



1. OBJECTIF DU PROJET

Cette infrastructure permet :

- La segmentation réseau avec des VLANs
- Le routage inter-VLAN
- La distribution automatique des adresses IP (DHCP)
- La sécurisation des équipements via SSH
- La traduction d'adresses NAT
- La redondance Layer 2 avec PVSTP
- L'agrégation de liens avec EtherChannel LACP
- Le routage dynamique OSPF
- Le filtrage réseau avec ACL

- La sécurisation des ports avec Port-Security
- L'accès au serveur Web depuis tous les réseaux

ÉTAPE 1 — Configuration des Hostnames

Objectif

Attribuer un nom à chaque équipement afin de faciliter l'administration réseau.

Router0

```
enable  
configure terminal  
hostname R-TEHRAN
```

Explication

- enable → passe en mode privilégié
 - configure terminal → passe en mode configuration globale
 - hostname → change le nom de l'équipement
-

Switch Core L3

```
enable  
configure terminal  
hostname SW-CORE
```

Switch Access

```
enable
configure terminal
hostname SW-ACCESS
```

ÉTAPE 2 — Configuration SSH + Bannière MOTD

Objectif

Sécuriser l'accès distant des équipements.

Configuration SSH complète

```
configure terminal

ip domain-name tehran.local

username admin privilege 15 secret Cisco123!

crypto key generate rsa
1024

ip ssh version 2

line vty 0 15
login local
transport input ssh
exit
```

Explication des commandes

Commande	Rôle
ip domain-name	Définit le domaine utilisé pour générer les clés RSA
username	Crée un utilisateur local
secret	Définit un mot de passe chiffré

Commande	Rôle
crypto key generate rsa	Génère les clés RSA nécessaires à SSH
ip ssh version 2	Active SSH version 2
line vty	Configure les accès distants
login local	Utilise la base locale des utilisateurs
transport input ssh	Autorise uniquement SSH

Bannière MOTD

```
banner motd #  
ACCES INTERDIT AUX PERSONNES NON AUTORISEES  
#
```

Explication

Affiche un message légal lors de la connexion.

ÉTAPE 3 — Création des VLANs

Objectif

Segmenter le réseau afin d'isoler les différents services.

Création des VLANs

```
vlan 10  
name USERS
```

```
vlan 20  
name RH
```

```
vlan 30  
name FINANCE
```

vlan 40
name ADMIN

Explication

VLAN Fonction

VLAN10 Utilisateurs

VLAN20 Ressources humaines

VLAN30 Finance

VLAN40 Administrateurs

Affectation des ports

interface fa0/1
switchport mode access
switchport access vlan 10

interface fa0/2
switchport mode access
switchport access vlan 20

interface fa0/3
switchport mode access
switchport access vlan 30

interface fa0/6
switchport mode access
switchport access vlan 40

Explication

Commande	Rôle
switchport mode access	Configure le port en mode accès
switchport access vlan X	Affecte le port au VLAN

Configuration Trunk

```
interface range fa0/3 - 4  
switchport mode trunk
```

Explication

Le trunk transporte plusieurs VLANs entre les switches.

ÉTAPE 4 — DHCP sur le Switch Layer 3

Objectif

Distribuer automatiquement les adresses IP.

Activation du routage

```
ip routing
```

Explication

Permet le routage inter-VLAN sur le switch L3.

Configuration des interfaces VLAN

```
interface vlan 10  
ip address 192.168.10.1 255.255.255.0  
no shutdown
```

```
interface vlan 20  
ip address 192.168.20.1 255.255.255.0  
no shutdown
```

```
interface vlan 30
ip address 192.168.30.1 255.255.255.0
no shutdown
```

```
interface vlan 40
ip address 192.168.40.1 255.255.255.0
no shutdown
```

Explication

Les interfaces VLAN deviennent les passerelles des PCs.

Exclusion des adresses réservées

```
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
```

DHCP Pools

VLAN10

```
ip dhcp pool VLAN10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
```

VLAN20

```
ip dhcp pool VLAN20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 8.8.8.8
```

VLAN30

```
ip dhcp pool VLAN30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 8.8.8.8
```

VLAN40

```
ip dhcp pool VLAN40
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
dns-server 8.8.8.8
```

ÉTAPE 5 — NAT sur Router0

Objectif

Permettre aux réseaux privés d'accéder à Internet.

Interface LAN

```
interface g0/0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
no shutdown
```

Interface WAN

```
interface g0/0/1
ip address 200.1.1.1 255.255.255.252
ip nat outside
no shutdown
```

ACL NAT

```
access-list 1 permit 192.168.0.0 0.0.255.255
```

Activation NAT Overload

```
ip nat inside source list 1 interface g0/0/1 overload
```

Route par défaut

```
ip route 0.0.0.0 0.0.0.0 200.1.1.2
```

ÉTAPE 6 — EtherChannel LACP

Objectif

Augmenter la bande passante et fournir de la redondance.

Configuration LACP

```
interface range fa0/3 - 4  
channel-group 1 mode active
```

Interface logique Port-Channel

```
interface port-channel 1  
switchport mode trunk
```

Explication

Commande	Rôle
----------	------

channel-group	Crée EtherChannel
---------------	-------------------

mode active	Active LACP
-------------	-------------

port-channel	Interface logique agrégée
--------------	---------------------------

ÉTAPE 7 — Accès au serveur Web

Configuration du serveur

IP : 192.168.1.100
MASK : 255.255.255.0
GATEWAY : 192.168.1.1

Route par défaut du switch L3

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ÉTAPE 8 — ACL VLAN20 ↔ VLAN30

Objectif

Empêcher VLAN20 et VLAN30 de communiquer.

ACL

```
access-list 110 deny icmp 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
```

```
access-list 110 deny icmp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
access-list 110 permit ip any any
```

Application ACL

```
interface vlan 20  
ip access-group 110 in
```

```
interface vlan 30  
ip access-group 110 in
```

ÉTAPE 9 — Admin peut tout ping

Explication

Le VLAN40 ne possède aucune ACL restrictive.

Donc :

- L'administrateur peut accéder à tous les réseaux
 - Tous les équipements peuvent être administrés
-

ÉTAPE 10 — Description des interfaces

Objectif

Faciliter le dépannage et la documentation.

Exemple

```
interface g0/0/0
description LINK_TO_CORE_SWITCH
```

```
interface g0/0/1
description LINK_TO_INTERNET
```

```
interface fa0/1
description PC_VLAN10
```

ÉTAPE 11 — Port Security

Objectif

Empêcher les connexions non autorisées.

Configuration

```
interface fa0/1
switchport mode access

switchport port-security
switchport port-security maximum 1

switchport port-security mac-address sticky

switchport port-security violation shutdown
```

Explication

Commande Rôle

maximum 1 Une seule MAC autorisée

sticky Apprend automatiquement la MAC

shutdown Désactive le port si violation

ÉTAPE 12 — Protection des interfaces VLAN

Objectif

Empêcher les utilisateurs de ping les gateways.

ACL

```
access-list 120 deny icmp any 192.168.10.1 0.0.0.0
```

```
access-list 120 deny icmp any 192.168.20.1 0.0.0.0
```

```
access-list 120 deny icmp any 192.168.30.1 0.0.0.0
```

```
access-list 120 permit ip any any
```

Application

```
interface vlan 10  
ip access-group 120 in
```

```
interface vlan 20  
ip access-group 120 in
```

```
interface vlan 30  
ip access-group 120 in
```

IMPORTANT

Ne PAS appliquer ACL120 sur VLAN40 (ADMIN).

3. CONFIGURATION — SITE ESFEHAN

ÉTAPE 1 — Hostname

```
hostname R2  
hostname R3  
hostname R4  
hostname R5
```

ÉTAPE 2 — SSH

Même configuration SSH que Tehran.

ÉTAPE 3 — OSPF

Objectif

Permettre le routage dynamique entre les routeurs.

Configuration OSPF

```
router ospf 1  
  
router-id 1.1.1.1  
  
network 12.1.1.0 0.0.0.3 area 0  
network 192.168.23.0 0.0.0.3 area 0  
network 192.168.25.0 0.0.0.3 area 0  
network 192.168.34.0 0.0.0.3 area 0  
network 192.168.43.0 0.0.0.3 area 0
```

Explication

Élément	Fonction
router ospf 1	Lance OSPF
router-id	Identifiant unique
network	Active OSPF sur les interfaces

ÉTAPE 4 — Accès PC5 au Web Server

Route par défaut

```
ip route 0.0.0.0 0.0.0.0 12.1.1.1
```

Routes de retour

```
ip route 192.168.200.0 255.255.255.0 12.1.1.2
```

```
ip route 192.168.201.0 255.255.255.0 12.1.1.2
```

```
ip route 192.168.202.0 255.255.255.0 12.1.1.2
```

ÉTAPE 5 — PVSTP + Root Bridge

Objectif

Éviter les boucles Layer 2.

Activation PVST

```
spanning-tree mode pvst
```

Définition Root Bridge

```
spanning-tree vlan 1 priority 4096
```

Vérifications importantes

show vlan brief

show ip route

show ip ospf neighbor

show etherchannel summary

show spanning-tree

show port-security

show ip nat translations
