Document de Synthèse : TP1 – Skills Integration Challenge

I. Documentation Initiale

Cette section récapitule les informations clés issues de l'activité Packet Tracer – Skills Integration Challenge, utilisées pour la configuration des périphériques **HQ** et **HQ-Sw.**

1 Topologie du Réseau

La topologie du réseau est centrée autour du routeur **HQ** (Headquarters) assurant le routage inter-VLAN et la connexion vers l'Internet, et du commutateur **HQ-Sw** fournissant l'accès aux segments LAN internes (Serveurs, PCs, Management). D'autres routeurs (**B1**, **B2**) sont connectés, et la connectivité pour les PCs internes (dont **Staff**) est assurée par DHCP.

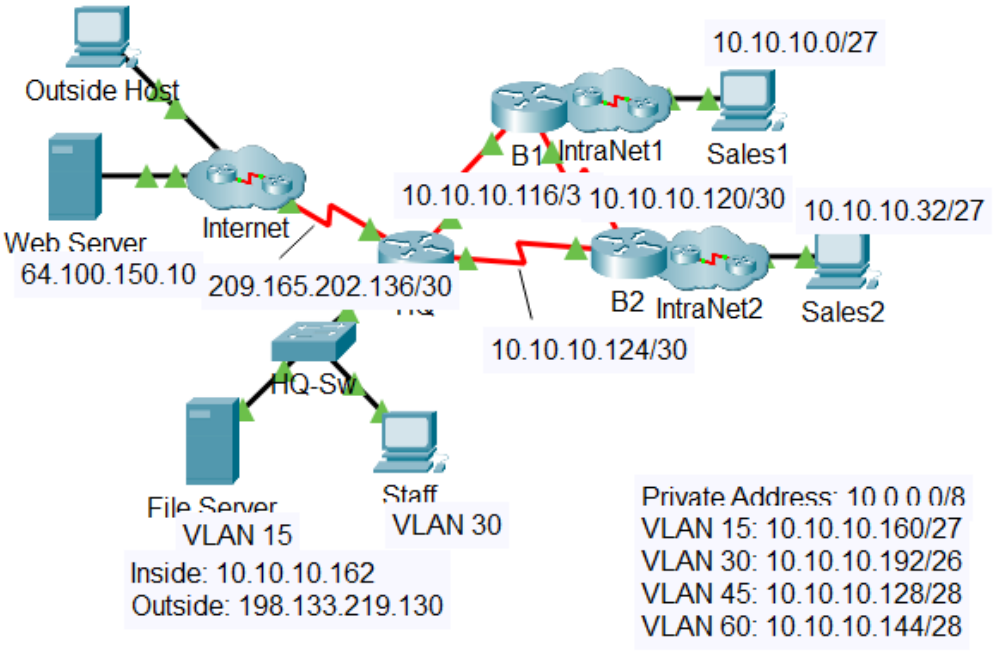

Figure 1 : Topologie du réseau

2 Tableau d'Adressage Complet

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/0.15	10.10.10.161	255.255.255.224	N/A
	G0/0.30	10.10.10.193	255.255.255.192	N/A
	G0/0.45	10.10.10.129	255.255.255.240	N/A
	G0/0.60	10.10.10.145	255.255.255.240	N/A
	S0/0/0	10.10.10.117	255.255.255.252	N/A
	S0/0/1	10.10.10.126	255.255.255.252	N/A
	S0/1/0	209.165.202.138	255.255.255.252	N/A
B1	G0/0	10.10.10.1	255.255.255.224	N/A
	S0/0/0	10.10.10.121	255.255.255.252	N/A
	S0/0/1	10.10.10.118	255.255.255.252	N/A
B2	G0/0	10.10.10.33	255.255.255.224	N/A
	S0/0/0	10.10.10.125	255.255.255.252	N/A
	S0/0/1	10.10.10.122	255.255.255.252	N/A
HQ-Sw	VLAN 60	10.10.10.146	255.255.255.240	10.10.10.145
Staff	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned

3 Tableau des VLANs et Affectations de Ports

Ce tableau définit les VLANs à configurer sur **HQ-Sw** et l'adressage de leurs réseaux respectifs.

VLAN Number - Name	Port assignment	Network
15 - Servers	F0/11 - F0/20	10.10.10.160/27
30 - PCs	F0/1 - F0/10	10.10.10.192/26
45 - Native	G0/1	10.10.10.128/28
60 - Management	VLAN 60	10.10.10.144/28

II. Implémentation des Configurations (HQ-Sw)

1. Configuration des VLANs et Trunking

Cette section détaille les étapes de configuration du commutateur **HQ-Sw**, y compris la gestion des VLANs, le *trunking*, l'accès SSH, et la sécurité des ports.

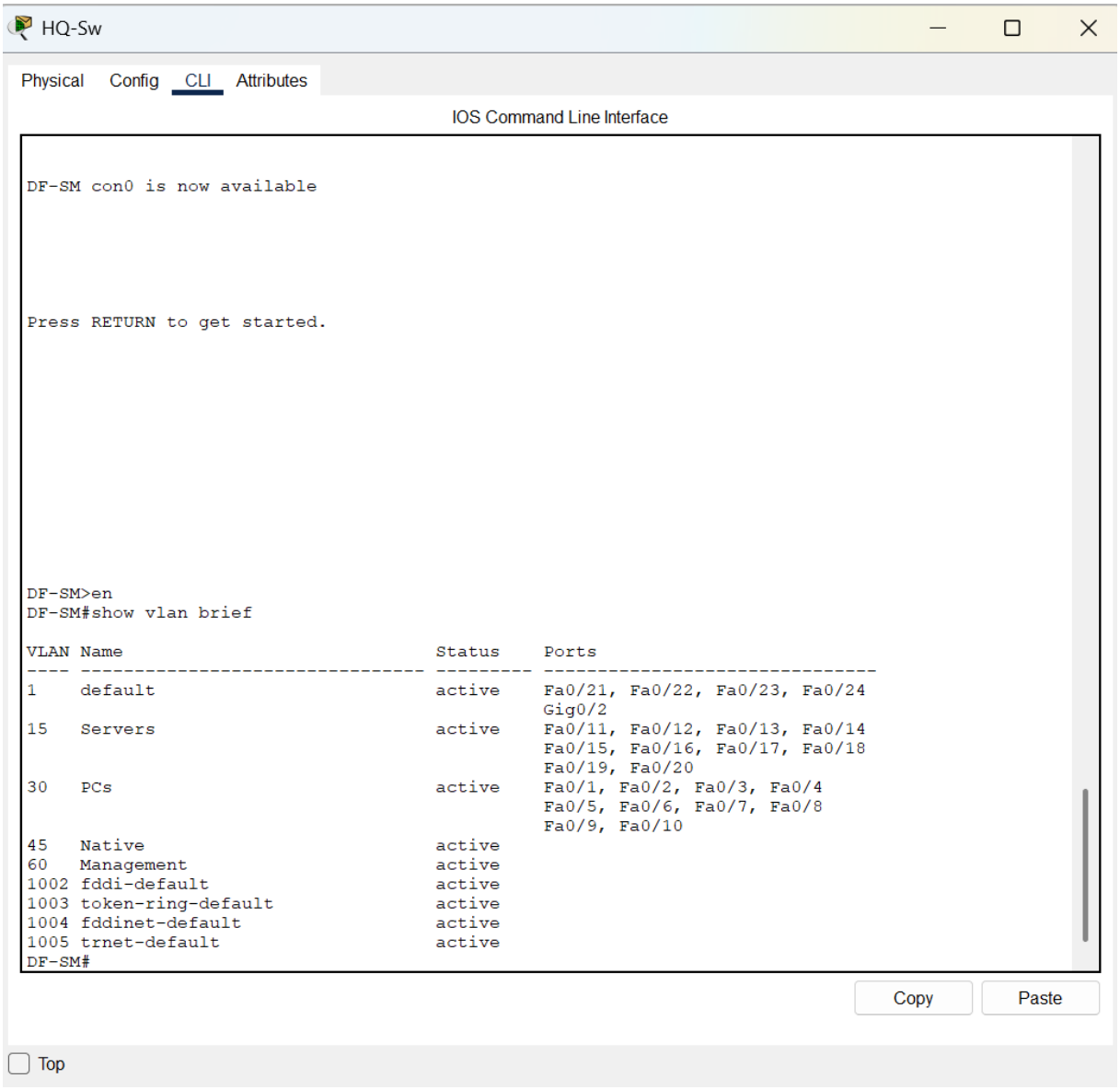

Figure 2 : Création des VLANs et noms

```
DF-SM#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      45

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,15,30,45,60

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,15,30,45,60
```

Figure 3 : Configuration du Trunk

2. Configuration de l'Accès SSH

L'accès à la gestion à distance est sécurisé par SSH version 2, avec un utilisateur local et un chiffrement des mots de passe.

```
DF-SM#show running-config
Building configuration...

Current configuration : 2714 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname DF-SM
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 60
ip domain-name cisco.com
!
username Admin privilege 1 password 7 082D495A041C0C19
```

Figure 4 : Configuration ssh et utilisateur

```
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
```

Figure 5 : Configuration vty pour accéder à ssh

3. Implémentation de la Sécurité des Ports

La sécurité des ports est appliquée à l'interface F0/1 et tous les ports non utilisés sont désactivés pour des raisons de sécurité.

```
DF-SM#show port-security interface F0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.C90E.8923:30
Security Violation Count   : 0
```

Figure 6 : Configuration des ports de sécurités

```
DF-SM#show interface status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    30         auto    auto  10/100BaseTX
Fa0/2                        notconnect   30         auto    auto  10/100BaseTX
Fa0/3                        notconnect   30         auto    auto  10/100BaseTX
Fa0/4                        notconnect   30         auto    auto  10/100BaseTX
Fa0/5                        notconnect   30         auto    auto  10/100BaseTX
Fa0/6                        notconnect   30         auto    auto  10/100BaseTX
Fa0/7                        notconnect   30         auto    auto  10/100BaseTX
Fa0/8                        notconnect   30         auto    auto  10/100BaseTX
Fa0/9                        notconnect   30         auto    auto  10/100BaseTX
Fa0/10                       notconnect   30         auto    auto  10/100BaseTX
Fa0/11                       connected    15         auto    auto  10/100BaseTX
Fa0/12                       notconnect   15         auto    auto  10/100BaseTX
Fa0/13                       notconnect   15         auto    auto  10/100BaseTX
Fa0/14                       notconnect   15         auto    auto  10/100BaseTX
Fa0/15                       notconnect   15         auto    auto  10/100BaseTX
Fa0/16                       notconnect   15         auto    auto  10/100BaseTX
Fa0/17                       notconnect   15         auto    auto  10/100BaseTX
Fa0/18                       notconnect   15         auto    auto  10/100BaseTX
Fa0/19                       notconnect   15         auto    auto  10/100BaseTX
Fa0/20                       notconnect   15         auto    auto  10/100BaseTX
Fa0/21                       disabled 1          auto    auto  10/100BaseTX
Fa0/22                       disabled 1          auto    auto  10/100BaseTX
Fa0/23                       disabled 1          auto    auto  10/100BaseTX
Fa0/24                       disabled 1          auto    auto  10/100BaseTX
Gig0/1                       connected    trunk      auto    auto  10/100BaseTX
Gig0/2                       disabled 1          auto    auto  10/100BaseTX
```

Figure 7 : Etat des interfaces

III. Implémentation des Configurations (HQ Router)

Cette section documente les configurations du routeur **HQ**, y compris le routage inter-VLAN, les services DHCP, le routage **RIPv2** et l'implémentation de la **NAT** (Statique et Dynamique/PAT).

1 Routage Inter-VLAN (Router-on-a-Stick)

Les sous-interfaces ont été créées sur l'interface physique G0/0 pour gérer le trafic des différents VLANs, en utilisant l'encapsulation dot1Q et les adresses IP définies dans la documentation. L'interface G0/0.45 est configurée comme native.

```
DF-SM#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.15  10.10.10.161    YES manual up                    up
GigabitEthernet0/0.30  10.10.10.193    YES manual up                    up
GigabitEthernet0/0.45  10.10.10.129    YES manual up                    up
GigabitEthernet0/0.60  10.10.10.145    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            10.10.10.117    YES manual up                    up
Serial0/0/1            10.10.10.126    YES manual up                    up
Serial0/1/0            209.165.202.138 YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Figure 8 : Etat des sous-interfaces avec leurs adresses ip

2 Configuration DHCP (VLAN 30)

Le service DHCP est configuré pour le VLAN 30 (PCs) sous le nom de pool **LAN** (sensible à la casse), avec exclusion de l'adresse de la passerelle.

```
DF-SM#show running-config
Building configuration...

Current configuration : 1917 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname DF-SM
!
!
!
!
ip dhcp excluded-address 10.10.10.193
!
ip dhcp pool LAN
 network 10.10.10.192 255.255.255.192
 default-router 10.10.10.193
!
```

Figure 9 : Configuration DHCP

3 Routage RIPv2 et Route par Défaut

Le protocole de routage **RIP version 2** est activé, et une seule instruction réseau est utilisée pour l'espace 10.0.0.0/8. Une route statique par défaut est ajoutée pour la connexion Internet.

```
DF-SM#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 12 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           22
  Serial0/0/1           22
  GigabitEthernet0/0.15 22
  GigabitEthernet0/0.30 22
  GigabitEthernet0/0.45 22
  GigabitEthernet0/0.60 22
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
        10.0.0.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
        10.10.10.118         120      00:00:14
        10.10.10.125         120      00:00:21
Distance: (default is 120)
```

Figure 10 : Configuration du protocole RIP v2

```
DF-SM#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 15 subnets, 5 masks
R       10.10.10.0/27 [120/1] via 10.10.10.118, 00:00:08, Serial0/0/0
R       10.10.10.32/27 [120/1] via 10.10.10.125, 00:00:16, Serial0/0/1
C       10.10.10.116/30 is directly connected, Serial0/0/0
L       10.10.10.117/32 is directly connected, Serial0/0/0
R       10.10.10.120/30 [120/1] via 10.10.10.118, 00:00:08, Serial0/0/0
                        [120/1] via 10.10.10.125, 00:00:16, Serial0/0/1
C       10.10.10.124/30 is directly connected, Serial0/0/1
L       10.10.10.126/32 is directly connected, Serial0/0/1
C       10.10.10.128/28 is directly connected, GigabitEthernet0/0.45
L       10.10.10.129/32 is directly connected, GigabitEthernet0/0.45
C       10.10.10.144/28 is directly connected, GigabitEthernet0/0.60
L       10.10.10.145/32 is directly connected, GigabitEthernet0/0.60
C       10.10.10.160/27 is directly connected, GigabitEthernet0/0.15
L       10.10.10.161/32 is directly connected, GigabitEthernet0/0.15
C       10.10.10.192/26 is directly connected, GigabitEthernet0/0.30
L       10.10.10.193/32 is directly connected, GigabitEthernet0/0.30
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.136/30 is directly connected, Serial0/1/0
L       209.165.202.138/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

Figure 11 : Configuration de la route par défaut

4 Configuration NAT

La NAT est implémentée pour fournir une connectivité Internet aux hôtes internes.

```
ip nat pool NAT_POOL 198.133.219.128 198.133.219.129 netmask 255.255.255.252
ip nat inside source list 1 pool NAT_POOL overload
ip nat inside source static 10.10.10.162 209.165.202.137
ip nat inside source static 10.10.10.162 198.133.219.130
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
!
ip flow-export version 9
!
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
!
!
```

Figure 12 : Configuration du pool NAT

```
DF-SM#show ip nat statistics
Total translations: 2 (2 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: Serial0/0/0 , Serial0/0/1 , GigabitEthernet0/0.15 , GigabitEthernet0/0.30 ,
GigabitEthernet0/0.45 , GigabitEthernet0/0.60
Hits: 0  Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool NAT_POOL refCount 0
 pool NAT_POOL: netmask 255.255.255.252
       start 198.133.219.128 end 198.133.219.129
       type generic, total addresses 2 , allocated 0 (0%), misses 0
```

Figure 13 : Interface configurée NAT inside

IV. Vérification de l'Implémentation

Cette section confirme l'état de fonctionnement du réseau après l'application des configurations sur **HQ-Sw** et **HQ**.

1 Vérification DHCP et Connectivité de Base

L'objectif ici est de vérifier que le PC Staff a reçu son adressage complet de HQ.

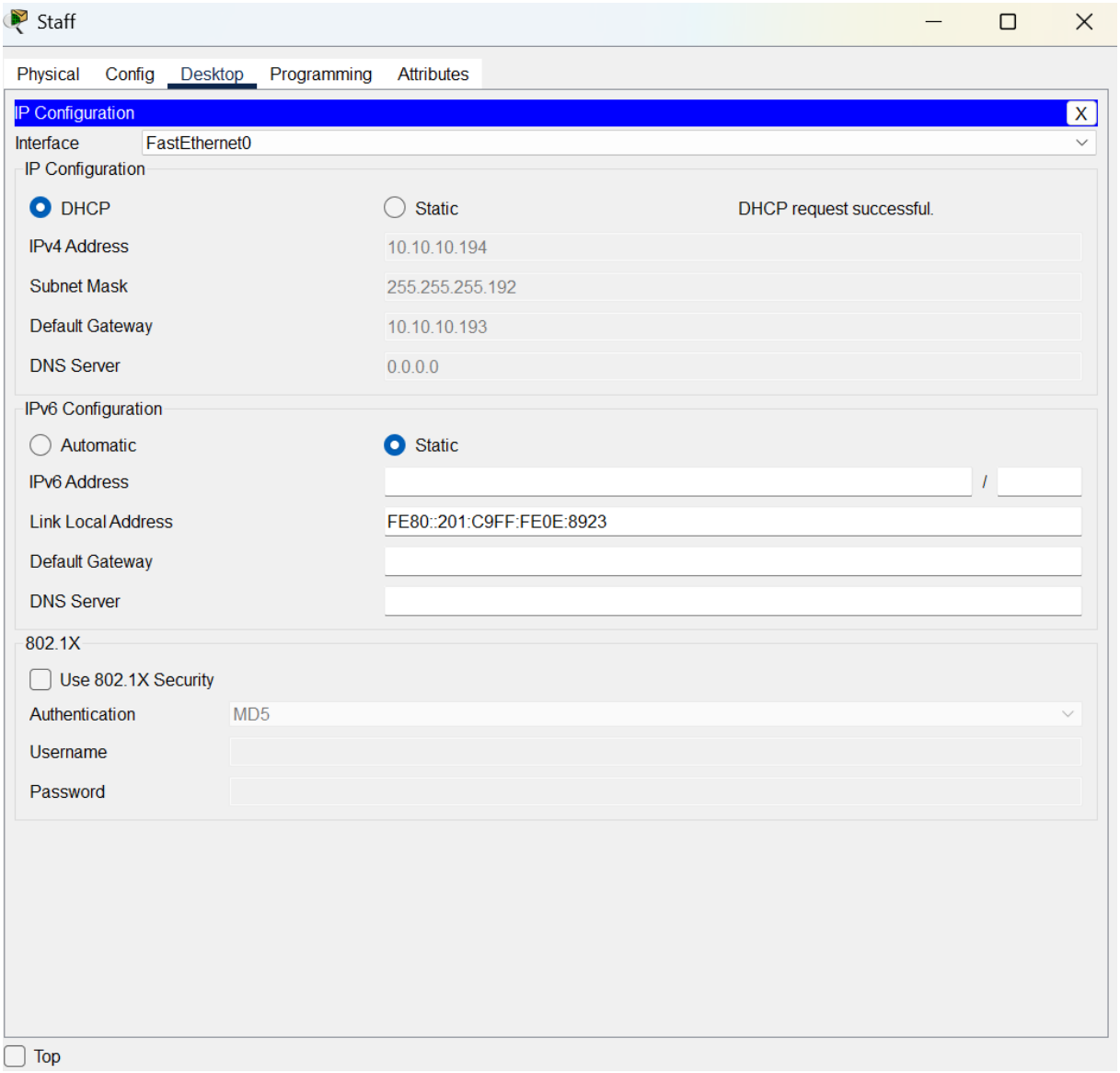

Figure 14 : Attribution d'adressage DHCP

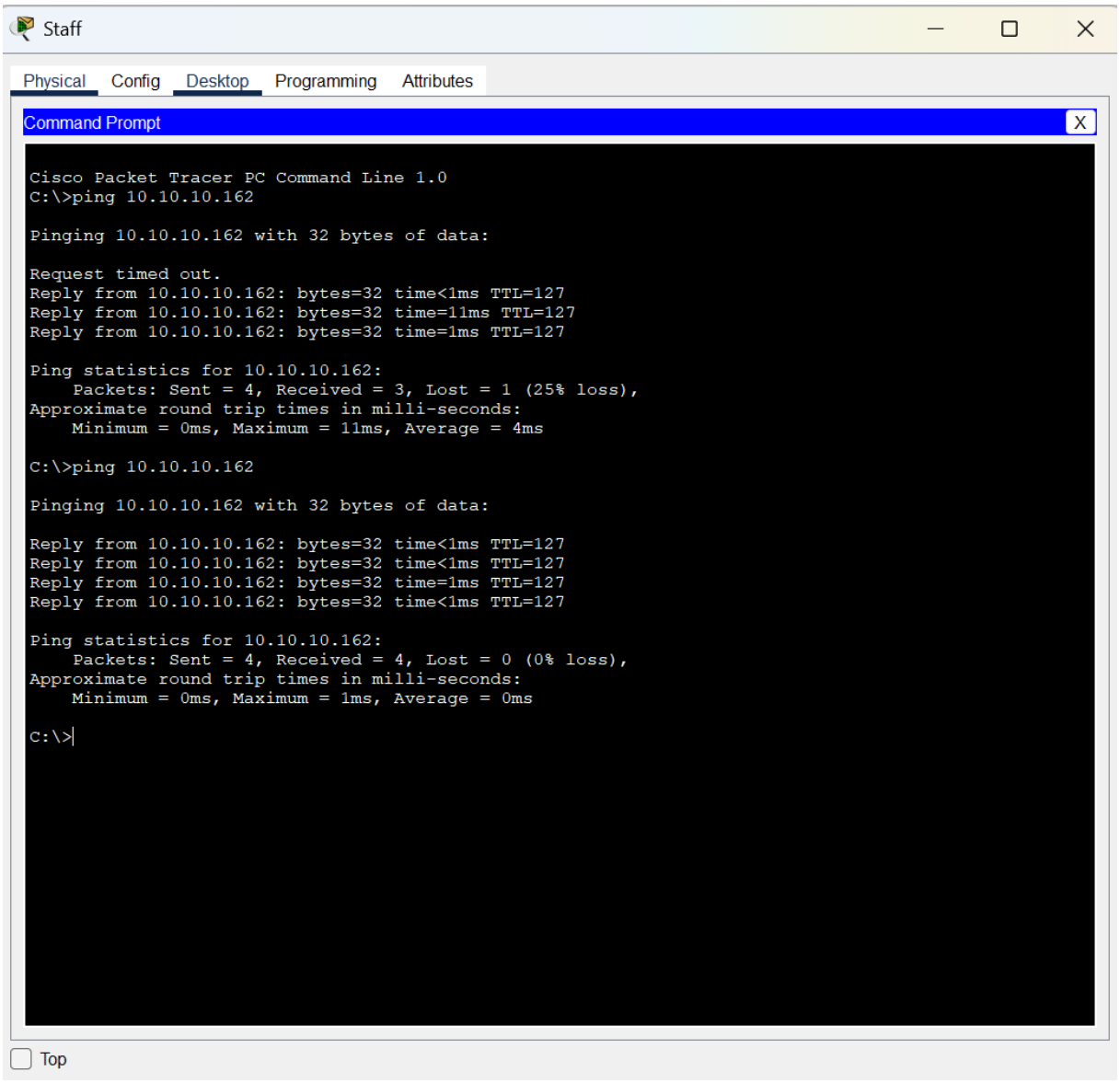

Figure 15 : Test Inter-VLAN de Pc Staff vers File Server

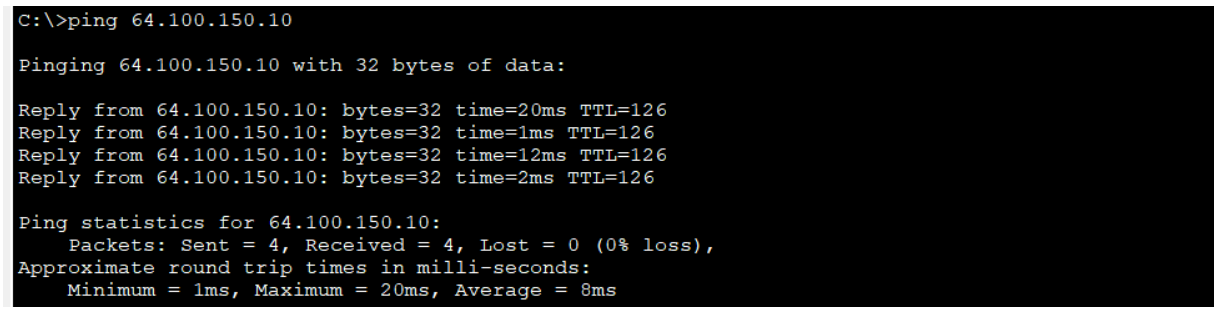

Figure 16 : Test vers l'Internet/Web Server pour vérifier le routage, le NAT et la route par défaut

2 Test des Fonctionnalités Avancées (SSH, NAT et Sécurité)

L’objectif ici es de vérifier l'accès à distance sécurisé au commutateur. Le PC **Staff** devrait pouvoir se connecter au commutateur de gestion via SSH en utilisant les identifiants configurés.

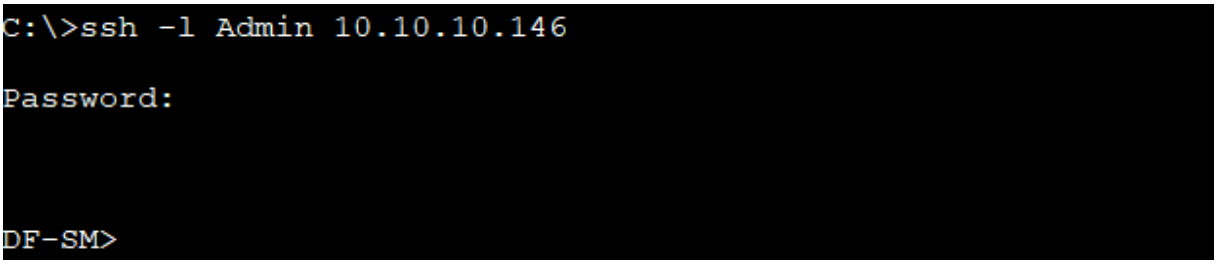

Figure 17 : Test SSH connexion depuis le Pc Staff vers le serveur HQ-Sw

Vérifions à présent les traductions NAT. Il est essentiel de confirmer que la NAT statique fonctionne pour le **File Server** et que la PAT est utilisée pour le trafic sortant des utilisateurs internes.

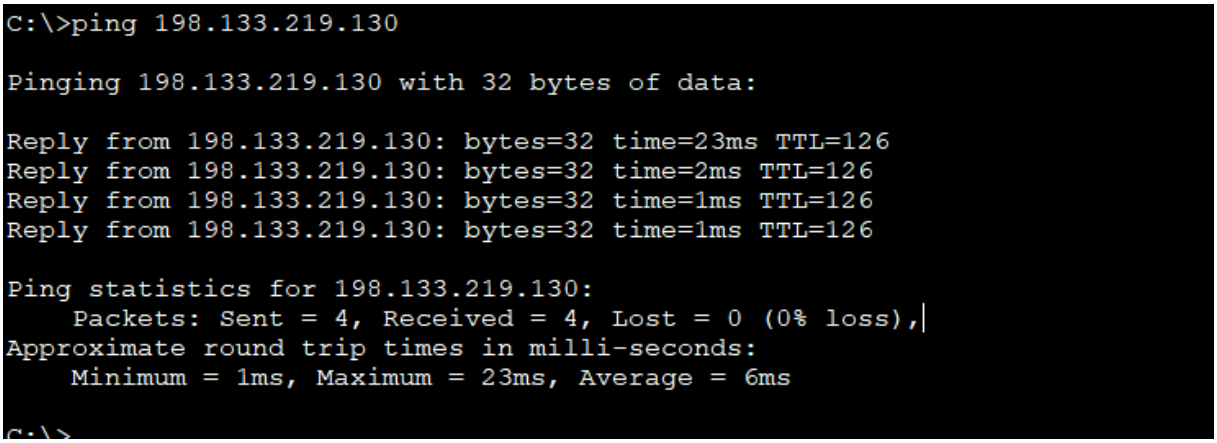

Figure 18 : Test NAT Statique réussi depuis l'Outside Host vers l'adresse publique du File Server

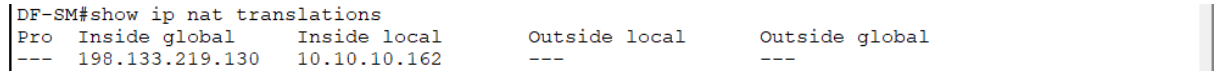

Figure 19 : Traduction des adresses Ip du File Server

V. Explication des Mots-Clés

- **NAT (Network Address Translation)**

Est un mécanisme qui permet de traduire les adresses IP privées internes en une ou plusieurs adresses IP publiques routables sur Internet. Son rôle est de conserver les adresses IPv4 publiques en permettant à de nombreux hôtes privés d'accéder au monde extérieur. Dans le cadre de notre exercice, nous avons utilisé le NAT sur le **routeur HQ** pour permettre aux

réseaux internes (**10.0.0.0/8**) d'accéder au Web et pour rendre le **File Server** accessible depuis l'extérieur.

- **Static NAT**

Le NAT Statique est une traduction un-à-un où une adresse IP privée spécifique est mappée de manière permanente à une adresse IP publique spécifique. Il a été utilisé pour le **File Server** (une ressource interne qui doit être accessible de l'extérieur) afin qu'il ait toujours la même adresse publique pour la vérification.

- **Dynamic NAT (Overloading/PAT)**

Le concept de **Surcharge** (ou **PAT** - Port Address Translation) est une forme de NAT dynamique qui permet à plusieurs adresses privées de partager une seule adresse IP publique en utilisant des numéros de port différents pour chaque session. C'est l'économie maximale d'adresses IPv4. Le NAT **Dynamique avec PAT** traduit les adresses privées en utilisant un pool d'adresses publiques disponibles (**198.133.219.128-129**) avec surcharge.

- **SSH (Secure Shell)**

Est un protocole réseau crypté utilisé pour l'accès sécurisé aux dispositifs réseau à distance. Son rôle est de remplacer des protocoles non sécurisés comme Telnet. On l'a configuré sur le **commutateur HQ-Sw** pour sécuriser l'accès de gestion à distance (**VLAN 60**) via les lignes VTY.

- **ACL (Access Control List)**

Est une liste de règles (instructions permit ou deny) utilisées pour filtrer le trafic ou identifier des paquets. Elle a été utilisée ici pour identifier l'ensemble des adresses privées (**10.0.0.0/8**) autorisées à utiliser les services NAT dynamique (PAT) pour sortir sur Internet.

- **Trunking**

Est un mode de liaison entre un switch et un autre switch ou un routeur (comme **HQ**) qui permet de transporter le trafic de plusieurs VLANs à travers un seul lien physique. Il a été utilisé sur le port **G0/1** du **commutateur HQ-Sw** pour se connecter au **routeur HQ**, permettant à toutes les sous-interfaces du routeur d'accéder à leurs VLANs respectifs.

- **RIPv2 (Routing Information Protocol v2)**

Est un protocole de routage dynamique de type vecteur distance, utilisé pour échanger des informations sur les chemins et les métriques entre routeurs. Il est utilisé sur le **routeur HQ** pour apprendre dynamiquement les routes vers les réseaux distants et annoncer son propre réseau 10.0.0.0/8 aux autres routeurs (**B1**, **B2**).

- **Default Route (Route par Défaut)**

Est un type de route statique qui dirige tout le trafic dont la destination n'est pas explicitement connue vers un point de sortie unique (la passerelle Internet). Elle est indispensable sur le **routeur HQ** pour que le trafic interne (comme les requêtes Web) sache comment quitter le réseau et atteindre Internet via l'interface S0/1/0.

- **DHCP (Dynamic Host Config. Protocol)**

Est un protocole réseau qui attribue automatiquement des paramètres d'adressage IP (IP, masque, passerelle, DNS) aux hôtes clients. Le **routeur HQ** est configuré comme un serveur DHCP pour le **VLAN 30** (PCs), assurant que le **PC Staff** reçoive automatiquement ses informations d'adressage.

- **Port Security**

Une fonctionnalité de switch qui restreint l'accès aux ports en limitant le nombre d'adresses MAC autorisées à se connecter, et en spécifiant l'action à prendre en cas de violation. Elle est utilisée sur le **commutateur HQ-Sw** (port **F0/1**) pour n'autoriser que **2** adresses MAC et générer un message **Syslog** en cas de violation (mode restrict).

Devoir de groupe de DEFFO FOKOU Franck Emerite et SOPPO BWAME Aline Marion