Lyon-HQ

Infrastructure Reseau d'Entreprise

Architecture Core / Access / DMZ — Securite Multi-couches

VLAN ACL NAT DHCP DNS SYSLOG

Projet	Infrastructure Cisco Packet Tracer
Site	Lyon Headquarters (LYN-HQ)
Version	1.0 — Production Ready
Date	May 4, 2026
Auteur	Ghodbane Rachid – CISCO Network Engineer
Statut	**CONFIDENTIEL**

Table des matieres

CHAPITRE 1

Presentation du Projet

1.1 Contexte et Objectifs

Ce rapport documente la conception, l'implementation et la validation d'une infrastructure reseau d'entreprise complete pour le siege social de Lyon (LYN-HQ). Le projet est realise dans l'environnement de simulation **Cisco Packet Tracer**, en respectant les meilleures pratiques industrielles CCNA/CCNP.

Objectif Principal

Deployer une infrastructure reseau professionnelle multi-couches integrant la segmentation VLAN, le routage inter-VLAN L3, la securite par ACL etendues, le NAT, les services reseau (DHCP, DNS, HTTP) et la supervision centralisee via SOC/Syslog.

1.1.1 Perimetre fonctionnel

- **Architecture :** Core Layer (L3) / Access Layer (L2) / DMZ isolee
- **Segmentation :** 7 VLANs metiers — DSI, RH, Finance, Users, Servers, DMZ, SOC
- **Routage :** Inter-VLAN via Switch L3 Cisco 3560 (`ip routing`)
- **Securite :** ACL etendues par zone, isolation stricte de la DMZ
- **Services :** DHCP multi-pool avec relay, DNS interne, HTTP interne et public
- **Connectivite WAN :** NAT Overload (PAT) vers Internet simule
- **Supervision :** Centralisation Syslog vers serveur SOC dedie

1.1.2 Schema general de l'infrastructure

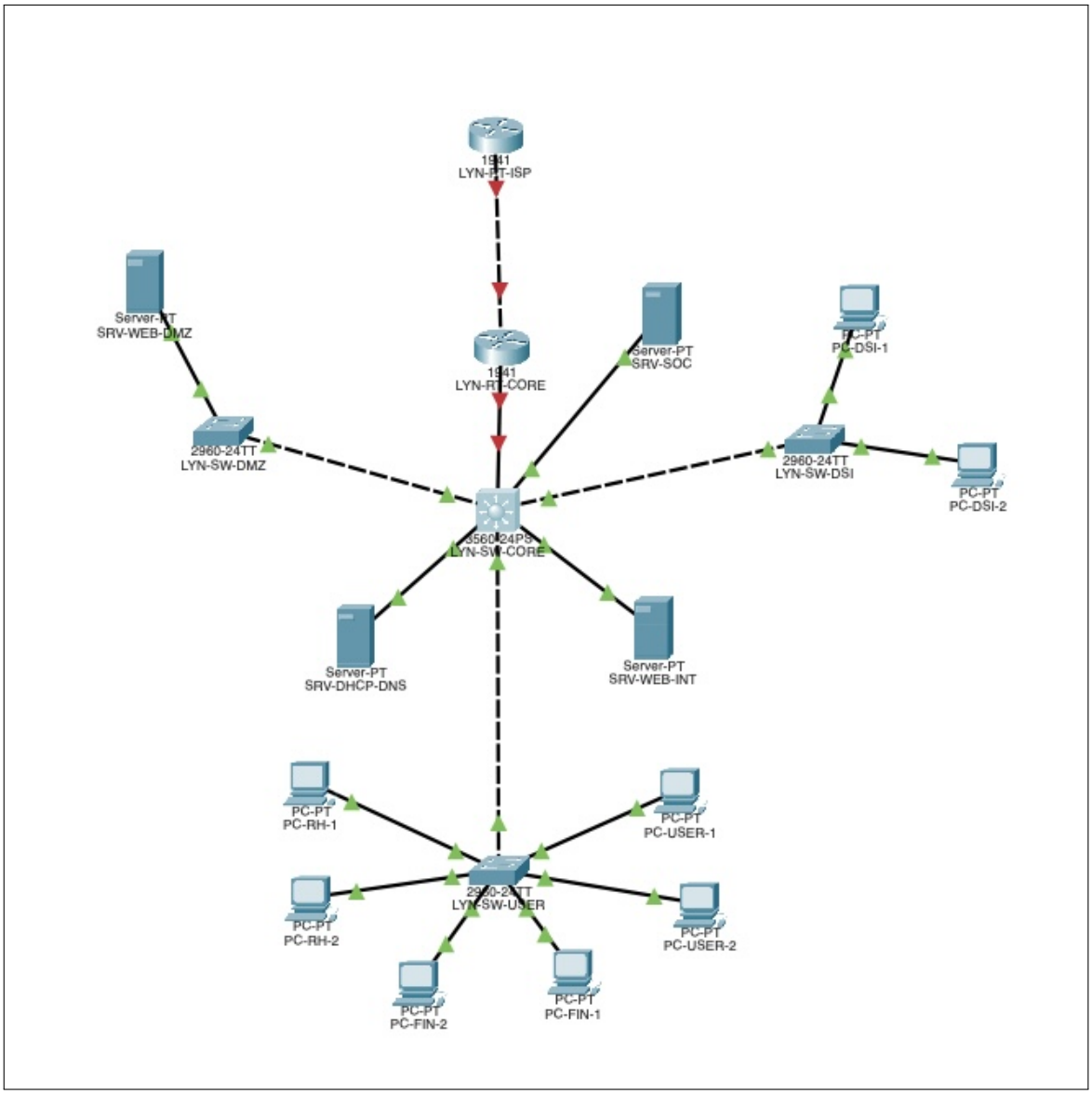

Figure 1.1. Vue d'ensemble de l'infrastructure reseau Lyon HQ

1.2 Inventaire des Equipements

Table 1.1. Inventaire complet des equipements

#	Hostname	Modele	Qte	Role
1	LYN-RT-CORE	Cisco 1941	1	Gateway principale, NAT, ACL
2	LYN-RT-ISP	Cisco 1941	1	Routeur ISP simule
3	LYN-SW-CORE	Cisco 3560-24PS	1	Switch Core L3 — routage inter-VLAN
4	LYN-SW-DSI	Cisco 2960-24TT	1	Switch Access — VLAN DSI
5	LYN-SW-USERS	Cisco 2960-24TT	1	Switch Access — VLAN RH/Finance/Users
6	LYN-SW-DMZ	Cisco 2960-24TT	1	Switch DMZ isolee
7	SRV-DHCP-DNS	Server-PT	1	Services DHCP + DNS
8	SRV-WEB-INT	Server-PT	1	Serveur Web intranet
9	SRV-WEB-DMZ	Server-PT	1	Serveur Web public (DMZ)
10	SRV-SOC	Server-PT	1	Collecteur Syslog / SIEM
11	PC-DSI-01/02	PC-PT	2	Postes equipe DSI
12	PC-RH-01/02	PC-PT	2	Postes equipe RH
13	PC-FIN-01/02	PC-PT	2	Postes equipe Finance
14	PC-USR-01/02	PC-PT	2	Postes utilisateurs generiques

CHAPITRE 2

Plan d'Adressage Reseau

2.1 Architecture d'Adressage IPv4

Le plan d'adressage suit la plage `192.168.0.0/16` pour le reseau interne, avec une segmentation en sous-reseaux /**24** par VLAN (254 hotes utilisables par segment). Le lien WAN utilise un /**30** pour le lien point-a-point routeur–ISP.

Table 2.1. Plan d'adressage VLAN complet

Nom	VLAN	ID	Reseau	Plage DHCP	Gateway
DSI	VLAN 10	10	`192.168.10.0/24`	.100 – .150	`192.168.10.1`
RH	VLAN 20	20	`192.168.20.0/24`	.100 – .150	`192.168.20.1`
Finance	VLAN 30	30	`192.168.30.0/24`	.100 – .150	`192.168.30.1`
Users	VLAN 40	40	`192.168.40.0/24`	.100 – .150	`192.168.40.1`
Servers	VLAN 50	50	`192.168.50.0/24`	Statique	`192.168.50.1`
DMZ	VLAN 60	60	`192.168.60.0/24`	Statique	`192.168.60.1`
SOC	VLAN 70	70	`192.168.70.0/24`	Statique	`192.168.70.1`
WAN	—	–	`10.0.0.0/30`	—	—

2.2 Adresses Statiques des Serveurs

Table 2.2. Adressage statique des serveurs et interfaces cles

Equipement	Adresse IP	Masque	Gateway	VLAN
SRV-DHCP-DNS	192.168.50.10	/24	192.168.50.1	VLAN 50
SRV-WEB-INT	192.168.50.20	/24	192.168.50.1	VLAN 50
SRV-WEB-DMZ	192.168.60.10	/24	192.168.60.1	VLAN 60
SRV-SOC	192.168.70.10	/24	192.168.70.1	VLAN 70
LYN-SW-CORE (uplink)	192.168.1.2	/24	192.168.1.1	L3 route
LYN-RT-CORE (LAN)	192.168.1.1	/24	—	L3 route
LYN-RT-CORE (WAN)	10.0.0.1	/30	10.0.0.2	WAN
LYN-RT-ISP	10.0.0.2	/30	—	WAN

CHAPITRE 3

Architecture et Topologie

3.1 Modele Hierachique Cisco

L'infrastructure repose sur le modele a trois couches de Cisco, garantissant une separation claire des responsabilites reseau, une meilleure scalabilite et un depannage facilite.

- **Core Layer :** LYN-RT-CORE assure la connectivite WAN, le NAT/PAT et les ACL de perimetre. LYN-SW-CORE (3560) centralise le routage inter-VLAN.
- **Distribution Layer :** Role assure par le 3560 — routage L3, DHCP relay (`ip helper-address`), application des ACL par zone.
- **Access Layer :** Switches 2960 (LYN-SW-DSI, LYN-SW-USERS, LYN-SW-DMZ) — connexion des terminaux, affectation VLAN.

3.2 Plan de Cablage

Table 3.1. Plan de cablage port a port

Equipement A	Port A	Equipement B	Port B	Cable
LYN-RT-ISP	Se0/0/0	LYN-RT-CORE	Se0/0/0	Serial DCE
LYN-RT-CORE	Gi0/0	LYN-SW-CORE	Gi0/1	Straight
LYN-SW-CORE	Fa0/1	LYN-SW-DSI	Gi0/1	Crossover
LYN-SW-CORE	Fa0/2	LYN-SW-USERS	Gi0/1	Crossover
LYN-SW-CORE	Fa0/3	LYN-SW-DMZ	Gi0/1	Crossover
LYN-SW-CORE	Fa0/10	SRV-DHCP-DNS	Fa0	Straight
LYN-SW-CORE	Fa0/11	SRV-WEB-INT	Fa0	Straight
LYN-SW-CORE	Fa0/12	SRV-SOC	Fa0	Straight
LYN-SW-DMZ	Fa0/1	SRV-WEB-DMZ	Fa0	Straight
LYN-SW-DSI	Fa0/1-2	PC-DSI-01/02	Fa0	Straight
LYN-SW-USERS	Fa0/1-6	PCs RH/FIN/USR	Fa0	Straight

CHAPITRE 4

Configuration des Equipements

4.1 Switch Core — LYN-SW-CORE (3560)

Le Cisco 3560 est le pivot de l'infrastructure. La commande `ip routing` active le moteur L3. Chaque VLAN dispose d'une **SVI** (Switched Virtual Interface) faisant office de passerelle. La commande `ip helper-address` sur chaque SVI redirige les requetes DHCP broadcast vers le serveur centralise.

```
! -- Initialisation ------------------------------------------
enable
configure terminal
hostname LYN-SW-CORE
no ip domain-lookup
enable secret Cisco123!

! -- Activation du routage L3 (OBLIGATOIRE sur 3560) ---------
ip routing

! -- Creation des VLANs --------------------------------------
vlan 10
 name DSI
vlan 20
 name RH
vlan 30
 name FINANCE
vlan 40
 name USERS
vlan 50
 name SERVERS
vlan 60
 name DMZ
vlan 70
 name SOC
exit
```

Listing 4.1. Configuration complete LYN-SW-CORE (3560)

```

! -- Interfaces SVI (gateways + DHCP relay) ------------------
interface vlan 10
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.50.10
 description Gateway-DSI
 no shutdown
!
interface vlan 20
 ip address 192.168.20.1 255.255.255.0
 ip helper-address 192.168.50.10
 description Gateway-RH
 no shutdown
!
interface vlan 30
 ip address 192.168.30.1 255.255.255.0
 ip helper-address 192.168.50.10
 description Gateway-Finance
 no shutdown
!
interface vlan 40
 ip address 192.168.40.1 255.255.255.0
 ip helper-address 192.168.50.10
 description Gateway-Users
 no shutdown
!
interface vlan 50
 ip address 192.168.50.1 255.255.255.0
 description Gateway-Servers
 no shutdown
!
interface vlan 60
 ip address 192.168.60.1 255.255.255.0
 description Gateway-DMZ
 no shutdown
!
interface vlan 70
 ip address 192.168.70.1 255.255.255.0
 description Gateway-SOC
 no shutdown
!
```

Listing 4.2. Configuration complete LYN-SW-CORE (3560) - Suite

```
! -- Uplink vers LYN-RT-CORE (port route L3) -----------------
interface gigabitEthernet 0/1
 no switchport
 ip address 192.168.1.2 255.255.255.0
 description UPLINK-TO-LYN-RT-CORE
 no shutdown
!
! -- Trunks vers switches access -----------------------------
interface fastEthernet 0/1
 description TRUNK-TO-LYN-SW-DSI
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10
 no shutdown
!
interface fastEthernet 0/2
 description TRUNK-TO-LYN-SW-USERS
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 20,30,40
 no shutdown
!
interface fastEthernet 0/3
 description TRUNK-TO-LYN-SW-DMZ
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 60
 no shutdown
!
```

Listing 4.3. Configuration complete LYN-SW-CORE (3560) - Suite

```
! -- Ports serveurs (access) ----------------------------------
interface fastEthernet 0/10
 description SRV-DHCP-DNS
 switchport mode access
 switchport access vlan 50
 no shutdown
!
interface fastEthernet 0/11
 description SRV-WEB-INT
 switchport mode access
 switchport access vlan 50
 no shutdown
!
interface fastEthernet 0/12
 description SRV-SOC
 switchport mode access
 switchport access vlan 70
 no shutdown
!
! -- Route par defaut et logging ------------------------------
ip route 0.0.0.0 0.0.0.0 192.168.1.1
logging host 192.168.70.10
logging trap informational
service timestamps log datetime msec
end
write memory
```

Listing 4.4. Configuration complete LYN-SW-CORE (3560) - Suite

4.2 Routeur Core — LYN-RT-CORE (1941)

Le routeur 1941 assure trois fonctions critiques : la **terminaison WAN** (lien Serie vers ISP), le **NAT Overload** (PAT) pour la sortie Internet, et les **routes statiques** de retour vers les VLANs internes via le SW-CORE.

```
enable
configure terminal
hostname LYN-RT-CORE
no ip domain-lookup
enable secret Cisco123!

! -- Interface WAN ------------------------------------------
interface serial 0/0/0
 description WAN-TO-LYN-RT-ISP
 ip address 10.0.0.1 255.255.255.252
 ip nat outside
 no shutdown
!
! -- Interface LAN ------------------------------------------
interface gigabitEthernet 0/0
 description LAN-TO-LYN-SW-CORE
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 no shutdown
!
! -- Routes statiques retour vers VLANs ---------------------
ip route 192.168.10.0 255.255.255.0 192.168.1.2
ip route 192.168.20.0 255.255.255.0 192.168.1.2
ip route 192.168.30.0 255.255.255.0 192.168.1.2
ip route 192.168.40.0 255.255.255.0 192.168.1.2
ip route 192.168.50.0 255.255.255.0 192.168.1.2
ip route 192.168.60.0 255.255.255.0 192.168.1.2
ip route 192.168.70.0 255.255.255.0 192.168.1.2
! -- Route par defaut vers ISP ------------------------------
ip route 0.0.0.0 0.0.0.0 10.0.0.2
! -- ACL NAT ------------------------------------------------
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
access-list 1 permit 192.168.50.0 0.0.0.255
access-list 1 permit 192.168.60.0 0.0.0.255
access-list 1 permit 192.168.70.0 0.0.0.255
```

Listing 4.5. Configuration LYN-RT-CORE — Gateway + NAT + Routage

```
! -- NAT Overload / PAT ----------------------------------------
ip nat inside source list 1 interface serial 0/0/0 overload
! -- Logging ---------------------------------------------------
logging host 192.168.70.10
logging trap informational
service timestamps log datetime msec
end
write memory
```

Listing 4.6. Configuration LYN-RT-CORE — Gateway + NAT + Routage - Suite

4.3 Switches Access (2960)

```
enable
configure terminal
hostname LYN-SW-DSI
no ip domain-lookup
enable secret Cisco123!
vlan 10
 name DSI
exit
interface gigabitEthernet 0/1
 description TRUNK-TO-LYN-SW-CORE
 switchport mode trunk
 switchport trunk allowed vlan 10
 no shutdown
!
interface fastEthernet 0/1
 description PC-DSI-01
 switchport mode access
 switchport access vlan 10
 no shutdown
!
interface fastEthernet 0/2
 description PC-DSI-02
 switchport mode access
 switchport access vlan 10
 no shutdown
!
end
write memory
```

Listing 4.7. LYN-SW-DSI — VLAN 10

```
enable
configure terminal
hostname LYN-SW-USERS
no ip domain-lookup
enable secret Cisco123!
vlan 20
 name RH
vlan 30
 name FINANCE
vlan 40
 name USERS
exit
interface gigabitEthernet 0/1
 description TRUNK-TO-LYN-SW-CORE
 switchport mode trunk
 switchport trunk allowed vlan 20,30,40
 no shutdown
!
interface fastEthernet 0/1
 description PC-RH-01
 switchport mode access
 switchport access vlan 20
 no shutdown
!
interface fastEthernet 0/2
 description PC-RH-02
 switchport mode access
 switchport access vlan 20
 no shutdown
!
interface fastEthernet 0/3
 description PC-FIN-01
 switchport mode access
 switchport access vlan 30
 no shutdown
!
interface fastEthernet 0/4
 description PC-FIN-02
 switchport mode access
 switchport access vlan 30
 no shutdown
!
```

Listing 4.8. LYN-SW-USERS — VLAN 20/30/40

```
interface fastEthernet 0/5
 description PC-USR-01
 switchport mode access
 switchport access vlan 40
 no shutdown
!
interface fastEthernet 0/6
 description PC-USR-02
 switchport mode access
 switchport access vlan 40
 no shutdown
!
end
write memory
```

Listing 4.9. LYN-SW-USERS — VLAN 20/30/40 - Suite

CHAPITRE 5

Politique de Securite et ACL

5.1 Logique de Securite par Zone

La politique applique le principe du **moindre privilege** : chaque zone n'accede qu'a ce qui lui est strictement necessaire. Les ACL sont appliquees en direction `in` (au plus pres de la source) pour bloquer le trafic non autorise avant qu'il ne consomme des ressources reseau.

5.2 Matrice de Controle d'Acces

Table 5.1. Matrice inter-zones — Droits d'acces

Source	DSI	RH	Finance	Users	Servers	DMZ	WAN
DSI	✓	✓	✓	✓	✓	✓	✓
RH	✓	✓	✗	✗	✓	✗	✓
Finance	✗	✗	✓	✗	✓	✗	✓
Users	✗	✗	✗	✓	▲	✗	✓
DMZ	✗	✗	✗	✗	✗	✓	✓
SOC	✗	✗	✗	✗	✗	✗	✗

✓ Autorise ✗ Bloque ▲ Partiel (HTTP/80 + DNS/53 uniquement)

5.3 ACL Etendues

```
ip access-list extended ACL-DMZ-TO-LAN
 ! Reponses TCP etablies (retours legitimes)
 permit tcp 192.168.60.0 0.0.0.255 any established
 ! Bloquer DMZ vers tout le reseau interne
 deny ip 192.168.60.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.60.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny ip 192.168.60.0 0.0.0.255 192.168.30.0 0.0.0.255
 deny ip 192.168.60.0 0.0.0.255 192.168.40.0 0.0.0.255
 deny ip 192.168.60.0 0.0.0.255 192.168.50.0 0.0.0.255
 deny ip 192.168.60.0 0.0.0.255 192.168.70.0 0.0.0.255
 ! Autoriser sortie vers Internet
 permit ip any any
!
interface vlan 60
 ip access-group ACL-DMZ-TO-LAN in
```

Listing 5.1. ACL-DMZ-TO-LAN — Isolation stricte de la DMZ

```
ip access-list extended ACL-FINANCE
 ! Autoriser Finance vers serveurs internes (VLAN 50)
 permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
 ! Bloquer Finance vers DSI
 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
 ! Autoriser Internet
 permit ip 192.168.30.0 0.0.0.255 any
 permit ip any any
!
interface vlan 30
 ip access-group ACL-FINANCE in
```

Listing 5.2. ACL-FINANCE — Restrictions zone Finance

```
ip access-list extended ACL-USERS
 ! DNS vers serveur interne (UDP/53)
 permit udp 192.168.40.0 0.0.0.255 host 192.168.50.10 eq 53
 ! Web intranet (HTTP/80)
 permit tcp 192.168.40.0 0.0.0.255 host 192.168.50.20 eq 80
 ! Navigation Internet
 permit tcp 192.168.40.0 0.0.0.255 any eq 80
 permit tcp 192.168.40.0 0.0.0.255 any eq 443
 ! Bloquer zones sensibles
 deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
 deny ip 192.168.40.0 0.0.0.255 192.168.70.0 0.0.0.255
 permit ip any any
!
interface vlan 40
 ip access-group ACL-USERS in
```

Listing 5.3. ACL-USERS — Restrictions postes utilisateurs

Regle implicite DENY ALL — Point critique

Toute ACL Cisco se termine par un `deny ip any any` **implicite et invisible**. Tout trafic non couvert par une regle `permit` est silencieusement bloque. Toujours verifier qu'un `permit ip any any` final est present si du trafic de transit doit passer.

CHAPITRE 6

Services Reseau

6.1 Service DHCP Multi-pool avec Relay

Table 6.1. Configuration des pools DHCP

Nom du pool	VLAN	Plage IPs	Gateway	DNS
VLAN10-DSI	10	.100 – .150	192.168.10.1	192.168.50.10
VLAN20-RH	20	.100 – .150	192.168.20.1	192.168.50.10
VLAN30-FINANCE	30	.100 – .150	192.168.30.1	192.168.50.10
VLAN40-USERS	40	.100 – .150	192.168.40.1	192.168.50.10

DHCP Relay — Point critique

Le serveur DHCP (VLAN 50) ne repond pas directement aux broadcasts des autres VLANs. La commande `ip helper-address 192.168.50.10` sur chaque SVI du LYN-SW-CORE est **indispensable** pour relayer les requetes en unicast.

6.2 Service DNS Interne

Table 6.2. Enregistrements DNS — Zone `lyon-hq.local`

FQDN	Type	Adresse IP	Service
www.lyon-hq.local	A	192.168.50.20	Web intranet
dmz.lyon-hq.local	A	192.168.60.10	Web public DMZ
soc.lyon-hq.local	A	192.168.70.10	SIEM / Syslog
dhcp.lyon-hq.local	A	192.168.50.10	DHCP + DNS

6.3 NAT Overload (PAT)

Le mécanisme de **NAT Overload (PAT)** a été mis en œuvre sur le routeur *LYN-RT-CORE* afin de permettre à l'ensemble des hôtes internes d'accéder au réseau Internet simulé.

Dans cette architecture, toutes les machines appartenant aux réseaux privés (VLAN 10 à VLAN 70) utilisent des adresses IP de type `192.168.X.0/24`, qui ne sont pas routables sur Internet. Le NAT permet donc de traduire ces adresses privées en une adresse IP publique unique, associée à l'interface WAN du routeur.

6.3.1 Configuration des interfaces NAT

Les interfaces du routeur sont configurées de la manière suivante :

- L'interface `GigabitEthernet0/0` est définie comme **inside**, représentant le réseau local (LAN).
- L'interface `Serial0/0/0` est définie comme **outside**, représentant le réseau étendu (WAN).

6.3.2 Activation du NAT Overload

Le NAT Overload est configuré à l'aide de la commande suivante :

```
ip nat inside source list 1 interface serial 0/0/0 overload
```

Ce mécanisme permet à plusieurs hôtes internes de partager une seule adresse IP publique (10.0.0.1). La distinction des sessions est assurée par les numéros de ports TCP/UDP source, ce qui correspond au fonctionnement des box Internet modernes.

6.3.3 Principe de fonctionnement

Lorsqu'un poste client (par exemple PC-RH ou PC-USERS) initie une connexion vers Internet, le processus suivant est appliqué :

1. Le paquet est envoyé vers la passerelle par défaut du VLAN.
2. Le routeur *LYN-RT-CORE* intercepte le trafic.
3. L'adresse IP source privée est traduite en adresse publique (10.0.0.1).
4. Un port source unique est attribué à la session.
5. Le paquet est transmis vers le routeur ISP.
6. Les réponses suivent le chemin inverse grâce à la table NAT.

6.3.4 Table de translation NAT

Le routeur maintient une table de translation dynamique consultable via :

```
show ip nat translations
```

Cette table permet de suivre les correspondances entre adresses privées et publiques en temps réel.

6.3.5 Conclusion

Le NAT Overload joue un rôle essentiel dans l'infrastructure :

- accès Internet pour l'ensemble des VLANs
- mutualisation de l'adresse IP publique
- protection de l'architecture interne du réseau

CHAPITRE 7

Supervision et SOC

7.1 Architecture de Collecte Syslog

7.1.1 Principe de fonctionnement

L'architecture de supervision repose sur un mécanisme de centralisation des journaux d'événements via le protocole **Syslog**. L'ensemble des équipements réseau de l'infrastructure transmettent leurs logs vers un serveur central de supervision : *SRV-SOC* (192.168.70.10). Les équipements concernés sont :

- LYN-RT-CORE (routeur principal)
- LYN-SW-CORE (switch Layer 3)
- LYN-SW-DSI
- LYN-SW-USERS
- LYN-SW-DMZ

7.2 Configuration de la collecte

La configuration Syslog appliquée sur les équipements est la suivante :

```
! Appliquer sur : LYN-RT-CORE, LYN-SW-CORE,
!                 LYN-SW-DSI, LYN-SW-USERS, LYN-SW-DMZ
logging host 192.168.70.10
logging trap informational
logging on
service timestamps log datetime msec
```

Listing 7.1. Syslog — a appliquer sur tous les equipements reseau

Cette configuration permet :

- l'envoi des logs vers le serveur SOC
- la définition du niveau de gravité des événements (niveau informational)
- l'activation du service de journalisation
- l'ajout d'un horodatage précis pour chaque événement

7.2.1 Flux de collecte des logs

Le flux de journalisation suit le processus suivant :

1. Un événement réseau est généré sur un équipement (ex : changement d'état d'interface)
2. L'événement est converti en message Syslog
3. Le message est envoyé vers le serveur *SRV-SOC*
4. Le serveur stocke et affiche les logs en temps réel

7.2.2 Rôle de l'architecture Syslog

Cette architecture permet :

- une centralisation des événements réseau
- une supervision en temps réel de l'infrastructure
- une amélioration de la détection d'incidents

7.3 Niveaux de Severite Syslog

Table 7.1. Niveaux Syslog (RFC 3164)

Niveau	Nom	Description	Contexte
0	Emergencies	Systeme inutilisable	Critique
1	Alerts	Action immediate requise	Critique
2	Critical	Conditions critiques	Production
3	Errors	Erreurs systeme	Production
4	Warnings	Avertissements	Production
5	Notifications	Conditions normales significatives	Recommande
6	Informational	Messages informatifs	**Ce projet**
7	Debugging	Debogage tres verbeux	Lab only

CHAPITRE 8

Plan de Tests et Validation

8.1 Matrice de Tests

Table 8.1. Plan de tests complet — connectivite et securite

#	Source	Destination	Resultat	Commande
Connectivite de base				
T01	PC-DSI-01	PC-DSI-02	✓ OK	`ping 192.168.10.101`
T02	PC-DSI-01	Gateway VLAN10	✓ OK	`ping 192.168.10.1`
T03	PC-DSI-01	PC-RH-01	✓ OK	`ping 192.168.20.100`
T04	PC-DSI-01	SRV-DHCP-DNS	✓ OK	`ping 192.168.50.10`
T05	PC-DSI-01	SRV-WEB-INT	✓ OK	`ping 192.168.50.20`
NAT / Internet				
T06	PC-DSI-01	LYN-RT-ISP	✓ OK	`ping 10.0.0.2`
T07	PC-DSI-01	8.8.8.8	✓ OK	`ping 8.8.8.8`
Securite — ACL (resultats BLOQUES attendus)				
T08	PC-FIN-01	PC-DSI-01	✗ BLOQUE	`ping 192.168.10.100`
T09	PC-FIN-01	SRV-WEB-INT	✓ OK	`ping 192.168.50.20`
T10	PC-USR-01	PC-FIN-01	✗ BLOQUE	`ping 192.168.30.100`
T11	SRV-WEB-DMZ	PC-DSI-01	✗ BLOQUE	`ping 192.168.10.100`
T12	SRV-WEB-DMZ	SRV-WEB-INT	✗ BLOQUE	`ping 192.168.50.20`
Services DNS + HTTP				
T13	PC-DSI-01	www.lyon-hq.local	✓ OK	Web Browser
T14	PC-DSI-01	dmz.lyon-hq.local	✓ OK	Web Browser
DHCP				
T15	PC-RH-01	IP DHCP auto	✓ OK	Config. DHCP auto
T16	PC-FIN-01	IP DHCP auto	✓ OK	Config. DHCP auto

8.2 Commandes de Verification

Sur LYN-SW-CORE

```
show vlan brief show interfaces trunk show ip interface brief show ip
route show ip dhcp binding show ip access-lists show interfaces status
```

Sur LYN-RT-CORE

```
show ip interface brief show ip route show ip nat translations show ip
nat statistics show logging show access-lists show controllers serial
0/0/0
```

8.3 Criteres de Validation

Infrastructure 100% operationnelle

- ✓ Tous les PCs recoivent une IP DHCP dans leur VLAN respectif
- ✓ Routage inter-VLAN fonctionnel depuis les postes DSI
- ✓ ACL bloquent Finance vers DSI et Users vers Finance
- ✓ DMZ totalement isolee du reseau LAN interne
- ✓ NAT permet l'acces Internet depuis tous les VLANs
- ✓ Serveur Web intranet accessible via DNS
- ✓ SOC recoit les logs Syslog de tous les equipements

CHAPITRE 9

Depannage et Resolution

9.1 Guide de Diagnostic Rapide

Table 9.1. Problemes frequents, causes et corrections

Symptome	Cause probable	Diagnostic	Correction
IP 169.254.x.x	DHCP relay absent	`show ip int vlan X`	Ajouter `ip helper-address`
Ping inter-VLAN KO	`ip routing` manquant	`show ip route`	`ip routing` sur 3560
Trunk KO	Encapsulation absente	`show int trunk`	Ajouter `encap dot1q`
NAT inactif	inside/outside inverses	`show ip nat stat`	Revoir `ip nat` sur ifaces
DNS ne resout pas	Service DNS eteint	Verifier Services PT	Activer DNS sur SRV
ACL trop restrictive	Ordre des regles	`show ip access-lists`	Reorganiser les entrees
Serial reste DOWN	`clock rate` absent	`show controllers se0/0/0`	Ajouter `clock rate 64000`
SVI DOWN/DOWN	VLAN non cree	`show vlan brief`	Creer le VLAN d'abord
Logs SOC vides	Service Syslog eteint	`show logging`	Activer sur SRV-SOC

Commandes debug — A utiliser avec precaution

Les commandes `debug` sont tres verboses et peuvent surcharger le CPU. Toujours executer `undebug all` apres usage en production.

Commandes debug principales

```
debug ip routing ! Suivi changements de route debug ip dhcp server
events ! Debug attribution DHCP debug ip nat ! Debug translations NAT
debug ip packet detail ! Inspection paquet par paquet undebug all !
Desactiver TOUS les debugs !
```

CHAPITRE 9

Conclusion

Ce projet demontre la conception et le deploiement d'une infrastructure reseau d'entreprise complete sur Cisco Packet Tracer, couvrant les competences attendues au niveau **CCNA 200-301** et partiellement **CCNP ENCOR 350-401**.

Bilan des competences demontrees

- ✓ **Switching L2/L3 :** VLAN, 802.1Q trunk, SVI, routage inter-VLAN
- ✓ **Routage IP :** routes statiques, route par defaut, modele hierarchique
- ✓ **Services reseau :** DHCP multi-pool, DHCP relay, DNS, HTTP
- ✓ **Securite reseau :** ACL etendues, isolation DMZ, moindre privilege
- ✓ **Acces Internet :** NAT Overload (PAT), lien WAN serie
- ✓ **Supervision :** Syslog centralise vers SOC dedie
- ✓ **Documentation :** Adressage, topologie, tests, nomenclature pro

Les evolutions naturelles de cette infrastructure incluraient : OSPF pour un routage dynamique, HSRP pour la haute disponibilite, un Cisco ASA en coupure de la DMZ, une authentification centralisee TACACS+ et l'adoption d'un stack IPv4/IPv6 dual-stack.

Rapport technique — Infrastructure Reseau Lyon HQ — v1.0
Usage pedagogique — Formation CCNA/CCNP — Cisco Packet Tracer

Document confidentiel — Usage interne uniquement