Colombelle Malone
Bardet Arthur
BTS SIO 2

Document de validation de compétences

HSRP

15/10/2026

Equipe4

1. Présentation du contexte d'entreprise

Nous avons notre entreprise soit PRESBOIS , qui avait un routeur en 192.168 connecté au LAB , problème étant nous sommes globalement isolé du réseau externe et s'il y a une panne nos utilisateurs n'auront plus de réseau ce qui peut être problématique, donc nous allons rajouter 1 routeur qui sera sur une autre connexion internet soit en 172.18 ce qui permettra de faire une redondance en cas de problème et s'assurer aussi que nous pouvons contacter notre infrastructure depuis l'extérieur.

2. Objectifs attendus

Installation d'un nouveau routeur et configuration de celui-ci afin d'assurer une redondance et configuration aussi du routeur 1 afin qu'il puisse s'en assurer nous vérifierons notre travail avec un tracert / ping vers 8.8.8.8.

3. Plan de travail

Première Phase :

- Etude du Problème
    - Recensement pannes possibles
    - Moyens Matériels à mettre en place
    - Impact sur l'infra existante

- Application sur un Cisco Packet Tracer

Deuxième phase :

- Application dans la réalité.

4. Réalisation

Première Phase :

Recensement Pannes Possibles :

Premier Panne : Surcharge du Routeur
Deuxième Panne Possible : Coupure de l'alimentation du Routeur
Troisième Panne Possible : Port Ethernet physique endommagé
Quatrième Panne Possible : Suppression de la configuration lors d'un redémarrage
Cinquième Panne Possible : Problème chez le fournisseur.

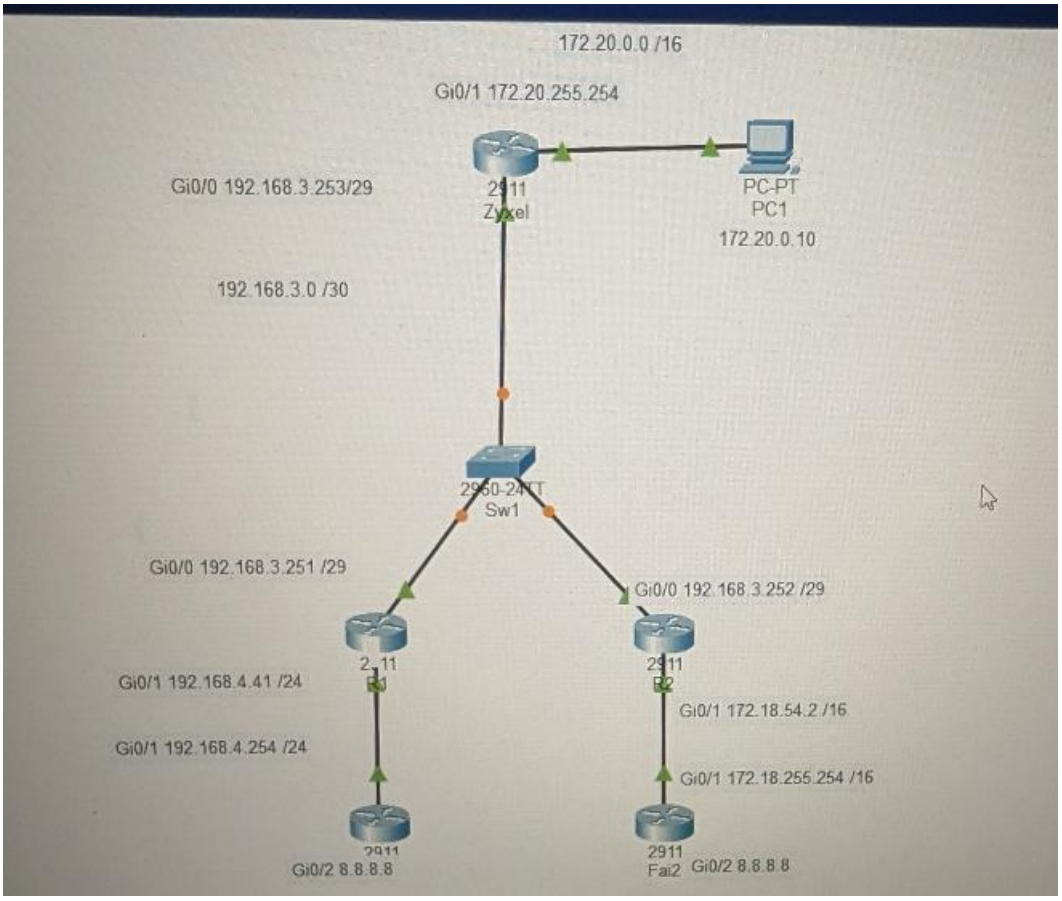
Moyens Matériels à mettre en place :

Equipement : Routeur
câble : deux câble RJ45

Impact sur l'infra existante :

- Modification de l'adressage IP (Passerelle Virtuelle HSRP)
- Utilisations d'un port en plus sur le switch

Application Sur Cisco Packet Tracer Soit voici le schéma et adresse IP Choisi :



Voici toute notre Infrastructure. Ensuite nous allons donc appliquer cela dans le réel premièrement nous allons retourner sur le Routeur numéro 1 et nous allons y mettre ces configurations :

Pour les Ports :

```
interface GigabitEthernet0/0
 ip address 192.168.3.251 255.255.255.248
 ip nat inside
 ip virtual-reassembly in
 standby 1 ip 192.168.3.249
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 1 decrement 20
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.4.41 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
```

Pour l'interface GI0/0 qui représente l'intérieur donc vers l'infrastructure

ip virtual-reassembly in : Active le réassemblage virtuel des paquets IP fragmentés arrivant sur cette interface, souvent utilisé conjointement avec le NAT ou le pare-feu

standby 1 ip 192.168.3.249 : Configure le protocole **HSRP** (Hot Standby Router Protocol) sous le groupe 1. L'adresse IP 192.168.3.249 est l'adresse IP virtuelle partagée par les routeurs de secours pour les clients du réseau.

standby 1 priority 110 : Définit la priorité HSRP de ce routeur à 110 (la valeur par défaut étant 100). Une priorité plus élevée augmente les chances que ce routeur devienne le routeur actif (« Active Router »).

standby 1 preempt : Permet à ce routeur de reprendre automatiquement son rôle de routeur actif s'il redevient plus prioritaire qu'un autre routeur (par exemple, après une panne).

standby 1 track 1 decrement 20 : Permet de surveiller (track) un objet ou une interface (numéro 1). Si la liaison surveillée tombe en panne, la priorité du routeur diminue de 20 (passant ici de 110 à 90), ce qui permet à un autre routeur de prendre le relais.

Pour l'interface GI0/1 :

ip virtual-reassembly in : Active également le réassemblage virtuel des paquets IP sur cette interface externe.

Ensuite nous allons prendre le Routeur 2 soit le Routeur que nous venons d'installer et nous allons y mettre ces configurations :

```
interface GigabitEthernet0/0
 ip address 192.168.3.250 255.255.255.248
 ip nat inside
 ip virtual-reassembly in
 standby 1 ip 192.168.3.249
 standby 1 timers 1 3
 standby 1 preempt
 standby 1 track 1 decrement 10
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.18.54.2 255.255.0.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
```

```
ip nat pool AP 172.18.4.40 172.18.4.41 netmask 255.255.0.0
ip nat inside source list NAT_ACL pool AP overload
ip nat inside source static 10.41.10.11 172.18.54.46
ip route 0.0.0.0 0.0.0.0 172.18.255.254
!
ip access-list standard NAT_ACL
 permit 172.16.0.0
 permit 172.20.0.0 0.0.255.255
 permit 10.4.0.0 0.0.255.255
 permit 192.168.0.0 0.0.255.255
 permit 10.42.0.0 0.0.255.255
 permit 10.41.0.0 0.0.255.255
 permit 172.0.0.0 0.255.255.255
 permit 192.168.3.0 0.0.0.255
```

Dans ce routeur étant donné qu'il vient d'être pris nous allons faire le nat dynamique et nat statique en ajoutant les permissions possibles pour les réseau choisis soit nous lui avons donné un pool de 172.18.4.40 à 172.18.4.41 en overload et un nat statique pour le serveur WEB afin qu'on puisse y accéder. Et donc toutes les ACL permettant d'autoriser tous les réseaux à pouvoir avoir Internet.

Pour l'interface GI0/1 je vais mettre seulement ce qui y a de plus que le routeur 1 :

standby 1 timers 1 3 : Modifie les minuteurs HSRP. Le temps de message "hello" est réglé à 1 seconde et le temps de "hold" (délai avant de déclarer le routeur mort) à 3 secondes (les valeurs par défaut étant respectivement de 3 et 10 secondes), ce qui permet une bascule plus rapide en cas de panne.

standby 1 track 1 decrement 10 : Surveille l'objet/interface 1. Si la liaison surveillée tombe en panne, la priorité de ce routeur diminue de 10 points pour laisser la main à un autre routeur de secours.

Pour l'interface GI0/0 rien de nouveau.

Et pour terminer sur les deux routeurs nous allons mettre ces commandes :

configure terminal
ip sla 1 icmp-echo 8.8.8.8
frequency 5
ip sla schedule 1 life forever start-time now

Puis

track 10 ip sla 1 reachability

soit :

```
!
track 10 ip sla 1 reachability
!
```

```
ip sla 1
 icmp-echo 8.8.8.8
 frequency 5
ip sla schedule 1 life forever start-time now
```

Après cela nous allons pouvoir Tester la connexion , nous allons essayer premièrement normalement , le tracert vers 8.8.8.8 donne ceci :

```
C:\Users\gamin>tracert 8.8.8.8

Détermination de l'itinéraire vers dns.google [8.8.8.8]
avec un maximum de 30 sauts :

  1     1 ms     1 ms     1 ms  172.20.60.254
  2    <1 ms    <1 ms    <1 ms  172.20.90.253
  3    <1 ms    <1 ms    <1 ms  192.168.3.251
  4     1 ms     1 ms    <1 ms  192.168.4.254
  5     4 ms     2 ms     2 ms  192.168.3.254
  6     5 ms     3 ms     3 ms  80.10.252.253
  7    12 ms     6 ms     7 ms
```

Lorsque désormais nous mettons une interface en down :

```
C:\Users\gamin>tracert 8.8.8.8

Détermination de l'itinéraire vers dns.google [8.8.8.8]
avec un maximum de 30 sauts :

  1     1 ms     1 ms     1 ms  172.20.60.254
  2    <1 ms    <1 ms    <1 ms  172.20.90.253
  3    <1 ms    <1 ms    <1 ms  192.168.3.250
  4     1 ms    <1 ms    <1 ms  172.18.255.254
  5     2 ms     1 ms     1 ms  192.168.3.254
  6     2 ms     2 ms     2 ms  80.10.252.253
```

Et lorsque nous coupons le réseau directement :

```
C:\Users\gamin>tracert 8.8.8.8

Détermination de l'itinéraire vers dns.google [8.8.8.8]
avec un maximum de 30 sauts :

  1     5 ms     5 ms     5 ms  172.18.255.254
  2     5 ms     5 ms     5 ms  192.168.3.254
  3     6 ms     9 ms     5 ms  80.10.252.253
```

Donc la redondance marche , pour vérifier vous pouvez utiliser des commandes sur le routeur 2 comme : show standby brief pour regarder la liaison.