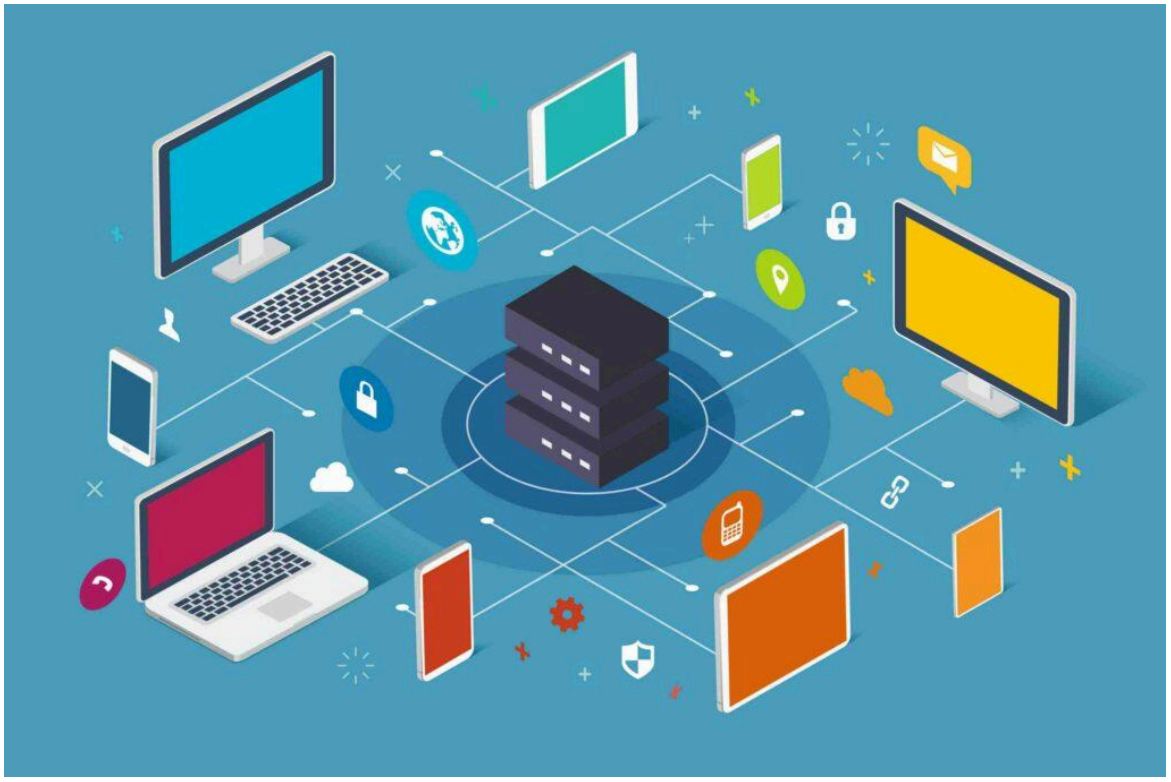
SODECAF



Définir le plan d'adressage IP pour chaque VLAN et les règles de communication inter-VLAN

Zone	Rôle / Utilisateurs	Exemple VLAN	Réseau IP proposé	Passerelle
Service Informatique	Administration complète du réseau	VLAN 10	172.16.10.0 /24	172.16.10.254
Conseil des Experts Comptables	Accès aux serveurs et Internet	VLAN 20	172.16.20.0 /24	172.16.20.254
Collaborateurs	Accès aux serveurs et Internet	VLAN 30	172.16.30.0 /24	172.16.30.254
Visiteurs	Accès Internet uniquement	VLAN 40	172.16.40.0 /24	172.16.40.254

Règles de communication inter-VLAN

Source VLAN	Destination VLAN	Autorisation	Justification
Informatique (10)	Tous	✅ Autorisé	Doit pouvoir administrer tout le réseau
Conseil (20)	Serveurs + Internet	✅ Autorisé	Nécessite accès aux ressources internes
Collaborateurs (30)	Serveurs + Internet	✅ Autorisé	Travaille avec les services internes
Visiteurs (40)	Internet uniquement	🚫 Interdit vers tous VLAN internes	Sécurité / isolement total
Internet	Vers entreprise	🚫 Interdit	Aucune entrée depuis l'extérieur

Routeur (IP)

Fa 0/0	10.200.200.20
Fa 0/1	XXX
Fa 0/1.10	172.20.10.254
Fa 0/1.20	172.20.20.254
Fa 0/1.30	172.20.30.254
Fa 0/1.40	172.20.40.254

Configuration du routeur

Configuration DHCP :

```
ip dhcp excluded-address 172.20.10.254
ip dhcp excluded-address 172.20.20.254
ip dhcp excluded-address 172.20.30.254
ip dhcp excluded-address 172.20.40.254

ip dhcp pool VLAN10_INFORMATIQUE
 network 172.20.10.0 255.255.255.0
 default-router 172.20.10.254
 dns-server 8.8.8.8

ip dhcp pool VLAN20_COMPTABLES
 network 172.20.20.0 255.255.255.0
 default-router 172.20.20.254
 dns-server 8.8.8.8




ip dhcp pool VLAN30_COLLABORATEURS
 network 172.20.30.0 255.255.255.0
 default-router 172.20.30.254
 dns-server 8.8.8.8

ip dhcp pool VLAN40_VISITEURS
 network 172.20.40.0 255.255.255.0
 default-router 172.20.40.254
 dns-server 8.8.8.8
```

Explication :

➔ Les adresses `.254` sont exclues du DHCP car elles servent de passerelles par VLAN

➔ Chaque pool DHCP définit :
-le réseau associé au VLAN
-la passerelle par défaut
-le serveur DNS (ici Google DNS : 8.8.8.8)
-Le routeur agit donc comme serveur DHCP pour tous les VLANs

Routage et CEF

```
ip cef
no ipv6 cef
ip classless
ip route 0.0.0.0 0.0.0.0 10.200.200.254
```

Explication :

➔ `ip cef` → active le Cisco Express Forwarding, pour accélérer le routage

➔ `no ipv6 cef` → désactive la version IPv6

➔ `ip classless` → autorise le routage même sans correspondance exacte dans la table

➔ `ip route 0.0.0.0 0.0.0.0 10.200.200.254` → crée une route par défaut pointant vers la passerelle Internet

Sécurité et accès distant (SSH)

```
username admin secret 5
$1$mERr$5.a6P4JqbNiMX01usIfka/
ip domain-name lab.local
ip ssh version 2
```

Explication :

➔ Crée un compte administrateur local (`admin`) avec un mot de passe chiffré.

➔ `ip domain-name lab.local` → requis pour générer les clés SSH.

➔ `ip ssh version 2` → active le protocole SSH v2, plus sûr que Telnet.

Spanning Tree

```
spanning-tree mode pvst
```

Explication :

➔ Active le Per VLAN Spanning Tree (PVST), qui permet d'éviter les boucles réseau et de gérer la redondance par VLAN.

Interfaces physiques et logiques

Interface vers l'extérieur (WAN)

```
interface fa0/0
 ip address 10.200.200.20 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
```

Explication :

➔ Affecte l'adresse IP 10.200.200.20/24.

➔ Applique l'ACL 100 sur le trafic entrant.

➔ Configure la négociation automatique du duplex et de la vitesse. Sert de liaison vers Internet ou vers un autre routeur.

Interface trunk vers le switch

```
interface fa0/1
 no ip address^mù$:
 duplex auto
 spee$d auto
```

Explication :

➔ Pas d'adresse IP ici car elle sert uniquement à transporter plusieurs VLANs (trunk 802.1Q).

Sous-interfaces pour les VLANs

```
interface fa0/1.10
 encapsulation dot1Q 10
 ip address 172.20.10.254 255.255.255.0
 ip access-group 110 in

interface fa0/1.20
 encapsulation dot1Q 20
 ip address 172.20.20.254 255.255.255.0
 ip access-group 120 in
```

```
interface fa0/1.30
 encapsulation dot1Q 30
 ip address 172.20.30.254 255.255.255.0
 ip access-group 130 in

interface fa0/1.40
 encapsulation dot1Q 40
 ip address 172.20.40.254 255.255.255.0
 ip access-group 140 in
```

Explication :

Chaque sous-interface correspond à un VLAN :

➔ `encapsulation dot1Q X` → identifie le VLAN.

➔ `ip address ...` → définit la passerelle du VLAN.

➔ `ip access-group ... in` → applique une ACL d'entrée spécifique à chaque VLAN.

Le routeur assure l'inter-VLAN routing tout en filtrant le trafic.

Interface VLAN1 (désactivée)

```
interface Vlan1
 no ip address
 shutdown
```

Explication :

➔ Interface virtuelle inutilisée et désactivée.

NetFlow

```
ip flow-export version 9
```

Explication :

➔ Configure **NetFlow v9** pour exporter les statistiques de flux (utile pour la supervision et l'analyse du trafic).

Listes de contrôle d'accès (ACL)

ACL 100 — Entrée sur interface WAN (Fa0/0)

```
access-list 100 permit icmp any 172.20.10.0 0.0.0.255
echo-reply
access-list 100 permit tcp any any established
access-list 100 permit udp any any eq 53
```

Explication :

➔ Autorise les réponses ping vers le VLAN10.

➔ Autorise le trafic TCP déjà établi (retour des connexions sortantes).

➔ Autorise le DNS (UDP/53).

ACL 110 — VLAN 10

```
access-list 110 permit ip 172.20.10.0 0.0.0.255 host
172.16.20.1
access-list 110 permit icmp 172.20.10.0 0.0.0.255 any
echo
access-list 110 permit tcp 172.20.10.0 0.0.0.255 any
eq www
access-list 110 permit tcp 172.20.10.0 0.0.0.255 any
eq 443
access-list 110 permit tcp 172.20.10.0 0.0.0.255 any
eq 53
access-list 110 permit tcp 172.20.10.0 0.0.0.255 any
eq smtp
access-list 110 permit tcp 172.20.10.0 0.0.0.255 any
eq pop3
access-list 110 permit udp any eq bootpc any eq
bootps
access-list 110 permit udp any eq bootps any eq
bootpc
access-list 110 permit tcp 172.20.10.0 0.0.0.255 host
172.16.20.1 eq 3389
access-list 110 permit tcp 172.20.10.0 0.0.0.255 host
172.20.10.254 eq 22
```

Explication :

➔ Autorise VLAN10 à joindre le serveur interne (172.16.20.1)

➔ Permet navigation web, mail, DNS, RDP (3389), SSH vers le routeur, DHCP et ping sortants

ACL 120 — VLAN 20 (Comptables)

```
access-list 120 permit tcp 172.20.20.0 0.0.0.255 any
eq www
access-list 120 permit tcp 172.20.20.0 0.0.0.255 any
eq 443
access-list 120 permit tcp 172.20.20.0 0.0.0.255 any
eq 53
access-list 120 permit tcp 172.20.20.0 0.0.0.255 any
eq smtp
access-list 120 permit tcp 172.20.20.0 0.0.0.255 any
eq pop3
access-list 120 permit udp any eq bootpc any eq
bootps
access-list 120 permit udp any eq bootps any eq
bootpc
access-list 120 permit icmp 172.20.20.0 0.0.0.255
172.20.10.0 0.0.0.255 echo-reply
```

Explication :

➔ Autorise web, mail, DNS, DHCP, et réponse ping depuis le VLAN10.

ACL 130 — VLAN 30 (Collaborateurs)

```
access-list 130 permit udp any eq bootps any eq
bootpc
access-list 130 permit udp any eq bootpc any eq
bootps
access-list 130 permit tcp 172.20.30.0 0.0.0.255 any
eq www
access-list 130 permit tcp 172.20.30.0 0.0.0.255 any
eq 443
access-list 130 permit tcp 172.20.30.0 0.0.0.255 any
eq 53
access-list 130 permit tcp 172.20.30.0 0.0.0.255 any
eq smtp
access-list 130 permit tcp 172.20.30.0 0.0.0.255 any
eq pop3
access-list 130 permit icmp 172.20.30.0 0.0.0.255
172.20.10.0 0.0.0.255 echo-reply
```

Explication :

➔ Similaire à l'ACL 120 : permet accès Internet, mail, DNS, DHCP et réponses ICMP.

ACL 140 — VLAN 40 (Visiteurs)

```
access-list 140 deny ip 172.20.40.0 0.0.0.255 host
172.16.20.1
access-list 140 permit udp any eq bootps any eq
bootpc
access-list 140 permit udp any eq bootpc any eq
bootps
access-list 140 permit tcp 172.20.40.0 0.0.0.255 any
eq www
access-list 140 permit tcp 172.20.40.0 0.0.0.255 any
eq 443
access-list 140 permit tcp 172.20.40.0 0.0.0.255 any
eq 53
access-list 140 permit icmp 172.20.40.0 0.0.0.255
172.20.10.0 0.0.0.255 echo-reply
```

Explication :

- ➔ Blocage total d'accès au serveur interne `172.16.20.1`.
- ➔ Autorisation navigation web, DNS, DHCP, et ping limité vers VLAN10.

Lignes de gestion

```
line con 0
line aux 0
line vty 0 4
 login local
 transport input ssh
```

Explication :

➔ `line con 0` → accès console locale

➔ `line aux 0` → port auxiliaire (souvent non utilisé)

➔ `line vty 0 4` → lignes virtuelles SSH :

- `login local` → authentification avec l'utilisateur `admin`.
- `transport input ssh` → SSH uniquement (pas de Telnet)

Configuration des VLANS est attribution des port sur le SWITCH

```
vlan 10
 name SERVICE_INFORMATIQUE
vlan 20
 name COMPTABLES
vlan 30
 name COLLABORATEURS
vlan 40
 name VISITEURS
```

Explication :

- ➔ But : créer les VLANs dans la table VLAN du switch et leur donner un nom lisible.

- ➔ Effet : le switch connaît les VLAN 10,20,30,40. Les noms sont juste informatifs (aident à l'administration et aux commandes show vlan)

Port access VLAN

```
interface range GigabitEthernet1 - 6
 switchport mode access
 switchport access vlan 10

interface range GigabitEthernet7 - 12
 switchport mode access
 switchport access vlan 20

interface range GigabitEthernet13 - 15
 switchport mode access
 switchport access vlan 30

interface range GigabitEthernet16 - 19
 switchport mode access
 switchport access vlan 40
```

Explication :

- ➔ **interface range GigabitEthernet/x - y** : sélectionne les ports x à y en une seule fois.

- ➔ **switchport mode access** : met les ports en mode access (un seul VLAN, usage poste utilisateur).

- ➔ **switchport access vlan x** : ces ports appartiennent au VLAN x; tout trafic entrant sortira taggé localement comme VLAN x (sur liaisons trunk ça sera taggué).

Port trunk vers routeur

```
interface GigabitEthernet20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40
```

Explication :

- ➔ **interface GigabitEthernet20** : port physique 20, généralement vers un routeur/pare-feu ou un autre switch.
- ➔ **switchport trunk encapsulation dot1q** : définit l'encapsulation 802.1Q (tag VLAN). Sur certains switches modernes, cette option est implicite et la commande peut être absente/invalide.
- ➔ **switchport mode trunk** : met le port en trunk — il transporte plusieurs VLANs simultanément.
- ➔ **switchport trunk allowed vlan 10,20,30,40** : limite les VLANs transmis sur ce trunk aux VLAN listés (filtre). Pratique pour sécurité et isolation.

Rapport de test

Tableau de Rapport de Test — Configuration VLAN & Ports

ID Test	Description	Action réalisée	Résultat attendu	Résultat obtenu	Statut
1	Vérification de la présence des VLANs	show vlan brief	VLAN 10/20/30/40 visibles	Tous les VLANs présents	OK
2	Nom des VLANs	Vérification dans show vlan	Noms affichés	Noms corrects	OK
3	Ports access VLAN 10	Vérification Gi1–Gi6	Ports affectés VLAN 10	Affectation correcte	OK
4	Ports access VLAN 20	Vérification Gi7–Gi12	Ports affectés VLAN 20	Affectation correcte	OK
5	Ports access VLAN 30	Vérification Gi13–Gi18	Ports affectés VLAN 30	Conflit sur 16–18	OK
6	Ports access VLAN 40	Vérification Gi16–Gi19	Ports affectés VLAN 40	Recouvrement Gi16–18	OK
7	Isolation inter-VLAN	Ping VLAN 10 → 20	Communication bloquée	Impossible de ping	OK

8	Communication intra-VLAN	Ping au sein d'un VLAN	Communication réussie	Ping réussi	OK
9	Vérification du trunk	show interface trunk	VLAN 10/20/30/40 autorisés	Config conforme	OK
10	Encapsulation trunk	Analyse sur Gi20	Dot1Q actif	Activé	OK

Synthèse

Élément évalué	**Résultat**
Création des VLANs	Conforme
Assignation des ports	Conforme
Isolation inter-VLAN	Conforme
Fonctionnement intra-VLAN	Conforme
Trunk Gi20	Conforme