

BRETON Théo
BERLINGEN Gary
CAMPUS CARLO ACUTIS



Document de validation de compétences

AP4 – Segmentation du réseau

1. Présentation du contexte d'entreprise

La maison des ligues projette de cloisonner son réseau et vient de réaliser une étude afin d'établir le plan d'adressage réseau et le nommage des vlan.

Toutes les salles de réunion sont équipées d'un point d'accès Wifi positionné par défaut dans le VLAN "Visiteurs" qui autorise uniquement un accès Internet.

Les portables connectés en wifi à ce point d'accès reçoivent ainsi une adresse IP et n'ont, par conséquent accès qu'aux services DHCP et DNS.

Le point d'accès peut être configuré à la demande pour être raccordé à un VLAN présent au niveau de l'étage.

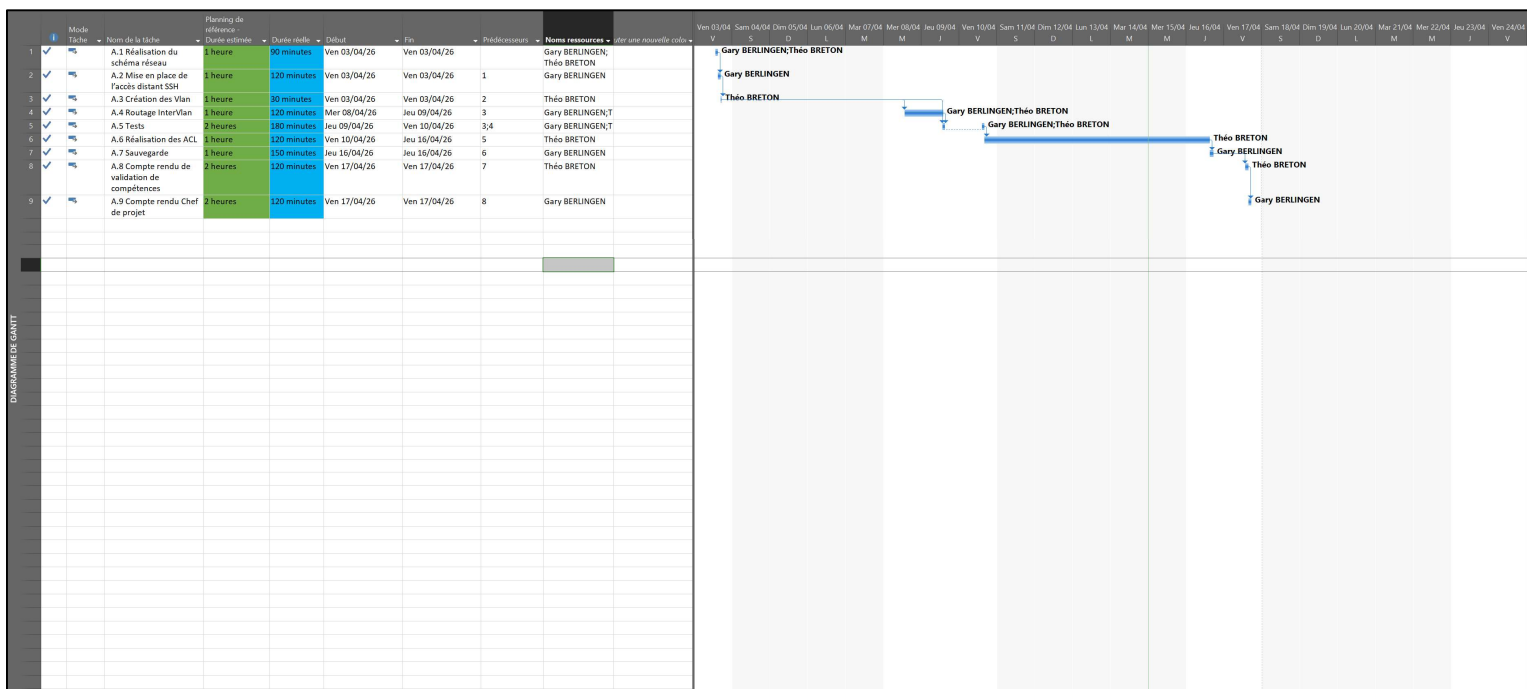
Chaque salle de réunion dispose d'un vidéoprojecteur, d'enceintes et d'un tableau numérique interactif.

La salle "Démonstration" est destinée à l'accueil des organismes de santé (AFSSAPS notamment) et des partenaires scientifiques. Elle dispose de paillasses et d'équipements de laboratoire, en plus d'une salle de réunion.

2. Objectifs attendus

Mettre en place l'administration réseau au sein de la maison des ligues. Chaque service aura un VLAN qui lui est attribué. Il faudra mettre en place toute les sous interfaces sur le Routeur pour chaque VLAN. De plus il aura une couche de sécurité au niveau des accès qui sera gérer aux moyens des ACLs. Pour que nous puissions avoir une sauvegarde de nos équipements il faudra faire une sauvegarde de l'ensemble de l'infrastructure monté.

3. Plan de travail

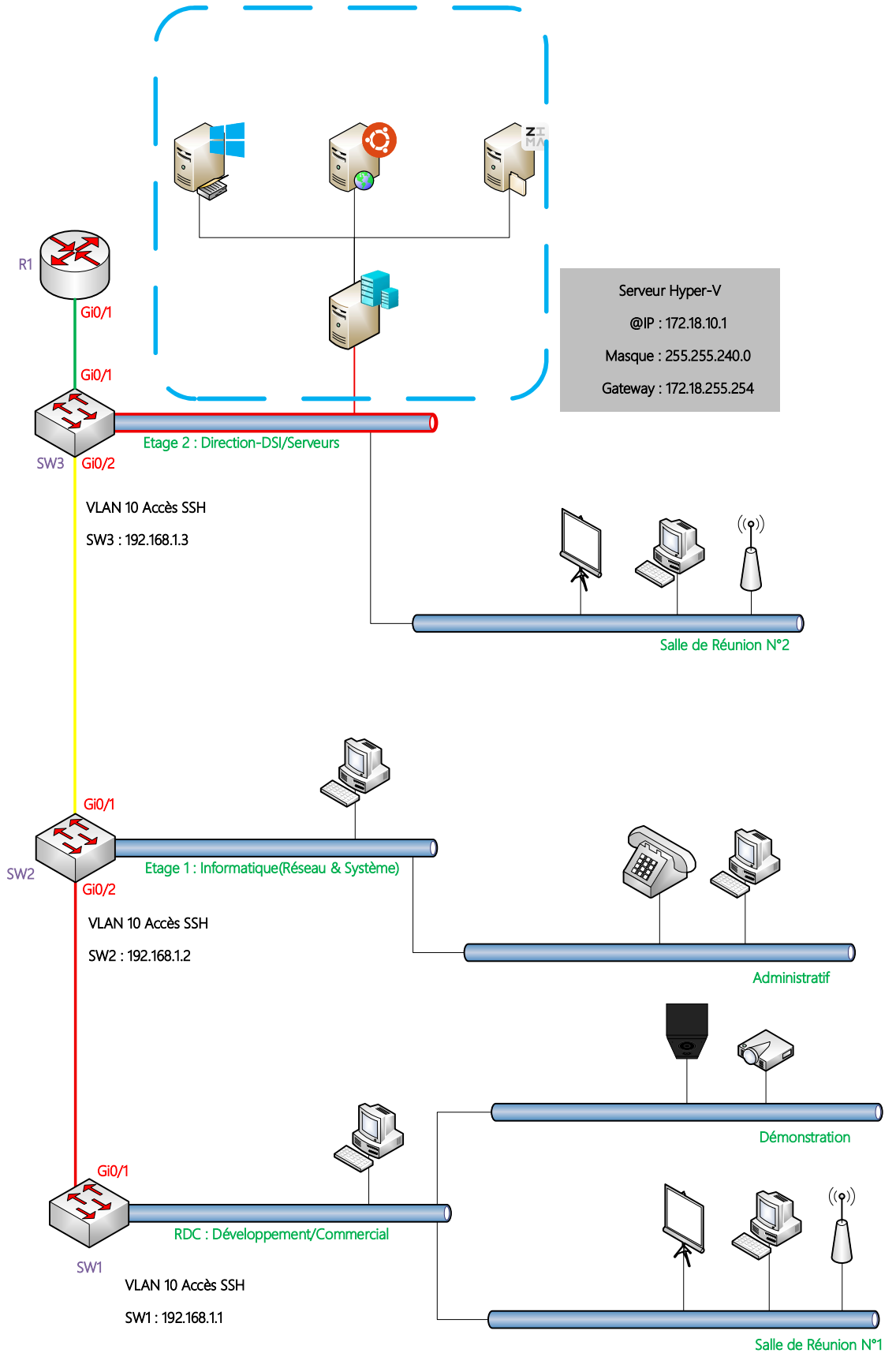


A.1 Réalisation du schéma réseau

VM WinServer2022 @IP : 172.18.10.2 Masque : 255.255.240.0 Gateway : 172.18.255.254	VM UbuntuServer @IP : 172.18.10.3 Masque : 255.255.240.0 Gateway : 172.18.255.254	VM ZIMAOS @IP : 172.18.10.4 Masque : 255.255.240.0 Gateway : 172.18.255.254
---	--	--

Sous-interfaces :

- VLAN 10 – Réseaux & Systèmes
→ @Réseau : 192.168.10.0/24
Gateway : 192.168.10.254
- VLAN 20 – Direction-DSI
→ @Réseau : 192.168.20.0/24
Gateway : 192.168.20.254
- VLAN 30 – Administratif
→ @Réseau : 192.168.30.0/24
Gateway : 192.168.30.254
- VLAN 40 – Commercial
→ @Réseau : 192.168.40.0/24
Gateway : 192.168.40.254
- VLAN 50 – Développement
→ @Réseau : 192.168.50.0/24
Gateway : 192.168.50.254
- VLAN 150 – Visiteurs
→ @Réseau : 192.168.150.0/24
Gateway : 192.168.150.254
- VLAN 200 - Démonstration
→ @Réseau : 192.168.200.0/24
Gateway : 192.168.200.254
- VLAN 300 – Serveurs
→ @Réseau : 172.18.0.0/16
Gateway : 172.18.0.254



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

Sur tous les commutateurs :

```
Password:
```

```
SW>en
```

```
Password:
```

```
SW#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
X = NUMERO SWITCH
```

```
SWX(config)#line vty 0 4
```

```
SWX(config-line)#transport input ssh
```

```
SWX(config-line)#transport output ssh
```

```
SWX(config-line)#login
```

```
SWX(config-line)#password cisco
```

```
SWX(config-line)#ip domain-name mdl.local
```

```
SWX(config)#ip ssh version 2
```

```
SWX(config)#crypto key generate rsa general-keys modulus 2048
```

```
The name for the keys will be: sw.mdl.local
```

```
% The key modulus size is 2048 bits
```

```
% Generating 2048 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 21 seconds)
```

T.1 Mise en place du trunk sur les ports :

SW1 :

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SW1(config)#int Gi0/1
```

```
SW1(config-if)#sw mode trunk
```

```
SW1(config-if)#no sh
```

```
SW1(config-if)#end
```

```
SW1#
```

SW2 :

```
SW2>en
```

```
Password:
```

```
SW2#en
```

```
SW2#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SW2 (config)#int Gi0/1
```

```
SW2 (config-if)#sw mode tr
```

```
SW2 (config-if)#no sh
```

```
SW2 (config-if)#end
```

```
SW2#
```

```
SW2 (config)#int Gi0/2
```

```
SW2 (config-if)#sw mode tr
```

```
SW2 (config-if)#no sh
```

```
SW2 (config-if)#exit
```

```
SW2 (config)#end
```

SW3 :

```
SW3 (config)#int Gi0/1
```

```
SW3 (config-if)#sw mode trunk
```

```
SW3 (config-if)#no sh
```

```
SW3 (config-if)#end
```

```
SW3#
```

```
SW3#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SW3 (config)#int Gi0/2
```

```
SW3 (config-if)#sw mode tr
```

```
SW3 (config-if)#no sh
```

```
SW3 (config-if)#end
```



Vérification :

→ sh run

SW3 :

```
interface GigabitEthernet0/1
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport mode trunk
```

SW2 :

```
interface GigabitEthernet0/1
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport mode trunk
```

SW1 :

```
interface GigabitEthernet0/1
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport mode trunk
!
```

T.2 Déploiement des VLAN au moyen du protocole VTP :

```
SW1(config)#vtp mode server
```

```
Device mode already VTP SERVER.
```

```
SW1(config)#vtp domain theo
```

```
Changing VTP domain name from NULL to theo
```

X = NUMERO SWITCH

```
SWX(config)#vtp mode client
```

```
SWX>en
```

```
SWX#show vtp status
```

A.3 Création des VLAN

```
SW1 (config) #vlan 10
SW1 (config-vlan) #name RESEAU_SYSTEM
SW1 (config-vlan) #exit
SW1 (config) #
SW1 (config) #vlan 20
SW1 (config-vlan) #name DIRECTION_DSI
SW1 (config-vlan) #exit
SW1 (config) #
SW1 (config) #vlan 30
SW1 (config-vlan) #name ADMINISTRATIF
SW1 (config-vlan) #exit
SW1 (config) #
SW1 (config) #vlan 40
SW1 (config-vlan) #name COMMERCIAL
SW1 (config-vlan) #ex
SW1 (config) #vlan 50
SW1 (config-vlan) #name DEVELOPPEMENT
SW1 (config-vlan) #ex
SW1 (config) #vlan 150
SW1 (config-vlan) #name VISITEURS
SW1 (config-vlan) #ex
SW1 (config) #vlan 200
SW1 (config-vlan) #name DEMONSTRATION
SW1 (config-vlan) #ex
SW1 (config) #vlan 300
SW1 (config-vlan) #name SERVEURS
SW1 (config-vlan) #ex
SW1 (config) #
```



Vérification :

→ sh run

Affectation des VLAN sur les ports de chaque Switch.

SW3 :

5	ACCES_DISTANT	active	Fa0/24
10	RESEAU_SYSTEM	active	Fa0/1, Fa0/2, Fa0/3
20	DIRECTION_DSI	active	Fa0/4, Fa0/5, Fa0/6
30	ADMINISTRATIF	active	Fa0/7, Fa0/8, Fa0/9
40	COMMERCIAL	active	Fa0/10, Fa0/11, Fa0/12
50	DEVELOPPEMENT	active	Fa0/13, Fa0/14, Fa0/15
150	VISITEURS	active	Fa0/16, Fa0/17, Fa0/18
200	DEMONSTRATION	active	Fa0/19, Fa0/20, Fa0/21
300	SERVEURS	active	Fa0/22, Fa0/23

SW2 :

5	ACCES_DISTANT	active	Fa0/24
10	RESEAU_SYSTEM	active	Fa0/1, Fa0/2, Fa0/3
20	DIRECTION_DSI	active	Fa0/4, Fa0/5, Fa0/6
30	ADMINISTRATIF	active	Fa0/7, Fa0/8, Fa0/9
40	COMMERCIAL	active	Fa0/10, Fa0/11, Fa0/12
50	DEVELOPPEMENT	active	Fa0/13, Fa0/14, Fa0/15
150	VISITEURS	active	Fa0/16, Fa0/17, Fa0/18
200	DEMONSTRATION	active	Fa0/19, Fa0/20

SW1:

5	ACCES_DISTANT	active	
10	RESEAU_SYSTEM	active	
20	DIRECTION_DSI	active	
30	ADMINISTRATIF	active	
40	COMMERCIAL	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
50	DEVELOPPEMENT	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22
150	VISITEURS	active	Fa0/24
200	DEMONSTRATION	active	Fa0/23
300	SERVEURS	active	

A.4 Routage InterVlan

Assurer la communication des différents services autorisés vers le serveur

Sous-interface – VLAN 10 – Réseau & Système :

```
Router(config)# interface Gi 0/0.10
```

```
Router(config-subif)# encapsulation dot1q 10
```

```
Router(config-subif)# ip address 192.168.10.254 255.255.255.0
```

```
Routeur1(config-subif)# exit
```

Sous-interface – VLAN 20 – Direction - DSI:

```
Router(config)# interface Gi 0/0.20
```

```
Router(config-subif)# encapsulation dot1q 20
```

```
Router(config-subif)# ip address 192.168.20.254 255.255.255.0
```

```
Routeur1(config-subif)# exit
```

Sous-interface – VLAN 30 – Direction - DSI:

```
Router(config)# interface Gi 0/0.30
```

```
Router(config-subif)# encapsulation dot1q 30
```

```
Router(config-subif)# ip address 192.168.30.254 255.255.255.0
```

```
Routeur1(config-subif)# exit
```

Sous-interface – VLAN 40 – Commercial :

```
Router(config)# interface Gi 0/0.40
```

```
Router(config-subif)# encapsulation dot1q 40
```

```
Router(config-subif)# ip address 192.168.40.254 255.255.255.0
```

```
Routeur1(config-subif)# exit
```

Sous-interface – VLAN 50 – Développement :

```
Router(config)# interface 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)# ex
```

Sous-interface – VLAN 150 – Visiteurs :

```
Router(config)# interface Gi 0/0.150
```

```
Router(config-subif)# encapsulation dot1q 150
```



```
Router(config-subif)#ip address 192.168.150.254 255.255.255.0
```

```
Router(config-subif)#ex
```

```
Router(config)#
```

Sous-interface – VLAN 200 – Démonstration :

```
Router(config)#interface Gi 0/0.200
```

```
Router(config-subif)#encapsulation dot1q 200
```

```
Router(config-subif)#ip address 192.168.200.254 255.255.255.0
```

```
Router(config-subif)#ex
```

Sous-interface – VLAN 300 – Serveurs :

```
Router(config)#interface Gi 0/0.300
```

```
Router(config-subif)#encapsulation dot1q 300
```

```
Router(config-subif)#ip address 172.18.0.254 255.255.255.0
```

```
Router(config-subif)#ex
```



Vérification :

→ sh run

```
!  
interface GigabitEthernet0/0  
no ip address  
duplex auto  
speed auto  
!  
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 172.18.0.254 255.255.0.0
```

```
ip access-group 100 out
```

```
!
```

A.5 Tests

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

Source	Destination	Interface	Commentaire	Statut
ACCES SSH				
192.168.1.12 (PC GARY)	192.168.1.3 (VLAN5) SW3	Fa0/24	TEST SSH (22) SUR LE PORTS 24 AFFECTER AU VLAN5.	
192.168.1.12 (PC GARY)	192.168.1.3 (VLAN5) SW2	Fa0/24	TEST SSH (22) SUR LE PORTS 24 AFFECTER AU VLAN5.	
192.168.1.12 (PC GARY)	192.168.1.3 (VLAN5) SW1	Fa0/24	TEST SSH (22) SUR LE PORTS 24 AFFECTER AU VLAN5.	
PING SWITCHs DEPUIS PCClient				
192.168.1.12 (PC GARY)	192.168.1.3 (VLAN5) SW3	Fa0/24	<pre>PS C:\Users\garyb> ping 192.168.1.3 Envoi d'une requête 'Ping' 192.168.1.3 avec 32 octets de données : Réponse de 192.168.1.3 : octets=32 temps=4 ms TTL=255 Réponse de 192.168.1.3 : octets=32 temps=2 ms TTL=255 Réponse de 192.168.1.3 : octets=32 temps=3 ms TTL=255 Réponse de 192.168.1.3 : octets=32 temps=1 ms TTL=255 Statistiques Ping pour 192.168.1.3: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 1ms, Maximum = 4ms, Moyenne = 2ms</pre>	
192.168.1.12 (PC GARY)	192.168.1.2 (VLAN5) SW2	Fa0/24	<pre>PS C:\Users\garyb> ping 192.168.1.2 Envoi d'une requête 'Ping' 192.168.1.2 avec 32 octets de données : Réponse de 192.168.1.2 : octets=32 temps=1 ms TTL=255 Réponse de 192.168.1.2 : octets=32 temps=3 ms TTL=255 Réponse de 192.168.1.2 : octets=32 temps=1 ms TTL=255 Réponse de 192.168.1.2 : octets=32 temps=3 ms TTL=255 Statistiques Ping pour 192.168.1.2: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 1ms, Maximum = 3ms, Moyenne = 2ms</pre>	
192.168.1.12 (PC GARY)	192.168.1.1 (VLAN5) SW1	Fa0/24	<pre>PS C:\Users\garyb> ping 192.168.1.1 Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données : Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=255 Réponse de 192.168.1.1 : octets=32 temps=3 ms TTL=255 Réponse de 192.168.1.1 : octets=32 temps=2 ms TTL=255 Réponse de 192.168.1.1 : octets=32 temps=2 ms TTL=255 Statistiques Ping pour 192.168.1.1: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 1ms, Maximum = 3ms, Moyenne = 2ms</pre>	
PING ENTRE SWITCH				

SW1	192.168.1.3 (VLAN5) SW3	Fa0/24	<pre>SW1# SW1#ping 192.168.1.3 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds: !!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 1/4/9 ms SW1#</pre>	
SW1	192.168.1.2 (VLAN5) SW2	Fa0/24	<pre>SW1#ping 192.168.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds: !!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/9 ms SW1#</pre>	
SW2	192.168.1.1 (VLAN5) SW2	Fa0/24	<pre>SW2#ping 192.168.1.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms</pre>	

TESTS PING INTERVLAN

192.168.2 0.1 (PC GARY)	192.168.20.254 (Passerelle VLAN20)	Fa0/5 – SW3	<pre>Statistiques Ping pour 192.168.20.254: Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%), PS C:\Users\garyb> ping 192.168.20.254 Envoi d'une requête 'Ping' 192.168.20.254 avec 32 octets de données : Réponse de 192.168.20.254 : octets=32 temps<1ms TTL=255 Réponse de 192.168.20.254 : octets=32 temps<1ms TTL=255 Réponse de 192.168.20.254 : octets=32 temps=1 ms TTL=255 Réponse de 192.168.20.254 : octets=32 temps<1ms TTL=255 Statistiques Ping pour 192.168.20.254: Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%), Durée approximative des boucles en millisecondes : Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms</pre>	
192.168.2 0.1 (PC GARY)	192.168.10.1 (PCThéo – VLAN)	Fa0/5 – SW3	<pre>PS C:\Users\garyb> ping 192.168.10.1 Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données : Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé. Délai d'attente de la demande dépassé. Statistiques Ping pour 192.168.10.1: Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),</pre> <p>La communication est impossible car ce sont des VLAN différents.</p>	
192.168.1 0.2 PC GARY)	192.168.10.1 (PCThéo – VLAN)	Fa0/1 – SW3	<pre>PS C:\Users\garyb> ping 192.168.10.1 Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données : Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=128 Réponse de 192.168.10.1 : octets=32 temps<1ms TTL=128 Réponse de 192.168.10.1 : octets=32 temps=8 ms TTL=128 Réponse de 192.168.10.1 : octets=32 temps<1ms TTL=128 Statistiques Ping pour 192.168.10.1: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 0ms, Maximum = 8ms, Moyenne = 2ms</pre> <p>La communication fonctionne car nous sommes sur les mêmes VLANs.</p>	

192.168.200.2 PC GARY)	192.168.200.254 (Passerelle VLAN200)	Fa0/20 – SW3	<pre>PS C:\Users\garyb> ping 192.168.200.254 Envoi d'une requête 'Ping' 192.168.200.254 avec 32 octets de données : Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=255 Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=255 Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=255 Réponse de 192.168.200.254 : octets=32 temps=1 ms TTL=255 Statistiques Ping pour 192.168.200.254: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms</pre>	
192.168.200.2 PC GARY)	192.168.200.3 (PCThéo – VLAN)	Fa0/20 – SW3	<pre>PS C:\Users\garyb> ping 192.168.200.3 Envoi d'une requête 'Ping' 192.168.200.3 avec 32 octets de données : Réponse de 192.168.200.3 : octets=32 temps=12 ms TTL=128 Réponse de 192.168.200.3 : octets=32 temps=1 ms TTL=128 Réponse de 192.168.200.3 : octets=32 temps<1ms TTL=128 Réponse de 192.168.200.3 : octets=32 temps<1ms TTL=128 Statistiques Ping pour 192.168.200.3: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 0ms, Maximum = 12ms, Moyenne = 3ms</pre>	

TESTS ACL

ACL N°1 : Accès TFTP

192.168.10.1 (PC Théo « Stagiaire »)	172.18.0.1	Fa0/20 – SW3	<p>Ping refuser vers le serveur TFTP.</p> <p>→ Destination host is unreachable</p>	
192.168.10.2 (PC Gary « Serveur TFTP »)	172.18.0.1	Fa0/22 – SW2	<p>Ping passe vers le serveur TFTP.</p>	

Manque de temps pour les dernières capture.

A.6 Réalisation des ACL

Réalisation des règles d'accès aux différentes zones

1) Accès TFTP

- Le serveur TFTP est accessible **uniquement** depuis le **Vlan Réseau & Système**.
- **Attention !** Le service Réseau & Système accueille régulièrement un stagiaire qui dispose pendant toute la durée de son stage d'un pc configuré en statique avec l'adresse suivante : 192.x.10.1/24. Ce stagiaire ne doit pas avoir accès au serveur TFTP.

ACL Etendue

Je n'autorise le PC Stagiaire à y accéder.

```
access-list 100 deny ip host 192.168.10.1 host 172.18.0.1
```

J'autorise tout le réseau du VLAN 10 (Réseaux & Système).

```
access-list 100 permit ip 192.168.10.0 0.0.0.255 host 172.18.0.1
```

Je bloque tout autre accès au serveur TFTP (Sécurité).

```
access-list 100 deny ip any host 172.18.0.1
```

Mise en place:

```
!  
access-list 100 deny ip host 192.168.10.1 host 172.18.0.1  
access-list 100 permit ip 192.168.10.0 0.0.0.255 host 172.18.0.1  
access-list 100 deny ip any host 172.18.0.1
```

```
!
```

2) Accès Active Directory

- Le serveur Active Directory est accessible pour tous les Vlan sauf les Vlan Démonstration et Visiteurs.

ACL Etendue

Je bloque le VLAN Démonstration

```
access-list 101 deny ip 192.168.200.0 0.0.0.255 host 172.18.10.2
```

Je bloque le VLAN Visiteur

```
access-list 101 deny ip 192.168.150.0 0.0.0.255 host 172.18.10.2
```

J'autorise le reste des VLANs

```
access-list 101 permit ip any any
```

Manque de temps.

3) Accès NextCloud

- Le serveur NextCloud est accessible uniquement pour les Vlan Commercial et Développement.
- **Attention !** Le service Commercial accueille régulièrement un alternant qui dispose pendant toute la durée de son alternance d'un pc configuré en statique avec l'adresse suivante : 192.x.40.1/24. Ce stagiaire ne doit pas avoir accès au serveur WebIntranet.

ACL Etendue

Je n'autorise pas le PCStagiaire à accéder au SERV.INTRANET

```
access-list 101 deny ip host 192.168.40.1 host 172.18.10.3
```

Je n'autorise pas le VLAN40 – Commercial à accéder au SERV.INTRANET

```
access-list 101 permit ip 192.168.40.0 0.0.0.255 host 172.18.10.3
```

Je n'autorise pas le VLAN50 – Développement à accéder au SERV.INTRANET

```
access-list 101 permit ip 192.168.50.0 0.0.0.255 host 172.18.10.3
```

Permet de voir les matchs

```
access-list 101 deny ip any any
```

Manque de temps.

4) Accès Internet



ACL Standard !!!!!

- Tout le monde peut aller sur Internet (Serveurs et postes) sauf le Vlan Démonstration.

Je n'autorise pas le VLAN200 – Démonstration à accéder à Internet

```
access-list 102 deny ip 192.168.200.0 0.0.0.255
```

```
access-list 102 permit any any
```

Manque de temps.

5) Administration à distance

- L'ensemble des équipements 'interconnexion devront pouvoir être administrés à distance uniquement pour les membres du service Réseau & Système (sauf pour le stagiaire) en SSH avec les options nécessaires à une sécurité optimale.

ACL Etendue

```
access-list 103 deny tcp host 192.168.10.1 any eq 22
```

J'autorise le VLAN10 – Réseaux & Système à accéder au SSH

```
access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 22
```

```
access-list 103 deny tcp any any eq 22
```

```
Router(config)# line vty 0 4
```

```
Router(config-line)# access-class 103 in
```

```
Router(config-line)# password cisco
```

```
Router(config-line)# login
```

Manque de temps.

A.7 Sauvegarde


Réaliser l'ensemble des sauvegardes nécessaires

Mise en place du serveur TFTP sur le serveur :

Manque de temps.

Bonus : Mettre en place le DHCP sur le Routeur

Commande :

TITRE	COMMANDE – CREATION DE POOL DHCP, LE ROUTEUR PREND LE ROLE DE SERVEUR DHCP.
EQUIPEMENT	
COMMANDE 	<pre>Routeur(config)#ip dhcp pool DEVELOPPEMENT Router(dhcp-config)#network 192.168.200.0 255.255.255.0 Router(dhcp-config)#default-router 192.168.200.254 Router(dhcp-config)#dns-server 172.18.10.2 Router(dhcp-config)#domain-name mdl.local Router(dhcp-config)#ip dhcp excluded-address 192.168.200.254</pre>



Vérification :

→ sh run

```
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.20.254
ip dhcp excluded-address 192.168.50.254
ip dhcp excluded-address 192.168.40.254
ip dhcp excluded-address 192.168.30.254
ip dhcp excluded-address 192.168.200.254
ip dhcp excluded-address 192.168.150.254
ip dhcp excluded-address 172.18.0.254
!
ip dhcp pool RESEAUSYSTEM
network 192.168.10.0 255.255.255.0
dns-server 172.18.10.2
domain-name mdl.local
default-router 192.168.10.254
!
ip dhcp pool DIRECTION_DSI
network 192.168.20.0 255.255.255.0
default-router 192.168.20.254
dns-server 172.18.10.2
domain-name mdl.local
!
ip dhcp pool ADMINISTRATIF
network 192.168.30.0 255.255.255.0
default-router 192.168.30.254
domain-name mdl.local
dns-server 172.18.10.2
!
```



```
ip dhcp pool COMMERCIAL
network 192.168.40.0 255.255.255.0
default-router 192.168.40.254
domain-name mdl.local
dns-server 172.18.10.2
```

!

```
ip dhcp pool DEVELOPPEMENT
network 192.168.50.0 255.255.255.0
default-router 192.168.50.254
dns-server 172.18.10.2
```

```
domain-name mdl.local
```

!

```
ip dhcp pool VISITEURS
network 192.168.150.0 255.255.255.0
dns-server 172.18.10.2
```

```
domain-name mdl.local
```

```
default-router 192.168.150.254
```

!

```
ip dhcp pool DEMONSTRATION
network 192.168.200.0 255.255.255.0
default-router 192.168.200.254
```

```
domain-name mdl.local
```

!

```
ip dhcp pool SERVEURS
network 172.18.0.0 255.255.0.0
default-router 172.18.0.254
```

```
domain-name mdl.local
```

```
dns-server 172.18.10.2
```



