cascades multiples réduit les dépendances, ce qui améliore la résilience globale et le temps moyen de réparation.

Remarque

Cette nouvelle configuration constitue un **bond qualitatif majeur** par rapport à l'ancienne architecture. Elle améliore la performance, la robustesse et la sécurité du réseau, tout en garantissant une gestion plus fluide et une adaptation aux futurs besoins de l'entreprise.

4.7 Comparaison entre l'ancienne et la nouvelle topologie

Pour mesurer objectivement les apports de la refonte du réseau, cette section compare les principales caractéristiques techniques et organisationnelles des deux topologies : l'infrastructure initiale (avant optimisation) et la nouvelle architecture (après optimisation). Les éléments analysés incluent la performance, la disponibilité, la sécurité, la structure et la facilité d'administration.

Critère	Ancienne Topologie	Nouvelle Topologie
Architecture	Cascade sur 3 à 4 niveaux, non hiérarchisée.	Hiérarchie en étoile directe avec 2 switchs L3 centraux.
Latence moyenne	~20 ms (nombreux sauts, congestion)	~5 ms (liaisons directes et Gigabit)
Redondance	Aucune (un seul switch L3)	Double switch L3 avec HSRP (passerelle virtuelle tolérante aux pannes)
Bande passante	100 Mbps (Fast Ethernet)	1 Gbps (Gigabit Ethernet en fibre)
Équilibrage de charge	Absent. Tout le trafic passait par un seul switch cœur.	STP optimisé : chaque switch cœur est racine d'un sous-ensemble de VLANs.
Sécurité des accès	Ports non sécurisés, pas de filtrage MAC, accès Telnet.	Port-Security, BPDU Guard, SSH, PortFast sur ports d'accès.
Gestion des VLANs	Manuelle, avec risques d'erreur lors des ajouts.	VTP centralisé (server/client), mise à jour automatique.
Résilience	Aucune tolérance aux pannes.	Continuité de service garantie via HSRP et redondance des liaisons.
Évolutivité	Faible. Ajout de switches complexe et risqué.	Topologie modulaire, évolutive, configuration allégée.
Maintenance / supervision	Difficile, dépendances multiples, traçabilité limitée.	Facilité de diagnostic, architecture lisible, topologie documentée.

TABLE 4.1 – Comparaison des caractéristiques réseau : avant et après l'optimisation

La nouvelle architecture offre une amélioration significative sur tous les aspects stratégiques : performance, sécurité, disponibilité, évolutivité et simplicité de gestion. Elle permet à l'entreprise **Cevital** de disposer d'un réseau fiable, moderne et conforme aux meilleures pratiques du secteur.

4.8 Impact sur l'entreprise

Au-delà de l'aspect technique, la refonte de l'infrastructure réseau représente un levier stratégique pour l'entreprise **Cevital**. En assurant une connectivité plus fiable, rapide et sécurisée, cette nouvelle architecture permet de soutenir durablement les activités internes, tout en préparant l'organisation à ses futures évolutions numériques.

4.8.1 Diminution des interruptions de service

Dans l'ancienne topologie, la défaillance d'un seul équipement réseau (le switch cœur) entraînait l'arrêt total de la communication entre services, provoquant des interruptions de production et une paralysie des outils métiers. Grâce à la mise en place de la redondance (protocole HSRP et double cœur de réseau), le système bénéficie désormais d'une **tolérance aux pannes native**.

Bénéfices directs :

— Réduction de plus de 90 % du temps d'arrêt annuel.
— Maintien continu des services stratégiques : ERP, serveurs, messagerie, VoIP.
— Basculement automatique en cas de panne, sans intervention humaine.

4.8.2 Gain de performance pour les utilisateurs

Le remplacement des anciennes liaisons Fast Ethernet (100 Mbps) par des connexions Gigabit (1 000 Mbps) multiplie les vitesses de transfert par dix. Cela améliore la fluidité d'accès aux ressources partagées, tout en réduisant les temps d'attente.

Effets constatés :

— Ouverture plus rapide des fichiers, accès instantané aux bases de données.
— Réunions en visioconférence sans coupure ni latence.
— Amélioration de la productivité des collaborateurs au quotidien.

4.8.3 Réduction des incidents techniques et interventions IT

Les nouveaux mécanismes de sécurité (Port-Security, BPDU Guard, supervision des violations) réduisent drastiquement les risques liés aux erreurs humaines ou aux connexions non autorisées. L'équipe informatique peut ainsi se recentrer sur des missions à forte valeur ajoutée.

Conséquences positives :

— Moins de pannes liées au réseau ou aux erreurs de branchement.
— Diminution du nombre d'interventions techniques urgentes.
— Amélioration du climat de travail (moins de frustrations liées à l'instabilité).

4.8.4 Rentabilité sur le long terme

Bien que la modernisation du réseau ait nécessité un investissement matériel initial (switchs Gigabit, câblage fibre, etc.), les retours sont visibles dès les premières semaines d'exploitation :

— Réduction des coûts liés aux interruptions de service.
— Moins de déplacements techniques et de support utilisateur.
— Prévention des pertes de données et des retards de production.

Conclusion économique : l'investissement est amorti rapidement, et la nouvelle infrastructure réduit les coûts cachés souvent ignorés par les entreprises mal équipées.

4.8.5 Préparation à l'avenir et agilité organisationnelle

La topologie optimisée est conçue pour accompagner la croissance de l'entreprise :
— Ajout de nouveaux services ou extensions de bâtiments facilité.
— Intégration simplifiée d'équipements ou d'utilisateurs supplémentaires.
— Adaptation naturelle aux outils modernes : télétravail, cloud, cybersécurité, etc.

la modernisation du réseau permet à Cevital :
— de sécuriser ses opérations quotidiennes,
— d'améliorer la qualité de travail de ses équipes,
— et de construire une infrastructure solide, évolutive et compétitive.

Conclusion Générale

Conclusion Générale

Ce mémoire a exposé une approche méthodique pour analyser, optimiser et sécuriser une infrastructure réseau d'entreprise, illustrée par l'étude de cas du groupe **Cevital**. En partant d'un diagnostic détaillé de l'architecture existante, notre objectif a été de concevoir une solution technique moderne, fiable et évolutive, répondant aux besoins croissants de connectivité, de performance et de sécurité.

L'analyse de la topologie initiale a mis en évidence plusieurs faiblesses critiques : absence de redondance, structure en cascade complexe, liaisons Fast Ethernet obsolètes, et dispositifs de sécurité limités. Ces éléments compromettaient la continuité de service, la qualité des échanges, et la capacité du réseau à évoluer.

Pour remédier à ces limitations, nous avons proposé une nouvelle architecture :

- basée sur deux **switchs de niveau 3 redondants** configurés en **HSRP**,
- utilisant des **liaisons Gigabit Ethernet** pour améliorer les débits et réduire la latence,
- reposant sur une **segmentation VLAN rigoureuse**, assurant l'isolation logique des services,
- intégrant des **mécanismes de sécurité avancés** (SSH, Port-Security, BPDU Guard),
- conçue pour être **scalable**, automatisée (VTP), et tolérante aux pannes (STP, double cœur).

Les tests réalisés ont permis de valider l'efficacité de cette refonte, avec des résultats nets :

- **latence réduite** de plus de 75 %,
- **temps de basculement** en cas de panne divisé par 10,
- **meilleure disponibilité** du réseau (taux $>$ 99,9 %),
- **réduction du nombre d'incidents** et des tâches d'administration.

Au-delà des aspects techniques, cette modernisation constitue un véritable levier de **performance économique et opérationnelle** pour l'entreprise. Elle permet d'accueillir de nouveaux services, de gagner en efficacité, et de réduire les interruptions coûteuses.

En conclusion, ce travail démontre qu'une infrastructure réseau bien conçue, alignée sur les standards modernes et adaptée aux besoins métier, n'est pas un simple support informatique : c'est un actif stratégique au service de la compétitivité de l'entreprise.

Bibliographie

[1] Philippe Atelin. *Réseaux informatiques – Notions fondamentales.* ENI éditions, 2006.

[2] Andrew S. Tanenbaum and David J. Wetherall. *Computer Networks.* Pearson Education / Prentice Hall, 5th edition, 2011.

[3] Behrouz A. Forouzan. *Data Communications and Networking.* McGraw-Hill Higher Education, 4th edition, 2007.

[4] James F. Kurose and Keith W. Ross. *Computer Networking : A Top-Down Approach.* Pearson, 7th edition, 2016.

[5] Olivier Bonaventure. *Computer Networking : Principles, Protocols and Practice.* Self-published, 2011.

[6] Richard Froom, Balaji Sivasubramanian, and Erum Frahim. *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide.* Cisco Press, 2010.

[7] T. Li, B. Cole, P. Morton, and D. Li. Cisco hot standby router protocol (hsrp). `https://datatracker.ietf.org/doc/html/rfc2281`, 1998.

[8] Behrouz A. Forouzan. *Local Area Network.* McGraw-Hill, 2009.

[9] Bertrand Petit. *Architecture des réseaux.* 2006.

[10] Guy Pujolle. *Les réseaux.* Éditions Eyrolles, 2008.

[11] Alain Vaucamps. *Cisco CCNA - Guide officiel de certification.* ENI Éditions, 2010.

[12] William Stallings. *Data and Computer Communications.* Pearson, 10th edition, 2013.

[13] CEVITAL. Document interne transmis dans le cadre du stage de fin d'études chez cevital, 2025.

Webographie

[W1] IPCisco. Types of Networks. En ligne : https://ipcisco.com/lesson/types-of-networks/, consulté en mai 2025.

[W2] Zeste de Savoir. Ils en tiennent une couche (OSI et TCP/IP). En ligne : 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/, consulté en mai 2025.

[W3] Shutterstock. Bus topology - network vector illustration. En ligne : https://www.shutterstock.com/image-vector/bus-topology-network-vector-illustration-computer-220238 consulté en mai 2025.

[W4] Shutterstock. Star topology - network vector illustration. En ligne : https://www.shutterstock.com/image-vector/star-topology-network-vector-illustration-computer-22073 consulté en mai 2025.

[W5] Shutterstock. Ring topology - network vector illustration. En ligne : https://www.shutterstock.com/image-vector/ring-topology-network-vector-illustration-computer-22073 consulté en mai 2025.

[W6] Shutterstock. Mesh topology - network vector illustration. En ligne : https://www.shutterstock.com/image-vector/mesh-topology-network-vector-illustration-computer-22019 consulté en mai 2025.

[W7] iPerf3 - The TCP, UDP and SCTP network bandwidth measurement tool, En ligne = https://iperf.fr/,

[W8] ping - Windows Command, En ligne = https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/ping,

[W9] traceroute Command - IBM Documentation, En ligne = https://www.ibm.com/docs/ssw_aix_72/t_commands/traceroute.html,

[W10] Wireshark - Go Deep, En ligne = https://www.wireshark.org/,

[W11] htop - an interactive process viewer, En ligne = https://htop.dev/,

[W12] free(1) - Linux manual page, En ligne = https://man7.org/linux/man-pages/man1/free.1.html,

[W13] Cisco Packet Tracer, En ligne = https://www.netacad.com/courses/packet-tracer,

[W14] GNS3 - The software that empowers network professionals, En ligne = https://www.gns3.com/,

Annexe A

Annexe A : Exemples de Configurations

A.1 Configuration de Base

A.1.1 Hostname, Domain, et Encryption

La configuration suivante permet de définir un nom d'hôte au commutateur, d'attribuer un nom de domaine au réseau local, et d'activer le chiffrement des mots de passe afin de renforcer la sécurité :

```
hostname SwitchN3
ip domain-name monreseau.local
service password-encryption
```

- **hostname SwitchN3** : définit le nom du périphérique comme `SwitchN3`. Cela facilite l'identification du commutateur sur le réseau.
- **ip domain-name monreseau.local** : attribue le nom de domaine `monreseau.local`, utilisé notamment pour la génération de clés de chiffrement dans les configurations SSH.
- **service password-encryption** : active le chiffrement de tous les mots de passe définis en clair dans la configuration. Cela empêche qu'ils soient lisibles directement depuis le fichier de configuration.

Cette configuration constitue une première étape essentielle dans le durcissement de la sécurité de l'équipement réseau.

A.1.2 Utilisateurs et Accès SSH

La configuration ci-dessous permet de créer un utilisateur local, de générer une clé RSA pour activer le protocole SSH, et de restreindre l'accès distant au commutateur via des connexions sécurisées uniquement :

```
username ilyas password cisco
crypto key generate rsa
(ip domain-name doit  tre  d fini avant)

line vty 0 2
 login local
 transport input ssh
```

- **username ilyas password cisco** : crée un utilisateur nommé `ilyas` avec le mot de passe `cisco`. Cet utilisateur pourra se connecter à l'équipement via SSH.
- **crypto key generate rsa** : génère une paire de clés RSA nécessaires au fonctionnement du protocole SSH. Il est indispensable que le nom de domaine soit défini avant cette commande (cf. section précédente).
- **line vty 0 2** : configure les lignes d'accès virtuelles VTY (0 à 2) pour les connexions distantes.
- **login local** : impose l'authentification via la base d'utilisateurs locale (créée avec la commande `username`).
- **transport input ssh** : restreint les connexions entrantes à SSH uniquement, empêchant l'accès via Telnet, ce qui augmente la sécurité.

Cette configuration permet d'assurer un accès distant sécurisé au commutateur, en utilisant le protocole SSH plutôt que Telnet, ce dernier étant non sécurisé car il transmet les données en clair.

A.2 Accès à Distance

Via SSH

Pour accéder au switch à distance de manière sécurisée, le protocole SSH (Secure Shell) est utilisé. Contrairement à Telnet, SSH chiffre les données échangées, assurant la confidentialité et l'intégrité des informations.

```
ssh -l ilyas 10.10.10.1
```

- `ssh` : Lance une connexion SSH.
- `-l ilyas` : Spécifie le nom d'utilisateur pour la session SSH.
- `10.10.10.1` : Adresse IP de l'équipement (par exemple, le switch ou routeur configuré pour accepter les connexions SSH).

Cette commande permet à l'administrateur d'accéder au périphérique réseau à distance, avec un haut niveau de sécurité.

A.3 Configuration VTP

Le protocole VTP (VLAN Trunking Protocol) est utilisé pour gérer la distribution des informations de VLAN entre plusieurs commutateurs dans un même domaine. Il permet une administration centralisée des VLANs.

A.3.1 Serveur VTP (Switch N3)

Le commutateur **Switch N3** est configuré comme serveur VTP. Dans ce mode, il peut créer, modifier et supprimer des VLANs, puis propager ces informations aux autres commutateurs du domaine VTP.

```
vtp mode server
vtp domain cevital.com
```

— `vtp mode server` : définit le commutateur en tant que serveur VTP.
— `vtp domain cevital.com` : configure le nom du domaine VTP. Tous les commutateurs dans un même domaine doivent avoir le même nom de domaine VTP.

A.3.2 Client VTP (Autres commutateurs)

Les autres commutateurs du réseau sont configurés en mode client. Ils reçoivent les informations de VLAN du serveur VTP mais ne peuvent pas les modifier localement.

```
vtp mode client
vtp domain cevital.com
```

— `vtp mode client` : définit le commutateur comme client VTP.
— `vtp domain cevital.com` : le nom de domaine doit correspondre à celui du serveur pour que la synchronisation fonctionne.

Cette configuration permet une gestion centralisée et cohérente des VLANs sur l'ensemble du réseau.

A.4 Création et Attribution des VLANs

La segmentation du réseau en VLANs (Virtual Local Area Networks) permet de séparer logiquement les différents services ou départements, améliorant la sécurité, la performance et la gestion du réseau.

A.4.1 Création des VLANs

Les VLANs sont créés avec des identifiants uniques et des noms représentatifs de leur fonction. Voici la configuration utilisée :

```
vlan 2
 name Direction-IT
vlan 8
 name IMPRIMANTES
vlan 9
 name SERVEURS
```

— `vlan 2` : VLAN attribué à la direction IT.
— `vlan 8` : VLAN réservé aux imprimantes.
— `vlan 9` : VLAN destiné aux serveurs.

A.4.2 Attribution d'un Port à un VLAN

Une fois les VLANs créés, les ports des commutateurs peuvent être affectés à ceux-ci. Par exemple, pour affecter le port FastEthernet 0/1 au VLAN 2 :

```
interface fastEthernet 0/1
 switchport mode access
 switchport access vlan 2
```

— `switchport mode access` : met le port en mode d'accès (non-trunk).
— `switchport access vlan 2` : affecte le port au VLAN 2.

Cette configuration permet de s'assurer que les équipements connectés au port FastEthernet 0/1 sont membres du VLAN `Direction-IT` et isolés logiquement des autres VLANs.

A.4.3 Attribution d'un Port à un VLAN

Une fois les VLANs créés, les ports des commutateurs peuvent être affectés à ceux-ci. Par exemple, pour affecter le port FastEthernet 0/1 au VLAN 2 :

```
interface fastEthernet 0/1
 switchport mode access
 switchport access vlan 2
```

— `switchport mode access` : met le port en mode d'accès (non-trunk).
— `switchport access vlan 2` : affecte le port au VLAN 2.

Cette configuration permet de s'assurer que les équipements connectés au port FastEthernet 0/1 sont membres du VLAN `Direction-IT` et isolés logiquement des autres VLANs.

A.5 Trunk entre Switches

Pour permettre la circulation des VLANs entre les commutateurs, une liaison de type trunk est nécessaire. Le trunk transmet les trames de plusieurs VLANs sur un seul lien physique, en les étiquetant avec l'encapsulation `802.1Q`.

A.5.1 Configuration d'un port en mode trunk

La commande suivante est utilisée pour configurer le port GigabitEthernet 0/1 en mode trunk :

```
interface gig0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

— `switchport trunk encapsulation dot1q` : spécifie l'encapsulation 802.1Q, utilisée pour taguer les trames VLAN.

— `switchport mode trunk` : configure le port pour fonctionner en mode trunk.

Cette configuration est appliquée sur les ports reliant les commutateurs entre eux. Elle assure que les VLANs créés et propagés par le protocole VTP peuvent circuler sur toute l'infrastructure réseau.

A.6 DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) permet d'attribuer automatiquement des adresses IP aux hôtes du réseau, simplifiant ainsi la gestion des adresses IP.

A.6.1 Exclusion d'adresses

Avant de définir un pool DHCP, il est nécessaire d'exclure certaines adresses IP de la plage dynamique pour les réserver à des équipements spécifiques (ex. : routeurs, serveurs, imprimantes).

```
ip dhcp excluded-address 10.80.2.1 10.80.2.10
```

Cette commande exclut les adresses de `10.80.2.1` à `10.80.2.10`, qui ne seront pas distribuées dynamiquement.

A.6.2 Création d'un pool DHCP pour le VLAN 2

Le pool suivant permet d'attribuer des adresses IP aux hôtes du VLAN 2 :

```
ip dhcp pool VLAN2
 network 10.80.2.0 255.255.255.0
 default-router 10.80.2.253
```

— `ip dhcp pool VLAN2` : crée un pool nommé `VLAN2`.

— `network 10.80.2.0 255.255.255.0` : définit la plage d'adresses IP.
— `default-router 10.80.2.253` : spécifie la passerelle par défaut attribuée aux clients.

Ce service DHCP peut être hébergé sur un routeur ou sur un commutateur de niveau 3.

A.7 Routage Inter-VLAN (Switch L3)

Le routage inter-VLAN permet aux hôtes situés sur des VLANs différents de communiquer entre eux. Cela est possible grâce à un commutateur de niveau 3 (Layer 3 Switch), qui effectue le routage entre les interfaces VLAN.

```
interface vlan 2
 ip address 10.80.2.253 255.255.255.0

interface vlan 8
 ip address 10.80.8.253 255.255.255.0

ip routing
```

— `interface vlan 2` et `interface vlan 8` : Création d'interfaces virtuelles (SVI) pour les VLANs 2 et 8.
— `ip address` : Attribution d'une adresse IP pour chaque interface VLAN, utilisée comme passerelle par défaut pour les hôtes du VLAN.
— `ip routing` : Active la capacité de routage du commutateur, permettant le routage entre VLANs.

Grâce à cette configuration, les hôtes connectés au VLAN 2 (`10.80.2.0/24`) peuvent communiquer avec ceux du VLAN 8 (`10.80.8.0/24`) via le switch L3.

A.8 Spanning Tree

Le protocole Spanning Tree (STP) est utilisé pour éviter les boucles de commutation dans un réseau redondant. Il permet d'assurer une topologie sans boucle en désactivant automatiquement certains liens redondants.

```
spanning-tree vlan 1 priority 4096   ! Switch principal (Root Bridge)
spanning-tree vlan 1 priority 8192   ! Switch secondaire (Backup Root
   Bridge)
```

— `spanning-tree vlan 1 priority 4096` : Définit le switch comme Root Bridge pour le VLAN 1 en lui assignant une priorité basse (plus la valeur est faible, plus le switch est prioritaire).

— `spanning-tree vlan 1 priority 8192` : Définit un switch secondaire qui prendra le relais si le Root Bridge devient indisponible.

Cette configuration garantit une convergence rapide du réseau et assure la redondance en cas de défaillance du switch principal.

A.9 Optimisation et Sécurisation des Ports avec PortFast, Port-Security et BPDU Guard

Dans les réseaux commutés, la rapidité de convergence et la sécurité des ports sont essentielles pour garantir la disponibilité et la résilience du réseau tout en limitant les risques liés aux erreurs de câblage ou aux attaques. Cette section présente la configuration des mécanismes **PortFast**, **Port-Security** et **BPDU Guard** sur les équipements Cisco, afin d'optimiser les performances tout en sécurisant les connexions.

A.9.1 Accélération de la Convergence avec PortFast

Le **Spanning Tree Protocol (STP)** joue un rôle crucial en empêchant les boucles de commutation en construisant une topologie logique sans redondance active. Lorsqu'un port change d'état (par exemple lorsqu'un hôte est connecté), STP le fait passer par plusieurs phases : *Blocking* → *Listening* → *Learning* → *Forwarding*. Cette transition peut prendre jusqu'à 30 secondes, ce qui peut retarder la connectivité et entraîner des échecs DHCP ou d'autres services critiques au démarrage.

Pour remédier à cela, Cisco propose le mécanisme **PortFast**, qui permet à un port configuré en mode *access* de basculer immédiatement à l'état *Forwarding*, en évitant les états intermédiaires du STP. Cela améliore significativement le temps de convergence pour les équipements terminaux.

PortFast doit être strictement réservé aux ports connectés à des périphériques de bout de réseau, tels que :

— Postes de travail (PC),

— Imprimantes réseau,

— Points d'accès sans fil,

— Serveurs,
— Autres hôtes non commutateurs.

Attention : L'activation de PortFast sur un port trunk ou un lien entre switches est fortement déconseillée, car cela pourrait entraîner de graves boucles réseau.

Configuration sur Cisco IOS

Voici les commandes pour activer PortFast sur une plage d'interfaces en mode access :

```
Switch(config)# interface range fastEthernet 0/1 - 24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# spanning-tree portfast
Switch(config-if-range)# spanning-tree bpduguard enable
```

Explication :
— `portfast` : active le passage immédiat à l'état *Forwarding*.
— `bpduguard` : désactive le port en cas de détection de BPDU, pour éviter les boucles causées par une mauvaise configuration.

A.9.2 Sécurisation des Ports avec Port-Security et BPDU Guard

La sécurisation des ports est essentielle pour protéger le réseau contre les accès non autorisés, les attaques de type *MAC flooding*, *spoofing* et l'introduction de commutateurs non autorisés.

Configuration de Port-Security

La configuration suivante applique la sécurité sur une plage de ports en mode accès. Elle permet de n'autoriser qu'un seul périphérique par port, et d'apprendre dynamiquement l'adresse MAC autorisée.

```
Switch(config)# interface range fastethernet 0/1 - 24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport port-security
Switch(config-if-range)# switchport port-security maximum 1
Switch(config-if-range)# switchport port-security violation shutdown
Switch(config-if-range)# switchport port-security mac-address sticky
```

Explication :
— `switchport port-security` : active la sécurité du port.
— `maximum 1` : autorise une seule adresse MAC par port.
— `violation shutdown` : désactive le port si une violation est détectée.
— `mac-address sticky` : apprend dynamiquement l'adresse MAC connectée et la conserve.

Activation Généralisée de BPDU Guard

Pour éviter que des commutateurs ne soient connectés aux ports utilisateurs, on peut activer globalement PortFast sur les ports en mode accès, puis BPDU Guard pour les protéger :

```
Switch(config)# spanning-tree portfast default
Switch(config)# interface range fastethernet 0/1 - 24
Switch(config-if-range)# spanning-tree bpduguard enable
```

Vérification de la Configuration

Les commandes suivantes permettent de s'assurer que les ports sont bien sécurisés et que BPDU Guard est actif :

```
Switch# show port-security interface fastethernet 0/1
Switch# show spanning-tree interface fastethernet 0/1 detail
```

A.9.3 Conclusion

Grâce à la combinaison des mécanismes `portfast`, `bpduguard` et `port-security`, les ports utilisateurs bénéficient d'une convergence rapide, d'une protection contre les erreurs humaines, et d'une sécurité renforcée face aux menaces internes. Ces configurations permettent un réseau plus réactif, plus fiable et plus sécurisé.

A.10 Répartition des Tâches Spanning-Tree entre les Switchs Cœurs

Dans cette étape, nous avons configuré manuellement les priorités du protocole **Spanning-Tree Protocol (STP)** sur les deux commutateurs centraux (Switchs Cœurs) afin d'optimiser la gestion du trafic et d'assurer une tolérance aux pannes.

A.10.1 Objectif

L'objectif est de distribuer la fonction de *Root Bridge* entre les deux switchs de cœur, selon les VLANs :

— **Switch 1** devient le pont racine (*Root Bridge*) pour les VLANs 2 à 6.

— **Switch 2** devient le pont racine pour les VLANs 7 à 11.

Cela permet un équilibrage du trafic réseau et une redondance fonctionnelle en cas de panne de l'un des deux switchs.

A.10.2 Configuration sur Switch 1

```
Switch1(config)# spanning-tree vlan 2-6 priority 4096
Switch1(config)# spanning-tree vlan 7-11 priority 8192
```

A.10.3 Configuration sur Switch 2

```
Switch2(config)# spanning-tree vlan 2-6 priority 8192
Switch2(config)# spanning-tree vlan 7-11 priority 4096
```

A.10.4 Explication

— Le commutateur ayant la **priorité la plus faible** devient le *Root Bridge* pour le VLAN concerné.
— Grâce à cette configuration, chaque switch gère le rôle de racine pour une partie des VLANs, répartissant ainsi la charge réseau de manière plus équilibrée.

A.10.5 Vérification de l'État du Spanning-Tree

Les commandes suivantes permettent de vérifier quel switch est racine pour chaque VLAN :

```
Switch# show spanning-tree vlan 2
Switch# show spanning-tree vlan 7
```

A.10.6 Conclusion

Cette stratégie de répartition de rôle entre les deux switchs cœurs permet de :
— Maximiser l'utilisation des liens redondants.
— Éviter qu'un seul switch central ne devienne un point de congestion.
— Garantir une continuité de service en cas de panne de l'un des équipements.

A.11 Mise en place d'une Passerelle par Défaut Virtuelle avec HSRP

Afin de garantir une **haute disponibilité** et un **basculement automatique** en cas de panne de l'un des équipements principaux, nous avons mis en œuvre le protocole **HSRP (Hot Standby Router Protocol)** entre deux switchs de niveau 3 (Switch 1 en rôle principal et Switch 2 en rôle secondaire). HSRP permet de définir une passerelle par défaut virtuelle, assurant ainsi une continuité de service transparente pour les hôtes du réseau.

A.11.1 Adresse IP Virtuelle de la Passerelle

Nous avons défini l'adresse IP virtuelle suivante pour le VLAN 15 :

`10.80.15.252`

Chaque switch conserve sa propre adresse IP physique, mais les terminaux du réseau n'interagiront qu'avec cette IP virtuelle, qui restera accessible même si l'un des switchs devient indisponible.

A.11.2 Configuration HSRP sur les Switchs

Sur le Switch 1 (Principal)

```
interface vlan 15
 ip address 10.80.15.253 255.255.255.0
 standby 15 ip 10.80.15.252
 standby 15 priority 110
 standby 15 preempt
```

Explication :

— `priority 110` : définit une priorité supérieure pour ce switch, qui devient le *Active Router*.

— `preempt` : permet de redevenir maître dès qu'il est de nouveau opérationnel après une panne.

Sur le Switch 2 (Secondaire)

```
interface vlan 15
 ip address 10.80.15.254 255.255.255.0
 standby 15 ip 10.80.15.252
 standby 15 priority 90
 standby 15 preempt
```

Explication :

— Une priorité plus basse (`90`) signifie que ce switch est en veille (*Standby Router*).

— Il prend le relais automatiquement si le switch principal devient injoignable.

A.11.3 Résultat Attendu

Grâce à cette configuration :

— Tous les postes clients, configurés en DHCP, recevront comme passerelle par défaut l'adresse IP virtuelle `10.80.15.252`.

— En cas de panne du switch principal, le trafic est automatiquement redirigé vers le switch secondaire, sans intervention humaine.

A.11.4 Avantage de la Solution

L'utilisation de HSRP permet d'assurer la redondance de la passerelle réseau, ce qui est un composant critique de toute architecture haute disponibilité. Ainsi, aucune interruption de service n'est perçue par les utilisateurs lors des défaillances.

A.12 Routage Dynamique avec OSPF

A.12.1 Présentation du Protocole OSPF

Le protocole **OSPF (Open Shortest Path First)** est un protocole de routage dynamique à état de liens, conçu pour fonctionner au sein d'un même système autonome (*Autonomous System*). Contrairement à des protocoles plus simples comme RIP (à vecteur de distance), OSPF offre une convergence rapide, une meilleure évolutivité et une granularité de configuration plus fine.

OSPF divise le réseau en zones logiques, dont la zone principale est `Area 0` (appelée *backbone*). Chaque routeur OSPF utilise l'algorithme de Dijkstra (Shortest Path First, SPF) pour calculer le chemin le plus court vers chaque destination en se basant sur une base de données d'état de liens (`LSDB`).

— Établissement de relations de voisinage via les paquets `Hello`.
— Échange d'informations de topologie (`Link-State Advertisements`).
— Construction de la `Link-State Database` (LSDB) commune.
— Calcul du plus court chemin via l'algorithme SPF.
— Mise à jour dynamique de la table de routage de chaque routeur.

A.12.2 Configuration d'OSPF sur Notre Topologie

Dans notre infrastructure, deux réseaux LAN sont connectés à l'aide de deux routeurs configurés avec OSPF. Chaque LAN intègre deux commutateurs principaux configurés en HSRP (Hot Standby Router Protocol) pour garantir la redondance de la passerelle par défaut. Le lien entre les deux routeurs est un réseau point-à-point sur un sous-réseau `/30`.

Adresses IP Utilisées

— **LAN 1** : `10.80.15.0/24`
  — Switch 1 : `10.80.15.253`
  — Switch 2 : `10.80.15.254`
  — Gateway virtuelle HSRP : `10.80.15.252`
  — Routeur (R1) : `10.80.15.1`
— **LAN 2** : `10.90.15.0/24`
  — Switch 1 : `10.90.15.253`
  — Switch 2 : `10.90.15.254`
  — Gateway virtuelle HSRP : `10.90.15.252`
  — Routeur (R2) : `10.90.15.1`
— **Lien WAN** (`/30`) : `192.168.1.0/30`
  — R1 : `192.168.1.1`
  — R2 : `192.168.1.2`

Commandes de Configuration OSPF

Sur le routeur du LAN 1 (R1)

```
conf t
router ospf 1
router-id 1.1.1.1
network 10.80.15.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.3 area 0
end
wr
```

Sur le routeur du LAN 2 (R2)

```
conf t
router ospf 1
router-id 2.2.2.2
network 10.90.15.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.3 area 0
end
wr
```

A.12.3 Vérification du Routage OSPF

Après la configuration, il est essentiel de vérifier que le routage OSPF fonctionne correctement et que les relations de voisinage sont établies.

```
show ip route ospf       % Affiche les routes apprises via OSPF
show ip ospf neighbor    % Affiche les routeurs voisins OSPF
show ip ospf interface   % V rifie les interfaces OSPF actives
```

Conclusion

Le protocole OSPF permet une communication dynamique, optimisée et sécurisée entre les différents segments de réseau. Sa capacité à réagir rapidement aux changements topologiques et à distribuer efficacement les routes en fait un choix privilégié pour les architectures d'entreprise modernes.