DIRECTION DES SYSTÈMES D'INFORMATION

Pôle Infrastructures & Sécurité

Projet Bidouille : Architecture Réseau Sécurisée

Livrables - Topologie et Plan d'adressage

Objet : Segmentation VLAN et Sécurisation par ACLs

Auteur : Damien POLINSKY
Date : 13 mars 2026

Table des matières

1 SCHÉMA D'ARCHITECTURE RÉSEAU

Voici la topologie physique du réseau de l'entreprise Bidouille. L'architecture repose sur un modèle hiérarchique intégrant une redondance au niveau du cœur de réseau (commutateurs et routeurs) et une segmentation stricte par VLANs.

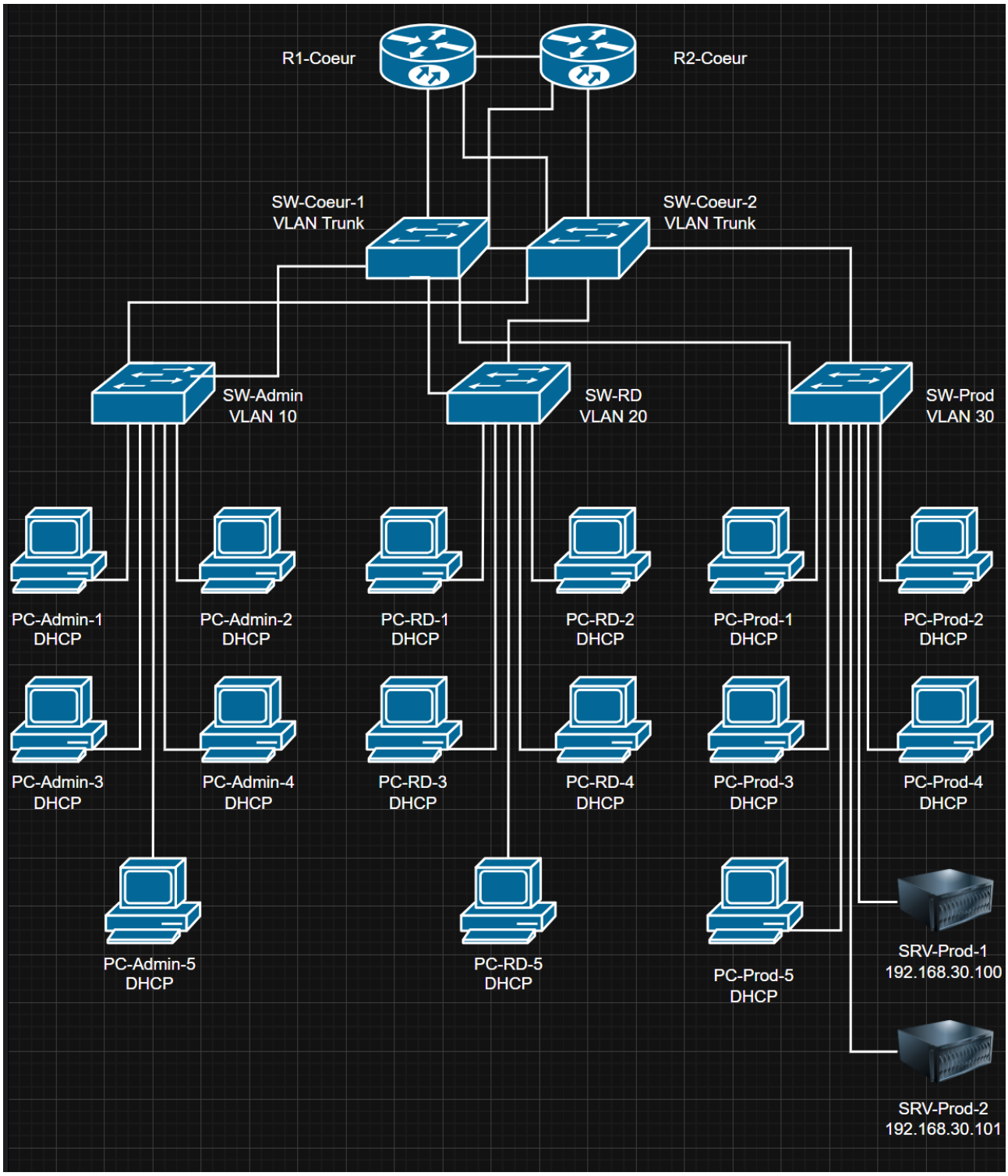

FIGURE 1 – Topologie physique et logique du réseau

2 PLAN D'ADRESSAGE

2.1 Cœur de Réseau (Routage Inter-VLAN)

La passerelle par défaut pour tous les VLANs est assurée par une adresse virtuelle partagée entre les deux routeurs (via le protocole de haute disponibilité HSRP).

Équipement	Interface	VLAN	Adresse IP	Masque
R1-Coeur (Principal)	Sous-int 10	**10**	192.168.10.2	255.255.255.0
R1-Coeur (Principal)	Sous-int 20	**20**	192.168.20.2	255.255.255.0
R1-Coeur (Principal)	Sous-int 30	**30**	192.168.30.2	255.255.255.0
R2-Coeur (Secours)	Sous-int 10	**10**	192.168.10.3	255.255.255.0
R2-Coeur (Secours)	Sous-int 20	**20**	192.168.20.3	255.255.255.0
R2-Coeur (Secours)	Sous-int 30	**30**	192.168.30.3	255.255.255.0

2.2 Équipements d'Accès (PC et Serveurs)

Les postes utilisateurs sont configurés en DHCP. Les serveurs industriels de la Production disposent d'adresses statiques pour garantir l'accessibilité continue des services (HTTPS).

Zone	Équipement	VLAN	Adresse IP	Passerelle
Administration	PC-Admin-1 à 5	**10**	DHCP (.20 à .99)	192.168.10.1 *(Virtuelle)*
R&D	PC-RD-1 à 5	**20**	DHCP (.20 à .99)	192.168.20.1 *(Virtuelle)*
Production	PC-Prod-1 à 5	**30**	DHCP (.20 à .99)	192.168.30.1 *(Virtuelle)*
Production	SRV-Prod-1	**30**	192.168.30.100	192.168.30.1 *(Virtuelle)*
Production	SRV-Prod-2	**30**	192.168.30.101	192.168.30.1 *(Virtuelle)*

3 IMPLÉMENTATION DANS PACKET TRACER

La maquette a ensuite été reproduite dans le simulateur Cisco Packet Tracer afin de valider l'architecture et les règles de sécurité. Afin d'alléger la simulation tout en conservant la logique complète du réseau, la liberté a été prise de ne représenter qu'un seul poste client par zone. La configuration étant rigoureusement identique pour les cinq postes de chaque service, cette approche n'impacte en rien la validité des tests.

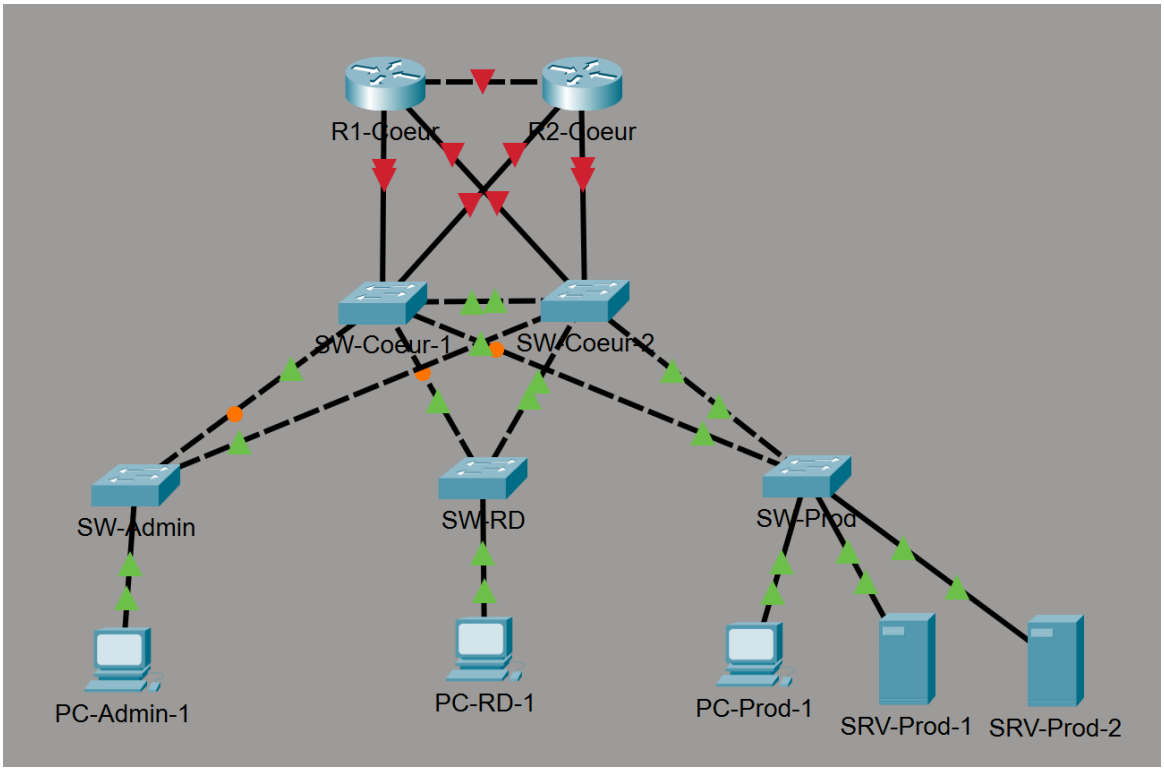

FIGURE 2 – Topologie physique sous Cisco Packet Tracer

3.1 Tableau de Câblage Réseau

Le tableau ci-dessous recense l'intégralité des connexions physiques réalisées entre les équipements.

Équipement Source	Port Source	Type de Câble	Équipement Dest.	Port Dest.
R1-Coeur	Gig0/0	Droit	**SW-Coeur-1**	Gig0/1
R1-Coeur	Gig0/1	Droit	**SW-Coeur-2**	Gig0/1
R2-Coeur	Gig0/0	Droit	**SW-Coeur-1**	Gig0/2
R2-Coeur	Gig0/1	Droit	**SW-Coeur-2**	Gig0/2
R1-Coeur	Gig0/2	Croisé	**R2-Coeur**	Gig0/2
SW-Coeur-1	Fa0/24	Croisé	**SW-Coeur-2**	Fa0/24
SW-Coeur-1	Fa0/1	Croisé	**SW-Admin**	Fa0/24
SW-Coeur-1	Fa0/2	Croisé	**SW-RD**	Fa0/24
SW-Coeur-1	Fa0/3	Croisé	**SW-Prod**	Fa0/24
SW-Coeur-2	Fa0/1	Croisé	**SW-Admin**	Fa0/23
SW-Coeur-2	Fa0/2	Croisé	**SW-RD**	Fa0/23

Équipement Source	Port Source	Type de Câble	Équipement Dest.	Port Dest.
SW-Coeur-2	Fa0/3	Croisé	**SW-Prod**	Fa0/23
SW-Admin	Fa0/1	Droit	**PC-Admin-1**	FastEthernet0
SW-RD	Fa0/1	Droit	**PC-RD-1**	FastEthernet0
SW-Prod	Fa0/1	Droit	**PC-Prod-1**	FastEthernet0
SW-Prod	Fa0/10	Droit	**SRV-Prod-1**	FastEthernet0
SW-Prod	Fa0/11	Droit	**SRV-Prod-2**	FastEthernet0

4 CONFIGURATION DES ÉQUIPEMENTS

4.1 Configuration Initiale et Création des VLANs

La configuration de base (nommage et création des VLANs) est identique pour les cinq commutateurs de l'architecture. Seul l'identifiant de l'équipement (`hostname`) diffère pour chaque unité.

Les commandes suivantes ont été appliquées sur **SW-Coeur-1**, **SW-Coeur-2**, **SW-Admin**, **SW-RD** et **SW-Prod**.

Afin de valider la bonne création des interfaces virtuelles, la commande `show vlan brief` est utilisée. Elle permet de confirmer que les VLANs sont actifs et correctement nommés dans la base de données du commutateur.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-Coeur-2
SW-Coeur-2(config)#vlan 10
SW-Coeur-2(config-vlan)#name Administration
SW-Coeur-2(config-vlan)#vlan 20
SW-Coeur-2(config-vlan)#name RD
SW-Coeur-2(config-vlan)#vlan 30
SW-Coeur-2(config-vlan)#name Production
SW-Coeur-2(config-vlan)#exit
SW-Coeur-2(config)#exit
SW-Coeur-2#
%SYS-5-CONFIG_I: Configured from console by console

SW-Coeur-2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Administration                   active
20   RD                               active
30   Production                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-Coeur-2#
```

FIGURE 3 – Vérification de la création des VLANs et de l'état du switch (SW-Coeur-2)

Point de contrôle

L'image ci-dessus confirme que les VLANs 10, 20 et 30 sont bien enregistrés avec le statut *active*. Cette vérification garantit que la base de données des VLANs est correctement synchronisée avant de passer au câblage logique.

4.2 Affectation des ports d'accès

Une fois les VLANs créés, il est nécessaire d'affecter chaque port physique du commutateur à son réseau logique respectif (Mode *Access*). Cette étape garantit que chaque terminal (PC ou Serveur) communique uniquement dans son périmètre de sécurité.

4.2.1 Configuration des zones Administration et R&D

Pour chaque zone, un port physique est dédié à un poste de travail unique. Dans un déploiement complet comprenant 5 postes par service, la configuration serait appliquée sur une plage de ports (par exemple `Fa0/1` à `Fa0/5`) via la commande `interface range`.

Dans le cadre de cette maquette, nous avons configuré le premier port de chaque switch d'accès :

```
SW-Admin#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-Admin(config)#interface FastEthernet0/1
SW-Admin(config-if)# switchport mode access
SW-Admin(config-if)# switchport access vlan 10
SW-Admin(config-if)#exit
SW-Admin(config)#
```

(a) Configuration VLAN 10 sur SW-Admin

```
SW-RD#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-RD(config)#interface FastEthernet0/1
SW-RD(config-if)# switchport mode access
SW-RD(config-if)# switchport access vlan 20
SW-RD(config-if)#exit
SW-RD(config)#
```

(b) Configuration VLAN 20 sur SW-RD

FIGURE 4 – Affectation des ports individuels en mode accès

4.2.2 Configuration de la zone Production

Pour le commutateur **SW-Prod**, nous avons configuré le port du poste de travail ainsi qu'une plage de ports (*interface range*) pour les deux serveurs industriels.

```
SW-Prod#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-Prod(config)#interface FastEthernet0/1
SW-Prod(config-if)# switchport mode access
SW-Prod(config-if)# switchport access vlan 30
SW-Prod(config-if)#exit
SW-Prod(config)#interface range FastEthernet0/10 - 11
SW-Prod(config-if-range)# switchport mode access
SW-Prod(config-if-range)# switchport access vlan 30
SW-Prod(config-if-range)#exit
SW-Prod(config)#
```

FIGURE 5 – Configuration du VLAN 30 pour le PC et les serveurs sur SW-Prod

4.3 Vérification de l'affectation des ports

La commande `show vlan brief` sur le commutateur de production permet de confirmer que les ports *Fa0/1*, *Fa0/10* et *Fa0/11* sont désormais isolés au sein du VLAN 30.

```
SW-Prod#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   Administration                   active
20   RD                               active
30   Production                       active    Fa0/1, Fa0/10, Fa0/11
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-Prod#
```

FIGURE 6 – Preuve d'affectation des ports physiques au VLAN 30

5 CONFIGURATION DU BACKBONE ET HAUTE DISPONIBILITÉ

5.1 Agrégation de liens (Trunking) et Spanning-Tree

Afin de permettre la circulation des flux de tous les VLANs entre les équipements et garantir une topologie sans boucle, nous avons configuré les liens d'interconnexion en mode *Trunk*. Parallèlement, le protocole **Spanning-Tree (STP)** a été paramétré pour désigner **SW-Coeur-1** comme commutateur racine (Root Bridge).

```
SW-Coeur-1>enable
SW-Coeur-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-Coeur-1(config)#spanning-tree vlan 10,20,30 priority 4096
SW-Coeur-1(config)#interface range f0/1 - 3, f0/24, g0/1 - 2
SW-Coeur-1(config-if-range)# switchport mode trunk



SW-Coeur-1(config-if-range)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up
```

(a) Priorité STP 4096 sur SW-Coeur-1

```
SW-Coeur-2>enable
SW-Coeur-2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-Coeur-2(config)#spanning-tree vlan 10,20,30 priority 8192
SW-Coeur-2(config)#interface range f0/1 - 3, f0/24, g0/1 - 2
SW-Coeur-2(config-if-range)# switchport mode trunk



SW-Coeur-2(config-if-range)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

(b) Priorité STP 8192 sur SW-Coeur-2

FIGURE 7 – Configuration de la hiérarchie Spanning-Tree sur le cœur

5.2 Activation du mode Trunk sur l'accès

Les commutateurs d'accès (**SW-Admin**, **SW-RD**, **SW-Prod**) ont également été configurés. Les ports `Fa0/23` et `Fa0/24`, qui assurent la remontée d'informations vers le cœur de réseau, ont été basculés en mode *Trunk*.

```
SW-Admin>enable
SW-Admin#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-Admin(config)#interface range f0/23 - 24
SW-Admin(config-if-range)# switchport mode trunk
SW-Admin(config-if-range)#exit
```

FIGURE 8 – Configuration des liens montants sur SW-Admin

5.3 Vérification de la topologie logique

La validation finale du Backbone repose sur la commande `show spanning-tree`. Le message *"This bridge is the root"* confirme que la priorité de 4096 (devenue 4106 avec l'ID du VLAN) a permis l'élection correcte du commutateur principal.

```
SW-Coeur-1#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     0090.2BEA.D04A
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4106  (priority 4096 sys-id-ext 10)
              Address     0090.2BEA.D04A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/24           Desg FWD 19        128.24   P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

FIGURE 9 – Preuve de l'élection du Root Bridge pour le VLAN 10

Analyse technique

La mise en place du mode *Trunk* combinée à une priorité STP maîtrisée permet d'assurer que le trafic inter-VLAN transite de manière optimale. En cas de défaillance du lien principal, le switch secondaire (**SW-Coeur-2**) prendra automatiquement le relais sans interruption de service majeure.

6 ROUTAGE INTER-VLAN ET SERVICES IP

6.1 Configuration du routeur principal (R1-Coeur)

Le routage entre les différents VLANs est assuré par une topologie *Router-on-a-Stick*. La première étape consiste à activer l'interface physique reliée au cœur de réseau.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1-Coeur
R1-Coeur(config)#interface GigabitEthernet0/0
R1-Coeur(config-if)# no shutdown

R1-Coeur(config-if)#exit
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

FIGURE 10 – Initialisation de R1-Coeur et activation de l'interface Gig0/0

L'interface physique est ensuite segmentée en sous-interfaces logiques. Chaque sous-interface correspond à un VLAN et reçoit l'étiquetage *802.1Q* adéquat ainsi qu'une adresse IP servant de passerelle.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1-Coeur(config)#interface GigabitEthernet0/0.10
R1-Coeur(config-subif)# encapsulation dot1Q 10
R1-Coeur(config-subif)# ip address 192.168.10.1 255.255.255.0
R1-Coeur(config-subif)#exit
R1-Coeur(config)#
R1-Coeur(config)#interface GigabitEthernet0/0.20
R1-Coeur(config-subif)# encapsulation dot1Q 20
R1-Coeur(config-subif)# ip address 192.168.20.1 255.255.255.0
R1-Coeur(config-subif)#exit
R1-Coeur(config)#
R1-Coeur(config)#interface GigabitEthernet0/0.30
R1-Coeur(config-subif)# encapsulation dot1Q 30
R1-Coeur(config-subif)# ip address 192.168.30.1 255.255.255.0
R1-Coeur(config-subif)#exit
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.10, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

%LINK-3-UPDOWN: Interface GigabitEthernet0/0.20, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

%LINK-3-UPDOWN: Interface GigabitEthernet0/0.30, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up
```

FIGURE 11 – Configuration des sous-interfaces logiques (.10, .20, .30)

Note importante sur l'adressage

Dans cette phase de test, les sous-interfaces de **R1-Coeur** ont été configurées avec l'adresse `.1` (ex : `192.168.10.1`). Cette configuration est **provisoire**. À terme, cette adresse `.1` deviendra l'adresse virtuelle partagée par le protocole de haute disponibilité, tandis que l'adresse physique de **R1-Coeur** sera basculée en `.2`.

6.2 Configuration du service DHCP

Pour automatiser l'adressage des postes de travail, un serveur DHCP est activé sur le routeur. Afin de respecter une segmentation stricte, des plages d'exclusions sont définies pour ne distribuer que les adresses comprises entre **.20 et .99**.

```
R1-Coeur(config)#! On interdit le debut (.1 a .19)
R1-Coeur(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.19
R1-Coeur(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.19
R1-Coeur(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.19
R1-Coeur(config)#
R1-Coeur(config)#! On interdit la fin (.100 a .254)
R1-Coeur(config)#ip dhcp excluded-address 192.168.10.100 192.168.10.254
R1-Coeur(config)#ip dhcp excluded-address 192.168.20.100 192.168.20.254
R1-Coeur(config)#ip dhcp excluded-address 192.168.30.100 192.168.30.254
R1-Coeur(config)#
R1-Coeur(config)#! On cree les reservoirs
R1-Coeur(config)#ip dhcp pool POOL-ADMIN
R1-Coeur(dhcp-config)# network 192.168.10.0 255.255.255.0
R1-Coeur(dhcp-config)# default-router 192.168.10.1
R1-Coeur(dhcp-config)#exit
R1-Coeur(config)#
R1-Coeur(config)#ip dhcp pool POOL-RD
R1-Coeur(dhcp-config)# network 192.168.20.0 255.255.255.0
R1-Coeur(dhcp-config)# default-router 192.168.20.1
R1-Coeur(dhcp-config)#exit
R1-Coeur(config)#
R1-Coeur(config)#ip dhcp pool POOL-PROD
R1-Coeur(dhcp-config)# network 192.168.30.0 255.255.255.0
R1-Coeur(dhcp-config)# default-router 192.168.30.1
R1-Coeur(dhcp-config)#exit
R1-Coeur(config)#
R1-Coeur#
%SYS-5-CONFIG_I: Configured from console by console
```

FIGURE 12 – Paramétrage des exclusions et des pools DHCP sur R1-Coeur

6.3 Mise en miroir sur le routeur de secours (R2-Coeur)

Une configuration rigoureusement identique a été appliquée sur le second routeur, **R2-Coeur**, afin d'assurer la redondance du service. La seule distinction technique réside dans l'adressage physique des interfaces :

- **R1-Coeur :** Utilise l'adresse physique `.2` (provisoirement `.1` pour les tests).
- **R2-Coeur :** Utilise l'adresse physique `.3` sur toutes ses sous-interfaces.

L'utilisation de paramètres DHCP identiques sur les deux équipements garantit que, quel que soit le routeur actif, les clients recevront une configuration réseau cohérente avec le plan d'adressage de Bidouille.

7 VALIDATION ET TESTS DE CONNECTIVITÉ

7.1 Attribution dynamique des adresses (DHCP)

Le succès de la configuration DHCP est validé par la réception correcte des adresses IP sur les postes clients de chaque zone. On observe que la première adresse disponible (.20) est bien attribuée conformément aux exclusions définies.

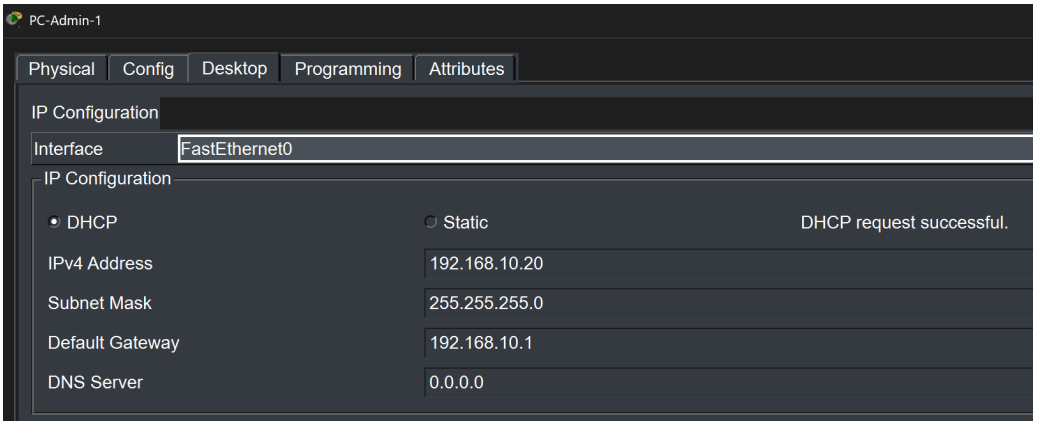

FIGURE 13 – Validation DHCP : PC-Admin-1 (VLAN 10)

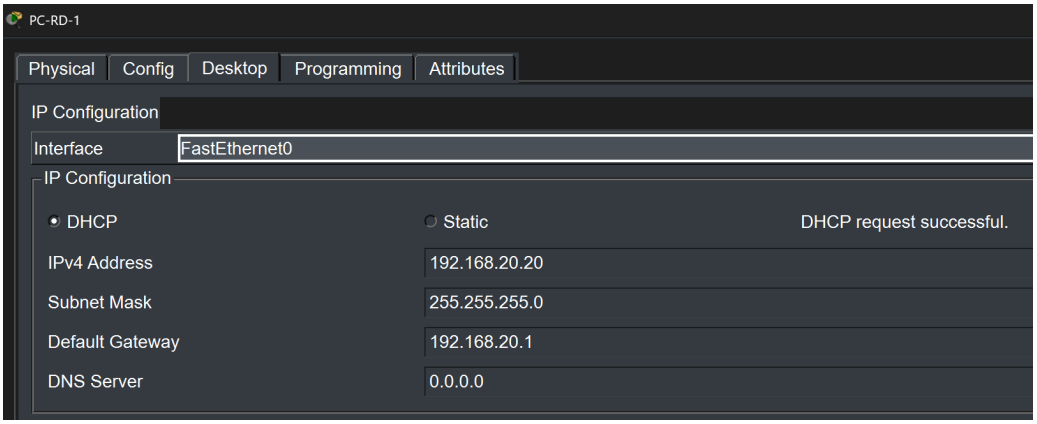

FIGURE 14 – Validation DHCP : PC-RD-1 (VLAN 20)

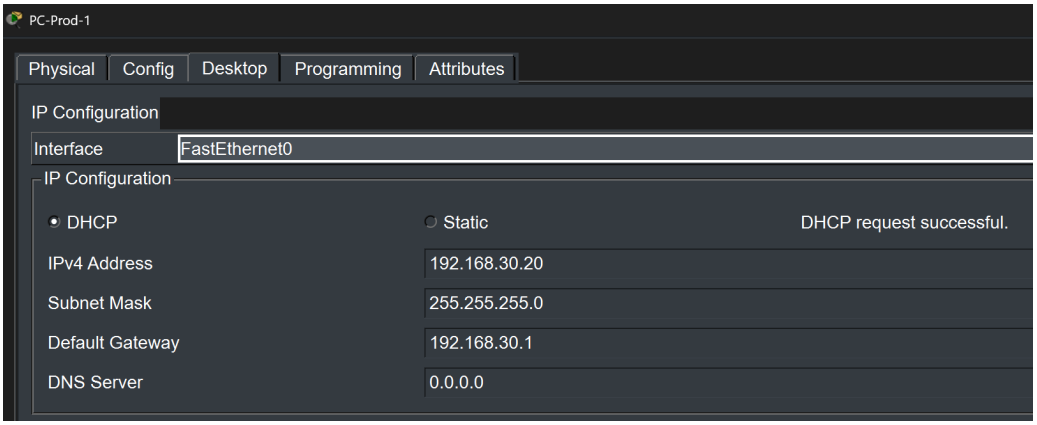

FIGURE 15 – Validation DHCP : PC-Prod-1 (VLAN 30)

7.2 Tests de communication Inter-VLAN (Ping)

Un test de connectivité ICMP (Ping) depuis le réseau d'Administration vers les réseaux R&D et Production confirme que le routeur assure correctement son rôle de passerelle entre les VLANs.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20B:BEFF:FE55:3EE9
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.10.20
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.10.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.20.20

Pinging 192.168.20.20 with 32 bytes of data:

Reply from 192.168.20.20: bytes=32 time<1ms TTL=127
Reply from 192.168.20.20: bytes=32 time<1ms TTL=127
Reply from 192.168.20.20: bytes=32 time=30ms TTL=127
Reply from 192.168.20.20: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 30ms, Average = 7ms

C:\>ping 192.168.30.20

Pinging 192.168.30.20 with 32 bytes of data:

Reply from 192.168.30.20: bytes=32 time<1ms TTL=127
Reply from 192.168.30.20: bytes=32 time=1ms TTL=127
Reply from 192.168.30.20: bytes=32 time<1ms TTL=127
Reply from 192.168.30.20: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.30.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

FIGURE 16 – Tests de connectivité réussis vers les VLANs 20 et 30

7.3 Adressage statique des serveurs de Production

Les serveurs de la zone de Production (**VLAN 30**) nécessitent un adressage fixe pour garantir la persistance des services. Les adresses ont été choisies au-delà de la plage DHCP (.100 et .101).

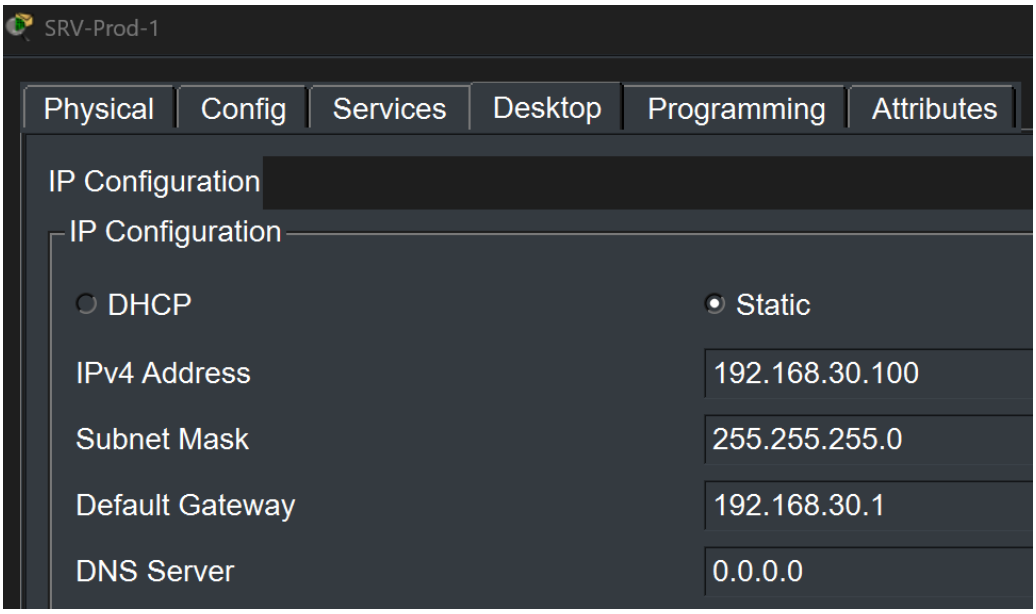

FIGURE 17 – Configuration statique du serveur SRV-Prod-1

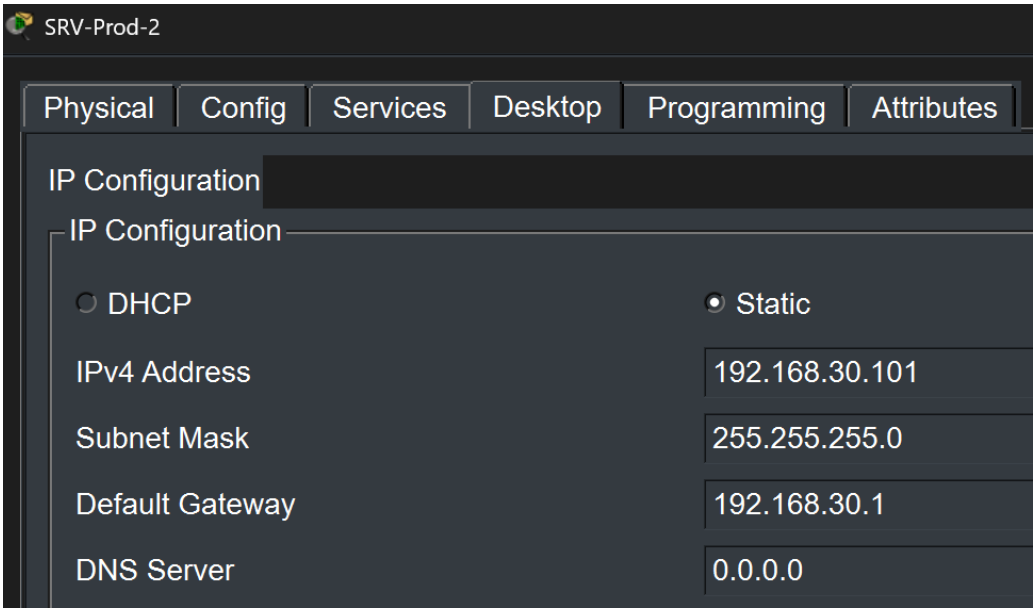

FIGURE 18 – Configuration statique du serveur SRV-Prod-2

7.4 Validation de l'accès aux ressources critiques

Afin de finaliser la phase de connectivité, un test de communication est réalisé depuis le VLAN d'Administration vers le serveur de Production. Ce test valide le bon fonctionnement des autoroutes (Trunks) et de la passerelle de routage.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20B:BEFF:FE55:3EE9
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.10.20
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.10.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.30.100

Pinging 192.168.30.100 with 32 bytes of data:

Reply from 192.168.30.100: bytes=32 time<1ms TTL=127
Reply from 192.168.30.100: bytes=32 time<1ms TTL=127
Reply from 192.168.30.100: bytes=32 time<1ms TTL=127
Reply from 192.168.30.100: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.30.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

FIGURE 19 – Succès du Ping entre l'Administration (10.20) et le Serveur Prod (30.100)

Bilan de l'étape

L'infrastructure réseau permet désormais une communication fluide entre les postes clients et les serveurs, tout en respectant la segmentation par VLAN. Les passerelles actuelles (.1) répondent correctement aux requêtes ICMP.

8 HAUTE DISPONIBILITÉ DU COEUR DE RÉSEAU

8.1 Mise en œuvre du protocole HSRP

Afin de garantir une continuité de service, le protocole **HSRP (Hot Standby Router Protocol)** a été déployé. Ce mécanisme permet de définir une passerelle virtuelle (*Virtual IP*) qui reste active même en cas de défaillance physique de l'un des routeurs.

```
R1-Coeur>enable
R1-Coeur#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1-Coeur(config)#
R1-Coeur(config)#! VLAN 10
R1-Coeur(config)#interface g0/0.10
R1-Coeur(config-subif)# ip address 192.168.10.2 255.255.255.0
R1-Coeur(config-subif)# standby 10 ip 192.168.10.1
R1-Coeur(config-subif)# standby 10 priority 110
R1-Coeur(config-subif)# standby 10 preempt
R1-Coeur(config-subif)#exit
R1-Coeur(config)#
R1-Coeur(config)#! VLAN 20
R1-Coeur(config)#interface g0/0.20
R1-Coeur(config-subif)# ip address 192.168.20.2 255.255.255.0
R1-Coeur(config-subif)# standby 20 ip 192.168.20.1
R1-Coeur(config-subif)# standby 20 priority 110
R1-Coeur(config-subif)# standby 20 preempt
R1-Coeur(config-subif)#exit
R1-Coeur(config)#
R1-Coeur(config)#! VLAN 30
R1-Coeur(config)#interface g0/0.30
R1-Coeur(config-subif)# ip address 192.168.30.2 255.255.255.0
R1-Coeur(config-subif)# standby 30 ip 192.168.30.1
R1-Coeur(config-subif)# standby 30 priority 110
R1-Coeur(config-subif)# standby 30 preempt
R1-Coeur(config-subif)#exit
R1-Coeur(config)#
```

FIGURE 20 – Configuration HSRP sur R1-Coeur (Priorité 110 et Preempt)

```
R2-Coeur>enable
R2-Coeur#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2-Coeur(config)#
R2-Coeur(config)#! VLAN 10
R2-Coeur(config)#interface g0/0.10
R2-Coeur(config-subif)# ip address 192.168.10.3 255.255.255.0
R2-Coeur(config-subif)# standby 10 ip 192.168.10.1
R2-Coeur(config-subif)#exit
R2-Coeur(config)#
R2-Coeur(config)#! VLAN 20
R2-Coeur(config)#interface g0/0.20
R2-Coeur(config-subif)# ip address 192.168.20.3 255.255.255.0
R2-Coeur(config-subif)# standby 20 ip 192.168.20.1
R2-Coeur(config-subif)#exit
R2-Coeur(config)#
R2-Coeur(config)#! VLAN 30
R2-Coeur(config)#interface g0/0.30
R2-Coeur(config-subif)# ip address 192.168.30.3 255.255.255.0
R2-Coeur(config-subif)# standby 30 ip 192.168.30.1
R2-Coeur(config-subif)#exit
R2-Coeur(config)#
```

FIGURE 21 – Configuration HSRP sur R2-Coeur (Rôle passif par défaut)

8.2 Validation des états Redondants

La commande `show standby brief` permet de confirmer la bonne synchronisation des deux équipements. Le routeur **R1** est correctement passé en état *Active*, tandis que le routeur **R2** s'est placé en état *Standby*.

```
R1-Coeur#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         10   110 P Active   local           192.168.10.3    192.168.10.1
Gig         20   110 P Active   local           192.168.20.3    192.168.20.1
Gig         30   110 P Active   local           192.168.30.3    192.168.30.1
R1-Coeur#
```

FIGURE 22 – État HSRP sur R1-Coeur : Le routeur est actif pour tous les VLANs

```
R2-Coeur#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         10   100   Standby  192.168.10.2    local           192.168.10.1
Gig         20   100   Standby  192.168.20.2    local           192.168.20.1
Gig         30   100   Standby  192.168.30.2    local           192.168.30.1
R2-Coeur#
```

FIGURE 23 – État HSRP sur R2-Coeur : Le routeur est prêt à prendre le relais

Analyse de la tolérance aux pannes

L'IP virtuelle **192.168.x.1** est désormais portée par le cluster de routeurs. Les tests montrent que les deux routeurs communiquent bien entre eux : R1 identifie son voisin en `.3` et R2 identifie son voisin en `.2`. La redondance est opérationnelle.

9 TESTS DE RÉSILIENCE ET TOLÉRANCE AUX PANNES

9.1 Simulation d'une défaillance du routeur actif

Pour valider l'efficacité du protocole **HSRP**, nous avons simulé une coupure totale du routeur principal **R1-Coeur** en désactivant manuellement son interface de liaison (*Gig0/0*).

```
R1-Coeur#write
Building configuration...
[OK]
R1-Coeur#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1-Coeur(config)#interface GigabitEthernet0/0
R1-Coeur(config-if)# shutdown

R1-Coeur(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down

%LINK-3-UPDOWN: Interface GigabitEthernet0/0.10, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to down

%LINK-3-UPDOWN: Interface GigabitEthernet0/0.20, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to down

%LINK-3-UPDOWN: Interface GigabitEthernet0/0.30, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to down
```

FIGURE 24 – Désactivation manuelle (shutdown) de l'interface principale sur R1-Coeur

9.2 Validation de la continuité de service (Failover)

Le succès du test est confirmé par un test de *ping* permanent effectué depuis un poste client vers le serveur de production. On observe une perte de seulement deux paquets lors de la coupure, avant que le routeur de secours (**R2-Coeur**) ne reprenne le trafic de manière transparente.

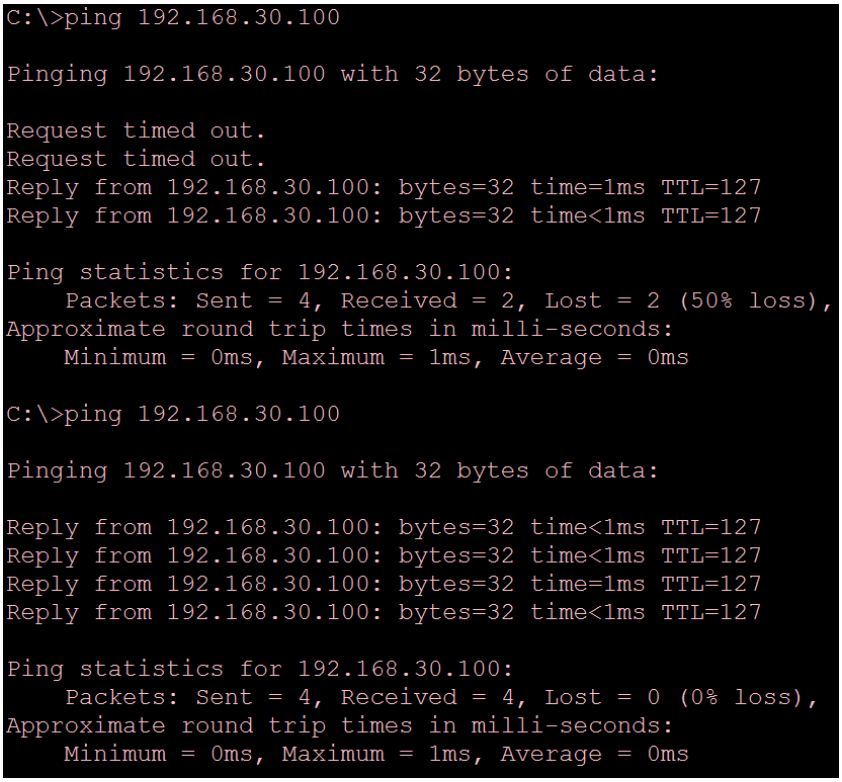

FIGURE 25 – Preuve du basculement : Reprise du flux après deux "Request timed out"

Analyse du test

Le temps de basculement constaté est extrêmement court (environ 2 à 3 secondes). Cela prouve que l'infrastructure de Bidouille est capable de maintenir l'accès aux serveurs critiques même en cas de panne matérielle majeure sur le routeur principal.

10 SÉCURITÉ ET CONTRÔLE DES FLUX (ACLS)

10.1 Configuration des listes de contrôle d'accès étendues

Pour répondre aux exigences de sécurité de Bidouille, des ACL étendues ont été configurées. La logique adoptée respecte la règle du *"First Match"* : les autorisations spécifiques (trafic retour, services particuliers) sont placées avant les interdictions génériques.

```
R1-Coeur#enable
R1-Coeur#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1-Coeur(config)#
R1-Coeur(config)#! --- On ecrase et on recommence proprement pour la RD ---
R1-Coeur(config)#no ip access-list extended ACL-RD
R1-Coeur(config)#ip access-list extended ACL-RD
R1-Coeur(config-ext-nacl)# permit icmp any 192.168.10.0 0.0.0.255 echo-reply
R1-Coeur(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1-Coeur(config-ext-nacl)# deny ip any 192.168.10.0 0.0.0.255
R1-Coeur(config-ext-nacl)# deny ip any 192.168.30.0 0.0.0.255
R1-Coeur(config-ext-nacl)# permit ip any any
R1-Coeur(config-ext-nacl)#exit
R1-Coeur(config)#
R1-Coeur(config)#! --- On fait pareil pour la PROD ---
R1-Coeur(config)#no ip access-list extended ACL-PROD
R1-Coeur(config)#ip access-list extended ACL-PROD
R1-Coeur(config-ext-nacl)# permit icmp any 192.168.10.0 0.0.0.255 echo-reply
R1-Coeur(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1-Coeur(config-ext-nacl)# deny ip any 192.168.10.0 0.0.0.255
R1-Coeur(config-ext-nacl)# deny ip any 192.168.20.0 0.0.0.255
R1-Coeur(config-ext-nacl)# permit ip any any
R1-Coeur(config-ext-nacl)#exit
R1-Coeur(config)#exit
R1-Coeur#
%SYS-5-CONFIG_I: Configured from console by console
```

FIGURE 26 – Saisie des règles ACL sur R1-Coeur avec priorité aux flux de réponse

L'utilisation des mots-clés `echo-reply` et `established` est ici cruciale. Elle permet d'autoriser les paquets de réponse vers le VLAN Administration sans pour autant permettre à la R&D ou à la Production d'initier une nouvelle connexion vers cette zone sensible.

10.2 Activation du filtrage sur les interfaces

Une ACL n'est effective que lorsqu'elle est associée à une interface. Dans notre topologie *Router-on-a-Stick*, le filtrage est appliqué en entrée (*in*) sur chaque sous-interface correspondant aux VLANs.

```
R1-Coeur(config)#interface g0/0.10
R1-Coeur(config-subif)# ip access-group ACL-ADMIN in
R1-Coeur(config-subif)#exit
R1-Coeur(config)#interface g0/0.20
R1-Coeur(config-subif)# ip access-group ACL-RD in
R1-Coeur(config-subif)#exit
R1-Coeur(config)#interface g0/0.30
R1-Coeur(config-subif)# ip access-group ACL-PROD in
R1-Coeur(config-subif)#exit
R1-Coeur(config)#
```

FIGURE 27 – Application des ACLs sur les sous-interfaces g0/0.10, .20 et .30

10.3 Vérification du fonctionnement des compteurs

La commande `show access-lists` permet de vérifier en temps réel si les règles sont sollicitées. Les compteurs (*matches*) valident que le routeur identifie et traite correctement les flux traversants.

```
R1-Coeur#show access-list
Extended IP access list ACL-ADMIN
    10 permit ip any 192.168.20.0 0.0.0.255 (8 match(es))
    20 permit tcp any host 192.168.30.100 eq 443
    30 permit tcp any host 192.168.30.101 eq 443
    40 deny ip any host 192.168.30.100
    50 deny ip any host 192.168.30.101
    60 permit ip any 192.168.30.0 0.0.0.255 (8 match(es))
    70 permit ip any any (690 match(es))
Extended IP access list ACL-RD
    10 permit icmp any 192.168.10.0 0.0.0.255 echo-reply
    20 permit tcp any 192.168.10.0 0.0.0.255 established
    30 deny ip any 192.168.10.0 0.0.0.255
    40 deny ip any 192.168.30.0 0.0.0.255
    50 permit ip any any (4 match(es))
Extended IP access list ACL-PROD
    10 permit icmp any 192.168.10.0 0.0.0.255 echo-reply
    20 permit tcp any 192.168.10.0 0.0.0.255 established
    30 deny ip any 192.168.10.0 0.0.0.255
    40 deny ip any 192.168.20.0 0.0.0.255
    50 permit ip any any (4 match(es))
```

FIGURE 28 – Visualisation des compteurs d'interception de paquets

10.4 Validation finale par tests d'intrusion (Ping)

La validation repose sur la comparaison entre le résultat attendu et le résultat obtenu sur les terminaux clients.

Tests depuis le VLAN Administration : Le poste Admin doit pouvoir administrer les postes de la R&D (Ping OK), mais ne doit accéder aux serveurs de production que via le port sécurisé 443. Le rejet du Ping vers le serveur (`.100`) confirme l'efficacité du filtrage.

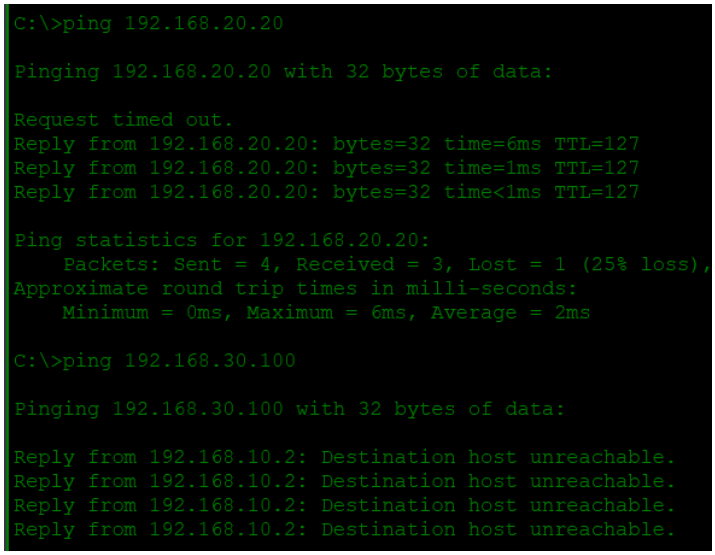

FIGURE 29 – Test de connectivité depuis PC-Admin : Succès vers RD, Échec vers Serveur Prod

Tests d'isolation de la Production : Le poste de production (`192.168.30.20`) tente de joindre le VLAN Administration. Le message *"Destination host unreachable"* renvoyé par la passerelle (`192.168.30.1`) prouve que l'ACL bloque activement la tentative d'intrusion.

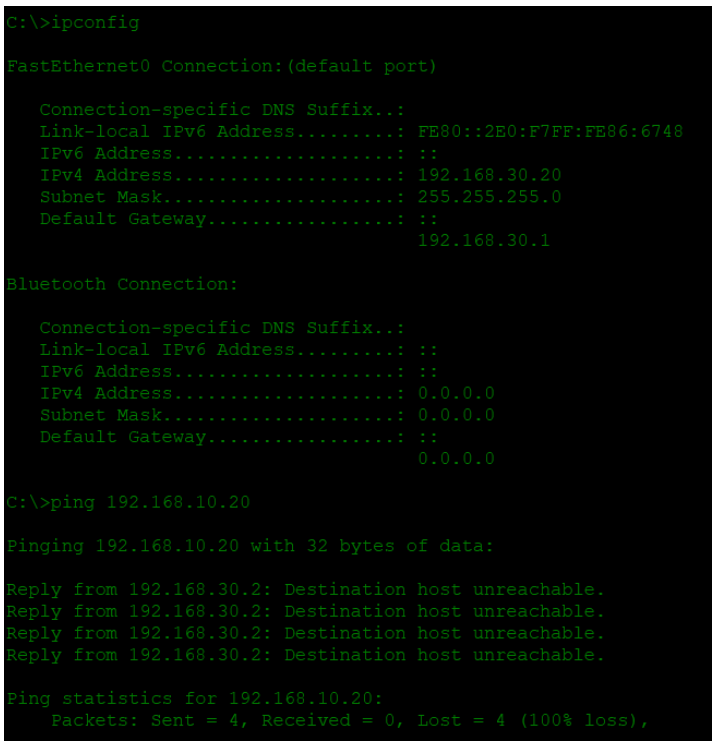

FIGURE 30 – Preuve d'isolation : Échec de la tentative de Ping de la Prod vers l'Admin

Bilan de sécurité

L'infrastructure est désormais sécurisée. Les flux sont strictement cloisonnés conformément à la matrice des flux, tout en préservant les capacités d'administration centralisées nécessaires à la maintenance du parc.

11 CONCLUSION GÉNÉRALE

Le déploiement de l'infrastructure réseau pour l'entreprise **Bidouille** est désormais finalisé et opérationnel. Ce projet a permis de répondre aux trois piliers fondamentaux d'un réseau moderne :

- **La Segmentation :** L'utilisation des VLANs assure que les flux de l'Administration, de la R&D et de la Production sont parfaitement isolés, garantissant une sécurité accrue des données.
- **La Performance et Flexibilité :** L'implémentation du routage Inter-VLAN et du service DHCP permet une gestion dynamique et fluide du parc informatique.
- **La Haute Disponibilité :** La combinaison des protocoles **STP** (Couche 2) et **HSRP** (Couche 3) garantit qu'aucune panne isolée d'un commutateur ou d'un routeur ne pourra paralyser l'activité de l'entreprise.

Les tests de résilience et les audits de sécurité via ACLs ont démontré que le réseau est capable de s'auto-réparer en quelques secondes tout en bloquant les tentatives d'accès non autorisées. L'architecture est donc prête pour une mise en production réelle, offrant un environnement à la fois stable, sécurisé et évolutif.

Livrables numériques joints

L'intégralité des sources techniques est jointe à ce rapport pour permettre l'audit et l'évolution de la solution :

- Le fichier de simulation **Cisco Packet Tracer (Bidouille.pkt)** contenant les configurations et permettant de reproduire les tests.
- Le schéma d'infrastructure réseau détaillé Bidouille.drawio (source originale).