BREIZHTIC

Rapport de modernisation de l'infrastructure réseau (Switch, Routeur, VLAN)

Fait à Montauban-de-Bretagne, le 17/9/2025

Rédigé par :

Ayman EZZAMANI – Stagiaire BTS SIO (option SISR)

Destinataire :

Benjamin Frangeul – Tuteur de stage

Sommaire

1. Introduction.....

Contexte et objectifs du projet de modernisation .....

2.Schéma du réseau actuel .....

Topologie existante (locaux techniques et accueil) .....

Inventaire du matériel utilisé (switchs, routeurs, câbles RJ45, firewall) .....

3. Nouvelle architecture réseau proposée .....

Schéma cible (séparation technique / accueil clients).....

Plan d'adressage IP et segmentation réseau.....

4. Configuration approximative d'un VLAN.....

Configuration d'un VLAN sur Cisco Packet Tracer : switch et routeur .....

4. Conclusion .....

Résumé des améliorations apportées.....

Bénéfices attendus (sécurité, performance, organisation) .....

Introduction

Ce compte rendu a pour objectif de présenter un projet de modernisation complète du réseau informatique de l'entreprise **Breizhtic**. L'idée directrice est de repartir sur des bases solides, en repensant entièrement l'infrastructure afin de la rendre plus claire, plus performante et surtout plus sécurisée.

Aujourd'hui, les réseaux d'entreprise, et en particulier celui de Breizhtic, jouent un rôle essentiel : ils assurent la communication entre les différents services, facilitent l'accès aux ressources partagées et garantissent la protection des données. Une infrastructure bien conçue contribue non seulement à la productivité quotidienne, mais aussi à la continuité de l'activité. C'est pourquoi ce projet de refonte vise à anticiper les besoins actuels et futurs, en proposant une solution moderne et évolutive.

La démarche consiste donc à mettre en place des améliorations et des solutions concrètes, notamment :

- Une nouvelle topologie réseau pour mieux organiser les flux de données,
- Une organisation claire du câblage et des équipements,
- La configuration des switchs, routeurs et firewall Cisco,
- Ainsi que l'intégration de mesures de sécurité adaptées.

En résumé, ce projet a pour ambition d'offrir à Breizhtic un réseau fiable, sécurisé et performant, capable de soutenir efficacement son activité et son développement futur.

Schéma du réseau actuel

a) Topologie existante (locaux techniques et accueil)

Le réseau actuel de l'entreprise repose sur un switch Ethernet Netgear **(8 ports),** installé dans la partie accueil. Ce switch sert de point central et relie directement les postes de l'accueil.

Cependant, plusieurs problèmes sont constatés :

- Les câbles RJ45 et électriques sont mal organisés et non protégés, ce qui augmente les risques de détérioration et complique la maintenance.
- Certains câbles passent à même le sol, exposant le réseau aux risques liés au passage des employés et aux déplacements de chaises.
- Les caméras de surveillance ne fonctionnent pas, ce qui réduit la sécurité physique.
- Le switch **(24 ports)**, même s'il est en état de marche, n'est pas configuré correctement. Actuellement, il ne garantit ni la segmentation du réseau ni la sécurité. Il sera donc nécessaire de le configurer avec plusieurs VLAN (Accueil, Technique, Responsable) afin de séparer les flux et de renforcer la protection de l'infrastructure de l'entreprise.

b) Inventaire du matériel utilisé et solutions proposées

- **Switch Cisco 24 ports (switch principal)**
  + Solution : Le conserver mais le configurer avec plusieurs **VLAN** pour mieux segmenter le réseau :
    - VLAN 10 → Accueil
    - VLAN 20 → Locaux techniques
    - VLAN 30 → Bureau du responsable

Cette séparation permettra de protéger les données sensibles. Par exemple, si un virus ou un pirate infecte le réseau technique, il ne pourra pas accéder aux ressources de l'accueil ni au réseau du responsable.

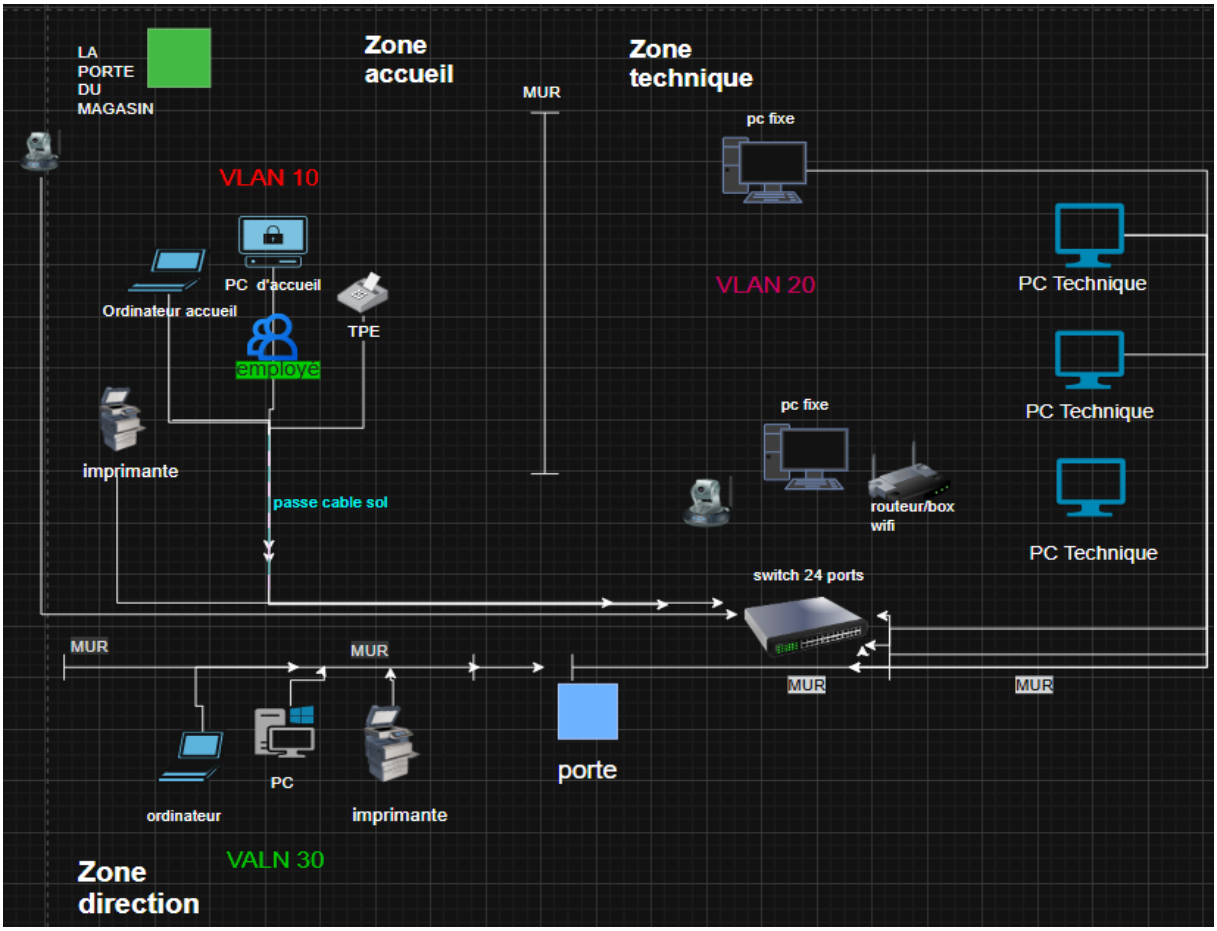
- **Câbles RJ45 et câbles électriques mal organisés**
  + Solution : Mettre en place une gestion du câblage (passe-câbles, attaches, goulottes) pour regrouper et fixer les câbles. Cela facilitera la maintenance et améliorera la circulation d'air, limitant ainsi les risques de surchauffe.

- **Câbles au sol**
  +Solution : Utiliser des goulottes, chemins de câbles ou passe-fils pour éviter tout contact direct avec le sol et protéger les câbles contre l'usure.

- **Absence de firewall dédié**
  +Solution : Déployer un **firewall** afin de protéger le réseau contre les attaques extérieures (Internet) et limiter également les menaces internes.

Nouvelle architecture réseau proposée

a) Schéma cible (séparation technique / accueil clients)



Le réseau proposé repose sur un switch Cisco 24 ports, qui devient le point central de l'infrastructure. Tous les équipements de l'entreprise sont connectés à ce switch à l'aide de câbles RJ45 protégés et organisés.

- Les équipements de la zone accueil (PC d'accueil, TPE, imprimante, caisse) sont situés au milieu de la boutique. Leurs câbles RJ45 passent donc par un passe-câble au sol, ce qui permet de protéger les câbles, d'éviter qu'ils traînent et de réduire les risques de détérioration ou d'accident. Ces câbles rejoignent ensuite le switch 24 ports.
- Les équipements de la zone technique (PC fixes, caméras, routeur/box Wi-Fi) et ceux de la zone direction (PC responsable, imprimante direction) sont reliés directement au switch par des câbles RJ45 passant dans les murs ou goulottes murales. Cela permet une installation plus propre et sécurisée.

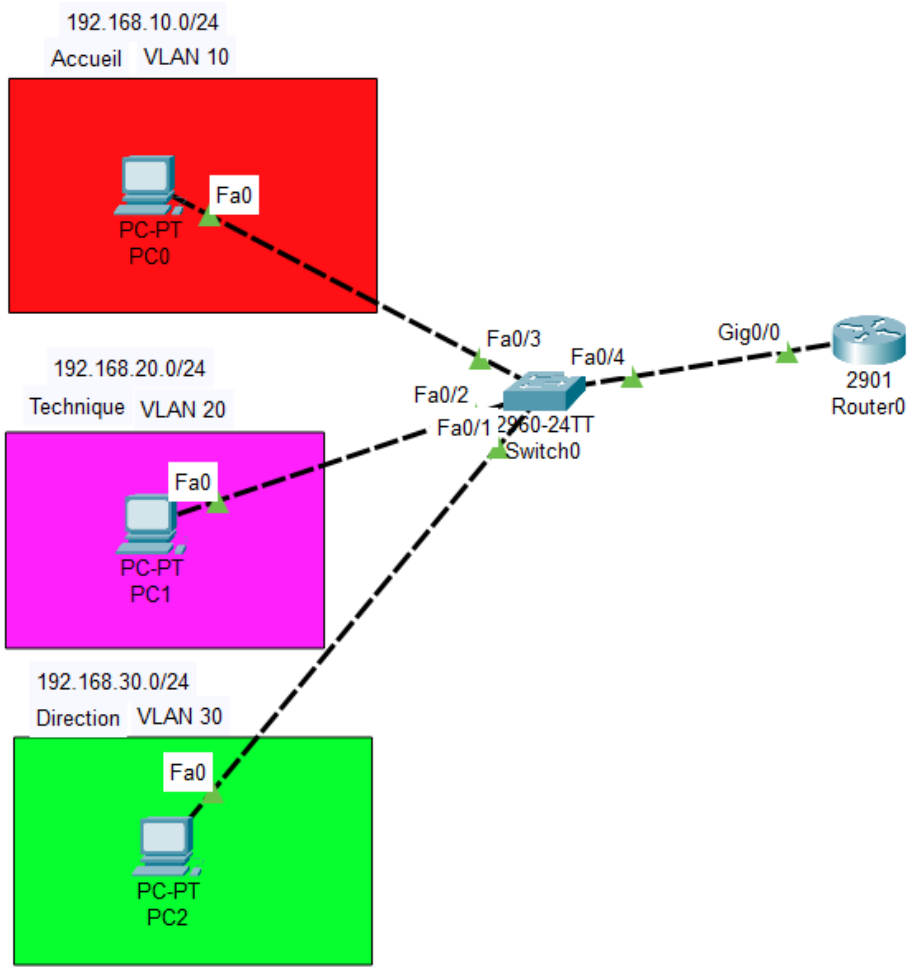
- Le switch Cisco est configuré avec trois VLAN distincts :
    - VLAN 10 – Accueil : regroupe le PC d'accueil, le TPE et l'imprimante d'accueil.
    - VLAN 20 – Technique : inclut les PC techniques, les caméras et le routeur/box Wi-Fi.
    - VLAN 30 – Direction : réservé au PC et à l'imprimante du responsable.

Cette segmentation logique (VLAN) permet d'isoler chaque partie de l'entreprise (Accueil, Technique, Direction) tout en utilisant un seul et même switch. Ainsi, si un virus ou une intrusion affecte un VLAN, les autres restent protégés.

B) Plan d'adressage IP et segmentation réseau

Vlan	Zone	Réseau IP	Équipements concernés	Exemple d'adresses IP
10	Accueil	192.168.10.0/24	PC accueil, imprimante accueil, TPE	PC : 192.168.10.10 Imprimante : 192.168.10.20 TPE : 192.168.10.30
20	Technique	192.168.20.0/24	PC techniques, caméras, Routeur/point d'accès Wi-Fi (TP-Link)	PC : 192.168.20.10-50 Caméras : 192.168.20.60-70 Routeur : 192.168.20.1
30	Direction	192.168.30.0/24	PC responsable, imprimante direction	PC : 192.168.30.10 Imprimante : 192.168.30.20

Configuration approximative d’un VLAN



Topologie simulée reliant trois VLANs (Accueil 192.168.10.0/24, Technique 192.168.20.0/24, Direction 192.168.30.0/24) via un trunk 802.1Q vers un routeur en router-on-a-stick afin d’assurer le routage inter-VLAN et permettre à tous les postes de communiquer et de se pinguer.

VLAN 10 → Accueil (192.168.10.0/24)

VLAN 20 → Locaux techniques (192.168.20.0/24)

VLAN 30 → Bureau du responsable (192.168.30.0/24)

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name acceuil
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name technique
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name direction
Switch(config-vlan)#
```

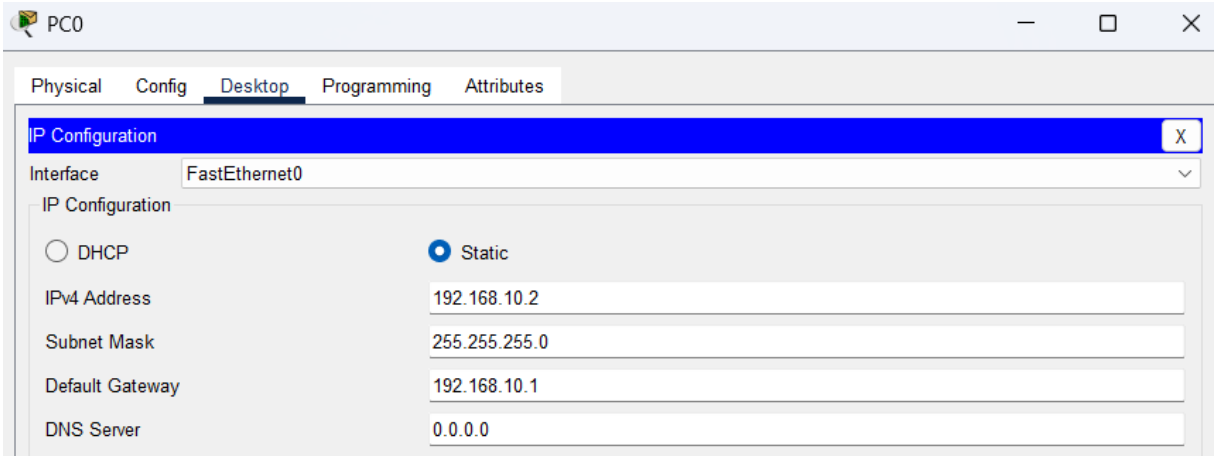
J'ai créé trois VLANs sur le switch — VLAN 10 (Accueil), VLAN 20 (Technique) et VLAN 30 (Direction) — et leur ai attribué des noms explicites pour faciliter l'administration.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
```

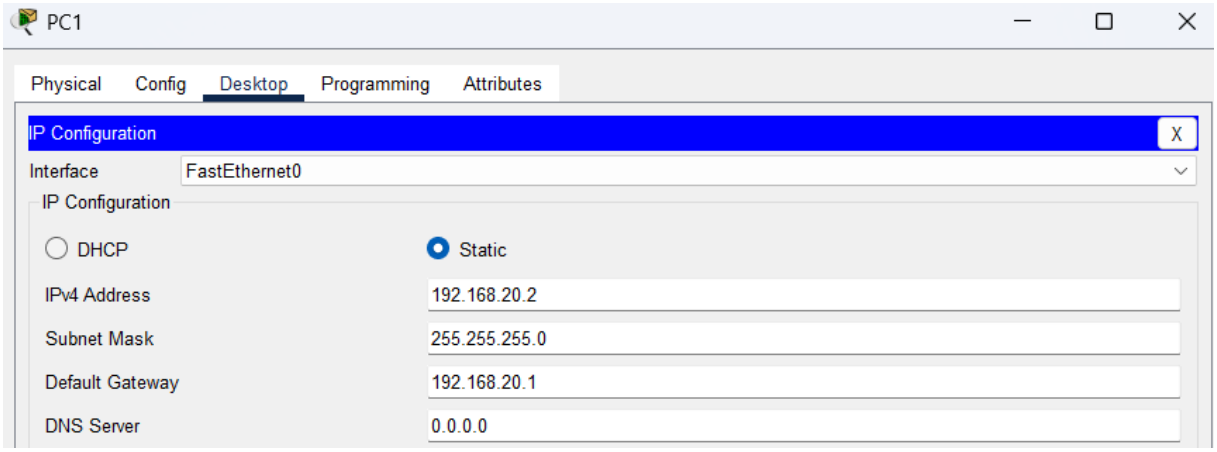
J'ai configuré les ports du switch en **mode access** et les ai affectés aux VLANs correspondants : **Fa0/3 → VLAN10 (Accueil)**, **Fa0/2 → VLAN20 (Technique)**, **Fa0/1 → VLAN30 (Direction)**. Cette affectation garantit que chaque poste appartienne uniquement à son sous-réseau et facilite l'isolation des flux.

```
Switch(config-if)#int fa0/4
Switch(config-if)#switchport mode trunk
```

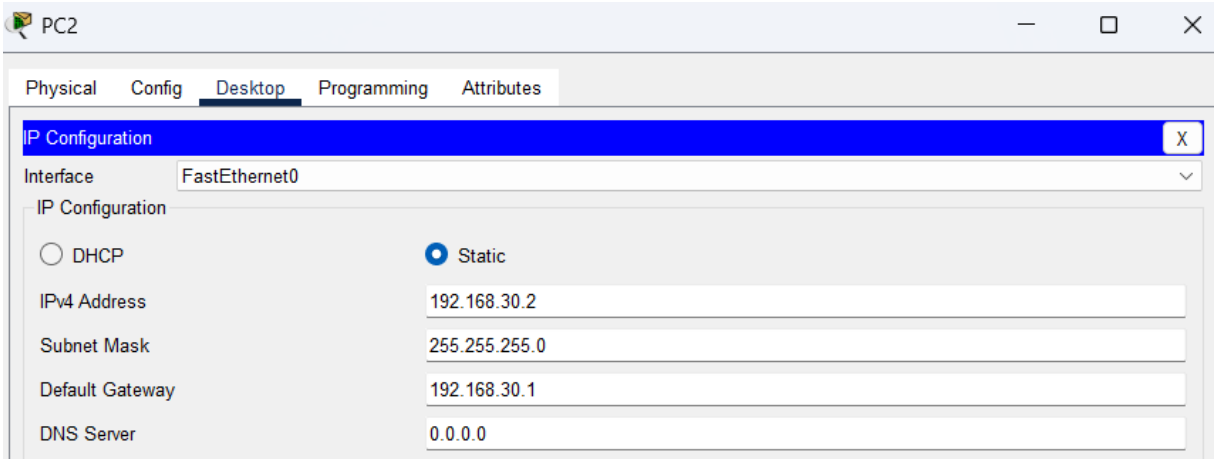
Le port Fa0/4 a été configuré en switchport mode trunk afin d'établir l'uplink 802.1Q vers le routeur et permettre le transport de plusieurs VLANs.



PC0 (VLAN 10 — Accueil) : IP statique 192.168.10.2 / Masque 255.255.255.0 — Passerelle 192.168.10.1



PC1 (VLAN 20 — Technique) : IP statique 192.168.20.2 / Masque 255.255.255.0 — Passerelle 192.168.20.1



PC2 (VLAN 30 — Technique) : IP statique 192.168.30.2 / Masque 255.255.255.0 — Passerelle 192.168.0.1

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#no shutdown
Router(config-if)#int g0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

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

Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#int g0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

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

Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#int g0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

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

Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#wr
Building configuration...
[OK]
Router#
```

Le routeur a été configuré en router-on-a-stick : l'interface physique Gi0/0 est activée (no shutdown) et trois sub-interfaces 802.1Q ont été créées (Gi0/0.10, Gi0/0.20, Gi0/0.30) avec encapsulation dot1Q <VLAN> et l'adresse IP de passerelle pour chaque VLAN (respectivement 192.168.10.1, 192.168.20.1, 192.168.30.1).

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20  192.168.20.1    YES manual up                    up
GigabitEthernet0/0.30  192.168.30.1    YES manual up                    up
```

La commande show ip interface brief confirme que les sub-interfaces **Gi0/0.10**, **Gi0/0.20** et **Gi0/0.30** sont bien créées, chacune avec son adresse IP de passerelle (192.168.10.1, 192.168.20.1, 192.168.30.1) et en état **up/up**, ce qui prouve qu'elles sont opérationnelles pour assurer le **routage inter-VLAN**

```
Switch>en
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/4       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/4       1-1005

Port        Vlans allowed and active in management domain
Fa0/4       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/4       1,10,20,30
```

La commande **show interfaces trunk** montre que le port Fa0/4 est configuré en trunk 802.1Q avec la VLAN native 1. Les VLANs 10 (Accueil), 20 (Technique) et 30 (Direction) sont autorisés, actifs et transmis sur ce lien. Cela permet de transporter plusieurs VLANs sur une seule interface entre le switch et le routeur afin d'assurer la communication inter-VLAN.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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   acceuil                          active    Fa0/3
20   technique                        active    Fa0/2
30   direction                        active    Fa0/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

La commande **show vlan brief** montre que les VLANs 10 (accueil), 20 (technique) et 30 (direction) sont bien créés, actifs et affectés respectivement aux ports Fa0/3, Fa0/2 et Fa0/1. Le VLAN 1 par défaut reste actif sur plusieurs ports non utilisés.

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Le **PC0 du VLAN 10 (192.168.10.2)** arrive à joindre sa **passerelle (192.168.10.1)** ainsi que le **PC1 du VLAN 20 (192.168.20.2)**. Cela confirme que la communication inter-VLAN fonctionne correctement et que les différents réseaux peuvent échanger entre eux via le routeur.

```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=11ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 5ms
```

Le PC du VLAN 30 (192.168.30.2) arrive à joindre **sa passerelle (192.168.30.1)** ainsi que le **PC0 du VLAN 10 (192.168.10.2)**. Cela confirme que la communication inter-VLAN fonctionne correctement et que les différents réseaux peuvent échanger entre eux via le routeur.

Conclusion

Résumé des améliorations apportées

- **Refonte complète de l'architecture** autour d'un **switch Cisco 24 ports** central.
- **Segmentation par VLAN** (VLAN 10 Accueil, VLAN 20 Technique, VLAN 30 Direction) + **routage inter-VLAN** (router-on-a-stick).
- **Plan d'adressage IP clair** par zone avec passerelles dédiées.
- **Organisation du câblage** : goulottes murales, **passe-câble au sol/colonne** pour l'accueil au centre, repérage des ports.
- **Base d'exploitation** : sauvegardes de config, documentation (plan IP, tableau des ports).

Bénéfices attendus

- **Sécurité :** isolement des services (limite la propagation d'un virus), contrôle fin des accès (ACL possibles), réduction de la surface d'attaque.
- **Performance :** moins de broadcast grâce aux VLAN, trafic mieux maîtrisé, câblage propre donc moins d'incidents.
- **Organisation & maintenabilité :** topologie lisible, ports/équipements identifiés, procédures de sauvegarde et de mise à jour, diagnostics plus rapides.