TP PACKET TRACER

PROGRESSION PÉDAGOGIQUE

Pierre-Louis

01

Consolidation VLSM & OSPF

02

Haute disponbilité et services réseau

03

Sécurité et DMZ

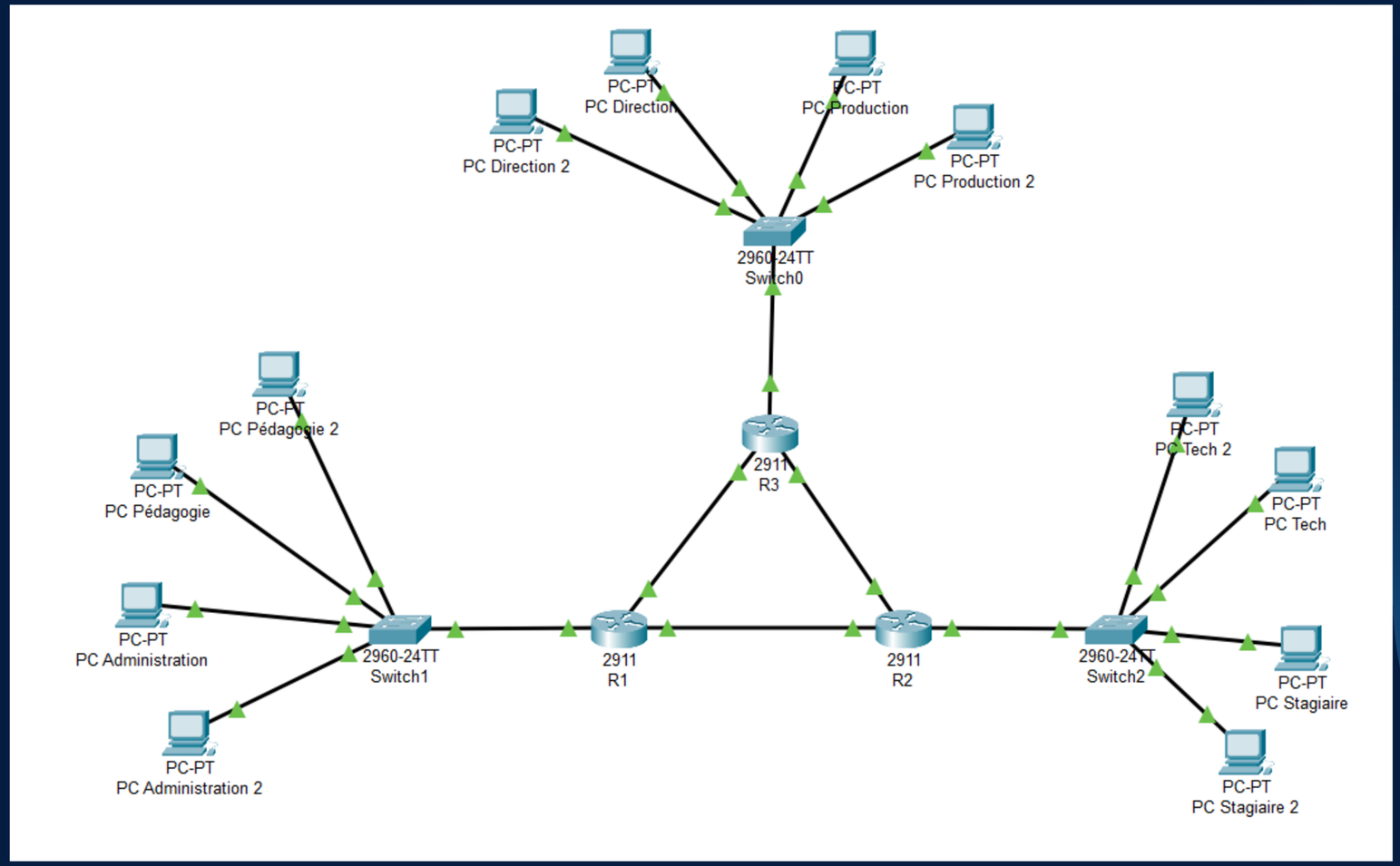
04

Supervision et projet final

01 CONSOLIDATION VLSM & OSPF

TOPOLOGIE MULTI-SITES

R1 = Siège (Pédagogie + Admin)
R2 = Agence A (Technique + Stagiaires)
R3 = Agence B (Direction + Production)



01 CONSOLIDATION VLSM & OSPF

PLAN D'ADRESSAGE VLSM

VLAN	Réseau	Masque	Passerelle	Exemple PC
10 – Pédagogie	192.168.0.0/25	255.255.255.128	192.168.0.1	192.168.0.10
20 – Admin	192.168.0.192/26	255.255.255.192	192.168.0.193	192.168.0.200
30 – Tech	192.168.1.0/27	255.255.255.224	192.168.1.1	192.168.1.10
40 – Stagiaires	192.168.1.32/28	255.255.255.240	192.168.1.33	192.168.1.34
50 – Direction	192.168.1.48/29	255.255.255.248	192.168.1.49	192.168.1.50
60 – Production	192.168.0.128/26	255.255.255.192	192.168.0.129	192.168.0.140

Équipement	Rôle	VLAN / Réseau	IP / Masque	Passerelle	Remarques
Server-DNS	DNS local	VLAN 20 – Admin (192.168.0.192/26)	192.168.0.195 /26	192.168.0.193	Service DNS activé, zones internes (ex: www.tp.local → 192.168.2.2)
Server-SYSLOG	Syslog (et SNMP mgr si besoin)	VLAN 50 – Direction (192.168.1.48/29)	192.168.1.52 /29	192.168.1.49	Syslog ON, reçoit les logs des équipements
PC-SNMP	Manager SNMP (MIB Browser)	VLAN 20 – Admin (192.168.0.192/26)	192.168.0.210 /26	192.168.0.193	Utilisé pour interroger R1/R2/R3 en SNMP
Server-WEB	Web en DMZ	VLAN 70 – DMZ (192.168.2.0/28)	192.168.2.2 /28	192.168.2.1	Cible publique (HTTP/HTTPS depuis le WAN)
PC-WAN	Client “Internet” externe	VLAN 99 – WAN test (10.0.0.0/24)	10.0.0.2 /24	10.0.0.1	Sert à tester l’accès au Web DMZ comme “Internet”

01 CONSOLIDATION VLSM & OSPF

CONFIGURATION OSPF

COMMANDES →

```
router ospf 1
 router-id 1.1.1.1
 network 192.168.0.0 0.0.3.255 area 0
```

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
2.2.2.2           0   FULL/  -        00:00:37    192.168.1.58
GigabitEthernet0/0
3.3.3.3           0   FULL/  -        00:00:37    192.168.1.66
GigabitEthernet0/1
```

← VERIFICATIONS (POUR R1)

01 CONSOLIDATION VLSM & OSPF

VÉRIFICATION DE LA CONNECTIVITÉ

Tous les VLANs communiquent entre eux grâce à OSPF ✅

ADMIN → PROD

```
C:\>ping 192.168.0.140

Pinging 192.168.0.140 with 32 bytes of data:

Reply from 192.168.0.140: bytes=32 time<1ms TTL=126
Reply from 192.168.0.140: bytes=32 time<1ms TTL=126
Reply from 192.168.0.140: bytes=32 time=11ms TTL=126
Reply from 192.168.0.140: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.0.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms
```

```
C:\>tracert 192.168.1.50

Tracing route to 192.168.1.50 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.33
  2    0 ms      0 ms      0 ms      192.168.1.62
  3    0 ms      0 ms      0 ms      192.168.1.50

Trace complete.
```

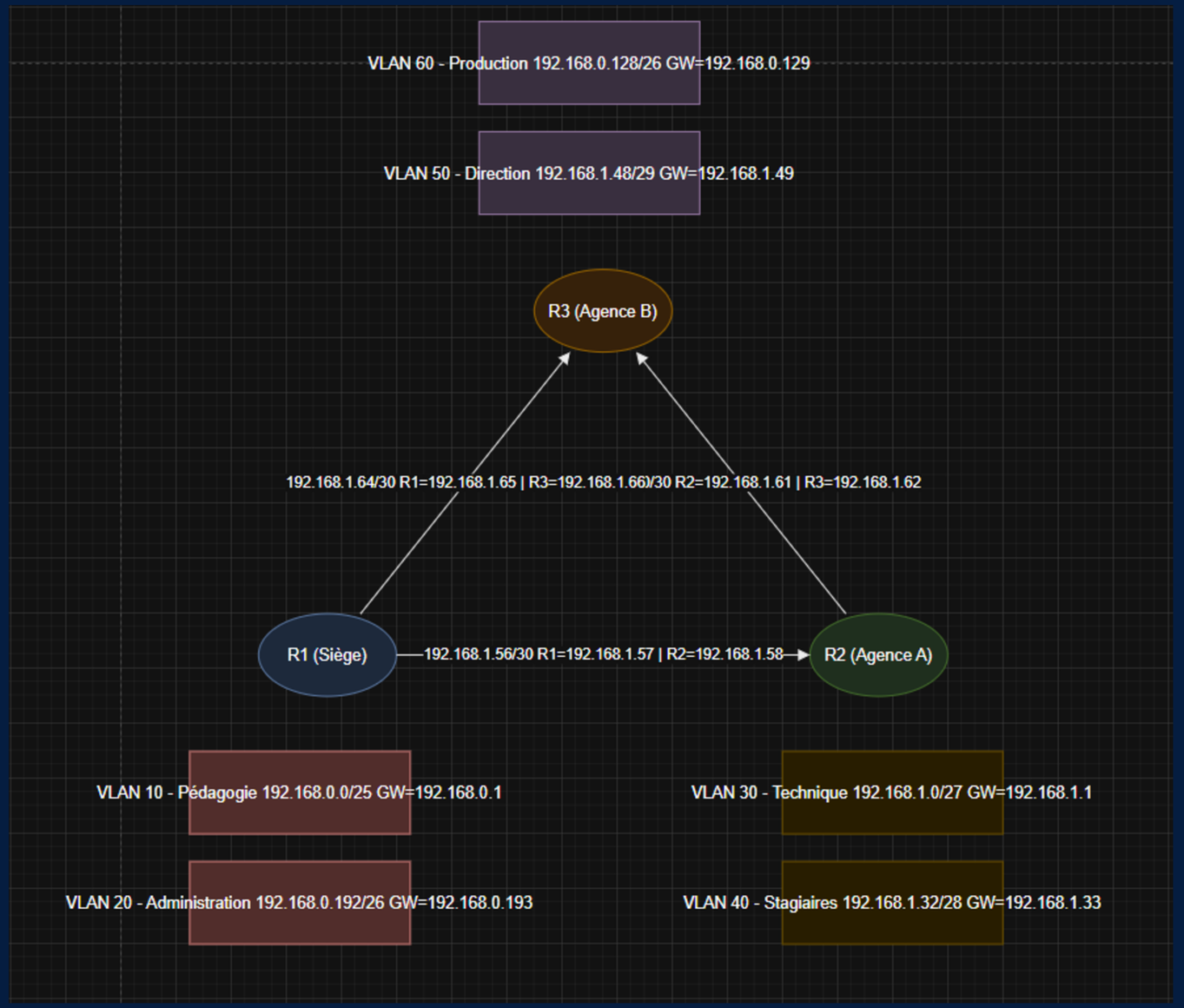
STAGIAIRE → DIRECTION

```
C:\>ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:

Reply from 192.168.1.50: bytes=32 time=1ms TTL=126
Reply from 192.168.1.50: bytes=32 time=2ms TTL=126
Reply from 192.168.1.50: bytes=32 time<1ms TTL=126
Reply from 192.168.1.50: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

```
C:\>tracert 192.168.0.140

Tracing route to 192.168.0.140 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.0.193
  2    0 ms      0 ms      0 ms      192.168.1.66
  3    0 ms      0 ms      0 ms      192.168.0.140

Trace complete.
```

01 CONSOLIDATION VLSM & OSPF

SCHÉMA LOGIQUE



02

HAUTE DISPONBILITÉ ET SERVICES RÉSEAU

DEPLOYER LES SERVICES DE BASE (DHCP + DNS)

DHCP RELAY

Le but était de ne pas multiplier les serveurs DHCP sur chaque site, mais d'avoir un seul serveur DHCP centralisé (hébergé sur R1) qui distribue des adresses IP à toutes les machines du réseau.

Chaque VLAN (Pédagogie, Administration, Tech, Stagiaires, Direction, Production) a un pool d'adresses défini avec son masque, sa passerelle et son DNS.

Les routeurs R2 et R3, qui desservent leurs propres VLANs, ont été configurés en DHCP relay : cela signifie que lorsqu'un PC envoie une requête DHCP (broadcast), le routeur la redirige vers le serveur DHCP central sur R1.

Résultat attendu : tous les PC du réseau obtiennent automatiquement une IP cohérente avec leur VLAN + le DNS du serveur interne (192.168.0.195).

02

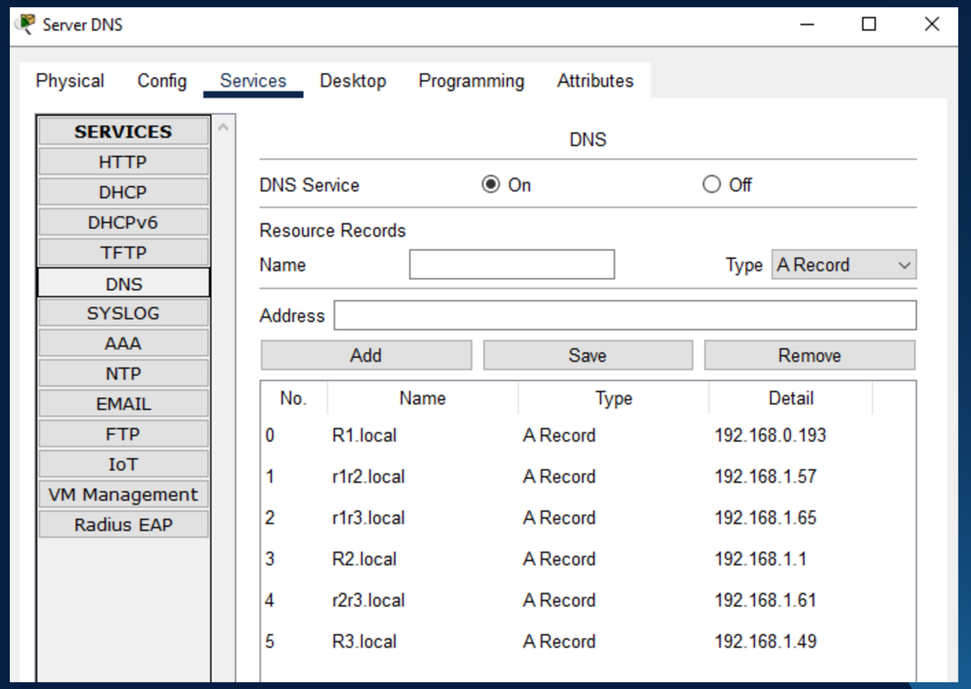
HAUTE DISPONBILITÉ ET SERVICES RÉSEAU

DEPLOYER LES SERVICES DE BASE (DHCP + DNS)

DNS LOCAL

Nous avons mis en place un serveur DNS interne (adresse 192.168.0.195).

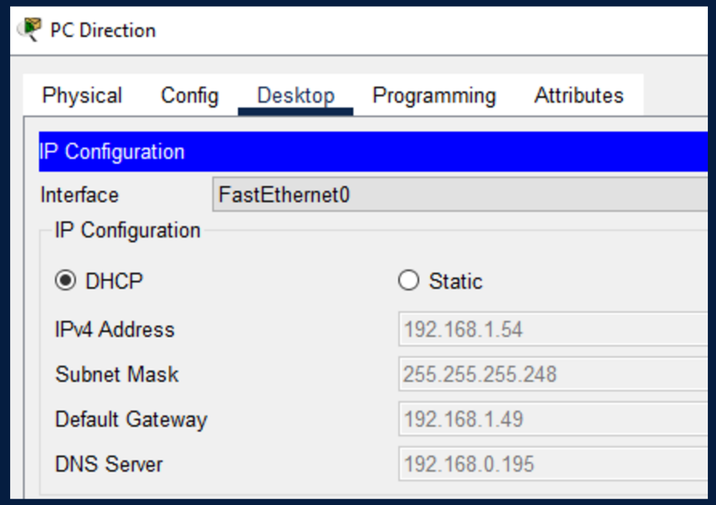
- Le serveur a été configuré pour répondre aux requêtes locales (exemple : R1.local) qui pointe vers le serveur web en DMZ, r1.local pour le routeur R1, etc.).
- Le serveur DHCP de R1 distribue cette IP (192.168.0.195) comme DNS par défaut pour tous les postes.



02

HAUTE DISPONBILITÉ ET SERVICES RÉSEAU

DEPLOYER LES SERVICES DE BASE (DHCP + DNS)



LE PC DIRECTION OBTIENT BIEN UNE IP VIA LE DHCP ET L'IP DU DNS

TEST

```
C:\>ping R1.local

Pinging 192.168.0.193 with 32 bytes of data:

Reply from 192.168.0.193: bytes=32 time=10ms TTL=254
Reply from 192.168.0.193: bytes=32 time<1ms TTL=254
Reply from 192.168.0.193: bytes=32 time<1ms TTL=254
Reply from 192.168.0.193: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.0.193:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

LE PC TECH REUSSI BIENEN À COMMUNIQUUER AVEC L'IP DU SERVEUR WEB

02

HAUTE DISPONBILITÉ ET SERVICES RÉSEAU

DEPLOYER LES SERVICES DE BASE (DHCP + DNS)

CONCLUSION

Cette étape a permis de mettre en place :

Un DHCP centralisé (simplification de l'adressage).
Un DNS local (résolution interne des services).

Donc l'ensemble contribue à la fiabilité et la résilience du réseau : les utilisateurs n'ont pas besoin de reconfigurer leurs postes.

03

SÉCURITÉ & DMZ

MISE EN PLACE D’UNE ZONE DMZ

L’objectif était d’ajouter une zone DMZ (Demilitarized Zone) reliée à R1 pour héberger un serveur web.

- La DMZ a été créée sous forme d’un VLAN spécifique (VLAN 70) avec son propre plan d’adressage (192.168.2.0/28).
- Le serveur web de test a été placé dans ce VLAN, avec une IP fixe (exemple : 192.168.2.2).
- R1 a été configuré avec une sous-interface pour ce VLAN, jouant le rôle de passerelle de la DMZ (192.168.2.1).

Intérêt : isoler le serveur web des LAN internes tout en le rendant accessible depuis l’extérieur (WAN).

03

SÉCURITÉ & DMZ

APPLICATION DES ACL (LISTES DE CONTRÔLE D'ACCÈS)

Pour sécuriser les flux, des ACLs ont été appliquées sur R1 (interface reliée au WAN).

- Autoriser WAN → DMZ uniquement sur les ports HTTP (80) et HTTPS (443).
- Interdire WAN → LAN afin d'empêcher toute tentative d'accès direct aux VLAN internes depuis l'extérieur.
- Autoriser LAN → DMZ et LAN → WAN pour que les utilisateurs internes puissent consulter le serveur web et accéder à Internet.

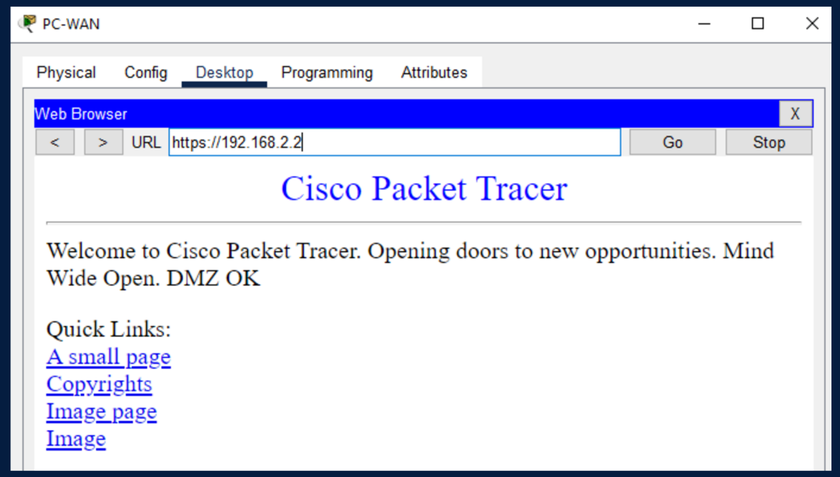
Intérêt : limiter strictement ce que le WAN peut atteindre, tout en préservant les communications internes.

03

SÉCURITÉ & DMZ

TESTS DE SECURITÉ DOCUMENTÉS

TEST



Depuis le pc WAN, on peut accéder au contenu du serveur web grâce au DMZ

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Depuis le pc WAN, le ping vers un VLAN du réseau est un echec

03

SÉCURITÉ & DMZ

DOCUMENTATION DE LA POLITIQUE DE SÉCURITÉ

Intérêt de la DMZ et des ACLs

- La DMZ permet de mettre un serveur accessible depuis Internet tout en limitant l’exposition du LAN.
- Les ACLs agissent comme un pare-feu simple sur le routeur, en filtrant les flux selon leur origine, destination et protocole.
- On respecte ainsi le principe de séparation des zones de sécurité : WAN, DMZ, LAN.

04

SUPERVISION ET PROJET FINAL

MISE EN PLACE DU SYSLOG

CENTRALISER LA SUPERVISION DU RÉSEAU

L’objectif était de centraliser les logs réseau pour faciliter le suivi et le diagnostic.

- Un serveur Syslog a été ajouté dans le réseau (IP : 192.168.1.52).
- Tous les équipements (routeurs et switches) ont été configurés pour envoyer leurs journaux vers ce serveur.
- Chaque événement (ex. perte de lien, authentification, changements de configuration) remonte automatiquement au serveur Syslog.

Intérêt : cela permet une vision centralisée des événements réseau au lieu de devoir vérifier chaque équipement séparément.

04

SUPERVISION ET PROJET FINAL

CENTRALISER LA SUPERVISION DU RÉSEAU

Le protocole SNMP (Simple Network Management Protocol) a été activé sur les routeurs pour permettre une supervision externe.

ACTIVATION DE SNMP

- Chaque routeur agit comme un agent SNMP, exposant des informations de base : interfaces, uptime, état des liens.
- Un poste client (PC SNMP) joue le rôle de manager SNMP grâce à l'outil MIB Browser.
- Le manager peut interroger les routeurs en temps réel pour connaître par exemple l'état d'une interface ou la durée de fonctionnement d'un équipement.
-

Intérêt : SNMP complète le Syslog. Là où Syslog envoie des événements, SNMP permet des mesures et statistiques en continu (état, performance).

04

SUPERVISION ET PROJET FINAL

MINI PROJET INTÉGRÉ

À ce stade, tout le projet complet est en place :

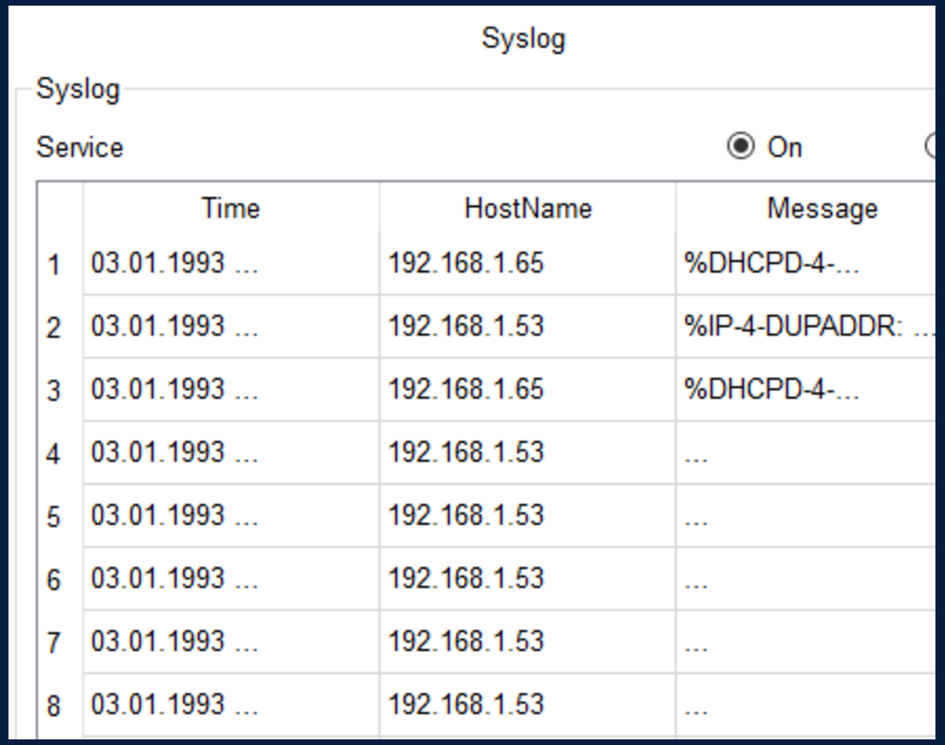
- VLSM + OSPF : adressage IP optimisé et routage dynamique opérationnel.
- DHCP centralisé + DNS local : attribution automatique des IP et résolution de noms internes.
- HSRP : mise en redondance des passerelles pour la haute disponibilité.
- DMZ + ACL : sécurité assurée avec isolation des zones et filtrage du trafic.
- Syslog + SNMP : supervision centralisée et interrogation des équipements.

Ce projet intègre connectivité, services, sécurité et supervision, ce qui correspond à une architecture réseau complète.

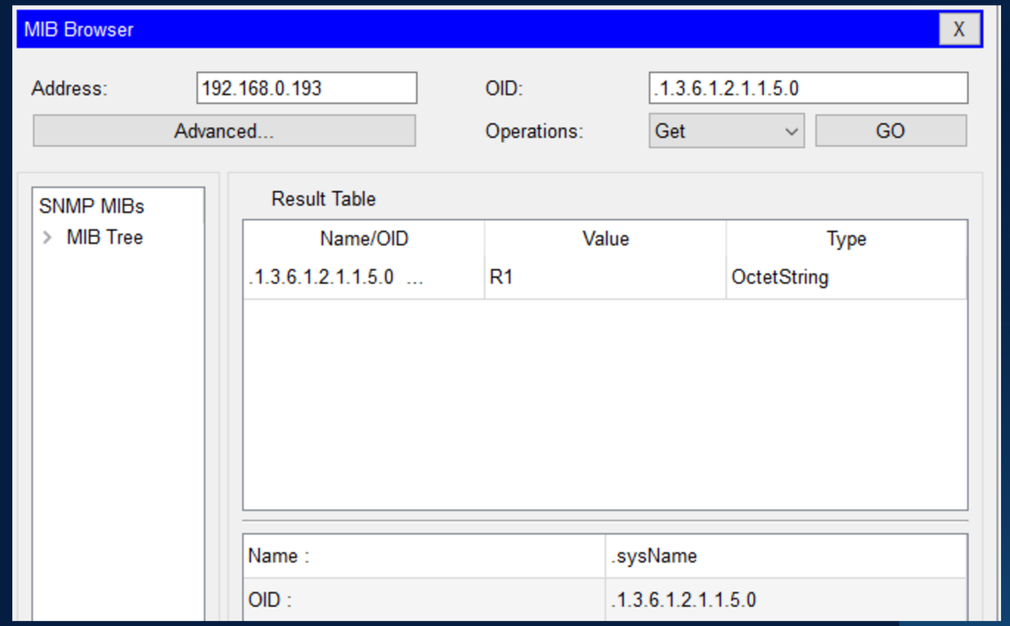
04

SUPERVISION ET PROJET FINAL

VALIDATION ET TESTS



Syslog : les événements générés par les routeurs et switches apparaissent bien sur le serveur Syslog.



SNMP : depuis le PC manager, interrogation des routeurs

04

CONCLUSION

RAPPORT FINAL

Avec cette dernière étape, le projet est complet :
Supervision (Syslog + SNMP) assure une visibilité sur l’état du réseau.

Les services et protocoles (DHCP, DNS, OSPF, HSRP, ACL) sont tous intégrés et fonctionnels.

Le réseau est désormais fiable, sécurisé, redondant et monitoré.

Ce projet final illustre la mise en place d’une infrastructure professionnelle regroupant adressage, routage, services de base, sécurité et supervision.