

Compte Rendu Final SAE3 Cyber03

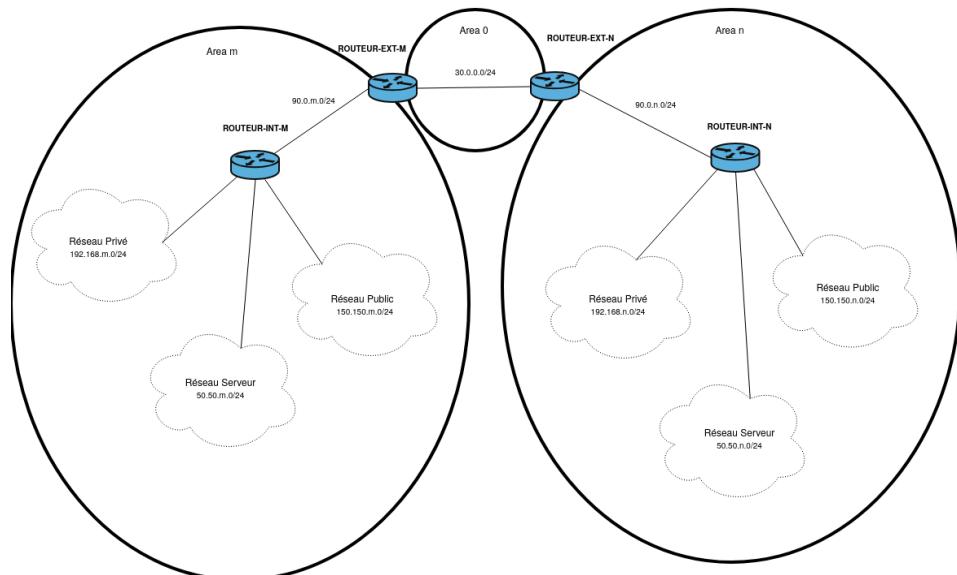
XXXXXXX | XXXXXXX | Erwann GIRAULT

Contexte

Dans ce projet, nous devons mettre en place une architecture sur deux sites d'une entreprise reliés entre eux.

Nous sommes deux groupes, XXXX et XXXX ont le numéro de poste **m = 31** et Erwann a le numéro de poste **n = 32**.

Pour réaliser l'architecture, nous nous appuyons sur le schéma logique ci-dessous.



Sommaire

1. Topologie	2
2. Configuration IP	4
3. Routage dynamique avec OSPF	14
4. Translation d'adresses (PAT)	17
5. Service web	22
6. Service DNS	24
7. Service FTP et SSH	30
8. Service RADIUS	33
9. Service Video	38
10. Filtrage (ACL)	41
11. Qualité de Service (QoS)	44
12. Cahier de recettes	48
13. Conclusion	59
14. Annexes	61

I : Topologie

1. Analyse du Cahier des Charges

Le projet impose le déploiement d'une architecture réseau sur le site 31, interconnectée à un site distant via une liaison WAN. L'infrastructure doit supporter trois réseaux distincts :

- Réseau Serveurs Publics : Zone critique hébergeant les services (S31)
- Réseau Clients Publics : Zone à forte densité (jusqu'à 253 hôtes)
- Réseau Clients Privés : Zone interne sécurisée (jusqu'à 128 hôtes)

La topologie exige l'utilisation de deux routeurs par site pour assurer la hiérarchie du routage OSPF.

2. Justification des Choix Techniques

2.1. Choix des Équipements de Routage

Conformément aux contraintes matérielles et logiques :

Routeur Externe (ISR 4331) : Nous utilisons ce routeur car il dispose des interfaces séries déjà reliées pour la liaison WAN avec le fournisseur d'accès. Il agit comme routeur de bordures.

Routeur interne (Cisco 26xx) : Ce routeur assure la distribution interne. Il fait le lien entre les réseaux locaux (LAN) et le routeur de bordures. L'utilisation de deux routeurs distincts permet de séparer clairement la zone du LAN (Area 31) de la zone de backbone (Area 0).

2.2. Topologie de Commutation et Sécurité

Nous avons opté pour une séparation physique à l'aide de deux switch distincts :

- **Switch-Public-31** : Ce switch est dédié exclusivement au **Réseau Public**.
- **Switch-Prive-31** : Ce switch gère le **Réseau Privé** et le **Réseau Serveurs**.

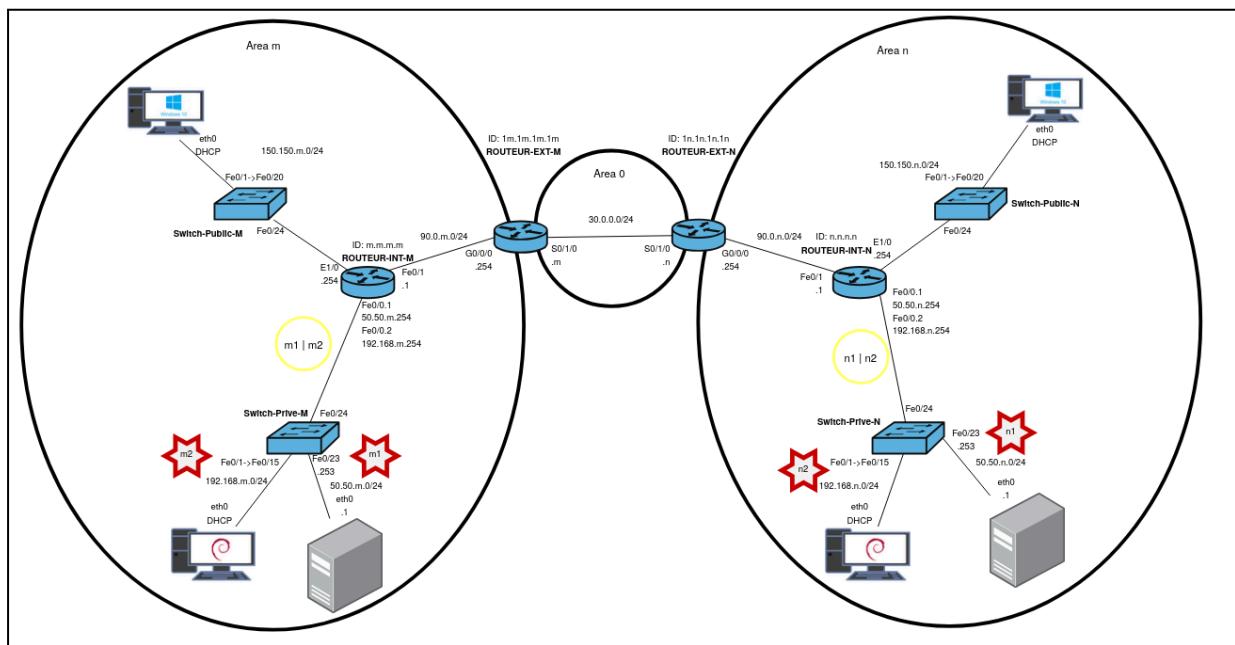
Raisonnement : Cette séparation physique vise à réduire la surface d'attaque potentielle. Le réseau public, identifié comme un vecteur de menace (car moins contrôlé), est ainsi physiquement isolé des infrastructures critiques. Si nous avions utilisé un seul switch pour tous les réseaux, une compromission de celui-ci aurait pu permettre à un attaquant d'intercepter le trafic serveur via des attaques comme le VLAN Hopping ou l'ARP Spoofing. Ici, même en cas de compromission du **Switch-Public-31**, l'attaquant n'a aucun lien physique direct avec les interfaces du serveur ou des clients privés. Le trafic doit obligatoirement remonter au routeur où des ACLs peuvent le filtrer.

3. Schéma Logique et Câblage

L'architecture finale respecte le schéma de câblage suivant :

- Le **Routeur-Ext-31** est connecté au WAN via son interface Série et au Routeur Interne via GigabitEthernet0/0/0.
- Le **Routeur-Int-31** dessert les deux switchs.
 - Lien vers **Switch-Public-31** : Interface physique dédiée **Ethernet1/0**.
 - Lien vers **Switch-Prive-31** : Interface physique **FastEthernet0/0** avec des VLANs pour les 2 réseaux desservis.
 - Il est également connecté au lien inter-routeur via l'interface physique **FastEthernet0/1**.

La configuration des services délégués par le routeur sera principalement sur le routeur interne afin d'éviter d'étaler nos configurations sensibles sur un routeur directement connecté au WAN. Cependant, centraliser les configurations sur un même routeur peut être risqué. Imaginons que ce routeur n'est pas en état de marche, tous les accès seront bloqués.



Justification des Systèmes d'Exploitation

Serveurs et Clients Privés (Linux Debian) :

Nous avons choisi Linux car la majorité des services requis sont pré-installés dans l'environnement de l'IUT, facilitant le déploiement. De plus, on supposera que les utilisateurs internes sont formés ou expérimentés.

Clients Publics (Windows 10) :

L'utilisation de Windows est liée au fait suivant : la grande majorité de la population étant familière avec cet OS, cela garantit une prise en main immédiate pour tout utilisateur externe, quel que soit son profil technique.

II : Configuration IP

1. Analyse et Stratégie d'Adressage

L'architecture réseau du site 31 est un miroir du site 32 donc chaque adresse IP en **31** est identique en **32**.

L'architecture du site 31 repose sur un plan d'adressage imposé par le cahier des charges. Ce plan doit supporter trois réseaux distincts et l'interconnexion WAN.

- **Réseau Serveurs Publics** : 50.50.31.0/24 (VLAN 311)
- **Réseau Clients Privés** : 192.168.31.0/24 (VLAN 312)
- **Réseau Clients Publics** : 150.150.31.0/24
- **Réseau Inter-Routeurs** : 90.0.31.0/24
- **Réseau WAN (FAI)** : 30.0.0.31/24

Logique d'adressage : Pour faciliter la maintenance et la configuration, nous appliquons la règle suivante :

- Les passerelles des réseaux locaux prennent la dernière adresse disponible (.254).
- Sur les liens inter-routeurs, l'adresse la plus basse est affectée à l'équipement le plus bas topologiquement (Routeur Interne = .1, Routeur Externe = .254).

2. Configuration du Routeur Interne (Routeur-Int-31)

Rôle : Ce routeur agit comme passerelle par défaut pour les trois réseaux locaux et assure le routage vers le routeur externe.

La configuration du routeur interne repose sur l'utilisation de sous-interfaces pour prendre en charge les VLAN associés aux différents réseaux. Ainsi, les interfaces **FastEthernet0/0.1** et **FastEthernet0/0.2** correspondent respectivement aux réseaux **services publics** et **clients privés**, tandis que l'interface physique **Ethernet1/0** est dédiée au réseau **clients publics**. L'interface **FastEthernet0/1** assure quant à elle le lien direct vers le réseau du routeur externe.

Remarque : Étant donné que nous utilisons les 3 interfaces des routeurs, si nous avons besoin d'une autre interface pour, par exemple, un autre réseau, nous sommes obligés soit de configurer une sous-interface dédiée et de faire la configuration liée sur le switch derrière l'interface (quel que soit le switch), soit de rajouter physiquement une interface au routeur.

La configuration IP complète du routeur interne est la suivante :

```
Router# configure terminal
Router(config)# hostname Routeur-Int-31
Routeur-Int-31(config)# ip routing

Routeur-Int-31(config)# interface FastEthernet0/1
```

```

Routeur-Int-31(config-if)# ip address 90.0.31.1 255.255.255.0
Routeur-Int-31(config-if)# no shutdown
Routeur-Int-31(config-if)# exit

Routeur-Int-31(config)# interface Ethernet1/0
Routeur-Int-31(config-if)# ip address 150.150.31.254 255.255.255.0
Routeur-Int-31(config-if)# no shutdown
Routeur-Int-31(config-if)# exit

Routeur-Int-31(config)# interface FastEthernet0/0
Routeur-Int-31(config-if)# no shutdown
Routeur-Int-31(config-if)# exit

Routeur-Int-31(config)# interface FastEthernet0/0.1
Routeur-Int-31(config-subif)# encapsulation dot1Q 311
Routeur-Int-31(config-subif)# ip address 50.50.31.254 255.255.255.0
Routeur-Int-31(config-subif)# no shutdown
Routeur-Int-31(config-subif)# exit

Routeur-Int-31(config)# interface FastEthernet0/0.2
Routeur-Int-31(config-subif)# encapsulation dot1Q 312
Routeur-Int-31(config-subif)# ip address 192.168.31.254
255.255.255.0
Routeur-Int-31(config-subif)# no shutdown
Routeur-Int-31(config-subif)# exit

```

3. Configuration du Routeur Externe (Routeur-Ext-31 / ISR)

Rôle : Routeur de bordure assurant la connexion au WAN.

Analyse des contraintes : Conformément au cahier des charges, l'interface `Serial0/1/0` se connecte au réseau du FAI (`30.0.0.0/24`). L'adresse IP se termine par le numéro de site (**31**) pour respecter l'adressage du réseau WAN. L'interface GigabitEthernet fait le lien avec le routeur interne.

La configuration IP du routeur externe est la suivante :

```

Router# configure terminal
Router(config)# hostname Routeur-Ext-31
Routeur-Ext-31(config)# ip routing

Routeur-Ext-31(config)# interface Serial0/1/0
Routeur-Ext-31(config-if)# ip address 30.0.0.31 255.255.255.0
Routeur-Ext-31(config-if)# no shutdown
Routeur-Ext-31(config-if)# exit

```

```
Routeur-Ext-31(config)# interface GigabitEthernet0/0/0
Routeur-Ext-31(config-if)# ip address 90.0.31.254 255.255.255.0
Routeur-Ext-31(config-if)# no shutdown
Routeur-Ext-31(config-if)# exit
```

Remarque :

Afin de faciliter le débogage et la configuration de ces routeurs, nous implémentons le service telnet sur ces 2 routeurs via les commandes suivantes.

Routeur externe :

```
Routeur-Ext-31(config)# enable secret lannion
! Définit un mdp pour le mode admin, absent de ce routeur dans la
configuration par défaut

Routeur-Ext-31(config)# line vty 0 4
Routeur-Ext-31(config-line)# password lannion
Routeur-Ext-31(config-line)# login
Routeur-Ext-31(config-line)# exit
```

Routeur interne :

```
Routeur-Ext-31(config)# enable secret lannion
Routeur-Int-31(config)# line vty 0 4
Routeur-Int-31(config-line)# password lannion
Routeur-Int-31(config-line)# login
Routeur-Int-31(config-line)# exit
```

4. Configuration des switchs privé et public

Rôle : Le switch privé doit héberger à la fois les clients privés et le serveur, nécessitant une séparation logique par VLANs pour éviter que les clients n'accèdent au trafic serveur sans passer par le filtrage du routeur et pour avoir 2 réseaux séparés conformément au cahier des charges. Le Switch-Public-31 est dédié exclusivement à la gestion du Réseau Clients Publics (150.150.31.0/24).

VLANs : Nous définissons les VLANs **311** (SERVEUR) et **312** (PRIVE). L'utilisation d'IDs propres au site 31 facilite la gestion des VLAN.

Sécurité des ports :

- Sur le Switch Public, nous limitons l'usage aux ports 1-20 et désactivons le reste.
- Sur le Switch Privé, nous utiliserons les ports 1-15 pour le réseau privé. Le port 23 sera uniquement dédié au serveur et le port 24 pour le lien inter vlan avec le routeur. Nous désaktivons tous les ports non utilisés (16-22).

Remarque : L'interface **Fa0/24** vers le routeur est configurée en mode **Trunk**. Cela permettra de faire remonter le trafic des deux VLANs (311 et 312) vers le routeur interne, qui

assurera ensuite le routage inter-VLAN et le filtrage. Nous choisissons de désactiver une partie des ports pour garder un matelas de sécurité au cas de besoin de ports supplémentaires.

La configuration du switch public est la suivante :

```
Switch# configure terminal
Switch(config)# hostname Switch-Public-31
Switch-Public-31(config)# interface range FastEthernet0/21 - 23
Switch-Public-31(config-if-range)# shutdown
Switch-Public-31(config-if-range)# exit
```

La configuration du switch privé est la suivante :

```
Switch# configure terminal
Switch(config)# hostname Switch-Prive-31

Switch-Prive-31(config)# vlan 311
Switch-Prive-31(config-vlan)# name SERVEUR
Switch-Prive-31(config-vlan)# exit
Switch-Prive-31(config)# vlan 312
Switch-Prive-31(config-vlan)# name PRIVE
Switch-Prive-31(config-vlan)# exit

Switch-Prive-31(config)# interface FastEthernet0/24
Switch-Prive-31(config-if)# switchport mode trunk
Switch-Prive-31(config-if)# exit

Switch-Prive-31(config)# interface range FastEthernet0/1 - 15
Switch-Prive-31(config-if-range)# switchport mode access
Switch-Prive-31(config-if-range)# switchport access vlan 312
Switch-Prive-31(config-if-range)# exit

Switch-Prive-31(config)# interface FastEthernet0/23
Switch-Prive-31(config-if)# switchport mode access
Switch-Prive-31(config-if)# switchport access vlan 311
Switch-Prive-31(config-if)# exit

Switch-Prive-31(config)# interface range FastEthernet0/16 - 22
Switch-Prive-31(config-if-range)# shutdown
Switch-Prive-31(config-if-range)# exit
```

5. Configuration des machines

Une fois l'infrastructure active, nous devons configurer les ordinateurs :

- **Serveur (S31)** : Il héberge des services critiques (DHCP, Web, RADIUS, etc). Il nécessite une adresse IP statique pour être joignable de manière fiable et permanente en théorie par les clients et les routeurs.
- **Clients (G31, D31)** : Pour faciliter la gestion, ils obtiendront leur configuration dynamiquement via DHCP. Cependant, pour les premiers tests de connectivité (avant activation du service DHCP), une configuration statique temporaire peut être utilisée.

La machine S31 est située dans le VLAN 311. Nous lui attribuons la première adresse de sa plage.

- Adresse IP : **50.50.31.1/24**
- Passerelle par défaut : **50.50.31.254** (Interface du Routeur Interne)

Le serveur S31 est déployé sous Linux donc sa configuration est la suivante

Comme seule une interface du réseau est nécessaire, nous désaktivons **eth1** et **eth2**, puis configurons **eth0** avec une adresse statique.

```
root@S31~# ip a flush dev eth0
root@S31~# ip a flush dev eth1
root@S31~# ip a flush dev eth2
root@S31~# ip link set down eth1
root@S31~# ip link set down eth2

# Adresse statique sur eth0
root@S31~# ip a add 50.50.31.1/24 dev eth0
root@S31~# ip link set up dev eth0
# Route par défaut
root@S31~# ip route add default via 50.50.31.254
```

6. Tests et Validation avec des adresses statiques

Avant de passer au routage dynamique (avec OSPF) ou aux services, nous devons valider que le **Routage Inter-VLAN** fonctionne au sein du site 31. Le routeur interne doit permettre à S31 de communiquer avec sa passerelle.

Test Effectué : Ping depuis le serveur vers sa passerelle

- **Commande :** **ping 50.50.31.254** (IP du Routeur-Int-31 dans le VLAN 311)
- **Résultat Attendu :** Succès.
- **Analyse :** Ce test valide trois points :
 1. La configuration IP du serveur est correcte.
 2. Le Trunk entre le Switch Privé et le Routeur fonctionne (VLAN 311 transporté).
 3. L'encapsulation **dot1Q** sur la sous-interface **Fa0/0.1** du routeur est validée

```

root@S29:~# ping 50.50.31.254 -c 3
PING 50.50.31.254 (50.50.31.254) 56(84) bytes of data.
64 bytes from 50.50.31.254: icmp_seq=1 ttl=255 time=1.28 ms
64 bytes from 50.50.31.254: icmp_seq=2 ttl=255 time=1.38 ms
64 bytes from 50.50.31.254: icmp_seq=3 ttl=255 time=1.28 ms

--- 50.50.31.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.276/1.312/1.382/0.049 ms

```

Remarque : Nous avons changé de paillasse donc certains screenshots sont sous les numéros de poste 30 et 29. Correspondant respectivement au site 31 et 32.

En complément des pings, nous devons vérifier la bonne prise des configuration sur nos équipements.

Test Effectué : Vérification des VLAN sur le switch

```
Switch-Prive-31#sh vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Gi0/1 Gi0/2
2 radius	active	
5 server	active	
19 user	active	
26 VLAN0026	active	
36 VLAN0036	active	
50 vlan-50	active	
126 VLAN0126	active	
150 vlan-150	active	
192 vlan-192	active	
311 SERVEUR	active	Fa0/23
312 PRIVE	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Nous avons bien nos VLANs, le VLAN SERVEUR avec uniquement l'interface Fa0/23 qui correspond à l'interface connecté au serveur et le VLAN PRIVE avec les ports dédiés au réseau privé.

Test Effectué : Vérification des interfaces sur le routeur

```
Router-Int-31#sh ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	up	up
FastEthernet0/0.1	50.50.31.254	YES	manual	up	up
FastEthernet0/0.2	192.168.31.254	YES	manual	up	up
FastEthernet0/1	90.0.31.1	YES	manual	up	up
Ethernet1/0	150.150.31.254	YES	manual	up	up

Nous avons bien nos interfaces configuré avec 2 sous interface pour le lien inter-vlan.

7. Configuration du DHCP

1. Analyse

Le service DHCP a pour rôle d'automatiser l'attribution des paramètres IP (Adresse, Masque, Passerelle, DNS) aux clients. Dans notre architecture, le serveur DHCP (S31) est situé dans le VLAN 311 (**50.50.31.0/24**), mais il doit desservir deux autres réseaux distants :

1. **Réseau Clients Publics** : **150.150.31.0/24**.
2. **Réseau Clients Privés** : **192.168.31.0/24**.

Le cahier des charges nous impose de réaliser un adressage dynamique sur le réseau des clients publics. Cependant, afin de simplifier le travail de l'administrateur réseau, nous configurons aussi le DHCP sur le réseau privé avec une attention particulière à l'accessibilité réseau des machines du ce réseau.

2. Justification de la Configuration

Rappel : le fichier `/etc/dhcp/dhcpd.conf` permet de configurer le service DHCP via la déclaration de réseaux et des options qu'on leur associe. La commande pour démarrer ce service est `systemctl start isc-dhcp-server`.

La configuration du fichier `/etc/dhcp/dhcpd.conf` a besoin de trois déclarations de sous-réseaux :

- **Le Réseau Serveur (50.50.31.0)** : Bien qu'aucune adresse dynamique ne soit distribuée ici (déclaration vide), cette entrée est obligatoire. Le service refusera de démarrer si le sous-réseau de l'interface d'écoute (`eth0`) n'est pas déclaré.
- **Le Réseau Public (150.150.31.0)** : Nous allouons la quasi-totalité de la plage (.1 à .253) pour maximiser la capacité d'accueil (253 hôtes).
- **Le Réseau Privé (192.168.31.0)** : Nous appliquons une restriction liée à la sécurité. La plage dynamique est définie de .64 à .128.
 - Raisonnement : Le cahier des charges stipule que seules les machines ayant une IP < .63 ont accès aux machines publiques en face. En distribuant des adresses à partir de .64, nous nous assurons que tout client DHCP par défaut n'aura pas cet accès (cf la configuration du PAT). Il devient un privilège accordé uniquement via une configuration IP statique (entre .1 et .63).

3. Configuration Détailée du Serveur

Fichier : /etc/dhcp/dhcpd.conf

```
# Options Globales
ddns-update-style none;
option domain-name "site31.iut";
option domain-name-servers 50.50.31.1;

# Déclaration du réseau local du serveur
subnet 50.50.31.0 netmask 255.255.255.0 {
}

# Déclaration du réseau Clients Publics
subnet 150.150.31.0 netmask 255.255.255.0 {
    range dynamic-bootp 150.150.31.1 150.150.31.253;
    option routers 150.150.31.254;
    default-lease-time 30;
    max-lease-time 30;
}
# Déclaration du réseau Clients Privés
subnet 192.168.31.0 netmask 255.255.255.0 {
    range dynamic-bootp 192.168.31.64 192.168.31.128;
    option routers 192.168.31.254;
    default-lease-time 30;
    max-lease-time 30;
}
```

Pour des raisons que nous détaillerons plus tard, nous allons implémenter un service DNS ainsi pour cette raison, on transmet via l'option `domain-name` le nom du domaine et via `domain-name-servers` l'adresse IP du serveur DNS (S31).

4. Problématique du Routage et Relais DHCP

Le protocole DHCP repose sur le Broadcast (Message `DHCP DISCOVER` envoyé à `255.255.255.255`). Or, les routeurs ne propagent pas ces diffusions entre les réseaux. Sans intervention, les requêtes des clients (Publics et Privés) seraient bloquées par le routeur interne et n'atteindraient jamais le serveur S31.

Solution : Nous devons configurer le Routeur-Int-31 pour agir comme un Relais DHCP. Il intercepte les diffusions sur les interfaces clients et les convertit en Unicast vers l'IP du serveur (`50.50.31.1`).

Configuration du Routeur Interne : Nous appliquons la commande `ip helper-address` sur les interfaces d'arrivée des requêtes clients .

```
Routeur-Int-31(config)# interface FastEthernet0/0.2
Routeur-Int-31(config-if)# ip helper-address 50.50.31.1
```

```
Routeur-Int-31(config-if)# interface Ethernet1/0
Routeur-Int-31(config-if)# ip helper-address 50.50.31.1
```

Désormais, le routeur achemine vers S31 toute requête destinée à l'ensemble des machines du réseau (au broadcast).

5. Configuration des machines clientes

Rappel : G31 est dans le réseau clients privé et D31 est dans le réseau client public.

La machine G31 est un client DHCP sous Linux. Pour qu'elle puisse récupérer son adresse IP, il faut donc lancer la commande pour le déclarer comme client.

```
dhclient -v eth0
```

Cette commande force une nouvelle requête DHCP et affiche en détail les échanges avec S31, ce qui permet de valider facilement le fonctionnement du service.

Voici ci dessous une capture du résultat de la commande :

```
root@G29:~# dhclient -v
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/34:17:eb:99:ba:58
Sending on LPF/eth0/34:17:eb:99:ba:58
Sending on Socket/fallback
DHCPCDISCOVER on eth0 to 255.255.255.255 port 67 interval 6
DHCPOffer of 192.168.31.64 from 192.168.31.254
DHCPREQUEST for 192.168.31.64 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.31.64 from 192.168.31.254
bound to 192.168.31.64 -- renewal in 13 seconds.
```

Trame côté client :

7 10.163661543	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0xa39c1b0d
8 10.168029857	Cisco_95:ca:00	Broadcast	ARP	60 Who has 192.168.31.64? Tell 192.168.31.254
9 11.171234649	192.168.31.254	192.168.31.64	DHCP	342 DHCP Offer - Transaction ID 0xa39c1b0d
10 11.171353882	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID 0xa39c1b0d
11 11.200512255	192.168.31.254	192.168.31.64	DHCP	342 DHCP ACK - Transaction ID 0xa39c1b0d

Trame côté serveur :

6 6.416590905	192.168.31.254	50.50.31.1	DHCP	342 DHCP Discover - Transaction ID 0xa39c1b0d
7 6.416888026	50.50.31.1	192.168.31.64	ICMP	62 Echo (ping) request id=0xf2e3, seq=0/0, ttl=64 (no response found!)
8 7.418165915	50.50.31.1	192.168.31.254	DHCP	342 DHCP Offer - Transaction ID 0xa39c1b0d
9 7.424269348	192.168.31.254	50.50.31.1	DHCP	342 DHCP Request - Transaction ID 0xa39c1b0d
10 7.447944924	50.50.31.1	192.168.31.254	DHCP	342 DHCP ACK - Transaction ID 0xa39c1b0d

On observe sur les 2 trames la phase d'initialisation de la demande du client et enfin les premiers échanges ACK assurant la continuité de l'adresse IP.

Remarque : Actuellement, le service RADIUS n'est pas configuré sur le switch et le serveur donc le switch laisse passer la requête de G31 mais lorsque le service radius est actif, la machine devra d'abord s'authentifier puis pourra recevoir une adresse via DHCP.

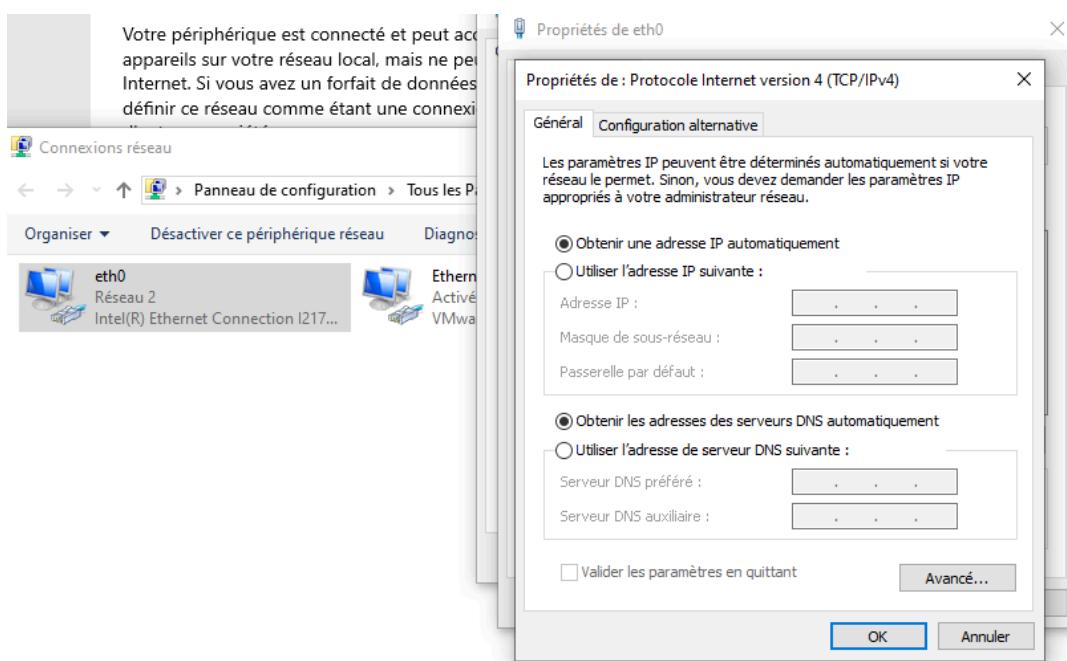
La machine D31 étant sous Windows, on fera la configuration via l'interface graphique.

Le chemin à emprunter est le suivant :

Application paramètre > Réseau et Internet > Centre Réseau et Partage dans l'onglet état > eth0 > Propriétés > Protocole Internet version 4 (TCP/IPv4)

Nous sélectionnons :

- **Obtenir une adresse IP automatiquement**
- **Obtenir les adresses des serveurs DNS automatiquement**



Une fois ceci appliqué (en sélectionnant OK), on teste avec la commande suivante dans l'invite de commande :

```
ipconfig
```

```
C:\Users\root>ipconfig
Configuration IP de Windows

Carte Ethernet eth0 :

    Suffixe DNS propre à la connexion... : site31.iut
    Adresse IPv6 de liaison locale... : fe80::3800:ab05:e590:7ec9%8
    Adresse IPv4... : 150.150.31.1
    Masque de sous-réseau... : 255.255.255.0
    Passerelle par défaut... : 150.150.31.254
```

No.	Time	Source	Destination	Protocol	Length	Info
5102	6368.269438	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x64907b9d
5378	6702.261482	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x195bb06
5383	6703.268801	150.150.31.254	150.150.31.1	DHCP	342	DHCP Offer - Transaction ID 0x195bb06
5384	6703.270584	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x195bb06
5385	6703.279975	150.150.31.254	150.150.31.1	DHCP	342	DHCP ACK - Transaction ID 0x195bb06
5535	6717.511501	150.150.31.1	50.50.31.1	DHCP	342	DHCP Request - Transaction ID 0x1f7af36a
5536	6717.516309	50.50.31.1	150.150.31.1	DHCP	342	DHCP ACK - Transaction ID 0x1f7af36a

Capture Wireshark prise depuis D31 pour observer l'attribution d'une adresse IP via DHCP.

Ainsi, la configuration DHCP est fonctionnelle : les machines Linux et Windows reçoivent bien une IP cohérente à la configuration, ainsi que les paramètres réseau fournis par le serveur S31.

III : Routage dynamique avec OSPF

1. Analyse du Cahier des Charges

Le déploiement du routage est soumis à trois contraintes :

- L'ensemble des routeurs (Interne et Externe) doit utiliser exclusivement le protocole OSPF.
- Le réseau du fournisseur d'accès (FAI) appartient à la Zone 0 (Backbone). Notre site doit impérativement se raccorder à cette zone via le routeur externe, tout en plaçant ses réseaux internes dans une zone spécifique portant le numéro du site (soit Area 31 pour nous).
- L'interconnexion se fait via le réseau **30.0.0.0/24**, où notre routeur externe porte l'adresse **30.0.0.31**.

2. Justification des Choix Techniques

Le Routeur Externe agit comme un ABR (Area Border Router), faisant le pont entre le backbone (WAN) et la zone locale. Donc nous devons séparer notre zone 31 de la zone 0 via ce routeur.

Le protocole OSPF identifie chaque routeur par un ID unique. Pour éviter que cet ID ne change si une interface physique tombe en panne ou d'évolution des interfaces physiques, nous créons des interfaces Loopback (**31.31.31.31/32** et **131.131.131.131/32**). Elles garantissent un identifiant stable à l'OSPF.

Le cahier des charges demande de ne fournir aucune information du réseau (au public mais nous l'étendons à tous les réseaux) inutilement. En configurant les interfaces LAN (vers les clients et serveurs) en passive-interface, nous empêchons le routeur d'envoyer des paquets OSPF vers les utilisateurs et le serveur. Cela permet d'inviter à un attaquant interne de cartographier la topologie ou d'injecter de fausses routes via ces accès.

3. Configuration des Routeurs

La configuration du Routeur Interne (par exemple celui du poste 31) est la suivante :
Il appartient intégralement à la Zone 31.

```
Routeur-Int-31# configure terminal

Routeur-Int-31(config)# interface loopback 31
Routeur-Int-31(config-if)# ip address 31.31.31.31 255.255.255.255
Routeur-Int-31(config-if)# no shutdown
Routeur-Int-31(config-if)# exit

Routeur-Int-31(config)# router ospf 31
Routeur-Int-31(config-router)# router-id 31.31.31.31
Routeur-Int-31(config-router)# network 50.50.31.0 0.0.0.255 area
31
Routeur-Int-31(config-router)# network 150.150.31.0 0.0.0.255 area
31
Routeur-Int-31(config-router)# network 90.0.31.0 0.0.0.255 area 31
Routeur-Int-31(config-router)# network 31.31.31.31 0.0.0.0 area 31

Routeur-Int-31(config-router)# passive-interface FastEthernet0/0
Routeur-Int-31(config-router)# passive-interface FastEthernet0/0.1
Routeur-Int-31(config-router)# passive-interface FastEthernet0/0.2
Routeur-Int-31(config-router)# passive-interface Ethernet1/0
Routeur-Int-31(config-router)# exit
```

La configuration du Routeur Externe (par exemple celui du poste 31) est la suivante :
Il assure la jonction entre la Zone 31 (LAN) et la Zone 0 (WAN).

```
Routeur-Ext-31# configure terminal

Routeur-Ext-31(config)# interface loopback 131
Routeur-Ext-31(config-if)# ip address 131.131.131.131
255.255.255.255
Routeur-Ext-31(config-if)# no shutdown
Routeur-Ext-31(config-if)# exit

Routeur-Ext-31(config)# router ospf 1
Routeur-Ext-31(config-router)# router-id 131.131.131.131
Routeur-Ext-31(config-router)# network 90.0.31.0 0.0.0.255 area
31
Routeur-Ext-31(config-router)# network 30.0.0.0 0.0.0.255 area 0
Routeur-Ext-31(config-router)# network 131.131.131.131 0.0.0.0
area 31
Routeur-Ext-31(config-router)# exit
```

4. Tests et Validation

Une fois l'ensemble des routeurs configurés, nous avons procédé à une série de vérifications permettant de confirmer le bon fonctionnement d'OSPF.

La première vérification consiste à observer la relation de voisinage OSPF entre les routeurs interne et externe. Pour cela, nous utilisons la commande :

```
Routeur-Int-31# show ip ospf neighbor
```

Cette commande permet de vérifier que chaque routeur a bien détecté son voisin et que l'état atteint est Full, ce qui signifie que la base de données OSPF est synchronisée.

Routeur Interne :

```
Routeur-Int-31#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
131.131.131.131	1	FULL/DR	00:00:34	90.0.31.254	FastEthernet0/1

Routeur Externe voisin :

```
Routeur-Ext-31#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
132.132.132.132	0	FULL/ -	00:00:32	30.0.0.32	Serial0/1/0
31.31.31.31	1	FULL/BDR	00:00:35	90.0.31.1	GigabitEthernet0/0

Nous avons ensuite consulté la table de routage pour vérifier que les routes apprises via OSPF sont bien présentes. La commande utilisée est :

```
Routeur-Int-31#show ip route ospf
```

L'apparition des routes préfixées par la lettre **O** (intra-area) ou **O IA** (inter-area) confirme que les réseaux distants sont correctement propagés et interprétés par le protocole.

Les routes **inter-area** correspondent aux routes apprises depuis une autre zone OSPF, tandis que les routes **intra-area** désignent les routes appartenant à la zone dans laquelle se situe le routeur sur lequel la commande a été effectuée. On remarque que les réseaux privés ne sont pas partagés et que le routeur externe ne connaît pas leur existence.

```

Routeur-Int-31#sh ip route
Codes: 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
      i - IS-IS, su - IS-IS summary, 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 not set

      50.0.0.0/24 is subnetted, 2 subnets
C        50.50.31.0 is directly connected, FastEthernet0/0.1
O IA    50.50.32.0 [110/53] via 90.0.31.254, 00:01:23, FastEthernet0/1
      32.0.0.0/32 is subnetted, 1 subnets
O IA    32.32.32.32 [110/53] via 90.0.31.254, 00:05:12, FastEthernet0/1
C        192.168.31.0/24 is directly connected, FastEthernet0/0.2
      131.131.0.0/32 is subnetted, 1 subnets
O        131.131.131.131 [110/2] via 90.0.31.254, 04:02:40, FastEthernet0/1
      132.132.0.0/32 is subnetted, 1 subnets
O IA    132.132.132.132 [110/52] via 90.0.31.254, 00:05:12, FastEthernet0/1
      31.0.0.0/32 is subnetted, 1 subnets
C        31.31.31.31 is directly connected, Loopback31
      90.0.0.0/24 is subnetted, 2 subnets
C        90.0.31.0 is directly connected, FastEthernet0/1
O IA    90.0.32.0 [110/52] via 90.0.31.254, 00:05:12, FastEthernet0/1
      30.0.0.0/24 is subnetted, 1 subnets
O IA    30.0.0.0 [110/51] via 90.0.31.254, 04:02:40, FastEthernet0/1
      150.150.0.0/24 is subnetted, 2 subnets
C        150.150.31.0 is directly connected, Ethernet1/0
O IA    150.150.32.0 [110/62] via 90.0.31.254, 00:05:12, FastEthernet0/1
      31.0.0.0/32 is subnetted, 1 subnets

```

Enfin, afin de valider la connectivité réelle (et pas seulement la présence des routes) nous avons réalisé plusieurs ping inter-sites. Les tests ont été effectués depuis les machines clientes G31 et D31 vers leurs équivalents du site voisin. Les réponses positives démontrent que le routage dynamique fonctionne de bout en bout et que les flux transitent bien via les deux routeurs (interne31 → externe31 → FAI → site 32).

S31 → Routeur (remise direct):

```

root@S31:~# ping 50.50.31.254
PING 50.50.31.254 (50.50.31.254) 56(84) bytes of data.
64 bytes from 50.50.31.254: icmp_seq=1 ttl=255 time=1.38 ms
^C
--- 50.50.31.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.376/1.376/1.376/0.000 ms

```

D31→ routeur (remise direct)

D31 → G31

D31 → S31

```
C:\Users\root>ping 150.150.31.254

Envoi d'une requête 'Ping' 150.150.31.254 avec 32 octets de données :
Réponse de 150.150.31.254 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 150.150.31.254:
    Paquets : envoyés = 1, reçus = 1, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
Ctrl+C
^C
C:\Users\root>ping 192.168.31.1

Envoi d'une requête 'Ping' 192.168.31.1 avec 32 octets de données :
Réponse de 150.150.31.254 : Impossible de joindre le réseau de destination.
Réponse de 150.150.31.254 : Impossible de joindre le réseau de destination.

Statistiques Ping pour 192.168.31.1:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Ctrl+C
^C
C:\Users\root>ping 50.50.31.1

Envoi d'une requête 'Ping' 50.50.31.1 avec 32 octets de données :
Réponse de 50.50.31.1 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 50.50.31.1:
    Paquets : envoyés = 1, reçus = 1, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

G31→ S31:

```
root@G31:~# ping 50.50.31.1
PING 50.50.31.1 (50.50.31.1) 56(84) bytes of data.
64 bytes from 50.50.31.1: icmp_seq=1 ttl=63 time=0.975 ms
^C
--- 50.50.31.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.975/0.975/0.975/0.000 ms
```

G31 → voisin:

```
root@G31:~# ping 90.0.32.1 -c 1
PING 90.0.32.1 (90.0.32.1) 56(84) bytes of data.
64 bytes from 90.0.32.1: icmp_seq=1 ttl=60 time=4.70 ms

--- 90.0.32.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.696/4.696/4.696/0.000 ms
```

ATTENTION : Le test précédent est bien valide car au moment du test, le PAT dynamique et le NAT statique vers le serveur S32 était déjà actif donc le routeur interne du site 32 dirigeait le paquet vers S32 qui nous répondait par la suite. Cependant, nous sommes conscients de l'erreur que nous avons fait concernant le NAT statique étant donné qu'il n'a pas lieu d'être mais ce test reste valide car derrière **90.0.31.1**, il y a bien le serveur S31 (**50.50.31.1**).

IV : Translation d'adresses (PAT)

1. Analyse du Cahier des Charges

Le déploiement doit répondre à deux contraintes :

1. **Masquage du réseau privé** : Les routeurs de bordure (ISR) ainsi que les autres réseaux publics ne doivent jamais routeur ou recevoir d'adresses privées
2. **Accès Distant (WAN)** : Seules les **63 premières machines** du réseau privé sont autorisées à communiquer avec le site distant (**150.150.32.0**).
3. **Accès Local (LAN)** : L'ensemble du réseau privé doit pouvoir communiquer avec les Serveurs (**50.50.31.0**) et le réseau Public Local (**150.150.31.0**).

2. Justification de la Solution

Pour satisfaire ces exigences, nous implémentons le mécanisme de translation suivant sur le Routeur Interne (Routeur-Int-31) :

- **PAT Dynamique** : Utilisé pour les clients privés autorisés. L'option `overload` permet de mettre plusieurs adresses privées sur l'unique adresse publique de l'interface de sortie (**FastEthernet0/1**) en jouant sur les ports sources.

Au lieu d'utiliser deux ACLs distinctes (une pour le filtrage, une pour le NAT), nous exploitons l'ACL étendue de sécurité **ACL_PRIVE_IN** pour définir le domaine de translation.

Choix de l'ACL Nommée : Pour identifier le trafic éligible au PAT, nous utilisons une ACL Standard Nommée (**ACL_PRIVE_IN**). Ce choix, par rapport aux ACLs numérotées classiques, offre une meilleure lisibilité et facilite la maintenance future (ajout/suppression de règles). De plus, nous ne l'avons pas utilisé en TP donc cela nous permet de diversifier nos acquis.

3. Configuration Déttaillée

3.1. Définition des Zones

Le routeur doit distinguer le réseau de confiance des réseaux externes.

- **Inside** : L'interface des clients privés (**Fa0/0.2**).
- **Outside** : Toutes les autres interfaces dont le WAN (**Fa0/1**), mais aussi les Serveurs (**Fa0/0.1**) et le Public Local (**Eth1/0**).
 - Note : Le fait de placer les serveurs et le public local en Outside forcera la translation du réseau privé vers ces zones.

```
Routeur-Int-31(config)# interface FastEthernet0/0.2
Routeur-Int-31(config-subif)# ip nat inside
!
```

```

Routeur-Int-31(config)# interface FastEthernet0/1
Routeur-Int-31(config-if)# ip nat outside
!
Routeur-Int-31(config)# interface FastEthernet0/0.1
Routeur-Int-31(config-subif)# ip nat outside
!
Routeur-Int-31(config)# interface Ethernet1/0
Routeur-Int-31(config-if)# ip nat outside

```

3.2. L'ACL pour la translation (ACL_PRIVE_IN)

Cette ACL étendue définit les permissions suivantes :

```

Routeur-Int-31(config)# ip access-list extended ACL_PRIVE_IN
Routeur-Int-31(config-std-nacl)#permit ip 192.168.31.0 0.0.0.63
150.150.32.0 0.0.0.255
Routeur-Int-31(config-std-nacl)#permit ip 192.168.31.0 0.0.0.255
50.50.32.0 0.0.0.255
Routeur-Int-31(config-std-nacl)#permit ip 192.168.31.0 0.0.0.255
50.50.31.0 0.0.0.255
Routeur-Int-31(config-std-nacl)#permit ip 192.168.31.0 0.0.0.255
150.150.31.0 0.0.0.255
Routeur-Int-31(config-std-nacl)# permit udp any any eq bootps
Routeur-Int-31(config-std-nacl)# permit udp any any eq bootpc

```

Justification : Nous avons ajouté les règles `permit ip 192.168.31.0 0.0.0.255 50.50.31/32.0 0.0.0.255`. Cette règle permet à tous les clients privés d'accéder aux serveurs.

4. Tests et Validation

La validation permet de vérifier que la translation s'opère correctement et que les restrictions d'adressage sont respectées.

Test 1 : Vérification de la table NAT

- **Action :** Ping depuis un client privé (`192.168.31.10`) vers le serveur (`50.50.31.1`).
- **Observation :**

```

Routeur-Int-31(config)#do sh ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
icmp 90.0.31.1:43568   192.168.31.1:43568 50.50.32.1:43568  50.50.32.1:43568

```

Test 2 : Validation de la restriction (ACL)

- Un ping depuis **192.168.31.10** (autorisé) **doit réussir**. On remarque que son adresse du côté du voisin est **50.50.31.1** avec un port.
- Un ping depuis **192.168.31.100** vers une adresse IP de l'autre site par exemple **90.90.32.1** (hors plage) **doit échouer**, car il ne sera pas translaté.

```
root@G30:~# ping 50.50.32.1 -c 1
PING 50.50.32.1 (50.50.32.1) 56(84) bytes of data.
64 bytes from 50.50.32.1: icmp_seq=1 ttl=60 time=4.57 ms

--- 50.50.32.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.569/4.569/4.569/0.000 ms
```

```
+ 4 5.164304820 90.0.31.1      50.50.32.1      ICMP    98 Echo (ping) request id=0x5d25, seq=1/256, ttl=60 (reply in 5)
← 5 5.164325379 50.50.32.1      90.0.31.1      ICMP    98 Echo (ping) reply   id=0x5d25, seq=1/256, ttl=64 (request in 4)
+ 6 6.014407880 Cisco_23:30:17  Nearest-Customer-Br... STP     60 Conf. Root = 32768/321/00:18:18:23:30:00 Cost = 0 Port = 0x8017
+ 7 6.164380244 90.0.31.1      50.50.32.1      ICMP    98 Echo (ping) request id=0x5d25 seq=2/512 ttl=60 (reply in 8)

> Frame 4: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
└> Ethernet II, Src: Cisco_59:24:60 (00:0a:b7:59:24:60), Dst: HP_10:2b:e1 (2c:58:b9:10:2b:e1)
   |> Destination: HP_10:2b:e1 (2c:58:b9:10:2b:e1)
   |> Source: Cisco_59:24:60 (00:0a:b7:59:24:60)
   |> Type: IPv4 (0x0800)
   |   [Stream index: 1]
   > Internet Protocol Version 4, Src: 90.0.31.1, Dst: 50.50.32.1
```

```
root@G29:~# dhclient -v
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/34:17:eb:99:ba:58
Sending on  LPF/eth0/34:17:eb:99:ba:58
Sending on  Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPOFFER of 192.168.31.64 from 192.168.31.254
DHCPREQUEST for 192.168.31.64 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.31.64 from 192.168.31.254
bound to 192.168.31.64 -- renewal in 13 seconds.
root@G29:~# ping 90.0.32.1
PING 90.0.32.1 (90.0.32.1) 56(84) bytes of data.
^C
--- 90.0.32.1 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5110ms
```

Lorsque l'IP n'est pas dans la plage d'autorisation de l'ACL, le paquet est rejeté car filtré.

V : Service web

1. Analyse du Cahier des Charges

Le cahier des charges stipule que la machine serveur S31 doit héberger un service Web. Ce service a une double vocation :

- Fournir une page web aux utilisateurs.
- Pour nous, servir de cible pour valider la connectivité de bout en bout avec ACL du port TCP/80 depuis les réseaux internes et externes (site distant).

2. Justification de la Solution

Nous utilisons le serveur HTTP Apache2.

Ce logiciel est préinstallé sur les environnements Linux de l'IUT, ce qui dispense d'une phase d'installation de paquets. De plus, la configuration par défaut d'Apache (écoutes sur le port 80 et servant le répertoire /var/www/html) est suffisante pour répondre à notre besoin. Elle permet de délivrer une page index.html de test.

3. Configuration Détailée

Machine : Serveur S31 (Linux)

Le service étant pré-installé, l'intervention consiste à démarrer le service et à vérifier son état.

```
root@S31:~# systemctl start apache2
# Activation au démarrage de la machine
root@S31:~# systemctl enable apache2
```

4. Tests et Validation

La validation du service se fait en deux temps : vérification locale du processus et test fonctionnel distant.

Test 1 : État du Service (Côté Serveur)

Nous vérifions que le processus est actif et qu'il n'y a pas d'erreur de configuration.

Commande : `systemctl status apache2`

Résultat : Le statut doit indiquer `active (running)`.

```

root@S30:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: enabled)
   Active: active (running) since Mon 2026-01-05 09:16:00 CET; 53min ago
     Docs: https://httpd.apache.org/docs/2.4/
 Process: 274119 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 274136 (apache2)
    Tasks: 55 (limit: 37802)
   Memory: 7.1M
      CPU: 245ms
     CGroup: /system.slice/apache2.service
             ├─274136 /usr/sbin/apache2 -k start
             ├─274137 /usr/sbin/apache2 -k start
             └─274138 /usr/sbin/apache2 -k start

janv. 05 09:16:00 S30.tp301.iut systemd[1]: Starting apache2.service - The Apache HTTP Server...
janv. 05 09:16:00 S30.tp301.iut apachectl[274135]: AH00558: apache2: Could not reliably determine the server's fully qualified name, using 127.0.0.1 for Port 80
janv. 05 09:16:00 S30.tp301.iut systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-17/17 (END)

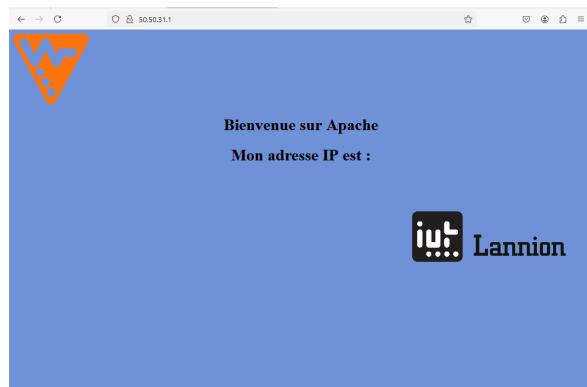
```

Test 2 : Accès HTTP (Côté Client)

Depuis un client du réseau (ex: D31 ou G31), nous ouvrons un navigateur ou utilisons la commande curl vers l'adresse IP du serveur (après la mise en place du DNS, on pourra utiliser l'URL).

URL : <http://50.50.31.1> (ou www.site31.iut. si DNS actif)

Résultat : Affichage de la page par défaut "Bienvenue sur Apache".



capture d'écran prise depuis la machine G31

5. Conclusion

Le service Web est opérationnel sur le port 80. Il est désormais prêt à être interrogé par les clients internes et externes, sous réserve que les règles de filtrage (ACL) et de translation (NAT) configurées précédemment autorisent ce flux TCP.

VI : Service DNS

1. Analyse et Besoin

Dans un réseau d'entreprise, la mémorisation des adresses IP (ex: 50.50.31.1) peut être embêtante pour les utilisateurs. Le service DNS est donc très utile pour assurer la traduction entre les noms de domaine/FQDN et les adresses IP. Le serveur S31 doit assurer :

1. La résolution des noms locaux (`site31.iut`).
2. La résolution inverse (IP vers Nom), utile pour les logs et l'évolution du réseau (on peut citer le mail par exemple).
3. La résolution des noms du site distant (`site32.iut`) via un mécanisme de redirection (Forwarding).

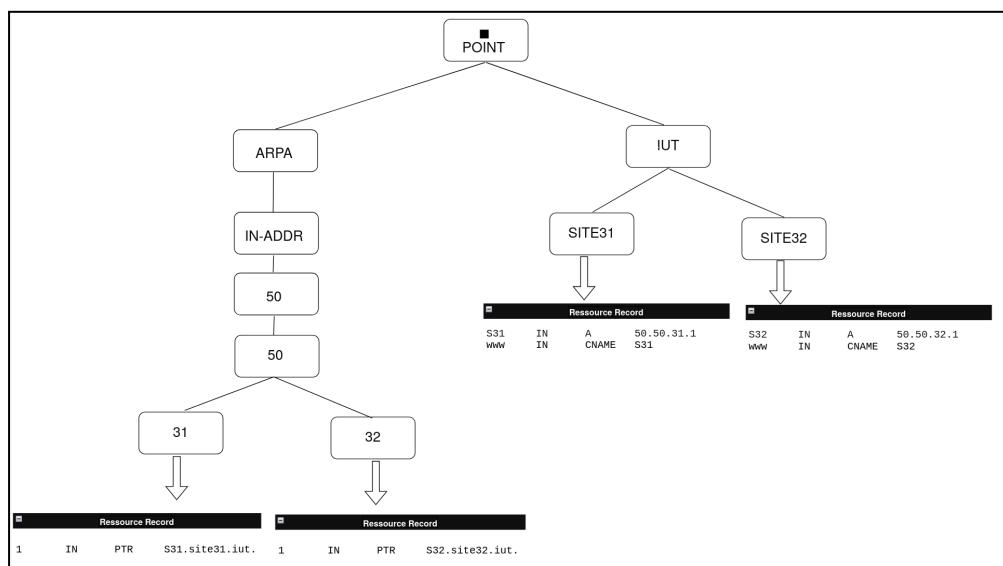
2. Justification de la Solution

Nous utilisons le serveur named car comme pour `Apache2`, il est déjà installé.

- **Architecture de Zone** : Nous définissons le site 31 comme Maître pour sa propre zone.
- **Forwarding** : Pour résoudre les noms du site voisin (`site32.iut`), notre serveur ne connaît pas les réponses. Il est configuré pour transmettre (Forward) ces requêtes spécifiques vers l'adresse publique du routeur du site 32 (50.50.32.1), qui transmettra à son tour à son serveur DNS local (grâce au NAT statique configuré précédemment).
- **Désactivation IPv6** : Notre architecture étant exclusivement IPv4, nous désaktivons l'écoute IPv6 pour optimiser les performances et la sécurité.

3. Arborescence DNS

La configuration DNS mis en place respecte la hiérarchie suivante :



4. Configuration Détailée

4.1. Options Globales (`named.conf.options`)

Nous limitons l'écoute aux adresses IPv4.

```
options {
    directory "/var/cache/bind";
    dnssec-validation no;
    allow-recursion { any; }; ! -> permet la redirection vers les
clients
    listen-on-v6 { none; };
    allow-query { any; };
};
```

4.2. Déclaration des Zones (`named.conf.local`)

Ce fichier définit les rôles du serveur pour chaque zone.

```
// Zone Directe Locale
zone "site31.iut" {
    type master;
    file "/etc/bind/db.site31.iut";
};

// Zone Inverse Locale
zone "31.50.50.in-addr.arpa" {
    type master;
    file "/etc/bind/db.31.50.50";
};

// Forwarding vers le Site 32
zone "site32.iut" {
    type forward;
    forwarders { 50.50.32.1; };
};

zone "32.50.50.in-addr.arpa" {
    type forward;
    forwarders { 50.50.32.1; };
};
```

4.3. Fichier de Zone Directe (`db.site31.iut`)

Ce fichier associe les noms aux IP. Nous utilisons un enregistrement CNAME pour le service Web, ce qui permet d'accéder au serveur via l'alias `www` sans lier ce nom directement à une IP. On utilise cet alias car il est régulièrement présent sur internet donc plus facile pour la majorité à retenir.

```
$ORIGIN site31.iut.  
$TTL 604800  
@ IN SOA site31.iut. root.site31.iut. (  
    3 ; Serial  
    604800 ; Refresh  
    86400 ; Retry  
    2419200 ; Expire  
    604800 ) ; Negative Cache TTL  
  
; Name Server  
@ IN NS S31.site31.iut.  
  
; Enregistrements  
S31 IN A 50.50.31.1  
www IN CNAME S31
```

4.4. Fichier de Zone Inverse (`db.31.50.50`)

Permet de retrouver le nom à partir de l'IP (ex: `50.50.31.1` → `S31.site31.iut`).

```
$ORIGIN 31.50.50.in-addr.arpa.  
$TTL 604800  
@ IN SOA site31.iut. root.site31.iut. (  
    3 ; Serial  
    604800 ; Refresh  
    86400 ; Retry  
    2419200 ; Expire  
    604800 ) ; Negative Cache TTL  
  
@ IN NS S31.site31.iut.  
1 IN PTR S31.site31.iut.
```

5. Configuration Client et Démarrage

Pour que le serveur S31 utilise son propre service DNS, nous modifions son fichier de résolution.

Fichier `/etc/resolv.conf` :

```
domain site31.iut
search site31.iut
nameserver 50.50.31.1
```

Commandes liées au service :

```
systemctl restart named # Redémarrage
systemctl start named # Démarrage
systemctl stop named # Arret
systemctl enable named # Démarrage automatique
```

6. Tests et Validation

Nous vérifions le fonctionnement à l'aide de la commande `nslookup` (ou `dig` sur linux) depuis une machine cliente.

Test 1 : Résolution Locale

- Commande : `nslookup www.site31.iut`
- Résultat attendu : Renvoie l'IP `50.50.31.1` (avec mention de l'alias `canonical name de S31.site31.iut`).

```
C:\Users\root>nslookup www.site31.iut
Serveur :   S31.site31.iut
Address:  50.50.31.1

Nom :   S31.site31.iut
Address: 50.50.31.1
Aliases: www.site31.iut
```

```
^Croot@G30:~# dig www.site31.iut
; <>> DiG 9.18.33-1~deb12u2-Debian <>> www.site31.iut
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4683
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1232
;; COOKIE: d586136458ef120201000000695b848b7f98b295fbc638b6 (good)
;; QUESTION SECTION:
;www.site31.iut.           IN      A

;; ANSWER SECTION:
www.site31.iut.       604800  IN      CNAME   S31.site31.iut.
S31.site31.iut.       604800  IN      A       50.50.31.1

;; Query time: 3 msec
;; SERVER: 50.50.31.1#53(50.50.31.1) (UDP)
;; WHEN: Mon Jan 05 10:31:05 CET 2026
;; MSG SIZE  rcvd: 105

root@G30:~#
```

Test 2 : Forwarding

- Commande : `nslookup S32.site32.iut`
- Résultat attendu : Le serveur doit interroger `50.50.32.1` et renvoyer l'IP publique du serveur distant.

```
root@G51:~# dig www.site32.iut.

; <>> DiG 9.18.33-1~deb12u2-Debian <>> www.site32.iut.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6333
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d12eb9958d6759aa01000000695eb276d24849d4c183e777 (good)
;; QUESTION SECTION:
;www.site32.iut.           IN      A

;; ANSWER SECTION:
www.site32.iut.      0      IN      CNAME   S32.site32.iut.
S32.site32.iut.     604800  IN      A       50.50.32.1

;; Query time: 19 msec
;; SERVER: 50.50.31.1#53(50.50.31.1) (UDP)
;; WHEN: Wed Jan 07 18:23:04 CET 2026
;; MSG SIZE rcvd: 105
```

706 799.283020435 90.0.31.1	50.50.31.1	DNS	97 Standard query 0x18bd A www.site32.iut OPT
707 799.284798428 50.50.31.1	50.50.32.1	DNS	97 Standard query 0x4d6f A www.site32.iut OPT
710 799.291147005 50.50.32.1	50.50.31.1	DNS	147 Standard query response 0x406f A www.site32.iut CNAME S32.site32.iut A 50.50.32.1 OPT
713 799.299644562 50.50.31.1	90.0.31.1	DNS	147 Standard query response 0x18bd A www.site32.iut CNAME S32.site32.iut A 50.50.32.1 OPT

Trame n°1 : Requête du client vers le server S31

Trame n°2 : Requête du serveur S31 vers le server S32 (Le forwarding rentre en jeu)

Trame n°3 : Réponse du serveur S32 vers le server S31

Trame n°4 : Réponse du serveur S31 vers le client S31

Remarque : Le PAT dynamique est actif dans sur cette capture donc le client privé est caché derrière 90.0.31.1.

Test 3 : Validation DHCP Sur le client Windows, la commande `ipconfig` permet de confirmer que le **Suffixe DNS** est bien `site31.iut` et que le **Serveur DNS** attribué est `50.50.31.1`.

```
C:\Users\root>ipconfig

Configuration IP de Windows

Carte Ethernet eth0 :

    Suffixe DNS propre à la connexion. . . . . : site31.iut
    Adresse IPv6 de liaison locale. . . . . : fe80::3800:ab05:e590:7ec9%8
    Adresse IPv4. . . . . : 150.150.31.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 150.150.31.254
```

7. Conclusion

Le service DNS est fonctionnel. Il assure la résolution locale et l'interconnexion avec le site distant. On pourra donc l'utiliser pour tous autres services nécessitant un accès IP à la machine serveur.

VII : Service FTP et SSH

1. Analyse du Cahier des Charges

Le cahier des charges nous demande que la machine serveur (S31) héberge les services SSH et FTP avec l'exigence suivante. Ces services doivent être accessibles **de l'intérieur** (autres réseaux du site 31) mais également **de l'extérieur** (les réseaux du site d'en face, 32). Cette contrainte implique que :

- Le routage et le NAT statique doivent être fonctionnels pour permettre l'accès distant.
- La sécurité (ACL) devra être configurée ultérieurement pour autoriser spécifiquement ces flux entrants tout en bloquant le reste.

2. Justification de la Solution

Pour répondre à ces besoins, nous utilisons les solutions disponibles dans l'environnement de l'IUT :

- **OpenSSH Server** : Protocole sécurisé pour l'administration distante en ligne de commande.
- **ProFTPD** : Serveur FTP pour le transfert de fichiers. Cependant, il n'est pas chiffré par défaut (contrairement à SFTP).

Stratégie de Test : Pour valider les accès sans exposer le compte **root** (ce qui est une mauvaise pratique de sécurité, bloquée par défaut en SSH), nous créons un utilisateur dédié nommé **etu**.

3. Configuration Détailée

Machine : Serveur S31

La configuration consiste à créer l'environnement utilisateur et à activer les services.

```
# Création de l'utilisateur etu avec son répertoire personnel
root@S31:~# useradd -m -s /bin/bash etu
# Attribution du mot de passe lannion
root@S31:~# echo "etu:lannion" | chpasswd
# Démarrage des services
root@S31:~# systemctl start ssh
root@S31:~# systemctl start proftpd
```

4. Tests et Validation

Nous devons prouver que l'accès fonctionne depuis l'intérieur (LAN) et l'extérieur (WAN), conformément au cahier des charges.

4.1. Test SSH (Intérieur et Extérieur)

- **Test Interne** : Depuis le client G31 (Réseau Public) vers l'IP locale du serveur ([50.50.31.1](#)).
 - Commande : `ssh etu@50.50.31.1`
 - Résultat : Demande de mot de passe et obtention du shell.

```
root@G31:~# ssh etu@50.50.31.1
etu@50.50.31.1's password:
Linux S31.tp311.iut 6.12.12+bpo-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.12-1+bpo12+1 (2025-02-23) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec 17 18:34:04 2025 from 150.150.31.1
etu@S31:~$
```

On observe sur wireshark

No.	Time	Source	Destination	Protocol	Length	Info
48	18:052696897	192.168.31.64	50.50.31.1	SSHv2	106	Client: Protocol (SSH-2.0-OpenSSH_9_2p1 Debian-2+deb12u5)
42	18:059723250	50.50.31.1	192.168.31.64	SSHv2	105	Server: Protocol (SSH-2.0-OpenSSH_9_2p1 Debian-2+deb12u5)
44	18:060252311	192.168.31.64	50.50.31.1	SSHv2	155	Client: Key Exchange Init
45	18:061202195	50.50.31.1	192.168.31.64	SSHv2	1202	Server: Diffie-Hellman Key Exchange Init
48	18:061381999	192.168.31.64	50.50.31.1	SSHv2	1274	Client: Diffie-Hellman Key Exchange Reply, New Keys
49	18:077330430	50.50.31.1	192.168.31.64	SSHv2	1630	Server: Diffie-Hellman Key Exchange Reply, New Keys
52	21:093282108	192.168.31.64	50.50.31.1	SSHv2	82	Client: New Keys
54	21:0935961293	192.168.31.64	50.50.31.1	SSHv2	110	Client:
56	21:0936860425	50.50.31.64	192.168.31.64	SSHv2	110	Server:
58	21:0936961016	192.168.31.64	50.50.31.1	SSHv2	126	Client:
59	21:0945431093	50.50.31.1	192.168.31.64	SSHv2	110	Server:
69	24:114361179	192.168.31.64	50.50.31.1	SSHv2	206	Client:
70	24:123128648	50.50.31.1	192.168.31.64	SSHv2	94	Server:
72	24:123241988	192.168.31.64	50.50.31.1	SSHv2	170	Client:
73	24:163896945	50.50.31.1	192.168.31.64	SSHv2	558	Server:
75	24:206811479	50.50.31.1	192.168.31.64	SSHv2	110	Server:
77	24:207001479	192.168.31.64	50.50.31.1	SSHv2	899	Client:
78	24:209001387	50.50.31.1	192.168.31.64	SSHv2	150	Server:
79	24:209351497	50.50.31.1	192.168.31.64	SSHv2	558	Server:
81	24:229722649	50.50.31.1	192.168.31.64	SSHv2	158	Server:
86	27:046253549	192.168.31.64	50.50.31.1	SSHv2	94	Client:
87	27:047722829	50.50.31.1	192.168.31.64	SSHv2	94	Server:
94	28:380014288	192.168.31.64	50.50.31.1	SSHv2	94	Client:
95	28:381335486	50.50.31.1	192.168.31.64	SSHv2	94	Server:
97	28:578177224	192.168.31.64	50.50.31.1	SSHv2	94	Client:
98	28:571617398	50.50.31.1	192.168.31.64	SSHv2	94	Server:
106	28:834174803	192.168.31.64	50.50.31.1	SSHv2	94	Client:
101	28:835553938	50.50.31.1	192.168.31.64	SSHv2	94	Server:
103	28:835553945	192.168.31.64	50.50.31.1	SSHv2	94	Client:
104	28:2893604949	50.50.31.1	192.168.31.64	SSHv2	110	Server:
105	28:203365286	50.50.31.1	192.168.31.64	SSHv2	110	Server:
108	28:204752761	50.50.31.1	192.168.31.64	SSHv2	210	Server:
110	29:204854208	192.168.31.64	50.50.31.1	SSHv2	94	Client:
111	29:204867996	192.168.31.64	50.50.31.1	SSHv2	126	Client:

- **Test Externe :** Depuis le client D31 vers le serveur du **site distant** (S32), en utilisant l'IP publique de son routeur (**50.50.32.1**).
 - Commande : **ssh etu@50.50.32.1**
 - Résultat : La connexion réussit. Cela valide que le paquet a traversé notre routeur, le WAN, le routeur distant, et a été correctement redirigé par le NAT statique distant vers S32.

Remarque : Le NAT statique n'a pas lieu d'être cependant la redirection fonctionne donc ce test reste valide pour les raisons citées en III.

```
C:\Users\root>ssh etu@90.0.32.1
The authenticity of host '90.0.32.1 (90.0.32.1)' can't be established.
ED25519 key fingerprint is SHA256:kaoQDsF1D436aS0LFdJn1LVIJntN1Hj9T6W41wCpGGg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '90.0.32.1' (ED25519) to the list of known hosts.
etu@90.0.32.1's password:
Linux S32.tp321.iut 6.12.12+bpo-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.12-1~bpo12+1 (2025-02-23) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec 17 18:17:32 2025 from 90.0.31.1
etu@S32:~$
```

4.2. Test FTP (Transfert de fichier)

- **Test interne :** Depuis G31, nous envoyons un fichier vers S31.
 - Commande :

```
ftp 50.50.31.1
> put fichier_test.txt
```

Résultat : On se connecte puis on réalise le transfert qui s'effectue (226 Téléchargement terminé).

```
root@G31:~# ftp site31.iut
Connected to site31.iut.site31.iut.
220 ProFTPD Server (Debian) [::ffff:50.50.31.1]
Name (site31.iut:root): etu
331 Mot de passe requis pour etu
Password:
230 Utilisateur etu authentifié
Remote system type is UNIX.
Using binary mode to transfer files.
```

```
ftp> put fichier_test.txt
local: fichier_test.txt remote: fichier_test.txt
229 Entering Extended Passive Mode (|||16700|)
150 Ouverture d'une connexion de données en mode BINARY pour fichier_test.txt
100% |*****| 7 189.88 KiB/s 00:00 ETA
226 Téléchargement terminé
7 bytes sent in 00:00 (4.65 KiB/s)
```

- **Test externe** : Depuis G31, nous envoyons un fichier vers S32.
 - Commande :

```
ftp 50.50.32.1
> put fichier_test.txt
```

Résultat : Le transfert s'effectue (On se connecte puis on réalise le transfert qui s'effectue (Code 226 Transfer complete)).

```
root@G31:~# ftp site32.iut
Connected to site31.iut.site31.iut.
220 ProFTPD Server (Debian) [::ffff:50.50.32.1]
Name (site32.iut:root): etu
331 Mot de passe requis pour etu
Password:
230 Utilisateur etu authentifié
Remote system type is UNIX.
Using binary mode to transfer files.

ftp> put fichier_test.txt
local: fichier_test.txt remote: fichier_test.txt
229 Entering Extended Passive Mode (|||16700|)
150 Ouverture d'une connexion de données en mode BINARY pour fichier_test.txt
100% |*****| 7 189.88 KiB/s 00:00 ETA
226 Téléchargement terminé
7 bytes sent in 00:00 (4.65 KiB/s)
```

5. Conclusion

Les services SSH et FTP sont installés et fonctionnels. Les tests de connectivité confirment que les services sont accessibles depuis les réseaux locaux et distants, validant ainsi les exigences d'ouverture du cahier des charges.

VIII : Service RADIUS

1. Analyse et Besoin

Le cahier des charges impose de sécuriser l'accès au réseau "Clients Privés". Une simple connexion par câble ne doit pas suffire pour accéder au réseau : l'utilisateur doit s'authentifier. Pour cela, nous mettons en œuvre le protocole RADIUS.

Ce protocole repose sur trois entités :

1. **Le Supplicant (Client)** : La machine qui veut se connecter (G31).
2. **L'Authenticator (Intermédiaire)** : Le switch **Switch-Prive-31** qui bloque le port tant que l'identité n'est pas validée.
3. **L'Authentication Server** : Le serveur RADIUS (S31) qui détient la base de données des utilisateurs.

Le serveur utilisera le logiciel **FreeRADIUS**, déjà installé sur les machines de l'IUT.

2. Configuration du Switch

Le switch agit comme un relais. Il bloque les ports par défaut et transmet les trames d'authentification (trame EAPOL) au serveur RADIUS.

Configuration :

```
Switch-Prive-31# configure terminal

! -> Active le protocole 802.1X sur le switch
Switch-Prive-31(config)#dot1x system-auth-control
! -> Active le modèle AAA (Authentication, Authorization,
Accounting)
Switch-Prive-31(config)#aaa new-model

! -> Définit que pour l'authentification 802.1X, le switch doit
interroger le groupe de serveurs radius défini plus bas

Switch-Prive-31(config)#aaa authentication dot1x default group
radius

! -> Définit que l'autorisation (accès au réseau, VLAN dynamique,
etc)
Switch-Prive-31(config)#aaa authorization network default group
radius

! -> On doit configurer un IP sur le switch pour qu'il puisse
```

```

communiquer avec le serveur
Switch-Prive-31(config)# interface Vlan311
Switch-Prive-31(config-if)# ip address 50.50.31.253 255.255.255.0
Switch-Prive-31(config-if)# no shut
Switch-Prive-31(config-if)# exit

! Déclaration du Serveur RADIUS
Switch-Prive-31(config)#radius server RADIUS_31
Switch-Prive-31(config-radius-server)#address ipv4 50.50.31.1
auth-port 1812 acct-port 1813
Switch-Prive-31(config-radius-server)#key P4ssw0rd!
Switch-Prive-31(config-radius-server)#exit

! -> On déclare le serveur S31 (50.50.31.1).
! -> auth-port 1812 : Port standard pour l'authentification.
! -> acct-port 1813 : Port standard pour les logs de radius.
! -> key : Clé secrète partagée qui permet de chiffrer les
échanges
! les échanges entre le switch et le serveur. Elle doit être
identique des deux côtés

Switch-Prive-31(config)#interface range FastEthernet0/1 - 15
Switch-Prive-31(config-if-range)#authentication port-control auto
! -> Le port passe en mode "auto".
! État initial : Bloqué
! État final : Débloqué uniquement si le serveur RADIUS accepte

Switch-Prive-31(config-if-range)#dot1x pae authenticator
! -> Définit le rôle du port comme "Authenticator"
! Il initie et relaie les demandes d'authentification vers le
serveur.

Switch-Prive-31(config-if-range)#spanning-tree portfast
! -> Passe immédiatement le port en mode "Forwarding".
! Pour éviter que le client ne tombe en timeout Radius pendant le
démarrage du port

```

Quand on parle de démarrage du port, on parle du moment entre le branchement du câble et le moment où le port est utilisable. Cet instant peut durer assez longtemps jusqu'à ce que le client invalide sa requête RADIUS.

3. Configuration du Serveur RADIUS (S31)

Sur le serveur, nous devons déclarer un utilisateur autorisé. Cela se fait dans le fichier de configuration des utilisateurs de FreeRADIUS.

Fichier : /etc/freeradius/3.0/users Nous ajoutons la ligne suivante au début du fichier :

```
login Cleartext-Password := "pass"  
# Ne rien modifier dans la suite
```

Cette ligne crée un utilisateur nommé `login` avec le mot de passe `pass`. L'attribut `Cleartext-Password` indique que le serveur connaît le mot de passe en clair, ce qui est nécessaire pour certains protocoles d'authentification comme MD5 qu'on utilise.

Il faut également déclarer le switch comme client autorisé dans le fichier `clients.conf` du serveur avec la même clé `P4ssw0rd!`.

Fichier : /etc/freeradius/3.0/clients.conf

Nous ajoutons les lignes suivantes au début du fichier :

```
# Ne rien modifier avant  
  
client 50.50.31.253 {  
    shortname = switch-prive-31  
    secret = P4ssw0rd!  
    nastype=cisco  
    ipaddr = 50.50.31.253  
}
```

Cette configuration autorise l'équipement ayant l'IP `50.50.31.253` (notre Switch Privé) à interroger le serveur RADIUS. La clé secrète `P4ssw0rd!` permet de chiffrer et d'authentifier les échanges entre le switch et le serveur, empêchant un équipement non autorisé de tester des mots de passe.

Remarque : Cette configuration implique que le Switch-Prive-31 possède une interface configurée avec l'IP `50.50.31.253` dans le VLAN 311 (Serveur) et qu'il puisse pinger le serveur ce qui est le cas avec notre configuration actuelle.

4. Configuration du Client (Supplicant)

La machine cliente (Linux) utilise le service `wpa_supplicant` pour gérer l'authentification.

Fichier de configuration : /etc/wpa_supplicant/mon_radius.conf

```
# Configuration du socket de contrôle  
ctrl_interface=/var/run/wpa_supplicant  
ctrl_interface_group=0
```

```

# Désactivation du scan Wi-Fi
ap_scan=0

# Configuration des identifiants
network={
    key_mgmt=IEEE8021X
    eap=MD5          # Méthode d'authentification
    identity="login" # Nom utilisateur
    password="pass"  # Mot de passe associé
    eapol_flags=0
}

```

5. Tests et Validation

Pour valider la sécurisation du port, nous effectuons le test suivant sur la machine cliente G31 connectée au port **Fa0/1** du switch privé.

Étape 1 : Avant authentification

- **Test :** `ping 192.168.31.254` (Passerelle)
- **Résultat :** Échec (`Destination Host Unreachable`). Le port du switch est physiquement monté (`up`) mais bloqué logiquement par le 802.1X.

Étape 2 : Lancement du Supplicant Nous exécutons la commande suivante pour initier l'échange :

```
wpa_supplicant -D wired -c /etc/wpa_supplicant/mon_radius.conf -i eth0
```

- `-D wired` : Force le driver filaire.
- `-i eth0` : Interface à authentifier.

Analyse de la sortie : Nous observons les messages `CTRL-EVENT-EAP-STARTED`, puis `CTRL-EVENT-EAP-SUCCESS`. Le serveur RADIUS a validé les identifiants `login/pass` et a envoyé un message Access-Accept au switch.

```

Switch-Prive-31(config)#
*Mar 1 02:21:14.104: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan311, p
*Mar 1 02:21:30.806: %AUTHMGR-5-START: Starting 'dot1x' for client (f8b1.569a.B
*Mar 1 02:21:31.829: %DOT1X-5-SUCCESS: Authentication successful for client (fB
*Mar 1 02:21:31.829: %AUTHMGR-7-RESULT: Authentication result 'success' from 'B
*Mar 1 02:21:32.785: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (fB
*Mar 1 02:21:32.852: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherp

```

Étape 3 : Après authentification

- **Test :** ping 192.168.31.254
- **Résultat :** Succès. Le switch débloque le port et autorisé le trafic.

Vérification sur le Switch : La commande `show dot1x interface FastEthernet0/1 details` confirme que l'état du port est passé à **AUTHORIZED** et que le dernier utilisateur authentifié provient de G31 (on le voit grâce l'adresse MAC).

```
Switch-Prive-31(config)#do sh dot1x int F0/1 details

Dot1x Info for FastEthernet0/1
-----
PAE          = AUTHENTICATOR
PortControl   = AUTO
ControlDirection = Both
HostMode      = SINGLE_HOST
QuietPeriod    = 60
ServerTimeout  = 0
SuppTimeout    = 30
ReAuthMax     = 2
MaxReq        = 2
TxPeriod       = 30

Dot1x Authenticator Client List
-----
EAP Method    = MD5
Supplicant    = f8b1.569a.43e9
Session ID    = 32321FFD000000F008186DB
  Auth SM State = AUTHENTICATED
  Auth BEND SM State = IDLE

Switch-Prive-31(config)#[
```

6. Conclusion

Le service RADIUS est fonctionnel. Il assure un contrôle d'accès au niveau de la couche physique : aucune machine ne peut communiquer sur le réseau privé sans disposer d'un compte valide sur le serveur, respectant ainsi les exigences de sécurité du cahier des charges.

IX : Service Vidéo

1. Analyse du Cahier des Charges

Le cahier des charges stipule que le serveur du site (S31) doit héberger un service de diffusion vidéo. Ce service doit être accessible par les clients du réseau public du site opposé (Site 32). De plus, en cas de congestion des liens, la vidéo doit rester fluide, ce qui implique une réservation de bande passante (traitée dans la partie XI QoS).

2. Justification de la Solution

Pour répondre à ce besoin, nous utilisons le logiciel VLC Media Player.

- **Choix du Protocole** : Nous utiliserons le protocole RTP qui est encapsulé dans de l'UDP.
- **Encapsulation** : Le flux utilise le standard MPEG-TS, conçu pour avoir l'audio et la vidéo dans le même paquet.
- **Port d'écoute** : Le flux sera émis sur le port UDP 5004. Ce choix servira de critère de classification pour la QoS (**ACL_QOS_VIDEO**) définie ultérieurement.

Ces choix sont issus du documents fournis dans le cadre de la SAE pour configurer ce serveur.

3. Configuration Détailée

3.1. Configuration du Serveur (S31)

Machine : Serveur S31 (Debian Linux). **Rôle** : émetteur du flux.

L'installation de VLC va nécessiter une commande pour autoriser son exécution en tant qu'utilisateur **root** (l'utilisateur par défaut de nos TPs).

```
# Installation du paquet
root@S31~# apt install vlc

# Autorisation de l'exécution en root
root@S31~# sed -i 's/geteuid/getppid/' /usr/bin/vlc
```

Procédure pour la diffusion :

1. Lancer **VLC** et ouvrir le menu **Média > Diffuser (Ctrl+S)**.
2. Ajoutez le fichier vidéo source et cliquez sur **Diffuser**.
3. Dans "**Destination**", choisissez **RTP / MPEG Transport Stream**, cochez "**Afficher localement**" et cliquez sur **Ajouter**.
4. Configurer les paramètres de flux :
 - **Adresse** : **150.150.32.1** (IP d'un client public du site distant, pour simuler un flux Unicast vers une cible précise)
 - **Port de base** : **5004**
 - **Transcodage** : Déscocher "**Activer le transcodage**" (pour minimiser la charge CPU du serveur S31)
5. Valider jusqu'au démarrage du flux.

3.2. Configuration du Client (D32)

Machine : Client Public du Site 32. **Rôle** : Récepteur du flux.

Pour la configuration côté client, il suffit d'écouter le port sur lequel le serveur envoie les données.

Procédure de réception :

1. Ouvrir VLC sur le client.
2. Aller dans Média > Ouvrir un flux réseau (Ctrl+N).
3. Entrer l'URL réseau : `rtp://:@:5004`
 - **Remarque** : Le caractère @ indique à VLC d'écouter sur toutes les interfaces locales le trafic entrant sur le port 5004.
4. Cliquer sur Lire.

4. Tests et Validation

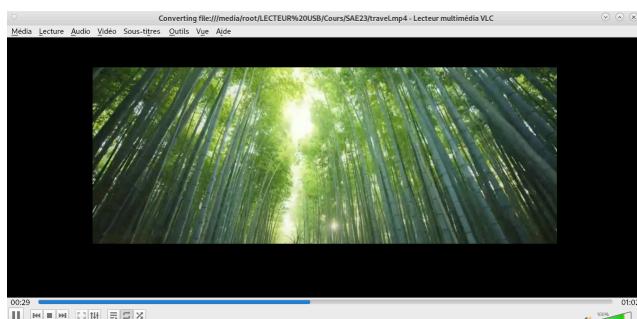
L'objectif est de valider que le flux vidéo traverse correctement toute l'infrastructure (S32->Switch Privé 31 -> Routeur Int 31 -> Routeur Ext 31 -> WAN -> Routeur Ext 32 -> Routeur Int 32 -> Switch Public 32->G32).

Test : Lancement de la vidéo sur S31 vers l'IP de D32 (150.150.32.1).

Résultat attendu : La vidéo s'affiche sur le poste client avec le son.

Résultat Obtenu :

- L'image est fluide.
- En regardant une capture wireshark, on pourra observer une suite de paquet UDP venant du serveur.



Analyse de la capture : On observe bien des paquets UDP dont la source est **50.50.31.1** (S31) et la destination voisine par exemple **150.150.32.1** (Client).

Le protocole décodé est MPEG TS. Cela valide que :

1. Le routage OSPF est fonctionnel de bout en bout.
2. Les ACLs configurées (Section X) laissent passer le protocole UDP sur le port 5004.

8 0.170499685	50..59..32..1	50..50..31..1	UDP	1370 32927 – 5004 Len=1328
9 0.192739956	50..59..32..1	50..50..31..1	UDP	1370 32927 – 5004 Len=1328
10 0.214977179	50..59..32..1	50..50..31..1	UDP	1370 32927 – 5004 Len=1328
11 0.237218743	50..59..32..1	50..50..31..1	UDP	1370 32927 – 5004 Len=1328
12 0.259461355	50..59..32..1	50..50..31..1	UDP	1370 32927 – 5004 Len=1328
13 0.281699897	50..59..32..1	50..50..31..1	UDP	1370 32927 – 5004 Len=1328
14 0.303950688	50..59..32..1	50..50..31..1	UDP	1370 32927 – 5004 Len=1328
15 0.325123493	50..59..32..1	50..50..31..1	UDP	1370 32927 – 5004 Len=1328
16 0.335247911	50..59..32..1	224..2..127..254	SADP/SDP	305 Announcement (v1)
17 0.344763261	50..59..32..1	50..50..31..1	MPEG TS	1370 PT=MPEG-II transport streams, SSRC=0x35D79E79, Seq=36271, Time=13800602267
18 0.364620382	50..59..32..1	50..50..31..1	MPEG TS	1370 PT=MPEG-II transport streams, SSRC=0x35D79E79, Seq=36272, Time=13800604043
19 0.384328328	50..59..32..1	50..50..31..1	MPEG TS	1370 PT=MPEG-II transport streams, SSRC=0x35D79E79, Seq=36273, Time=13800605820
20 0.404971362	50..59..32..1	50..50..31..1	MPEG TS	1370 PT=MPEG-II transport streams, SSRC=0x35D79E79, Seq=36274, Time=13800607596 [MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
21 0.423804937	50..59..32..1	50..50..31..1	MPEG TS	1370 video-stream [MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
22 0.443541743	50..59..32..1	50..50..31..1	MPEG	1370 video-stream
23 0.463278535	50..59..32..1	50..50..31..1	MPEG TS	1370 [MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
24 0.483023270	50..59..32..1	50..50..31..1	MPEG TS	1370 video-stream [MP2T fragment of a reassembled packet]
25 0.502755149	50..59..32..1	50..50..31..1	MPEG TS	1370 video-stream
26 0.521406749	50..59..32..1	50..50..31..1	MPEG TS	1370 PT=MPEG-II transport streams, SSRC=0x35D79E79, Seq=36280, Time=13800618157 Service Description Table (SDT) [MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
27 0.537332984	50..59..32..1	50..50..31..1	MPEG TS	1370 video-stream [MP2T fragment of a reassembled packet]
28 0.553259246	50..59..32..1	50..50..31..1	MPEG TS	1370 [MP2T fragment of a reassembled packet]
29 0.569186147	50..59..32..1	50..50..31..1	MPEG TS	1370 PT=MPEG-II transport streams, SSRC=0x35D79E79, Seq=36283, Time=13800622457 [MP2T fragment of a reassembled packet]

Remarque : Sur cette capture, on observe un échange entre le serveur et le serveur voisin cependant le service vidéo entre les sites avait été validé avec ACL entre le réseau public et le serveur. On ne dispose cependant pas de cette capture.

5. Conclusion

Le service vidéo est opérationnel. L'architecture supporte le streaming RTP/UDP à travers le WAN. Ce service servira de témoin pour valider l'efficacité de la Qualité de Service mise en place dans la section XI, notamment lors des tests de saturation de lien.

X : Filtrage (ACL)

1. Analyse

Conformément au cahier des charges, nous devons sécuriser les flux inter-réseaux et protéger les infrastructures critiques. Nous avons fait le choix technique de centraliser le filtrage sur le Routeur Interne.

Justification :

1. Centraliser les ACL sur le point de d'arrivée des VLANs permet un débogage plus rapide et une vision claire des flux internes.
2. Cela évite de modifier la configuration du Routeur Externe (ISR) qui est en lien direct avec le FAI (**Zone 0**), minimisant les risques d'erreur de configuration qui couperaient l'accès au backbone.
3. Le Routeur Interne est le seul à voir le trafic avant qu'il ne soit potentiellement translaté, permettant un filtrage sur les adresses IP privées.

2. ACL du LAN (Filtrage Interne)

Ces listes contrôlent le trafic entrant dans le routeur depuis les réseaux locaux.

2.1. Configuration Détailée

```
Routeur-Int-31# configure terminal

! Déjà défini avant mais nous la rappelons
Routeur-Int-31(config)# ip access-list extended ACL_PRIVE_IN
Routeur-Int-31(config-std-nacl)# permit udp any any eq bootps
Routeur-Int-31(config-std-nacl)# permit udp any any eq bootpc
Routeur-Int-31(config-std-nacl)# permit ip 192.168.31.0 0.0.0.63
150.150.32.0 0.0.0.255
Routeur-Int-31(config-std-nacl)# permit ip 192.168.31.0 0.0.0.255
50.50.31.0 0.0.0.255
Routeur-Int-31(config-std-nacl)# permit ip 192.168.31.0 0.0.0.255
50.50.32.0 0.0.0.255
Routeur-Int-31(config-std-nacl)# permit ip 192.168.31.0 0.0.0.255
150.150.31.0 0.0.0.255
Routeur-Int-31(config-std-nacl)# permit ip 192.168.31.0 0.0.0.255
192.168.31.0 0.0.0.255
Routeur-Int-31(config-std-nacl)# exit

Routeur-Int-31(config)# ip access-list extended ACL_PUBLIC_IN
! Interdire par sécurité l'accès au réseau Privé
Routeur-Int-31(config-std-nacl)# deny ip 150.150.31.0 0.0.0.255
192.168.31.0 0.0.0.255
Routeur-Int-31(config-std-nacl)# permit udp any any eq bootps
Routeur-Int-31(config-std-nacl)# permit udp any any eq bootpc

! Autoriser l'accès aux services du Serveur S31
Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.31.1 eq 22
Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.31.1 eq www
Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.31.1 eq domain
Routeur-Int-31(config-std-nacl)#permit udp 150.150.31.0 0.0.0.255
host 50.50.31.1 eq 5004
Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.31.1 eq ftp
Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.31.1 eq ftp-data

! Autoriser l'accès aux services du Serveur S32
Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.32.1 eq 22
```

```

Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.32.1 eq www
Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.32.1 eq domain
Routeur-Int-31(config-std-nacl)#permit udp 150.150.31.0 0.0.0.255
host 50.50.32.1 eq 5004
Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.32.1 eq ftp
Routeur-Int-31(config-std-nacl)#permit tcp 150.150.31.0 0.0.0.255
host 50.50.32.1 eq ftp-data

! Autoriser les échanges entre les réseaux publiques
Routeur-Int-31(config-std-nacl)# permit ip 150.150.31.0 0.0.0.255
150.150.32.0 0.0.0.255
Routeur-Int-31(config-std-nacl)#permit tcp any any established
Routeur-Int-31(config-std-nacl)#exit

! Application des ACLs aux interfaces
Routeur-Int-31(config)# interface Ethernet1/0
Routeur-Int-31(config-if)# ip access-group ACL_PUBLIC_IN in
Routeur-Int-31(config-if)# exit

Routeur-Int-31(config)# interface FastEthernet0/0.2
Routeur-Int-31(config-subif)# ip access-group ACL_PRIVE_IN in
Routeur-Int-31(config-subif)# exit

```

2.2. Justification par rapport au Cahier des Charges

- **Pourquoi `permit udp any any bootps/bootpc`** ? Le DHCP fonctionne par broadcast (255.255.255.255) avant que la machine n'ait une IP. Si l'ACL bloque ce trafic initial, la machine ne reçoit jamais d'IP et ne peut accéder à aucun réseau.
- **Gestion des Droits** : Dans `ACL_PRIVE_IN`, nous utilisons `0.0.0.63` pour la règle vers `150.150.32.0`. Cela restreint strictement l'accès au réseau public distant aux IP de `.1` à `.63`. En revanche, nous utilisons `0.0.0.255` (tout le sous-réseau) pour les règles vers les serveurs (`50.50.31.0` et `50.50.32.0`) et le public local. Cela garantit que tout le réseau privé peut accéder aux services critiques (DNS, Web, Vidéo), quel que soit le site.
- **Pourquoi `deny ip 150.150...`** ? Le réseau public est considéré comme une zone non fiable. Cette règle empêche tout client public de tenter une connexion vers le réseau privé, assurant la séparation entre les deux zones clients.

3. ACL vers le WAN (Filtrage Externe)

Cette ACL filtre le trafic entrant depuis le Routeur Externe vers le Routeur Interne. C'est la protection externe du site.

3.1. Configuration Détailée

```
Routeur-Int-31(config)# ip access-list extended ACL_SEC_IN
Routeur-Int-31(config-ext-nacl)# permit ospf any any
Routeur-Int-31(config-ext-nacl)# permit icmp any any
Routeur-Int-31(config-ext-nacl)# permit udp any any eq 5004
Routeur-Int-31(config-ext-nacl)# permit tcp any host 50.50.31.1 eq
www
Routeur-Int-31(config-ext-nacl)# permit udp any host 50.50.31.1 eq
domain
Routeur-Int-31(config-ext-nacl)# permit tcp any host 50.50.31.1 eq
ftp
Routeur-Int-31(config-ext-nacl)# permit tcp any host 50.50.31.1 eq
ftp-data
Routeur-Int-31(config-ext-nacl)# permit tcp any host 50.50.31.1 eq
22
Routeur-Int-31(config-ext-nacl)# permit ip any 150.150.31.0
0.0.0.255
Routeur-Int-31(config-ext-nacl)# permit tcp any any established
Routeur-Int-31(config-ext-nacl)# deny ip any any log
Routeur-Int-31(config-ext-nacl)# exit

Routeur-Int-31(config)# interface FastEthernet0/1
Routeur-Int-31(config-if)# ip access-group ACL_SEC_IN in
Routeur-Int-31(config-if)# exit
```

3.2. Justification par rapport au Cahier des Charges

- **Autorisation** : Nous autorisons explicitement les ports 80 (www), 53 (domain), 21 (ftp), 22 (ssh) et 5004 (vidéo) vers **50.50.31.1**. Cela permet aux utilisateurs distants d'accéder aux services hébergés sur S31. Nous autorisons également les flux ospf pour le routage dynamique ainsi que les flux icmp pour le débogage.
- **La règle permit tcp any any established** : Le cahier des charges implique que les clients internes doivent pouvoir accéder au WEB. Les ACLs classiques ne mémorisent pas l'état des connexions. Cette commande autorise le retour des paquets correspondant aux connexions initiées depuis l'intérieur (ex: réponse d'une page demandée par un client privé).
- **deny ip any any log** : L'option **log** facilite le débogage et permet de tracer les tentatives d'accès non autorisées (scans, attaques), facilitant l'audit de sécurité.

Remarque : L'ensemble des ACL sont des ACL nommées, cela permet de faciliter le débogage. Par exemple, on souhaite tester la connectivité entre le réseau public et privé. Par défaut, on bloque tous les flux entre ces réseaux et grâce aux ACLs nommées, on peut juste désactiver la ligne qu'on souhaite puis la remettre.

XI : Qualité de Service (QoS)

1. Analyse du Cahier des Charges

Le cahier des charges impose une contrainte sur le service vidéo : "*En cas de congestion des liens, ce service doit continuer à fonctionner.*" Sur un lien WAN (interconnexion avec le FAI), la bande passante est limitée. Si plusieurs utilisateurs lancent des téléchargements simultanés (FTP, Web), le lien peut saturer. Sans gestion de trafic, le routeur applique une politique FIFO (First-In, First-Out), traitant tous les paquets à égalité. Cela provoquerait pour la vidéo de la latence, de la gigue ou encore de la perte de paquets par exemple.

2. Justification de la Solution Technique

Pour répondre à ce besoin, nous mettons en place une stratégie de classification sur le routeur interne, avant de routeur vers le WAN.

2.1. Choix de la Méthode de Classification

Nous utilisons des ACLs étendues pour identifier les flux. Leur utilisation est plus rapide à configurer, consomme moins de ressources CPU sur le routeur et correspond aux méthodes que nous avons étudiées.

2.2. Stratégie de File d'Attente

Nous appliquons une stratégie qui établit la hiérarchie suivante :

1. **Priorité Absolue (Classe Vidéo)** : Le flux RTP ([UDP 5004](#)) est sensible au délai. Nous lui attribuons une file prioritaire stricte. Tant qu'il y a des paquets vidéo (dans la limite définie), ils passent avant tout le reste.
2. **Priorité Garantie (Classe Serveur et Privé)** : Les flux "métiers" ([SSH](#), [FTP](#), [Web interne](#)) et les utilisateurs du réseau privé sont importants. Nous leur réservons un pourcentage garanti de la bande passante restante. Ils ne sont pas prioritaires sur la vidéo, mais ils sont prioritaires sur le trafic "tout venant".
3. **Best Effort (Classe Default et Public)** : Le réseau public n'a aucune garantie. Il utilise la bande passante laissée libre par les autres classes.

3. Configuration Détailée

La configuration se déroule en trois étapes : Classification (ACL), Catégorisation (Class-Map) et Politique (Policy-Map).

3.1. Étape 1 : Classification des flux (ACL)

Nous définissons trois listes d'accès pour identifier le trafic.

```
Routeur-Int-31(config)# ip access-list extended ACL_QOS_VIDEO
Routeur-Int-31(config-ext-nacl)# permit udp any any eq 5004
Routeur-Int-31(config-ext-nacl)# exit

Routeur-Int-31(config)# ip access-list extended ACL_QOS_SERVEUR
Routeur-Int-31(config-ext-nacl)# permit ip 50.50.31.0 0.0.0.255
any
Routeur-Int-31(config-ext-nacl)# exit

Routeur-Int-31(config)# ip access-list extended ACL_QOS_PRIVE
Routeur-Int-31(config-ext-nacl)# permit ip 192.168.31.0 0.0.0.255
any
Routeur-Int-31(config-ext-nacl)# exit
```

3.2. Étape 2 : Création des Classes (Class-Map)

Nous associons les ACLs à des classes reconnues par le routeur.

```
Routeur-Int-31(config)# class-map match-all CLASS_VIDEO
Routeur-Int-31(config-cmap)# match access-group name ACL_QOS_VIDEO
Routeur-Int-31(config-cmap)# exit

Routeur-Int-31(config)# class-map match-all CLASS_SERVEUR
Routeur-Int-31(config-cmap)# match access-group name
ACL_QOS_SERVEUR
Routeur-Int-31(config-cmap)# exit

Routeur-Int-31(config)# class-map match-all CLASS_PRIVE
Routeur-Int-31(config-cmap)# match access-group name ACL_QOS_PRIVE
Routeur-Int-31(config-cmap)# exit
```

3.3. Étape 3 : Définition et Application de la Politique (Policy-Map)

C'est ici que nous définissons les règles de bande passante et le marquage DSCP.

```
Routeur-Int-31(config)# policy-map QOS
```

```

Routeur-Int-31(config-pmap)# class CLASS_VIDEO
Routeur-Int-31(config-pmap-c)# priority 2000
Routeur-Int-31(config-pmap-c)# set dscp ef
Routeur-Int-31(config-pmap-c)# exit

Routeur-Int-31(config-pmap)# class CLASS_SERVEUR
Routeur-Int-31(config-pmap-c)# bandwidth remaining percent 40
Routeur-Int-31(config-pmap-c)# set dscp cs3
Routeur-Int-31(config-pmap-c)# exit

Routeur-Int-31(config-pmap)# class CLASS_PRIVE
Routeur-Int-31(config-pmap-c)# bandwidth remaining percent 30
Routeur-Int-31(config-pmap-c)# set dscp cs2
Routeur-Int-31(config-pmap-c)# exit

```

3.4. Application sur l'interface WAN

La QoS n'a de sens qu'en cas de congestion sortante. Nous l'appliquons donc en sortie vers le routeur externe/FAI.

```

Routeur-Int-31(config)# interface FastEthernet0/1
Routeur-Int-31(config-if)# service-policy output QOS
Routeur-Int-31(config-if)# exit

```

4. Tests et Validation

Pour valider l'efficacité de la QoS, nous devons créer une situation de congestion.

Protocole de Test :

1. **État Initial** : Lancer une lecture vidéo via VLC (Client Public Site Distant → Serveur Site Local).
 - Observation : L'image est fluide.
2. **Création de Congestion** : Lancer un ping lourd (`ping -s 65000 -i 0 150.150.31.1`) depuis le Serveur vers un Client Public, qui va saturer la bande passante montante.
 - Observation SANS QoS : La vidéo pixelisée, se fige ou le son coupe.
 - Observation AVEC QoS : La vidéo reste parfaitement fluide. Le débit du ping diminue automatiquement pour laisser la place à la vidéo.

Vérification : La commande `show policy-map interface FastEthernet0/1` permet de voir les compteurs s'incrémenter dans les classes correspondantes.

```
Router-Int-31#sh policy-map int F0/1
FastEthernet0/1

Service-policy output: QOS

Class-map: CLASS_VIDEO (match-all)
 26527 packets, 36341990 bytes
 5 minute offered rate 506000 bps, drop rate 0 bps
Match: access-group name ACL_QOS_VIDEO
Queueing
  Strict Priority
  Output Queue: Conversation 264
  Bandwidth 2000 (kbps) Burst 50000 (Bytes)
  (pkts matched/bytes matched) 17/23290
  (total drops/bytes drops) 0/0
QoS Set
  dscp ef
  Packets marked 26528

Class-map: CLASS_SERVEUR (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name ACL_QOS_SERVEUR
Queueing
  Output Queue: Conversation 265
  Bandwidth remaining 40 (%) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
QoS Set
  dscp cs3
  Packets marked 0

Class-map: CLASS_PRIVE (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name ACL_QOS_PRIVE
Queueing
  Output Queue: Conversation 266
  Bandwidth remaining 30 (%) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
QoS Set
  dscp cs2
  Packets marked 0

Class-map: class-default (match-any)
 2697 packets, 3409306 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
Router-Int-31#
```

5. Conclusion

La mise en place de la QoS assure la résilience du service vidéo. Nous garantissons que même si le réseau public ou privé sature le lien WAN, les paquets vidéo seront toujours traités en priorité, respectant ainsi l'exigence de continuité de service du cahier des charges.

XII : Cahier de recettes

Ce cahier de recette a pour but de valider la conformité de l'infrastructure déployée vis-à-vis du cahier des charges. Chaque test suit la procédure suivante : rappel de l'objectif, tests, résultats, analyse et enfin conclusion.

1. Routage OSPF

Rappel de l'objectif : Assurer l'interconnexion entre les sites via le protocole OSPF, en respectant les zones (Area 0 pour le WAN, Area 31/32 pour le site local).

Tests :

- **Sous-test 1.1 :** Vérification des voisins OSPF sur le Routeur Interne.
 - Commande : `show ip ospf neighbor`
- **Sous-test 1.2 :** Vérification de la présence des routes du site voisin dans la table de routage.

- Commande : `show ip route ospf`
- **Sous-test 1.3 :** Test de connectivité (Ping) depuis un client du site 31 vers un client du site 32.
 - Commande : `ping 50.50.32.1` (Serveur) et `ping 150.150.32.1` (Client).

Résultats avec preuve :

- La commande affiche le voisin `131.131.131.131` (Routeur Externe) en état `FULL/DR`.

```
Router-Int-31#sh ip ospf neighbor

Neighbor ID      Pri  State            Dead Time    Address          Interface
131.131.131.131   1    FULL/DR        00:00:32    90.0.31.254    FastEthernet0/1
Router-Int-31#■
```

- Les réseaux du site voisin (ex: `90.0.32.0, 150.150.32.0`) apparaissent marqués par `0 IA` (OSPF Inter-Area).

```

Routeur-Int-31#sh ip route
Codes: 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
      i - IS-IS, su - IS-IS summary, 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 not set

```

      50.0.0.0/24 is subnetted, 2 subnets
C        50.50.31.0 is directly connected, FastEthernet0/0.1
0 IA    50.50.32.0 [110/53] via 90.0.31.254, 00:01:23, FastEthernet0/1
      32.0.0.0/32 is subnetted, 1 subnets
0 IA    32.32.32.32 [110/53] via 90.0.31.254, 00:05:12, FastEthernet0/1
C    192.168.31.0/24 is directly connected, FastEthernet0/0.2
      131.131.0.0/32 is subnetted, 1 subnets
0        131.131.131.131 [110/2] via 90.0.31.254, 04:02:40, FastEthernet0/1
      132.132.0.0/32 is subnetted, 1 subnets
0 IA    132.132.132.132 [110/52] via 90.0.31.254, 00:05:12, FastEthernet0/1
      31.0.0.0/32 is subnetted, 1 subnets
C        31.31.31.31 is directly connected, Loopback31
      90.0.0.0/24 is subnetted, 2 subnets
C        90.0.31.0 is directly connected, FastEthernet0/1
0 IA    90.0.32.0 [110/52] via 90.0.31.254, 00:05:12, FastEthernet0/1
      30.0.0.0/24 is subnetted, 1 subnets
0 IA    30.0.0.0 [110/51] via 90.0.31.254, 04:02:40, FastEthernet0/1
      150.150.0.0/24 is subnetted, 2 subnets
C        150.150.31.0 is directly connected, Ethernet1/0
0 IA    150.150.32.0 [110/62] via 90.0.31.254, 00:05:12, FastEthernet0/1
      31.0.0.0/32 is subnetted, 1 subnets

```

- Les pings inter-sites vers **150.150.32.1** (clients publiques) et **50.50.32.1** (S31) réussissent.

```

root@G30:~# ping 50.50.32.1 -c 1
PING 50.50.32.1 (50.50.32.1) 56(84) bytes of data.
64 bytes from 50.50.32.1: icmp_seq=1 ttl=60 time=4.57 ms

--- 50.50.32.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.569/4.569/4.569/0.000 ms

```

Analyse : L'état **FULL** confirme que les bases de données sont synchronisées. La présence de routes **IA** prouve que les LSA traversent correctement la zone Backbone (Area 0).

Conclusion : Le routage OSPF est opérationnel et conforme à l'architecture multi-zones.

2. Accessibilité des Services Serveur (Web, SSH, FTP)

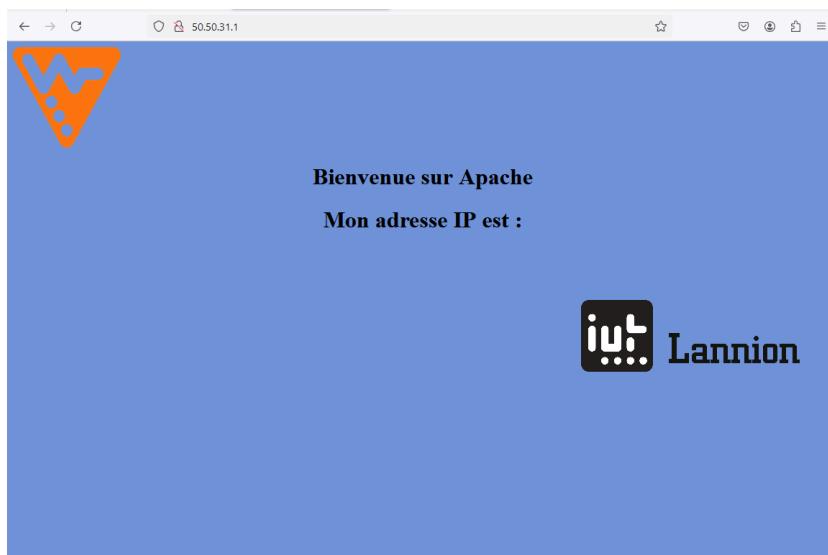
Rappel de l'objectif : La machine serveur S31 doit héberger les services Web, SSH et FTP, et ceux-ci doivent être accessibles tant depuis le LAN (Réseaux Public/Privé) que depuis le WAN (Site voisin) .

Tests :

- **Sous-test 2.1** : Accès HTTP depuis le client D31 (LAN Public).
 - Action : Ouvrir <http://50.50.31.1> dans un navigateur.
- **Sous-test 2.2** : Accès SSH depuis le site distant.
 - Commande : `ssh etu@50.50.31.1` (IP publique du serveur).
- **Sous-test 2.3** : Transfert de fichier via FTP.
 - Commande : `ftp 50.50.31.1` (Interne) et `ftp 50.50.32.1` (Externe).

Résultats avec preuve :

- **Web** : La page par défaut "Bienvenue sur Apache - Mon adresse IP est..." s'affiche correctement .



- **SSH** : Connexion réussie à l'utilisateur `etu`, obtention du prompt `etu@S31:~$` .

```
root@G31:~# ssh etu@50.50.31.1
etu@50.50.31.1's password:
Linux S31_tp311_iut 6.12.12+bpo-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.12-1+bpo12+1 (2025-02-23) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec 17 18:34:04 2025 from 150.150.31.1
etu@S31:~$
```

- **FTP** : Connexion réussie (Code 220/230), transfert du fichier `fichier_test.txt` réussi (Code 226 Transfer complete) .

```
root@G30:~# ftp 50.50.31.1
Connected to 50.50.31.1.
220 ProFTPD Server (Debian) [::ffff:50.50.31.1]
Name (50.50.31.1:root): etu
331 Mot de passe requis pour etu
Password:
230 Utilisateur etu authentifié
Remote system type is UNIX.
Using binary mode to transfer files.
```

```
ftp> put fichier_test.txt
local: fichier_test.txt remote: fichier_test.txt
229 Entering Extended Passive Mode (|||16700|)
150 Ouverture d'une connexion de données en mode BINARY pour fichier_test.txt
100% |*****| 7 189.88 KiB/s 00:00 ETA
226 Téléchargement terminé
7 bytes sent in 00:00 (4.65 KiB/s)
```

Analyse : Les services sont actifs et écoutent sur les bons ports. Les ACLs sont correctement configurés pour laisser passer ces flux spécifiques.

Conclusion : Les services Web, SSH et FTP sont fonctionnels et accessibles conformément aux CdC.

3. Serveur DHCP sur le Réseau Public

Rappel de l'objectif : Fournir une configuration IP dynamique (Adresse, Masque, Passerelle) aux clients du réseau Clients Publics via le serveur S31.

Tests :

- **Sous-test 3.1** : Renouvellement de l'adresse IP sur le client Windows D31 (Réseau Public).
 - Action : Désactiver puis réactiver l'interface de D31.
- **Sous-test 3.2** : Vérification des relais DHCP.
 - Preuve : Capture Wireshark montrant les messages DHCP (Discover/Offer) avec une adresse statique qui correspond au routeur.

Résultats avec preuve :

- **Adressage** : Le client D31 reçoit une IP dans la plage **150.150.31.x**, avec le suffixe DNS **site31.iut** et la passerelle **150.150.31.254**

```
C:\Users\root>ipconfig

Configuration IP de Windows

Carte Ethernet eth0 :

    Suffrage DNS propre à la connexion. . . . : site31.iut
    Adresse IPv6 de liaison locale. . . . . : fe80::3800:ab05:e590:7ec9%8
    Adresse IPv4. . . . . . . . . . . . . . . . : 150.150.31.1
    Masque de sous-réseau. . . . . . . . . . . : 255.255.255.0
    Passerelle par défaut. . . . . . . . . . . : 150.150.31.254
```

- **Wireshark** : On observe les paquets DHCP Discover relayés et l'offre (Offer) provenant de 50.50.31.1.

No.	Time	Source	Destination	Protocol	Length	Info
5102	6368.269438	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x64907b9d
5378	6702.261482	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x195bb06
5383	6703.268801	150.150.31.254	150.150.31.1	DHCP	342	DHCP Offer - Transaction ID 0x195bb06
5384	6703.270584	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x195bb06
5385	6703.279975	150.150.31.254	150.150.31.1	DHCP	342	DHCP ACK - Transaction ID 0x195bb06
5535	6717.511501	150.150.31.1	50.50.31.1	DHCP	342	DHCP Request - Transaction ID 0x1f7af36a
5536	6717.516309	50.50.31.1	150.150.31.1	DHCP	342	DHCP ACK - Transaction ID 0x1f7af36a

Analyse : Le serveur DHCP est correctement configuré pour le sous-réseau distant. Le Routeur Interne transfère bien les trames Broadcast vers le serveur en Unicast.

Conclusion : Le service DHCP assure l'adressage automatique du réseau Public.

4. Restriction d'Accès WAN (63 machines du privé)

Rappel de l'objectif : Seules les 63 adresses IP les plus basses du réseau Clients Privés (192.168.31.1 à .63) doivent pouvoir communiquer avec l'extérieur (Site voisin).

Tests :

- **Sous-test 4.1** : Ping vers l'extérieur depuis une IP statique autorisée (ex: 192.168.31.10).
- **Sous-test 4.2** : Ping vers l'extérieur depuis une IP de la plage DHCP (ex: 192.168.31.100, car plage DHCP commence à .64).
- **Sous-test 4.3** : Contrôle de la table de translation.

Résultats avec preuve :

- **Autorisé** : Le ping depuis une IP <.64 réussit et génère une entrée dans la table NAT (`show ip nat translations`).

```
Routeur-Int-31(config)#do sh ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
icmp 90.0.31.1:43568   192.168.31.1:43568 50.50.32.1:43568  50.50.32.1:43568
```

- **Refusé** : Le ping depuis une IP $\geq .64$ échoue ("Packet filtered). (Preuve : capture d'écran d'un ping échoué depuis une IP DHCP).

962 1521.7901691...	Cisco_23:39:81	Spanning-tree-(for-...	STP
963 1522.8284329...	192.168.31.100	150.150.31.1	ICMP
964 1523.7949573...	Cisco_23:39:81	Spanning-tree-(for-...	STP
965 1523.8394352...	192.168.31.100	150.150.31.1	ICMP
966 1525.7998308...	Cisco_23:39:81	Spanning-tree-(for-...	STP
967 1526.3244069...	192.168.31.100	150.150.32.1	ICMP
968 1526.3266722...	192.168.31.254	192.168.31.100	ICMP
969 1527.3259131...	192.168.31.100	150.150.32.1	ICMP
970 1527.3273318...	192.168.31.254	192.168.31.100	ICMP

```
root@G31:~# ping 150.150.32.1
PING 150.150.32.1 (150.150.32.1) 56(84) bytes of data.
From 192.168.31.254 icmp_seq=1 Packet filtered
From 192.168.31.254 icmp_seq=2 Packet filtered
From 192.168.31.254 icmp_seq=3 Packet filtered
^C
--- 150.150.32.1 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2003ms
```

Analyse : L'ACL filtre strictement les adresses sources éligibles au PAT. Les adresses non translatées sont jetées car non routables sur le WAN

Conclusion : La restriction d'accès est conforme : les clients DHCP (IP $> .63$) sont bloqués par défaut, seuls les postes fixes configurés en statique (IP $< .63$) accèdent au WAN.

5. Isolation des IPs Privées sur l'ISR (Routeur Externe)

Rappel de l'objectif :

Les routeurs de bordures (ISR) ne doivent jamais recevoir ou router de paquets avec des adresses sources privées.

Tests :

- **Sous-test 5.1** : Vérification de l'emplacement du PAT.
 - Vérification : Configuration du [Routeur-Int-31](#).
- **Sous-test 5.2** : Capture de trafic sur le lien entre Routeur Interne et Routeur Externe.

Résultats avec preuve :

- **Configuration** : Le PAT est configuré sur le Routeur Interne ([ip nat inside](#) sur l'interface Fa0/0.1, [ip nat outside](#) sur Fa0/1, Fa0/0.2 et Eth1/0).
- **Translation** : La table NAT montre que les IPs privées ([192.168.xx](#)) sont transformées en [90.0.31.1](#) avant de sortir vers les réseaux publics .

```

→ 2872 2039.9573307... 90.0.31.1      50.50.31.1      ICMP      98 Echo (ping) request id=0xe884, seq=1/256, ttl=63 (reply in 2873)
← 2873 2039.9573657... 50.50.31.1      90.0.31.1      ICMP      98 Echo (ping) reply id=0xe884, seq=1/256, ttl=64 (request in 2872)
2874 2040.9578351... 90.0.31.1      50.50.31.1      ICMP      98 Echo (ping) request id=0xe884, seq=2/512, ttl=63 (reply in 2875)
2875 2040.9578700... 50.50.31.1      90.0.31.1      ICMP      98 Echo (ping) reply id=0xe884, seq=2/512, ttl=64 (request in 2874)
2876 2041.5635195... Cisco_23:39:97    Nearest-Customer-Br... STP      60 Conf. Root = 32768/311/00:18:23:39:80 Cost = 0 Port = 0x8017
2877 2041.5635195... 90.0.31.1      50.50.31.1      PING     0100 PING R = 1 T = 1 L = 16 D = 32.811

> Frame 2872: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
> Ethernet II, Src: Cisco_42:f9:60 (00:0f:24:42:f9:60), Dst: HP_58:a5:c7 (d0:ad:08:58:a5:c7)
└ Internet Protocol Version 4, Src: 90.0.31.1, Dst: 50.50.31.1
  | 0100 .... = Version: 4
  | .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 84
  - Identification: 0xc36f (50031)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 63
  - Protocol: ICMP (1)
  - Header Checksum: 0xae05 [validation disabled]
  [Header checksum status: Unverified]
  - Source Address: 90.0.31.1
  - Destination Address: 50.50.31.1
  [Stream index: 4]
└ Internet Control Message Protocol
  - Type: Echo (ping) request (8)
  - Code: 0
  - Checksum: 0xa194 [correct]
  [Checksum Status: Good]
  - Identifier (BE): 59524 (0xe884)
  - Identifier (LE): 34024 (0x8e48)
  - Sequence Number (BE): 1 (0x0001)
  - Sequence Number (LE): 256 (0x0100)
  [Response frame: 2873]
> ICMP Data: 24845e699000000002a25020000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637

```

Remarque : Le projet nous demande une attention particulière à l'anonymisation des IP privés lorsqu'elle sort de leur réseau. On regarde sur la capture précédente un ping entre G31 (translaté en 90.0.31.1) et S31. L'adresse IP est traduite donc on ne peut pas trouver la source via la capture, même chose pour l'adresse MAC. Donc les 2 principaux moyens de trouver les adresses privées sont anonymisés.

Analyse : Puisque le PAT s'effectue sur le routeur interne, le routeur externe (ISR) ne verra que des adresses publiques (du réseau **90.0.31.0/24**). Il ne route aucune IP privée et ces dernières sont totalement masquées derrière l'IP **90.0.31.1**.

Conclusion : L'exigence d'isolation de l'ISR vis-à-vis de l'adressage privé est respectée.

6. Accès Réseau Privé via RADIUS

Rappel de l'objectif : Sécuriser l'accès physique au réseau Clients Privés. Aucun accès réseau ne doit être possible sans authentification .

Tests :

- **Sous-test 6.1 :** Brancher le client G31 sur le port du switch privé. Tenter un ping vers la passerelle.
- **Sous-test 6.2 :** Lancer le supplicant (**wpa_supplicant**) avec les identifiants corrects.
- **Sous-test 6.3 :** Tenter à nouveau le ping.

Résultats avec preuve :

- **Avant Auth :** Le ping échoue ("Destination Host Unreachable"). Le port est bloqué par le protocole 802.1X.

```

eth0: CTRL-EVENT-DSCP-POLICY clear_all
eth0: CTRL-EVENT-TERMINATING
root@G30:~# ping 192.168.31.254 -c 1
PING 192.168.31.254 (192.168.31.254) 56(84) bytes of data.
From 192.168.31.1 icmp_seq=1 Destination Host Unreachable

--- 192.168.31.254 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

root@G30:~# wpa_supplicant -D wired -c /etc/wpa_supplicant/mon_radius.conf -i eth0
Successfully initialized wpa_supplicant
eth0: Associated with 01:80:c2:00:00:03
eth0: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
eth0: CTRL-EVENT-EAP-STARTED EAP authentication started
eth0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=4
eth0: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 4 (MD5) selected
eth0: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
eth0: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 completed [id=0 id_str=]

```

Dans un même temps :

```

root@G30:~# ping 192.168.31.254
PING 192.168.31.254 (192.168.31.254) 56(84) bytes of data.
From 192.168.31.1 icmp_seq=10 Destination Host Unreachable
From 192.168.31.1 icmp_seq=11 Destination Host Unreachable
From 192.168.31.1 icmp_seq=12 Destination Host Unreachable
From 192.168.31.1 icmp_seq=13 Destination Host Unreachable
From 192.168.31.1 icmp_seq=14 Destination Host Unreachable
From 192.168.31.1 icmp_seq=15 Destination Host Unreachable
From 192.168.31.1 icmp_seq=16 Destination Host Unreachable
From 192.168.31.1 icmp_seq=17 Destination Host Unreachable
From 192.168.31.1 icmp_seq=18 Destination Host Unreachable

```

- **Pendant Auth** : Le supplicant affiche CTRL-EVENT-EAP-SUCCESS .

```

root@G30:~# wpa_supplicant -D wired -c /etc/wpa_supplicant/mon_radius.conf -i eth0
Successfully initialized wpa_supplicant
eth0: Associated with 01:80:c2:00:00:03
eth0: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
eth0: CTRL-EVENT-EAP-STARTED EAP authentication started
eth0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=4
eth0: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 4 (MD5) selected
eth0: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
eth0: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 completed [id=0 id_str=]

```

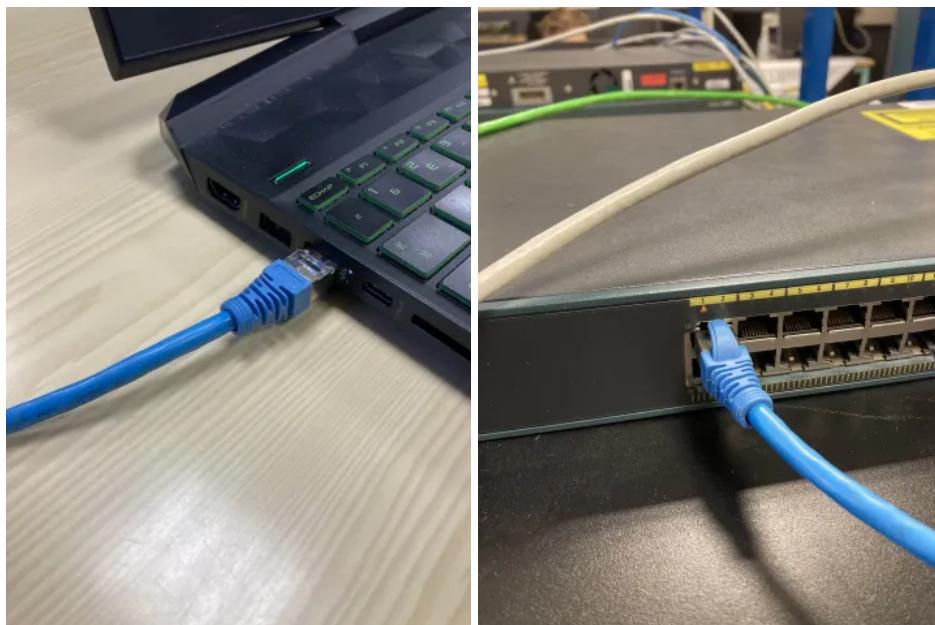
- **Après Auth** : Le ping vers la passerelle 192.168.31.254 réussit . Le switch affiche le port comme AUTHORIZED.

```
root@G30:~# ping 192.168.31.254
PING 192.168.31.254 (192.168.31.254) 56(84) bytes of data.
64 bytes from 192.168.31.254: icmp_seq=1 ttl=255 time=1.43 ms
64 bytes from 192.168.31.254: icmp_seq=2 ttl=255 time=1.48 ms
64 bytes from 192.168.31.254: icmp_seq=3 ttl=255 time=1.50 ms
^C
--- 192.168.31.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.432/1.472/1.500/0.029 ms
```

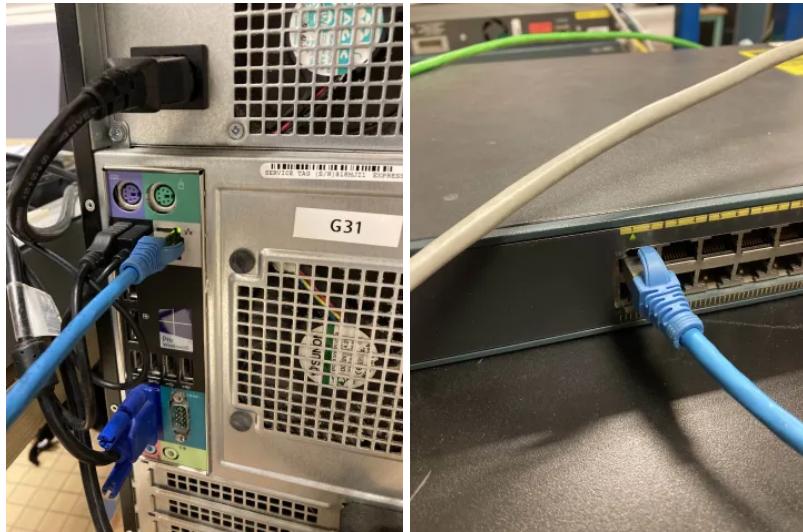
Analyse : Le switch bloque le trafic tant que le serveur RADIUS n'a pas validé les logins envoyés par le client/supplicant.

On peut également vérifier au niveau physique en branchant une machine autorisée et une non-autorisée:

En branchant une machine autorisé on voit que le voyant du switch passe bien au vert :



Tandis que, lorsqu'on branche une machine non autorisée, le voyant reste orange (image précédente) :



Ici, G31 est bien connecté et authentifié avec RADIUS donc le voyant est vert.

Conclusion : L'accès au réseau privé est strictement contrôlé par RADIUS.

7. Service Vidéo et QoS (Continuité de Service)

Rappel de l'objectif : Le service vidéo VLC doit être accessible depuis le réseau public distant et résister à la congestion grâce à une réservation de bande passante .

Tests :

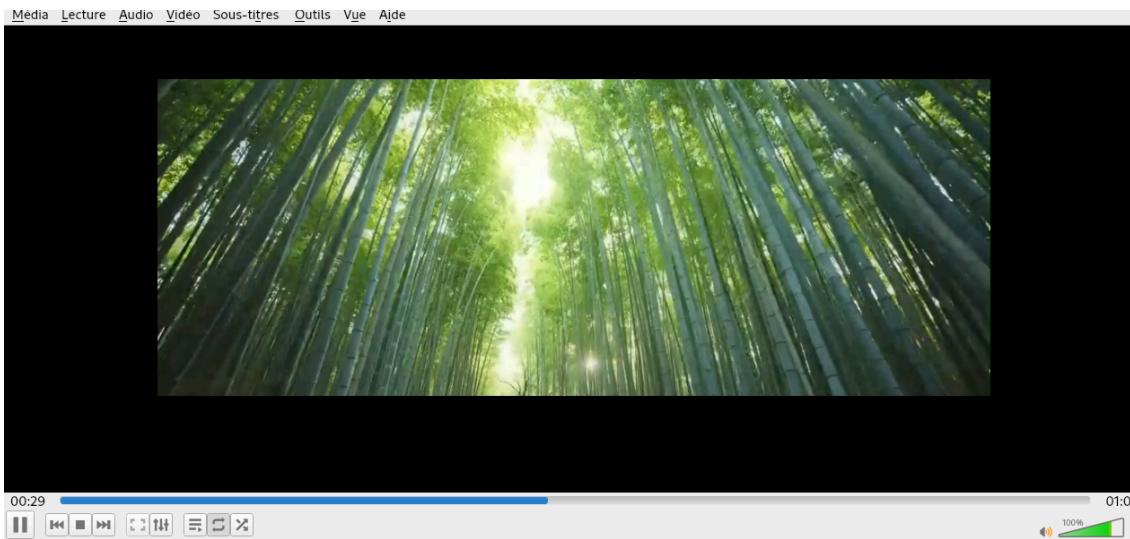
- **Sous-test 7.1 :** Diffusion d'une vidéo depuis S31 vers le client distant D32.
- **Sous-test 7.2 :** Lancement simultané d'un ping saturant le lien WAN.
- **Sous-test 7.3 :** Vérification de la politique QoS.
 - Commande : `show policy-map interface FastEthernet0/1`.

Résultats avec preuve :

- La vidéo est reçue sur D32, image fluide et son synchronisé. Capture Wireshark confirme le protocole MPEG-TS sur UDP .

No.	Time	Source	Destination	Protocol	Length	Info
1398..	68.488562566	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.488912226	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.489263211	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.489614284	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.489964594	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.490315560	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
1398..	68.490666518	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.491017454	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.491368664	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.491719614	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassembled packet]
1398..	68.492071567	50.50.31.1	150.150.31.1	MPEG TS	1370	video-stream Program Association Table (PAT)
1398..	68.492522761	50.50.31.1	150.150.31.1	MPEG TS	1370	PT-MPEG-II transport streams, SSRC=0x02CE57DE, Seq=61902, Time=2174295665 Program Map Table (PMT) Service Description
1398..	68.492883297	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.493349515	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.493761898	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.494198730	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.494637616	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]
1398..	68.495077848	50.50.31.1	150.150.31.1	MPEG TS	1370	[MP2T fragment of a reassembled packet]

- La vidéo reste fluide malgré la saturation du lien.



- La classe **CLASS_VIDEO** (UDP 5004) montre des paquets matchés et traités en priorité (**priority 2000**).

```
Router-Int-31#sh policy-map int F0/1
FastEthernet0/1

Service-policy output: QoS

Class-map: CLASS_VIDEO (match-all)
26527 packets, 36341990 bytes
5 minute offered rate 506000 bps, drop rate 0 bps
Match: access-group name ACL_QOS_VIDEO
Queueing
  Strict Priority
  Output Queue: Conversation 264
  Bandwidth 2000 (kbps) Burst 50000 (Bytes)
  (pkts matched/bytes matched) 17/23290
  (total drops/bytes drops) 0/0
QoS Set
  dscp ef
  Packets marked 26528

Class-map: CLASS_SERVEUR (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name ACL_QOS_SERVEUR
Queueing
  Output Queue: Conversation 265
  Bandwidth remaining 40 (%) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
QoS Set
  dscp cs3
  Packets marked 0
```

```
Class-map: CLASS_VIDEO (match-all)
26527 packets, 36341990 bytes
5 minute offered rate 506000 bps, drop rate 0 bps
Match: access-group name ACL_QOS_VIDEO
Queueing
  Strict Priority
  Output Queue: Conversation 264
  Bandwidth 2000 (kbps) Burst 50000 (Bytes)
  (pkts matched/bytes matched) 17/23290
  (total drops/bytes drops) 0/0
QoS Set
  dscp ef
  Packets marked 26528
```

Analyse : La configuration QoS (**priority 2000** pour la vidéo) garantit que les paquets vidéo passent avant le reste du trafic lors de la congestion.

Conclusion : Le service vidéo est fonctionnel et la QoS assure sa continuité en cas de charge réseau.

8. Sécurité du Réseau Serveur (ACL)

Rappel de l'objectif : Contrôler l'accès au réseau Serveurs Publics pour n'autoriser que les flux strictement nécessaires (Web, SSH, FTP, DNS, Vidéo) et protéger les performances et le serveur.

Tests :

- **Sous-test 8.1** : (Validé par les tests précédents : Web, SSH, FTP, Vidéo fonctionnent).
- **Sous-test 8.2** : Tentative de connexion sur un port non ouvert (ex: Telnet)
- **Sous-test 8.3** : Tentative d'accès au réseau Privé depuis le réseau Public.

Résultats :

- **Interdictions** : Le trafic non explicitement autorisé par les ACLs (`ACL_PUBLIC_IN`, `ACL_SEC_IN`) est bloqué par la règle implicite ou explicite `deny ip any any`.
- **Isolation** : Un ping du réseau Public (150.150.x) vers le Privé (192.168.x) est bloqué par la règle `deny ip 150.150.31.0... 192.168.31.0...`.

Analyse : Les ACLs appliquées sur le Routeur Interne filtrent le trafic pour minimiser le traitement inutile en étant proche des sources et sécuriser les zones critiques.

Conclusion : Le contrôle d'accès est conforme au CdC et sécurise le réseau serveur.

XIII : Conclusion

Ce projet a permis de déployer une architecture réseau inter-sites répondant aux exigences du cahier des charges.

L'infrastructure mise en place possède une séparation des différents réseaux via des VLANs et une interconnexion inter-site via le routage dynamique OSPF. Les services réseaux DHCP et DNS et les services Web, SSH et FTP sont opérationnels et accessibles selon les politiques de sécurité définies dans le cahier des charges.

La sécurité du réseau a été traitée à travers plusieurs mécanismes :

- Authentification 802.1x via RADIUS pour le réseau privé.
- ACLs sur le routeur interne protégeant le serveur et isolant les réseaux clients.
- NAT/PAT garantissant qu'aucune adresse privée ne transite sur le WAN, avec une restriction spécifique aux 63 premières IP du réseau privés.

Enfin, la mise en œuvre de la Qualité de Service (QoS) avec une file prioritaire a permis de maintenir la fluidité du service vidéo en situation de congestion du lien WAN. L'ensemble des tests validés dans le cahier de recette confirme la conformité de la maquette avec le cahier des charges.

Cependant, la maquette contient certaines limites :

L'usage de protocoles en clair (FTP, HTTP, TELNET) expose les données et les identifiants à des risques d'interception (Sniffing) ou d'attaque de l'homme du milieu (Man-in-the-Middle). Une migration vers des protocoles chiffrés (SFTP, HTTPS) permettrait dans un environnement de production de garantir la confidentialité de bout en bout.

L'architecture repose sur des liens WAN uniques, créant des points de défaillance uniques. La perte de ce lien entraîne l'isolement total du site. Bien que l'augmentation des accès (on parle ici de redondance des points d'accès) permettrait de régler ce problème, mais elle augmenterait la surface d'attaque potentielle, nécessitant un durcissement au niveau de la sécurité des configurations des routeurs de bordure.

XIV : Annexe

Rapport hebdomadaire N°1 | Semaine 42 | 4h (TD+TP)

1. Objectifs de la semaine

- Analyse du cahier des charges
- Répartition des binômes par postes
- Maquette et câblage de cette dernière

2. Réalisations

- **Répartition des binômes :**
 - XXXX et XXXX s'occupent du poste 31 et Erwann et XXXX s'occupent du poste 32.
 - Liste des services à mettre en place ainsi que l'ordre de mise en place et création d'une maquette (schéma de dépannage et schéma logique).
- **Infrastructure :**
 - Câblage à partir de la maquette.
 - Test de connectivité sous la configuration avec des adresses statiques et les VLANs

3. Problèmes Rencontrés et Solutions

Problème	Cause	Solution
X	X	X

4. Répartition des tâches :

Binôme	Tâche Durée
Erwann et XXXX	Répartition des binômes, analyse du CdC, création du schéma de dépannage 2h configuration IP des machines et des routeurs 30min VLANs sur les switchs 1h Début OSPF (cf planification) 30 min
XXXX et XXXX	Répartition des binômes, analyse du CdC, création du schéma de dépannage 2h configuration IP des machines et des routeurs 30min VLANs sur les switchs 1h Début OSPF (cf planification) 30 min

5. Planification

A faire avant la prochaine semaine : Préparer les différents configuration OSPF qu'on peut réaliser

Objectif prochaine semaine :

Configuration du protocole OSPF multi-zones.

Validation de la communication inter-sites.

Rapport hebdomadaire N°2 | Semaine 43 | 2h (TP)**1. Objectifs de la semaine**

Configuration du protocole OSPF multi-zones et du NAT/PAT.

Validation de la communication inter-sites.

2. Réalisations**• OSPF :**

- Configuration du `router ospf 31` sur le routeur interne et `router ospf 131` sur le routeur externe.
- Déclaration de la `zone 31` pour le LAN et connexion à la `zone 0` via le routeur externe.

• NAT/PAT :

- Configuration du NAT statique pour le serveur et configuration du PAT dynamique pour le réseau client privé

• Interface:

- Configuration des interfaces de Loopback

• Tests :

- Ping entre les PC des 2 sites pour valider la connectivité

• Préparation :

- Récupération les fichiers de configuration de base des services DNS, DHCP et WEB
- Récupération des "`sh run`"

3. Problèmes Rencontrés et Solutions

Problème	Cause	Solution
Les réseaux privés étaient partagés entre les routeurs.	On les avait déclarés avec la commande <code>network</code> ce qui active leurs annonces.	On retire la ligne correspondant à leurs déclarations.

4. Répartition des tâches :

Binôme	Tâche
Erwann et XXXX	Configuration de la dernière séance 30 min Configuration OSPF 30min Test et validation avec correction 15 min Configuration du NAT et du PAT 30min Test et validation avec correction 15 min
XXXX et XXXX	Configuration de la dernière séance 45 min

	activation des services (apache2, ssh, ftp) 5 min Configuration OSPF 30min Test et validation avec correction 15 min
--	--

5. Planification

A faire avant la prochaine semaine : Préparer les fichiers de configuration des services DHCP et DNS.

Objectif prochaine semaine : Installation et configuration des services DHCP, WEB, DNS.

Rapport hebdomadaire N°3 | Semaine 45 | 4h (TP)

1. Objectifs de la semaine

Installation et configuration des services DHCP, WEB, DNS.

2. Réalisations

- **DHCP :**
 - Configuration des plages d'adresses
 - Configuration des routeurs en relais DHCP
- **WEB :**
 - Démarrage du service apache2 et test local et distant (avec le site voisin)
- **DNS :**
 - Configuration des zones locales (direct et inverse)
- **Préparation :**
 - Récupération des fichiers de configurations de SSH, ProFTPD et FreeRadius

3. Problèmes Rencontrés et Solutions

Problème	Cause	Solution
Le serveur DHCP Il manquait la déclaration du sous-réseau du serveur pour l'interface locale.	refusait de démarrer. (50.50.31.0) dans le fichier de configuration.	Ajout d'un bloc subnet vide pour l'interface locale.
Routage ne fonctionnait pas sur le site 31.	2 câbles défectueux (malgré les led allumées).	Changement des câbles.

4. Répartition des tâches :

Binôme	Tâche
Erwann et XXXX	Configuration de la dernière séance 30 min Etablissement de la logique du DNS (arborescence) 30min Configuration du DNS 1h30 Configuration du WEB 30min

	Test et validation avec correction si nécessaire 30min Récupération des fichiers de configuration 30min
XXXX et XXXX	Configuration de la dernière séance 50 min Découverte et résolution problème sur le routage (lié au câble) 30min Test de vérification 20 min DHCP 30 min

5. Planification

A faire avant la prochaine semaine : Préparer les fichiers de configuration des services SSH, FTP et RADIUS.

Objectif prochaine semaine : Mise en place des services SSH, FTP et RADIUS.

Rapport hebdomadaire N°4 | Semaine 46 | 4h (TP)

1. Objectifs de la semaine

Mise en place des services SSH, FTP et RADIUS.

2. Réalisations

- **SSH et FTP :**
 - Création utilisateur 'etu'.
 - Test connexion SSH et transfert FTP depuis le site distant.
- **RADIUS :**
 - Configuration du Switch, du serveur FreeRadius et du supplicant (G31)
 - Test de l'authentification du supplicant

3. Problèmes Rencontrés et Solutions

Problème	Cause	Solution
L'authentification ne fonctionnait pas avec l'erreur "Cleartext: ... invalid"	Il faut que le fichier autorize soit mis à jour (il contient pour notre cas la même chose que user).	dans certains cas relancer le service sinon remplacer le contenu d'autorize par celui de users.
Le service ProFTPD ne voulait pas démarrer.	Le service ne connaît pas/plus l'attribut IdentLookups qui est présent dans le fichier proftpd.conf.	On commente cette ligne avec un #.

4. Répartition des tâches :

Binôme	Tâche

Erwann et XXXX	Configuration de la dernière séance 30 min Préparation de la configuration du service radius (réflexion de la manière de faire et du “comment”) 30min Configuration du serveur Radius, du Switch et du Supplicant 2H Test et validation avec correction si nécessaire 1h
XXXX et XXXX	Configuration de la dernière séance 45 min Finalisation DHCP 50 min Test des services ssh, ftp et web 40 min Test 30 min

5. Planification

A faire avant la prochaine semaine : Préparation des ACLs

Objectif de la prochaine semaine : Réaliser les ACLs permettant d'aller vers le WAN (donc l'autre site)

Rapport hebdomadaire N°4 | Semaine 47 | 4h (TP + TD)

1. Objectifs de la semaine

Rapport de mi projet avec établissement du point d'avancement
Mise en place des ACL

2. Réalisations

- Compte Rendu :** Récapitulation de notre avancement en réalisant un tableau To-Do-List (cf annexe de ce rapport hebdomadaire).
- ACL WAN :** Création d'une ACL étendue pour protéger le serveur des accès extérieurs
- PAT/NAT :** Mise en place d'un NAT statique vers le serveur et d'un PAT dynamique pour le réseau privé.
- Application :** Placement des `ip access-group` sur les interfaces du routeur.

3. Problèmes Rencontrés et Solutions

Problème	Cause	Solution
Plus d'accès à l'autre site (WEB et autre) depuis le LAN après activation de l'ACL WAN.	Le trafic de retour (réponse du site web) était bloqué.	Ajout des règles <code>permit tcp any any established</code>

4. Répartition des tâches :

Binôme	Tâche
Erwann et XXXX	Compte rendu intermédiaire et réalisation du tableau To-Do-List 2h

	Configuration de la dernière séance 30 min Configuration du routeur pour configurer les ACL WAN 45min Test et validation avec correction si nécessaire 45min
XXXX et XXXX	Compte rendu intermédiaire et réalisation du tableau To-Do-List 2h Configuration de la dernière séance 45 min DNS 30 min Test 10 min

5. Planification

A faire avant la prochaine séance : Préparer les ACLs internes, récupérer une vidéo à partager pour le serveur VLC, Prendre en compte la procédure de démarrage du service VLC (client et serveur).

Objectif de la prochaine séance :

Mettre en place le service VLC.

Finaliser les tests des ACLs en fonction des services SSH, WEB, FTP et DNS.

5. Annexe

to do	in progress	finish
ACL LAN Schéma logique Service vidéo Test et résultat + explication Justification des décision prise Cahier de recette (conforme à la maquette)	DNS, RADIUS NAT statique PAT dynamique ACL vers le wan	schéma de dépannage DHCP routage INT et EXT avec OSPF switch public switch privé avec Vlan Service Apache, FTP, SSH

Rapport hebdomadaire N°5 | Semaine 48 | 4h (TP)

1. Objectifs de la semaine

Mettre en place le service VLC.

Finaliser les tests des ACLs en fonction des services SSH, WEB, FTP et DNS.

2. Réalisations

- **VLC:**
 - Configuration du serveur vidéo et test avec la vidéo préparé puis avec la vidéo d'un autre groupe entre les serveurs et les PC clients.
- **ACL WAN:**
 - Configuration des ACLs sur le routeur intérieur.
 - Test des ACLs pour assurer l'échange des services (SSH, FTP, DNS et WEB).
- **DNS:**

- Créations des fichiers de configuration DNS (zone direct, zone inverse, résolutions, options)

3. Problèmes Rencontrés et Solutions

Problème	Cause	Solution
La vidéo ne marche pas lorsqu'on la diffuse sur un autre ordinateur du site voisin.	Le codage de la vidéo empêche la retransmission sur S31.	On a changé notre vidéo par la vidéo d'un autre poste.
Notre groupe passe de 4 à 3.	XXXX quitte la formation et donc le projet.	La répartition des binômes ne change pas. Erwann s'occupera seul de son poste.
DNS : Résolution inverse et du site voisin ne fonctionnaient pas.	Erreur dans les options.	Modifications des options/correction des erreurs.

4. Répartition des tâches :

Binôme	Tâche
Erwann	Configuration de la dernière séance 30 min Configuration du routeur pour configurer les ACL WAN 30min Test et validation avec correction si nécessaire 1h30 Configuration du service VLC 30 min Test et correction 1h
XXXX et XXXX	Configuration de la dernière séance 45 min Configuration DNS 1h Test et dépannage 30 min Début du CR 1h

5. Planification

A faire avant la prochaine semaine : Crédit d'ACL pour filtrer le LAN, Transposition des ACL numérotée vers des ACL nommés.

Objectif prochaine semaine :

Finalisation des ACLs
Séparation des réseaux Privé et Public
Passage des ACLs numéroté à des ACL nommées

Rapport hebdomadaire N°6 | Semaine 49 | 6h (TP)

1. Objectifs de la semaine

Finalisation des ACLs
Séparation des réseaux Privé et Public

Passage des ACLs numéroté à des ACL nommées

2. Réalisations

- **ACL LAN :** Isolation des réseaux Public/Privé.
 - Filtrage des paquets qu'on n'utilise pas dans le réseau en autorisant SSH, FTP, WEB, DNS, DHCP, etc.
- **DNS:** Correction des fichiers de configuration.
 - Correctif pour la résolution inverse et le serveur DNS du site voisin.

3. Problèmes Rencontrés et Solutions

Problème	Cause	Solution
Le DHCP ne passait plus après application de l'ACL LAN.	L'ACL bloquait le trafic UDP entrant sur l'interface, dont le retour du serveur DHCP.	Ajout de la règle <code>permit udp any any eq bootpc/bootps</code> .

4. Répartition des tâches :

Binôme	Tâche
Erwann	Configuration de la dernière séance 30 min Configuration du routeur pour configurer les ACL LAN 30min Test et validation avec correction si nécessaire 1h30 Passage en ACL nommés 30 min Test et correction 1h
XXXX et XXXX	Configuration de la dernière séance 45 min Finalisation DNS 45 min Test DNS 15 min Mise en place serveur vidéo 30 min Test VLC 30 min Avancement du CR 1h

5. Planification

A faire avant la prochaine semaine : Préparer les commandes de configuration pour la QoS et les fichiers de configurations pour le DNS forwarding

Objectif de la prochaine semaine :

Mettre en place la QoS et la tester en partageant une vidéo via le serveur VLC
Mettre à jour les fichiers du DNS pour faire du forwarding entre les sites.

Rapport hebdomadaire N°7 | Semaine 51 | 6h (TP)

1. Objectifs de la semaine

Mettre en place la QoS et la tester en partageant une vidéo via le serveur VLC
Mettre à jour les fichiers du DNS pour faire du forwarding entre les sites.

2. Réalisations

- **QoS:**
 - Marquage des paquets en fonctions de leur protocol et de leur source (serveur>privé>public/reste)
 - Mise en place des priorité pour respecter le cahier des charges
- **DNS (forwarding):**
 - Mettre à jours des configurations, teste inter site en accédant au site web via l'URL

3. Problèmes Rencontrés et Solutions

Problème	Cause	Solution
Le DNS forwarding partait mais n'arrivait pas à destination.	Les ACL bloquaient le DNS forwarding.	On a ajouté la règle pour autoriser le DNS

4. Répartition des tâches :

Binôme	Tâche
Erwann	Configuration de la dernière séance 30 min Configuration du routeur pour configurer la QoS 1h Test et validation 1h Mise au point de l'avancement et de la correspondance avec le cahier des charges 1h30
XXXX et XXXX	Configuration de la dernière séance 45 min Captures et test pour le Compte Rendu 2h15

5. Planification

A faire avant la prochaine semaine :

Finaliser le Rapport et réaliser une liste des tests à réaliser.

Objectif de la prochaine semaine :

Finaliser les dernières captures

Valider le projet

Rapport hebdomadaire N°8 | Semaine 2 | 4h (TP + validation)

1. Objectifs de la semaine

Finaliser les dernières captures

Valider le projet

2. Réalisations

- **NAT/PAT :**

- Suppression du NAT statique
- Déplacement du PAT dynamique sur l'interface directe du réseau privé.

3. Problèmes Rencontrés et Solutions

Problème	Cause	Solution
Le NAT statique n'a pas lieu d'être car le serveur a déjà une adresse publique.	Mauvaise compréhension de notre part.	Supprimer le NAT, corriger le CR avec l'adresse public du serveur
Les adresses privées arrivait sur les réseaux locaux serveur et publiques	Mauvaise compréhension de notre part.	Déplacer le PAT sur l'interface directe des réseaux, mettre à jour les ACL permettant le NAT

4. Répartition des tâches :

Binôme	Tâche
Erwann	Préparation captures 2h Validation 1h Correction 1h
XXXX et XXXX	Préparation et captures 2h Validation 1h Correction 1h

5. Planification

A faire avant la prochaine semaine : Finir et rendre les rapport avec les sources (script de commande, captures)

