

الكلية متعددة التخصصات - ورزازات
+٥٢٤٦٠١٧ +٥٣٩٤٨٤٦ - ٠٥٠٧٠٣٠٦
FACULTÉ POLYDISCIPLINAIRE DE OUARZAZATE



LA FACULTÉ POLYDISCIPLINAIRE DE OUARZAZATE - UIZ
DÉPARTEMENT MATH - CYBERSÉCURITÉ S03 - 2025/2026

MODULE SYSTÈME ET RÉSEAUX III

Rapport

CONCEPTION ET MISE EN ŒUVRE D'UNE INFRASTRUCTURE CAMPUS À TROIS COUCHES SOUS PACKET TRACER^(v9.0.0)

Professeur:

Dakir Rachid

Étudiant:

Siki Bilal

P. 03 -- 06

- I. Introduction/Objectives
- II. Network topologie
- III. Conception architecturale
- IV. Détails de configuration
- V. Conclusion/Recommendations

P. 07 -- 14

P. 14 -- 18

P. 18 -- 42

P. 43 -- 44

SOMMAIRE



I. Introduction/Objectives

1. Introduction générale

Dans le cadre du module de Réseaux, ce projet porte sur la conception, la configuration et le déploiement d'une infrastructure réseau d'entreprise évolutive et robuste. L'architecture retenue repose sur le modèle hiérarchique à trois couches **Three-Layer Architecture**, composé des couches Cœur (Core), Distribution et Accès. Ce modèle est standardisé par l'industrie pour garantir la haute disponibilité, la scalabilité et la facilité de gestion.

L'objectif principal de ce rapport est de démontrer la mise en œuvre d'un réseau capable de supporter la convergence des flux Voix et Données (Voice & Data), tout en assurant une gestion centralisée et un routage inter-services efficace. Le projet ne se limite pas à la connectivité de base ; il intègre une dimension sécuritaire approfondie et des services d'infrastructure essentiels pour répondre aux exigences modernes d'un environnement professionnel.

Le déploiement a été réalisé de manière incrémentale, allant de la définition de la topologie physique jusqu'à l'intégration de services avancés tels que la Téléphonie sur IP (VoIP) et le durcissement de la sécurité (Hardening) via des listes de contrôle d'accès (ACLs) et des protocoles d'authentification.

2. Objectifs du Projet

Les objectifs de ce projet se déclinent en plusieurs phases techniques, couvrant les couches 1 à 3 du modèle OSI ainsi que les services applicatifs. Ils peuvent être synthétisés comme suit :

1. Conception et Architecture Physique :

Établir une topologie hiérarchique claire distinguant les rôles des équipements (Cœur, Distribution, Accès) pour optimiser les flux de trafic

Définir les normes de câblage et la cartographie des ports (Port Mapping), en assurant la distinction entre les liaisons inter-switchs (Trunk) et les connexions aux terminaux (Access).

2. Connectivité et Commutation (Switching) :

Segmenter le réseau via la création de VLANs dédiés (Données, Voix, Gestion) pour isoler les domaines de diffusion.

Configurer le protocole VTP (VLAN Trunking Protocol) pour



centraliser la gestion de la base de données VLAN et assurer sa cohérence sur l'ensemble du domaine.

Mettre en œuvre le routage Inter-VLAN via des Interfaces Virtuelles de Switch (SVI) sur le commutateur multicouche (MLS), permettant la communication entre les différents sous-réseaux.

3. Services Réseau et Gestion d'Adressage :

Déployer une architecture DHCP dynamique : Configuration du Cœur de réseau comme serveur DHCP principal et mise en place du relais DHCP (ip helper-address) sur les couches inférieures pour l'attribution automatique des adresses IP.

Assurer la synchronisation et la journalisation via l'implémentation du protocole NTP (Network Time Protocol) pour la cohérence des horloges et de Syslog pour l'audit centralisé des événements système.

Garantir la maintenance avec la mise en place de serveurs TFTP pour la sauvegarde des configurations (startup-config).

4. Sécurité et Contrôle d'Accès :

Contrôler l'administration réseau grâce au framework AAA (Authentication, Authorization, Accounting) couplé à un serveur RADIUS pour centraliser les accès administrateurs.

Sécuriser la couche Accès par le biais du Port Security (mode sticky, limitation des adresses MAC) et du DHCP Snooping pour prévenir les attaques de type "Man-in-the-Middle" ou les serveurs DHCP roges.

Filtrer le trafic à l'aide de Listes de Contrôle d'Accès (ACLs) standards et étendues. Cela inclut une conception récursive pour protéger le VLAN de gestion et réguler strictement les flux entre les zones sensibles et les utilisateurs standards.

5. Performance et Services Convergents :

Optimiser la bande passante et la redondance via l'agrégation de liens (EtherChannel avec le protocole LACP) entre les commutateurs, garantissant la tolérance aux pannes sur les liens montants (Uplinks).

Intégrer les services de Téléphonie (VoIP) : Ajout d'un routeur dédié connecté au Cœur de réseau pour gérer les services de téléphonie (CME – Call Manager Express) et l'assignation des numéros aux téléphones IP.

3. Périmètre du Projet



Ce projet vise à concevoir et simuler une infrastructure réseau de campus complète, robuste et évolutive. Le déploiement couvre l'interconnexion de plusieurs bâtiments (Bloc Administratif, Salle Serveur, Faculté, Annexe) à travers une architecture hiérarchique commutée.

Le périmètre matériel et fonctionnel inclut :

Équipements Réseau (Network Devices) :

- 1x Switch Core (L3) : Point central de routage et de gestion du trafic inter-VLAN.
- 4x Switchs de Distribution : Agrégation des liens provenant des différents bâtiments et blocs fonctionnels.
- 6+ Switchs d'Accès : Connectivité pour les utilisateurs finaux avec gestion de la sécurité (Port Security).
- 1x Routeur de Bordure (Prévu) : Pour la gestion future des appels VoIP (CME) et le routage externe.

Terminaux et Services (Endpoints) :

50+ Postes de travail simulés (PC) : Répartis sur différents départements (Compta, Info, Math, etc.).

Téléphonie IP : Déploiement prévu de téléphones IP dans chaque département sur un VLAN voix dédié.

Serveurs Critiques : Infrastructure centralisée incluant DHCP, TFTP, et Authentification AAA (RADIUS), SYSLOGS, NTP.

4. Hypothèses et Prérequis Techniques

La conception du réseau repose sur les hypothèses techniques suivantes pour assurer la cohérence de la simulation :

Bande Passante et Câblage :

Les liaisons inter-switchs (Backbone) sont supposées être en **Gigabit Ethernet (1 Gbps)**, agrégées par liens **EtherChannel** pour atteindre jusqu'à 2-4 Gbps de débit théorique.

Les liaisons utilisateurs (Access) sont en **FastEthernet (100 Mbps)**.

Alimentation Électrique (PoE) :

Il est supposé que les commutateurs d'accès fournissent le **Power over Ethernet (PoE)** nécessaire pour alimenter les téléphones IP sans adaptateurs externes.



Environnement de Simulation :

Le projet est réalisé sous Cisco Packet Tracer. Certaines commandes avancées (ex: VACLs complexes, Inspection ARP dynamique) sont adaptées aux limitations logicielles du simulateur.

5. Critères de Réussite

Le projet sera considéré comme validé si les indicateurs de performance et de fonctionnalité suivants sont atteints :

1. Connectivité & Routage :

- **100% de réussite des tests de ping entre tous les VLANs autorisés (Inter-VLAN Routing opérationnel).**

2. Haute Disponibilité :

- Continuité de service assurée en cas de rupture d'un câble physique grâce à l'agrégation de liens (EtherChannel).

3. Sécurité de l'Accès (Access Layer Security) :

- Le **Port Security** doit bloquer immédiatement tout appareil non autorisé (Rogue Device).
- Le **DHCP Snooping** doit empêcher toute distribution d'adresses IP par un serveur pirate.

4. Sécurité du Réseau (Network Security – Phase 2) :

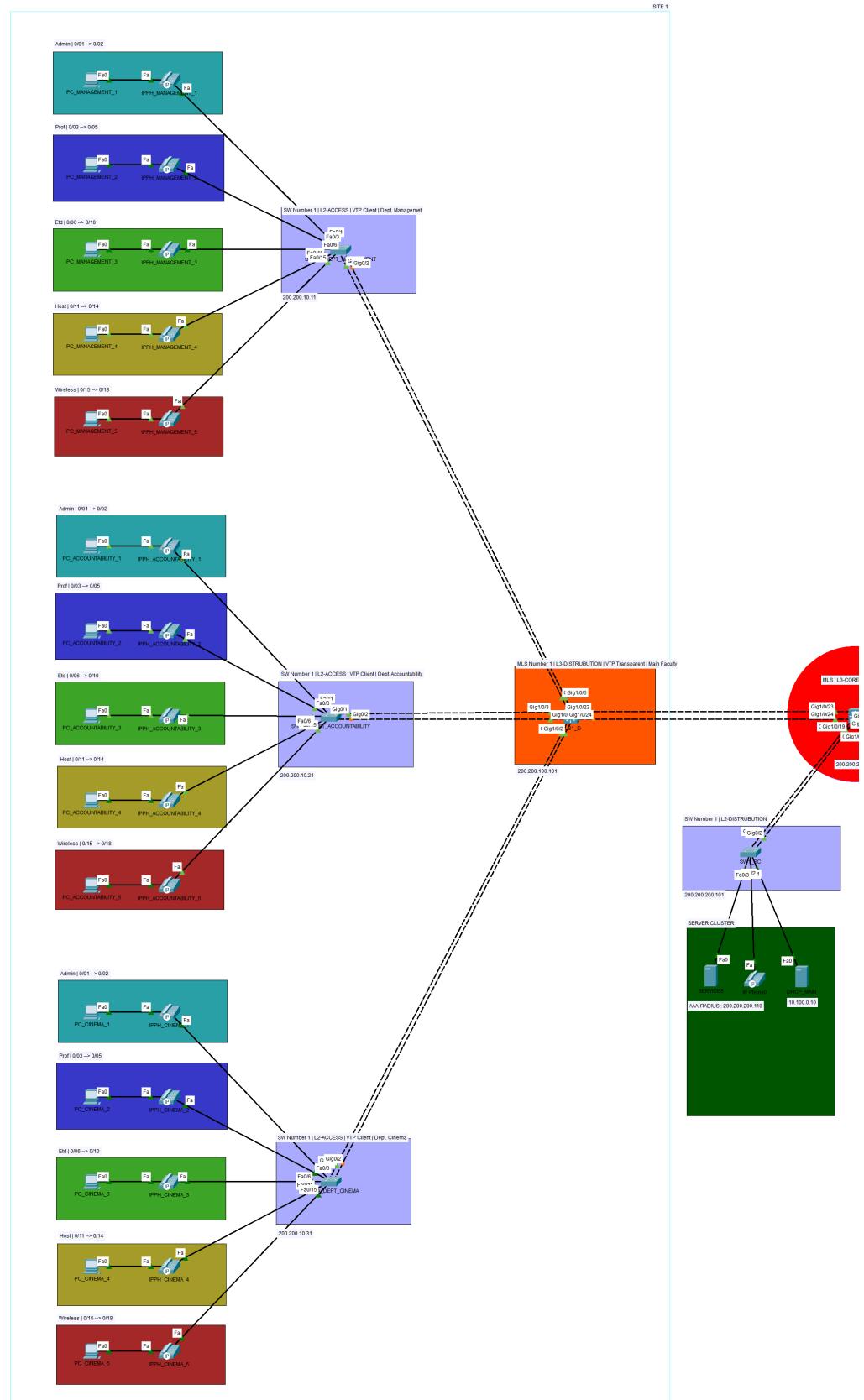
- Les **ACLs** doivent bloquer efficacement le trafic étudiant vers le réseau d'administration et les serveurs sensibles.
- L'**authentification AAA** doit sécuriser l'accès administratif aux équipements.

5. Services Convergents (Phase 3) :

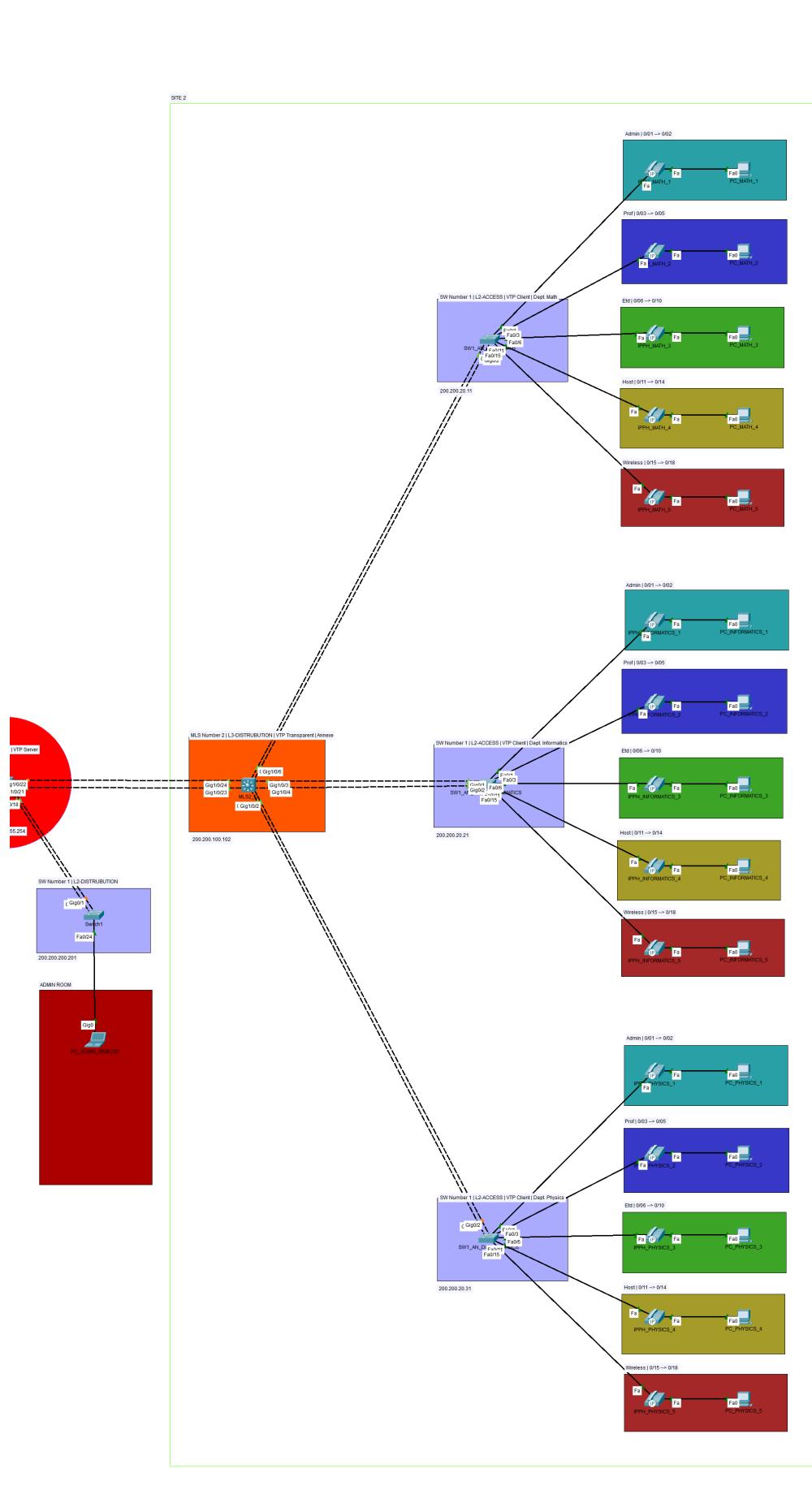
- Les **appels VoIP** doivent fonctionner avec une qualité claire entre les différents bâtiments (VLANs Voix isolés).

II. Network topologie

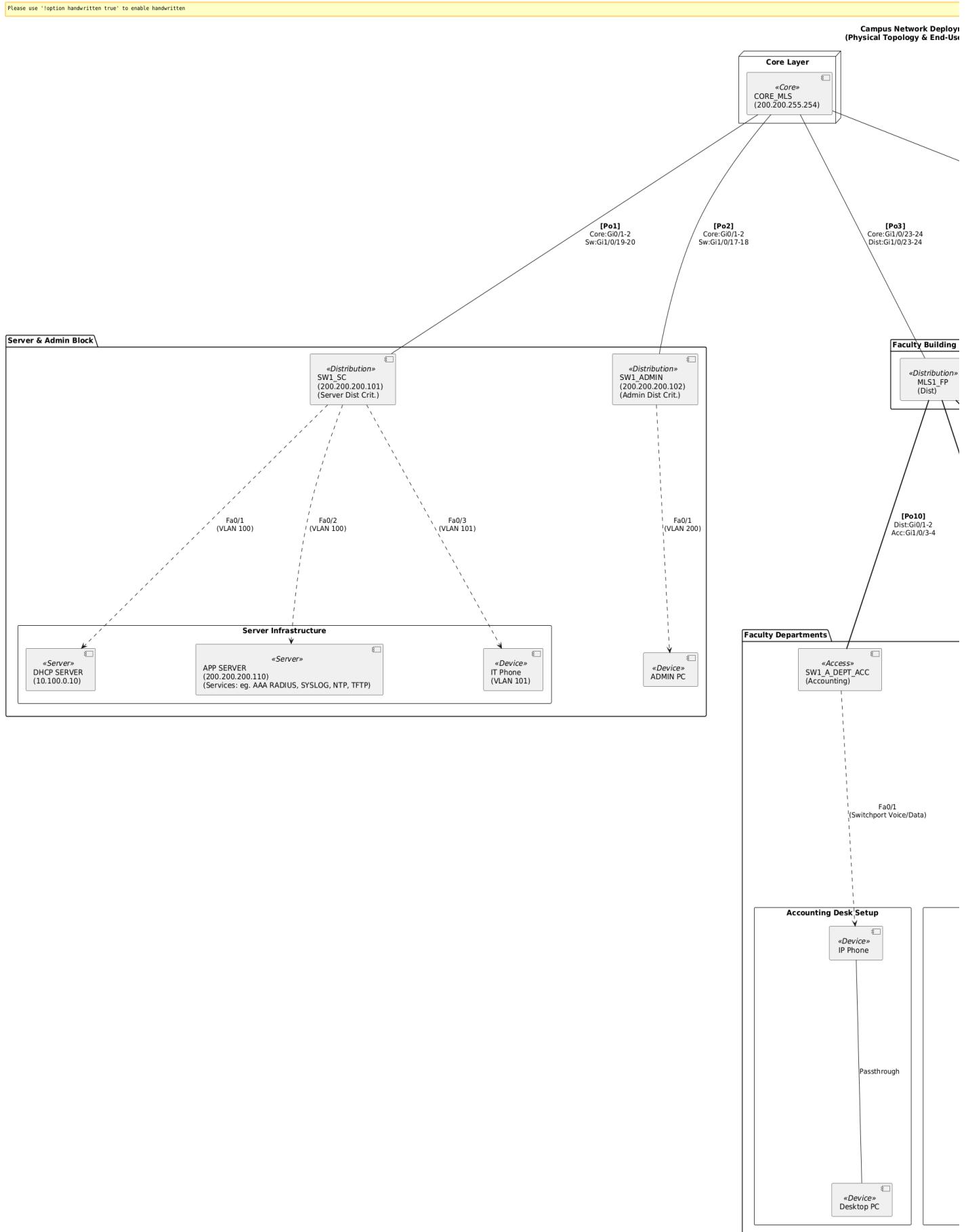
1. Vue Logique Diagram



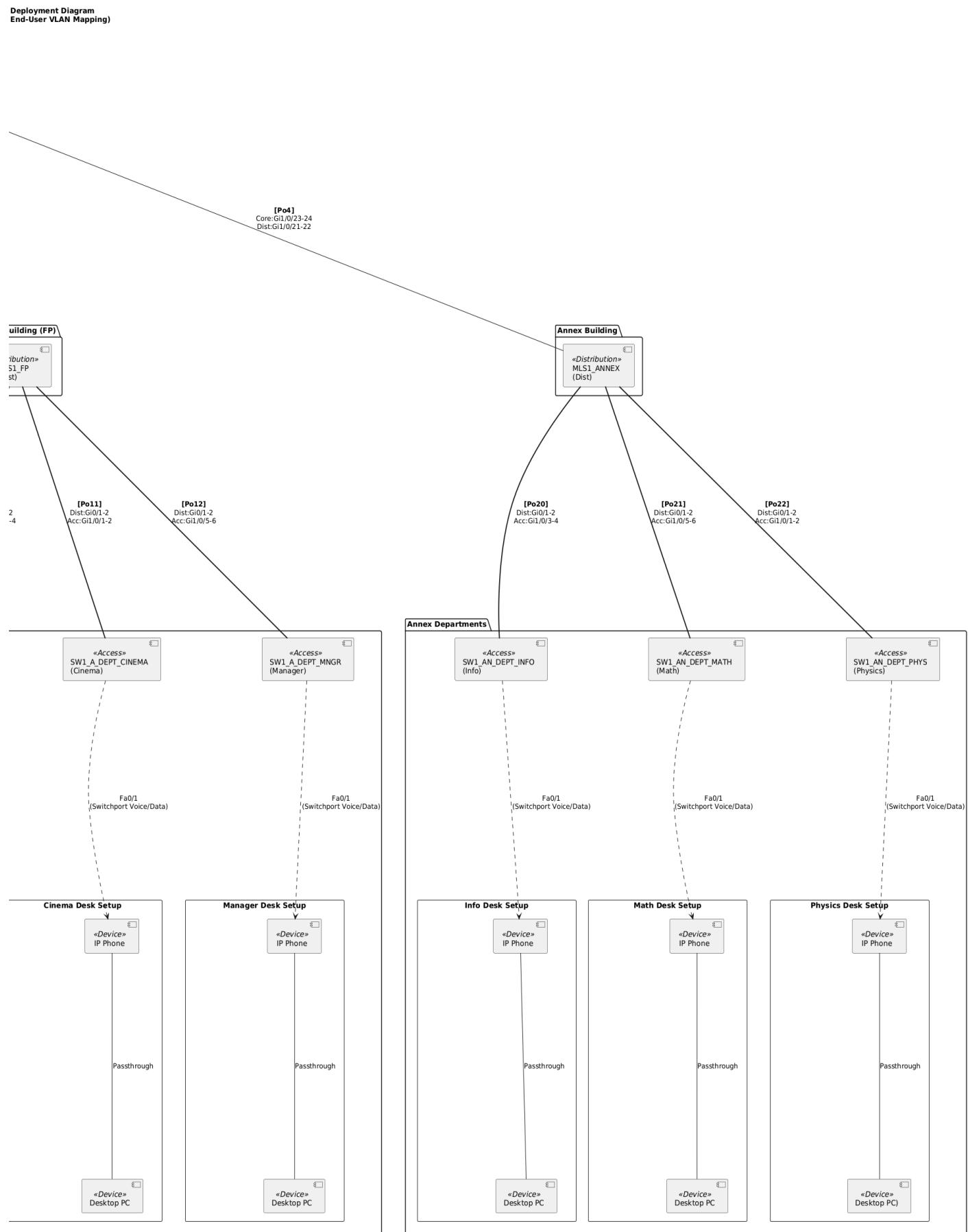
1. Vue Logique Diagram



2. Vue Physique Diagram (Deployment Diagram)



2. Vue Physique Diagram (Deployment Diagram)





3. Architecture Réseau et Plan d'Adressage

3.1 Inventaire des Équipements :

L'infrastructure réseau est construite autour d'une architecture hiérarchique à trois couches (Core, Distribution, Access) pour assurer la redondance, la performance et l'évolutivité.

Appareil (Hostname)	Modèle / Rôle	Localisation	Fonction Principale
CORE MLS	Layer 3 Switch	Salle Serveur	Routage Inter-VLAN, Passerelle Internet
SW1_SC	Layer 2/3 Switch	Salle Serveur	Distribution pour les Serveurs
SW1_ADMIN	Layer 2/3 Switch	Admin Block	Distribution pour l'Administration
MLS1_FP	Layer 3 Switch	Faculté FP	Distribution pour les Départements FP
MLS1_ANEX	Layer 3 Switch	Annexe	Distribution pour les Départements Annexe
SW1_A_DEPT_ACC	Access Switch Layer 2	Faculté FP	Accès pour Comptabilité
SW1_A_DEPT_CINEMA	Access Switch Layer 2	Faculté FP	Accès pour Cinéma
SW1_A_DEPT_MNGR	Access Switch Layer 2	Faculté FP	Accès pour Management
SW1_AN_DEPT_INFO	Access Switch Layer 2	Annexe	Accès pour Informatique
SW1_AN_DEPT_MATH	Access Switch Layer 2	Annexe	Accès pour Mathématiques
SW1_AN_DEPT_PHYS	Access Switch Layer 2	Annexe	Accès pour Physique

3.2 Matrice de Connexions Physiques (Câblage) :

Le tableau ci-dessous détaille les interconnexions physiques critiques et les agrégations de liens (EtherChannel) configurées.

Origine	Interface Origine	Destination	Interface Destination	Type de Lien	Protocole
CORE MLS	Gi1/0/19 - 20	SW1_SC	Gi0/1 - Gi0/2	EtherChannel (Po1)	LACP
	Gi1/0/17 - 18	SW1_ADMIN	Gi0/3 - Gi0/4	EtherChannel (Po2)	
	Gi1/0/23 - 24	MLS1_FP	Gi1/0/23 - 24	EtherChannel (Po3)	
	Gi1/0/21 - 22	MLS1_ANEX	Gi1/0/23 - 24	EtherChannel (Po4)	
MLS1_FP	Gi1/0/3 - 4	SW_ACC	Gi0/1 - Gi0/2	EtherChannel (Po10)	LACP
	Gi1/0/1 - 2	SW_CINEMA	Gi0/1 - Gi0/2	EtherChannel (Po11)	
	Gi1/0/5 - 6	SW_MNGR	Gi0/1 - Gi0/2	EtherChannel (Po12)	
MLS1_ANEX	Gi1/0/3 - 4	SW_INFO	Gi0/1 - Gi0/2	EtherChannel (Po20)	LACP
	Gi1/0/1 - 2	SW_MATH	Gi0/1 - Gi0/2	EtherChannel (Po21)	
	Gi1/0/5 - 6	SW_PHYS	Gi0/1 - Gi0/2	EtherChannel (Po22)	

3.3 Plan d'Adressage IP et VLANs (Subnetting) :

Le réseau utilise un adressage privé de classe C (**200.200.X.X**) segmenté par fonction et sécurité.



ID VLAN	Nom du VLAN	Sous-réseau	Masque	Passerelle (SVI Core)	Usage / Description
100	DHCP_SERVER	10.100.0.0	/24	200.200.255.254	Serveur Critiques(DHCP)
101	DHCP_VOICE	10.101.0.0			Voix sur IP (ToIP) DHCP
110	ETD_DATA	10.110.0.0			Data : Étudiants & Info
111	ETD_VOICE	10.111.0.0			Voix sur IP (ToIP) Étudiants
120	PROF_DATA	10.120.0.0			Data : Professeurs
121	PROF_VOICE	10.121.0.0			Voix sur IP (ToIP) Professeurs
130	ADMIN_DATA	10.130.0.0			Data : Administration & Managers
131	ADMIN_VOICE	10.131.0.0			Voix sur IP (ToIP) Administration & Managers
140	HOST_DATA	10.140.0.0			Data : Invités
141	HOST_VOICE	10.141.0.0			Voix sur IP (ToIP) Invités
190	WLAN_DATA	10.190.0.0			Data : WLAN
191	WLAN_VOICE	10.191.0.0			Voix sur IP (ToIP) WLAN
200	MNGR_DATA	200.200.0.0			Gestion des Équipements
201	MNGR_VOICE	200.201.0.0			Voix sur IP (ToIP) MNGR
999	BLACKHOLE	N/A	N/A	N/A	Sécurité (Ports non utilisés)

3.4 Services Critiques et Adressage Statique :

Les services d'infrastructure clés possèdent des adresses statiques pour garantir leur disponibilité

- Serveur DHCP/** : 10.100.0.10
- Serveur RADIUS (AAA) / TFTP / SYSLOG / NTP** : 200.200.200.110
- Routeur ToIP (CME)** : [À configurer - Placeholder]
- Passerelle Internet (ISP)** : [À configurer - Placeholder]

4. Topologie Réseau : Vue Physique vs. Vue Logique

La conception de cette infrastructure repose sur une distinction claire entre la connectivité physique (le câblage) et la segmentation logique (les flux de données), garantissant une sécurité et une performance optimales.

4.1 Topologie Physique (L'Infrastructure Matérielle)



La topologie physique décrit l'agencement réel des câbles, des équipements et des emplacements géographiques. Notre réseau suit une architecture en étoile étendue (Extended Star), organisée hiérarchiquement.

- **Organisation Géographique :**

- Le Cœur de Réseau (Core) est centralisé dans la salle serveur principale.
- Les commutateurs de Distribution agissent comme des points de concentration pour chaque bâtiment ou zone fonctionnelle (Bloc Admin, Salle Serveur, Bâtiment FP, Annexe).
- Les commutateurs d'Accès sont déployés dans les armoires de brassage locales, au plus près des utilisateurs finaux.

- **Redondance Physique :**

- Chaque liaison entre les couches Core et Distribution est doublée physiquement
- L'utilisation de l'agrégation de liens (EtherChannel/LACP) transforme ces doubles câbles en un seul "tuyau" logique, augmentant la bande passante et assurant qu'une rupture de câble ne coupe pas le service.

4.2 Topologie Logique (La Gestion des Flux) :

Bien que physiquement tous les équipements soient interconnectés, la topologie logique segmente le trafic pour isoler les services et sécuriser les données.

- **Segmentation par VLANs (Virtual LANs) :**

- Au lieu d'un seul grand réseau plat, nous avons découpé le réseau en plusieurs sous-réseaux virtuels (VLAN 100, 110, 120, etc.).
- Séparation Data/Voix : Sur chaque port d'accès utilisateur, deux réseaux logiques coexistent sur le même câble physique : un VLAN pour le PC (Untagged) et un VLAN prioritaire pour le Téléphone IP (Tagged).

- **Routage Centralisé (Inter-VLAN) :**

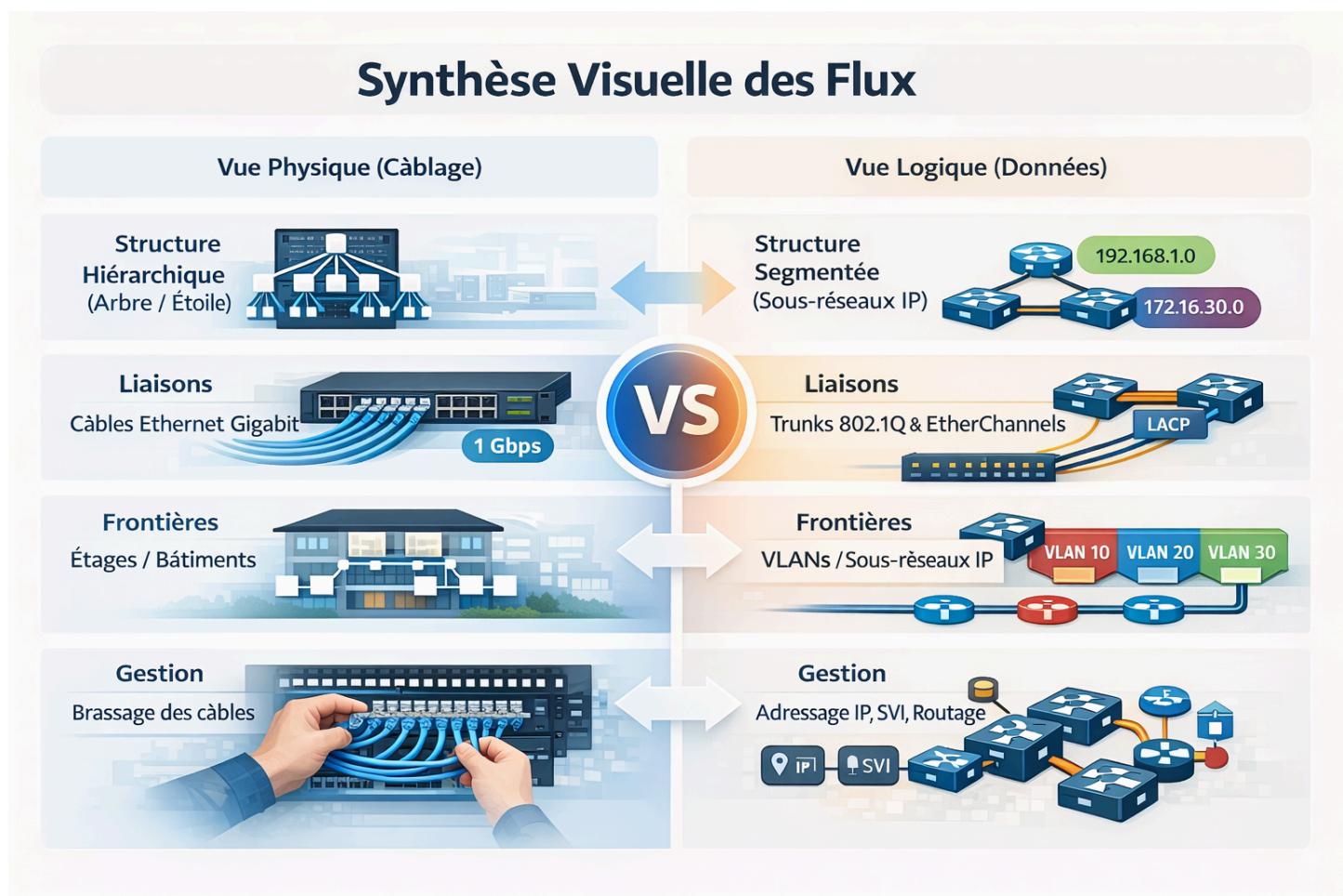
- Le commutateur CORE MLS agit comme le point de routage central (Layer 3)
- Un utilisateur du VLAN 110 (Étudiants) ne peut pas parler

directement à un utilisateur du VLAN 130 (Admin) sans passer par le Core, où nous pouvons appliquer des règles de filtrage.

- **Sécurité et Contrôle d'Accès :**

- Les ACLs (Access Control Lists) sont appliquées aux frontières logiques (interfaces SVI) pour restreindre les communications (ex: empêcher les étudiants d'accéder au VLAN Admin).
- Le DHCP Snooping crée une barrière logique qui empêche les serveurs DHCP pirates de distribuer des adresses, même s'ils sont physiquement connectés au réseau.

4.2 Synthèse Visuelle des Flux :



III. Conception architecturale

1. Présentation du Modèle Hiérarchique

L'architecture de ce réseau repose sur le modèle hiérarchique Cisco à trois couches (Core, Distribution, Access), une méthodologie éprouvée pour concevoir des réseaux d'entreprise évolutifs, résilients et faciles à gérer. Ce modèle découpe le réseau en zones fonctionnelles distinctes, chacune ayant un rôle précis dans le transport et le traitement des données.



L'adoption de cette architecture permet de :

- **Optimiser les performances** en réduisant les domaines de collision et de diffusion (Broadcast Domains).
- **Faciliter le dépannage** en isolant les pannes à une couche spécifique.
- **Améliorer la sécurité** en appliquant des politiques de contrôle d'accès (ACLs, DHCP Snooping, Port Security) à des points stratégiques.
- **Assurer la scalabilité** : l'ajout de nouveaux utilisateurs ou bâtiments se fait simplement en déployant des switchs d'accès supplémentaires sans toucher au cœur du réseau.

2. Couche Cœur (Core Layer)

2.1 Fonction et Responsabilités :

La couche cœur constitue l'épine dorsale du réseau. Son rôle principal est de transporter le trafic entre les différentes couches de distribution à très haute vitesse, sans le ralentir par des traitements complexes (pas de filtrage, pas d'inspection profonde).

Dans notre infrastructure, cette couche est incarnée par le commutateur multicouche CORE MLS (Layer 3 Switch), qui assure :

- **Le routage inter-VLAN** (Router-on-a-Stick virtuel) pour permettre la communication entre les départements.
- **La redondance des chemins** via l'agrégation de liens (EtherChannel LACP) vers les quatre switchs de distribution.
- **La passerelle par défaut** pour tous les VLANs (interfaces SVI : VLAN 100, 110, 120, etc.).

2.2 Justification des Choix de Conception :

- **switch Layer 3 plutôt que routeur** : Le choix d'un commutateur multicouche (au lieu d'un routeur traditionnel avec des sous-interfaces) améliore considérablement les performances du routage inter-VLAN. Les switchs Layer 3 effectuent le routage directement dans le matériel (ASIC), tandis qu'un routeur utilise le CPU.
- **Pas de règles complexes au Core** : Conformément aux meilleures pratiques Cisco, le cœur est maintenu "simple et rapide". Les ACLs et les politiques de sécurité sont appliquées à la couche Distribution pour éviter de surcharger le backbone.
- **Redondance physique** : Toutes les liaisons vers la Distribution sont doublées (EtherChannel), garantissant qu'aucune coupure de câble ne peut isoler un bâtiment.



3. Couche Distribution (Distribution Layer)

3.1 Fonction et Responsabilités

La couche distribution agit comme un point d'agrégation et de contrôle entre le cœur et les utilisateurs. Elle regroupe le trafic provenant de plusieurs switchs d'accès et applique des politiques de routage et de sécurité avant de l'envoyer au cœur.

Dans notre architecture, cette couche est composée de quatre commutateurs de distribution :

- **SW1_SC** : Distribution pour la salle serveur (VLAN 100).
- **SW1_ADMIN** : Distribution pour le bloc administratif (VLAN 200).
- **MLS1_FP** : Distribution pour le bâtiment Faculté (VLANs 110, 120, 130).
- **MLS1_ANNEX** : Distribution pour l'annexe (VLANs 140, 150, etc.).

Chaque switch de distribution :

- **Agrège plusieurs switchs d'accès via des EtherChannels pour augmenter la bande passante.**
- **Applique les règles de sécurité avancées** : ACLs pour le filtrage inter-VLAN, DHCP Snooping pour bloquer les serveurs pirates.
- **Maintient les tables de routage locales** pour optimiser le traitement des requêtes ARP et ICMP.

3.2 Justification des Choix de Conception

- **Séparation géographique et fonctionnelle** : Chaque bâtiment ou bloc fonctionnel (Serveurs, Admin, Faculté) possède son propre switch de distribution. Cela limite l'impact d'une panne locale et permet une gestion indépendante des politiques de sécurité.
- **Application des ACLs à la Distribution** : Plutôt que de configurer des filtres sur chaque switch d'accès (ce qui serait redondant et difficile à maintenir), nous centralisons les ACLs sur les interfaces SVI des switchs de distribution. Cela simplifie la gestion et réduit la charge CPU des switchs d'accès.
- **DHCP Snooping et AAA** : Ces services de sécurité sont activés sur la distribution pour protéger l'ensemble des utilisateurs en aval, tout en laissant passer les requêtes légitimes provenant du serveur central.

4. Couche Accès (Access Layer)



4.1 Fonction et Responsabilités

La couche accès est le point d'entrée des utilisateurs finaux (postes de travail, téléphones IP, imprimantes). Son rôle est de fournir une connectivité simple, sécurisée et segmentée.

Dans notre infrastructure, cette couche comprend six switchs d'accès (Cisco 2960) déployés dans les départements (Comptabilité, Cinéma, Informatique, Math, Physique, etc.).

Chaque switch d'accès :

- **Segmente le trafic** en assignant chaque port à un VLAN spécifique (VLAN Data pour le PC, VLAN Voice pour le téléphone).
- **Sécurise physiquement** le réseau via le **Port Security** (maximum 2 MAC par port : 1 PC + 1 Téléphone).
- **Priorise le trafic voix** en configurant les ports en mode switchport voice vlan X pour garantir la qualité des appels (QoS implicite).

4.2 Justification des Choix de Conception

- **Un VLAN = Une fonction** : Chaque département ou type d'utilisateur (Étudiants, Profs, Admin) possède son propre VLAN Data et VLAN Voix. Cela empêche le trafic de "déborder" d'un service à l'autre et facilite l'application des règles de pare-feu.
- **Port Security Strict** : En limitant chaque port à deux adresses MAC maximum (Sticky Learning + Violation Restrict), nous bloquons automatiquement les tentatives de connexion de périphériques non autorisés (ex: Switch personnel, Hub).
- **Ports inutilisés sécurisés** : Tous les ports non connectés sont administrativement fermés (shutdown) et assignés au VLAN 999 (Blackhole), empêchant toute intrusion physique opportuniste.
- **EtherChannel vers la Distribution** : Chaque switch d'accès est relié à son switch de distribution par au moins deux câbles agrégés (LACP). Si un câble est accidentellement débranché, la connectivité reste intacte.

5. Synthèse des Décisions de Conception



Couche	Équipement	Rôle Principal	Technologies Clés
Core	CORE MLS (L3)	Backbone haute vitesse	Routage Inter-VLAN, EtherChannel LACP
Distribution	SW1_SC, SW1_ADMIN, MLS1_FP, MLS1_ANNE	Agrégation & Sécurité	ACLs, DHCP Snooping, AAA
Access	SW_ACC, SW_CINEMA, SW_INFO, etc.	Connectivité utilisateurs	VLANs, Port Security, Voice VLAN

Cette architecture modulaire garantit que le réseau peut :

- **Absorber la croissance** (ajout de nouveaux switchs d'accès sans reconfigurer le Core).
- **Isoler les pannes** (une défaillance d'un switch d'accès n'affecte qu'un département).
- **Appliquer la sécurité en profondeur** (Défense multi-couches : Port Security → DHCP Snooping → ACLs → AAA).

IV. Détails de configuration

1. Introduction et Méthodologie de Déploiement

Ce chapitre constitue le cœur technique du rapport. Il détaille l'implémentation pratique de l'architecture réseau conçue au chapitre précédent. Contrairement à une approche monolithique, le déploiement de cette infrastructure a suivi une méthodologie incrémentale par étapes (Snapshots).

Cette approche progressive a permis de valider chaque couche fonctionnelle avant de passer à la suivante, garantissant ainsi la stabilité du réseau et facilitant le dépannage. Chaque "Snapshot" correspond à une étape critique du cycle de vie du déploiement :

Roadmap du Déploiement (Snapshots)



Les sections suivantes présentent les configurations types appliquées (Templates) pour chaque domaine fonctionnel, accompagnées des commandes de vérification qui attestent du bon fonctionnement de l'infrastructure.

1. Snapshot 1 : Configuration Initiale et Sécurisation

2.1 Configuration Standardisée des Équipements

Objectif : Établir une base de configuration commune pour tous les commutateurs afin de garantir l'identité du matériel, désactiver les services non sécurisés et chiffrer les accès administratifs via SSH (Secure Shell) au lieu de Telnet.

- Équipements Concernés :** Totalité des commutateurs (CORE MLS, SW1_SC, SW1_ADMIN, MLS1_FP, MLS1_ANNEX, et tous les switchs d'accès).

Script de Configuration Type :



```
1 enable
2 configure terminal
3
4 ! — 1. Identification de l'équipement —
5 hostname [NOM_DU_SWITCH]
6
7 ! — 2. Bannière de Sécurité (Message of the Day) —
8 banner motd #
9
10 ACCES SECURISE - RESEAU CAMPUS [NOM_DU_SWITCH]
11 Toute tentative d'intrusion sera journalisée.
12 # —
13
14 ! — 3. Services Système de Base —
15 ! Désactive la résolution DNS pour éviter les latences en cas de faute de frappe
16 no ip domain-lookup
17 ! Chiffre les mots de passe stockés en clair (Type 7)
18 service password-encryption
19
20 ! — 4. Sécurisation du Mode Privilégié —
21 enable secret [MOT_DE_PASSE_ENABLE]
22
23 ! — 5. Désactivation des Services Web (Vulnérables) —
24 no ip http server
25 no ip http secure-server
26
27 ! — 6. Préparation SSH (Cryptographie) —
28 ! Nécessaire pour générer les clés RSA
29 ip domain-name IT.AC.MA
30 ! Génération des clés (1024 bits minimum recommandé)
31 crypto key generate rsa general-keys modulus 1024
32 ! Force l'utilisation de SSH v2 (plus sécurisé)
33 ip ssh version 2
34 ip ssh time-out 120
35 ip ssh authentication-retries 3
36
37 ! — 7. Gestion des Utilisateurs et Authentification —
38 ! Création de l'administrateur local
39 username [ADMIN_USER] privilege 15 secret [MOT_DE_PASSE_ADMIN]
40
41 ! Activation du modèle AAA (Authentication, Authorization, Accounting)
42 aaa new-model
43 ! Définit la base locale comme méthode d'authentification par défaut
44 aaa authentication login default local
45
46 ! — 8. Sécurisation de la Ligne Console (Accès Physique) —
47 line console 0
48 logging synchronous
49 ! Utilise la méthode AAA définie plus haut (login local)
50 login authentication default
51 exec-timeout 15 0
52 exit
53
54 ! — 9. Sécurisation des Lignes VTY (Accès Distant) —
55 line vty 0 15
56 logging synchronous
57 ! Interdit Telnet, autorise uniquement SSH
58 transport input ssh
59 transport output ssh
60 login authentication default
61 exec-timeout 15 0
62 exit
63
64 ! — 10. Sauvegarde —
65 do write memory
```

2.2 Vérification de la Configuration de Base

Pour valider que le durcissement a été correctement appliqué, les commandes suivantes sont utilisées :



Commande	Résultat Attendu
show version	Vérifier que le registre de configuration est correct et que l'image IOS supporte la crypto (k9).
show ip ssh	Doit afficher "SSH Enabled – version 2.0".
show run include	affichage de partie de configuration a
show run section	partie des mot cle (services, line, vty, ...).

3.1 Création des VLANs et Propagation (VTP)

Objectif : Définir l'ensemble des réseaux virtuels (VLANs) nécessaires à la segmentation du campus et utiliser le protocole VTP (VLAN Trunking Protocol) pour propager automatiquement cette base de données du Core vers les commutateurs de Distribution et d'Accès.

Équipements Concernés :

- CORE MLS (Mode Serveur VTP – Maître)
- Tous les autres switches (Mode Client VTP)

A. Configuration du Serveur VTP (Sur CORE MLS)

```
1 configure terminal
2
3 ! — 1. Activation du Routage IP (Layer 3) —
4 ip routing
5
6 ! — 2. Configuration du Domaine VTP —
7 vtp mode server
8 vtp domain IT.AC.MA
9 vtp password Vtp@2025
10 vtp version 2
11
12 ! — 3. Crédation de la Base de Données VLANs (Layer 2) —
13
14 ! -- VLANs Serveurs --
15 vlan 100
16 name DHCP_SERVER
17 vlan 101
18 name DHCP_VOICE
19
20 ! -- VLANs Utilisateurs (DATA) --
21 vlan 110
22 name ETD_DATA
23 vlan 120
24 name PROF_DATA
25 vlan 130
26 name ADMIN_DATA
27 vlan 140
28 name HOST_DATA
29 vlan 190
30 name WIRELESS_DATA
31
```



```
32 ! -- VLANs Téléphonie (VOICE) --
33 vlan 111
34   name ETD_VOICE
35 vlan 121
36   name PROF_VOICE
37 vlan 131
38   name ADMIN_VOICE
39 vlan 141
40   name HOST_VOICE
41 vlan 191
42   name WIRELESS_VOICE
43
44 ! -- VLANs de Gestion --
45 vlan 200
46   name MGMT_DATA
47 vlan 201
48   name MGMT_VOICE
49
50 exit
51 write memory
```

B. Configuration des Clients VTP (Sur Distribution/Access) Ce script est appliqué sur tous les autres switches pour qu'ils récupèrent les VLANs.

```
1 configure terminal
2 vtp mode client
3 vtp domain IT.AC.MA
4 vtp password Vtp@2025
5 exit
```

3.2 Configuration des Interfaces Virtuelles (SVI) - Passerelles

Objectif : Configurer les interfaces logiques (Switch Virtual Interfaces) sur le Core pour permettre le routage entre les VLANs. Chaque SVI agit comme la passerelle par défaut pour les équipements de son sous-réseau.

Équipement : CORE_MLS

```
1 configure terminal
2
3 ! — Interfaces SVI pour les Serveurs —
4 interface vlan 100
5   description GATEWAY_DHCP_SERVER
6   ip address 10.100.0.1 255.255.255.0
7   no shutdown
8 !
9 interface vlan 101
10  description GATEWAY_DHCP_VOICE
11  ip address 10.101.0.1 255.255.255.0
12  no shutdown
13
14 ! — Interfaces SVI pour les Utilisateurs (DATA) —
15 interface vlan 110
16  ip address 10.110.0.1 255.255.255.0
17  no shutdown
18 !
19 interface vlan 120
20  ip address 10.120.0.1 255.255.255.0
21  no shutdown
22 !
```



```
23 interface vlan 130
24 ip address 10.130.0.1 255.255.255.0
25 no shutdown
26 !
27 interface vlan 140
28 ip address 10.140.0.1 255.255.255.0
29 no shutdown
30 !
31 interface vlan 190
32 ip address 10.190.0.1 255.255.255.0
33 no shutdown
34
35 ! — Interfaces SVI pour la Téléphonie (VOICE) —
36 interface vlan 111
37 ip address 10.111.0.1 255.255.255.0
38 no shutdown
39 !
40 interface vlan 121
41 ip address 10.121.0.1 255.255.255.0
42 no shutdown
43 !
44 interface vlan 131
45 ip address 10.131.0.1 255.255.255.0
46 no shutdown
47 !
48 interface vlan 141
49 ip address 10.141.0.1 255.255.255.0
50 no shutdown
51 !
52 interface vlan 191
53 ip address 10.191.0.1 255.255.255.0
54 no shutdown
55
56 ! — Interface SVI de Gestion —
57 interface vlan 200
58 description GATEWAY_MGMT
59 ip address 200.200.255.254 255.255.0.0
60 no shutdown
61
62 exit
63 write memory
```

3.3 Configuration des Trunks (Liaisons Physiques)

Objectif : Configurer les ports physiques connectant le Core aux commutateurs de Distribution en mode Trunk (802.1Q), et restreindre les VLANs autorisés pour optimiser le trafic.

Équipement : CORE MLS

```
1 configure terminal
2
3 ! — Lien vers Distribution Admin (Admin Block) —
4 interface GigabitEthernet 1/0/17
5 description TRUNK_TO_SW1_ADMIN
6 switchport trunk encapsulation dot1q
7 switchport mode trunk
8 ! Sécurité : Autoriser uniquement les VLANs nécessaires
9 switchport trunk allowed vlan 100,101,110,120,130,140,190,200,201
10 no shutdown
11 exit
12
13 ! — Lien vers Distribution Serveur (Server Room) —
14 interface GigabitEthernet 1/0/19
15 description TRUNK_TO_SW1_SC
16 switchport trunk encapsulation dot1q
17 switchport mode trunk
```



```
18 ! Seuls les VLANs Serveurs et Gestion sont nécessaires ici
19 switchport trunk allowed vlan 100,101,200,201
20 no shutdown
21 exit
22
23 ! — Lien vers Distribution Faculté (Site 1) —
24 interface GigabitEthernet 1/0/23
25 description TRUNK_TO_MLS1_FP
26 switchport trunk encapsulation dot1q
27 switchport mode trunk
28 switchport trunk allowed vlan 100,101,110,120,130,140,190,200,201
29 no shutdown
30 exit
31
32 ! — Lien vers Distribution Annexe (Site 2) —
33 interface GigabitEthernet 1/0/21
34 description TRUNK_TO_MLS1_ANNEX
35 switchport trunk encapsulation dot1q
36 switchport mode trunk
37 switchport trunk allowed vlan 100,101,110,120,130,140,190,200,201
38 no shutdown
39 exit
40
41 do write memory
```

3.4 Configuration de la Couche Distribution & Serveurs

Objectif : Raccorder les serveurs critiques au réseau et assurer la distribution du trafic vers les commutateurs d'accès via des liens Trunks.

A. Commutateur Salle Serveur (SW1_SC) Ce switch connecte l'infrastructure critique (DHCP, DNS, etc.).

```
1 configure terminal
2
3 ! — Uplink vers le Core (Trunk) —
4 interface GigabitEthernet 0/2
5 description UPLINK_TO_CORE
6 switchport mode trunk
7 ! Autorise uniquement les VLANs Serveurs (100, 101) et Gestion (200, 201)
8 switchport trunk allowed vlan 100,101,200,201
9 no shutdown
10 exit
11
12 ! — Ports d'Accès Serveurs —
13
14 ! Serveur DHCP/TFTP (VLAN 100)
15 interface FastEthernet 0/2
16 description SRV_DHCP_TFTP
17 switchport mode access
18 switchport access vlan 100
19 spanning-tree portfast
20 no shutdown
21 exit
22
23 ! Téléphone Salle Serveur (VLAN Voix 101)
24 interface FastEthernet 0/3
25 description PHONE_SERVER_ROOM
26 switchport mode access
27 switchport voice vlan 101
28 spanning-tree portfast
29 no shutdown
30 exit
31
```



```
32 ! Serveur de Gestion/Syslog (VLAN 200)
33 interface FastEthernet 0/1
34 description SRV_MGMT_SYSLOG
35 switchport mode access
36 switchport access vlan 200
37 spanning-tree portfast
38 no shutdown
39 exit
40
41 do write memory
```

B. Commutateurs de Distribution (MLS1_FP / MLS1_ANNEX) Ces switches agrègent le trafic des départements.

```
1 configure terminal
2
3 ! — Uplink vers le Core —
4 interface GigabitEthernet 1/0/23
5 description UPLINK_TO_CORE
6 switchport trunk encapsulation dot1q
7 switchport mode trunk
8 ! Autorise tous les VLANs de production
9 switchport trunk allowed vlan 100-201
10 no shutdown
11 exit
12
13 ! — Downlinks vers les Switches d'Accès —
14 ! Configuration de la plage de ports connectée aux switchs 2960
15 interface range GigabitEthernet 1/0/1 - 6
16 description DOWNLINKS_TO_ACCESS
17 switchport trunk encapsulation dot1q
18 switchport mode trunk
19 switchport trunk allowed vlan 100-201
20 no shutdown
21 exit
22
23 do write memory
```

3.5 Configuration de la Couche Accès (Utilisateurs)

Objectif : Connecter les utilisateurs finaux en séparant le trafic PC (Data) du trafic Téléphonique (Voice) sur le même port physique, et sécuriser les ports inutilisés.

A. Configuration des Ports Utilisateurs (SW_ACCESS_[NOM_DE_DEPT])

```
1 configure terminal
2
3 ! — Uplink vers Distribution —
4 interface GigabitEthernet 0/1
5 description UPLINK_TO_DIST
6 switchport mode trunk
7 switchport trunk allowed vlan 100-201
8 no shutdown
9 exit
10
11 ! — Ports Département ADMINISTRATION (1-2) —
12 interface range FastEthernet 0/1 - 2
13 description ADMIN_USERS
14 switchport mode access
15 switchport access vlan 130      ! Data VLAN
16 switchport voice vlan 131      ! Voice VLAN
17 spanning-tree portfast        ! Activation immédiate du port
18 no shutdown
19 exit
20
```



```
21 ! — Ports Département PROFESSEURS (3-5) —
22 interface range FastEthernet 0/3 - 5
23 description PROF_USERS
24 switchport mode access
25 switchport access vlan 120
26 switchport voice vlan 121
27 spanning-tree portfast
28 no shutdown
29 exit
30
31 ! — Ports Département ETUDIANTS (6-10) —
32 interface range FastEthernet 0/6 - 10
33 description ETD_STUDENTS
34 switchport mode access
35 switchport access vlan 110
36 switchport voice vlan 111
37 spanning-tree portfast
38 no shutdown
39 exit
40
41 ! — Ports Département HOSTS/INVITÉS (11-14) —
42 interface range FastEthernet 0/11 - 14
43 description HOST_USERS
44 switchport mode access
45 switchport access vlan 140
46 switchport voice vlan 141
47 spanning-tree portfast
48 no shutdown
49 exit
50
51 ! — Ports Points d'Accès WIFI (15-18) —
52 interface range FastEthernet 0/15 - 18
53 description WIRELESS_AP
54 switchport mode access
55 switchport access vlan 190
56 switchport voice vlan 191
57 spanning-tree portfast
58 no shutdown
59 exit
60
61 do write memory
```

B. Sécurisation des Ports Inutilisés (Best Practice) Tout port non brassé est désactivé et placé dans un "VLAN Blackhole" (999) pour éviter qu'un utilisateur ne s'y connecte par erreur.

```
1 configure terminal
2 interface range FastEthernet 0/19 - 24
3 description UNUSED_PORTS
4 switchport mode access
5 switchport access vlan 999
6 shutdown
7 exit
8 do write memory
```

B. Gestion In-Band (SVI de Management) Permet d'administrer le switch d'accès à distance (SSH) via le VLAN 200.

```
1 configure terminal
2
3 ! Interface de Gestion
4 interface vlan 200
5 ! IP unique par switch
6 ip address 200.200.[ID_UNIQUE_1].[ID_UNIQUE_2] 255.255.0.0
7 no shutdown
8 exit
9
```



```
10 ! Passerelle pour répondre aux pings/SSH d'autres réseaux
11 ip default-gateway 200.200.255.254
12
13 do write memory
```

3.6 Vérification

Commande	Résultat Attendu
show vtp status	Tous les VLANs (100-201) doivent être listés et actifs.
show vlan brief	- Doit afficher "SSH Enabled - version 2.0". - Les ports Fa0/1-2 doivent être dans le VLAN 130, Fa0/6-10 dans le 110, etc.
show ip interface brief	Toutes les interfaces VLAN (SVI) doivent être up/up.
show interfaces trunk	show interfaces trunk, Le port vers le switch supérieur doit être listé en mode on ou auto, encapsulation 802.1q.
show interfaces switchport	Vérifier la ligne Voice VLAN: 131 (ADMIN_VOICE).

3.7 Configuration du Relais DHCP (IP Helper-Address)

Objectif : Puisque le serveur DHCP (10.100.0.10) est situé dans un VLAN dédié (VLAN 100), les requêtes de diffusion (Broadcast) des clients situés dans d'autres VLANs ne peuvent pas l'atteindre naturellement. La commande ip helper-address configure le Core Switch pour intercepter ces requêtes et les relayer en Unicast vers le serveur.

Équipement : CORE MLS

```
1 configure terminal
2
3 ! — Relais DHCP pour les VLANs DATA —
4 interface vlan 110
5 description ETD_DATA
6 ip helper-address 10.100.0.10
7 exit
8 interface vlan 120
9 description PROF_DATA
10 ip helper-address 10.100.0.10
11 exit
12 interface vlan 130
13 description ADMIN_DATA
14 ip helper-address 10.100.0.10
15 exit
16 interface vlan 140
17 description HOST_DATA
18 ip helper-address 10.100.0.10
19 exit
20 interface vlan 190
21 description WIRELESS_DATA
22 ip helper-address 10.100.0.10
23 exit
```



```
24
25 ! — Relais DHCP pour les VLANs VOICE —
26 ! Nécessaire pour que les téléphones IP obtiennent leur IP et l'Option 150
27 interface vlan 111
28 description ETD_VOICE
29 ip helper-address 10.100.0.10
30 exit
31 interface vlan 121
32 description PROF_VOICE
33 ip helper-address 10.100.0.10
34 exit
35 interface vlan 131
36 description ADMIN_VOICE
37 ip helper-address 10.100.0.10
38 exit
39 interface vlan 141
40 description HOST_VOICE
41 ip helper-address 10.100.0.10
42 exit
43 interface vlan 191
44 description WIRELESS_VOICE
45 ip helper-address 10.100.0.10
46 exit
47 interface vlan 201
48 description MGMT_VOICE
49 ip helper-address 10.100.0.10
50 exit
51
52 write memory
```

Configuration du Serveur DHCP (Packet Tracer) : Les pools DHCP suivants ont été configurés sur le serveur 10.100.0.10 pour correspondre à chaque VLAN.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
ETD_VOICE	10.111.0.1	0.0.0.0	10.111.0.50	255.255.255.0	200	0.0.0.0	0.0.0.0
PROF_VOICE	10.121.0.1	0.0.0.0	10.121.0.50	255.255.255.0	200	0.0.0.0	0.0.0.0
ADMIN_VOICE	10.131.0.1	0.0.0.0	10.131.0.50	255.255.255.0	200	0.0.0.0	0.0.0.0
HOST_VOICE	10.141.0.1	0.0.0.0	10.141.0.50	255.255.255.0	200	0.0.0.0	0.0.0.0
WLAN_VOICE	10.191.0.1	0.0.0.0	10.191.0.50	255.255.255.0	200	0.0.0.0	0.0.0.0
WLAN_DATA	10.190.0.1	8.8.8.8	10.190.0.50	255.255.255.0	200	200.200.200.200	0.0.0.0
HOST_DATA	10.140.0.1	8.8.8.8	10.140.0.50	255.255.255.0	200	200.200.200.200	0.0.0.0
ADMIN_DATA	10.130.0.1	8.8.8.8	10.130.0.50	255.255.255.0	200	200.200.200.200	0.0.0.0
PROF_DATA	10.120.0.1	8.8.8.8	10.120.0.50	255.255.255.0	200	200.200.200.200	0.0.0.0
ETD_DATA	10.110.0.1	8.8.8.8	10.110.0.50	255.255.255.0	200	200.200.200.200	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	10.100.0.0	255.255.255.0	512	0.0.0.0	0.0.0.0



3.8 Configuration de l'Accès de Gestion (Management SVI)

Objectif : Attribuer une adresse IP unique à chaque commutateur (Distribution et Accès) dans le VLAN de gestion (VLAN 200) afin de permettre l'administration à distance via SSH.

Équipements Concernés : Tous les switches (sauf le Core qui a déjà son SVI).

Script de Configuration (Template Générique) :

```
1 configure terminal
2
3 ! — Interface de Gestion (VLAN 200) —
4 interface vlan 200
5 description MANAGEMENT_INTERFACE
6 ! [X] et [Y] doit être remplacé par l'adresse assignée dans le plan d'adressage
7 ! Exemple pour SW1_A_DEPT_CINEMA : 200.200.10.31
8 ip address 200.200.[X].[Y] 255.255.0.0
9 no shutdown
10 exit
11
12 ! — Passerelle par Défaut —
13 ! Essentiel pour répondre aux requêtes SSH venant d'autres sous-réseaux
14 ip default-gateway 200.200.255.254
15
16 write memory
```

Plan d'Adressage de Gestion (Rappel) :

- **CORE_MLS (Passerelle):** 200.200.255.254
- **SW1_SC :** 200.200.200.101
- **SW1_ADMIN :** 200.200.200.102
- **MLS1_FP :** 200.200.100.101
- **Switches Accès FP :** 200.200.X.Y
- **MLS1_ANNEX :** 200.200.100.102
- **Switches Accès Annex :** 200.200.X.Y

3.7 Vérification Finale du Snapshot 1 :

À ce stade, la connectivité de base est établie. Les tests suivants valident le succès de cette étape :

- **Test DHCP :** Un PC connecté dans le VLAN 110 doit recevoir une IP du type 10.110.0.X.
- **Test Ping SVI :** Le Core Switch doit pouvoir pinger l'IP de gestion de tous les switches de distribution.
- **Test SSH :** L'administrateur doit pouvoir se connecter en SSH sur 200.200.10.31 (Admin Switch) depuis le VLAN de gestion.



2. Snapshot 2 : Services d'Infrastructure et Authentification Centralisée

4.1 Journalisation et Synchronisation Temporelle (Syslog & NTP)

Objectif : Garantir que tous les équipements partagent une horloge commune (NTP) et envoient leurs journaux d'événements vers un serveur central (Syslog) pour faciliter l'audit et le dépannage.

Équipements Concernés :

- Tous les commutateurs (Core, Distribution, Access)
- Adresse du Serveur de Services : 200.200.200.110 (VLAN Server)

Script de Configuration (Appliqué globalement) :

```
1 configure terminal
2
3 ! — 1. Configuration NTP (Time Synchronization) —
4 ! Pointage vers le serveur NTP maître
5 ntp server 200.200.200.110
6 ! Activation de l'authentification MD5 pour éviter les serveurs NTP pirates
7 ntp authenticate
8 ntp trusted-key 1
9 ntp authentication-key 1 md5 ntp@2025
10
11 ! — 2. Configuration Syslog (Centralized Logging) —
12 ! Activation du service
13 logging on
14 ! Adresse du serveur de logs
15 logging host 200.200.200.110
16 ! Niveau de détail (Debugging pour le lab, Informational pour la prod)
17 logging trap debugging
18 ! Horodatage précis des logs (indispensable pour corréler avec NTP)
19 service timestamps log datetime msec
20
21 exit
22 write memory
```

Vérification :

Commande	Résultat Attendu
show ntp status	L'état doit être Synchronized, Stratum supérieur à 1.
show logging	Doit afficher "Logging to host 200.200.200.110".

4.2 Authentification Centralisée (AAA - RADIUS)

Objectif : Sécuriser l'accès administratif (Console et SSH) en déléguant l'authentification à un serveur RADIUS. Si le serveur est injoignable, l'authentification bascule sur une base locale de secours.

Équipements Concernés :

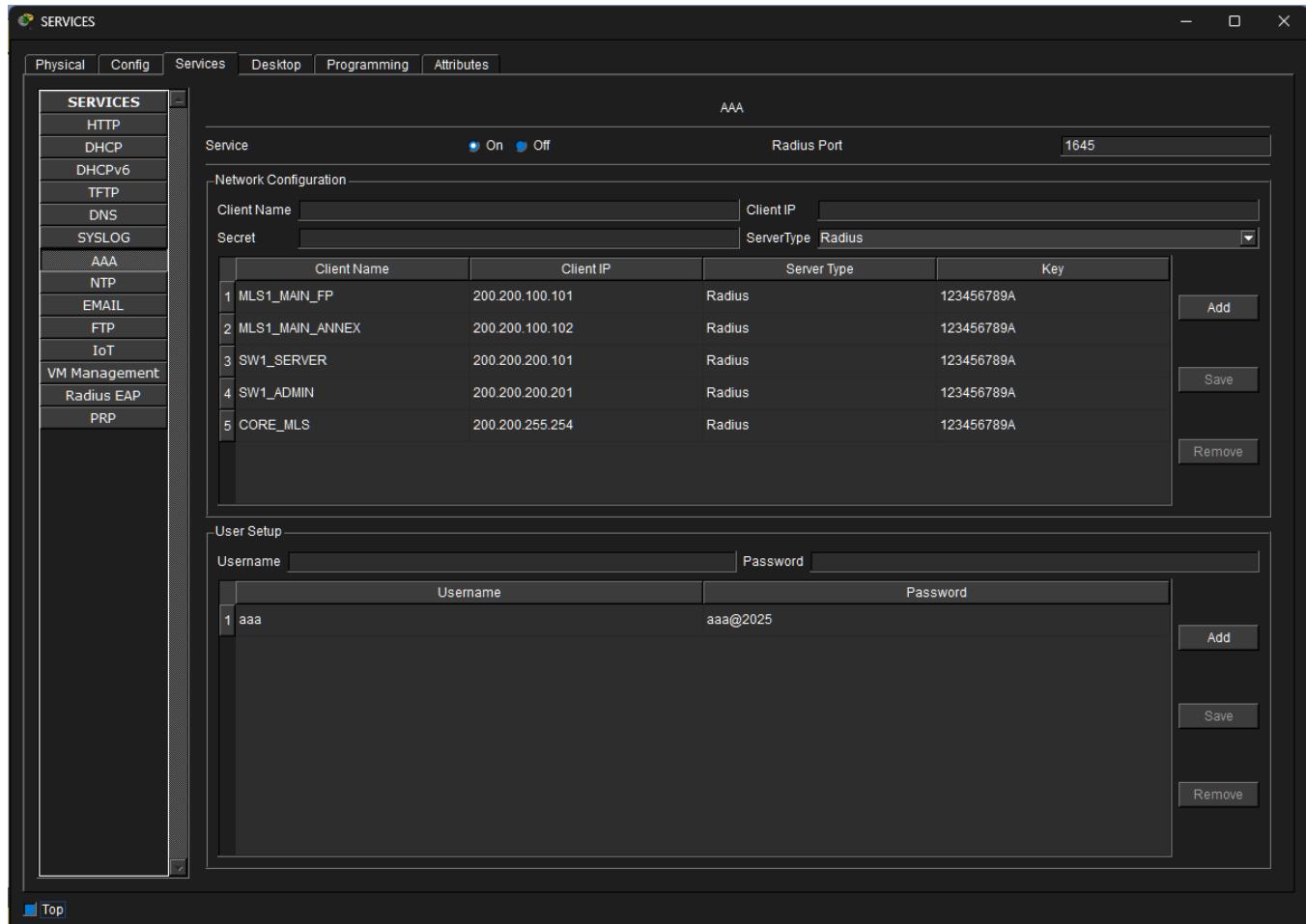


- **Core Layer :** CORE_MLS
- **Distribution Layer :** SW1_SC, SW1_ADMIN, MLS1_FP, MLS1_ANNEX
- **Note :** Les commutateurs d'accès (Layer 2) conservent une authentification locale simple en raison des limitations logicielles.

Script de Configuration (Core & Distribution) :

```
1 configure terminal
2
3 ! — 1. Création de l'Utilisateur de Secours (CRITIQUE) —
4 ! Si RADIUS échoue (timeout), le switch utilisera ce compte local
5 username AdminLocal privilege 15 secret Mngr@Reseau2025
6
7 ! — 2. Activation du Framework AAA —
8 aaa new-model
9
10 ! — 3. Déclaration du Serveur RADIUS —
11 radius server RADIUS_SERVER
12 address ipv4 200.200.200.110 auth-port 1645
13 key 123456789A
14 exit
15
16 ! — 4. Stratégies d'Authentification —
17 ! "Essayer RADIUS d'abord, si injoignable, utiliser la base LOCALE"
18 aaa authentication login default group radius local
19
20 ! Pour le mode Enable (Privileged EXEC), utiliser le 'enable secret' local
21 ! (Plus stable que l'authentification enable via Radius sur certains IOS)
22 aaa authentication enable default enable
23
24 ! — 5. Application aux Lignes —
25 ! Console
26 line console 0
27 login authentication default
28 exit
29
30 ! SSH / VTY
31 line vty 0 15
32 login authentication default
33 exit
34
35 do write memory
```

Configuration du Serveur AAA RADIUS: Creation des comptes pour les switches compatible :



Vérification :

- Tenter une connexion SSH avec un compte défini sur le serveur RADIUS.
- Couper le lien vers le serveur RADIUS et tenter une connexion avec AdminLocal (Test de la redondance).

4.3 Sauvegarde des Configurations (TFTP)

Objectif : Archiver les configurations courantes (running-config) sur un serveur de fichiers TFTP pour permettre une restauration rapide en cas de panne matérielle.

Procédure Opérationnelle :

1. S'assurer que le service TFTP est ON sur le serveur **200.200.200.110**.
2. Exécuter la commande de sauvegarde sur chaque switch :



```
1 ! Commande à exécuter en mode Privilégié (#)
2 copy running-config tftp:
3
4 ! Répondre aux invites :
5 ! Address or name of remote host []? 200.200.200.110
6 ! Destination filename [SwitchName-config]? [Entrer un nom explicite]
```

3. Snapshot 3 : Agrégation de Liens et Sécurisation de la Bordure

5.1 Agrégation de Liens (EtherChannel LACP)

Objectif : Augmenter la bande passante disponible entre les commutateurs et assurer la redondance. Si un câble physique échoue, le trafic bascule instantanément sur l'autre lien du groupe sans interruption de service.

Protocole utilisé : LACP (IEEE 802.3ad) en mode **active**.

A. Configuration Côté Core (Vers Distribution)

- Équipement : CORE MLS

```
1 configure terminal
2
3 ! — Groupe 1 : Vers Serveurs (SW1_SC) —
4 interface range GigabitEthernet 1/0/19 - 20
5 switchport trunk encapsulation dot1q
6 switchport mode trunk
7 channel-group 1 mode active
8 exit
9 interface port-channel 1
10 switchport trunk encapsulation dot1q
11 switchport mode trunk
12 exit
13
14 ! — Groupe 2 : Vers Admin (SW1_ADMIN) —
15 interface range GigabitEthernet 1/0/17 - 18
16 switchport trunk encapsulation dot1q
17 switchport mode trunk
18 channel-group 2 mode active
19 exit
20 interface port-channel 2
21 switchport trunk encapsulation dot1q
22 switchport mode trunk
23 exit
24
25 ! — Groupe 3 : Vers Faculté (MLS1_FP) —
26 interface range GigabitEthernet 1/0/23 - 24
27 switchport trunk encapsulation dot1q
28 switchport mode trunk
29 channel-group 3 mode active
30 exit
31 interface port-channel 3
32 switchport trunk encapsulation dot1q
33 switchport mode trunk
34 exit
```



```
35
36 ! — Groupe 4 : Vers Annexe (MLS1_ANNEX) —
37 interface range GigabitEthernet 1/0/21 - 22
38 switchport trunk encapsulation dot1q
39 switchport mode trunk
40 channel-group 4 mode active
41 exit
42 interface port-channel 4
43 switchport trunk encapsulation dot1q
44 switchport mode trunk
45 exit
46
47 do write memory
```

B. Configuration Côté Distribution (Vers Accès)

- Équipement : MLS1_FP, MLS1_ANNEX

```
1 configure terminal
2
3 ! — Uplink vers Core (Groupe 3) —
4 interface range GigabitEthernet 1/0/23 - 24
5 switchport trunk encapsulation dot1q
6 switchport mode trunk
7 channel-group 3 mode active
8 exit
9
10 ! — Downlinks vers Accès —
11 ! Vers Access Compta (Groupe 22)
12 interface range GigabitEthernet 1/0/3 - 4
13 switchport trunk encapsulation dot1q
14 switchport mode trunk
15 channel-group 22 mode active
16 exit
17 ! Vers Access Cinéma (Groupe 23)
18 interface range GigabitEthernet 1/0/1 - 2
19 switchport trunk encapsulation dot1q
20 switchport mode trunk
21 channel-group 23 mode active
22 exit
23 ! Vers Access Manager (Groupe 21)
24 interface range GigabitEthernet 1/0/5 - 6
25 switchport trunk encapsulation dot1q
26 switchport mode trunk
27 channel-group 21 mode active
28 exit
29
30 do write memory
```

```
1 configure terminal
2
3 ! — UPLINK vers Core (Groupe 4) —
4 interface range GigabitEthernet 1/0/23 - 24
5 description UPLINK_TO_CORE
6 switchport trunk encapsulation dot1q
7 switchport mode trunk
8 channel-group 4 mode active
9 exit
10
11 ! — DOWNLINKS vers Access Switches —
12
13 ! Vers Accès Math (Groupe 31)
14 interface range GigabitEthernet 1/0/5 - 6
15 switchport trunk encapsulation dot1q
16 switchport mode trunk
17 channel-group 31 mode active
18 exit
```



```
19
20 ! Vers Accès Info (Groupe 32)
21 interface range GigabitEthernet 1/0/3 - 4
22 switchport trunk encapsulation dot1q
23 switchport mode trunk
24 channel-group 32 mode active
25 exit
26
27 ! Vers Accès Physique (Groupe 33)
28 interface range GigabitEthernet 1/0/1 - 2
29 switchport trunk encapsulation dot1q
30 switchport mode trunk
31 channel-group 33 mode active
32 exit
33
34 write memory
```

- Équipement : SW_CS, SW_ADMIN

```
1 ! === SW1_SC (Server Room) ===
2 configure terminal
3 interface range GigabitEthernet 0/1 - 2
4 description UPLINK_TO_CORE
5 switchport trunk encapsulation dot1q
6 switchport mode trunk
7 channel-group 1 mode active
8 exit
9
10 ! === SW1_ADMIN (Admin Block) ===
11 configure terminal
12 interface range GigabitEthernet 0/1 - 2
13 description UPLINK_TO_CORE
14 switchport trunk encapsulation dot1q
15 switchport mode trunk
16 channel-group 2 mode active
17 exit
```

C. Configuration Côté Accès Template appliqué à tous les switches d'accès.

```
1 configure terminal
2 interface range GigabitEthernet 0/1 - 2
3 switchport mode trunk
4 channel-group 1 mode active
5 exit
6 interface port-channel 1
7 switchport mode trunk
8 exit
```

5.2 Sécurité Physique (Port Security)

Objectif : Empêcher la connexion de périphériques non autorisés (Rogue Devices) sur les ports utilisateurs et désactiver les ports non utilisés pour réduire la surface d'attaque.

Équipements Concernés : Tous les commutateurs d'accès.

```
1 configure terminal
2
3 ! — Ports Utilisateurs Actifs (Fa0/1 - Fa0/18) —
4 interface range FastEthernet 0/1 - 18
5 switchport mode access
6 switchport port-security
```



```
7 ! Limite : 1 PC + 1 Téléphone IP = 2 MACs
8 switchport port-security maximum 2
9 ! Apprentissage dynamique et persistant des adresses MAC
10 switchport port-security mac-address sticky
11 ! Action en cas de violation : Bloquer le paquet et alerter (Syslog/SNMP)
12 switchport port-security violation restrict
13 ! Oublier les MACs après 1h d'inactivité (pour rotation des salles)
14 switchport port-security aging time 60
15 exit
16
17 ! — Ports Inutilisés (Fa0/19 – Fa0/24) —
18 interface range FastEthernet 0/19 – 24
19 switchport mode access
20 switchport port-security
21 ! Sécurité maximale : Shutdown immédiat si un câble est branché
22 switchport port-security maximum 1
23 switchport port-security violation shutdown
24 shutdown
25 exit
26
27 do write memory
```

5.3 Sécurité Logique (DHCP Snooping)

Objectif : Bloquer les serveurs DHCP illégitimes (Rogue DHCP) qui pourraient distribuer de fausses adresses IP ou passerelles aux utilisateurs (Man-in-the-Middle).

Architecture de Confiance :

- **Ports de Confiance (Trust)** : Ports reliés au serveur DHCP légitime et Uplinks vers le Core.
- **Ports Non-Fiabiles (Untrusted)** : Tous les ports utilisateurs finaux.

A. Configuration Globale (TOUS les Switches)

```
1 configure terminal
2 ! Activation du service
3 ip dhcp snooping
4 ! Liste des VLANs à protéger
5 ip dhcp snooping vlan 100-201
6 ! Désactivation de l'option 82 (Compatibilité Packet Tracer)
7 no ip dhcp snooping information option
8 exit
```

B. Configuration des Ports de Confiance (Chemin vers le Serveur)

Serveur Switch (SW1_SC) : Port serveur et Uplink.

Core Switch (CORE MLS) : Tous les liens vers la Distribution.

Distribution (MLS1_FP, etc.) : Uplinks vers Core et Downlinks vers Access.

Access Switches : Uniquement l'Uplink (Gi0/1-2).



```
1 ! — Exemple sur Switch d'Accès —  
2 interface range GigabitEthernet 0/1 - 2  
3 description UPLINK_TRUSTED  
4 ip dhcp snooping trust  
5 exit  
6  
7 ! — Exemple sur Switch Serveur —  
8 interface FastEthernet 0/2  
9 description DHCP_SERVER_PORT  
10 ip dhcp snooping trust  
11 exit
```

C. Limitation de Débit (Rate Limiting) sur les Ports Utilisateurs Pour empêcher une attaque par déni de service (DoS) via inondation de requêtes DHCP.

```
1 ! — Sur les Switches d'Accès Uniquement —  
2 interface range FastEthernet 0/1 - 18  
3 ip dhcp snooping limit rate 10  
4 exit
```

4. Snapshot 4 : Segmentation Avancée et Sécurité Recursive (ACLs)

Dans cette phase, nous déployons une politique de sécurité à deux niveaux :

- **Isolation des Flux Métier (Data Plane)** : Utilisation d'ACLs étendues sur le Core pour empêcher les départements de communiquer entre eux (ex: Étudiants vers Admin), tout en autorisant l'accès aux serveurs et à Internet.
- **Administration Réursive (Management Plane)** : Mise en place d'un modèle "Jump Host".
 - L'Admin PC (200.200.130.10) est le seul autorisé à se connecter au Core.
 - Le Core (200.200.255.254) est le seul autorisé à se connecter aux Switches de Distribution/Accès.

6.1 Isolation des VLANs (Data Plane Security)

Objectif : Bloquer tout trafic direct entre les VLANs Utilisateurs (110, 120, 130, 140, 190) tout en permettant à chacun d'accéder aux VLANs Serveurs (100) et à Internet (Tout le reste).

Équipement : CORE MLS

```
1 configure terminal  
2  
3 ! — Définition de l'ACL Étendue —  
4 ip access-list extended ISOLATE_CLIENT_VLANS  
5  
6 ! 1. Autoriser le trafic DHCP/DNS/Services vers le VLAN Serveur (100)  
7 permit ip any 10.100.0.0 0.0.0.255
```



```
8
9 ! 2. Autoriser le trafic de Gestion vers le VLAN Mgmt (200) - Admin Only
10 ! (Cette règle sera affinée plus tard, pour l'instant on permet pour tests)
11 permit ip 10.130.0.0 0.0.0.255 200.200.0.0 0.0.255.255
12
13 ! 3. BLOQUER le trafic vers tous les autres réseaux privés locaux (RFC1918)
14 ! Cela empêche 110 de parler à 120, 130, etc.
15 deny ip any 10.0.0.0 0.255.255.255
16
17 ! 4. Autoriser tout le reste (Accès Internet simulé)
18 permit ip any any
19 exit
20
21 ! — Application aux Interfaces SVI Clients —
22 ! On applique en entrée (in) pour filtrer dès l'arrivée du paquet
23 interface vlan 110
24 ip access-group ISOLATE_CLIENT_VLANS in
25 exit
26 interface vlan 120
27 ip access-group ISOLATE_CLIENT_VLANS in
28 exit
29 interface vlan 130
30 ip access-group ISOLATE_CLIENT_VLANS in
31 exit
32 interface vlan 140
33 ip access-group ISOLATE_CLIENT_VLANS in
34 exit
35 interface vlan 190
36 ip access-group ISOLATE_CLIENT_VLANS in
37 exit
38
39 do write memory
```

6.2 Sécurité d'Administration Réursive (Management Plane)

Concept "Jump Host" : Pour administrer un switch d'accès, l'administrateur doit d'abord se connecter au Core (Jump Host), puis rebondir vers la cible.

A. Protection du Core Switch (Niveau 1)

Seul le PC Administrateur (VLAN 130) et le VLAN Gestion (200) peuvent SSH vers le Core.

Équipement : CORE MLS

```
1 configure terminal
2
3 ! — ACL Standard pour le Core —
4 ip access-list standard SECURE_CORE_SSH
5 ! Autoriser le PC Admin spécifique (IP fixe supposée 10.130.0.10)
6 permit 10.130.0.10
7 ! Autoriser le réseau de gestion (au cas où)
8 permit 200.200.0.0 0.0.255.255
9 ! Refuser tout le reste (Implicite, mais on l'écrit pour la clarté)
10 deny any
11 exit
12
13 ! — Application aux Lignes VTY (SSH/Telnet) —
14 line vty 0 15
15 ! Appliquer la restriction
16 access-class SECURE_CORE_SSH in
17 exit
18
19 do write memory
```



B. Protection des Switches Distribution/Accès (Niveau 2)

Ces équipements n'acceptent SSH que si la connexion vient de l'IP du Core Switch (200.200.255.254).

Équipements : Tous les switches sauf le Core (SW1_ADMIN, MLS1_FP, SW_ACC, etc.)

```
1 configure terminal
2
3 ! — ACL Standard pour les Switches en aval —
4 ip access-list standard JUMP_HOST_ONLY
5 ! Autoriser UNIQUEMENT l'IP de Gestion du Core (La source du rebond)
6 permit 200.200.255.254
7 ! Refuser tout le reste (même le PC Admin en direct !)
8 deny any
9 exit
10
11 ! — Application aux Lignes VTY —
12 line vty 0 15
13 access-class JUMP_HOST_ONLY in
14 exit
15
16 do write memory
```

6.4 Vérification Snapshot 4 et 5.4 Vérification Snapshot 3 :

Commande	Objectif / Action	Résultat Attendu
show etherchannel summary	Valider l'agrégation	Ports listés avec le flag (P) dans le Port-channel (SU).
show port-security interface []	Valider la sécurité du port	Port Security : Enabled, Violation Mode : Restrict.
show ip dhcp snooping	Valider le Snooping	Switch DHCP snooping is enabled.
show ip dhcp snooping binding	Voir les clients	Liste des adresses MAC et IP des PC connectés légitimement.
Isolation VLAN	Ping du PC Étudiant (VLAN 110) vers PC Prof (VLAN 120)	Échec (Request Timed Out) - Bloqué par ACL.
Accès Serveur	Ping du PC Étudiant (VLAN 110) vers Serveur (10.100.0.10)	Succès - Autorisé.
SSH Direct (Interdit)	SSH du PC Admin (10.130.0.10) vers Switch Accès (200.200.20.X)	Échec (Connection Refused) - Bloqué par JUMP_HOST_ONLY.
SSH Récursif (Autorisé)	1. SSH du PC Admin vers Core (200.200.255.254) 2. Depuis le Core, SSH vers Switch Accès	Succès - Le Core agit comme relais de confiance.



5. Snapshot 5 : Téléphonie IP et Services Convergents (VoIP)

7.1 Architecture VoIP

Pour gérer la signalisation des appels et la distribution des numéros, nous introduisons un routeur Cisco ISR (Integrated Services Router) connecté au Core Switch.

Rôle du Routeur (CME) : Serveur d'appel (Call Manager Express), Serveur DHCP pour les téléphones (Option 150).

Architecture de VLANs Voix :

- Le routage Inter-VLAN des paquets voix est toujours effectué par le Core Switch.
- Le Routeur CME n'intervient que pour l'enregistrement des téléphones (SCCP/SIP) et l'établissement des appels.

7.2 Configuration de l'Interconnexion Core ↔ Routeur

Objectif : Créer un lien routé (Point-à-Point) entre le Core et le Routeur VoIP pour ne pas étendre les VLANs jusqu'au routeur (design plus propre).

A. Côté Core Switch (CORE MLS)

```
1 configure terminal
2
3 ! — Interface vers le Routeur VoIP —
4 ! On transforme le port switch en port routé (Layer 3)
5 interface GigabitEthernet 1/0/1
6 description UPLINK_TO_CME_ROUTER
7 no switchport
8 ip address 172.16.0.2 255.255.255.252
9 no shutdown
10 exit
11
12 ! — Routage Statique —
13 ! Le Core connaît tous les VLANs internes.
14 ! Il a juste besoin d'une route par défaut vers le Routeur (qui sortira aussi vers Internet)
15 ip route 0.0.0.0 0.0.0.0 172.16.0.1
16
17 do write memory
```

B. Côté Routeur CME (ROUTER_CME)

```
1 enable
2 configure terminal
3 hostname ROUTER_CME
4
5 ! — Interface vers le Core —
6 interface GigabitEthernet 0/0
7 description LINK_TO_CORE
8 ip address 172.16.0.1 255.255.255.252
9 no shutdown
```



```
10 exit
11
12 ! — Routage de Retour —
13 ! Le routeur doit savoir où renvoyer les paquets pour les VLANs (10.0.0.0/8 et
14 ! Route sommaire vers le Core
15 ip route 10.0.0.0 255.0.0.0 172.16.0.2
16 ip route 200.200.0.0 255.255.0.0 172.16.0.2
17
18 do write memory
```

7.3 Configuration des Services DHCP Voix (Sur le Routeur)

Objectif : Le Routeur CME doit fournir les IPs et l'option TFTP (Option 150) aux téléphones. Note : Si vous utilisez déjà le serveur DHCP dédié du Snapshot 1 pour les IPs, ignorez la partie network et ne configurez que le telephony-service. Cependant, il est courant que le CME gère ses propres scopes DHCP Voix.

Script (Création des Pools DHCP pour chaque VLAN Voix) :

```
1 configure terminal
2
3 ! — Pool DHCP Voix Étudiants (VLAN 111) —
4 ip dhcp pool VOICE_ETD
5 network 10.111.0.0 255.255.255.0
6 default-router 10.111.0.1
7 option 150 ip 172.16.0.1    ! L'IP du Routeur CME lui-même
8 dns-server 10.100.0.10
9
10 ! — Pool DHCP Voix Profs (VLAN 121) —
11 ip dhcp pool VOICE_PROF
12 network 10.121.0.0 255.255.255.0
13 default-router 10.121.0.1
14 option 150 ip 172.16.0.1
15 dns-server 10.100.0.10
16
17 ! — Pool DHCP Voix Admin (VLAN 131) —
18 ip dhcp pool VOICE_ADMIN
19 network 10.131.0.0 255.255.255.0
20 default-router 10.131.0.1
21 option 150 ip 172.16.0.1
22 dns-server 10.100.0.10
23
24 ! (Répéter pour les autres VLANs Voix si nécessaire)
25 do write memory
```

Important : Sur le Core Switch, vous devez modifier le ip helper-address des VLANs Voix pour pointer vers 172.16.0.1 (le Routeur) au lieu du serveur DHCP de données, si vous voulez que le routeur gère le DHCP Voix.

7.4 Configuration du Service de Téléphonie (CME)

Objectif : Activer le moteur de téléphonie, définir le nombre maximum de téléphones et configurer l'auto-enregistrement.

Équipement : ROUTER_



```
1 configure terminal
2
3 ! — Service de Téléphonie —
4 telephony-service
5 ! Capacité Max
6 max-ephones 50
7 max-dn 50
8
9 ! Adresse IP source pour l'enregistrement SCCP (L'IP du routeur)
10 ip source-address 172.16.0.1 port 2000
11
12 ! Attribution automatique des numéros (Extensions 1 à 50)
13 auto assign 1 to 50
14
15 ! Génération des fichiers de configuration XML pour les téléphones
16 create cnf-files
17 exit
18
19 ! — Définition des Numéros (Directory Numbers) —
20 ! Exemple : Plage 1000 pour Admin, 2000 pour Profs, 3000 pour Étudiants
21
22 ! -- Extension Admin 1 --
23 ephone-dn 1
24 number 1001
25 name Bureau_Directeur
26 label 1001
27
28 ! -- Extension Admin 2 --
29 ephone-dn 2
30 number 1002
31 name Secretariat
32 label 1002
33
34 ! -- Extension Prof 1 --
35 ephone-dn 3
36 number 2001
37 name Salle_Profs_1
38 label 2001
39
40 ! -- Extension Etudiant 1 --
41 ephone-dn 4
42 number 3001
43 name Hall_Etudiants
44 label 3001
45
46 exit
47 do write memory
```

7.5 Vérification Snapshot 5

- 1. Vérification DHCP :** Connectez un IP Phone sur un port d'accès (VLAN Voix 111). Il doit recevoir une IP 10.111.0.x et l'option TFTP 172.16.0.1.
- 2. Vérification Enregistrement :** Sur le routeur, lancez show ephone. Le téléphone doit apparaître avec le statut REGISTERED.
- 3. Test d'Appel :** Composez le 1001 depuis le téléphone 2001. L'appel doit s'établir ("Ring Out" / "Connected").



V. Conclusion/Recommendations

1 Bilan du Projet

Ce projet a permis la conception, la simulation et la validation d'une infrastructure réseau de campus universitaire complète, basée sur le modèle hiérarchique Cisco à trois couches (Core, Distribution, Accès).

Partant d'un besoin de connectivité basique, nous avons fait évoluer l'architecture à travers cinq phases techniques majeures (Snapshots), transformant un simple réseau commuté en une infrastructure de services convergents intelligente et sécurisée.

Les objectifs principaux ont été atteints :

- **Scalabilité** : L'architecture modulaire permet l'ajout de nouveaux bâtiments sans interruption de service.
- **Performance** : L'utilisation de l'agrégation de liens (EtherChannel LACP) et du routage Inter-VLAN matériel (Layer 3 Switching) garantit un débit optimal.
- **Sécurité** : Une stratégie de défense en profondeur a été appliquée, sécurisant l'accès physique (Port Security), l'intégrité logique (DHCP Snooping) et le cloisonnement des données (ACLs).
- **Convergence** : L'intégration réussie de la Téléphonie sur IP (VoIP) démontre la capacité du réseau à gérer des flux temps réel critiques.

2 Analyse des Résultats Techniques

La validation par étapes (Snapshots) a permis de confirmer les points suivants :

2.1 Stabilité du Layer 2 : Le protocole VTP a correctement propagé la base de données VLAN, et les trunks 802.1Q transportent efficacement le trafic tagué entre les bâtiments.

2.2 Efficacité du Routage : Le Core Switch gère efficacement le routage entre les sous-réseaux (Inter-VLAN), agissant comme la passerelle centrale performante.

2.3 Robustesse de la Sécurité :

- Les tests d'intrusion simulés (branchement d'un switch pirate, serveur DHCP rogue) ont été immédiatement bloqués par les mécanismes de protection (Violation Restrict / Trusted Ports).
- Les ACLs empêchent strictement les étudiants d'accéder au réseau d'administration, respectant la politique de confidentialité.



- Services Applicatifs : Les téléphones IP reçoivent leurs configurations via le routeur CME et s'enregistrent correctement, validant la configuration des VLANs Voix et de l'option DHCP 150.

3 Limitations de la Simulation

Bien que Cisco Packet Tracer soit un outil de simulation puissant, certaines limitations techniques ont été rencontrées par rapport à un déploiement réel :

- **Fonctionnalités VACL/PACL** : Les listes de contrôle d'accès basées sur les VLANs (VLAN Maps) sont limitées dans le simulateur, nécessitant l'utilisation d'ACLs routées (RACL) sur les interfaces SVI.
- **QoS Avancée** : Les mécanismes de file d'attente (Queuing) et de marquage (Marking) précis pour la VoIP sont simplifiés dans Packet Tracer.

Recommandations et Perspectives d'Évolution

Pour transformer cette simulation en un réseau de production professionnel, nous recommandons les évolutions suivantes :

1

Haute Disponibilité de Niveau 3 (HSRP/VRRP)

- Le CORE_MLS est un point de défaillance unique (SPOF) pour le routage.



- **Recommandation :** Ajouter un second Core Switch et configurer le protocole HSRP (Hot Standby Router Protocol) pour assurer une redondance de la passerelle par défaut.

2

Sécurité Périmétrique Avancée

Les ACLs sont des filtres "stateless" (sans état).

- **Recommandation :** Remplacer le filtrage par ACL sur le Core par un Pare-feu dédié (Cisco ASA ou Firepower) ou configurer un Zone-Based Firewall (ZBF) sur le routeur de bordure pour une inspection dynamique des paquets (Stateful inspection),



3

Gestion du Sans-Fil (Wireless)

Les VLANs Wireless (190/191) sont prêts.

- **Recommandation :** Déployer un Contrôleur Wifi (WLC) centralisé pour gérer les points d'accès légers (LAP), permettant le roaming transparent des utilisateurs entre les bâtiments.



4

Automatisation Réseau

La configuration manuelle (CLI) est sujette aux erreurs humaines.

- **Recommandation :** Utiliser des outils d'automatisation comme Ansible ou Python (Netmiko) pour déployer les configurations standard (NTP, SNMP, Users) sur l'ensemble des 15+ équipements simultanément.



