



# Formation OpenClassrooms Administrateur Systèmes, Réseaux Et Sécurité

## Soutenance Projet-07

Stéphane Perfetti

16/10/2024



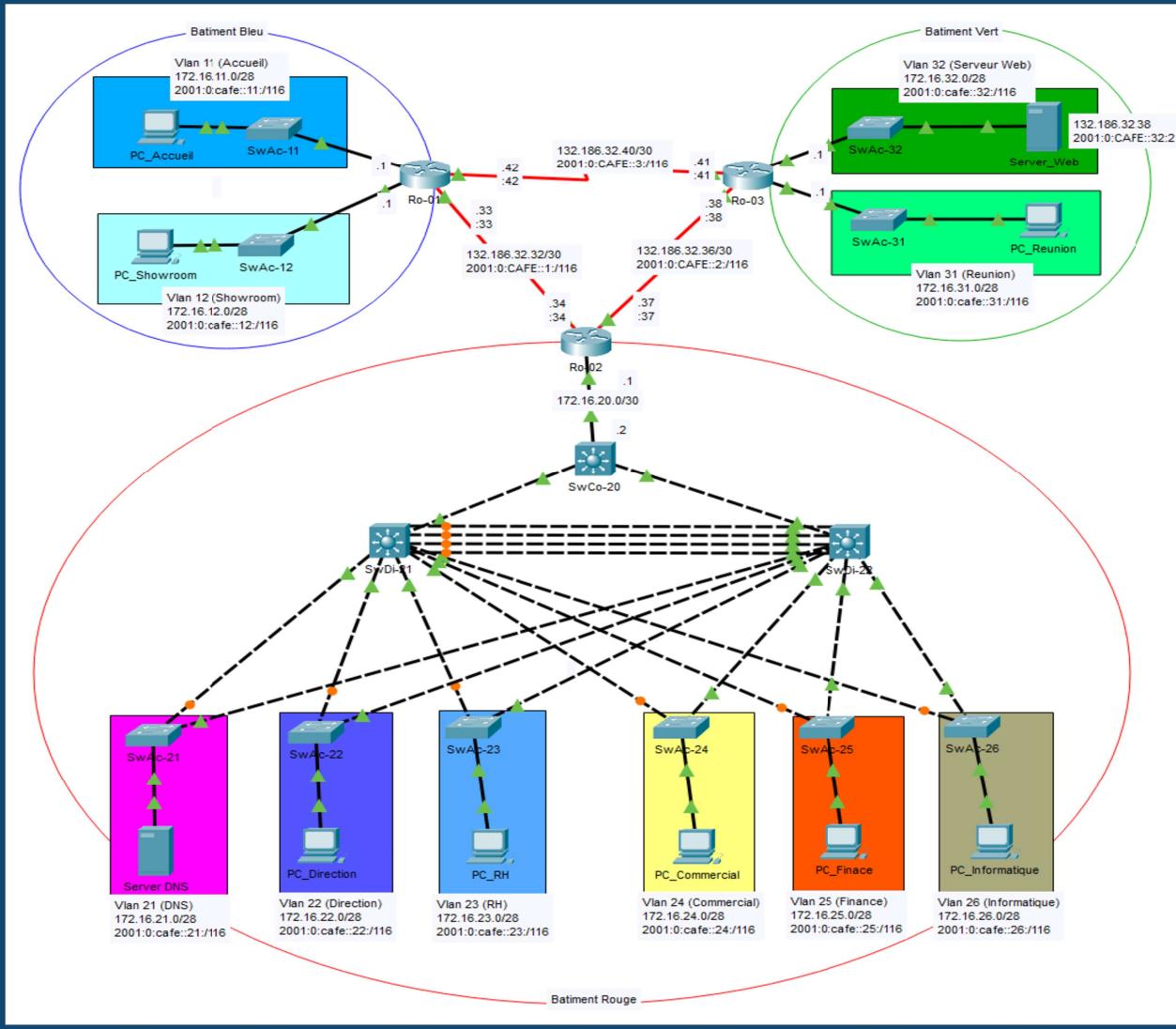
# Projet 07

-

## Configurez des services réseaux et des équipements d'interconnexion

- Scénario :
  - Mise en place du réseau de nouveaux locaux de la société Impact Influence.
- Plan d'action :
  - Architecture du laboratoire
  - Plan d'adressage
  - Réseaux des différents bâtiments
  - Préconisations d'amélioration de la cybersécurité

# Architecture du prototype



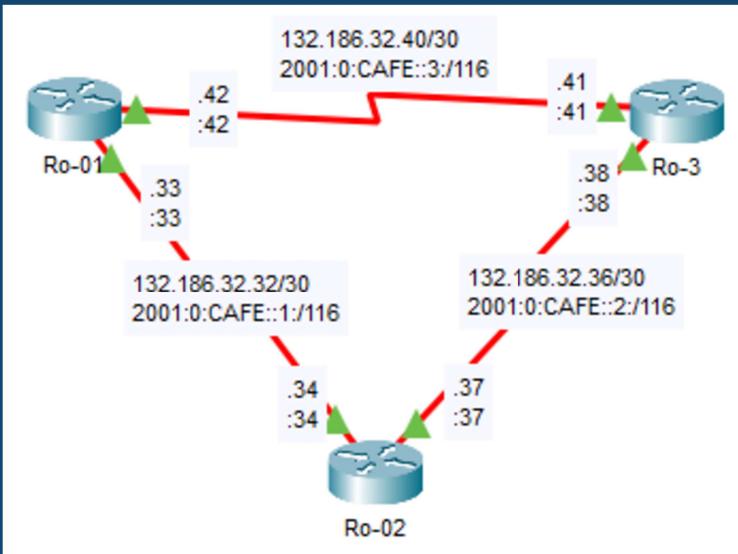
## Prototype sous Cisco Packet Tracer

- 3 bâtiments (Bleu; Rouge; Vert) avec réseaux privées LAN.
- Infrastructure inter bâtiment avec réseaux publiques WAN.
- Routeurs (Ro-xx), modèle Cisco ISR4331
- Switch Cœur (SwCo-xx) et switchs de distributions (SwDi-xx), modèle Cisco 3650 (Niveau 3)
- Switch d'Accès (SwAc-xx), modèle Cisco 2960

# Plan d'adressage

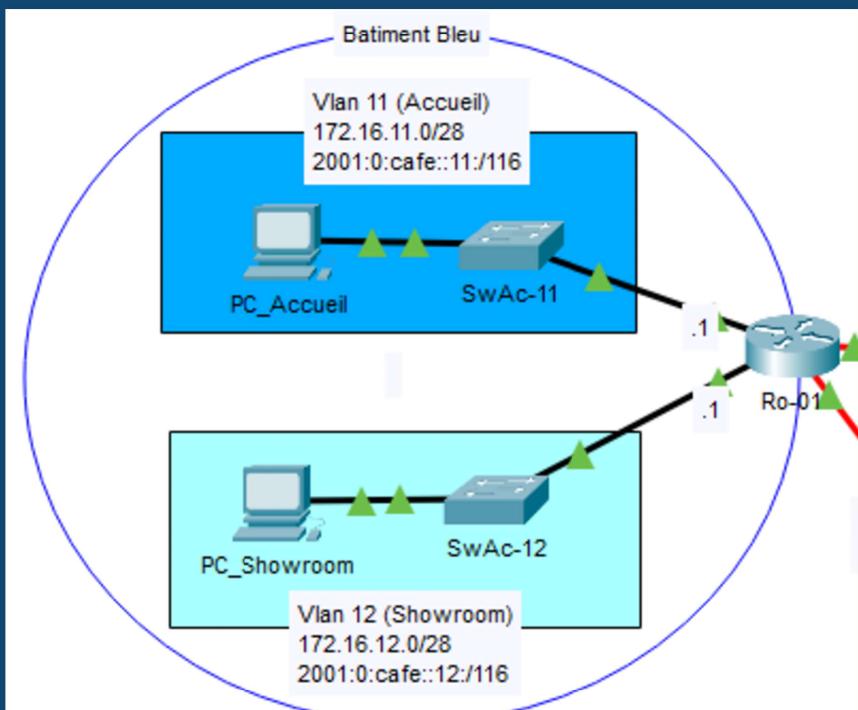
Groupe (abr.)	Sub-group		VLAN		IP							
	Sous-groupe	Nbs éléments	Nom	Numéro	Type adressage	Sous-réseau	Masque décimale	Nbs adresse	Plage début	Plage fin	Adresse diffusion	Passerelle
Infrastructure (Infra)	Infra-1	2			Statique	132.186.32.32/30	255.255.255.252	4	132.186.32.33	132.186.32.34	132.186.32.35	N/A
		2			Statique	2001:0:cafe::1/116			2001:0:cafe::1:0	2001:0:cafe::1:fff		
	Infra-2	2			Statique	132.186.32.36/30	255.255.255.252	4	132.186.32.37	132.186.32.38	132.186.32.39	N/A
		2			Statique	2001:0:cafe::2/116			2001:0:cafe::2:0	2001:0:cafe::2:fff		
	Infra-3	2			Statique	132.186.32.40/30	255.255.255.252	4	132.186.32.41	132.186.32.42	132.186.32.43	N/A
		2			Statique	2001:0:cafe::3/116			2001:0:cafe::3:0	2001:0:cafe::3:fff		
Administration (Admin)	N/A	32	Admin	99	Statique	172.16.99.0/26	255.255.255.192	64	172.16.99.1	172.16.99.62	172.16.99.63	172.16.99.1
Bleu (Bl)	Accueil	10	BI-Accueil	11	Statique	172.16.11.0/28	255.255.255.240	16	172.16.11.1	172.16.11.14	172.16.11.15	172.16.11.1
					Statique	2001:0:cafe::11/116			2001:0:cafe::11:0	2001:0:cafe::11:fff		
	Showroom	10	BI>Showroom	12	Statique	172.16.12.0/28	255.255.255.240	16	172.16.12.1	172.16.12.14	172.16.12.15	172.16.12.1
					Statique	2001:0:cafe::12/116			2001:0:cafe::12:0	2001:0:cafe::12:fff		
Rouge (Ro)	DNS	5	Ro-DNS	21	DHCP	172.16.21.0/29	255.255.255.248	8	172.16.21.1	172.16.21.6	172.16.21.7	172.16.21.1
					Statique	2001:0:cafe::21/116			2001:0:cafe::21:0	2001:0:cafe::21:fff		
	Direction	10	Ro-Direction	22	DHCP	172.16.22.0/28	255.255.255.240	16	172.16.22.1	172.16.22.14	172.16.22.15	172.16.22.1
					Statique	2001:0:cafe::22/116			2001:0:cafe::22:0	2001:0:cafe::22:fff		
	RH	10	Ro-RH	23	DHCP	172.16.23.0/28	255.255.255.240	16	172.16.23.1	172.16.23.14	172.16.23.15	172.16.23.1
					Statique	2001:0:cafe::23/116			2001:0:cafe::23:0	2001:0:cafe::23:fff		
	Commercial	10	Ro-Commercial	24	DHCP	172.16.24.0/28	255.255.255.240	16	172.16.24.1	172.16.24.14	172.16.24.15	172.16.24.1
					Statique	2001:0:cafe::24/116			2001:0:cafe::24:0	2001:0:cafe::24:fff		
Vert (Ve)	Finance	10	Ro-Finance	25	DHCP	172.16.25.0/28	255.255.255.240	16	172.16.25.1	172.16.25.14	172.16.25.15	172.16.25.1
					Statique	2001:0:cafe::25/116			2001:0:cafe::25:0	2001:0:cafe::25:fff		
	Informatique	10	Ro-Informatique	26	DHCP	172.16.26.0/28	255.255.255.240	16	172.16.26.1	172.16.26.14	172.16.26.15	172.16.26.1
					Statique	2001:0:cafe::26/116			2001:0:cafe::26:0	2001:0:cafe::26:fff		
	Web	10	Ve-Web	31	Statique	172.16.31.0/28	255.255.255.240	16	172.16.31.1	172.16.31.14	172.16.31.15	172.16.31.1
					Statique	2001:0:cafe::31/116			2001:0:cafe::31:0	2001:0:cafe::31:fff		
	Réunion	10	Ve-Reunion	32	Statique	172.16.32.0/28	255.255.255.240	16	172.16.32.1	172.16.32.14	172.16.32.15	172.16.32.1
					Statique	2001:0:cafe::32/116			2001:0:cafe::32:0	2001:0:cafe::32:fff		

# WAN: infrastructure inter-batiments



- Routeurs: Ro-01, Ro-02, Ro-03
- Liaison séries entre chaque routeurs
- Réseaux et adresses publiques:
  - Bat. Bleu ↔ Bat. Rouge:
    - IPv4: 132.186.32.32/30
    - IPv6: 2001:0:CAFE::1:/116
  - Bat. Rouge ↔ Bat. Vert:
    - IPv4: 132.186.32.36/30
    - IPv6: 2001:0:CAFE::2:/116
  - Bat. Vert ↔ Bat. Bleu:
    - IPv4: 132.186.32.36/30
    - IPv6: 2001:0:CAFE::2:/116
- Routage dynamique: EIGRP IPv4 et EIGRP IPv6

# Réseau Bâtiment Bleu

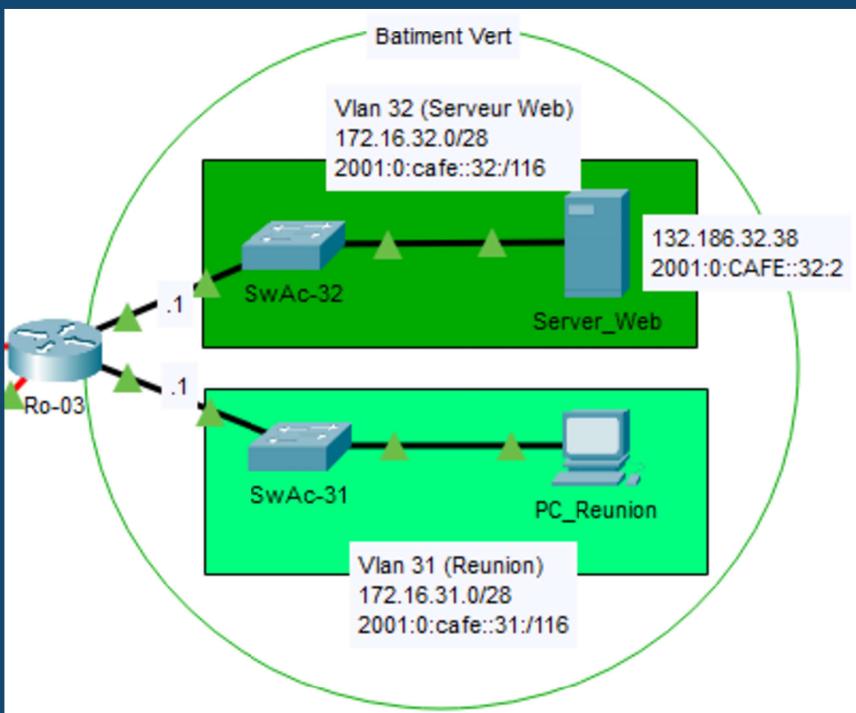


- **VLAN:**
  - VLAN 11 (Accueil): 172.16.11.0/28; 2001:0:CAFE::11:/116
  - VLAN 12 (Showroom): 172.16.12.0/28; 2001:0:CAFE::12:/116
- **Routeur Ro-01:**

Serial 0/1/0	132.186.32.33/30	2001:0:CAFE::1:33	FE80::1
Serial 0/1/1	132.186.32.42/30	2001:0:CAFE::3:42	FE80::1
Gig 0/0/0.11	172.16.11.1/28	2001:0:CAFE::11:1	FE80::1
Gig 0/0/1.12	172.16.12.1/28	2001:0:CAFE::12:1	FE80::1
Vlan 99	172.16.99.1/26		

  - Sous-interfaces pour chaque VLAN
- **Switch SwAc-11 et SwAc-12:**
  - Interfaces en mode Access côté équipement terminaux.
  - Interfaces mode Trunk côté routeur.

# Réseau Bâtiment Vert

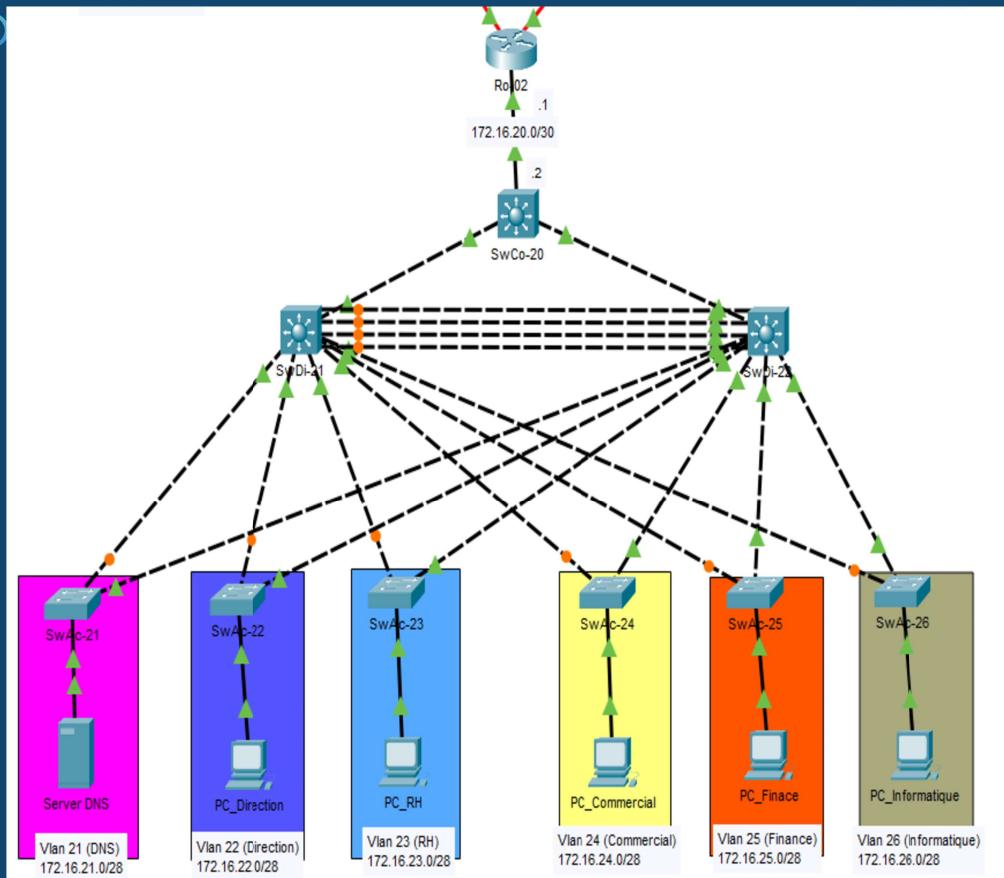


- **VLAN:**
  - VLAN 31 (Réunion): 172.16.31.0/28; 2001:0:CAFE::31:116
  - VLAN 32 (Web): 172.16.32.0/28; 2001:0:CAFE::32:116
- **Serveur Web:**
  - Add. Privées: 172.16.32.2
  - Add. Publiques: 132.186.32.38; 2001:0:CAFE::32:2
- **Routeur Ro-03:**

Serial 0/1/0	132.186.32.41/30	2001:0:CAFE::3:41	FE80::3
Serial 0/1/1	132.186.32.38/30	2001:0:CAFE::2:38	FE80::3
Gig 0/0/0.31	172.16.31.1/29	2001:0:CAFE::31:1	FE80::3
Gig 0/0/1.32	172.16.32.1/29	2001:0:CAFE::32:1	FE80::3
Vlan 99	172.16.99.3/26		

  - Sous-interfaces pour chaque VLAN
  - NAT transfert de port entre l'adresse publique Ipv4 du routeur et l'adresse Ipv4 du serveur Web.
- **Switch SwAc-31 et SwAc-32:**
  - Interfaces en mode Access côté équipement terminaux.
  - Interfaces mode Trunk côté routeur.

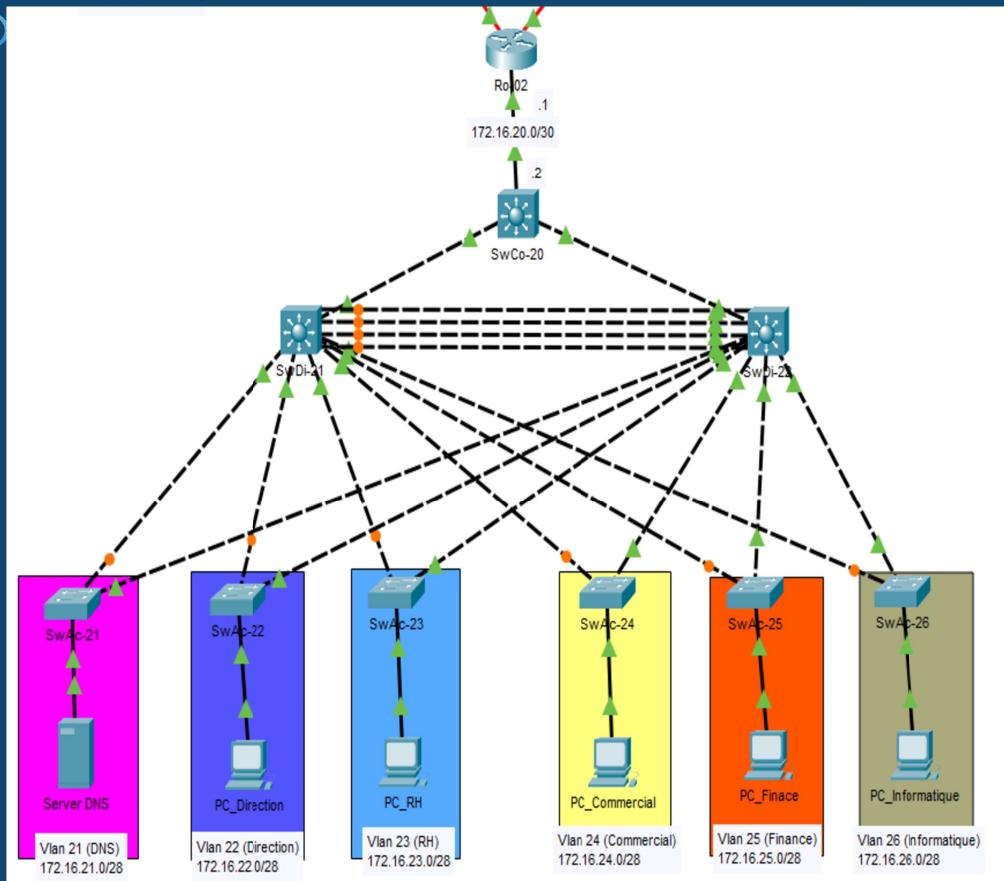
# Réseau Bâtiment Rouge



- VLAN:
  - VLAN 21 (DNS):
    - 172.16.21.0/28; 2001:0:CAFE::21:/116
    - Serveur DNS:
      - 172.16.21.4; 2001:0:CAFE::21:4
  - VLAN 22 (Direction):
    - 172.16.22.0/28; 2001:0:CAFE::22:/116
  - VLAN 23 (RH):
    - 172.16.23.0/28; 2001:0:CAFE::23:/116
  - VLAN 24 (Commercial):
    - 172.16.24.0/28; 2001:0:CAFE::24:/116
  - VLAN 25 (Finance):
    - 172.16.25.0/28; 2001:0:CAFE::25:/116
  - VLAN 26 (Informatique):
    - 172.16.26.0/28; 2001:0:CAFE::26:/116
- Serveur DNS:
  - 172.16.21.4; 2001:0:CAFE::21:4

DNS	Name	Type	Detail
SYSLOG			
AAA			
NTP			
EMAIL			
FTP			
IoT			
VM Management			
Radius EAP			
	Name	Type	Detail
	Add	Save	Remove
No.	Name	Type	Detail
0	impactinfluence.com	AAAA Record	2001:0:CAFE::32:2
1	impactinfluence.com	A Record	132.186.32.38

# Réseau Bâtiment Rouge



- **Routeur Ro-02:**

Serial 0/1/0	132.186.32.37/30	2001:0:CAFE::2:37	FE80::2
Serial 0/1/1	132.186.32.34/30	2001:0:CAFE::1:34	FE80::2
Gig 0/0/0	172.16.20.1/30	2001:0:CAFE::20:1	FE80::2
Vlan99	172.16.99.20/26		

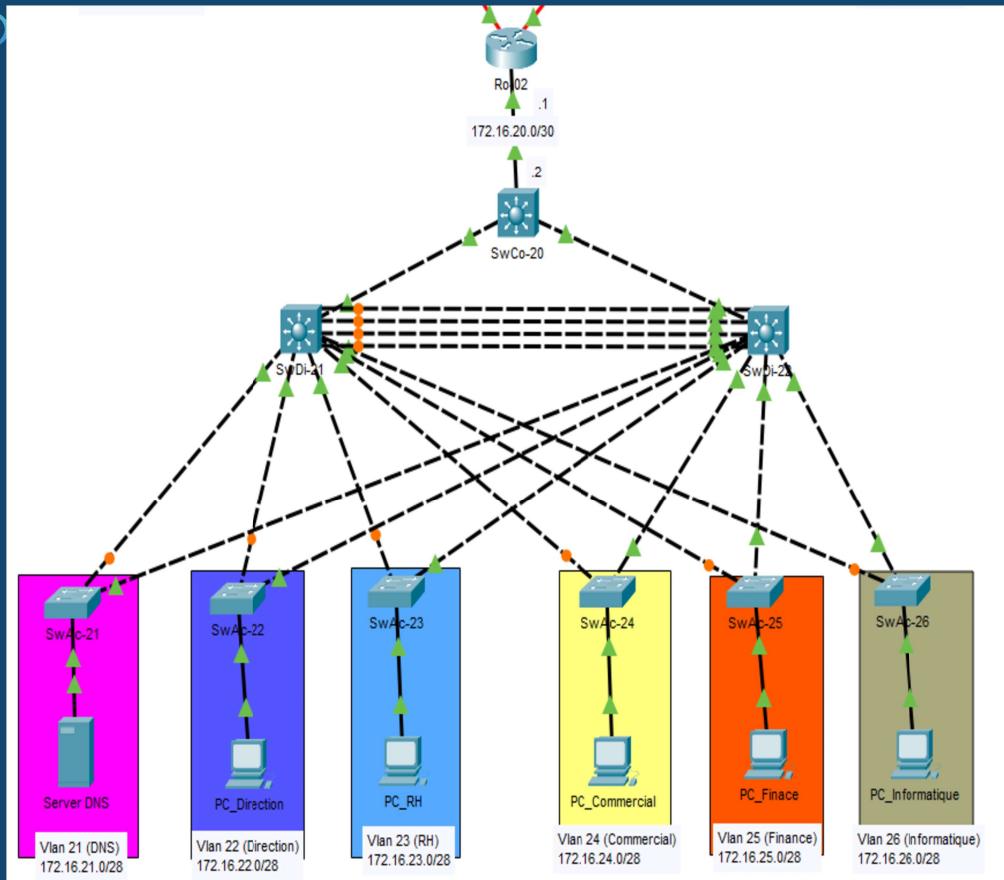
- Routage dynamique: EIGRP IPv4 et EIGRP IPv6
- IPv4, NAT surchargé, LAN vers WAN sur les interfaces séries (Fonctionnalité "route map" non disponible).
- Route statique vers switch core SwCo-20 pour les adresses IP à destination du LAN.

- **Switch SwCo-20 (Switch cœur):**

- Routage dynamique EIGRP IPv6
- SVI et passerelle par défaut pour chaque VLAN
- Fonction routage inter-vlan suivant liste d'accès

```
ip access-list extended InterVlan
  permit icmp any any echo-reply
  permit tcp any any established
  deny ip 172.16.22.0 0.0.0.255 172.16.26.0 0.0.0.255
  deny ip 172.16.23.0 0.0.0.255 172.16.26.0 0.0.0.255
  deny ip 172.16.24.0 0.0.0.255 172.16.26.0 0.0.0.255
  deny ip 172.16.25.0 0.0.0.255 172.16.26.0 0.0.0.255
  permit ip any any
```

# Réseau Bâtiment Rouge



- Switch SwDi-21 et SwDi-22 (Switch de distribution):
  - SVI pour chaque VLAN.
  - Serveurs DHCP avec des pools d'adresse pour chaque VLAN.
  - LACP sur les quatre liens entre SwDi.
- Switch SwAc-21 – SwAc-26 (Switch d'accès):
  - Interfaces en mode Access côté équipement terminaux.
  - Interfaces mode Trunk côté SwDi.

# Préconisations Techniques d'amélioration de la cybersécurité

- **Protection des flux inter-sites transitant sur un réseau tiers:**

Les flux inter-site (a minima les flux d'administration) transitant sur un réseau tiers doivent être chiffrés et authentifiés de bout en bout.

Utilisation du protocole IPsec pour établir des tunnels VPN entre chaque sites. *Application étendue de la préconisation ANSSI-PA-022 R21.*

R21

## Protéger les flux d'administration transitant sur un réseau tiers

Si les flux d'administration circulent à travers un réseau tiers ou hors de locaux avec un niveau de sécurité physique adéquat (ex : portion de fibre noire traversant l'espace public), ceux-ci doivent être chiffrés et authentifiés de bout en bout jusqu'à atteindre une autre zone du SI d'administration ou une ressource à administrer. Dans ce cas, un tunnel IPsec doit être établi.

Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [16] doivent être appliquées.

- **Gestion de l'authentification**

Mise en œuvre d'une gestion centralisée ou utilisation de certificats électroniques de confiance pour l'authentification (a minima sur les ressources d'administration). *Application étendue de la préconisation ANSSI-PA-022 R37 et R38.*

R38

## Mettre en œuvre une gestion centralisée de l'authentification

Une gestion centralisée de l'authentification doit être mise en œuvre en lieu et place d'une gestion exclusivement locale sur les ressources d'administration ou les ressources administrées.

- **Politique de sauvegarde du SI d'administration:**

Mise en place d'une politique (éléments à sauvegarder, lieu de sauvegarde, droits d'accès, procédures de restauration) et d'un système de sauvegarde du système SI d'administration. *Application de la préconisation ANSSI-PA-022 R45.*

R45

## Définir une politique de sauvegarde du SI d'administration

Pour permettre de pallier la corruption ou l'indisponibilité de données dues à un incident ou une compromission, une politique de sauvegarde doit être définie et appliquée pour le SI d'administration.

Pour les éléments les plus critiques, une sauvegarde hors ligne doit être prévue.

# Questions / Réponses

# Voies d'améliorations :