Rapport Technique Complet : Configuration LAN + WAN + VMs:

Sommaire

1. Introduction:

Ce TP a pour objectif de mettre en place un réseau hybride complet, comprenant : - un LAN interne segmenté en VLANs avec trunk et router-on-a-stick ; - un accès WAN simulé ou un accès Internet réel ;

- deux machines virtuelles Windows sous VMware ;

- un PC physique connecté au LAN ;

- une configuration IP statique puis DHCP ;

- des tests de connectivité complets (ping, tracert, DNS, gateway).

L'objectif final est de valider l'architecture réseau en assurant la communication entre tous les éléments du LAN et vers le WAN.

2. Matériel et logiciels utilisés:

Matériel :

- Routeur Cisco 1841/1941

- Switch Cisco 2960

- 2 PC physiques sous Windows

- Câbles RJ45 droits

- Box Internet

Logiciels :

- VMware Workstation / Player (1 VM par PC)

- Windows 10/11

- Putty

- Windows CMD / PowerShell

3. Topologie du Réseau:

Le réseau sera divisé en 2 VLANs (1 par PC) :

VLAN Nom Sous-réseau Rôle
VLAN Nom Sous-réseau Rôle
10 VLAN-PC1 192.168.10.0/24 PC physique 1 + VM1 20
VLAN-PC2 192.168.20.0/24 PC physique 2 + VM2

Le routeur effectuera :

- le routage inter-VLAN (router-on-a-stick) ;

- le NAT / PAT vers le WAN ;

- le DHCP pour chaque VLAN.

Chaque PC physique héberge **une VM** dans le même VLAN que le PC. 4. Câblage Physique:

4.1 Branchement du switch

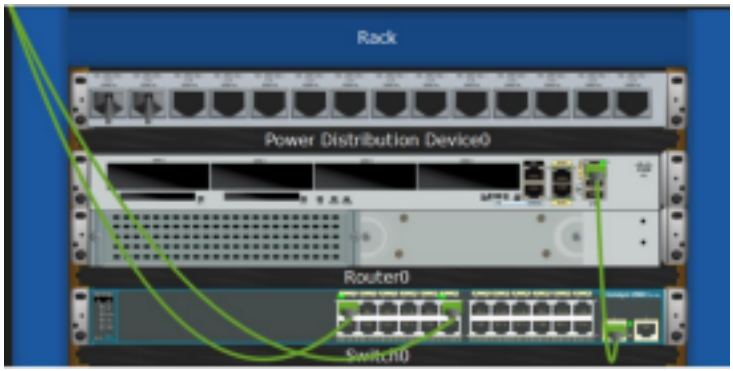
1. Brancher le **câble d'alimentation** du switch Cisco 2960. 2. Attendre le **boot complet** (LED vertes stables).
3. Brancher un câble RJ45 du **PC administrateur** vers **Fa0/1**. 4.2 Branchement du routeur
1. Alimenter le routeur 1841/1941.
2. Attendre la fin du démarrage.
3. Connecter via console au PC administrateur.
4. **Câbler G0/1 du routeur → G0/1 du switch** (trunk).

4.3 Branchement WAN

1. Prendre un câble RJ45.
2. Le connecter : Routeur **G0/0 → Box Internet (LAN 1)**.
3. Vérifier que la box distribue bien du DHCP.
4. Vérifier les LED de liaison :
    - Vert fixe = OK.
    - Clignotement = trafic.

4.4 Branchement PC physiques et VMs

• PC physique 1 → switch (Fa0/2), VLAN 10, VM1 en **Bridged** → VLAN 10 • PC physique 2 → switch (Fa0/3), VLAN 20, VM2 en **Bridged** → VLAN 20 • Chaque VM se comporte comme un PC réel dans son VLAN respectif



5. Configuration COMPLET du Switch Cisco:

```
enable
configure terminal

! VLANs
vlan 10
 name VLAN-PC1
exit
vlan 20
 name VLAN-PC2
exit

! Trunk vers routeur
interface GigabitEthernet0/1
 switchport mode trunk
 switchport trunk encapsulation
 dot1q switchport trunk allowed vlan
 10,20
 spanning-tree portfast trunk
exit

! Ports access
interface GigabitEthernet0/2
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
exit

interface GigabitEthernet0/3
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
exit

end
```

```
write memory
```

6. Configuration COMPLETE du Routeur Cisco:

```
enable
configure terminal

! Interfaces physiques
interface GigabitEthernet0/0
 ip address dhcp
 no shutdown
exit

interface GigabitEthernet0/1
 no shutdown
exit

! Router-on-a-stick
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
exit

interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
exit

! DHCP
ip dhcp excluded-address 192.168.10.1
192.168.10.20 ip dhcp excluded-address
192.168.20.1 192.168.20.20

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
exit

ip dhcp pool VLAN20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 1.1.1.1
exit

! NAT
interface GigabitEthernet0/0
 ip nat outside
```

```
exit
interface GigabitEthernet0/1
 ip nat inside
exit

access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255

ip nat inside source list 1 interface GigabitEthernet0/0 overload

end
write memory
```

7. Configuration VMware (Deux VMs):

7.1 Paramétrage réseau des VMs

1. Ouvrir VMware pour chaque PC.
2. Sélectionner la VM → Settings.
3. Network Adapter → choisir **Bridged**.
4. Cocher : *Replicate physical network connection state*. 5. Démarrer la VM.

7.2 Configuration IP statique:

Dans Windows → Paramètres → Réseau → Modifier les options d'adaptateur. 1. Clic droit → Propriétés.

2. IPV4 → Propriétés.

3. Renseigner :

- VM1 : IP 192.168.10.50, VLAN 10

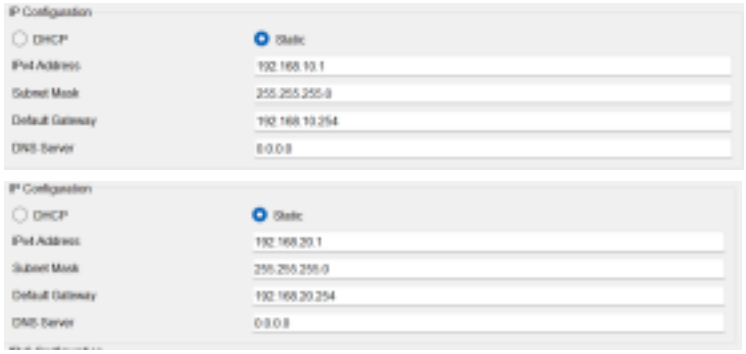
- VM2 : IP 192.168.20.50, VLAN 20

- Mask : 255.255.255.0

- Passerelle : 192.168.10.1 / 192.168.20.1

- DNS : 8.8.8.8

4. Entrer.



7.3 Configuration DHCP:

Dans IPV4 → Propriétés → sélectionner :

- Obtenir une adresse IP automatiquement

- Obtenir les DNS automatiquement

Faire :

```
ipconfig /release
ipconfig /renew
```

Résultat attendu :

- Adresse dans le bon VLAN

- Passerelle correcte

- DNS conforme au pool DHCP

7.4 Désactivation du pare-feu Windows

Pour éviter que les communications LAN/WAN soient bloquées par le pare-feu :

1. Sur chaque PC et VM, ouvrir **Panneau de configuration → Système et sécurité → Pare-feu Windows Defender → Activer ou désactiver le pare-feu**.
2. Désactiver le pare-feu pour **Réseau privé et public**.

8. Tests de connectivité:

8.1 Tests LAN

1. `ping` entre PC et VM dans le même VLAN → OK

2. `ping` inter-VLAN via routeur → OK

8.2 Test DHCP

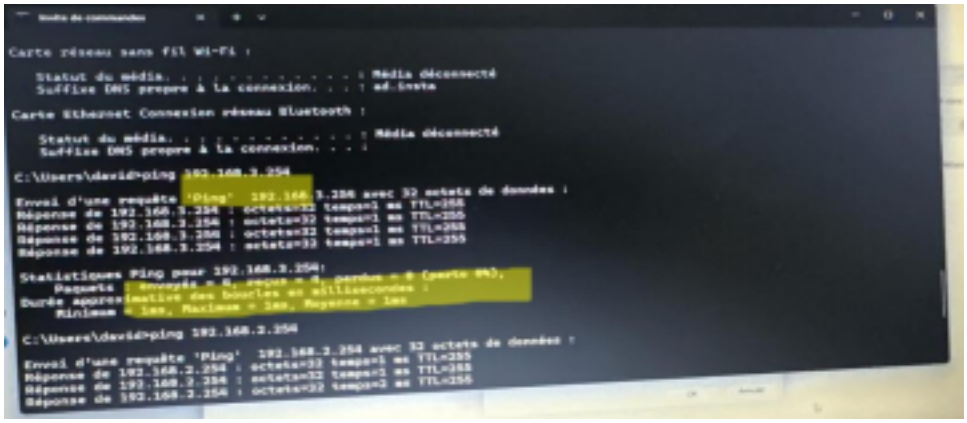
1. `ipconfig /release` / `renew`
2. Vérifier la plage DHCP
3. Vérifier la passerelle
4. Vérifier le DNS

8.3 Tests WAN + NAT

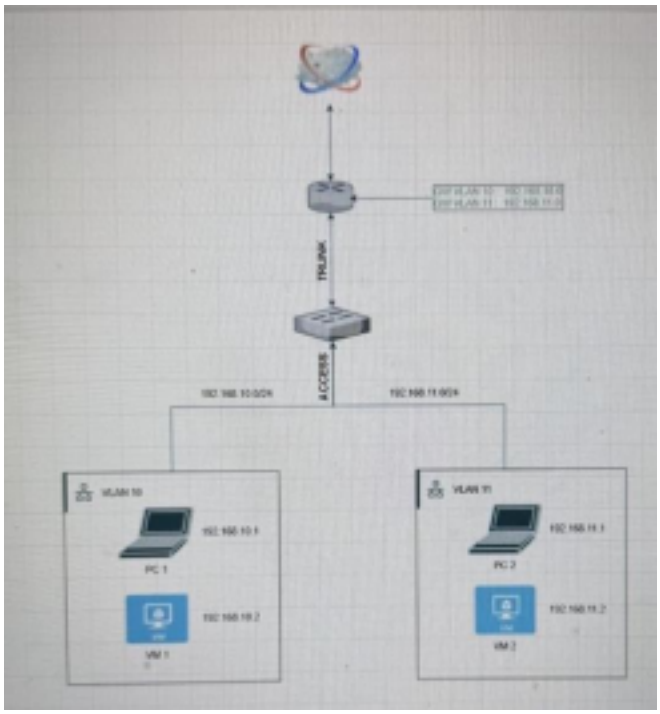
1. `ping 8.8.8.8` → OK
2. `ping google.com` → nécessite DNS
3. Sur routeur :

```
show ip nat translations
```

→ doit afficher les translations PAT.



9. Schéma réseau:



10. Emplacements Captures d’écran

10. Conclusion

Le réseau LAN/WAN est entièrement fonctionnel, segmenté en 2 VLANs (1 par PC), routé par router-on-a-stick, et testé avec deux PC physiques chacun hébergeant une VM. Le DHCP, NAT, routage et accès Internet ont été validés. Ce document constitue une référence complète et détaillée pour toute reproduction du réseau.