COMPTE-RENDU DE TP

ACL Standard

Listes de contrôle d'accès — Filtrage inter-VLAN

Étudiant : Ewen Bréhélin | **Identifiant labo :** Administrateur / Admin123
Matière : Infrastructure réseau — BTS SIO SISR | **Référence :** B2-3_6

1. Contexte

Une petite entreprise dispose d'un mini-réseau composé de trois ordinateurs connectés à un switch, lui-même relié à un routeur pour accéder au réseau externe.

Afin d'améliorer la sécurité, l'administrateur décide de mettre en place des listes de contrôle d'accès (ACL) sur le routeur.

Ces ACL permettront de filtrer et de contrôler les communications des trois PC selon des règles définies. L'infrastructure comporte : 3 PC, 1 switch et 2 routeurs.

2. Schéma de l'architecture

Schéma logique (Packet Tracer)

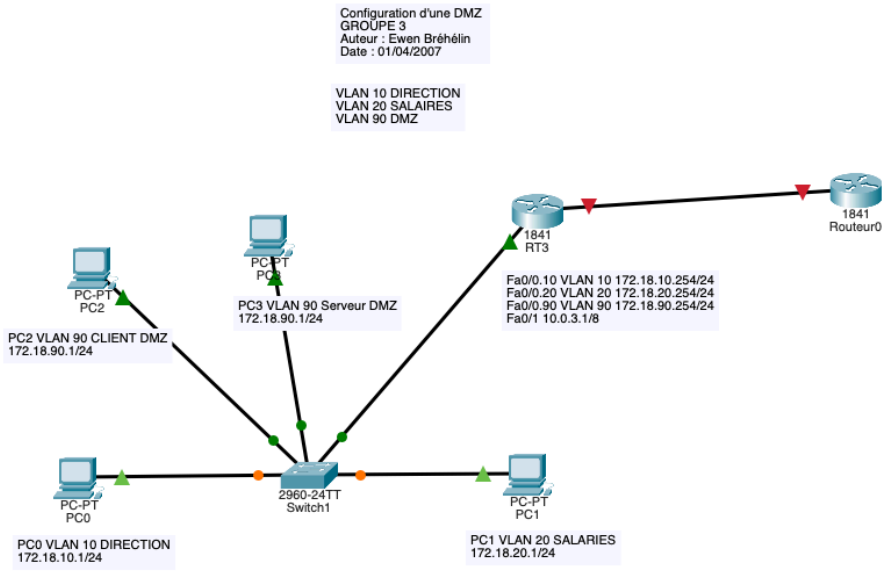
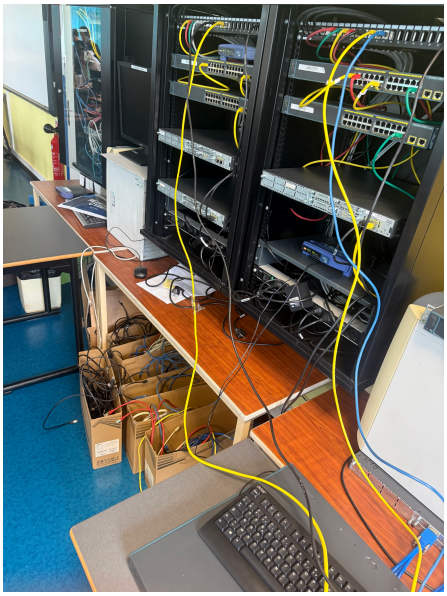
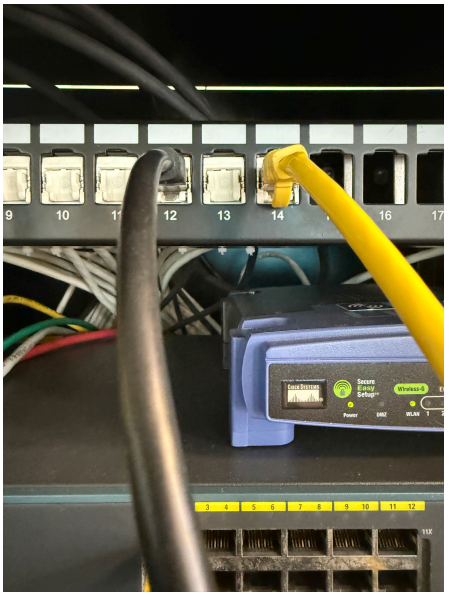


Figure 1 – Topologie réseau (Cisco Packet Tracer)

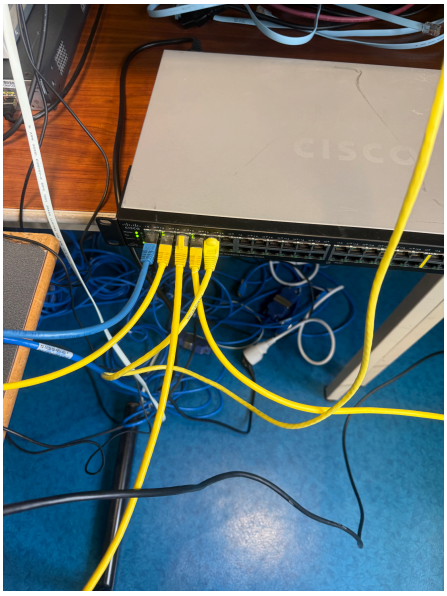
Photos du matériel



Switch SW3



Routeur RT3



Vue rack 1

Vue rack 2

Figure – Câblage

3. Plan d'adressage

Équipement	Adresse IP	Masque	Passerelle
PC0 – VLAN 10 (DIRECTION)	172.18.10.1/24	255.255.255.0	172.18.10.254
PC1 – VLAN 20 (SALARIÉS)	172.18.20.1/24	255.255.255.0	172.18.20.254
PC2 – VLAN 90 (DMZ)	172.18.90.1/24	255.255.255.0	172.18.90.254

Tableau 1 – Plan d'adressage IP par VLAN.

4. Liste des commandes de configuration

4.1 – Configuration du Switch SW3

Activation du mode privilégié et configuration globale :

```
SW3> en
SW3# conf t

! Création des VLANs
SW3(config)# vlan 10
SW3(config-vlan)# name DIRECTION
SW3(config)# vlan 20
SW3(config-vlan)# name SALARIES
SW3(config)# vlan 90
SW3(config-vlan)# name DMZ

! Attribution des ports
SW3(config)# int fa0/1
SW3(config-if)# switchport mode access
SW3(config-if)# switchport access vlan 10

SW3(config)# int fa0/2
SW3(config-if)# switchport mode access
SW3(config-if)# switchport access vlan 20

SW3(config)# int fa0/24
SW3(config-if)# switchport mode trunk
SW3(config-if)# switchport trunk allowed vlan 10,20,90
```

4.2 – Configuration du Routeur RT3

Création des sous-interfaces (Router-on-a-Stick) :

```
RT3> en
RT3# conf t

! VLAN 10 - DIRECTION
RT3(config)# int fa0/0.10
RT3(config-subif)# encapsulation dot1Q 10
RT3(config-subif)# ip address 172.18.10.254 255.255.255.0
RT3(config-subif)# no shutdown

! VLAN 20 - SALARIES
RT3(config)# int fa0/0.20
RT3(config-subif)# encapsulation dot1Q 20
RT3(config-subif)# ip address 172.18.20.254 255.255.255.0
RT3(config-subif)# no shutdown

! VLAN 90 - DMZ
RT3(config)# int fa0/0.90
```

```
RT3(config-subif)# encapsulation dot1Q 90
RT3(config-subif)# ip address 172.18.90.254 255.255.255.0
RT3(config-subif)# no shutdown
```

4.3 – Application des ACL

Définition et application des listes de contrôle d'accès :

```
! ACL 1 – VLAN 10 : autoriser proxy DMZ uniquement
access-list 1 permit host 172.18.90.10
access-list 1 deny   172.18.0.0 0.0.0.0
interface fa0/0.10
  ip access-group 1 out

! ACL 2 – VLAN 20 : bloquer accès au VLAN 10
access-list 2 deny   172.18.10.0 0.0.0.255
access-list 2 permit any
interface fa0/0.20
  ip access-group 2 out

! ACL 3 – Bloquer accès Internet (10.0.5.0/24)
access-list 3 deny   10.0.5.0 0.0.0.255
access-list 3 permit any
interface fa0/0.10
  ip access-group 3 out
interface F0/0.20
  ip access-group 3 out

! ACL 4 – DMZ : pas d'accès Internet
access-list 4 deny   10.0.5.0 0.0.0.255
interface fa0/0.90
  ip access-group 4 out
```

5. Plan de test

5.1 – Avant application des ACL

VLAN	PC0 (VLAN10)	PC1 (VLAN20)	PC2 (VLAN90)	Internet
10 – PC0	**OK**	**OK**	**OK**	**OK**
20 – PC1	**OK**	**OK**	**OK**	**OK**
90 – PC2	**OK**	**OK**	**OK**	**OK**

Tableau 2 – Connectivité complète avant ACL.

5.2 – Après application des ACL

VLAN	PC0 (VLAN10)	PC1 (VLAN20)	PC2 (VLAN90)	Internet
10 – PC0	OK	NON	OK	NON
20 – PC1	NON	OK	OUI	NON
90 – PC2	OUI	OUI	OK	NON (sauf proxy 172.18.90.10)

Tableau 3 – État attendu après configuration des ACL.

5.3 – Tableau récapitulatif des résultats attendus

Source	VLAN 10 – PC0	VLAN 20 – PC1	VLAN 90 – PC2	Internet	Proxy 172.18.90.10
PC0 – VLAN 10	OK	NON	OK	NON	OK
PC1 – VLAN 20	NON	OK	OK	NON	OK
PC2 – VLAN 90	OK	OK	OK	NON	OK

Tableau 4 – Matrice source/destination des accès.

6. Tests réalisés dans Packet Tracer

Objectifs des tests :

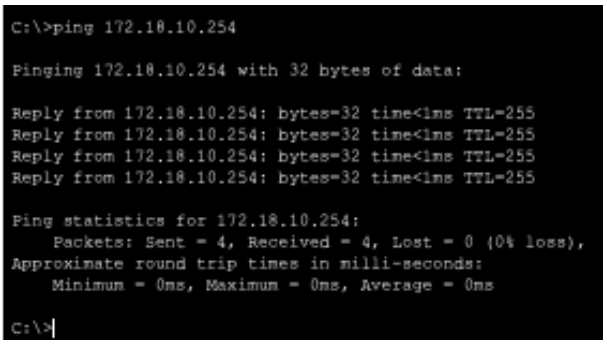
- VLAN 10 et VLAN 20 sont isolés l'un de l'autre ❌
- VLAN 10 et VLAN 20 peuvent accéder à la DMZ ✅
- La DMZ peut accéder aux VLAN internes ✅
- L'accès Internet est bloqué pour tous ❌
- Seul le proxy (172.18.90.10) est accessible depuis la DMZ ✅

VLAN 10 — PC0 (172.18.10.1)

Test 1 — Connectivité locale du VLAN 10

Depuis PC0, ping vers la passerelle 172.18.10.254.

Résultat attendu : ✅ OK – connectivité VLAN 10 confirmée

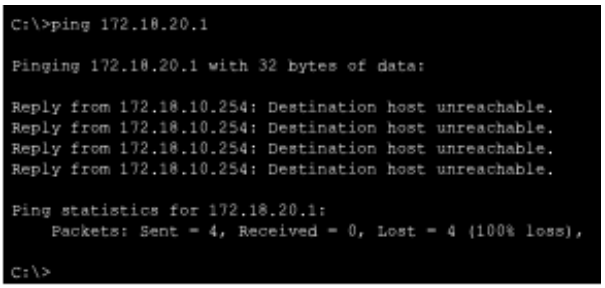


Capture 1 – Ping PC0 → passerelle VLAN 10

Test 2 — Isolation entre VLAN 10 et VLAN 20

Depuis PC0 (172.18.10.1), ping vers PC1 (172.18.20.1).

Résultat attendu : ❌ Échec – filtrage ACL inter-VLAN validé

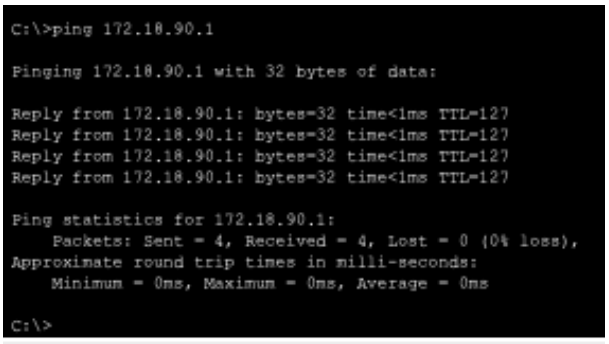


Capture 2 – Ping PC0 → PC1 bloqué

Test 3 — Accès du VLAN 10 à la DMZ

Depuis PC0 (172.18.10.1), ping vers PC2 (172.18.90.1).

Résultat attendu : ✅ OK – accès à la DMZ autorisé

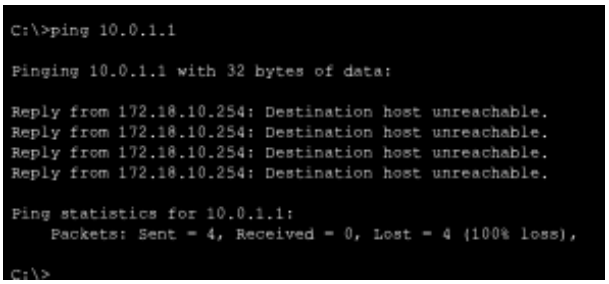


Capture 3 – Ping PC0 → DMZ

Test 4 — Accès Internet depuis le VLAN 10

Depuis PC0 (172.18.10.1), ping vers 10.0.1.1 (Internet simulé).

Résultat attendu : ❌ Échec – accès Internet bloqué par ACL



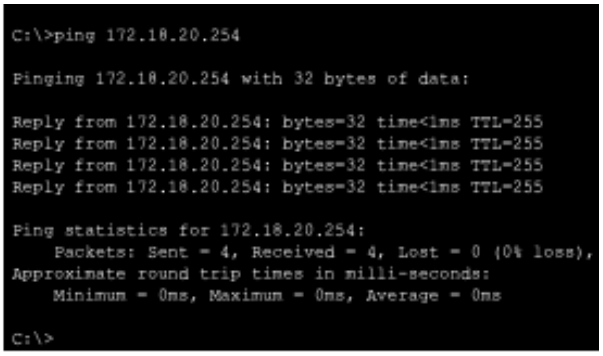
Capture 4 – Ping PC0 → Internet bloqué

VLAN 20 — PC1 (172.18.20.1)

Test 5 — Connectivité locale du VLAN 20

Depuis PC1, ping vers la passerelle 172.18.20.254.

Résultat attendu : ✅ OK – connectivité VLAN 20 confirmée

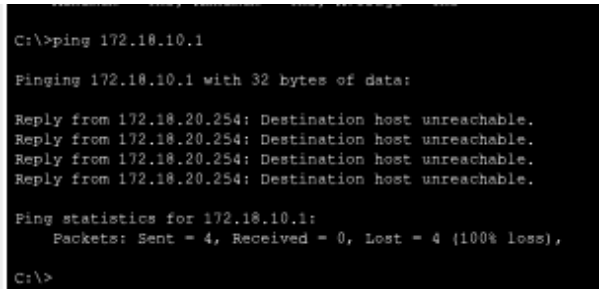


Capture 5 – Ping PC1 → passerelle VLAN 20

Test 6 — Isolation entre VLAN 20 et VLAN 10

Depuis PC1 (172.18.20.1), ping vers PC0 (172.18.10.1).

Résultat attendu : ❌ Échec – politique de sécurité respectée

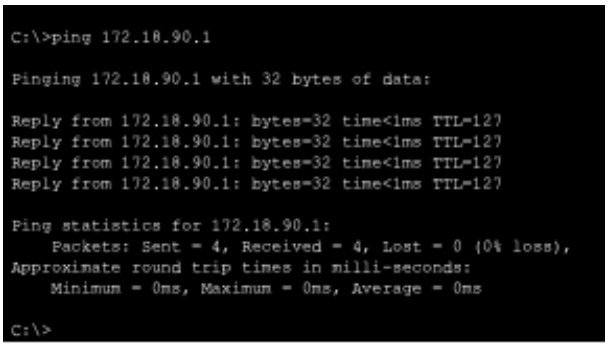


Capture 6 – Ping PC1 → PC0 bloqué

Test 7 — Accès du VLAN 20 à la DMZ

Depuis PC1 (172.18.20.1), ping vers PC2 (172.18.90.1).

Résultat attendu : ✅ OK – accès à la DMZ autorisé

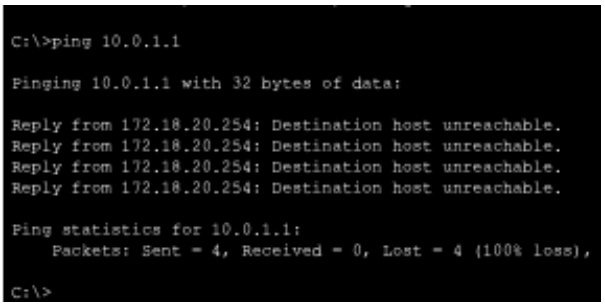


Capture 7 – Ping PC1 → DMZ

Test 8 — Accès Internet depuis le VLAN 20

Depuis PC1 (172.18.20.1), ping vers 10.0.1.1.

Résultat attendu : ❌ Échec – accès Internet interdit



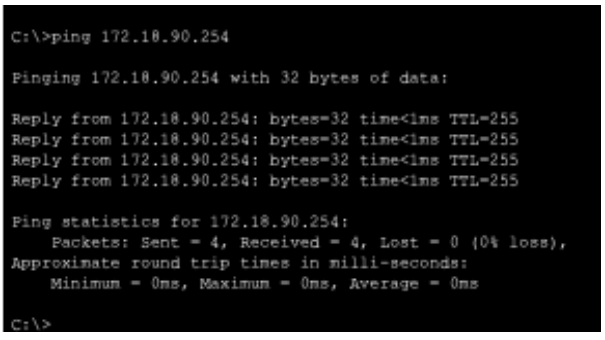
Capture 8 – Ping PC1 → Internet bloqué

VLAN 90 — PC2 / DMZ (172.18.90.1)

Test 9 — Connectivité locale de la DMZ

Depuis PC2, ping vers la passerelle 172.18.90.254.

Résultat attendu : ✅ OK – DMZ correctement configurée

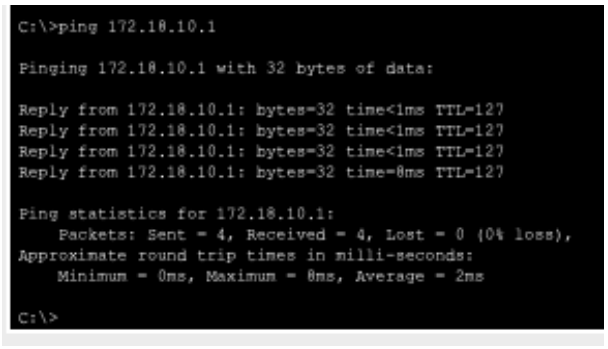


Capture 9 – Ping PC2 → passerelle DMZ

Test 10 — Accès de la DMZ vers le VLAN 10

Depuis PC2 (172.18.90.1), ping vers PC0 (172.18.10.1).

Résultat attendu : ✅ OK – communication DMZ → VLAN 10 autorisée

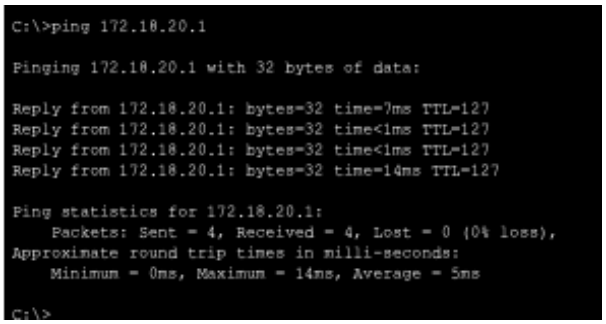


Capture 10 – Ping PC2 → PC0

Test 11 — Accès de la DMZ vers le VLAN 20

Depuis PC2 (172.18.90.1), ping vers PC1 (172.18.20.1).

Résultat attendu : ✅ OK – communication DMZ → VLAN 20 autorisée

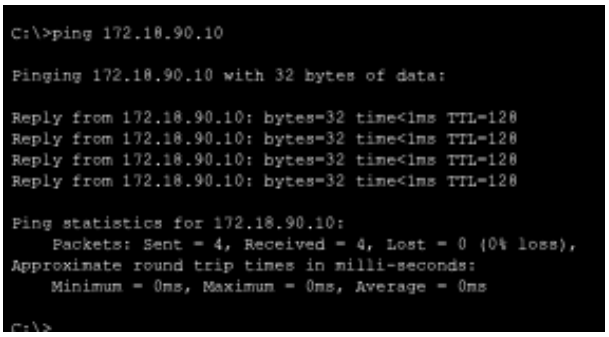


Capture 11 – Ping PC2 → PC1

Test 12 — Accès de la DMZ au proxy

Depuis PC2 (172.18.90.1), ping vers le proxy 172.18.90.10.

Résultat attendu : ✅ OK – accès proxy autorisé

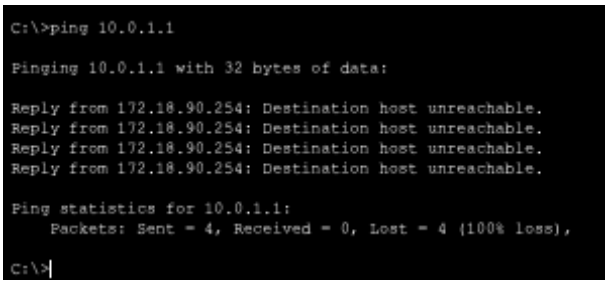


Capture 12 – Ping PC2 → proxy

Test 13 — Accès Internet depuis la DMZ

Depuis PC2 (172.18.90.1), ping vers 10.0.1.1.

Résultat attendu : ❌ Échec – pas d'accès Internet direct depuis la DMZ



Capture 13 – Ping PC2 → Internet bloqué

7. Conclusion des tests

Les essais réalisés dans Cisco Packet Tracer confirment que la configuration des VLANs et des ACL répond aux objectifs fixés :

- Le VLAN 10 et le VLAN 20 sont bien isolés l'un de l'autre ;
- Les deux VLANs utilisateurs peuvent accéder à la DMZ ;
- La DMZ peut communiquer avec les VLANs internes ;
- L'accès Internet direct est bloqué pour l'ensemble des VLANs ;
- Seul le proxy de la DMZ (172.18.90.10) reste joignable depuis VLAN 90.

8. Problèmes rencontrés

Lors de la mise en place de la configuration réseau, le switch et le routeur disposaient déjà d'une configuration existante, incluant notamment une protection par mot de passe.

Afin de repartir sur une base propre, nous avons procédé à une réinitialisation complète des équipements. Cette opération a permis d'effacer les paramètres précédents (adresses IP, VLANs, routage, mots de passe, etc.) et de reprendre entièrement la configuration selon nos besoins.

Bien que cette étape ait nécessité un temps supplémentaire, elle a garanti une meilleure maîtrise de l'environnement réseau et a permis d'éviter d'éventuels conflits liés à l'ancienne configuration.