# Faculté des Sciences et Technologie

(FST)

# Niveau : L3-FST

**Cours : Réseaux 2**

**Soumis au chargé de cours : Ismaël SAINT AMOUR**

## Préparé par : Jameson DOMINIQUE

**Date : 31 Mai 2025**

Projet : Mise en Œuvre Pratique d'un Réseau d'Entreprise

# TD 7

Présentation Synthétique du Projet

# Titre du Projet

**Mise en Œuvre Pratique d’un Réseau d’Entreprise Sécurisé et Évolutif**

# Objectifs

Concevoir et configurer un réseau d’entreprise sécurisé et segmenté.

Assurer la communication contrôlée entre différents départements via le routage inter-VLAN. Automatiser l'attribution des adresses IP à l’aide de DHCP.

Permettre un accès Internet aux utilisateurs à travers la translation d’adresses (NAT). Sécuriser les accès distants avec SSH et contrôler le trafic réseau via des ACLs.

Simuler un environnement Internet interne avec un serveur Web.

# Outils Utilisés

**Cisco Packet Tracer** (simulateur de réseau) **Systèmes Cisco IOS** pour la configuration réseau **Protocoles et technologies :**

VLAN (802.1Q)

DHCP (Dynamic Host Configuration Protocol) NAT (Network Address Translation)

SSH (Secure Shell)

ACLs (Access Control Lists)

# Titre du Projet

**Mise en Œuvre Pratique d’un Réseau d’Entreprise Sécurisé et Évolutif**

# Objectif

**Objectif Général**

Le projet vise à concevoir, déployer et sécuriser un réseau d’entreprise qui répond aux besoins de connectivité, d’isolement entre départements, de gestion centralisée des IP, d’accès à Internet et de protection contre les accès non autorisés.

**Objectifs Spécifiques**

Segmenter le réseau avec des **VLANs** pour isoler les départements.

Configurer le **routage inter-VLAN** pour permettre la communication entre VLANs autorisés. Mettre en place un **DHCP** pour l’attribution automatique des adresses IP.

Déployer un **accès sécurisé** via **SSH**.

Configurer un **NAT** pour l'accès Internet.

Sécuriser l'accès au réseau avec **ACLs** (Listes de Contrôle d’Accès).

Tester l'accès Internet via un **serveur Web** interne simulant Internet.

# Contexte

L'entreprise **SmartTech SARL** dispose de plusieurs départements : Administration

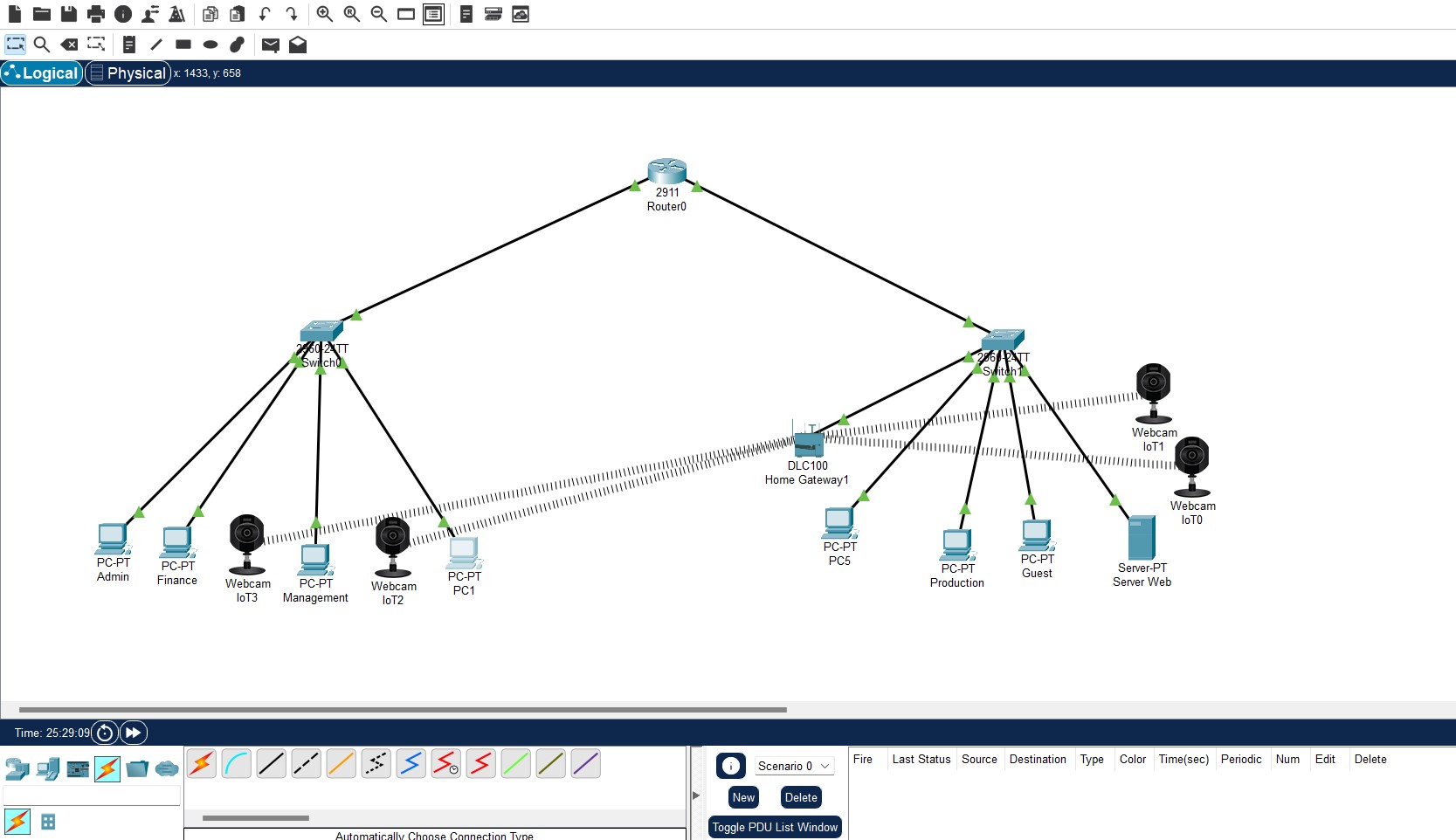
Finance Production Invités (Guest)

La politique de sécurité exige que :

Les invités n'aient pas accès aux ressources internes.

Les échanges entre départements soient autorisés uniquement si nécessaire. Tous les accès distants soient chiffrés.

# Architecture Réseau





# Technologies Utilisées

**Cisco Packet Tracer** (simulateur de réseau)

**Protocoles utilisés :** VLAN (IEEE 802.1Q) DHCP

NAT SSH ACL

**Adressage IP privé** (RFC 1918)

**Serveur Web interne** (HTTP pour test)

**Plan d'Adressage IP et VLAN**

|  |  |  |  |
| --- | --- | --- | --- |
| **VLAN** | **Département** | **Plage IP** | **VLAN ID** |
| 10 | Admin | 192.168.10.0/24 | 10 |
| 20 | Finance | 192.168.20.0/24 | 20 |
| 30 | Production | 192.168.30.0/24 | 30 |
| 40 | Guest | 192.168.40.0/24 | 40 |
| 99 | Management | 192.168.99.0/24 (Trunk Mgmt) | 99 |

|  |  |
| --- | --- |
| **Équipement** | **IP** |
| R1 (LAN) | 192.168.1.1 |
| R1 (WAN) | 203.0.113.2 (Internet Simulé) |
| Serveur Web | 192.168.100.10 |

# 

# Étapes de Configuration

# 

# 

# Tests à réaliser

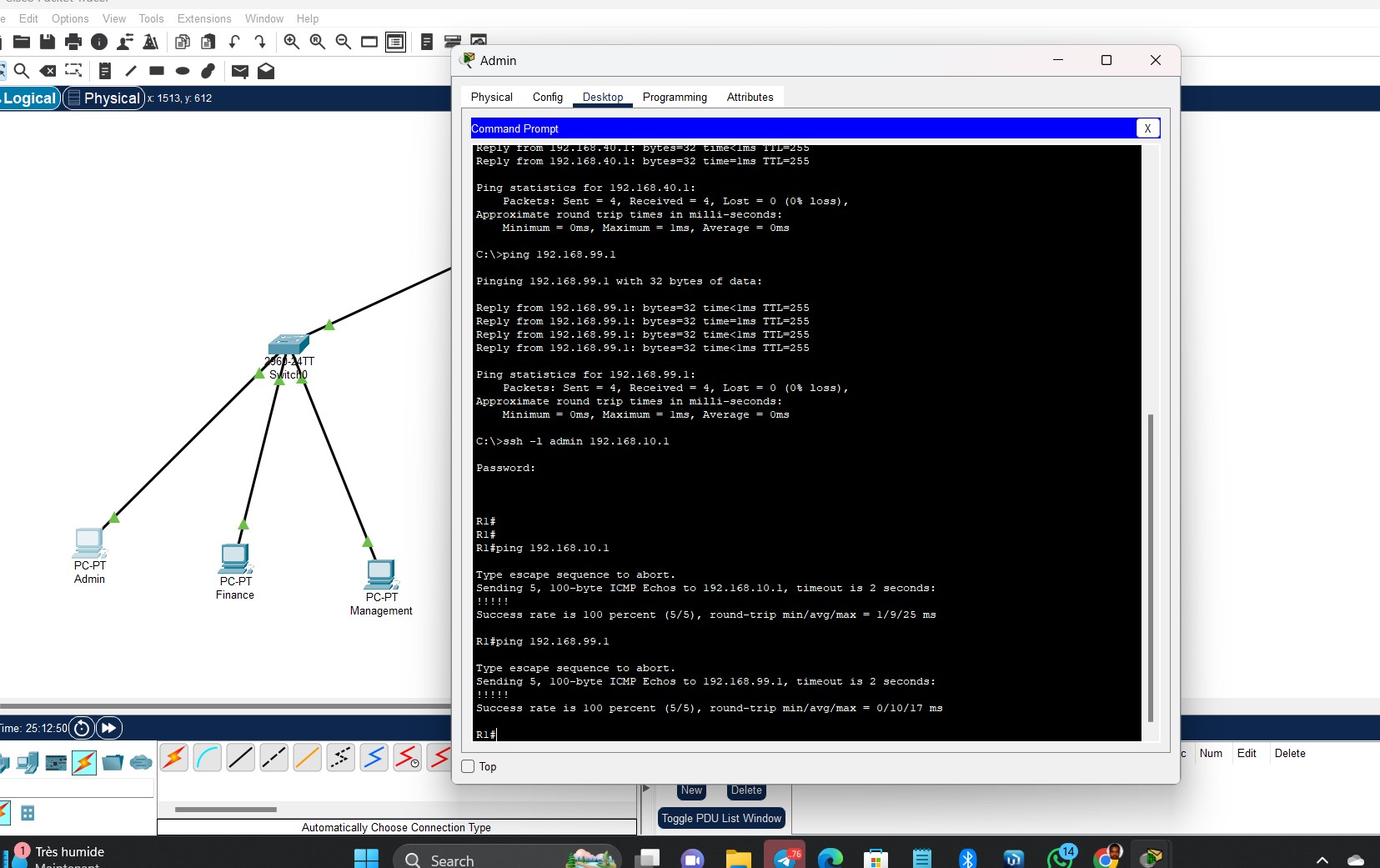
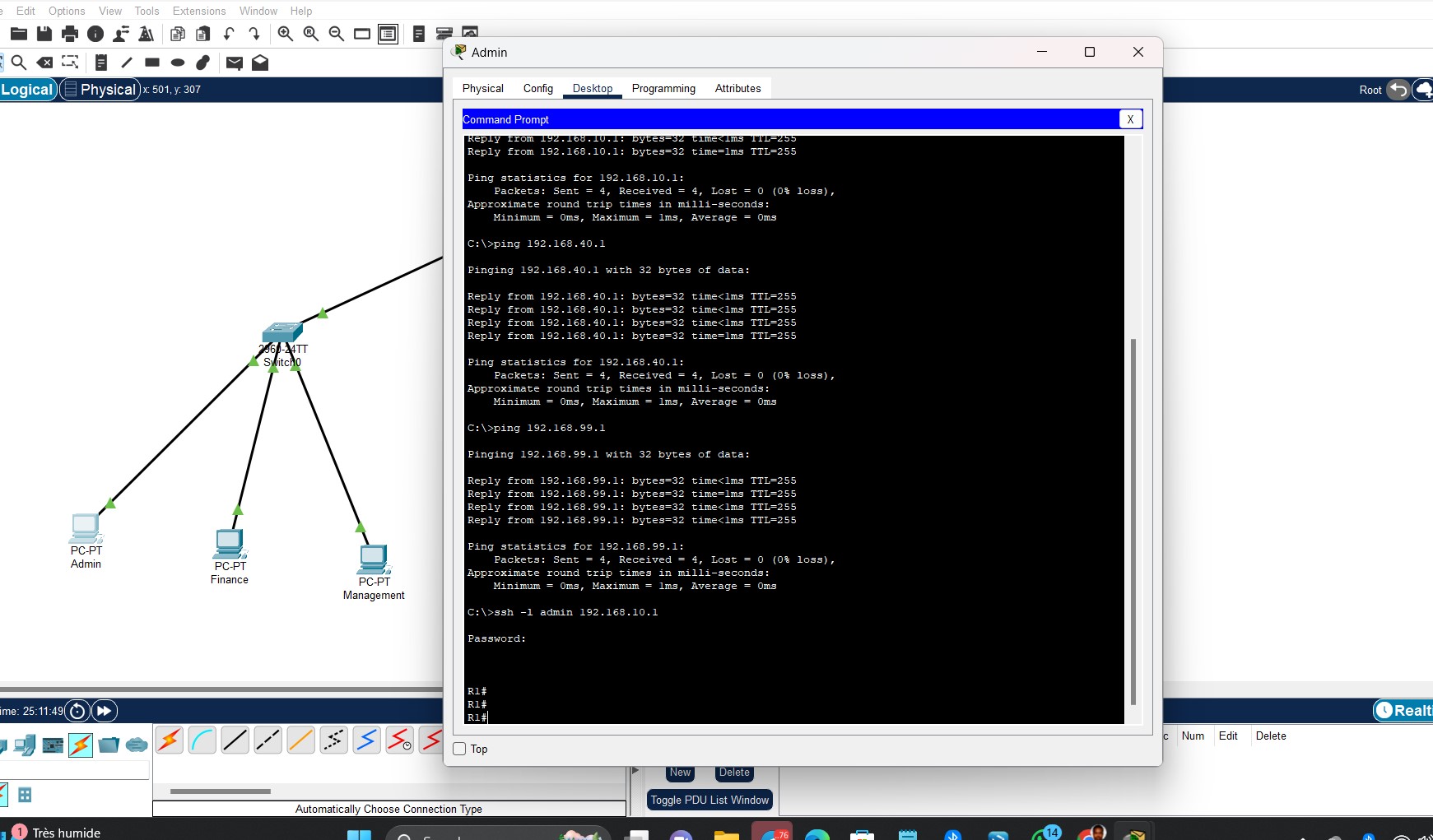
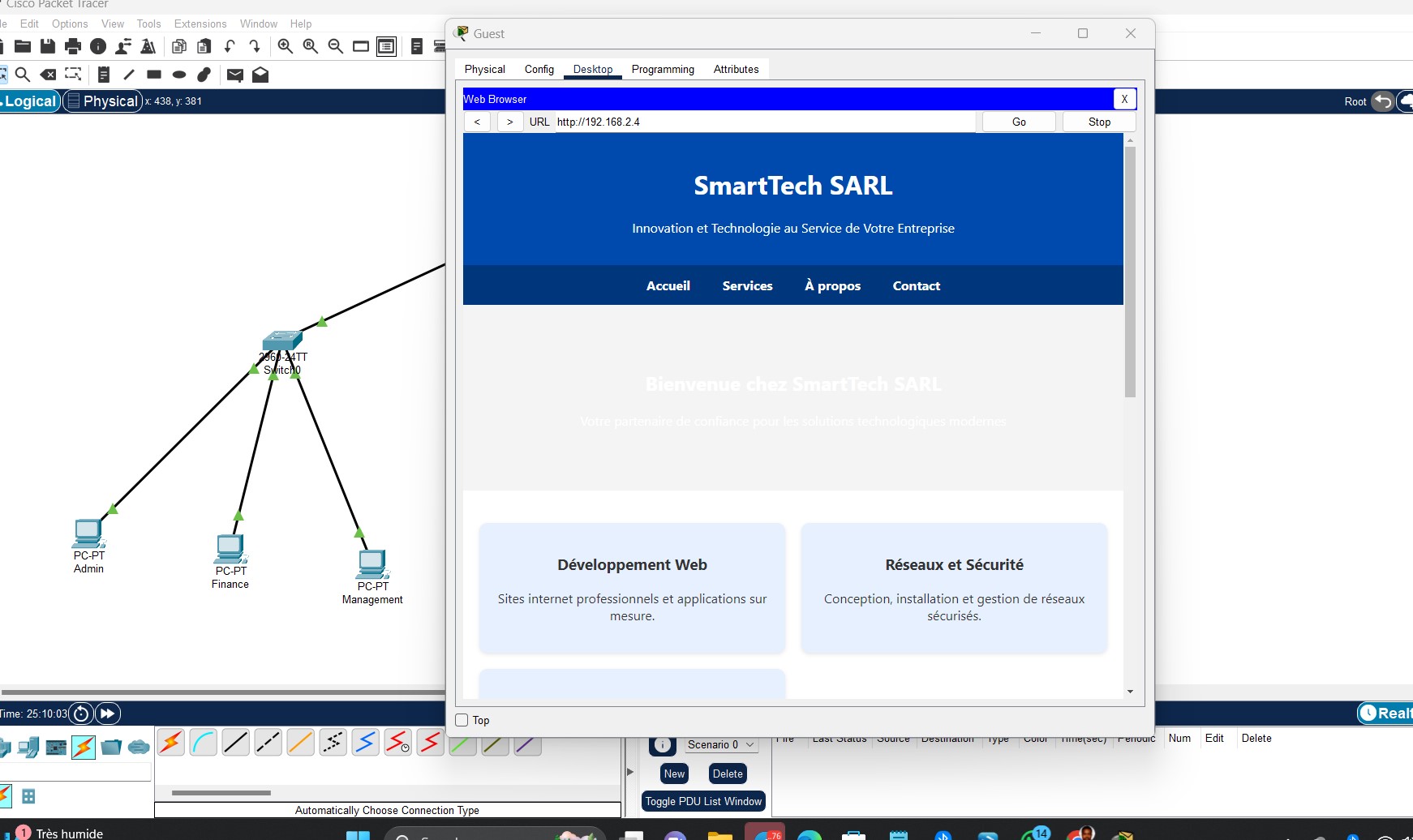
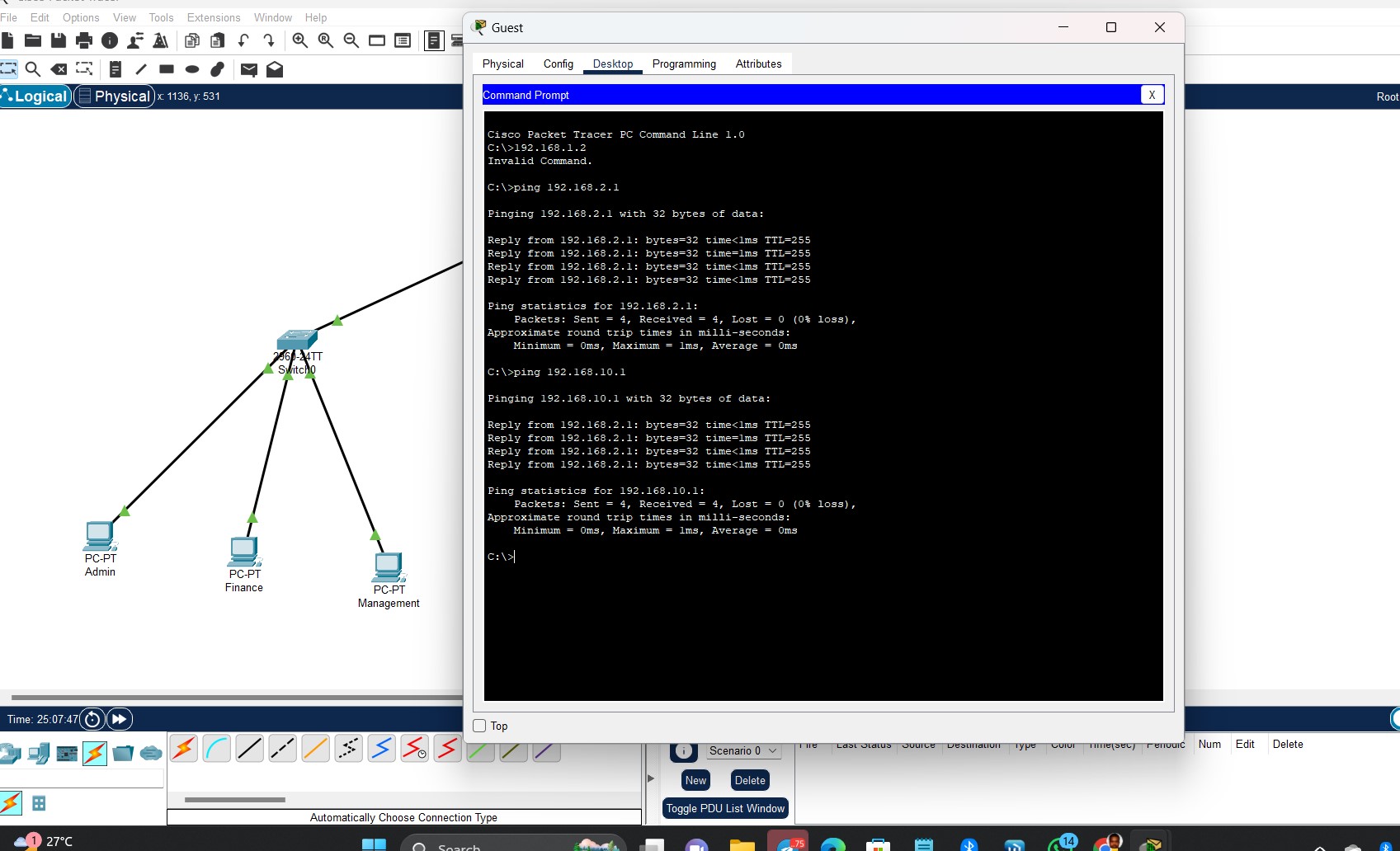
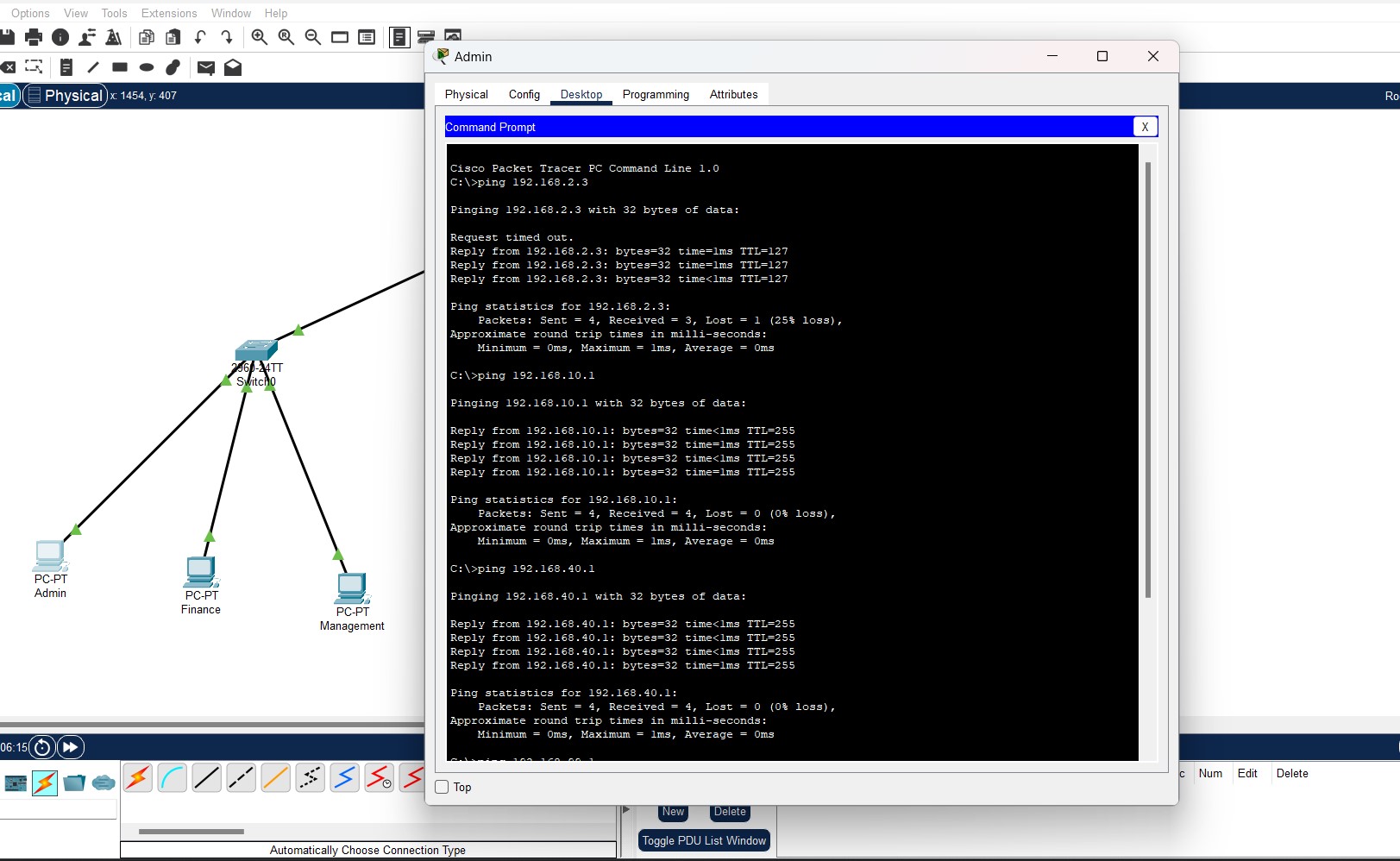
✅ Ping entre les PC de différents VLANs

✅ Accès Internet simulé vers le serveur Web

✅ Test d'accès SSH au routeur

✅ Vérification DHCP automatique sur les PCs

✅ ACL fonctionnelle : PC Guest bloqué vers autres VLANs



# Méthodologie

1. **Planification du réseau** : définition des VLANs, du schéma IP et de l'architecture physique.
2. **Création de la topologie** : mise en place des équipements dans Packet Tracer.
3. **Configuration des switchs** : création des VLANs et configuration du trunking.
4. **Configuration du routeur** :

Sous-interfaces pour le routage inter-VLAN. DHCP pour les clients.

NAT pour la sortie Internet. SSH pour l’accès sécurisé.

1. **Implémentation de la sécurité** : ACLs pour limiter l’accès des VLANs sensibles.
2. **Tests** : ping, accès Web, accès SSH, vérification des attributions DHCP.

# Résultats Obtenus

Tous les clients ont reçu automatiquement une adresse IP via DHCP. La communication inter-VLAN a été réussie selon les règles établies. Les clients pouvaient accéder au serveur Web simulé via NAT.

L’accès au routeur était sécurisé via SSH.

Le VLAN Guest a été correctement restreint grâce aux ACLs. Aucune perte de paquet détectée dans les tests de connectivité.

# Conclusion Générale

Le projet a permis de mettre en œuvre un réseau d’entreprise fonctionnel et sécurisé en appliquant des pratiques professionnelles.

Grâce à la segmentation par VLAN, au routage inter-VLAN, à l'utilisation de DHCP et de NAT, et à

l’implémentation de mesures de sécurité comme SSH et ACLs, le réseau répond aux besoins d’une infrastructure moderne, évolutive et fiable.

Cette expérience constitue une base solide pour des évolutions futures telles que la haute disponibilité, l'intégration VPN, ou encore la cybersécurisation avancée.