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.

Architecture

- **Un routeur principal (R1)** assurant le routage inter-VLAN, DHCP, NAT, et SSH.
- **Deux switchs (SW1 et SW2)** configurés avec VLANs et trunking.
- **Cinq ordinateurs clients (PCs)** répartis dans quatre VLANs : Admin, Finance, Production, Guest.
- **Un serveur Web** interne
- **Plan IP segmenté** par VLAN, routé via sous-interfaces du routeur.

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)

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.
5. **Implémentation de la sécurité** : ACLs pour limiter l'accès des VLANs sensibles.
6. **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.

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 :

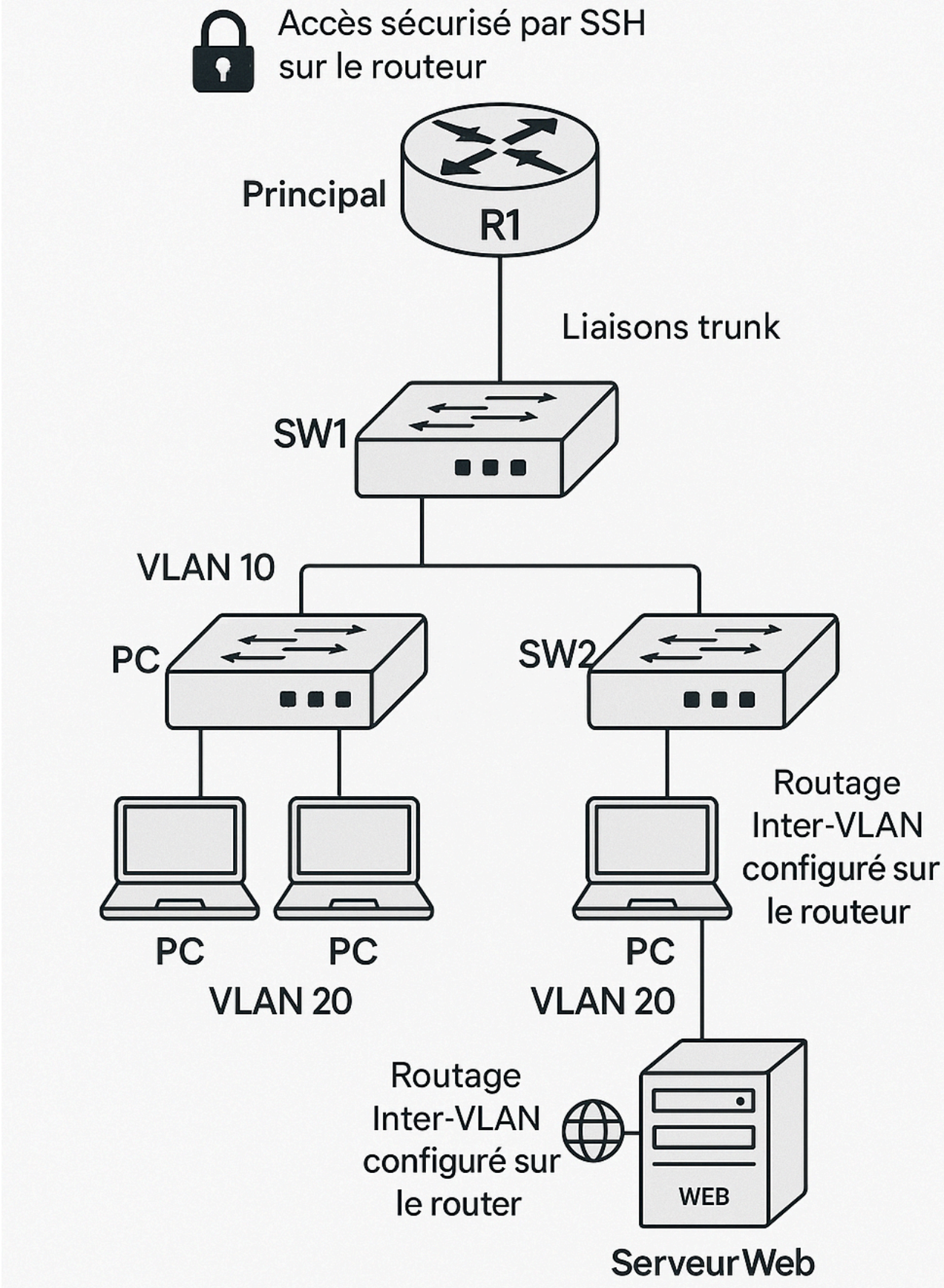
- Les invités n'aient pas accès aux ressources internes.
- Les échanges entre départements soient autorisés uniquement si nécessaire.
- Tous les accès distants soient chiffrés.

Architecture Réseau

- **1 Routeur Principal (R1)**
- **2 Switchs (SW1, SW2)**

- **5 Ordinateurs (PCs)** répartis entre les VLANs
- **1 Serveur Web** pour tester l’accès Internet
- **Routage Inter-VLAN** configuré sur le routeur
- **Liaisons trunk** entre switchs et routeur
- **Accès sécurisé** par SSH sur le routeur

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

Switches

- Création des VLANs
- Affectation des ports aux VLANs
- Configuration de Trunk entre SW1 et SW2

```
enable
conf t
hostname

vlan 10
name Admin

vlan 20
name Finance

vlan 30
name Production

vlan 40
name Guest

vlan 99
name Management

interface range fa0/1 - 5
switchport mode access
switchport access vlan 10

interface range fa0/6 - 10
switchport mode access
switchport access vlan 20

interface f0/24
switchport mode trunk
```

Routeur

- Configuration des interfaces sub-interfaces pour Inter-VLAN Routing
- Serveur DHCP
- NAT pour accès Internet
- Activation de SSH
- Application d'une ACL pour filtrer les invités

Configurer le Routage Inter-VLAN sur le Routeur

Créer des sous-interfaces pour chaque VLAN :

```
enable
conf t
hostname R1
```

```
interface g0/0.10
encapsulation dot1q 10
ip address 192.168.10.1 255.255.255.0

interface g0/0.20
encapsulation dot1q 20
ip address 192.168.20.1 255.255.255.0

interface g0/0.30
encapsulation dot1q 30
ip address 192.168.30.1 255.255.255.0

interface g0/0.40
encapsulation dot1q 40
ip address 192.168.40.1 255.255.255.0

interface g0/0.99
encapsulation dot1q 99
ip address 192.168.99.1 255.255.255.0
```

Configurer un Serveur DHCP

```
interface g0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit

ip dhcp pool ADMIN
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 8.8.8.8

interface g0/1
ip address 192.168.2.1 255.255.255.0
no shutdown
exit

ip dhcp pool Production
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 8.8.8.8
```

Sécuriser les Accès avec SSH

```
ip domain-name smarttech.local
crypto key generate rsa
username admin privilege 15 secret admin123

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

Configurer le NAT pour l'Accès Internet

```
access-list 1 permit 192.168.0.0 0.0.255.255

interface g0/1
ip nat outside

interface g0/0
ip nat inside

ip nat inside source list 1 interface g0/1 overload
```

Configurer ACL pour le VLAN Guest

```
access-list 100 deny ip 192.168.40.0 0.0.0.255 any
access-list 100 permit ip any any

interface g0/0.40
ip access-group 100 in
```

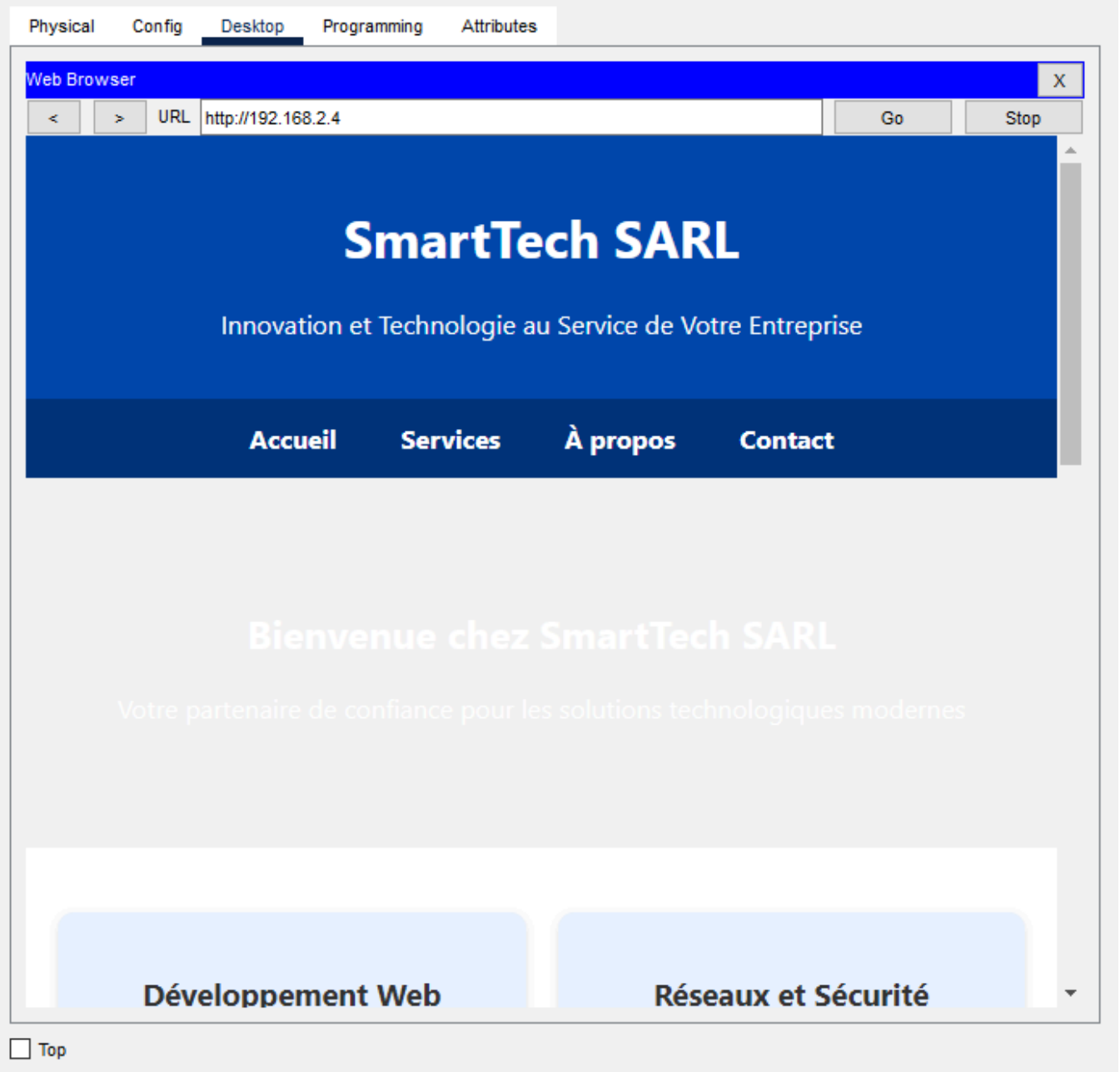
Configuration serveur Web

```
<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>SmartTech SARL</title>
    <style>
        body {
            margin: 0;
```

```
            font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
            background-color: #f4f4f4;
            color: #333;
        }
        header {
            background-color: #004aad;
            color: white;
            padding: 20px 0;
            text-align: center;
        }
        nav {
            display: flex;
            justify-content: center;
            background-color: #00367c;
        }
        nav a {
            color: white;
            padding: 14px 20px;
            text-decoration: none;
            font-weight: bold;
        }
        nav a:hover {
            background-color: #005fcc;
        }
        .hero {
            padding: 60px 20px;
            text-align: center;
            background: url('https://via.placeholder.com/1200x400') no-repeat center/cover;
            color: white;
        }
        .content {
            padding: 40px 20px;
            display: grid;
            grid-template-columns: repeat(auto-fit, minmax(250px, 1fr));
            gap: 20px;
            background: white;
        }
        .card {
            background-color: #e6f0ff;
            padding: 20px;
            border-radius: 10px;
            text-align: center;
            box-shadow: 0 2px 5px rgba(0,0,0,0.1);
        }
        footer {
            background-color: #00367c;
            color: white;
            text-align: center;
            padding: 15px 0;
            font-size: 0.9em;
        }
    </style>
</head>
```

```
<body>

    <header>
        <h1>SmartTech SARL</h1>
        <p>Innovation et Technologie au Service de Votre Entreprise</p>
    </header>

    <nav>
        <a href="#accueil">Accueil</a>
        <a href="#services">Services</a>
        <a href="#apropos">À propos</a>
        <a href="#contact">Contact</a>
    </nav>

    <section class="hero" id="accueil">
        <h2>Bienvenue chez SmartTech SARL</h2>
        <p>Votre partenaire de confiance pour les solutions technologiques modernes</p>
    </section>

    <section class="content" id="services">
        <div class="card">
            <h3>Développement Web</h3>
            <p>Sites internet professionnels et applications sur mesure.</p>
        </div>
        <div class="card">
            <h3>Réseaux et Sécurité</h3>
            <p>Conception, installation et gestion de réseaux sécurisés.</p>
        </div>
        <div class="card">
            <h3>Support Informatique</h3>
            <p>Assistance technique et maintenance pour vos équipements IT.</p>
        </div>
    </section>

    <section class="content" id="apropos">
        <div class="card">
            <h3>À propos de nous</h3>
            <p>SmartTech SARL est une entreprise innovante spécialisée dans les solutions
digitales pour les entreprises de toutes tailles.</p>
        </div>
    </section>

    <section class="content" id="contact">
        <div class="card">
            <h3>Contactez-nous</h3>
            <p>Email: contact@smarttechsarl.com</p>
            <p>Téléphone: +225 07 07 07 07 07</p>
        </div>
    </section>

    <footer>
        <p>&copy; 2025 SmartTech SARL. Tous droits réservés.</p>
    </footer>
```

```
</body>
</html>
```



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

Vérification du DHCP Automatique sur les PCs

- Objectif : S’assurer que tous les PCs reçoivent automatiquement leur adresse IP via DHCP.
- Vérification :
  - Vérifier l'adresse IP attribuée à chaque PC.
  - Elle doit être cohérente avec la plage IP du VLAN associé.

📋 Résultat attendu :

- Adresses IP correctes.

Test de Connectivité entre les PCs de différents VLANs

- Objectif : Vérifier que les PCs appartenant à différents VLANs peuvent communiquer via le routage Inter-VLAN.
- Commande à utiliser depuis chaque PC :

```
ping [Adresse IP d'un autre PC]
```

Accès Internet simulé via le Serveur Web

- Objectif : Tester que les PCs ont un accès vers un serveur Web interne simulant Internet.
- Commande ou action :
  - Ouvrir le navigateur du PC.
  - Accéder à l’adresse IP du serveur Web

📋 Résultat attendu :

- Affichage de la page web du serveur simulé.

Test d’Accès SSH au Routeur

- Objectif : Vérifier que le routeur est accessible de manière sécurisée via SSH.
- Commande à utiliser depuis un PC :

```
ssh -l admin 192.168.10.1
```

Travaux Dirigés

Installation d'une Infrastructure Réseau pour PME avec DNS, DHCP et Capteurs IoT

Objectifs :

- Déployer un réseau d’entreprise complet avec DHCP pour l’attribution automatique des adresses IP.
- Installer un serveur DNS local pour la résolution des noms internes.
- Intégrer des capteurs IoT (capteurs de température, détecteurs de mouvement) pour le suivi de l’environnement de travail.

Architecture :

- 1 Routeur principal
- 2 Switchs
- 1 Serveur DNS/DHCP sur Ubuntu Server
- 10 PCs (Administration + Technique)
- 5 Appareils IoT connectés (capteurs de température, caméras)
- VLAN IoT isolé pour sécuriser les objets connectés.

Contenu du rapport

Le rapport doit inclure :

1. Une page de couverture.
2. Une description des résultats de la tâche.
3. Les résultats de l'exécution des commandes (captures d'écran).
4. Les conclusions sur la tâche accomplie.
5. Hébergez le rapport de travail au format Markdown, Word ,HTML,PDF, le fichier gns3, ainsi que les images sur GitHub.