



**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

---

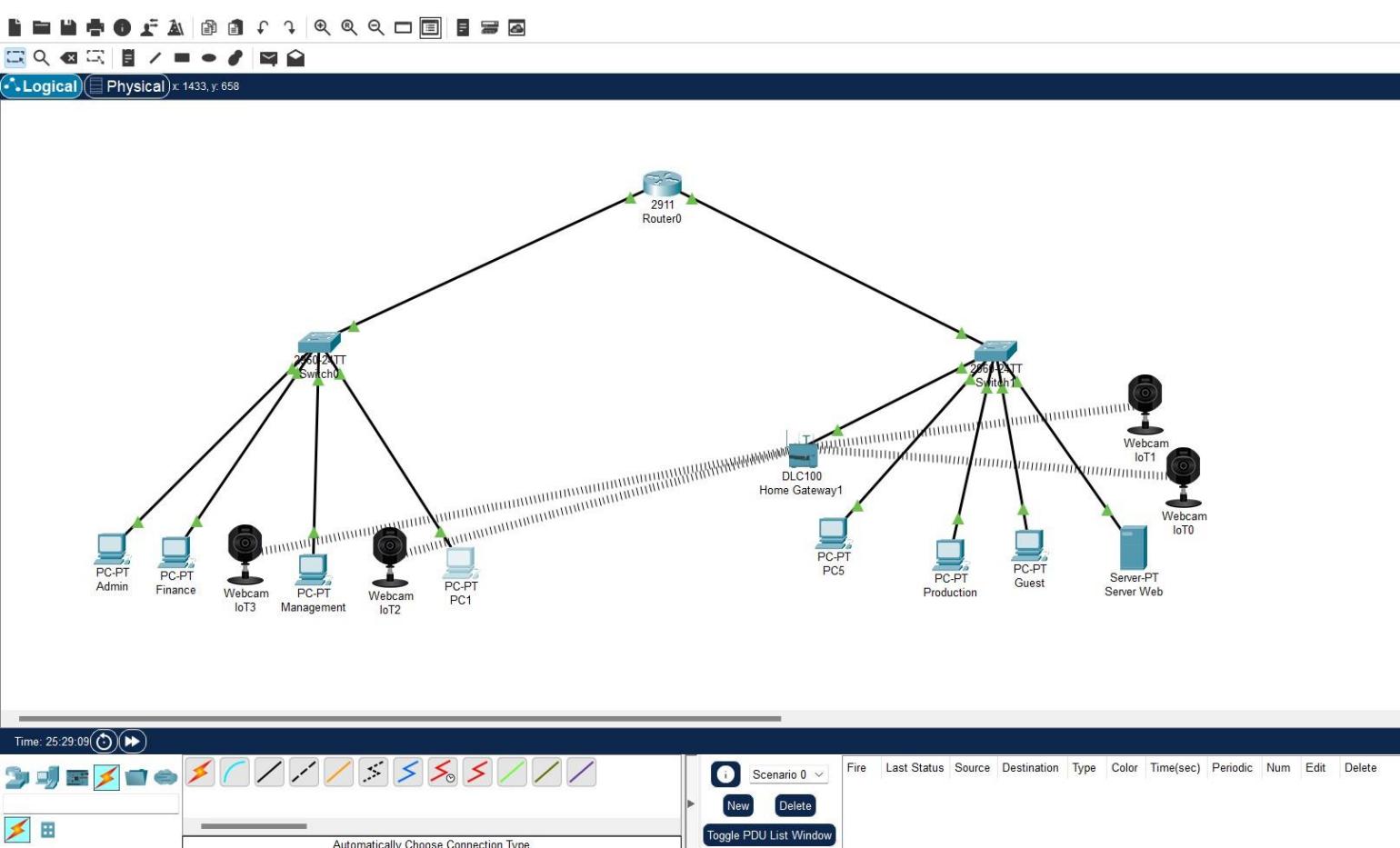
L'entreprise **SmartTech SARL** dispose de plusieurs départements :

- ♦ 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

Switch>en  
Switch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#vlan 10  
Switch(config-vlan)#name Admin  
Switch(config-vlan)#vlan 20  
Switch(config-vlan)#name Finance  
Switch(config-vlan)#vlan 30  
Switch(config-vlan)#name Production  
Switch(config-vlan)#vlan 40  
Switch(config-vlan)#name Guest  
Switch(config-vlan)#vlan 99  
Switch(config-vlan)#name Management  
Switch(config-vlan)#interface range fa0/1 -5  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 10  
Switch(config-if-range)#interface range fa0/6 -10  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 20  
Switch(config-if-range)#interface range fa0/11 -15  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 30  
Switch(config-if-range)#interface range fa0/16 -120  
interface range not validated - command rejected  
Switch(config)#interface range fa0/16 -20  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 40  
Switch(config-if-range)#interface range fa0/21 -24  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 99  
Switch(config-if-range)#interface f0/24  
Switch(config-if)#switchport mode trunk  
Switch(config-if) #

Copy Paste Delete

Switch>en  
Switch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#hostname S2  
S2(config)#vlan 10  
S2(config-vlan)#name Finance  
S2(config-vlan)#name Admin  
S2(config-vlan)#vlan 20  
S2(config-vlan)#name Finance  
S2(config-vlan)#vlan 30  
S2(config-vlan)#name Production  
S2(config-vlan)#vlan 40  
S2(config-vlan)#name Guest  
S2(config-vlan)#vlan 99  
S2(config-vlan)#name Management  
S2(config-vlan)#interface fa0/1 -5  
^  
% Invalid input detected at '^' marker.  
S2(config-vlan)#interface range fa0/1 -5  
S2(config-if-range)#switchport mode access  
S2(config-if-range)#switchport access vlan10  
^  
% Invalid input detected at '^' marker.  
S2(config-if-range)#switchport access vlan 10  
S2(config-if-range)#interface range fa0/6 -10  
S2(config-if-range)#switchport mode access  
S2(config-if-range)#switchport access vlan 20  
S2(config-if-range)#interface range fa0/11 -15  
S2(config-if-range)#switchport mode access  
S2(config-if-range)#switchport access vlan 30  
S2(config-if-range)#interface range fa0/16 -20  
S2(config-if-range)#switchport mode access  
S2(config-if-range)#switchport access vlan 40  
S2(config-if-range)#interface range fa0/20 -24  
S2(config-if-range)#switchport mode access  
S2(config-if-range)#switchport access vlan 99  
S2(config-if-range)#interface f0/24  
S2(config-if)#switchport mode trunk  
S2(config-if) #

Copy Paste Delete

Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch(config-vlan)#name Management
Switch(config-vlan)#interface range fa0/1 -5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#interface range fa0/6 -10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#interface range fa0/11 -15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#interface range fa0/16 -120
interface range not validated - command rejected
Switch(config)#interface range fa0/16 -20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#interface range fa0/21 -24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
Switch(config-if-range)#interface f0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#hostname S1
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#wr
Building configuration...
[OK]
S1#
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

S1 con0 is now available
```

Copy Paste

Creation Type Top

Search

Switch1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
S2(config-vlan)#name Guest
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management
S2(config-vlan)#interface fa0/1 -5
^
% Invalid input detected at '^' marker.

S2(config-vlan)#interface range fa0/1 -5
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan10
^
% Invalid input detected at '^' marker.

S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/6 -10
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#interface range fa0/11 -15
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/16 -20
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 40
S2(config-if-range)#interface range fa0/20 -24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 99
S2(config-if-range)#interface f0/24
S2(config-if)#switchport mode trunk
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#wr
Building configuration...
[OK]
S2#
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

S2 con0 is now available
```

Copy Paste

Creation Type Top

Search

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface g0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#
* Invalid input detected at '^' marker.

R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#interface g0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#interface g0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#interface g0/0.40
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#interface g0/0.99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#interface g0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
$LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
$LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up
$LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

R1(config-if)#
$LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to up
$LINK-5-CHANGED: Interface GigabitEthernet0/0.99, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.99, changed state to up
```

Copy Paste

pe Top

Re Delete

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
$LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to up
$LINK-5-CHANGED: Interface GigabitEthernet0/0.99, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.99, changed state to up

R1(config-if)#exit
R1(config)#ip dhcp pool ADMIN
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#exit
R1(config)#interface g0/1
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
$LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
$LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
exit
R1(config)#exit
R1#
$SYS-5-CONFIG_I: Configured from console by console

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool Production
R1(dhcp-config)#network 192.168.2.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.2.1
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#exit
R1(config)#domain-name smarttech.local
R1(config)#crypto key generate rsa
The name for the keys will be: R1.smarttech.local
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 512
```

Copy Paste

pe Top

Re Delete

**Router0**

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool Production
R1(dhcp-config)#network 192.168.2.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.2.1
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#exit
R1(config)#ip domain-name smarttech.local
R1(config)#crypto key generate rsa
The name for the keys will be: R1.smarttech.local
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 512
* Generating 512 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#username admin privilege 15 secret admin1234@#
*Mar 1 0:32:37.194: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#access-list permit 192.168.0.0 .0.0.255.255
^
* Invalid input detected at '^' marker.

R1(config)#access-list 1 permit 192.168.0.0 .0.0.255.255
^
* Invalid input detected at '^' marker.

R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#interface g0/1
R1(config-if)#ip nat outside
R1(config-if)#interface g0/0
R1(config-if)#ip nat inside
R1(config-if)#ip nat inside source list 1 interface g0/1 overload
R1(config)#access-list 100 deny ip 192.168.40.0 0.0.0.255 any
R1(config)#access-list 100 permit ip any any
R1(config)#interface g0/0.40
R1(config-subif)#ip access-group 100 in
R1(config-subif)#

```

Copy Paste

Top

**Admin**

Physical Config Desktop Programming Attributes

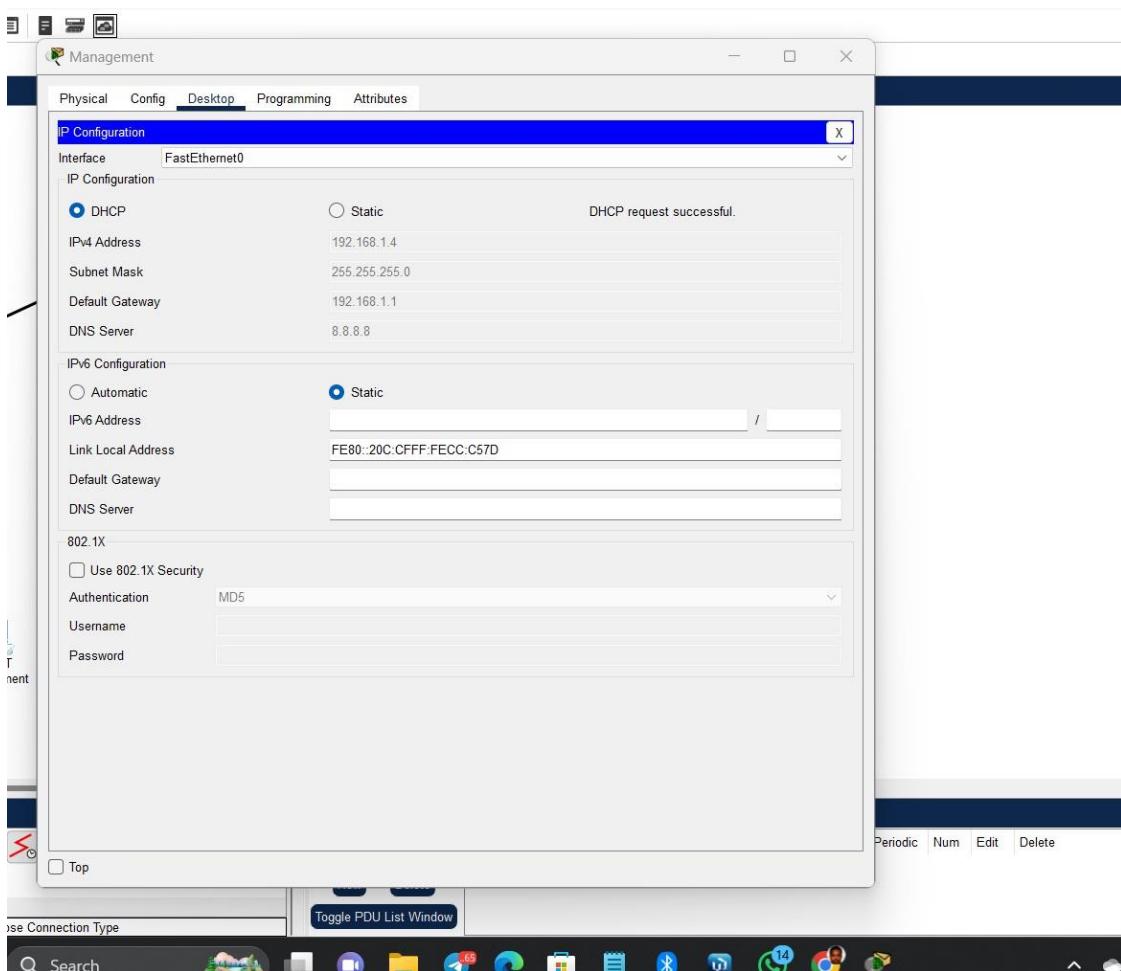
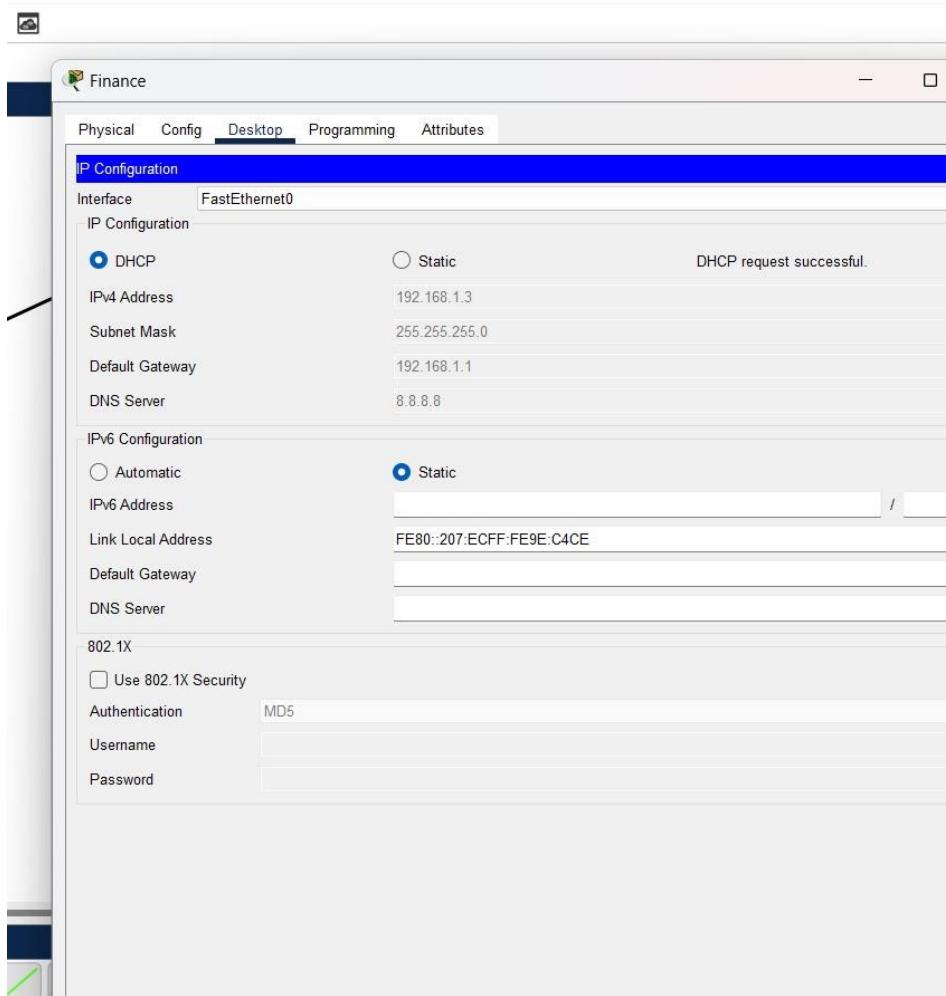
**IP Configuration**

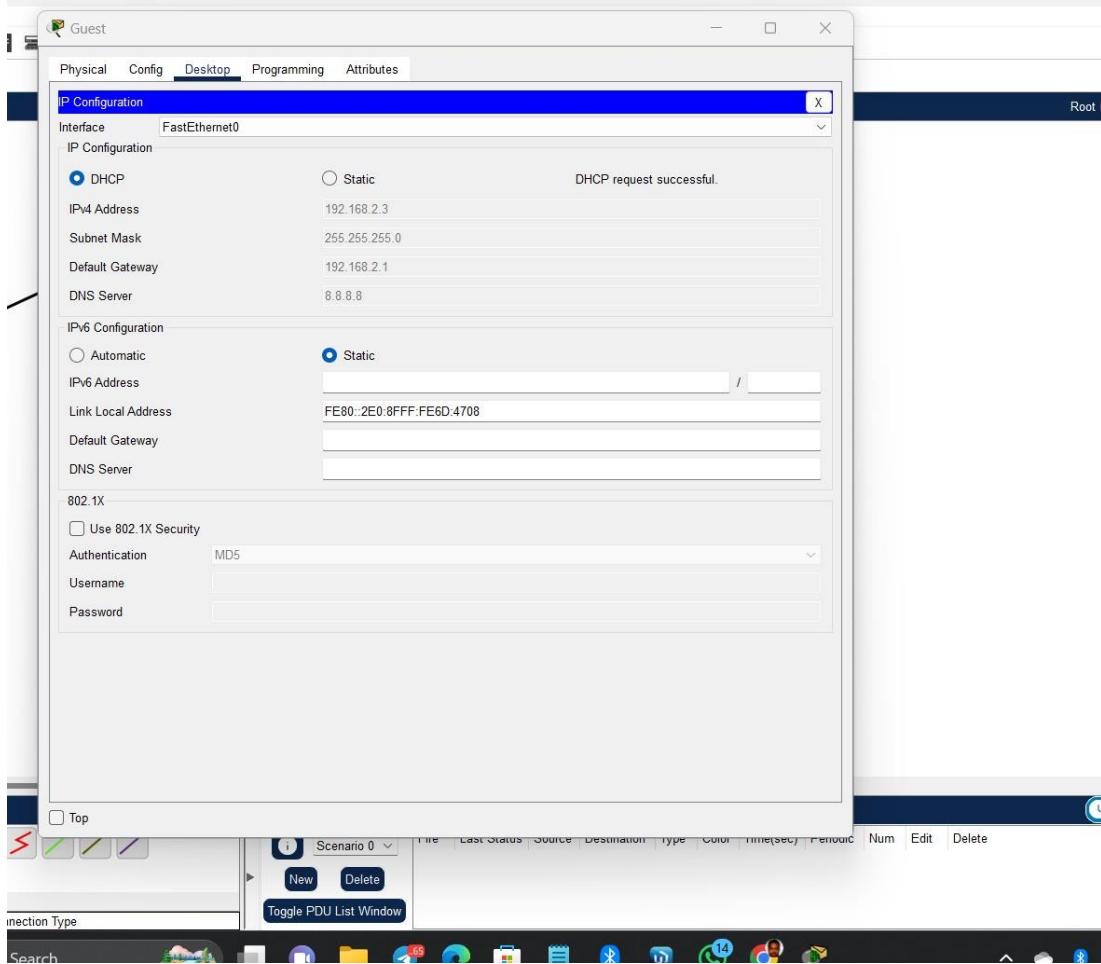
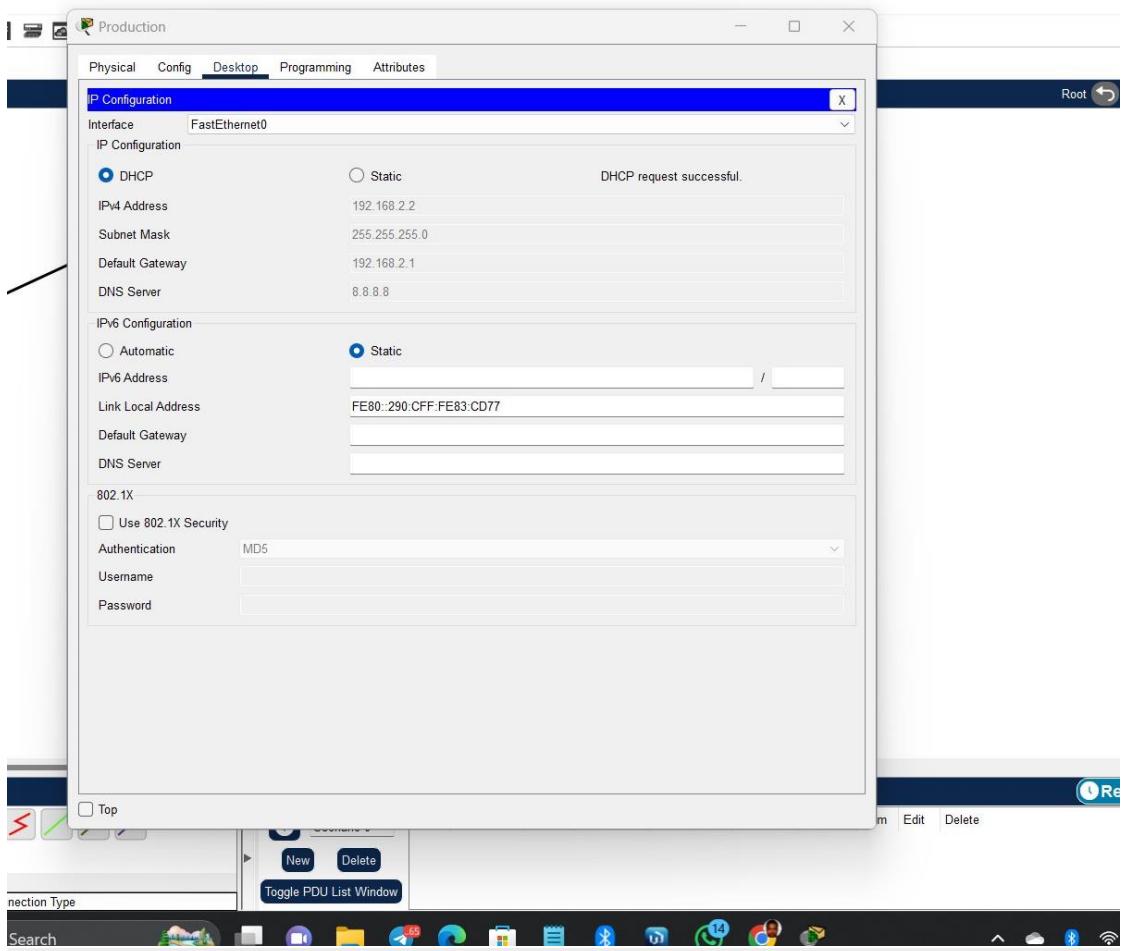
Interface	FastEthernet0
IP Configuration	<input checked="" type="radio"/> DHCP <input type="radio"/> Static      DHCP request successful.
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	8.8.8.8
IPv6 Configuration	<input type="radio"/> Automatic <input checked="" type="radio"/> Static      / /
IPv6 Address	
Link Local Address	FE80::20C:85FF:FEA6:2CEC
Default Gateway	
DNS Server	
802.1X	<input type="checkbox"/> Use 802.1X Security Authentication: MD5 Username: _____ Password: _____

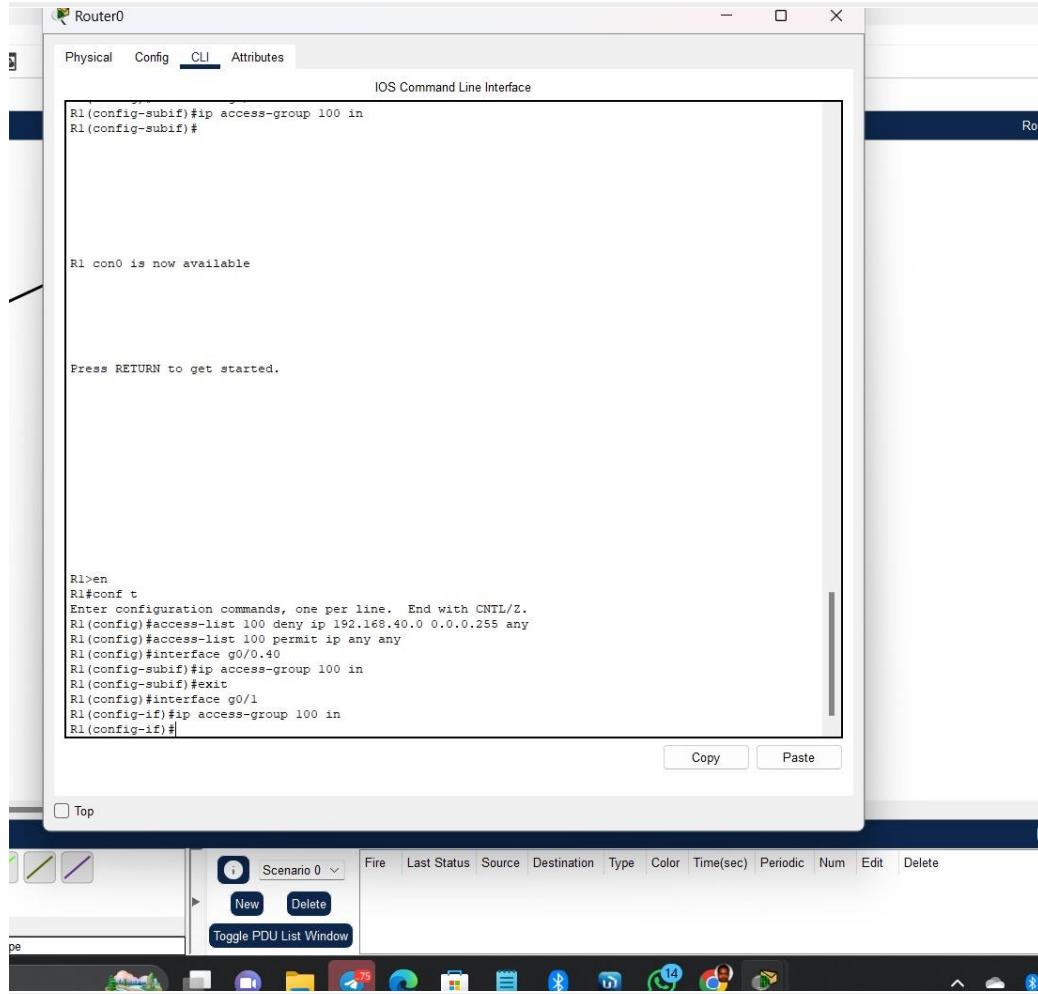
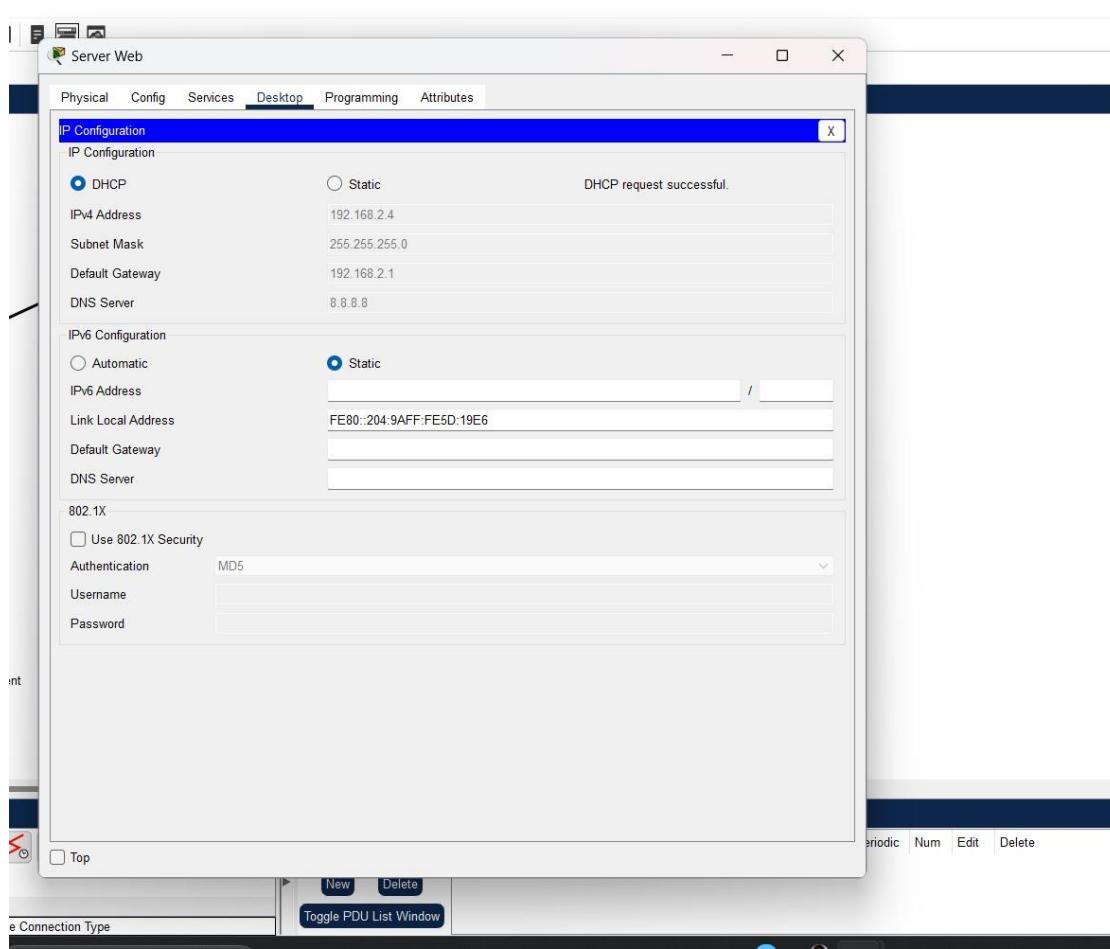
Top

New Delete Toggle PDU List Window

Search







Server Web

Physical Config Services Desktop Programming Attributes

**SERVICES**

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

**HTTP**

HTTP: On      HTTPS: On

**File Manager**

File Name	Edit	Delete
1 copyrights.html	(edit)	(delete)
2 cscptologo177x111.jpg		(delete)
3 helloworld.html	(edit)	(delete)
4 image.html	(edit)	(delete)
5 index.html	(edit)	(delete)

New File Import

⋮ Top

⋮ Choose Connection Type Toggle PDU List Window

Search

Root

Server Web

Physical Config Services Desktop Programming Attributes

**SERVICES**

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

**File Name:** index.html

```
<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>

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

</body>
</html>

File Manager Save

⋮ Top

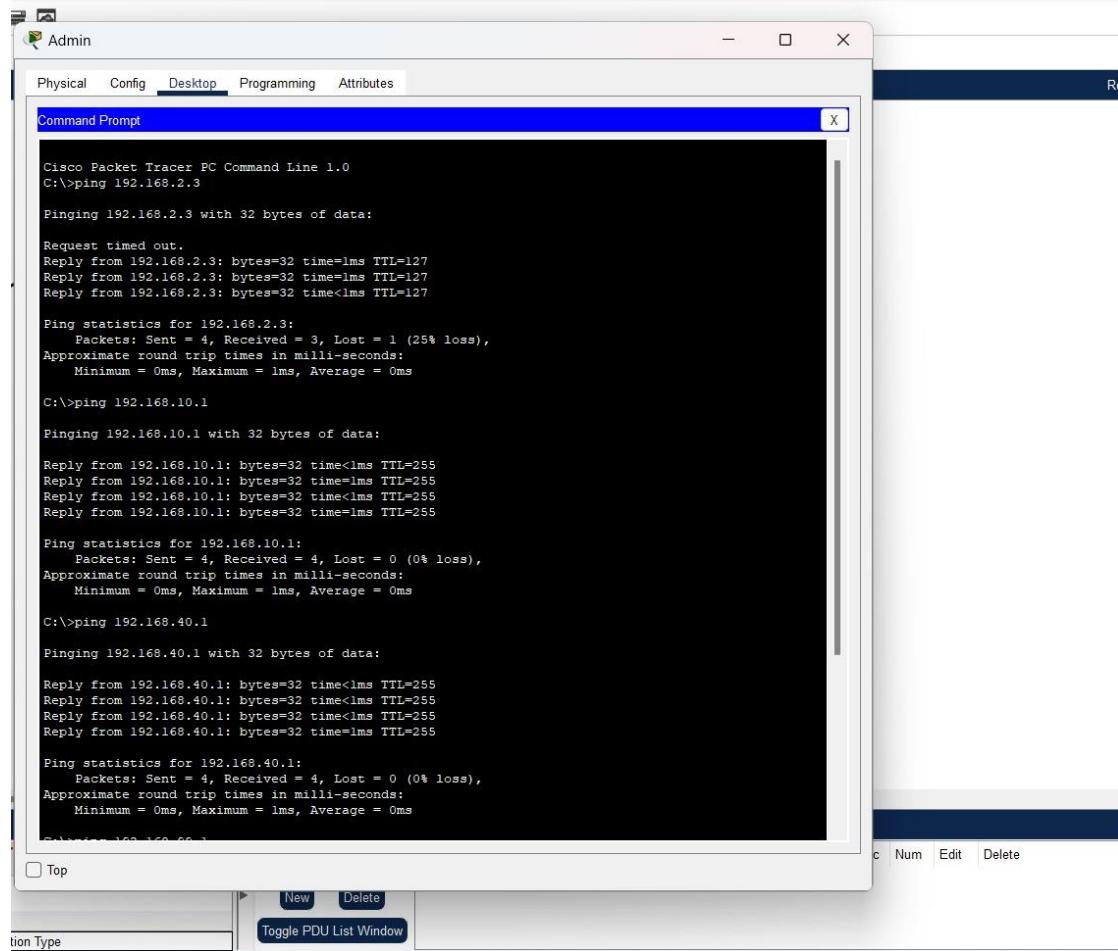
⋮ Choose Connection Type Toggle PDU List Window

Search

Root

# 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



The screenshot shows a Cisco Packet Tracer interface with a Command Prompt window open. The window title is "Command Prompt". The content of the window shows several ping commands being run from a Windows-like command line interface:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

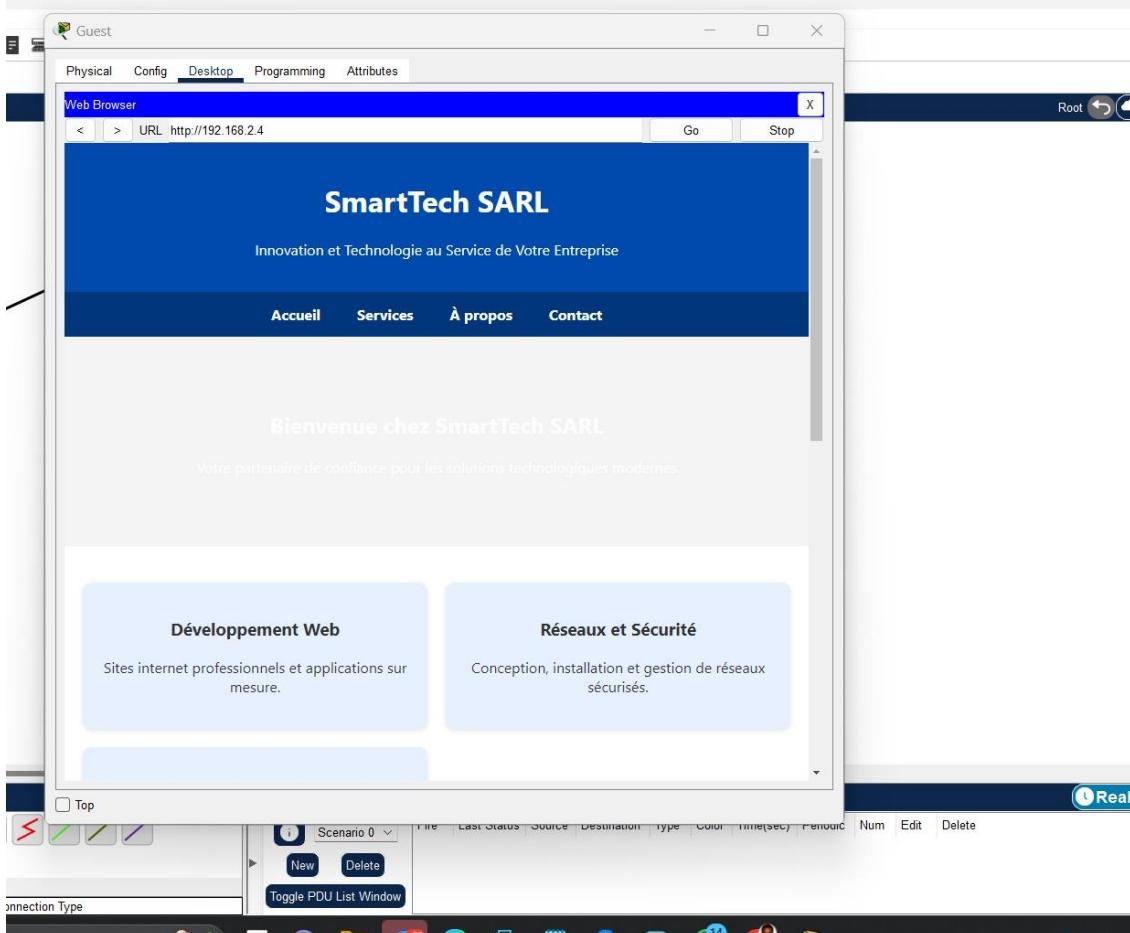
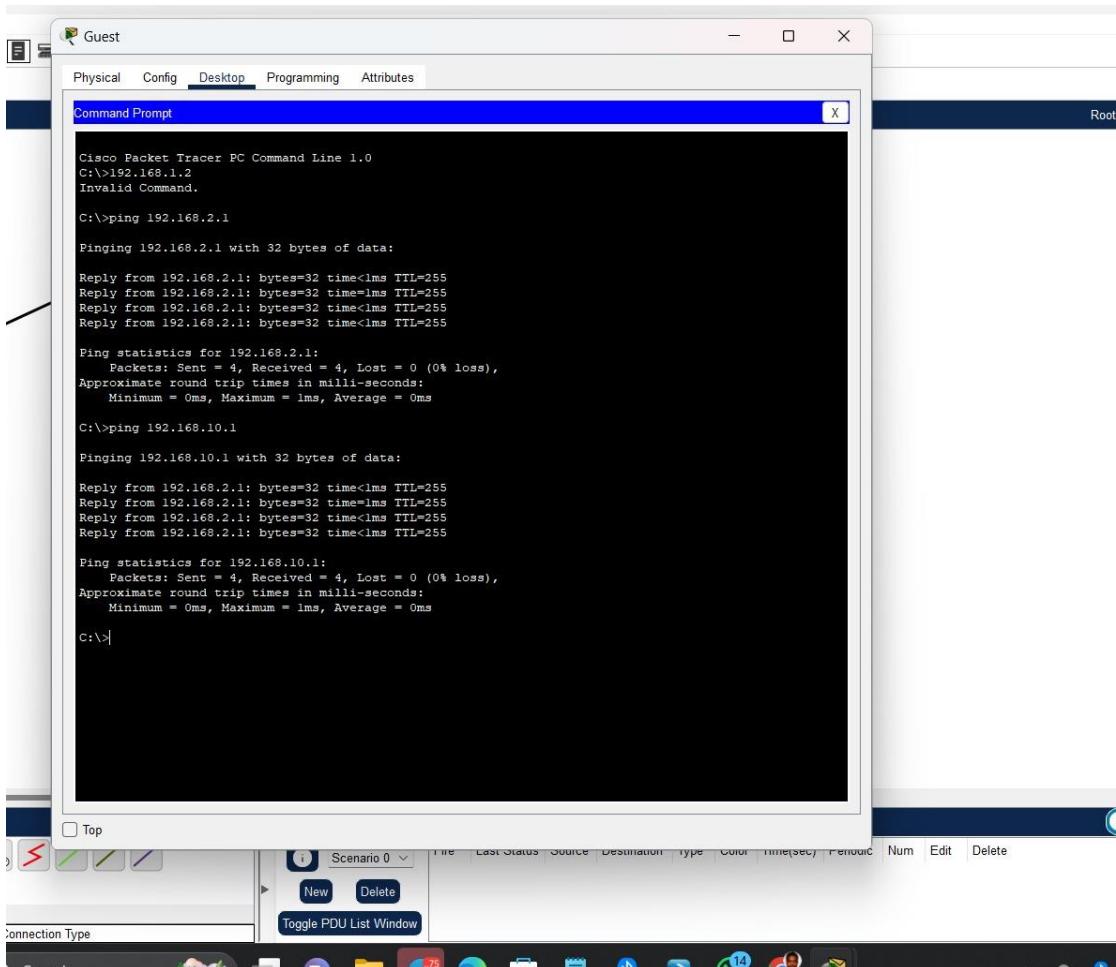
C:\>ping 192.168.40.1

Pinging 192.168.40.1 with 32 bytes of data:

Reply from 192.168.40.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Below the Command Prompt window, there is a toolbar with buttons for "Top", "New", "Delete", and "Toggle PDU List Window".



Admin

Physical Config Desktop Programming Attributes

Command Prompt

```
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.40.1

Pinging 192.168.40.1 with 32 bytes of data:

Reply from 192.168.40.1: bytes=32 time<1ms TTL=255
Reply from 192.168.40.1: bytes=32 time=1ms TTL=255
Reply from 192.168.40.1: bytes=32 time<1ms TTL=255
Reply from 192.168.40.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.99.1

Pinging 192.168.99.1 with 32 bytes of data:

Reply from 192.168.99.1: bytes=32 time<1ms TTL=255
Reply from 192.168.99.1: bytes=32 time=1ms TTL=255
Reply from 192.168.99.1: bytes=32 time<1ms TTL=255
Reply from 192.168.99.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.99.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ssh -l admin 192.168.10.1
Password:

R1#
```

Realt

New Delete

Connection Type

Toggle PDU List Window

Top

Admin

Physical Config Desktop Programming Attributes

Command Prompt

```
Reply from 192.168.40.1: bytes=32 time<1ms TTL=255
Reply from 192.168.40.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.99.1

Pinging 192.168.99.1 with 32 bytes of data:

Reply from 192.168.99.1: bytes=32 time<1ms TTL=255
Reply from 192.168.99.1: bytes=32 time=1ms TTL=255
Reply from 192.168.99.1: bytes=32 time<1ms TTL=255
Reply from 192.168.99.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.99.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ssh -l admin 192.168.10.1
Password:

R1#
R1#
R1#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/25 ms

R1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/10/17 ms

R1#
```

New Delete

Connection Type

Toggle PDU List Window

Search

## 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.