Projet HSRP – Phase 1 : étude de la résilience Internet

Maxime / Souhir - RIOCA

1. Étude du problème

Dans l'infrastructure actuelle, tout le trafic Internet (sortie du LAN, accès aux serveurs web de la DMZ) passe par **un seul routeur, RNET1**, relié à un seul FAI. Si RNET1 tombe, ou si son lien vers le FAI est coupé, l'entreprise perd tout accès à Internet et les serveurs de la DMZ deviennent injoignables depuis l'extérieur. Il s'agit d'un point de défaillance unique (SPOF, *Single Point of Failure*).

Objectif : assurer la continuité de service d'Internet en ajoutant un second routeur (RNET2) et un protocole de redondance de passerelle (HSRP). Si RNET1 tombe, RNET2 prend le relais automatiquement, sans intervention manuelle.

2. Recensement des pannes possibles

Élément	Panne possible	Conséquence actuelle	Couverte par HSRP ?
RNET1	Panne matérielle, plantage, coupure d'alimentation	Plus d'Internet	Oui
Lien RNET1 → FAI	Câble débranché, panne côté FAI	Plus d'Internet	Oui, avec suivi de l'interface (maquette) ou `track` + IP SLA
Lien RNET1 ↔ SwNET	Câble ou port défaillant	Plus d'Internet	Oui
SwNET	Panne du switch	Plus d'Internet	Non, hors périmètre
Pare-feu Zyxel	Panne	Plus d'accès WAN	Non, hors périmètre
FAI	Panne générale	Plus d'Internet	Non, il faudrait un second FAI

Les deux dernières lignes (SwNET, Zyxel) ainsi que la panne générale du FAI sont assumées comme hors périmètre du projet (coût et limites du sujet).

3. Moyens matériels à mettre en place

- 1 routeur Cisco 2911 (RNET2), identique à RNET1
- 1 port du switch SwNET à ouvrir dans le VLAN 92 pour RNET2 (les ports non utilisés sont en shutdown)
- 1 second lien vers le FAI (une autre prise de la salle 20 pour la zone Internet = Campus)
- Câblage Ethernet
- Côté logiciel : HSRP, IP SLA et `track`, inclus dans l'IOS sans licence supplémentaire à prévoir

- 2 adresses IP supplémentaires dans le 192.168.3.248/29 : une pour RNET2 et une pour l'IP virtuelle HSRP

4. Impact sur l'infrastructure existante

- **Zyxel :** sa route par défaut doit pointer vers l'IP virtuelle HSRP au lieu de l'IP de RNET1.
- **Adressage :** le /29 de la zone Internet suffit : après ajout de RNET2 et de l'IP virtuelle, il reste une seule adresse libre (192.168.3.252). Rien n'est prévu d'autre dans ce réseau ; en cas d'ajout, il faudrait passer en /28.
- **SwNET :** ajout d'un port dans le VLAN 92.
- **NAT :** le NAT statique (serveurs web de la DMZ) et le PAT doivent être reproduits à l'identique sur RNET2.
- **Sécurité :** les règles du Zyxel filtrent par zone et par objet, donc presque aucune ne change. Seule la règle Allow_TFTP_Backups est à adapter : ajouter l'IP de RNET2 au groupe EQUIP_BACKUP, sinon la sauvegarde TFTP de RNET2 sera bloquée. Le trafic HSRP reste dans le VLAN 92 et ne traverse pas le pare-feu.
- **Aucun impact** sur le LAN, la DMZ et les VLAN, ce qui limite les risques de la mise en production.

5. Maquette Packet Tracer

La maquette isole la zone Internet : un PC du LAN (Laptop0, 172.19.10.1) traverse Rparefeu, SWNET, puis l'un des deux routeurs RNET pour atteindre un routeur « FAI » qui porte la loopback 8.8.8.8. Réseau HSRP : 192.168.3.248/29, IP virtuelle 192.168.3.249.

Équipement	Interface	Adresse	Rôle
Laptop0		172.19.10.1/24, passerelle 172.19.10.254	PC de test du LAN
Rparefeu	Gi0/1	172.19.10.254/24	Passerelle du LAN de test
Rparefeu	Gi0/0	192.168.3.253/29	Côté zone Internet
SWNET	VLAN 92	192.168.3.254/29	Switch de la zone Internet
RNET1	Gi0/0	192.168.3.251/29	Routeur actif (priorité 105)
RNET2	Gi0/0	192.168.3.250/29	Routeur de secours (priorité 100)
HSRP		192.168.3.249	IP virtuelle, passerelle du Zyxel
RNET1	Gi0/1	192.168.4.31/24	Lien vers FAI0

Équipement	Interface	Adresse	Rôle
FAI0	Gi0/0	192.168.4.254/24	FAI simulé n°1, loopback 8.8.8.8
RNET2	Gi0/1	172.18.53.2/16	Lien vers FAI1
FAI1	Gi0/0	172.18.255.254/16	FAI simulé n°2, loopback 8.8.8.8

Les deux FAI portent la même loopback 8.8.8.8 : Internet reste joignable quel que soit le RNET actif. Il reste une seule adresse libre dans le /29 (192.168.3.252).

6. Document de configuration

Ces commandes sont celles appliquées sur la maquette. Dans Packet Tracer, `ip sla` et `standby track <n> decrement` ne sont pas acceptés : le suivi du lien FAI se fait avec `standby 1 track GigabitEthernet0/1`, au décrément fixe de 10. D'où la priorité de RNET1 à 105 : elle tombe à 95, sous les 100 de RNET2.

SWNET

```
enable
configure terminal
hostname SWNET
vlan 92
 name INTERNET
exit
interface range fa0/1-3
 switchport mode access
 switchport access vlan 92
 no shutdown
exit
interface range fa0/4-24
 shutdown
exit
interface vlan 92
 ip address 192.168.3.254 255.255.255.248
 no shutdown
exit
ip default-gateway 192.168.3.249
end
write memory
```

Rparefeu

```
enable
configure terminal
hostname Rparefeu
interface Gi0/0
 ip address 192.168.3.253 255.255.255.248
 no shutdown
exit
interface Gi0/1
```

```
 ip address 172.19.10.254 255.255.255.0
 no shutdown
exit
ip route 0.0.0.0 0.0.0.0 192.168.3.249
router rip
 version 2
 no auto-summary
 network 192.168.3.0
 network 172.19.0.0
 passive-interface Gi0/1
 default-information originate
exit
end
write memory
```

La route par défaut vise l'IP virtuelle HSRP, jamais un RNET en particulier.

RNET1 (actif, priorité 105)

```
enable
configure terminal
hostname RNET1
interface Gi0/0
 ip address 192.168.3.251 255.255.255.248
 ip nat inside
 standby 1 ip 192.168.3.249
 standby 1 priority 105
 standby 1 preempt
 standby 1 timers 1 3
 standby 1 track GigabitEthernet0/1
 no shutdown
exit
interface Gi0/1
 ip address 192.168.4.31 255.255.255.0
 ip nat outside
 no shutdown
exit
ip route 0.0.0.0 0.0.0.0 192.168.4.254
router rip
 version 2
 no auto-summary
 network 192.168.3.0
 passive-interface Gi0/1
exit
access-list 1 permit 172.19.0.0 0.0.255.255
access-list 1 permit 10.3.10.0 0.0.0.255
ip nat inside source list 1 interface Gi0/1 overload
end
write memory
```

RNET2 (secours, priorité 100)

```
enable
configure terminal
hostname RNET2
interface Gi0/0
```

```
 ip address 192.168.3.250 255.255.255.248
 ip nat inside
 standby 1 ip 192.168.3.249
 standby 1 priority 100
 standby 1 preempt
 standby 1 timers 1 3
 standby 1 track GigabitEthernet0/1
 no shutdown
exit
interface Gi0/1
 ip address 172.18.53.2 255.255.0.0
 ip nat outside
 no shutdown
exit
ip route 0.0.0.0 0.0.0.0 172.18.255.254
router rip
 version 2
 no auto-summary
 network 192.168.3.0
 passive-interface Gi0/1
exit
access-list 1 permit 172.19.0.0 0.0.255.255
access-list 1 permit 10.3.10.0 0.0.0.255
ip nat inside source list 1 interface Gi0/1 overload
end
write memory
```

FAI0 et FAI1 (simulation des fournisseurs d'accès)

```
! FAI0
hostname FAI0
interface Gi0/0
 ip address 192.168.4.254 255.255.255.0
 no shutdown
interface Loopback0
 ip address 8.8.8.8 255.255.255.255

! FAI1
hostname FAI1
interface Gi0/0
 ip address 172.18.255.254 255.255.0.0
 no shutdown
interface Loopback0
 ip address 8.8.8.8 255.255.255.255
```

Aucune route retour n'est nécessaire sur les FAI : le PAT des RNET ne leur montre que 192.168.4.31 et 172.18.53.2, directement connectés.

7. Rapport de tests

La bascule du lien FAI fonctionne : après la coupure de Gi0/1 sur RNET1, RNET2 devient actif et Laptop0 garde l'accès à 8.8.8.8 avec une seule perte de paquet. Les quatre scénarios sont validés, y compris la panne complète de RNET1.

Scénario	Action	Résultat attendu	Résultat obtenu	Statut
1. Fonctionnement normal	`show standby` sur RNET1 ; `ping` et `tracert 8.8.8.8` depuis Laptop0	RNET1 Active (105), RNET2 Standby ; trafic via 192.168.3.251	RNET1 Active, priorité 105, VIP 192.168.3.249, suivi de Gi0/1 « Up », décrément 10, standby 192.168.3.250. Tracert : 172.19.10.254, 192.168.3.251, 8.8.8.8. Ping : 3 réponses sur 4 (premier paquet perdu, résolution ARP)	Validé
2. Panne du lien FAI de RNET1	`shutdown` sur Gi0/1 de RNET1, puis `show standby brief` et `tracert 8.8.8.8`	Priorité de RNET1 à 95, RNET2 devient Active, accès Internet conservé	RNET1 passe à 95 puis en Standby ; RNET2 passe Active (priorité 100, standby 192.168.3.251). Tracert : 172.19.10.254, 192.168.3.250, 8.8.8.8. Ping : 3 réponses sur 4 (1 paquet perdu pendant la bascule)	Validé
3. Retour du lien FAI de RNET1	`no shutdown` sur Gi0/1 de RNET1, puis `show standby brief`	RNET1 reprend le rôle Active (`preempt`)	Liaisons RNET1-FAI0 de nouveau up. RNET1 repasse de Standby à Active (priorité 105, standby 192.168.3.250) grâce à preempt, constaté avec `show standby brief`	Validé

Scénario	Action	Résultat attendu	Résultat obtenu	Statut
4. Panne complète de RNET1	`shutdown` sur Gi0/0 de RNET1 (ou extinction), puis `tracert 8.8.8.8`	RNET2 devient Active en quelques secondes	Gi0/0 de RNET1 passe de Active à Init. RNET2 devient Active (priorité 100, standby « unknown » car RNET1 est coupé). Tracert : 172.19.10.254, 192.168.3.250, 8.8.8.8. Ping continu : 2 paquets perdus (le premier, ARP, et un pendant la bascule). Au retour de Gi0/0, RNET1 repasse Speak, Standby puis Active (105)	Validé

Captures à joindre au rapport : `show standby` de RNET1 avant et après la coupure, `ping` et `tracert` de Laptop0 dans les deux états, et la topologie avec le lien RNET1-FAI0 en rouge puis en vert.

8. Limites et améliorations pour la production

La solution couvre la panne d'un routeur RNET et la coupure du lien physique vers le FAI ; le reste du dispositif garde des points de défaillance uniques.

- **Suivi du lien FAI :** la maquette surveille l'état de l'interface Gi0/1, pas la connectivité jusqu'au FAI. Sur du matériel réel, un suivi par IP SLA (ping du FAI) avec `track` détecterait aussi une panne en amont alors que le lien reste actif.
- **Sessions :** après une bascule, les connexions déjà établies sont coupées, car la table NAT n'est pas partagée entre RNET1 et RNET2.
- **Adresse publique :** les deux RNET sortent par des réseaux différents. Les serveurs web de la DMZ (NAT statique) ne seront donc pas joignables par la même adresse après bascule.
- **Points non redondés :** SWNET, le Zyxel et le FAI lui-même restent des points de défaillance uniques.
- **Adressage :** le /29 est utilisé à 5 adresses sur 6 ; un équipement supplémentaire dans ce réseau imposerait de passer en /28.
- **Mise en production :** appliquer la même configuration sur les vrais équipements, ajouter l'IP de RNET2 au groupe `EQUIP_BACKUP` du Zyxel pour la sauvegarde TFTP, et pointer la route par défaut du Zyxel vers l'IP virtuelle 192.168.3.249.