Rhassef
Ayoub
BTS SIO 1

Compte rendu de validation de compétences

AP4 – GSBVélanne

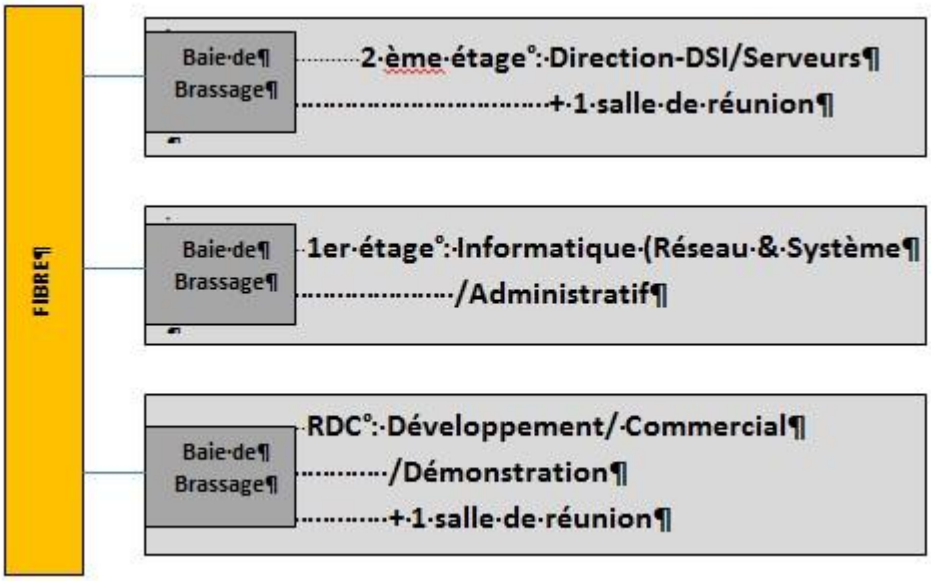
22/04/2025 - 27/05/2025

Equipier : MEJBOUR Merwan, Kassous Yamina

1. Présentation du contexte d'entreprise

L'entreprise GSB souhaite établir un plan d'adressage réseau visant à cloisonner celui-ci. Cette entreprise possède plusieurs étages avec différentes salles et services ainsi qu'un serveur pour le moment. Les salles doivent pouvoir communiquer avec le serveur mais ne peuvent communiquer entre elles. Chaque étage dispose d'une baie de brassage qui le relie par une fibre à la baie centrale de la salle serveurs.

L'entreprise souhaite que l'on maquette le projet afin de valider leur étude projet. Le bâtiment de l 'entreprise est organisée comme ceci :



2. Objectifs attendus

Différents objectifs sont attendus :

- Etablissement du tableau de plan d'adressage
- Réalisation d'un schéma réseau
- Création de VLAN
- Mise en place d'un routage Inter Vlan
- Elaboration d'ACL (Access Control List)
- Sauvegarde des données et de la configuration du serveur

- Liaison d'un Active Directory (Serveur) aux VLAN
- Tests à réaliser

3. Plan de travail

Concernant l'organisation les taches ont été dispatchées par le chef de projet au collaborateur.

Plan de travail :

A.1 Réalisation du schéma réseau

Concevoir le schéma réseau logique de votre solution répondant au cahier des charges. Vous pourrez utiliser les outils tels que Visio Packet Tracer ou tout autre outil de conception.

A.2 Mise en place de l'accès distant SSH

A.3 Création des Vlans

Paramétrer individuellement les différents switchs en respectant le cahier des charges et les informations de nommage fournies.

A.4 Routage InterVlan

Assurer la communication des différents services autorisés vers le serveur

A.5 Tests

Élaborer Réaliser l'ensemble des tests nécessaires à la validation de la solution proposée.

A.6 Réalisation des ACL

Réalisation des règles d'accès aux différentes zones

A.7 Sauvegarde

Réaliser l'ensemble des sauvegardes nécessaires

4. Réalisation

1. Tableau du plan d'adressage

N° VLAN	*Service(s)*	*Adressage IP*
10	Réseau & Système	192.168.10.0/24
20	Direction-DSI	192.168.20.0/24
30	Administratif	192.168.30.0/24
40	Commercial	192.168.40.0/24
50	Développement	192.168.50.0/24
150	Visiteurs	192.168.150.0/24
200	Démonstration	192.168.200.0/24
300	Serveurs	200.200.25.0/16

➔ Les switchs

Nom	**VLAN 10**	**VLAN 20**	**VLAN 30**	**VLAN 40**	**VLAN 50**	**VLAN 150**	**VLAN 200**	**VLAN 300**	**IP DU VLAN10**
Switch2		Fa0/1 -20				Fa0/2 4		Fa0/21 -23	192.168.10.25 3
Switch1	Fa0/1 -12		Fa0/13 -24						192.168.10.25 2
SwitchRD C				Fa0/1 -7	Fa0/8 -14	Fa0/2 4	Fa0/15 -23		192.168.10.25 1

➔ Le routeur

Interface/sous interface	**Adresse IP**
Gi0/0.10 (Vlan 10)	192.168.10.254/24
Gi0/0.20 (Vlan 20)	192.168.20.254/24
Gi0/0.30 (Vlan 30)	192.168.30.254/24
Gi0/0.40 (Vlan 40)	192.168.40.254/24
Gi0/0.50 (Vlan 50)	192.168.50.254/24
Gi0/0.150 (Vlan 150)	192.168.150.254/24
Gi0/0.200 (Vlan 200)	192.168.200.254
Gi0/0.300 (Vlan 300)	200.200.25.0/16

Masque : 255.255.255.0

➔ Les postes / serveurs

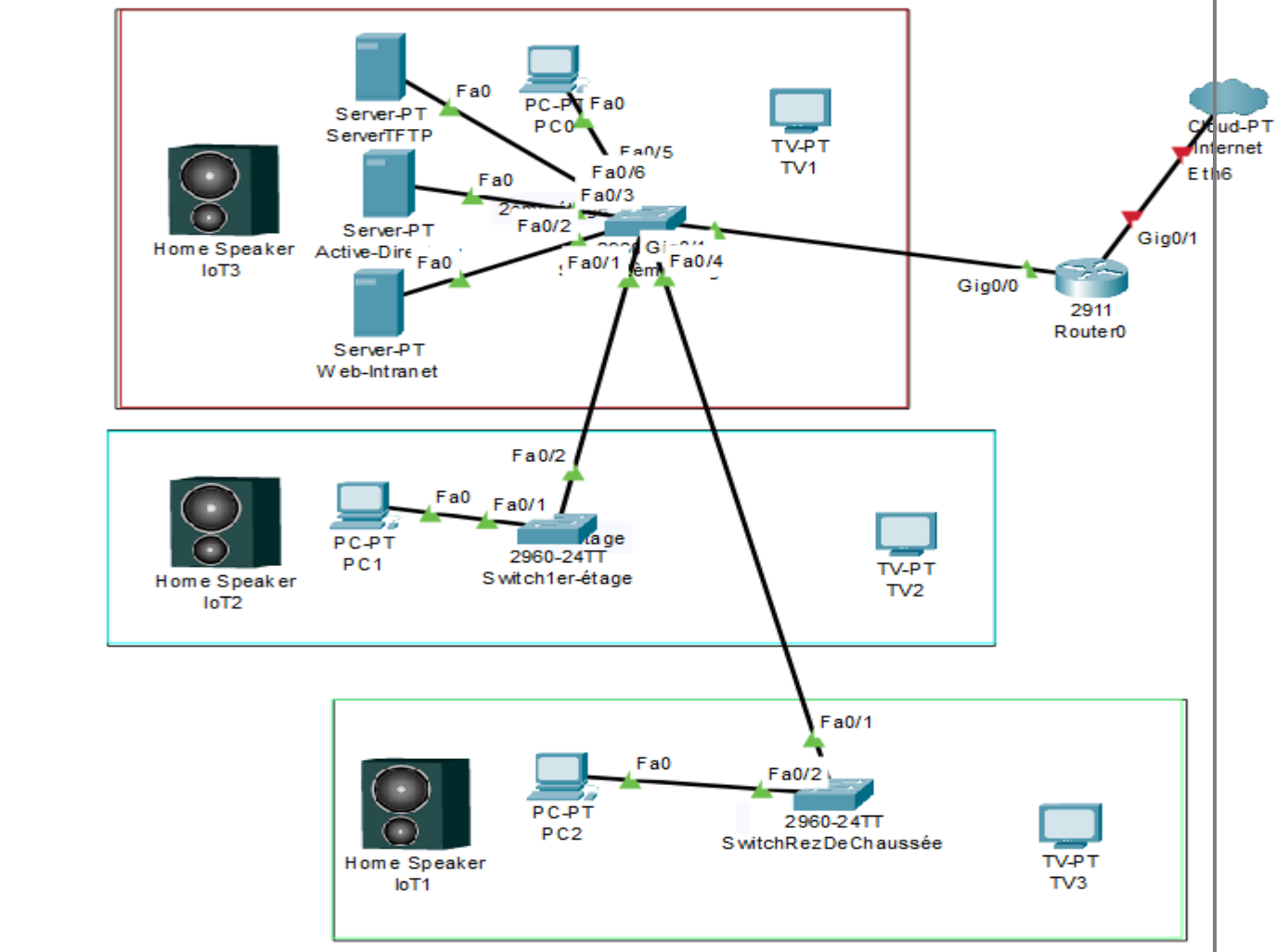
Nom	**Adresse IP**
ServeurTFTP	200.200.25.6/24
ServeurDHCP	200.200.25.1/24
PosteWEBINTRANET	200.200.25.3/24

PosteDSI	192.168.20.1
PosteINFO	192.168.10.2
PosteINFOstagiaire	192.168.10.1
PosteADMINI	192.168.30.1
PosteCOMMERCIAL	192.168.40.1
PosteVISITEUR1	192.168.150.1
PosteVISITEUR2	192.168.150.1
Poste DEV	192.168.50.1
Poste DEMO	192.168.200.1

Masque : 255.255.255.0

Schéma réseau

Voici le schéma réseau qui illustre cet AP au mieux.



Configuration des ports en mode trunk

Avant de pouvoir passer à l'étape 2 nous allons devoir configurer des ports en mode trunk.
Mise en port trunk du switch 2etage via la gi 0/1 vers le routeur, faire des no shutdown pour activer le port.

```
2etage#conf t
Enter configuration commands, one per line.
2etage(config)#int gi0/1
2etage(config-if)#switchport mode trunk
2etage(config-if)#no sh
2etage(config-if)#end
2etage#
```

Mise en port trunk le switch 2etage via l'interface gi 0/2 vers le switch 1etage

```
2etage(config)#int gi 0/2
2etage(config-if)#switchport mode trunk
2etage(config-if)#no s
```

Mêmes étapes réalisée avec le switch 1 étage.

```
1etage(config)#int gi 0/1
1etage(config-if)#switchport mode trunk
1etage(config-if)#no sh
1etage(config-if)#end
```

Nous avons activé l'interface gi 0/0 du Routeur en mettant en shutdown.
Vérification des interfaces en port trunk pour l'étage 2.

Configuration des switch en vtp

Mise en place du VTP sur les Switchs afin de permettre par la suite que tous les switch prennent en compte les VLANs qui seront crées
Le switch 2etage sera en en vtp mode server et le switch 1etage et rdc seront en vtp mode client

```
2etage#sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : GSB
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 8875.56f3.7c80
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 172.17.225.253 on interface Vl1 (lowest numbered VLAN interf
ace found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0xB3 0x3E 0xC3 0x6A 0x82 0x0C 0x59 0x07
                                    0x68 0xDA 0x03 0xD3 0x92 0xB3 0xCD 0x41
*** MD5 digest checksum mismatch on trunk: Gi0/2 ***
```

```
1etage#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : GSB
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00bf.77c5.f400
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
Configuration Revision          : 0
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                  0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC
*** MD5 digest checksum mismatch on trunk: Gi0/1 ***
```

2. Création des VLAN

Attribution d'un numéro de VLAN, en leur donnant un nom, en fonction de la demande de segmentation de GSB (cf : tableau segmentation)

Pour créer une Vlan il faut lui donné un numéro et un nom Création de VLAN 20 :

```
2etage#conf t
Enter configuration commands, one per li
2etage(config)#vlan 20
2etage(config-vlan)#name Direction_DSI
2etage(config-vlan)#end
```

Création de VLAN 50 /VLAN 150 / VLAN 200

```
2etage(config)#vlan 50
2etage(config-vlan)#name Developpement
```

```
2etage(config-vlan)#end
2etage#
*Mar  1 02:09:30.384: %SYS-5-CONFIG_I: (

Enter configuration commands, one per li
2etage(config)#vlan 150
2etage(config-vlan)#name Visiteurs
2etage(config-vlan)#end
2etage#
*Mar  1 02:09:53.880: %SYS-5-CONFIG_I: (

Enter configuration commands, one per li
2etage(config)#vlan 200
2etage(config-vlan)#name Demonstration
2etage(config-vlan)#end
```

Faire un sh vlan pour voir si les vlan créés sont biens existants :

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           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, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   Reseau_&_Systeme                  active
20   Direction_DSI                     active
30   Administratif                     active
40   Commercial                        active
50   Developpement                     active
150  Visiteurs                         active
200  Demonstration                     active
300  Serveurs                          active
```

Mettre une adresse IP au VLAN :

```
2etage(config)#int vlan 300
2etage(config-if)#
*Mar  1 02:31:00.803: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan300, c
hanged state to upip address 200.200.25.0 255.255.0.0
2etage(config-if)#no sh
2etage(config-if)#end
```

```
interface Vlan300
 ip address 200.200.25.0 255.255.0.0
```

Attribution des ports aux VLAN :
Pour le premier étage, attribution des ports dans les VLAN 10 et 30

```
1etage#
1etage#
1etage#
1etage#
1etage#
1etage#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   Reseau_&_Systeme                  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
20   Direction_DSI                     active
30   Administratif                     active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
40   Commercial                        active
50   Developpement                     active
150  Visiteurs                         active
200  Demonstration                     active
300  Serveurs                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
 --More--
```

Pour le 2etage, attribution des ports dans les VLAN 20 , 200 et 300 :

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   Reseau_&_Systeme                  active
20   Direction_DSI                     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, Fa0/16
                                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
30   Administratif                     active
40   Commercial                        active
50   Developpement                     active
150  Visiteurs                         active
200  Demonstration                     active    Fa0/24
300  Serveurs                          active    Fa0/21, Fa0/22, Fa0/23
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
 --More-- _
```

Routage InterVlan

Sur le routeur, réalisation de l'encapsulation pour permettre aux vlan de communiquer entre elles grâce au routeur, en effet l'adresse sera attribuée au vlan
Cela va permettre la création de sous-interfaces logiques sur une interface physique pour permettre la transmission de plusieurs VLANs sur un seul lien physique. Cela permet de segmenter le trafic en différents VLANs et d'améliorer la sécurité et les performances du réseau.
Création d'une sous-interface pour le VLAN 10 :

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gi 0/0.10
Router(config-subif)#encapsul
Router(config-subif)#encapsulation dot
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.254 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#end
```

Création d'une sous-interface pour le VLAN 40 / VLAN 50 :

```
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.254 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#end
Router#conf
Mar 23 14:14:56.003: %SYS-5-CONFIG_I: Configured from console b
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gi 0/0.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.50.254 255.255.255.0
Router(config-subif)#no sh
```

Création d'une sous-interface pour le VLAN 300 :

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gi 0/0.300
Router(config-subif)#encapsulation dot1Q 300
Router(config-subif)#ip address 200.200.25.254 255.255.255.0
Router(config-subif)#no sh
Router(config-subif)#end
```

En faisant un show run, on peut voir que le routage intervlan est créé.

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.254 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.254 255.255.255.0
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.254 255.255.255.0
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.254 255.255.255.0
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.50.254 255.255.255.0
!
interface GigabitEthernet0/0.150
 encapsulation dot1Q 150
 ip address 192.168.150.254 255.255.255.0
!
interface GigabitEthernet0/0.200
 encapsulation dot1Q 200
 ip address 192.168.200.254 255.255.255.0
!
!
interface GigabitEthernet0/0.300
 encapsulation dot1Q 300
 ip address 200.200.25.254 255.255.0.0
```

3. Création du DHCP sur le routeur

En mettant chaque VLAN en DHCP, il faut aussi mettre la carte Ethernet du pc en “obtenir une adresse IP automatiquement”

La mise en place du DHCP sur le routeur se fait avec la commande ipdhcp pool (mettant le nom du VLAN) network (avec l’adresse réseau du VLAN) dns-server (avec l’adresse ip du pc servant de dns) default-routeur(en mettant l’adresse ip de passerelle du routeur)

Mise en place du dhcp via le routeur sur le réseau dsi :

```
ip dhcp pool DSI
 network 192.168.20.0 255.255.255.0
 dns-server 200.200.25.1
 default-router 192.168.20.254
!
```

Mise en place du DHCP sur le réseau administratif :

```
Router(config)#ip dhcp pool Administratif
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#dns-server 200.200.25.1
Router(dhcp-config)#default-router 192.168.30.254
Router(dhcp-config)#_
```

Création des DHCP de réseaux et système / développement / visiteurs/ en fonction de leur VLAN, ainsi

que l’exclusion de l'attribution d'adresses IP environ 25 adresses possibles pouvant être attribuées sur des interfaces en statique

```
Router(config)#ip dhcp pool Reseau&Systeme
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#dns-server 200.200.25.1
Router(dhcp-config)#default-router 192.168.10.254
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.10.230 192.168.10.254
Router(config)#ip dhcp pool Developpement
Router(dhcp-config)#network 192.168.50.0 255.255.255.0
Router(dhcp-config)#dns-server 200.200.25.1
Router(dhcp-config)#default-routeur 192.168.50.254
                                   ^
% Invalid input detected at '^' marker.

Router(dhcp-config)#default-router 192.168.50.254
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.50.230 192.168.50.254
Router(config)#end
Router#
```

```
Router(config)#ip dhcp excluded-address 192.168.150.230 192.168.150.254
Router(config)#ip dhcp pool Visiteurs
Router(dhcp-config)#network 192.168.150.0 255.255.255.0
Router(dhcp-config)#dns-server 200.200.25.1
Router(dhcp-config)#default-router 192.168.150.254
Router(dhcp-config)#exit
Router(config)#
```

Exclusion du pc stagiaire et pc alternant.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.10.1
Router(config)#ip dhcp excluded-address 192.168.40.1
Router(config)#
```

En faisant un show run sur le routeur, on peut voir les différentes adresses IP qui ont été exclus de l’attribution en automatique.

```
!
ip dhcp excluded-address 192.168.20.230 192.168.20.254
ip dhcp excluded-address 192.168.30.230 192.168.30.254
ip dhcp excluded-address 192.168.10.230 192.168.10.254
ip dhcp excluded-address 192.168.50.230 192.168.50.254
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.40.1
ip dhcp excluded-address 192.168.200.230 192.168.200.254
ip dhcp excluded-address 192.168.40.230 192.168.40.254
!
```

Toujours avec le show run, on peut également voir que les DHCP ont bien été créé pour chaque VLAN

```
ip dhcp pool DSI
 network 192.168.20.0 255.255.255.0
 dns-server 200.200.25.1
 default-router 192.168.20.254
!
ip dhcp pool Administratif
 network 192.168.30.0 255.255.255.0
 dns-server 200.200.25.1
 default-router 192.168.30.254
!
ip dhcp pool Reseau&Systeme
 network 192.168.10.0 255.255.255.0
 dns-server 200.200.25.1
 default-router 192.168.10.254
!
ip dhcp pool Developpement
 network 192.168.50.0 255.255.255.0
 dns-server 200.200.25.1
 default-router 192.168.50.254
!
ip dhcp pool Demonstration
 network 192.168.200.0 255.255.255.0
 dns-server 200.200.25.1
```

```
ip dhcp pool Demonstration
 network 192.168.200.0 255.255.255.0
 dns-server 200.200.25.1
 default-router 192.168.200.254
!
ip dhcp pool Commercial
 network 192.168.40.0 255.255.255.0
 dns-server 200.200.25.1
 default-router 192.168.40.254
```

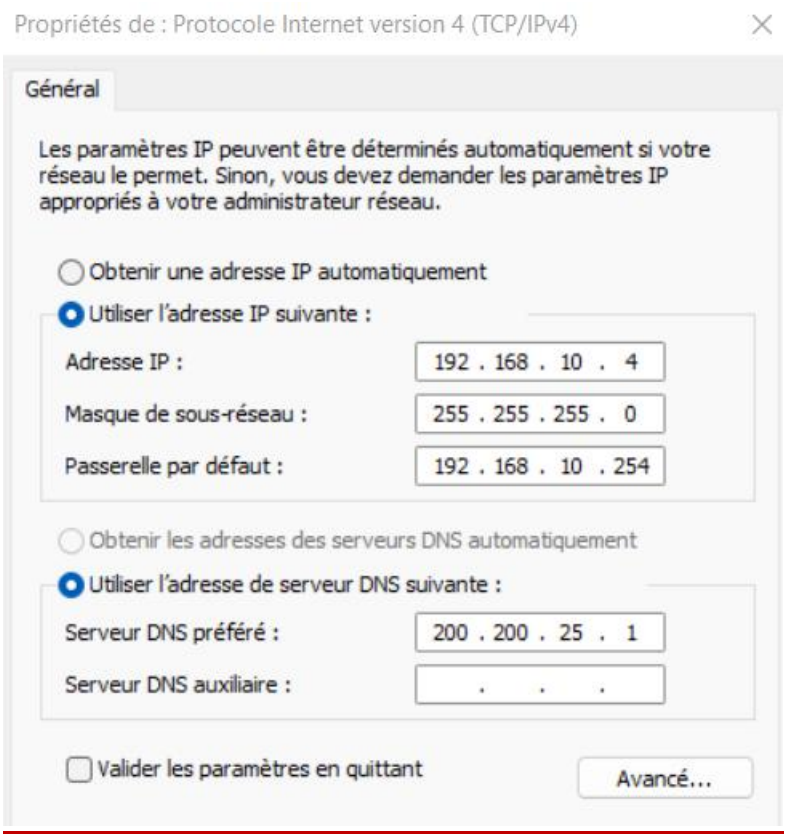
4. TESTS

Test avant la mise en place du DHCP :
Ping du pc 200.200.25.4 au 200.200.25.6 , qui actuellement sont tous les 2 dans le switch 1etage qui sont sur le VLAN 10 (fa0/1 et fa 0/5), ce qui montre que les pc peuvent communiquer dans un même VLAN .

```
C:\WINDOWS\system32>ping 200.200.25.6

Envoi d'une requête 'Ping'  200.200.25.6 avec 32 octets de données :
Réponse de 200.200.25.6 : octets=32 temps=5 ms TTL=128
Réponse de 200.200.25.6 : octets=32 temps=2 ms TTL=128
Réponse de 200.200.25.6 : octets=32 temps=2 ms TTL=128
Réponse de 200.200.25.6 : octets=32 temps=2 ms TTL=128

Statistiques Ping pour 200.200.25.6:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 5ms, Moyenne = 2ms
```



Changement de l'adresse du pc pour être dans la vlan 10

Mettre la passerelle en fonction de l'adresse de mon vlan ou le cableethernet est positionné → réalisation d'un ping envers l'adresse de passerelle de ce réseau

```
C:\WINDOWS\system32>ping 192.168.10.254

Envoi d'une requête 'Ping'  192.168.10.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 192.168.10.254:
    Paquets : envoyés = 4, reçus = 3, perdus = 1 (perte 25%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Ping du pc 192.168.20.1 qui est en vlan 20 alors que je suis en vlan 10

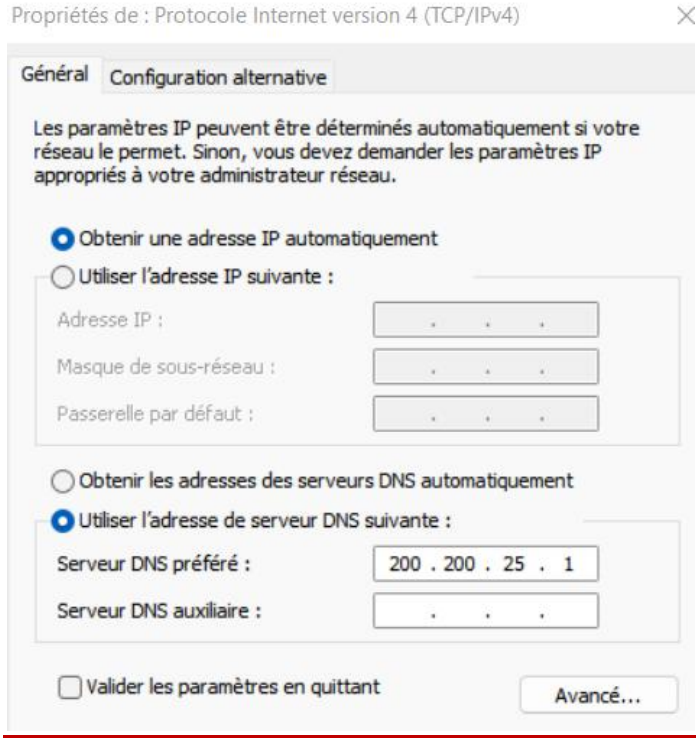
```
C:\WINDOWS\system32>ping 192.168.20.1

Envoi d'une requête 'Ping'  192.168.20.1 avec 32 octets de données :
Réponse de 192.168.20.1 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.20.1 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.20.1 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.20.1 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 192.168.20.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 3ms, Moyenne = 1ms
```

TEST après la configuration DHCP :

Mettre la carte réseau en automatique :



PC mis en DHCP → connecté à VLAN 20 :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::998e:c60c:dace:42a0%4
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.20.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.20.254
```

PC mis en DHCP connecté au switch comportant le VLAN 30, attribution automatique de l'adresse IP grâce au routeur.

```
arte Ethernet Ethernet :

  Suffixe DNS propre à la connexion. . . :
  Adresse IPv6 de liaison locale. . . . .: fe80::998e:c60c:dace:42a0%4
  Adresse IPv4. . . . . . . . . . . . . .: 192.168.30.1
  Masque de sous-réseau. . . . . . . . . : 255.255.255.0
  Passerelle par défaut. . . . . . . . . : 192.168.30.254
```

Dans VLAN 50 :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::998e:c60c:dace:42a0%4
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.50.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.50.254
```

On peut voir que l'adresse IPv4 est attribuée automatiquement en fonction du VLAN où le PC est connecté

Ip config de VLAN 40 en DHCP :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::998e:c60c:dace:42a0%4
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.40.2
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.40.254

Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::1c5:209:715f:193c%18
   Adresse d'autoconfiguration IPv4 . . . : 169.254.25.60
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . :
```

5. Réalisation des ACL

Réalisation des différentes ACL, pour permettre les différentes restrictions ainsi que les différentes acceptations.

Pour **l'ACL Active Directory**

Création de l'ACL _AD : en refusant au réseau 192.168.40.0/24 (donc le VLAN Démonstration) d'accéder au serveur AD (sachant qu'il existe 2 serveurs AD chez Centrecall, le serveur 200.200.25.1 qui est principal et le serveur 200.200.25.2 qui est le secondaire)

389 = LDAP ce qui signifie Lightweight Directory Access Protocol

```
Router(config)#ip access-list extended ACL_AD
Router(config-ext-nacl)#$0 0.0.0.255 200.200.25.1 0.0.255.255 eq 389
Router(config-ext-nacl)#$0 0.0.0.255 200.200.25.2 0.0.255.255 eq 389
Router(config-ext-nacl)#$2.168.150.0 0.0.0.255 200.200.25.1 0.0.255.255 eq 389
Router(config-ext-nacl)#$0 0.0.0.255 200.200.25.2 0.0.255.255 eq 389
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#int gi 0/0
Router(config-if)#ip access-group ACL_AD out
Router(config-if)#_
```

```
Router(config-if)#do sh access-lists
Extended IP access list ACL_AD
    10 deny tcp 192.168.200.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 389
    20 deny tcp 192.168.150.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 389
    30 permit ip any any
```

ACL WEB INTRANET

Création de l'ACL WEBIntranet rendant le serveur accessible uniquement pour les VLAN Commercial et Développement. De plus le pc stagiaire du service commercial : 192.168.40.1 ne doit pas avoir accès au serveur, donc il faut deny l'host

```
Router(config-if)#ip access-list extended ACL_WEBINTRANET
Router(config-if)#ip access-list extended ACL_WEBINTRANET
Router(config-ext-nacl)#deny tcp host 192.168.40.1 host 200.200.25.3 eq 443
Router(config-ext-nacl)#$st 192.168.40.1 200.200.25.3 0.0.255.255 eq 80
Router(config-ext-nacl)#$.0 0.0.0.255 200.200.25.3 0.0.255.255 eq 443
Router(config-ext-nacl)#$.0 0.0.0.255 200.200.25.3 0.0.255.255 eq 80
Router(config-ext-nacl)#$192.168.50.0 0.0.0.255 200.200.25.3 0.0.255.255 eq 443
Router(config-ext-nacl)#$.0 0.0.0.255 200.200.25.3 0.0.255.255 eq 80
Router(config-ext-nacl)#deny ip any any
Router(config-ext-nacl)#int gi 0/0
Router(config-if)#ip access-group ACL_WEBINTRANET out
Router(config-if)#end
```

Réalisation d'un show access-list

```
Router#sh access-list
Extended IP access list ACL_AD
    10 deny tcp 192.168.200.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 389
    20 deny tcp 192.168.150.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 389
    30 permit ip any any
Extended IP access list ACL_SERVER_TFTP
    10 deny tcp host 192.168.10.1 200.200.25.0 0.0.0.255 eq ftp
    20 deny icmp host 192.168.10.1 200.200.0.0 0.0.255.255
    30 permit tcp 192.168.10.0 0.0.0.255 200.200.25.0 0.0.0.255 eq ftp
    40 permit icmp 192.168.10.0 0.0.0.255 200.200.25.0 0.0.0.255
    50 deny ip any any
Extended IP access list ACL_WEBINTRANET
    10 deny tcp host 192.168.40.1 host 200.200.25.3 eq 443
    20 deny tcp host 192.168.40.1 200.200.0.0 0.0.255.255 eq www
    30 permit tcp 192.168.40.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 443
    40 permit tcp 192.168.40.0 0.0.0.255 200.200.0.0 0.0.255.255 eq www
    50 permit tcp 192.168.50.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 443
    60 permit tcp 192.168.50.0 0.0.0.255 200.200.0.0 0.0.255.255 eq www
    70 deny ip any any
Router#
```

ACL INTERNET

Ici, on interdit au VLAN Démonstration d'aller sur internet, mais en autorisant les autres à accéder à internet.

```
Router(config)#ip access-list standard ACL_INTERNET
Router(config-std-nacl)#deny 192.168.200.0 0
% Incomplete command.

Router(config-std-nacl)#deny 192.168.200.0 0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#int gi 0/1
Router(config-if)#ip access-group ACL_INTERNET out
Router(config-if)#_
```

```
Router#sh access-list
Standard IP access list ACL_INTERNET
    10 deny   192.168.200.0, wildcard bits 0.0.0.255
    20 permit any
Extended IP access list ACL_AD
    10 deny tcp 192.168.200.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 389
    20 deny tcp 192.168.150.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 389
    30 permit ip any any
Extended IP access list ACL_SERVER_TFTP
    10 deny tcp host 192.168.10.1 200.200.25.0 0.0.0.255 eq ftp
    20 deny icmp host 192.168.10.1 200.200.0.0 0.0.255.255
    30 permit tcp 192.168.10.0 0.0.0.255 200.200.25.0 0.0.0.255 eq ftp
    40 permit icmp 192.168.10.0 0.0.0.255 200.200.25.0 0.0.0.255
    50 deny ip any any (1662 matches)
Extended IP access list ACL_WEBINTRANET
    10 deny tcp host 192.168.40.1 host 200.200.25.3 eq 443
    20 deny tcp host 192.168.40.1 200.200.0.0 0.0.255.255 eq www
    30 permit tcp 192.168.40.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 443
    40 permit tcp 192.168.40.0 0.0.0.255 200.200.0.0 0.0.255.255 eq www
    50 permit tcp 192.168.50.0 0.0.0.255 200.200.0.0 0.0.255.255 eq 443
    60 permit tcp 192.168.50.0 0.0.0.255 200.200.0.0 0.0.255.255 eq www
    70 deny ip any any
Router#
```

ACL SERVER TFTP

Seul le Vlan Réseau & Système. Peut accéder au serveur TFTP sauf l'hôte stagiaire 192.168.10.1/24. Les autres réseaux ne peuvent avoir accès

```
Extended IP access list ACL_SERVER_TFTP
    10 deny tcp host 192.168.10.1 200.200.25.0 0.0.0.255 eq ftp
    15 deny icmp host 192.168.10.1 200.200.0.0 0.0.255.255
    20 permit tcp 192.168.10.0 0.0.0.255 200.200.25.0 0.0.0.255 eq ftp
    25 permit icmp 192.168.10.0 0.0.0.255 200.200.25.0 0.0.0.255
    30 deny ip any any
Router(config-ext-nacl)#
```

6. Sauvegarde TFTP

Pas eu le temps de le réaliser.