

# SMARTECH SA

## RAPPORT TECHNIQUE

*Conception et Déploiement d'une Infrastructure Réseau Multi-Sites*

Module	Technologies de l'Internet
Niveau	DUT2TR
Enseignant	Dr K. GUEYE
Présenté par	<b>AI Hassane BA</b>
Année	2025-2026
Durée	3 semaines
Outils	GNS3, Cisco IOS, Wireshark

---

# 1. Introduction et Cahier des Charges

## 1.1 Contexte du Projet

---

Smartech SA est une entreprise panafricaine en pleine expansion qui ouvre un nouveau campus principal à Dakar (Siège), accompagné de deux agences régionales à Saint-Louis et à Ziguinchor. L'objectif de ce projet est de concevoir, déployer et sécuriser une infrastructure réseau multi-sites complète, reflétant une architecture d'entreprise réelle.

Le réseau intègre trois protocoles de routage distincts : OSPF pour le réseau principal, EIGRP pour le réseau partenaire (AS 100), et RIP v2 pour un site legacy. La redistribution entre ces protocoles constitue l'un des défis majeurs du projet. La sécurisation par ACL et l'authentification des protocoles de routage complètent l'architecture.

## 1.2 Objectifs

---

- Concevoir une topologie réseau cohérente et un plan d'adressage IPv4 rigoureux
- Déployer OSPF en multi-zones (Zone 0, 1 et 2) avec gestion DR/BDR
- Configurer EIGRP AS 100 et assurer la redistribution bidirectionnelle OSPF ↔ EIGRP
- Intégrer le site legacy RIP v2 et gérer la redistribution OSPF ↔ RIP
- Sécuriser le réseau avec des ACL ciblées et l'authentification MD5 OSPF
- Analyser les échanges protocolaires avec Wireshark

## 1.3 Contraintes Techniques

---

Le projet impose plusieurs contraintes techniques cruciales. La continuité de la zone backbone OSPF 0 doit être garantie sur le segment 10.0.0.0/24. R1 doit impérativement être élu DR et R4 BDR. La redistribution mutuelle entre domaines nécessite une protection anti-boucles rigoureuse. Enfin, SRV1 ne doit être accessible depuis les agences qu'en HTTP, HTTPS et DNS.

# 2. Topologie et Plan d'Adressage

## 2.1 Architecture Générale

---

La topologie du réseau Smartech SA s'organise autour de trois domaines de routage interconnectés. L'architecture comporte 7 routeurs Cisco, 2 commutateurs de niveau 2, 3 hôtes utilisateurs, 1 serveur web (VM Ubuntu), et une connexion Internet simulée.

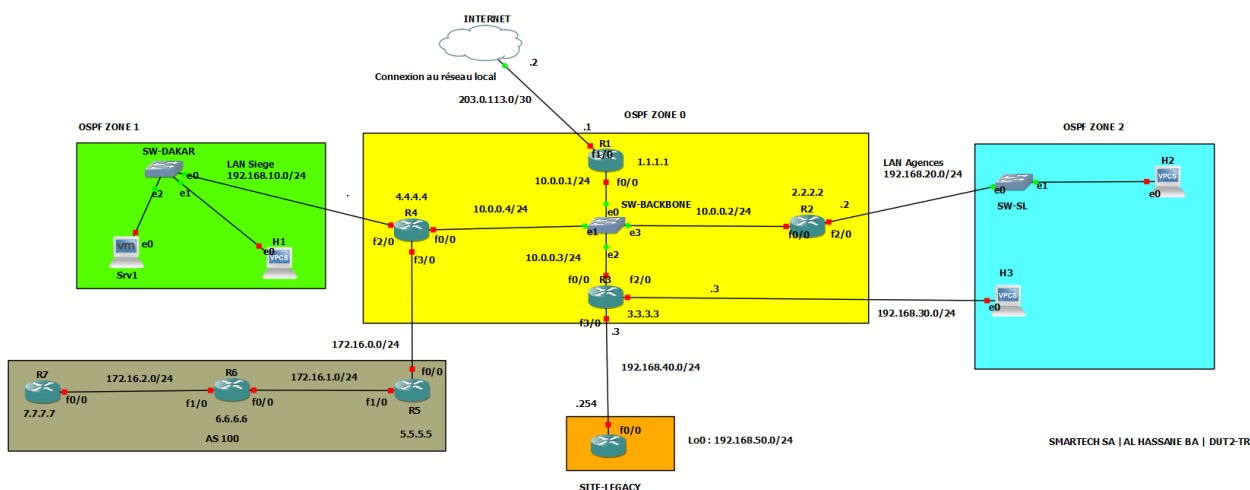


Figure 1 — Architecture logique du réseau Smartech SA

## 2.2 Composants du Réseau

Composant	Rôle	Zone / Protocole	Adresses Clés
R1	Border Router + DR OSPF + Passerelle Internet	OSPF Zone 0	1.1.1.1/32, 10.0.0.1/24, 203.0.113.1/30
R2	LAN Saint-Louis + ABR OSPF	OSPF Zone 0 / Zone 2	2.2.2.2/32, 10.0.0.2/24, 192.168.20.2/24
R3	LAN Ziguinchor + Passerelle RIP	OSPF Zone 0 / RIP v2	3.3.3.3/32, 10.0.0.3/24, 192.168.30.3/24
R4	LAN Siège + BDR OSPF + Passerelle EIGRP	OSPF Zone 0,1 / EIGRP	4.4.4.4/32, 10.0.0.4/24, 192.168.10.4/24
R5	Routeur EIGRP partenaire	EIGRP AS 100	5.5.5.5/32, 172.16.0.5/24, 172.16.1.5/24
R6	Routeur EIGRP partenaire	EIGRP AS 100	6.6.6.6/32, 172.16.1.6/24, 172.16.2.6/24
R7	Routeur EIGRP partenaire	EIGRP AS 100	7.7.7.7/32, 172.16.2.7/24
RRIP	Site legacy RIP v2	RIP v2	192.168.40.X/24
SW-Dakar	Commutateur L2 Siège	—	—
SW-SL	Commutateur L2 Saint-Louis	—	—
H1	Hôte Siège (DHCP)	LAN 192.168.10.0/24	192.168.10.X (DHCP)
H2	Hôte Saint-Louis (DHCP)	LAN 192.168.20.0/24	192.168.20.X (DHCP)
H3	Hôte Ziguinchor	LAN 192.168.30.0/24	192.168.30.X
SRV1	Serveur Web simulé	LAN Siège	192.168.10.100/24

## 2.3 Plan d'Adressage IPv4 Complet

La règle d'adressage est simple et cohérente : chaque routeur possède une loopback0 en /32 dont l'adresse correspond à son numéro (ex : R3 → 3.3.3.3/32). Sur les réseaux partagés, le dernier octet de l'adresse correspond également au numéro du routeur.

Routeur	Interface	Réseau	Adresse IP	Protocole
R1	Loopback0	1.1.1.1/32	1.1.1.1	OSPF Z0
R1	G0/0	10.0.0.0/24	10.0.0.1	OSPF Z0
R1	G0/1	203.0.113.0/30	203.0.113.1	Internet
R2	Loopback0	2.2.2.2/32	2.2.2.2	OSPF Z0
R2	G0/0	10.0.0.0/24	10.0.0.2	OSPF Z0
R2	G0/1	192.168.20.0/24	192.168.20.2	OSPF Z2
R3	Loopback0	3.3.3.3/32	3.3.3.3	OSPF Z0
R3	G0/0	10.0.0.0/24	10.0.0.3	OSPF Z0
R3	G0/1	192.168.30.0/24	192.168.30.3	OSPF Z2
R3	G0/2	192.168.40.0/24	192.168.40.3	RIP v2
R4	Loopback0	4.4.4.4/32	4.4.4.4	OSPF Z0
R4	G0/0	10.0.0.0/24	10.0.0.4	OSPF Z0
R4	G0/1	192.168.10.0/24	192.168.10.4	OSPF Z1
R4	G0/2	172.16.0.0/24	172.16.0.4	EIGRP AS100
R5	Loopback0	5.5.5.5/32	5.5.5.5	EIGRP AS100
R5	G0/0	172.16.0.0/24	172.16.0.5	EIGRP AS100
R5	G0/1	172.16.1.0/24	172.16.1.5	EIGRP AS100
R6	Loopback0	6.6.6.6/32	6.6.6.6	EIGRP AS100
R6	G0/0	172.16.1.0/24	172.16.1.6	EIGRP AS100
R6	G0/1	172.16.2.0/24	172.16.2.6	EIGRP AS100
R7	Loopback0	7.7.7.7/32	7.7.7.7	EIGRP AS100
R7	G0/0	172.16.2.0/24	172.16.2.7	EIGRP AS100
SRV1	—	192.168.10.0/24	192.168.10.100	LAN Siège

## 3. Configuration DHCP et DNS

### 3.1 DHCP sur R4 — LAN Siège (192.168.10.0/24)

R4 distribue dynamiquement des adresses IP aux hôtes du réseau siège. L'adresse 192.168.10.100 est exclue pour SRV1 (adresse statique). La plage dynamique couvre les adresses .10 à .254.

```

R4(config)#
R4(config)#
R4(config)#! --- DHCP pour LAN SiC(ge (192.168.10.0/24) ---
R4(config)#! SRV1 a une adresse fixe 192.168.10.100 -> C  exclure du pool
R4(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.20
R4(config)#ip dhcp excluded-address 192.168.10.100
R4(config)#
R4(config)#ip dhcp pool LAN-SIEGE
R4(dhcp-config)# network 192.168.10.0 255.255.255.0
R4(dhcp-config)# default-router 192.168.10.4
R4(dhcp-config)# dns-server 8.8.8.8
R4(dhcp-config)# lease 7
R4(dhcp-config)#

```

### 3.2 DHCP sur R2 — LAN Saint-Louis (192.168.20.0/24)

R2 joue le même rôle pour le LAN de l'agence de Saint-Louis.

```

R2(config)#
R2(config)#! --- DHCP pour LAN Saint-Louis (192.168.20.0/24) ---
R2(config)#! Exclure l'adresse du routeur et C)ventuellement les serveurs
R2(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.10
R2(config)#
R2(config)#ip dhcp pool LAN-SAINT-LOUIS
R2(dhcp-config)# network 192.168.20.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.20.2
R2(dhcp-config)# dns-server 8.8.8.8
R2(dhcp-config)# lease 7
R2(dhcp-config)#

```

### 3.3 Vérification DHCP

Test	Hôte	Adresse Obtenue	Passerelle	Résultat
DHCP Request H1	H1 (Siège)	192.168.10.X	192.168.10.4	SUCCESS
DHCP Request H2	H2 (Saint-Louis)	192.168.20.X	192.168.20.2	SUCCESS
Adresse fixe SRV1	SRV1	192.168.10.100	192.168.10.4	SUCCESS

```

H1> dhcp
DDORRA IP 192.168.10.21/24 GW 192.168.10.4
H1> sh ip
NAME          : H1[1]
IP/MASK       : 192.168.10.21/24
GATEWAY       : 192.168.10.4
DNS           : 8.8.8.8
DHCP SERVER   : 192.168.10.4
DHCP LEASE    : 604795, 604800/302400/529200
MAC           : 00:50:79:66:68:00
LPORT        : 10062
RHOST:PORT    : 127.0.0.1:10063
MTU:          : 1500
H1>

```

```

H2> dhcp
DDORRA IP 192.168.20.11/24 GW 192.168.20.2
H2> sh ip
NAME          : H2[1]
IP/MASK       : 192.168.20.11/24
GATEWAY       : 192.168.20.2
DNS           : 8.8.8.8
DHCP SERVER   : 192.168.20.2
DHCP LEASE    : 604795, 604800/302400/529200
MAC           : 00:50:79:66:68:02
LPORT        : 10066
RHOST:PORT    : 127.0.0.1:10067
MTU:          : 1500
H2>

```

---

## 4. Déploiement OSPF Multi-Zones

### 4.1 Configuration de Base OSPF

---

OSPF est activé avec le processus ID 1 sur R1, R2, R3 et R4. La zone backbone (Zone 0) s'étend sur le segment 10.0.0.0/24. Chaque routeur annonce sa loopback et ses réseaux connectés.

#### Configuration R1 (DR - Backbone + Internet)

```
R1(config)#
R1(config)#router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 1.1.1.1 0.0.0.0 area 0
R1(config-router)# network 10.0.0.0 0.0.0.255 area 0
R1(config-router)# default-information originate always
R1(config-router)#
```

```
R1(config-if)#interface f0/0
R1(config-if)# description ZONE0-SW-BACKBONE
R1(config-if)#
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# ip ospf priority 255
R1(config-if)# no shutdown
```

#### Configuration R2 (ABR - Zone 0 / Zone 2)

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#
R2(config)#router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 2.2.2.2 0.0.0.0 area 0
R2(config-router)# network 10.0.0.0 0.0.0.255 area 0
R2(config-router)# ! Annoncer le LAN Saint-Louis dans Zone 2
R2(config-router)# network 192.168.20.0 0.0.0.255 area 2
R2(config-router)##$PF Hello sur l'interface LAN (pas d'autre routeur)
R2(config-router)# passive-interface f2/0
R2(config-router)#
*Feb 28 00:22:49.119: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
R2(config-router)#end
R2#write memory
Building configuration...
[OK]
R2#
*Feb 28 00:23:03.075: %SYS-5-CONFIG_I: Configured from console by console
```

#### Configuration R3 (ABR - Zone 0 / Zone 2 + RIP)

```
R3(config)#
R3(config)#
R3(config)#router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 3.3.3.3 0.0.0.0 area 0
R3(config-router)# network 10.0.0.0 0.0.0.255 area 0
R3(config-router)# ! LAN Ziguinchor dans Zone 2
R3(config-router)# network 192.168.30.0 0.0.0.255 area 2
R3(config-router)# passive-interface f2/0
R3(config-router)# ! Redistribuer les routes RIP dans OSPF
R3(config-router)##$ire pour redistribuer les sous-réseaux classless
R3(config-router)##$OSPF pour les routes externes (type E2 par défaut)
R3(config-router)# redistribute rip subnets metric 20
R3(config-router)#
*Feb 28 00:25:18.295: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/0 from LOADING to FULL, Loading Done
R3(config-router)#
*Feb 28 00:25:20.995: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
R3(config-router)#
```

## Configuration R4 (BDR - Zone 0 / Zone 1 + EIGRP)

```
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#
R4(config)#
R4(config)#router ospf 1
R4(config-router)# router-id 4.4.4.4
R4(config-router)# network 4.4.4.4 0.0.0.0 area 0
R4(config-router)# network 10.0.0.0 0.0.0.255 area 0
R4(config-router)# ! LAN SiC(ge dans Zone 1
R4(config-router)# network 192.168.10.0 0.0.0.255 area 1
R4(config-router)# passive-interface f2/0
R4(config-router)# ! Redistribuer EIGRP dans OSPF
R4(config-router)# ! subnets obligatoire, metric 20 = coC;t E2
R4(config-router)# redistribute eigrp 100 subnets metric 20
R4(config-router)#
*Feb 28 00:26:25.611: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/0 from LOADING to FULL, Loading Done
R4(config-router)#
*Feb 28 00:26:27.683: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
```

## 4.2 Élection DR/BDR

### Justification de l'élection DR/BDR

L'élection DR/BDR sur OSPF se base sur deux critères par ordre de priorité :

1. La priorité d'interface OSPF (0-255, défaut = 1, 0 = exclusion de l'élection)
2. En cas d'égalité : le Router-ID le plus élevé l'emporte

Choix retenus :

- R1 : priorité 255 sur G0/0 => DR garanti
- R4 : priorité 100 sur G0/0 => BDR garanti
- R2, R3 : priorité par défaut (1) => DROTHER

ATTENTION : Modifier la priorité ne prend effet qu'après un clear ip ospf process ou un redémarrage. En production, planifier une fenêtre de maintenance.

## 4.3 Vérification OSPF

```
show ip ospf neighbor
show ip ospf database
show ip route ospf
show ip ospf interface fa0/0
```

Test Connectivité OSPF	Source	Destination	Résultat Attendu
Ping loopback R1->R4	1.1.1.1	4.4.4.4	SUCCES (OSPF Z0)
Ping loopback R2->R3	2.2.2.2	3.3.3.3	SUCCES (OSPF Z0)
Ping H1 -> H2	192.168.10.X	192.168.20.X	SUCCES (Inter-zones)
Ping H1 -> H3	192.168.10.X	192.168.30.X	SUCCES (Inter-zones)
Ping R2 -> Internet	10.0.0.2	203.0.113.2	SUCCES (route default)
Traceroute H1->H2	LAN Siège	LAN Saint-Louis	R4->R1/R4->R2->H2

```

R1#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/36/56 ms
R1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/40/60 ms
R1#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
R1#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/56/96 ms
R1#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/39/48 ms
R1#

```

```

R2#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/33/40 ms
R2#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/50/68 ms
R2#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/47/64 ms
R2#traceroute 1.1.1.1
Type escape sequence to abort.
Tracing the route to 1.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.0.1 64 msec 44 msec 28 msec
R2#traceroute 2.2.2.2
Type escape sequence to abort.
Tracing the route to 2.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
 1 2.2.2.2 8 msec 4 msec 8 msec
R2#traceroute 4.4.4.4
Type escape sequence to abort.
Tracing the route to 4.4.4.4
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.0.4 68 msec 24 msec 68 msec
R2#

```

```

R1#sh ip ospf route

OSPF Router with ID (1.1.1.1) (Process ID 1)

Base Topology (MTID 0)

Area BACKBONE(0)

Intra-area Route List
* 10.0.0.0/24, Intra, cost 1, area 0, Connected
  via 10.0.0.1, FastEthernet0/0
* 1.1.1.1/32, Intra, cost 1, area 0, Connected
  via 1.1.1.1, Loopback0
R1#

```

```

R3#traceroute 1.1.1.1
Type escape sequence to abort.
Tracing the route to 1.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.0.1 36 msec 12 msec 48 msec
R3#traceroute 4.4.4.4
Type escape sequence to abort.
Tracing the route to 4.4.4.4
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.0.4 8 msec 40 msec 32 msec
R3#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/46/56 ms
R3#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/24/48 ms
R3#

```

---

## 5. Déploiement EIGRP et Redistribution OSPF↔EIGRP

### 5.1 Configuration EIGRP AS 100

---

Le domaine EIGRP représente le réseau d'un partenaire commercial. Il couvre la plage 172.16.0.0/16 et interconnecte R4, R5, R6 et R7 en chaîne. La sommation automatique est désactivée pour préserver les préfixes /24.

#### Configuration R4 (point de redistribution)

```
R4(config-if)#
R4(config-if)#! --- Interface vers R5 (domaine EIGRP AS100) ---
R4(config-if)#in
*Feb 27 23:58:11.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
face f3/0
R4(config-if)# description EIGRP-LIEN-R4-R5
R4(config-if)# ip address 172.16.0.4 255.255.255.0
R4(config-if)# no shutdown
R4(config-if)#
```

#### Configuration R5

```
R5(config)#
R5(config)#hostname R5
R5(config)#
R5(config)#no ip domain-lookup
R5(config)#
R5(config)#! --- Loopback ---
R5(config)#interface Loopback0
R5(config-if)# ip address 5.5.5.5 255.255.255.255
R5(config-if)# no shutdown
R5(config-if)#
R5(config-if)#! --- Interface vers R4 (jonction OSPF/EIGRP) ---
R5(config-if)#interface f0/0
R5(config-if)# description EIGRP-LIEN-R5-R4
R5(config-if)# ip address 172.16.0.5 255.255.255.0
R5(config-if)# no shutdown
R5(config-if)#
*Feb 28 00:04:07.799: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R5(config-if)#
*Feb 28 00:04:10.779: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Feb 28 00:04:11.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R5(config-if)#! --- Interface vers R6 ---
R5(config-if)#$dth rC)duit pour que R5 soit prC)fC)rC) pour Internet
R5(config-if)#$nde passante sur le lien R6->R7, R5 sera le chemin prC)fC)rC)
R5(config-if)#interface f1/0
R5(config-if)# description EIGRP-LIEN-R5-R6
R5(config-if)# ip address 172.16.1.5 255.255.255.0
R5(config-if)#$r le dC)lai pour rendre ce lien moins prC)fC)rC) depuis R6/R7
R5(config-if)# ! (ainsi R5 reste le routeur prC)fC)rC) pour joindre Internet)
R5(config-if)# bandwidth 1000
R5(config-if)# delay 100
R5(config-if)# no shutdown
R5(config-if)#
*Feb 28 00:04:55.659: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Feb 28 00:04:56.659: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
```

#### Configurations R6 et R7 (similaires)

```

R6#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R6(config)#
R6(config)#hostname R6
R6(config)#
R6(config)#no ip domain-lookup
R6(config)#
R6(config)#! --- Loopback ---
R6(config)#interface Loopback0
R6(config-if)# ip address 6.6.6.6 255.255.255.255
R6(config-if)# no shutdown
R6(config-if)#
R6(config-if)#! --- Interface vers R5 (172.16.1.0/24) ---
R6(config-if)#interface f0/0
R6(config-if)# description EIGRP-LIEN-R6-R5
R6(config-if)# ip address 172.16.1.6 255.255.255.0
R6(config-if)# bandwidth 1000
R6(config-if)# delay 100
R6(config-if)# no shutdown
R6(config-if)#
R6(config-if)#! --- Interface vers R7 (172.16.2.0/24) ---
R6(config-if)#interface f1/0
R6(config-if)# description EIGRP-LIEN-R6-R7
R6(config-if)# ip address 172.16.2.6 255.255.255.0
R6(config-if)# bandwidth 512
R6(config-if)# delay 200
R6(config-if)# no shutdown
R6(config-if)#
*Feb 28 00:06:15.183: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R6(config-if)#
*Feb 28 00:06:18.327: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

```

## 5.2 Authentification MD5 entre R4 et R5

L'authentification EIGRP par MD5 sécurise les échanges de routage entre R4 (domaine OSPF) et R5 (domaine EIGRP). Elle prévient l'injection de fausses routes.

```

R5(config)#! --- Authentification MD5 EIGRP entre R5 et R4 ---
R5(config)#$) que R4 (obligatoire pour C)tablir la relation de voisinage)
R5(config)#key chain EIGRP-MD5
R5(config-keychain)# key 1
R5(config-keychain-key)# key-string SmartechEIGRP2025
R5(config-keychain-key)#
R5(config-keychain-key)#interface f0/0
R5(config-if)# ip authentication mode eigrp 100 md5
R5(config-if)# ip authentication key-chain eigrp 100 EIGRP-MD5
R5(config-if)#

```

La même clé EIGRP-KEY doit être configurée sur R4 interface F3/0 pour que l'adjacence s'établisse.

```

R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#
R4(config)#key chain EIGRP-MD5
R4(config-keychain)# key 1
R4(config-keychain-key)# key-string SmartechEIGRP2025
R4(config-keychain-key)#
R4(config-keychain-key)#interface f3/0
R4(config-if)# ip authentication mode eigrp 100 md5
R4(config-if)# ip authentication key-chain eigrp 100 EIGRP-MD5
R4(config-if)#
R4(config-if)#end
R4#write memory
*Feb 28 09:08:56.251: %SYS-5-CONFIG_I: Configured from console by console
*Feb 28 09:08:56.371: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 172.16.0.5 (FastEthernet3/0) is up:
ew adjacency
R4#write memory

```

## 5.3 Ajustement des Métriques EIGRP

Pour que R5 soit le routeur préféré pour joindre Internet depuis le domaine EIGRP, on augmente la métrique sur les liens R5-R6 et R6-R7. La métrique EIGRP (DUAL) se calcule selon la bande passante et le délai.

## 5.4 Redistribution Bidirectionnelle OSPF ↔ EIGRP sur R4

R4 assure la redistribution dans les deux sens. Des tags et route-maps sont utilisés pour prévenir les boucles de routage liées à la redistribution mutuelle.

### Redistribution OSPF → EIGRP + Redistribution EIGRP → OSPF

```
R4(config-router)#router ospf 1
R4(config-router)# redistribute eigrp 100 subnets metric 20
R4(config-router)#
R4(config-router)#
R4(config-router)#exit
R4(config)#route-map EIGRP_TO_OSPF deny 10
R4(config-route-map)# match tag 200
R4(config-route-map)#
R4(config-route-map)#route-map EIGRP_TO_OSPF permit 20
R4(config-route-map)#
R4(config-route-map)#route-map OSPF_TO_EIGRP permit 10
R4(config-route-map)# set tag 200
R4(config-route-map)#router eigrp 100
R4(config-router)#metric 1000 100 255 1 1500 route-map OSPF_TO_EIGRP
R4(config-router)#
```

## 5.5 Vérification EIGRP

Commande	Information affichée
show ip eigrp neighbors	Voisins EIGRP établis (R4-R5, R5-R6, R6-R7)
show ip eigrp topology	Table de topologie DUAL (successeurs, FS)
show ip route eigrp	Routes EIGRP dans la table de routage (D, D EX)
show ip route ospf	Sur R1/R2/R3 : routes 172.16.0.0/xx visibles (O E2)

```
R5#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address          Interface         Hold Uptime    SRTT   RTO  Q  Seq
                               (sec)          (ms)          Cnt Num
1   172.16.0.4         Fa0/0            14 00:00:53   63   378  0   3
0   172.16.1.6         Fa1/0            10 00:02:07   38   228  0  13
R5#
```

```
R7#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 124/138/168 ms
R7#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/125/136 ms
R7#
```

```
R4#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is 10.0.0.1 to network 0.0.0.0
```

```
5.0.0.0/32 is subnetted, 1 subnets
D      5.5.5.5 [90/156160] via 172.16.0.5, 00:01:30, FastEthernet3/0
6.0.0.0/32 is subnetted, 1 subnets
D      6.6.6.6 [90/2716160] via 172.16.0.5, 00:01:30, FastEthernet3/0
7.0.0.0/32 is subnetted, 1 subnets
D      7.7.7.7 [90/5207296] via 172.16.0.5, 00:01:30, FastEthernet3/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D      172.16.1.0/24 [90/2588160] via 172.16.0.5, 00:01:30, FastEthernet3/0
D      172.16.2.0/24 [90/5079296] via 172.16.0.5, 00:01:30, FastEthernet3/0
```

```
R4#
```

```
R4#
```

```
R5#ping 1.1.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/72/124 ms
```

```
R5#ping 2.2.2.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/62/72 ms
```

```
R5#
```

```
R4#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is 10.0.0.1 to network 0.0.0.0
```

```
5.0.0.0/32 is subnetted, 1 subnets
D      5.5.5.5 [90/156160] via 172.16.0.5, 00:01:30, FastEthernet3/0
6.0.0.0/32 is subnetted, 1 subnets
D      6.6.6.6 [90/2716160] via 172.16.0.5, 00:01:30, FastEthernet3/0
7.0.0.0/32 is subnetted, 1 subnets
D      7.7.7.7 [90/5207296] via 172.16.0.5, 00:01:30, FastEthernet3/0
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D      172.16.1.0/24 [90/2588160] via 172.16.0.5, 00:01:30, FastEthernet3/0
D      172.16.2.0/24 [90/5079296] via 172.16.0.5, 00:01:30, FastEthernet3/0
```

```
R4#
```

```
R4#
```

---

## 6. Déploiement RIP v2 et Redistribution OSPF↔RIP

### 6.1 Configuration RIP v2 sur R3 + Redistribution OSPF → RIP

R3 assure la connexion entre le domaine OSPF et le site legacy RIP. L'interface F3/0 (192.168.40.3/24) est activée en RIP v2. La sommation automatique est désactivée pour éviter la perte d'information de sous-réseau.

```
R3(config)#router rip
R3(config-router)# version 2
R3(config-router)# ! Annoncer le réseau legacy
R3(config-router)# network 192.168.40.0
R3(config-router)# $ver la sommation automatique (obligatoire pour VLSM)
R3(config-router)# no auto-summary
R3(config-router)# ! Redistribuer les routes OSPF dans RIP
R3(config-router)# $ = nombre de sauts attribués aux routes redistribuées
R3(config-router)# redistribute ospf 1 metric 5
R3(config-router)#
R3(config-router)#
```

### 6.2 Configuration du Routeur RRIP (Site Legacy)

RRIP simule le site legacy. Il annonce ses réseaux locaux en RIP v2 et apprend les routes OSPF redistribuées par R3.

```
RRIP(config)#router rip
RRIP(config-router)# version 2
RRIP(config-router)# ! Annoncer le réseau legacy et la loopback
RRIP(config-router)# network 192.168.40.0
RRIP(config-router)# network 192.168.50.0
RRIP(config-router)# no auto-summary
RRIP(config-router)#
RRIP(config-router)#end
RRIP#write memory
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
```

### 6.3 Redistribution Bidirectionnelle OSPF ↔ RIP sur R3

Les routes RIP apparaîtront comme O E2 dans les tables OSPF

```

[1] via 192.168.40.254, 00:00:09, FastEthernet3/0
R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.0.1, 01:17:56, FastEthernet0/0
O     1.0.0.0/32 is subnetted, 1 subnets
O     1.1.1.1 [110/2] via 10.0.0.1, 01:17:56, FastEthernet0/0
O     2.0.0.0/32 is subnetted, 1 subnets
O     2.2.2.2 [110/2] via 10.0.0.2, 01:17:51, FastEthernet0/0
C     3.0.0.0/32 is subnetted, 1 subnets
C     3.3.3.3 is directly connected, Loopback0
O     4.0.0.0/32 is subnetted, 1 subnets
O     4.4.4.4 [110/2] via 10.0.0.4, 01:17:56, FastEthernet0/0
O     5.0.0.0/32 is subnetted, 1 subnets
O E2  5.5.5.5 [110/20] via 10.0.0.4, 00:21:29, FastEthernet0/0
O E2  6.0.0.0/32 is subnetted, 1 subnets
O E2  6.6.6.6 [110/20] via 10.0.0.4, 00:21:29, FastEthernet0/0
O E2  7.0.0.0/32 is subnetted, 1 subnets
O E2  7.7.7.7 [110/20] via 10.0.0.4, 00:21:29, FastEthernet0/0
C     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C     10.0.0.0/24 is directly connected, FastEthernet0/0
L     10.0.0.3/32 is directly connected, FastEthernet0/0
C     172.16.0.0/24 is subnetted, 3 subnets
O E2  172.16.0.0 [110/20] via 10.0.0.4, 00:36:12, FastEthernet0/0
O E2  172.16.1.0 [110/20] via 10.0.0.4, 00:21:29, FastEthernet0/0
O E2  172.16.2.0 [110/20] via 10.0.0.4, 00:21:29, FastEthernet0/0
O IA  192.168.10.0/24 [110/2] via 10.0.0.4, 01:17:56, FastEthernet0/0
O IA  192.168.20.0/24 [110/2] via 10.0.0.2, 01:17:51, FastEthernet0/0
C     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.30.0/24 is directly connected, FastEthernet2/0
L     192.168.30.3/32 is directly connected, FastEthernet2/0
C     192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.40.0/24 is directly connected, FastEthernet3/0
L     192.168.40.3/32 is directly connected, FastEthernet3/0
R     192.168.50.0/24 [120/1] via 192.168.40.254, 00:00:04, FastEthernet3/0
R3#

```

## 6.4 Gestion des Boucles de Redistribution

### Analyse des risques et solution anti-boucle OSPF-RIP

Problème : Sans protection, une route OSPF redistribuée en RIP peut revenir dans OSPF avec une métrique dégradée, créant une boucle ou un sous-optimal routing.

Solution adoptée : Utilisation de route-maps avec tags :

- Les routes OSPF redistribuées vers RIP reçoivent le TAG 300
- Le filtre de redistribution RIP->OSPF exclut les routes avec TAG 300

Alternative : filtrage par prefix-list sur les réseaux redistribués.

Vérifier : 'show ip route' sur R3 ne doit pas montrer de routes E2 avec préfixe OSPF.

```

R3(config-router)#! Etape 1 : route-map pour taguer OSPF->RIP
R3(config-router)#route-map OSPF_TO_RIP permit 10
R3(config-route-map)# match ip address prefix-list OSPF_NETWORKS
R3(config-route-map)# set metric 5
R3(config-route-map)#
R3(config-route-map)#$rer RIP->OSPF (bloquer les routes dC)jC venues d'OSPF)
R3(config-route-map)#route-map RIP_TO_OSPF deny 10
R3(config-route-map)# match tag 100
R3(config-route-map)#
R3(config-route-map)#route-map RIP_TO_OSPF permit 20
R3(config-route-map)#
R3(config-route-map)#! Appliquer les route-maps dans les redistributions
R3(config-route-map)#router rip
R3(config-router)# redistribute ospf 1 metric 5 route-map OSPF_TO_RIP
R3(config-router)#
R3(config-router)#router ospf 1
R3(config-router)# redistribute rip subnets metric 20 route-map RIP_TO_OSPF
R3(config-router)#
R3(config-router)#

```

## 6.5 Tableau Comparatif OSPF / EIGRP / RIP

Critère	OSPF	EIGRP	RIP v2
Type	Link-State	Hybride (Distance-Vector avancé)	Distance-Vector
Algorithme	Dijkstra (SPF)	DUAL (Diffusing Update Algo)	Bellman-Ford
Métrique	Coût (BW inverse)	BW + Délai + Fiabilité + Charge	Hop count (max 15)
Convergence	Rapide (LSA immédiat)	Très rapide (DUAL calcul local)	Lente (30s updates)
Scalabilité	Haute (multi-zones)	Moyenne-haute	Faible (15 hops max)
VLSM	Oui	Oui	Oui (v2 seulement)
Authentification	MD5 / SHA	MD5	MD5 (v2)
Standard	Ouvert (RFC 2328)	Propriétaire Cisco	Ouvert (RFC 2453)
Cas d'usage	Grande entreprise, FAI	Réseaux Cisco moyens/grands	Très petits réseaux, legacy
Supporte ECMP	Oui	Oui (unequal BW avec variance)	Oui (6 chemins max)

```

R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

  1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
  2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 10.0.0.2, 01:12:52, FastEthernet0/0
  3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 10.0.0.3, 01:12:52, FastEthernet0/0
  4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/2] via 10.0.0.4, 01:12:57, FastEthernet0/0
  5.0.0.0/32 is subnetted, 1 subnets
O E2    5.5.5.5 [110/20] via 10.0.0.4, 00:16:29, FastEthernet0/0
  6.0.0.0/32 is subnetted, 1 subnets
O E2    6.6.6.6 [110/20] via 10.0.0.4, 00:16:29, FastEthernet0/0
  7.0.0.0/32 is subnetted, 1 subnets
O E2    7.7.7.7 [110/20] via 10.0.0.4, 00:16:29, FastEthernet0/0
 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/24 is directly connected, FastEthernet0/0
L       10.0.0.1/32 is directly connected, FastEthernet0/0
 172.16.0.0/24 is subnetted, 3 subnets
O E2    172.16.0.0 [110/20] via 10.0.0.4, 00:31:12, FastEthernet0/0
O E2    172.16.1.0 [110/20] via 10.0.0.4, 00:16:29, FastEthernet0/0
O E2    172.16.2.0 [110/20] via 10.0.0.4, 00:16:29, FastEthernet0/0
O IA    192.168.10.0/24 [110/2] via 10.0.0.4, 01:12:57, FastEthernet0/0
O IA    192.168.20.0/24 [110/2] via 10.0.0.2, 01:12:52, FastEthernet0/0
O IA    192.168.30.0/24 [110/2] via 10.0.0.3, 01:12:52, FastEthernet0/0
O E2    192.168.40.0/24 [110/20] via 10.0.0.3, 00:03:43, FastEthernet0/0
O E2    192.168.50.0/24 [110/20] via 10.0.0.3, 00:03:30, FastEthernet0/0
R1#

```

```

R4#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.0.1, 01:13:39, FastEthernet0/0
      1.0.0.0/32 is subnetted, 1 subnets
O      1.1.1.1 [110/2] via 10.0.0.1, 01:13:39, FastEthernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
O      2.2.2.2 [110/2] via 10.0.0.2, 01:13:34, FastEthernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
O      3.3.3.3 [110/2] via 10.0.0.3, 01:13:34, FastEthernet0/0
      4.0.0.0/32 is subnetted, 1 subnets
C      4.4.4.4 is directly connected, Loopback0
      5.0.0.0/32 is subnetted, 1 subnets
D      5.5.5.5 [90/156160] via 172.16.0.5, 00:17:11, FastEthernet3/0
      6.0.0.0/32 is subnetted, 1 subnets
D      6.6.6.6 [90/2716160] via 172.16.0.5, 00:17:11, FastEthernet3/0
      7.0.0.0/32 is subnetted, 1 subnets
D      7.7.7.7 [90/5207296] via 172.16.0.5, 00:17:11, FastEthernet3/0
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.0.0.0/24 is directly connected, FastEthernet0/0
L      10.0.0.4/32 is directly connected, FastEthernet0/0
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.16.0.0/24 is directly connected, FastEthernet3/0
L      172.16.0.4/32 is directly connected, FastEthernet3/0
D      172.16.1.0/24 [90/2588160] via 172.16.0.5, 00:17:11, FastEthernet3/0
D      172.16.2.0/24 [90/5079296] via 172.16.0.5, 00:17:11, FastEthernet3/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.10.0/24 is directly connected, FastEthernet2/0
L      192.168.10.4/32 is directly connected, FastEthernet2/0
O IA 192.168.20.0/24 [110/2] via 10.0.0.2, 01:13:34, FastEthernet0/0
O IA 192.168.30.0/24 [110/2] via 10.0.0.3, 01:13:34, FastEthernet0/0
O E2 192.168.40.0/24 [110/20] via 10.0.0.3, 00:04:26, FastEthernet0/0
O E2 192.168.50.0/24 [110/20] via 10.0.0.3, 00:04:12, FastEthernet0/0
R4#

```

```

RRIP#sh ip rip database
0.0.0.0/0 auto-summary
0.0.0.0/0
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
1.0.0.0/8 auto-summary
1.1.1.1/32
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
2.0.0.0/8 auto-summary
2.2.2.2/32
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
3.0.0.0/8 auto-summary
3.3.3.3/32
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
4.0.0.0/8 auto-summary
4.4.4.4/32
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
5.0.0.0/8 auto-summary
5.5.5.5/32
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
6.0.0.0/8 auto-summary
6.6.6.6/32
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
7.0.0.0/8 auto-summary
7.7.7.7/32
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
10.0.0.0/8 auto-summary
10.0.0.0/24
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
172.16.0.0/16 auto-summary
172.16.0.0/24
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
172.16.1.0/24
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
172.16.2.0/24
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
192.168.10.0/24 auto-summary
192.168.10.0/24
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
192.168.20.0/24 auto-summary
192.168.20.0/24
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
192.168.30.0/24 auto-summary
192.168.30.0/24
      [5] via 192.168.40.3, 00:00:24, FastEthernet0/0
192.168.40.0/24 auto-summary
192.168.40.0/24 directly connected, FastEthernet0/0
192.168.50.0/24 auto-summary
192.168.50.0/24 directly connected, Loopback0
RRIP#

```

```

RRIP#ping 192.168.10
% Unrecognized host or address, or protocol not running.

RRIP#ping 192.168.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/65/108 ms
RRTP#

```

## 7. Analyse du Trafic avec Wireshark

### 7.1 Méthodologie

Six captures Wireshark ont été réalisées sur différents segments du réseau pour analyser le fonctionnement des protocoles. Chaque capture est annotée et sauvegardée en format .pcap.

### 7.2 Capture 1 — Échanges OSPF Hello et DBD

Paramètre	Valeur observée
Interface capturée	R1 F0/0 (backbone 10.0.0.0/24)
IP Source	10.0.0.1 (R1), 10.0.0.2 (R2), etc.
IP Destination	224.0.0.5 (AllSPFRouters) / 224.0.0.6 (AllDRRouters)
Protocole	OSPF (IP protocol 89)
Type de paquet	Hello (type 1) + DBD (type 2)
Intervalles Hello	10 secondes (réseau multi-accès)
Dead interval	40 secondes (4 x Hello)
Analyse	Les Hello permettent la découverte des voisins et le maintien de l'adjacence. Le DBD contient le résumé de la LSDB pour la synchronisation initiale.

No.	Time	Source	Destination	Protocol	Length	Info
522	827.703751	10.0.0.2	10.0.0.1	OSPF	358	LS Acknowledge
523	827.915266	10.0.0.2	224.0.0.6	OSPF	110	LS Update
524	829.908076	10.0.0.3	224.0.0.6	OSPF	98	LS Acknowledge
525	829.908076	10.0.0.4	224.0.0.5	OSPF	98	LS Acknowledge
526	830.205058	10.0.0.2	224.0.0.6	OSPF	358	LS Acknowledge
527	832.195151	10.0.0.1	10.0.0.2	OSPF	138	LS Update
528	832.207685	10.0.0.2	10.0.0.1	OSPF	78	LS Acknowledge
529	832.617120	10.0.0.4	10.0.0.2	OSPF	138	LS Update
530	832.683610	10.0.0.2	10.0.0.4	OSPF	78	LS Acknowledge
531	832.804289	10.0.0.2	10.0.0.4	OSPF	110	LS Update
532	832.823222	10.0.0.4	10.0.0.2	OSPF	110	LS Update
533	832.875442	10.0.0.2	10.0.0.1	OSPF	110	LS Update
534	832.913623	10.0.0.1	10.0.0.2	OSPF	110	LS Update
535	832.923720	10.0.0.2	224.0.0.6	OSPF	110	LS Update
536	832.957832	10.0.0.1	224.0.0.5	OSPF	110	LS Update
537	834.733876	10.0.0.2	224.0.0.6	OSPF	118	LS Acknowledge
538	835.156515	10.0.0.1	224.0.0.5	OSPF	102	Hello Packet
539	835.456023	10.0.0.3	224.0.0.6	OSPF	78	LS Acknowledge
540	835.476326	10.0.0.4	224.0.0.5	OSPF	78	LS Acknowledge
541	836.222615	ca:03:68:d4:00:00	CDP/VTP/DTP/PAgP/UD...	CDP	366	Device ID: R3 Port ID: FastEthernet0/0
542	836.243017	10.0.0.3	224.0.0.5	OSPF	102	Hello Packet
543	836.526675	ca:02:5a:e0:00:00	ca:02:5a:e0:00:00	LOOP	60	Reply
544	836.724881	10.0.0.4	224.0.0.5	OSPF	102	Hello Packet
545	837.356077	10.0.0.2	224.0.0.5	OSPF	102	Hello Packet
546	837.577560	10.0.0.2	224.0.0.6	OSPF	98	LS Update
547	837.588177	10.0.0.1	224.0.0.5	OSPF	98	LS Update

### 7.3 Capture 2 — Échanges EIGRP Hello et Update

Paramètre	Valeur observée
Interface capturée	R4 F0/2 (172.16.0.0/24, vers R5)
IP Source/Destination	172.16.0.4 / 224.0.0.10 (EIGRP multicast)
Protocole	EIGRP (IP protocol 88)
Authentification	Champ Auth MD5 présent dans l'en-tête
Type de paquets	Hello (K-values) + Update (routes) + ACK
Hello interval	5 secondes (liens point-à-point)
Analyse	L'Update EIGRP transporte les vecteurs de distance avec métrique composite. L'ACK confirme la réception (protocole fiable RTP). L'authentification MD5 est visible.

No.	Time	Source	Destination	Protocol	Length	Info
477	685.461503	172.16.0.4	224.0.0.10	EIGRP	114	Hello
478	689.566178	172.16.0.5	224.0.0.10	EIGRP	114	Hello
479	690.253702	172.16.0.4	224.0.0.10	EIGRP	114	Hello
480	692.927970	ca:04:74:a4:00:54	ca:04:74:a4:00:54	LOOP	60	Reply
481	693.644990	ca:05:0b:34:00:00	ca:05:0b:34:00:00	LOOP	60	Reply
482	694.016755	172.16.0.5	224.0.0.10	EIGRP	114	Hello
483	695.228349	172.16.0.4	224.0.0.10	EIGRP	114	Hello
484	698.828642	172.16.0.5	224.0.0.10	EIGRP	114	Hello
485	698.844156	172.16.0.4	224.0.0.10	EIGRP	124	Hello
486	698.860158	172.16.0.4	172.16.0.5	EIGRP	94	Update
487	698.861155	172.16.0.5	224.0.0.10	EIGRP	124	Hello
488	698.875154	172.16.0.5	172.16.0.4	EIGRP	94	Update
489	698.891568	172.16.0.4	224.0.0.10	EIGRP	866	Update
490	698.906614	172.16.0.4	172.16.0.5	EIGRP	60	Hello (Ack)
491	698.923849	172.16.0.5	224.0.0.10	EIGRP	317	Update
492	698.938411	172.16.0.4	172.16.0.5	EIGRP	60	Hello (Ack)
493	698.955135	172.16.0.5	224.0.0.10	EIGRP	866	Update
494	698.969132	172.16.0.4	172.16.0.5	EIGRP	60	Hello (Ack)
495	699.047484	172.16.0.4	172.16.0.5	EIGRP	866	Update
496	699.063005	172.16.0.5	172.16.0.4	EIGRP	60	Hello (Ack)
497	699.079002	172.16.0.4	224.0.0.10	EIGRP	317	Update
498	699.096285	172.16.0.5	172.16.0.4	EIGRP	60	Hello (Ack)
499	702.923648	ca:04:74:a4:00:54	ca:04:74:a4:00:54	LOOP	60	Reply
500	703.858317	ca:05:0b:34:00:00	ca:05:0b:34:00:00	LOOP	60	Reply
501	703.968434	172.16.0.5	224.0.0.10	EIGRP	124	Hello
502	704.077749	172.16.0.4	224.0.0.10	EIGRP	124	Hello

## 7.4 Capture 3 — Échanges RIP v2

Paramètre	Valeur observée
Interface capturée	R3 F3/0 (192.168.40.0/24, vers RRIP)
IP Source	192.168.40.3 / 192.168.40.254 (RRIP)
IP Destination	224.0.0.9 (RIP v2 multicast)
Port UDP	520 (RIP)
Type de paquets	Request (1) + Response (2)
Contenu	Vecteurs de distances avec préfixes subnet (VLSM) et next-hop
Analyse	RIP envoie sa table de routage complète toutes les 30 secondes. L'absence d'acquittement le rend vulnérable aux pertes. Les routes redistribuées d'OSPF apparaissent avec métrique 5.

No.	Time	Source	Destination	Protocol	Length	Info
7	12.863699	192.168.40.3	224.0.0.9	RIPv2	346	Response
10	25.689891	192.168.40.254	224.0.0.9	RIPv2	66	Response
13	39.083091	192.168.40.3	224.0.0.9	RIPv2	346	Response
19	53.461717	192.168.40.254	224.0.0.9	RIPv2	66	Response
24	68.151484	192.168.40.3	224.0.0.9	RIPv2	346	Response
27	71.105480	192.168.40.3	224.0.0.9	RIPv2	66	Request
28	71.134480	192.168.40.254	192.168.40.3	RIPv2	66	Response
29	71.172482	192.168.40.3	224.0.0.9	RIPv2	66	Request
30	71.209484	192.168.40.254	192.168.40.3	RIPv2	66	Response
31	73.054480	192.168.40.3	224.0.0.9	RIPv2	346	Response
34	81.724483	192.168.40.254	224.0.0.9	RIPv2	66	Response

## 7.5 Capture 4 — Échange ARP

Paramètre	Valeur observée
LAN capturé	LAN Siège (192.168.10.0/24)
Type Ethernet	0x0806 (ARP)
ARP Request	Broadcast (FF:FF:FF:FF:FF:FF) : "Qui a 192.168.10.21 ?"
ARP Reply	Unicast SRV1 : "192.168.10.21 est à XX:XX:XX:XX:XX:XX"
Champs analysés	Hardware type, Protocol type, Sender/Target IP & MAC
Analyse	L'ARP est essentiel pour la résolution d'adresses au niveau 2. Il ne traverse pas les routeurs. Chaque routeur maintient son cache ARP par interface.

No.	Time	Source	Destination	Protocol	Length	Info
4	21.385845	ca:04:74:a4:00:38	Broadcast	ARP	60	Gratuitous ARP for 192.168.10.4 (Reply)
8	28.915838	ca:04:74:a4:00:38	Broadcast	ARP	60	Who has 192.168.10.21? Tell 192.168.10.4
15	33.918857	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.10.21 (Request)
16	34.915859	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.10.21 (Request)
17	35.928856	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.10.21 (Request)
21	67.087618	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.10.4? Tell 192.168.10.21
22	67.098646	ca:04:74:a4:00:38	Private_66:68:00	ARP	60	192.168.10.4 is at ca:04:74:a4:00:38

## 7.6 Capture 5 — Requête et Réponse DNS

Paramètre	Valeur observée
Port	UDP 53 (DNS)
Type	Query (Type A) + Response
TTL DNS	300 secondes (dans la réponse)
Flags	QR=0 (Query) / QR=1 (Response), AA, RA
Analyse	La requête DNS est envoyée vers 8.8.8.8 (Google DNS) via la route par défaut OSPF injectée par R1. La réponse contient l'enregistrement A (adresse IPv4).

No.	Time	Source	Destination	Protocol	Length	Info
22	86.349124	192.168.10.100	8.8.8.8	DNS	74	Standard query 0x0bc0 A www.google.com
24	86.506727	192.168.10.100	8.8.8.8	DNS	74	Standard query 0x0bc0 A www.google.com
26	86.674796	192.168.10.100	8.8.8.8	DNS	74	Standard query 0x0bc0 A www.google.com

## 7.7 Capture 6 — Connexion TCP (3-way Handshake) vers SRV1

Paramètre	Valeur observée
Source / Destination	10.0.0.2 (R2) -> 192.168.10.100 (SRV1)
Port destination	80 (HTTP)
Étape 1 - SYN	H1 envoie SYN, Seq=X, Flags=0x002
Étape 2 - SYN-ACK	SRV1 répond SYN-ACK, Seq=Y, Ack=X+1, Flags=0x012
Étape 3 - ACK	H1 confirme ACK, Seq=X+1, Ack=Y+1, Flags=0x010
TTL observé	64 (Linux) ou 128 (Windows) sur SRV1

Paramètre	Valeur observée
Analyse	Le 3-way handshake TCP établit la connexion fiable avant tout transfert HTTP. Les champs Seq/Ack assurent l'ordre et la fiabilité. Sur un même LAN le TTL n'est pas décrémenté.

No.	Time	Source	Destination	Protocol	Length	Info
2.48.975006	10.0.0.2	192.168.10.100	192.168.10.100	TCP	58	37599 → 80 [SYN] Seq=0 Win=4128 Len=0 MSS=536
3.48.994004	192.168.10.100	10.0.0.2	192.168.10.100	TCP	60	80 → 37599 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4.49.050002	10.0.0.2	192.168.10.100	192.168.10.100	TCP	54	37599 → 80 [ACK] Seq=1 Ack=1 Win=4128 Len=0
5.49.050002	10.0.0.2	192.168.10.100	192.168.10.100	TCP	54	[TCP Dup ACK 4#1] 37599 → 80 [ACK] Seq=1 Ack=1 Win=4128 Len=0

```

FROM LOADING TO FULL, LOADING DONE
R2#
R2#telnet 192.168.10.100 80
Trying 192.168.10.100, 80 ... Open

```

## 8. Politique de Sécurité — ACL et Authentification OSPF

### 8.1 Politique de Sécurité Définie

Cinq règles de sécurité sont implémentées. Le choix entre ACL standard et étendue dépend de la granularité requise : les ACL étendues permettent de filtrer par protocole et port, les ACL standard uniquement par adresse source.

### 8.2 Règle 1 — Accès Agences vers SRV1 (HTTP/HTTPS/DNS uniquement)

Type : ACL étendue (car filtre sur protocole ET adresse destination)

Placement : R4, interface f0/0 (entrée vers Zone 1), direction IN ou sur R2/R3 direction OUT vers Zone 1

Meilleure pratique : ACL étendue proche de la SOURCE -> sur R2 et R3

Choix : sur R4, interface 0/0 direction IN

```

R4(config)#
R4(config)#ip access-list extended AGENCES_VERS_SIEGE
R4(config-ext-nacl)# permit icmp 192.168.20.0 0.0.0.255 host 192.168.10.100
R4(config-ext-nacl)# permit icmp 192.168.30.0 0.0.0.255 host 192.168.10.100
R4(config-ext-nacl)#$ 192.168.20.0 0.0.0.255 host 192.168.10.100 eq 80
R4(config-ext-nacl)#$ 192.168.20.0 0.0.0.255 host 192.168.10.100 eq 443
R4(config-ext-nacl)#$ 192.168.20.0 0.0.0.255 host 192.168.10.100 eq 53
R4(config-ext-nacl)#$ 192.168.30.0 0.0.0.255 host 192.168.10.100 eq 80
R4(config-ext-nacl)#$ 192.168.30.0 0.0.0.255 host 192.168.10.100 eq 443
R4(config-ext-nacl)#$ 192.168.30.0 0.0.0.255 host 192.168.10.100 eq 53
R4(config-ext-nacl)# deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
R4(config-ext-nacl)# deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
R4(config-ext-nacl)# permit ip any any
R4(config-ext-nacl)#interface f0/0
R4(config-if)# ip access-group AGENCES_VERS_SIEGE in
R4(config-if)#end
R4#write memory
*Mar  5 23:38:37.167: %SYS-5-CONFIG_I: Configured from console by console
R4#write memory

```

Test :

```

H2> ping 192.168.10.100
84 bytes from 192.168.10.100 icmp_seq=1 ttl=62 time=117.793 ms
84 bytes from 192.168.10.100 icmp_seq=2 ttl=62 time=111.050 ms
84 bytes from 192.168.10.100 icmp_seq=3 ttl=62 time=112.429 ms
84 bytes from 192.168.10.100 icmp_seq=4 ttl=62 time=88.651 ms
84 bytes from 192.168.10.100 icmp_seq=5 ttl=62 time=96.680 ms

H2> ping 192.168.10.4
*10.0.0.4 icmp_seq=1 ttl=254 time=77.131 ms (ICMP type:3, code:13, Communication administratively prohi
bited)
*10.0.0.4 icmp_seq=2 ttl=254 time=52.634 ms (ICMP type:3, code:13, Communication administratively prohi
bited)
*10.0.0.4 icmp_seq=3 ttl=254 time=96.194 ms (ICMP type:3, code:13, Communication administratively prohi
bited)
*10.0.0.4 icmp_seq=4 ttl=254 time=56.098 ms (ICMP type:3, code:13, Communication administratively prohi
bited)
*10.0.0.4 icmp_seq=5 ttl=254 time=53.705 ms (ICMP type:3, code:13, Communication administratively prohi
bited)
H2>

```

## 8.3 Règle 2 — Blocage ICMP entrant depuis Internet

Type : ACL étendue (filtre protocole ICMP + source Internet)

Placement : R1, interface f1/0 (vers Internet), direction IN

```

R1(config)#ip access-list extended INTERNET_ENTRANT
R1(config-ext-nacl)#$r les rC)ponses aux pings lancC)s depuis l'intC)rieur
R1(config-ext-nacl)# permit icmp 203.0.113.0 0.0.0.3 any echo-reply
R1(config-ext-nacl)# ! Bloquer les pings entrants depuis Internet
R1(config-ext-nacl)# deny icmp 203.0.113.0 0.0.0.3 any echo
R1(config-ext-nacl)# ! Autoriser tout le reste
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)#
R1(config-ext-nacl)#interface f1/0
R1(config-if)# ip access-group INTERNET_ENTRANT in
R1(config-if)#
R1(config-if)#end

```

Test :

```
R-INTERNET#ping 203.0.113.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
R-INTERNET#
```

```
R1#ping 203.0.113.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/60/96 ms
R1#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/51/68 ms
R1#
```

## 8.4 Règle 3 — Isolation Saint-Louis / Ziguinchor

Type : ACL étendue (filtre source + destination)

Placement : R2, interface f2/0, direction IN (depuis Saint-Louis) et R3, interface f2/0, direction IN (depuis Ziguinchor)

```
R2(config)#
R2(config)#ip access-list extended SL_VERS_ZIGUINCHOR
R2(config-ext-nacl)# deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
R2(config-ext-nacl)# permit ip any any
R2(config-ext-nacl)#
R2(config-ext-nacl)#interface f2/0
R2(config-if)# ip access-group SL_VERS_ZIGUINCHOR in
R2(config-if)#
R2(config-if)#end
```

```
R3(config)#
R3(config)#ip access-list extended ZIGUINCHOR_VERS_SL
R3(config-ext-nacl)# deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
R3(config-ext-nacl)# permit ip any any
R3(config-ext-nacl)#
R3(config-ext-nacl)#interface f2/0
R3(config-if)# ip access-group ZIGUINCHOR_VERS_SL in
R3(config-if)#
R3(config-if)#end
```

Test :

```
H2> ping 192.168.30.100
*192.168.20.2 icmp_seq=1 ttl=255 time=55.038 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.20.2 icmp_seq=2 ttl=255 time=32.009 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.20.2 icmp_seq=3 ttl=255 time=47.995 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.20.2 icmp_seq=4 ttl=255 time=20.843 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.20.2 icmp_seq=5 ttl=255 time=5.478 ms (ICMP type:3, code:13, Communication administratively prohibited)

H2> ping 192.168.10.100
84 bytes from 192.168.10.100 icmp_seq=1 ttl=62 time=112.766 ms
84 bytes from 192.168.10.100 icmp_seq=2 ttl=62 time=125.243 ms
84 bytes from 192.168.10.100 icmp_seq=3 ttl=62 time=150.771 ms
84 bytes from 192.168.10.100 icmp_seq=4 ttl=62 time=95.190 ms
84 bytes from 192.168.10.100 icmp_seq=5 ttl=62 time=87.846 ms

H2>
```

```
H3> ping 192.168.20.11
*192.168.30.3 icmp_seq=1 ttl=255 time=60.394 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.30.3 icmp_seq=2 ttl=255 time=26.116 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.30.3 icmp_seq=3 ttl=255 time=15.466 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.30.3 icmp_seq=4 ttl=255 time=7.666 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.30.3 icmp_seq=5 ttl=255 time=35.342 ms (ICMP type:3, code:13, Communication administratively prohibited)

H3> █
```

## 8.5 Règle 4 — Blocage EIGRP → RIP

Type : ACL étendue

Placement : R4, interface f3/0 (vers EIGRP), direction IN ou sur R3, interface f3/0 (vers RIP), direction OUT

Choix : R4 f3/0 IN (bloquer à la source, proche du domaine EIGRP)

```
R4(config)#ip access-list extended EIGRP_VERS_RIP
R4(config-ext-nacl)# deny ip 172.16.0.0 0.0.255.255 192.168.40.0 0.0.0.255
R4(config-ext-nacl)# permit ip any any
R4(config-ext-nacl)#
R4(config-ext-nacl)#interface f3/0
R4(config-if)# ip access-group EIGRP_VERS_RIP in
R4(config-if)#
R4(config-if)#end
R4#write memory
```

Test :

```
R5#ping 192.168.40.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.3, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
R5#ping 192.168.40.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.254, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
R5#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/82/104 ms
R5#ping 192.168.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/61/68 ms
R5# █
```

```
R4#
R4#show ip access-lists EIGRP_VERS_RIP
Extended IP access list EIGRP_VERS_RIP
 10 deny ip 172.16.0.0 0.0.255.255 192.168.40.0 0.0.0.255 (10 matches)
 20 permit ip any any (58 matches)
R4# █
```

## 8.6 Règle 5 – Trafic interne OSPF

But : Autoriser tout autre trafic interne entre les sites OSPF

Type : ACL étendu, applique sur l'interface f0/0 de R1

```

R1(config)#
R1(config)#
R1(config)#ip access-list extended TRAFIC_INTERNE_OSPF
R1(config-ext-nacl)# permit ip 10.0.0.0 0.0.0.255 any
R1(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 any
R1(config-ext-nacl)# permit ip 192.168.20.0 0.0.0.255 any
R1(config-ext-nacl)# permit ip 192.168.30.0 0.0.0.255 any
R1(config-ext-nacl)# permit ip 192.168.40.0 0.0.0.255 any
R1(config-ext-nacl)# permit ip 1.0.0.0 0.0.0.255 any
R1(config-ext-nacl)# permit ip 2.0.0.0 0.0.0.255 any
R1(config-ext-nacl)# permit ip 3.0.0.0 0.0.0.255 any
R1(config-ext-nacl)# permit ip 4.0.0.0 0.0.0.255 any
R1(config-ext-nacl)#interface f0/0
R1(config-if)# ip access-group TRAFIC_INTERNE_OSPF in
R1(config-if)#
R1(config-if)#end
R1#write memory
*Mar 6 00:39:33.143: %SYS-5-CONFIG_I: Configured from console by console
R1#write memory

```

Test :

```

R1#show ip access-lists TRAFIC_INTERNE_OSPF
Extended IP access list TRAFIC_INTERNE_OSPF
 10 permit ip 10.0.0.0 0.0.0.255 any (158 matches)
 20 permit ip 192.168.10.0 0.0.0.255 any
 30 permit ip 192.168.20.0 0.0.0.255 any
 40 permit ip 192.168.30.0 0.0.0.255 any
 50 permit ip 192.168.40.0 0.0.0.255 any
 60 permit ip 1.0.0.0 0.0.0.255 any
 70 permit ip 2.0.0.0 0.0.0.255 any
 80 permit ip 3.0.0.0 0.0.0.255 any
 90 permit ip 4.0.0.0 0.0.0.255 any
R1#

```

## 8.7 Tableau de tests de sécurité

ACL	Test effectué	Interface	Résultat attendu	Résultat obtenu	Statut
ACL 1	H2 ping SRV1 (192.168.10.100)	R4 f0/0 IN	Autorisé	84 bytes TTL=62	✓ OK
ACL 1	H2 ping R4 (192.168.10.4)	R4 f0/0 IN	Bloqué	ICMP type 3 code 13	✓ OK
ACL 2	R-INTERNET ping R1	R1 f1/0 IN	Bloqué	Timeout	✓ OK
ACL 2	R1 ping R-INTERNET	R1 f1/0 IN	Autorisé	Success 100%	✓ OK
ACL 3	H2 ping H3 (Ziguinchor)	R2 f2/0 IN	Bloqué	Administratively prohibited	✓ OK
ACL 4	R5 ping 192.168.40.3	R4 f3/0 IN	Bloqué	Timeout	✓ OK
ACL 5	R1 ping 10.0.0.2	R1 f0/0 IN	Autorisé	Success 100% (158 matches)	✓ OK

## 9. Authentification OSPF

### 9.1 Authentification MD5 entre R1, R2 et R4

L'authentification MD5 est configurée sur les interfaces Zone 0 de R1, R2 et R4 pour sécuriser les échanges OSPF. Sans cette protection, un routeur malveillant pourrait injecter de fausses routes et perturber le réseau.

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#
R1(config)#interface f0/0
R1(config-if)# no ip ospf authentication
R1(config-if)# no ip ospf message-digest-key 1 md5 SmartechOSPF2025
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# ip ospf message-digest-key 1 md5 SmartechOSPF2025
R1(config-if)#end
R1#write memory
*Mar  6 00:58:08.907: %SYS-5-CONFIG_I: Configured from console by console

```

## 9.2 Authentification en texte clair entre R3 et R2

Le projet demande une authentification en texte clair entre R3 et R2. Cette méthode est moins sécurisée que MD5 car le mot de passe est visible en clair dans les paquets OSPF capturés avec Wireshark.

! ATTENTION : authentification en texte clair – mot de passe visible dans Wireshark  
! À des fins pédagogiques uniquement

```

R3(config)#
R3(config)#interface f0/0
R3(config-if)# ip ospf authentication ! Auth texte clair
R3(config-if)# authentication-key SmartechCLEAR ! CLC) visible en clair
% OSPF: Warning: The password/key will be truncated to 8 characters
R3(config-if)#

```

## 9.3 Vérification des adjacences après authentification

```

R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address        Interface
2.2.2.2          50    FULL/DROTHER    00:00:36   10.0.0.2       FastEthernet0/0
3.3.3.3          50    FULL/DROTHER    00:00:30   10.0.0.3       FastEthernet0/0
4.4.4.4          100   FULL/BDR        00:00:34   10.0.0.4       FastEthernet0/0
R1#

```

Routeur	Voisin	État	Rôle	Auth
R1	2.2.2.2 (R2)	FULL/DROTHER	DR	MD5 ✓
R1	3.3.3.3 (R3)	FULL/DR	DR	MD5 ✓
R1	4.4.4.4 (R4)	FULL/DROTHER	DR	MD5 ✓
R4	2.2.2.2 (R2)	FULL/DROTHER	BDR	MD5 ✓
R4	3.3.3.3 (R3)	FULL/BDR	BDR	MD5 ✓

# 9. Conclusion et Retour d'Expérience

## 9.1 Bilan du Projet

Ce projet a permis de concevoir et déployer une infrastructure réseau multi-sites complète pour Smartech SA, intégrant les trois principaux protocoles de routage (OSPF, EIGRP, RIP v2) avec

---

redistribution bidirectionnelle et sécurisation par ACL. L'architecture résultante assure la connectivité entre les sites Dakar, Saint-Louis et Ziguinchor, ainsi qu'avec le réseau partenaire EIGRP et le site legacy RIP.

## 9.2 Difficultés Rencontrées

---

- Élection DR/BDR : la priorité OSPF ne prend effet qu'après réinitialisation. Solution : clear ip ospf process en coordination avec une fenêtre de maintenance.
- Boucles de redistribution mutuelle OSPF↔EIGRP et OSPF↔RIP : résolu par l'usage de tags et route-maps asymétriques.
- Authentification EIGRP MD5 : la clé doit être identique sur les deux extrémités du lien, sinon l'adjacence ne s'établit pas.
- Seed metric EIGRP : sans metric valide dans la commande redistribute, les routes ne sont pas acceptées par EIGRP.

## 9.3 Apprentissages

---

- Maîtrise des mécanismes DR/BDR et de leur impact sur la convergence OSPF
- Compréhension de l'algorithme DUAL d'EIGRP et du concept de Feasible Successor
- Importance de la gestion des métriques et des filtres dans la redistribution inter-protocoles
- Analyse protocolaire détaillée avec Wireshark : maîtrise des en-têtes IP, TCP, UDP, OSPF
- Application pratique des ACL et leur positionnement stratégique sur les interfaces

## 9.4 Perspectives

---

Pour une évolution vers une architecture plus moderne, il serait pertinent d'envisager la migration vers OSPFv3 (support IPv6), le remplacement de RIP par OSPF ou BGP pour le site legacy, l'implémentation de VPN MPLS entre les sites, et l'adoption d'un système de surveillance réseau (Nagios, SNMP) pour la supervision en temps réel.

# 10. Annexes

## Annexe A — Commandes de Vérification Clés

---

Protocole	Commande	Information
OSPF	show ip ospf neighbor	Adjacences + rôles DR/BDR/DROTHER
OSPF	show ip ospf database	LSDB complète (Router, Network, Summary LSA)
OSPF	show ip ospf interface Gx/x	Détail interface : priorité, DR, BDR, timers
EIGRP	show ip eigrp neighbors	Voisins EIGRP + uptime
EIGRP	show ip eigrp topology	Table DUAL : successeurs et FS
EIGRP	show ip eigrp topology all-links	Tous les chemins (y compris non FS)
RIP	show ip rip database	Base de données RIP + métriques
Général	show ip route	Table de routage complète
Général	show ip route ospf	Routes apprises par OSPF

Protocole	Commande	Information
Général	show ip route eigrp	Routes apprises par EIGRP
ACL	show ip access-lists	Toutes les ACL + compteurs de correspondance
ACL	show ip interface Gx/x	ACL appliquées par interface
DHCP	show ip dhcp binding	Baux DHCP actifs
Général	debug ip routing	Débogage des changements de routes
OSPF	debug ip ospf adj	Débogage des adjacences OSPF

## Annexe B — Références RFC

- RFC 2328 — OSPF Version 2 (<https://www.rfc-editor.org/rfc/rfc2328>)
- RFC 2453 — RIP Version 2 (<https://www.rfc-editor.org/rfc/rfc2453>)
- RFC 7868 — EIGRP (<https://www.rfc-editor.org/rfc/rfc7868>)
- RFC 1812 — Requirements for IP Version 4 Routers

## Annexe C — Fichiers Inclus dans le Rendu

- rapport\_technique\_smartech.pdf — Ce rapport (20-30 pages)
- projet\_gns3.gns3 — Fichier projet GNS3 complet
- conf\_projet.txt — Dossier contenant les configurations .txt de R1 à R7 et RRIP, config du serveur DNS, config de l'internet simule
- captures-wireshark-projet — Dossier contenant les 6 fichiers .pcap annotés ainsi que les captures des ACLs.

*Rapport réalisé dans le cadre du module Technologies de l'Internet*

**Dr K. GUEYE — DUT2TR — 2025-2026**