LEIDOSCOPE

Projet AP1 Infrasite

Rapport de tests final



Deniz Elhasoglu et Nathan Ogoreck

Lycée Saint Adjutor
Groupe 5 • Mme PITOIS
Année scolaire 2026–2027

BTS SIO • OPTION SISR • DEUXIÈME ANNÉE

13 octobre 2026

Sommaire

Activité 4 – Administration SSH

Activité 6 – Routage et connectivité

Activité 7 – Serveur TFTP et sauvegardes

Activité 8 – Internet NAT/PAT et NAT statique

Activité 9 – Pare-feu

Activité 10 – ACL et services

Objet du document

Ce rapport regroupe les tests réalisés sur l'infrastructure, dans le même ordre que le document technique. Pour chaque test sont indiqués l'objectif, le périmètre, la procédure, le résultat attendu, le résultat observé et le statut. Un blocage attendu constitue un résultat conforme.

Les adresses, le schéma réseau et les comptes sont détaillés dans le document technique et dans le Notion du groupe.

Statuts utilisés : Validé (résultat visible sur la capture), Validé partiellement (une partie du périmètre seulement est visible), Constaté en séance (test réalisé et noté dans le suivi Trello, capture peu lisible).

Synthèse des tests

22 tests réalisés : 19 validés, 2 validés partiellement et 1 constaté en séance.

Activité	Test	Statut
4 – SSH	Accès SSH depuis le VLAN IT vers RNET1	**Validé**
4 – SSH	Accès SSH aux commutateurs internes (SwE1, SwCoeur)	**Validé**
4 – SSH	Connexion SSH acceptée sur SwRC et SwE2Serveur	**Validé partiellement**
4 – SSH	Refus SSH depuis un VLAN non autorisé	**Validé**
6 – Routage	Apprentissage des routes RIPv2	**Validé**
6 – Routage	Routes par défaut de SwCoeur et RNET1	**Validé**
6 – Routage	Lien cœur–pare-feu joignable depuis RNET1	**Validé**
6 – Routage	RNET1 vers la DMZ et le VLAN serveurs	**Validé**
6 – Routage	Retour depuis SwDMZ vers le LAN et RNET1	**Validé**
6 – Routage	Pings depuis le pare-feu	**Validé**
7 – TFTP	Connectivité locale du serveur TFTP	**Validé**
7 – TFTP	Réception des sauvegardes dans /srv/tftp/backups	**Validé partiellement**
8 – NAT	Sortie Internet de RNET1	**Validé**
8 – NAT	Sortie Internet des serveurs AD et TFTP	**Validé**
8 – NAT	Sortie Internet des postes utilisateurs	**Validé**
8 – NAT	NAT statique du serveur DMZ depuis le campus	**Validé**
9 – Pare-feu	Administration SSH après configuration du pare-feu	**Validé**
9 – Pare-feu	Accès Internet filaire depuis IT	**Validé**
10 – ACL	Attribution DHCP dans le VLAN 10	**Validé**

Activité	Test	Statut
10 – ACL	Accès à l’AD depuis un autre service	**Validé**
10 – ACL	Communication dans un même service	**Validé**
10 – ACL	Blocage entre services	**Constaté en séance**

Activité 4 – Administration SSH

Accès SSH depuis le VLAN IT

Objectif. Vérifier qu'un poste du VLAN 60 peut administrer RNET1 en SSH.

Périmètre. Client IT 172.21.60.2/24 vers RNET1 192.168.3.252.

Procédure de contrôle. Obtenir une adresse DHCP dans le VLAN IT puis ouvrir une session SSH vers RNET1.

Résultat attendu	Résultat observé
Authentification possible et invite de l'équipement affichée.	Le poste reçoit l'adresse 172.21.60.2 et la session SSH vers RNET1 s'ouvre.

Statut. Validé.



Figure 1 – Client du VLAN IT

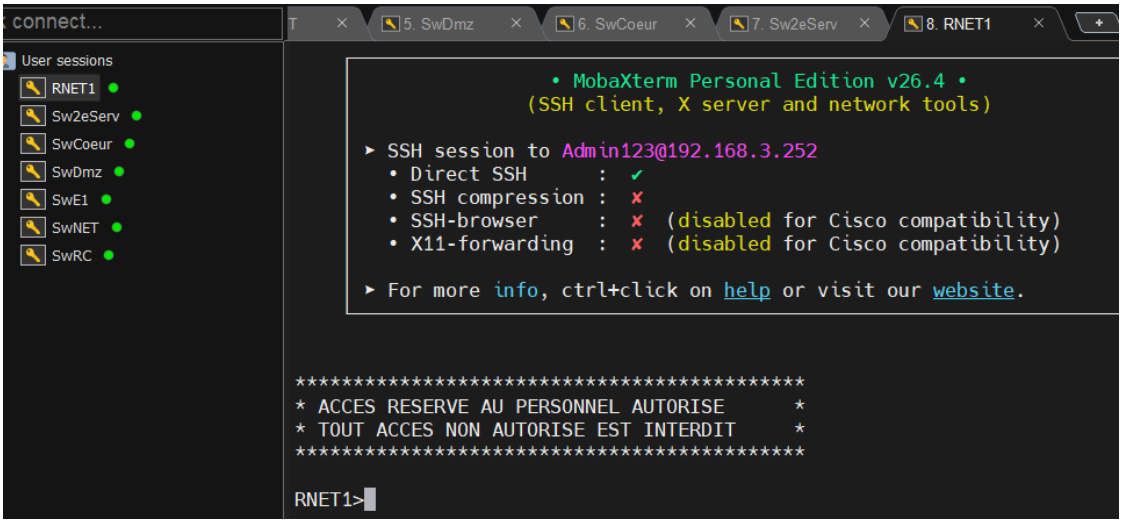


Figure 2 – SSH autorisé vers RNET1

Accès SSH aux commutateurs internes

Objectif. Vérifier l'accès individualisé aux adresses de gestion.

Périmètre. Poste autorisé vers SwE1 172.21.70.1 et SwCoeur 172.21.70.254.

Procédure de contrôle. Ouvrir une session SSH vers chaque adresse.

Résultat attendu	Résultat observé
Chaque équipement présente sa propre invite après authentification.	Deux sessions authentifiées sont visibles dans les captures.

Statut. Validé.

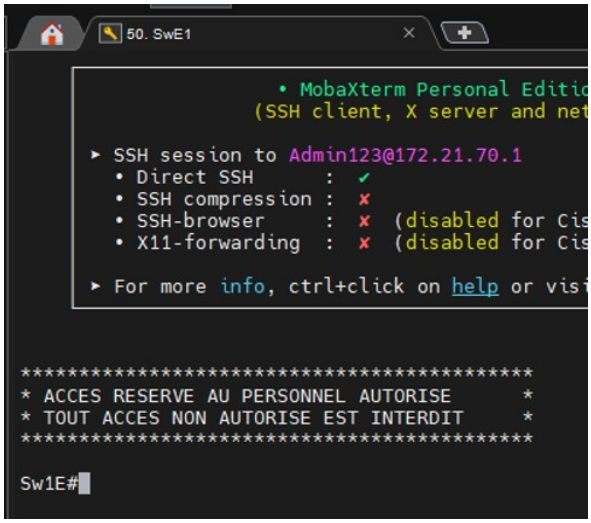


Figure 3 – SSH vers SwE1

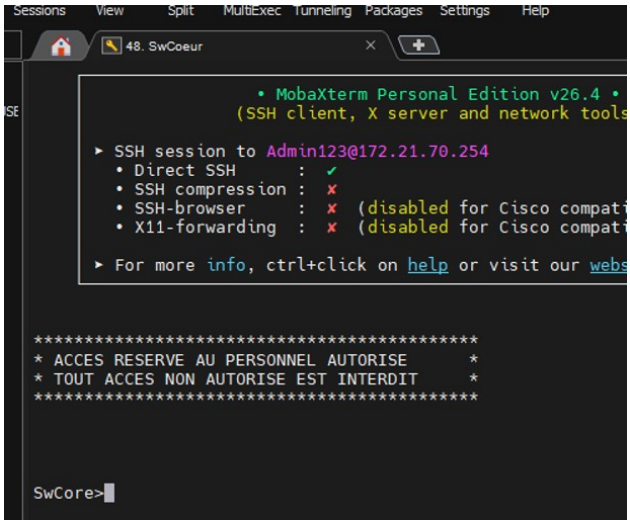


Figure 4 – SSH vers SwCoeur

SwRC et SwE2Serveur

Objectif. Compléter le contrôle d'administration individuelle.

Périmètre. Poste IT vers SwRC 172.21.70.3 et SwE2Serveur 172.21.70.2.

Procédure de contrôle. Ouvrir une session SSH vers chacune des adresses de gestion.

Résultat attendu	Résultat observé
Authentification réussie et invite propre à chaque commutateur.	SwRC et SwE2Serveur affichent l'invite d'identification « login as: » : la connexion SSH depuis le VLAN IT est acceptée par les deux commutateurs.

Statut. Validé partiellement : connexion acceptée, ouverture de session non capturée.

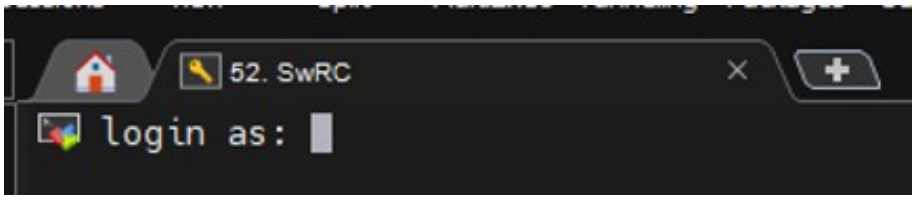


Figure 5 – Invite SSH de SwRC

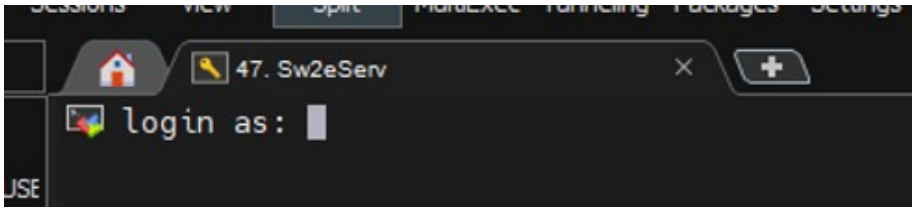


Figure 6 – Invite SSH de SwE2Serveur

Refus SSH depuis un VLAN non autorisé

Objectif. Vérifier que l'administration n'est pas accessible depuis le VLAN 80.

Périmètre. Client Direction/RH 172.21.80.1/24 vers RNET1 et les équipements Cisco.

Procédure de contrôle. Obtenir une adresse dans le VLAN 80 puis tenter une session SSH vers les équipements.

Résultat attendu	Résultat observé
La connexion doit être refusée. Un blocage attendu constitue un test réussi.	La connexion vers RNET1 est refusée. Sur SwRC, MobaXterm affiche « Network error: Connection refused ».

Statut. Validé pour RNET1 et SwRC ; refus constaté en séance sur les autres commutateurs.

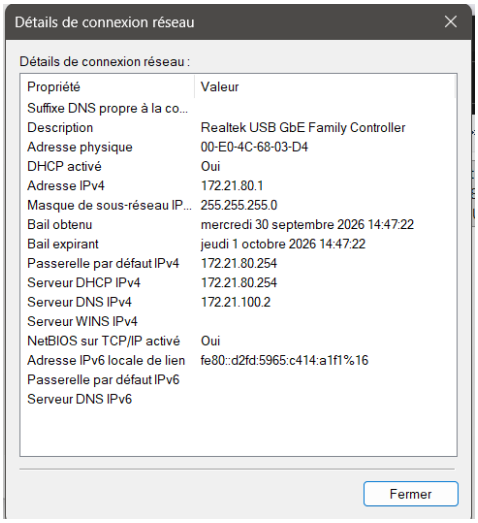


Figure 7 – Client du VLAN 80

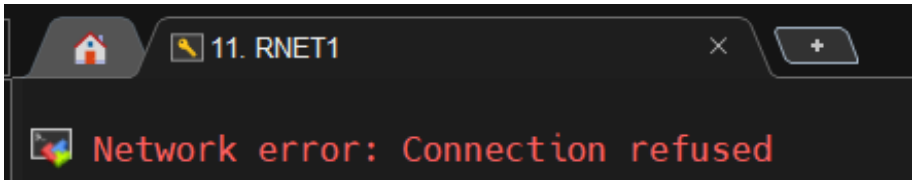


Figure 8 – SSH refusé vers RNET1

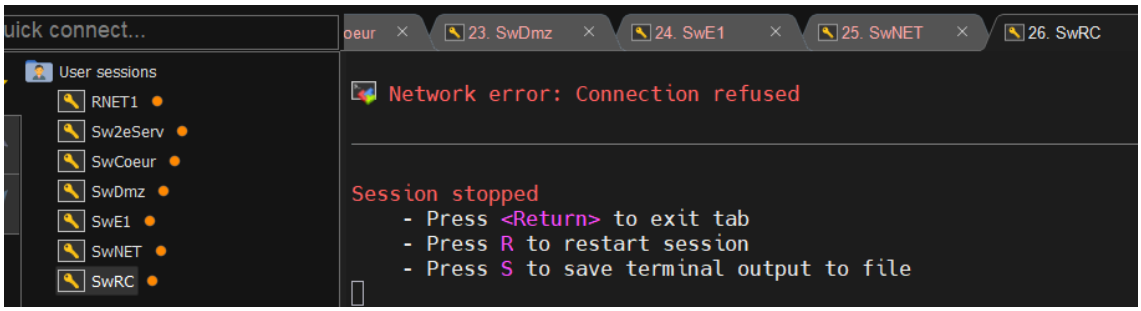


Figure 9 – Refus SSH hors IT

Activité 6 – Routage et connectivité

Apprentissage des routes

Objectif. Contrôler la présence des réseaux distants sur les trois équipements de routage.

Périmètre. SwCoeur, Zyxel et RNET1 ; LAN, transit et DMZ.

Procédure de contrôle. Afficher les tables de routage ; sur Cisco utiliser show ip route.

Résultat attendu	Résultat observé
Routes LAN connectées sur le cœur ; réseaux distants appris par RIP sur les équipements concernés.	Les réseaux distants apparaissent avec le code R (appris par RIP) dans les tables de routage.

Statut. Validé.

```
Gateway of last resort is not set

      10.0.0.0/16 is subnetted, 1 subnets
R        10.5.0.0 [120/1] via 172.21.90.253, 00:00:13, Vlan90
      172.21.0.0/16 is variably subnetted, 20 subnets, 3 masks
C        172.21.10.0/24 is directly connected, Vlan10
L        172.21.10.254/32 is directly connected, Vlan10
C        172.21.20.0/24 is directly connected, Vlan20
L        172.21.20.254/32 is directly connected, Vlan20
C        172.21.30.0/24 is directly connected, Vlan30
L        172.21.30.254/32 is directly connected, Vlan30
C        172.21.40.0/24 is directly connected, Vlan40
L        172.21.40.254/32 is directly connected, Vlan40
C        172.21.50.0/24 is directly connected, Vlan50
L        172.21.50.254/32 is directly connected, Vlan50
C        172.21.60.0/24 is directly connected, Vlan60
L        172.21.60.254/32 is directly connected, Vlan60
C        172.21.70.0/24 is directly connected, Vlan70
L        172.21.70.254/32 is directly connected, Vlan70
C        172.21.80.0/24 is directly connected, Vlan80
L        172.21.80.254/32 is directly connected, Vlan80
C        172.21.90.252/30 is directly connected, Vlan90
L        172.21.90.254/32 is directly connected, Vlan90
C        172.21.100.0/24 is directly connected, Vlan100
L        172.21.100.254/32 is directly connected, Vlan100
      192.168.3.0/29 is subnetted, 1 subnets
R        192.168.3.248 [120/1] via 172.21.90.253, 00:00:13, Vlan90
SwCore#
```

Figure 10 – Routes du cœur

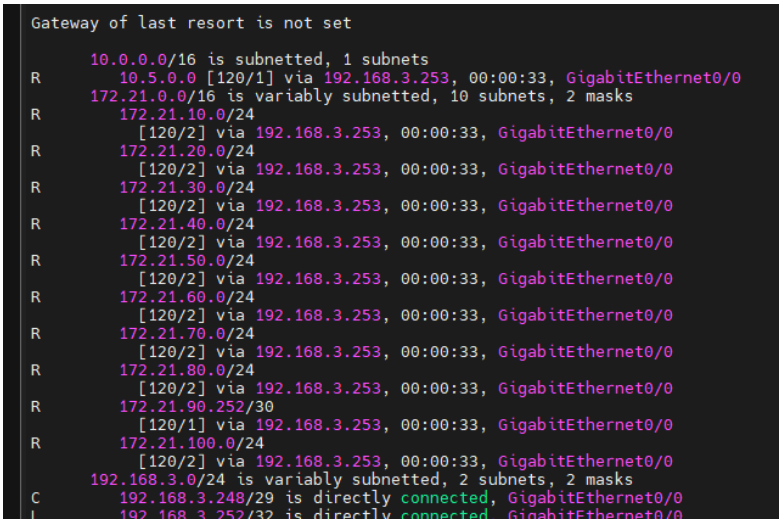


Figure 11 – Routes de RNET1

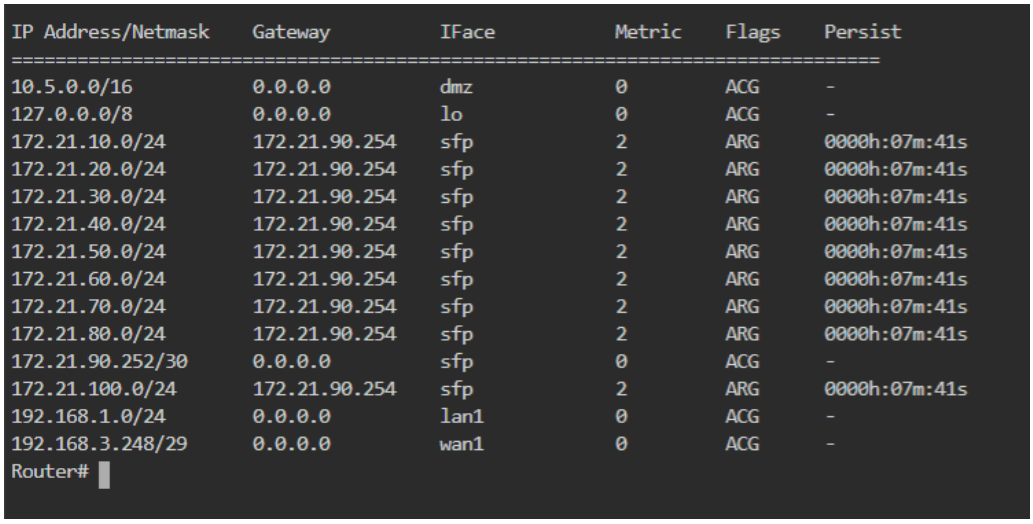


Figure 12 – Routes du Zyxel

Sortie de chaque zone

Objectif. Vérifier les prochains sauts par défaut.

Périmètre. SwCoeur vers 172.21.90.253 ; Zyxel vers 192.168.3.252 ; RNET1 vers 192.168.4.254.

Procédure de contrôle. Afficher la table de routage et rechercher la route 0.0.0.0/0.

Résultat attendu	Résultat observé
Une route par défaut vers le prochain saut prévu est présente.	Les tables de SwCoeur et de RNET1 contiennent la route par défaut vers le prochain saut prévu.

Statut. Validé pour SwCoeur et RNET1. La route par défaut du Zyxel est présentée dans le document technique (activité 6).

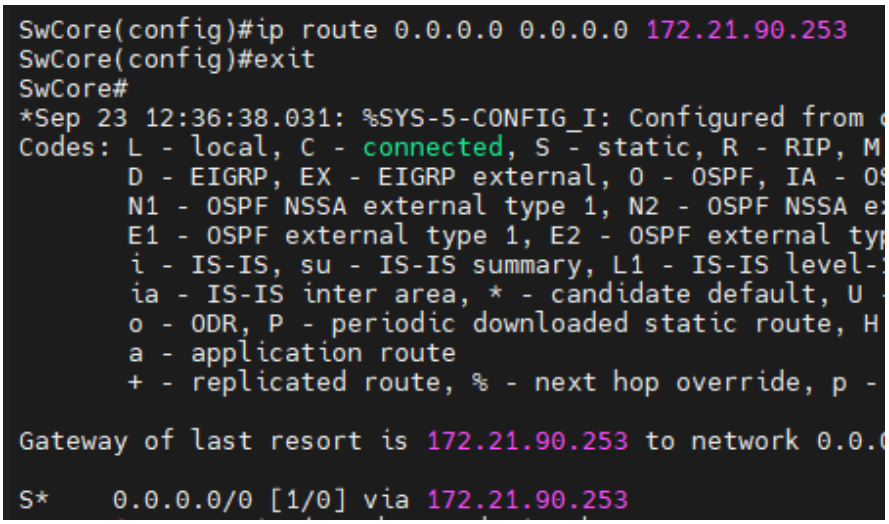


Figure 13 – Route par défaut du cœur

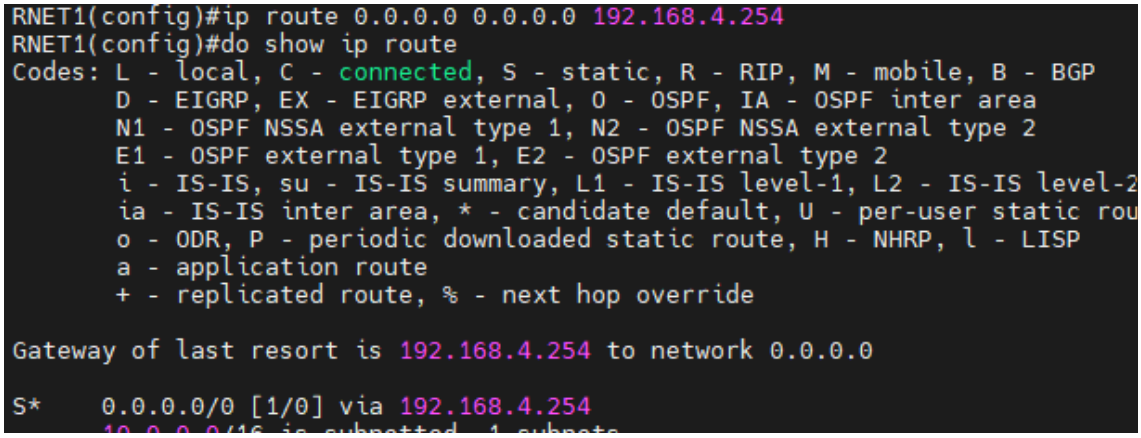


Figure 14 – Route par défaut de RNET1

Joignabilité du lien cœur–pare-feu depuis RNET1

Objectif. Vérifier le chemin de RNET1 jusqu'aux deux extrémités du VLAN 90.

Périmètre. RNET1 vers 172.21.90.253 et 172.21.90.254.

Procédure de contrôle. Lancer cinq requêtes ICMP vers chaque adresse.

Résultat attendu	Résultat observé
Cinq réponses sur cinq pour le Zyxel et le cœur.	Les deux séries reçoivent cinq réponses sur cinq.

Statut. Validé.

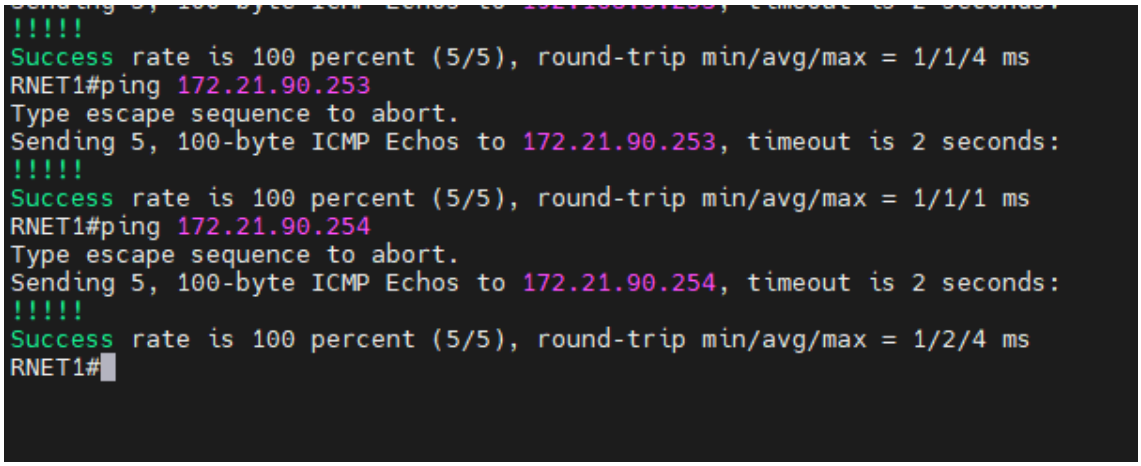


Figure 15 – RNET1 vers le VLAN 90

Connectivité RNET1 vers DMZ et serveurs

Objectif. Valider le transit de RNET1 vers SwDMZ et la passerelle du VLAN serveurs.

Périmètre. RNET1 vers 10.5.10.253 et 172.21.100.254.

Procédure de contrôle. Lancer cinq requêtes ICMP vers chaque cible.

Résultat attendu	Résultat observé
Cinq réponses sur cinq pour chaque cible.	SwDMZ répond 4 fois sur 5 (la première requête est perdue pendant la résolution ARP) ; la passerelle serveurs répond 5 fois sur 5.

Statut. Validé.

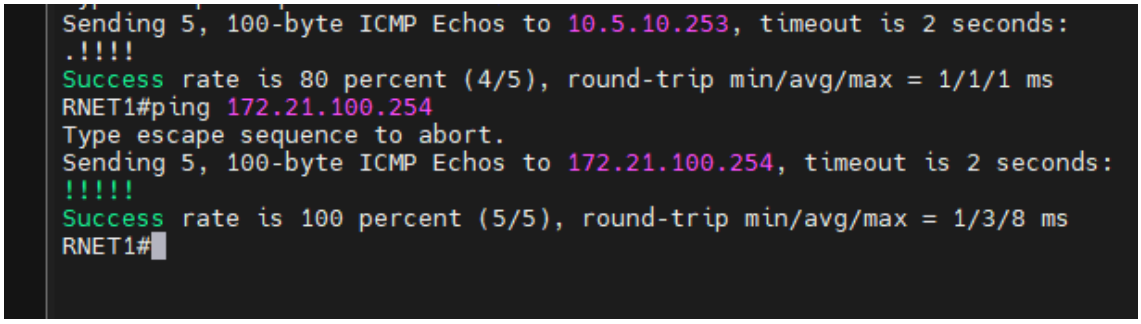


Figure 16 – RNET1 vers DMZ et serveurs

Connectivité depuis SwDMZ

Objectif. Vérifier le retour depuis la DMZ vers le LAN et RNET1.

Périmètre. SwDMZ vers 172.21.100.254 et 192.168.3.252.

Procédure de contrôle. Lancer cinq requêtes ICMP vers chaque cible.

Résultat attendu	Résultat observé
Cinq réponses sur cinq vers les deux cibles.	Les deux destinations répondent cinq fois sur cinq.

Statut. Validé.

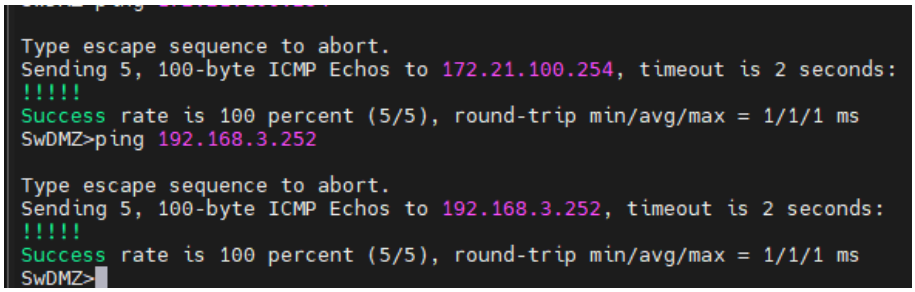


Figure 17 – SwDMZ vers LAN et RNET1

Ce test a été réalisé avant l'activation de la règle Isolation_DMZ_LAN (activité 9) : il valide le routage entre les zones, pas le filtrage final du pare-feu.

Connectivité des interfaces du pare-feu

Objectif. Vérifier depuis le Zyxel les équipements reliés.

Périmètre. Zyxel vers le cœur, SwDMZ et SwNET.

Procédure de contrôle. Utiliser l'outil Ping du pare-feu vers chaque cible.

Résultat attendu	Résultat observé
Réponses sans perte pour chaque cible.	Le cœur répond 3 fois sur 3. SwDMZ et SwNET répondent 2 fois sur 3 : seule la première requête est perdue, pendant la résolution ARP.

Statut. Validé.

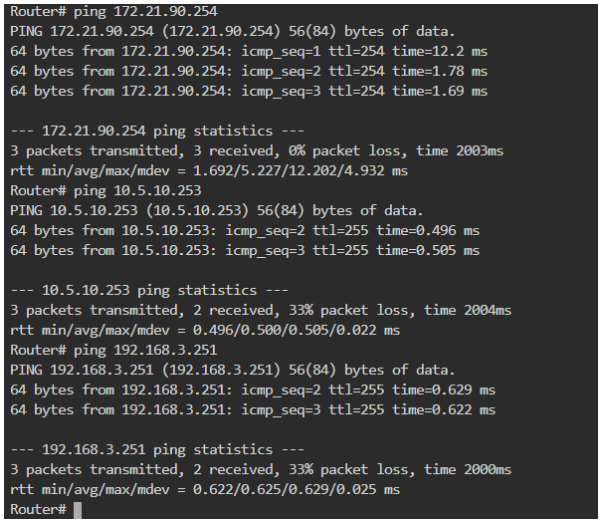


Figure 18 – Pings depuis le Zyxel

Activité 7 – Serveur TFTP et sauvegardes

Connectivité locale du serveur TFTP

Objectif. Vérifier que le serveur TFTP joint les services de son VLAN.

Périmètre. Ubuntu 172.21.100.3 vers AD 172.21.100.2 et Hyper-V 172.21.100.1.

Procédure de contrôle. Lancer des pings vers les deux adresses.

Résultat attendu	Résultat observé
Les deux cibles répondent.	Des réponses sont visibles pour les deux cibles.

Statut. Validé.

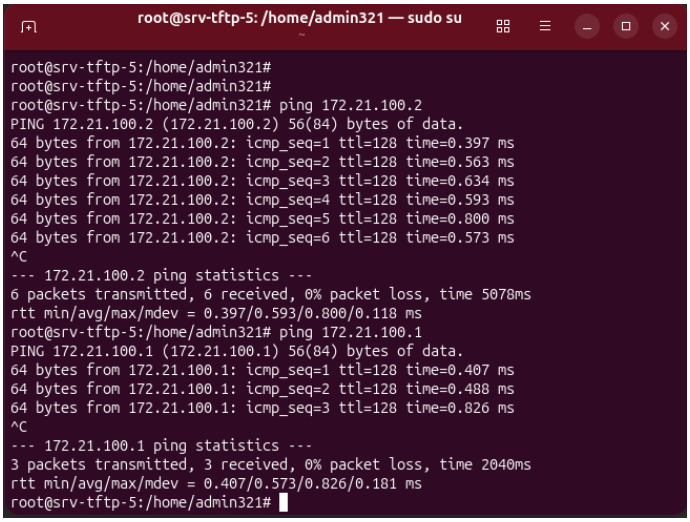


Figure 19 – TFTP vers AD et Hyper-V

Préparation du répertoire de sauvegarde

Observation. Le dossier /srv/tftp/backups est présent sur le serveur et contient 8 éléments.

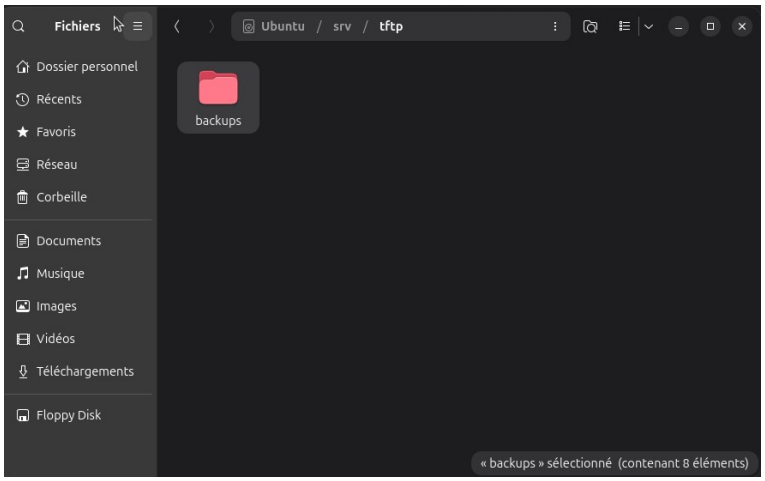


Figure 20 – Répertoire backups créé sur le serveur TFTP

Statut. Validé partiellement : le dossier de réception contient des fichiers, mais leurs noms n'apparaissent pas sur la capture.

Activité 8 – Internet NAT/PAT et NAT statique

Sortie Internet de RNET1

Objectif. Vérifier le chemin du routeur vers le campus et Internet.

Périmètre. RNET1 vers 192.168.4.254 et 8.8.8.8.

Procédure de contrôle. Lancer cinq requêtes ICMP vers chaque cible.

Résultat attendu	Résultat observé
Cinq réponses sur cinq.	Le campus et 8.8.8.8 répondent cinq fois sur cinq.

Statut. Validé.

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
RNET1#ping 192.168.4.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
RNET1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/12 ms
RNET1#
```

Figure 21 – RNET1 vers campus et Internet

Sortie Internet des serveurs

Objectif. Vérifier que les serveurs du VLAN 100 sortent vers Internet.

Périmètre. Serveur AD 172.21.100.2 et serveur TFTP 172.21.100.3 vers 8.8.8.8.

Procédure de contrôle. Lancer un ping depuis chaque serveur.

Résultat attendu	Résultat observé
Réponses reçues sans perte.	Le serveur AD reçoit 4 réponses sur 4. Le serveur TFTP reçoit 5 réponses de 8.8.8.8 avant l'arrêt du ping.

Statut. Validé.

```
Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octet
Réponse de 8.8.8.8 : octets=32 temps=11 ms TTL=11
Réponse de 8.8.8.8 : octets=32 temps=5 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=6 ms TTL=111

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0
Durée approximative des boucles en millisecondes
    Minimum = 5ms, Maximum = 11ms, Moyenne = 7ms
```

Figure 22 – Internet depuis AD

```
admin321@srv-tftp-5:/$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=6.16 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=5.47 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=6.94 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=6.58 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=111 time=5.85 ms
^C
```

Figure 23 – Internet depuis TFTP

Sortie Internet de postes utilisateurs

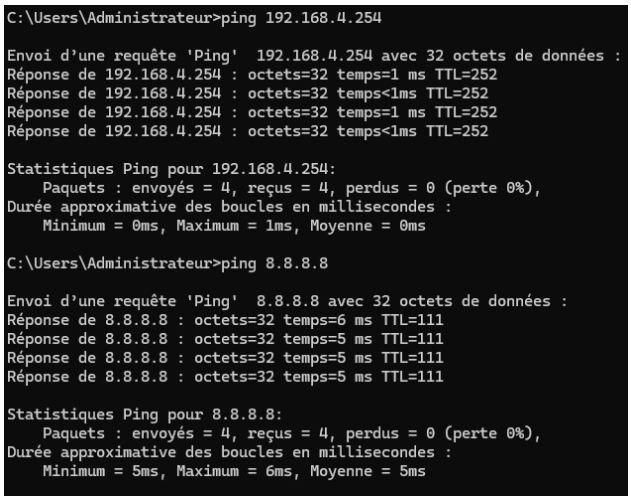
Objectif. Vérifier l’accès Internet depuis plusieurs VLAN du LAN.

Périmètre. Postes Windows, dont Formation, vers 192.168.4.254 et 8.8.8.8.

Procédure de contrôle. Lancer quatre requêtes ICMP depuis chaque poste.

Résultat attendu	Résultat observé
Quatre réponses sur quatre.	Les captures montrent quatre réponses sur quatre vers Internet et, pour un poste, vers la passerelle campus.

Statut. Validé.



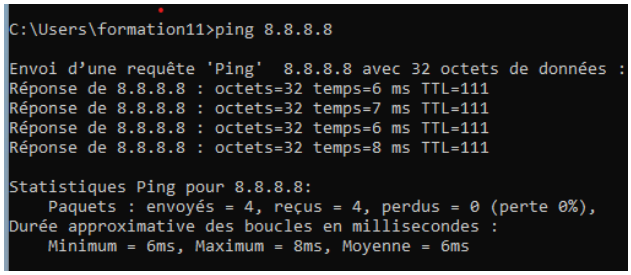


Figure 24 – Internet depuis un poste • Internet depuis Formation11

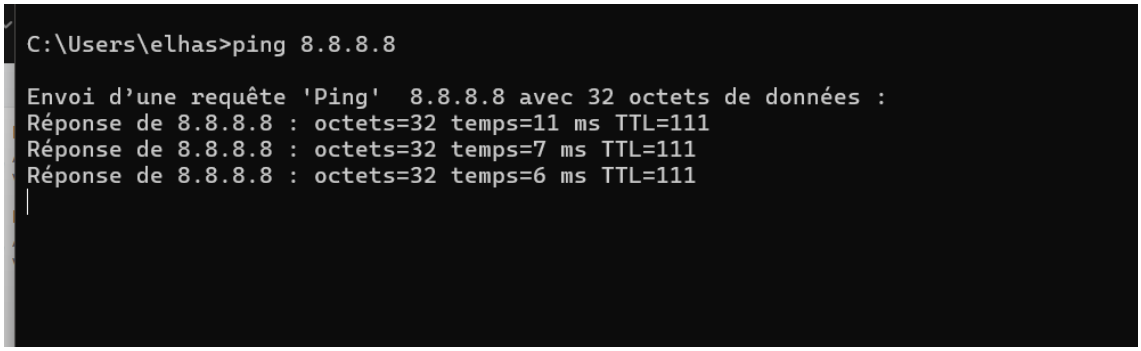


Figure 25 – Ping Internet depuis le LAN

Ces tests valident la sortie Internet des postes du LAN à travers le pare-feu et le NAT/PAT de RNET1.

NAT statique depuis le réseau campus

Objectif. Vérifier que l’adresse publiée 192.168.4.59 permet d’atteindre le serveur DMZ 10.5.10.1 à travers RNET1.

Périmètre. Poste du réseau campus (192.168.4.104) vers l’adresse publiée 192.168.4.59.

Procédure de contrôle. Depuis le réseau campus, lancer ping 192.168.4.59 ; sur RNET1, afficher show ip nat translations pendant le flux.

Contrôle	Résultat observé	Statut
Ping vers l’adresse publiée	Deux séries de 4 requêtes : 4 reçues, 0 perdu, soit 0 % de perte ; temps de 2 ms.	Validé

Contrôle	Résultat observé	Statut
Traduction sur RNET1	icmp : inside global 192.168.4.59:1 ; inside local 10.5.10.1:1 ; outside local et global 192.168.4.104:1.	Validé
Route de retour vers la DMZ	S 10.5.0.0 [1/0] via 192.168.3.253 apparaît dans la table de routage.	Validé

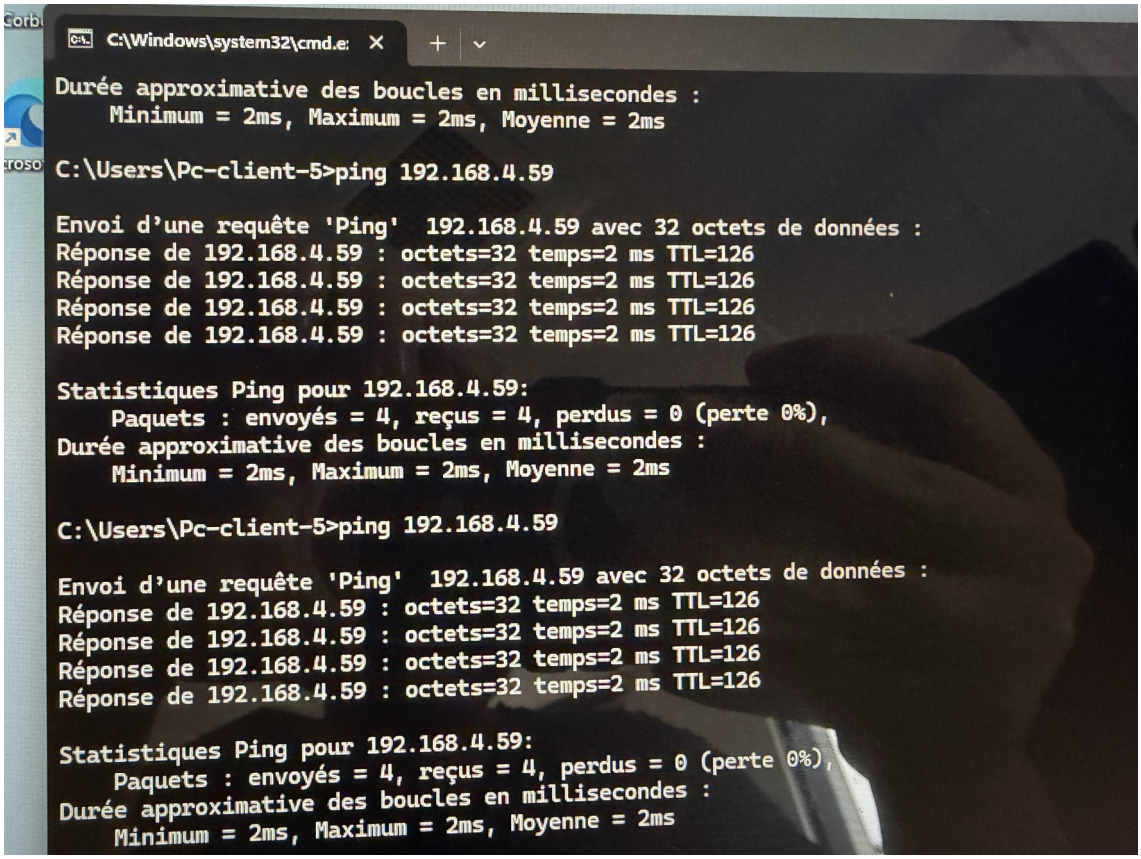


Figure 26 – Ping campus vers 192.168.4.59 avec aucune perte

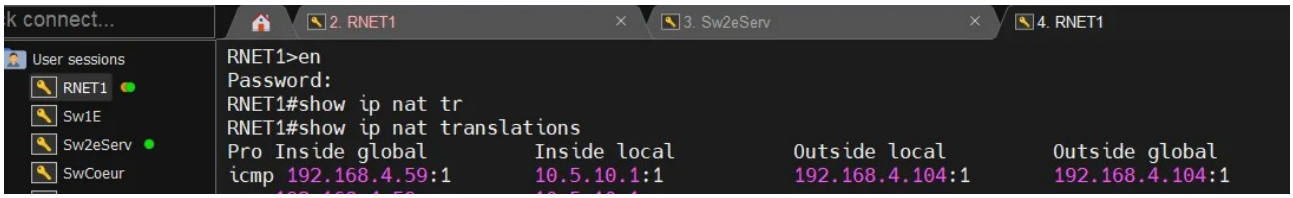


Figure 27 – Traduction ICMP observée sur RNET1 pendant le test campus

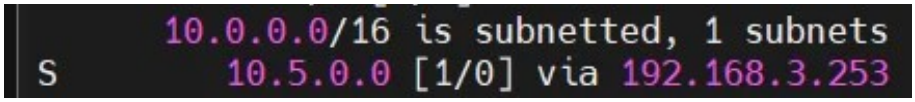


Figure 28 – Route statique DMZ observée dans la table de routage

Conclusion. L'adresse publiée 192.168.4.59 est joignable depuis le réseau campus et RNET1 la traduit vers le serveur DMZ 10.5.10.1. Le test a été réalisé en ICMP.

Activité 9 – Pare-feu

La politique finale utilise une zone SFP indépendante pour la liaison vers le cœur. Les tests suivants ont été réalisés après la mise en place de cette politique.

Tests après configuration du pare-feu

Administration SSH des équipements

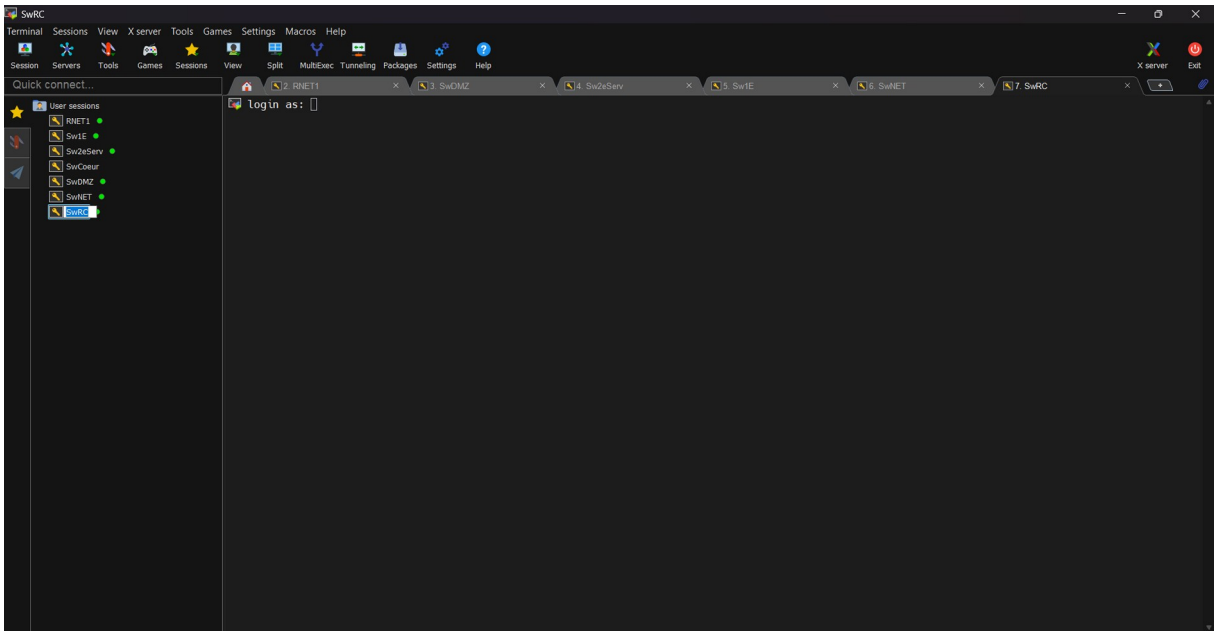
Objectif. Vérifier que les équipements sont accessibles en SSH après la configuration du pare-feu.

Périmètre. RNET1, SwDMZ, SwE2Serveur, SwE1, SwNET et SwRC, depuis le poste IT.

Procédure. Ouvrir les sessions SSH enregistrées dans MobaXterm. Résultat attendu : connexion acceptée sur chaque équipement.

Résultat observé. Les six sessions sont actives dans MobaXterm (indicateur vert) et SwRC affiche l'invite « login as: ».

Statut. Validé. Les équipements restent administrables depuis IT après l'application des règles du pare-feu.



Accès Internet depuis IT avec le Wi-Fi désactivé

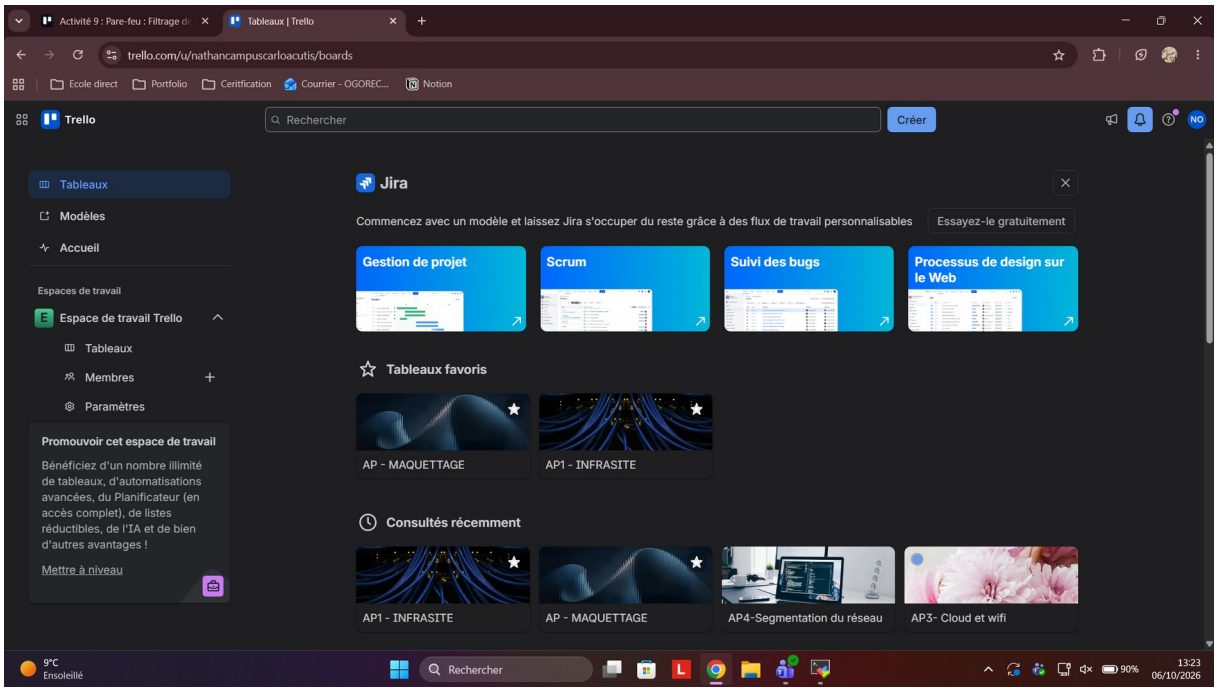
Objectif. Vérifier la sortie Internet du poste IT par l'infrastructure filaire.

Périmètre. Poste du service IT, pare-feu Zyxel et sortie Internet.

Procédure. Désactiver le Wi-Fi du poste puis ouvrir une page Web. Résultat attendu : la page se charge par la connexion filaire.

Résultat observé. La page Trello se charge dans Chrome avec le Wi-Fi désactivé.

Statut. Validé (constaté en séance).



Activité 10 – ACL et services

Attribution DHCP dans le VLAN 10

Objectif. Vérifier qu'un poste Comptabilité reçoit une configuration cohérente.

Périmètre. Client du VLAN 10, passerelle 172.21.10.254 et DNS 172.21.100.2.

Procédure de contrôle. Renouveler le bail puis afficher la configuration IP.

Résultat attendu	Résultat observé
Adresse dans le réseau 172.21.10.0/24, passerelle du VLAN et DNS de l'AD.	Le poste obtient 172.21.10.1/24, la passerelle .10.254 et le DNS .100.2. L'écran affiche le serveur DHCP .10.254.

Statut. Validé.



Figure 29 – Bail DHCP du VLAN 10

Accès à l'Active Directory depuis un autre service

Objectif. Vérifier que l'ACL laisse accéder au service commun AD.

Périmètre. Poste du VLAN 10 Comptabilité, compte Formation, serveur AD 172.21.100.2.

Procédure de contrôle. Ouvrir une session avec un compte du domaine sur un poste du VLAN 10, puis pinger le serveur AD.

Résultat attendu	Résultat observé
L'authentification aboutit malgré l'isolation inter-services.	La session du compte Formation11 est ouverte sur le poste (invite C:\Users\Formation11) et le ping vers l'AD 172.21.100.2 reçoit 4 réponses sur 4.

Statut. Validé.

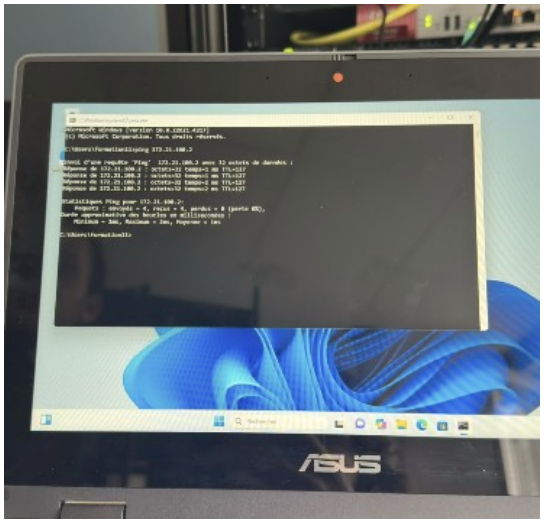


Figure 30 – Essai de connexion au domaine

Communication dans un même service

Objectif. Vérifier que l'ACL ne bloque pas deux postes du même VLAN.

Périmètre. Deux postes du VLAN 10.

Procédure de contrôle. Lancer un ping entre les deux adresses du même réseau.

Résultat attendu	Résultat observé
Les réponses sont reçues.	Le poste reçoit deux réponses de 172.21.10.1, situé dans le même VLAN.

Statut. Validé.

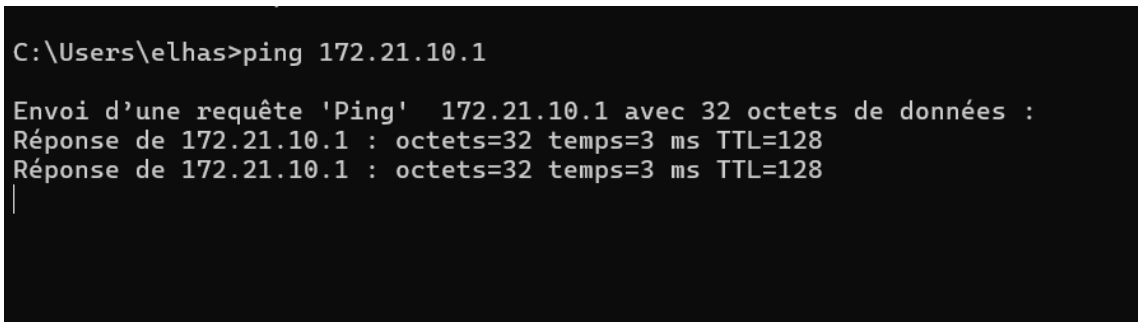


Figure 31 – Ping dans le VLAN 10

Blocage entre services

Objectif. Vérifier que deux VLAN utilisateurs isolés ne communiquent pas directement.

Périmètre. Paires de postes situées dans deux services différents.

Procédure de contrôle. Lancer des pings croisés et une tentative applicative autorisée seulement vers l’AD.

Résultat attendu	Résultat observé
Les échanges directs expirent ; l’accès autorisé vers l’AD reste possible.	Les essais ont été réalisés en séance et notés dans le suivi Trello ; la photographie ne permet pas de lire les adresses.

Statut. Constaté en séance ; capture peu lisible.



Figure 32 – Postes des essais interservices