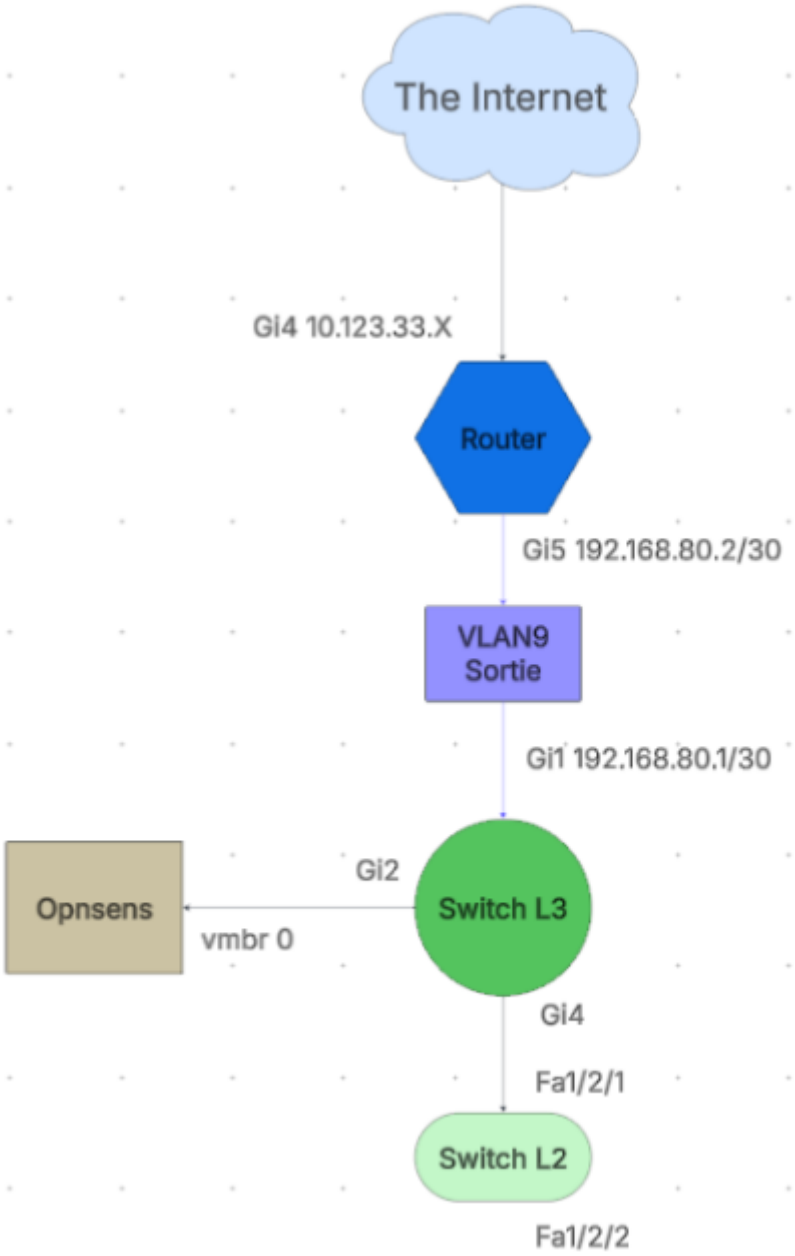
Cisco

- Config Routeur/SwitchL2-L3 AP
- Configuration SSH sur routeur
- Comment restaurer une config sur routeur/l3 et l2
- Routeur Nat interne

Config Routeur/SwitchL2-L3 AP

Rappel schéma Infra



Rappel tableau VLANS

NOM	VLAN	IP R	MASQUE	PASSERELLE	YA QUOI dd
x	1	x	x	x	x
Admin	2	.10.0	/24		Fedora d'administration
Accueil/ Visiteur	3	.20.0	/24		
Direction/DSI	4	.30.0	/24		
RH	5	.40.0	/24		
Com	6	.50.0	/24		
Commercial	7	.60.0	/24		
Démonstra / Salle réunion	8	.70.0	/24		
Sortie	9	.80.0	/30		(l3/router)
Front	10	.90.0	/28	.90.1	LAP Messaglab / Jurilab /Pglab /Labnnu/ winserv Fedora
Back	11	.100.0	/28	.100.1	BDD /Noticelab / BDmedoclab / BDmed / DBpharma dns
Sécu	12	.110.0	/29	.110.1	Logs / CL logs / Docker
OPN	13	.120.0	/30		
client X	14	.130.0	/24		

Documentation Routeur

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0	unassigned	YES	unset	down	down
GigabitEthernet1	unassigned	YES	unset	down	down
GigabitEthernet2	unassigned	YES	unset	down	down
GigabitEthernet3	unassigned	YES	unset	down	down
GigabitEthernet4	10.123.33.72	YES	DHCP	up	up
GigabitEthernet5	192.168.80.2	YES	NVRAM	up	up
NVI0	unassigned	YES	unset	up	up
Vlan1	unassigned	YES	unset	down	down
Vlan2	192.168.10.2	YES	NVRAM	down	down

Documentation Switch L3

IP Address	I/F	I/F Status admin/oper	Type	Directed Broadcast	Prec	Redirect	Status
0.0.0.0/32	vlan 1	UP/DOWN	DHCP	disable	No	enable	Not received
192.168.10.1/24	vlan 2	UP/DOWN	Static	disable	No	enable	Valid
192.168.20.1/24	vlan 3	UP/DOWN	Static	disable	No	enable	Valid
192.168.30.1/24	vlan 4	UP/DOWN	Static	disable	No	enable	Valid
192.168.40.1/24	vlan 5	UP/DOWN	Static	disable	No	enable	Valid
192.168.50.1/24	vlan 6	UP/DOWN	Static	disable	No	enable	Valid
192.168.60.1/24	vlan 7	UP/DOWN	Static	disable	No	enable	Valid
192.168.70.1/24	vlan 8	UP/DOWN	Static	disable	No	enable	Valid
192.168.80.1/30	vlan 9	UP/UP	Static	disable	No	enable	Valid
192.168.99.1/24	vlan 99	UP/DOWN	Static	disable	No	enable	Valid
192.168.250.2/29	vlan 100	UP/DOWN	Static	disable	No	enable	Valid

Vlan	Name	Tagged Ports	UnTagged Ports	Created by
1	1		gi2-3,gi5-10	D
2	2	gi2-3		S
3	3	gi3		S
4	4	gi3		S
5	5	gi3		S
6	6	gi3		S
7	7	gi3		S
8	8	gi3		S
9	9	gi2-3	gi1	S
10	10	gi2		S
11	11	gi2		S
12	12	gi2		S
13	13	gi2		S
14	14	gi2		S
99	99		gi4	S
100	100	gi2-3		S

```
S    0.0.0.0/0 [1/4] via 192.168.80.2, 01:44:04, vlan 9
S    192.168.0.0/16 [1/4] via 192.168.80.2, 01:44:04, vlan 9
C    192.168.10.0/24 is directly connected, vlan 2
C    192.168.20.0/24 is directly connected, vlan 3
C    192.168.30.0/24 is directly connected, vlan 4
C    192.168.40.0/24 is directly connected, vlan 5
C    192.168.50.0/24 is directly connected, vlan 6
C    192.168.60.0/24 is directly connected, vlan 7
C    192.168.70.0/24 is directly connected, vlan 8
C    192.168.80.0/30 is directly connected, vlan 9
S    192.168.90.0/24 [1/4] via 192.168.80.2, 00:00:39, vlan 9
S    192.168.100.0/24 [1/4] via 192.168.80.2, 00:00:21, vlan 9
S    192.168.110.0/24 [1/4] via 192.168.80.2, 00:00:18, vlan 9
S    192.168.120.0/24 [1/4] via 192.168.80.2, 00:00:14, vlan 9
S    192.168.130.0/24 [1/4] via 192.168.80.2, 00:00:05, vlan 9
C    192.168.250.0/29 is directly connected, vlan 100
```

Configuration SSH sur routeur

Routeur Cisco C921-4P

Tout se passe dans le mode configuration terminal, avec cette suite de commandes :

- **ip domain-name <nom de domaine>** : définit un nom de domaine dans lequel est le routeur, nécessaire pour configurer SSH
- **crypto key generate rsa :** génère une clé RSA
  - **How many bits in the modulus [512]: <taille de la clé>** : taille de la clé RSA à spécifier (512 est un exemple) (2048 au minimum de préférence)
- **ip ssh version 2** : active SSH
- **ip ssh logging events** : journalise les connexions SSH
- **ip ssh time-out <secondes>** : définit le temps d'inactivité avant la déconnexion d'un utilisateur qui a établi une connexion SSH sans encore s'être authentifié
- **ip ssh authentication-retries <nombre>** : définit le nombre de tentative ratées de connexion à l'utilisateur en SSH avant de le déconnecter
- **service password-encryption** : pour chiffrer le mot de passe des utilisateurs
- **username <nom d'utilisateur> password 0 <mot de passe>** : définit un utilisateur et un mot de passé associé pour la connexion SSH
- **line vty 0 3** : on entre dans la configuration de "line" en définissant le nombre de connexion distantes possibles en simultané (ici, 4)
  - "vty" : signifie les connexions à distance
  - "0 3" : pour faire très simple, le second nombre est le nombre de connexions simultanées possibles - 1 car on part de 0 (donc ici il y a 4 connexion simultanées possibles)
- (config-line) **transport input ssh** : autoriser la connexion SSH à distance
- (config-line) **login local** : définit la connexion à un compte local du routeur

Connexion SSH depuis une machine Linux (Fedora 43)

Certains éléments de connexion SSH qui sont demandés par le routeur peuvent être bloqués sur Linux. De ce fait, il faut modifier quelques éléments de configuration (ici, sur Fedora 43).
Dans le fichier /etc/ssh/ssh_config, on ajoute le contenu suivant à la fin du fichier (pour l'indentation, ne pas utiliser la tabulation, mais 4 espaces) :

```
Host 192.168.90.138
    KexAlgorithms +diffie-hellman-group1-sha1,diffie-hellman-group14-sha1
    PubkeyAcceptedAlgorithms +ssh-rsa
```

```
    PubkeyAcceptedKeyTypes +ssh-rsa
    HostKeyAlgorithms +ssh-rsa
    Ciphers aes256-ctr,3des-cbc
```

On entre la commande suivante :

```
update-crypto-policies --set DEFAULT:SHA1
```

Comment restaurer une config sur routeur/l3 et l2

AOMEI Partition assistant. pour la clé USB

Pour le routeur :

Se munir d'une clée avec une partition de moins de 2Go en FAT16 (clé PNY)

Pour copié le config avec la commande :

copy startup-config usbflash0:*nom du fichier*

Pour mettre en place la configuration sur l'élément réseau :

copy usbflash0:nom du fichier startup-config

Pour Le l3

Création interface Admin et console

Interface Admin :

int giX (entrer le port sur lequel nous voulons configurer l’interface Administrateur)

ip add 192.168.1.1 255.255.255.252 (adresse de passerelle et masque de sous-réseau recommandé)

Interface Console

Brancher le câble Ethernet sur le port console de l’équipement puis le rediriger vers une prise Ethernet de couleur sur la baie par exemple B-11 vert.

Après cela, se munir d’un ensemble USB vers VGA et VGA vers Ethernet que nous branchons sur un port USB de notre machine et à la prise Ethernet correspondant avec celle reliée dans la baie, dans notre exemple B-11 vert.

Ensuite aller sur le logiciel Putty et se mettre en serial avec la COM correspondant au port USB (voir gestionnaire des périphériques)

Routeur Nat interne

Documentation : Redirection de port sur routeur Cisco

Lister les redirections de port

Pour afficher les règles de redirection (NAT statique) actives :

```
show ip nat translations
```

Pour voir la configuration complète incluant les règles statiques :

```
show running-config | include ip nat inside source
```

Comprendre la redirection

Dans votre cas, l'accès à `10.123.33.205` redirige vers `192.168.120.2` (Proxmox) car une règle NAT statique est configurée, probablement de ce type :

```
ip nat inside source static tcp 192.168.120.2 80 10.123.33.205 80
```

Désactiver temporairement la redirection

Sur les routeurs Cisco traditionnels (IOS), il n'existe pas de commande pour désactiver temporairement une règle NAT statique sans la supprimer.
La seule solution est de **supprimer** la règle, puis de la **réinsérer** si besoin.

Supprimer la règle :

```
configure terminal
no ip nat inside source static tcp 192.168.120.2 [port] 10.123.33.205 [port]
```

> Exemple : `no ip nat inside source static tcp 192.168.120.2 80 10.123.33.205 80`

Réactiver plus tard :

Réexécutez la commande NAT sans `no`.

Sauvegarder :

```
write memory
```

Remarque

Sur les équipements **Cisco ASA/Firepower** (avec interface graphique), il est possible de **désactiver** une règle NAT sans la supprimer via une option *Enable/Disable*. Cette fonctionnalité **n’existe pas sur les routeurs Cisco IOS classiques**.