Bilel RAHMOUNI

Implémentation de SNMP et Syslog

Topologie :

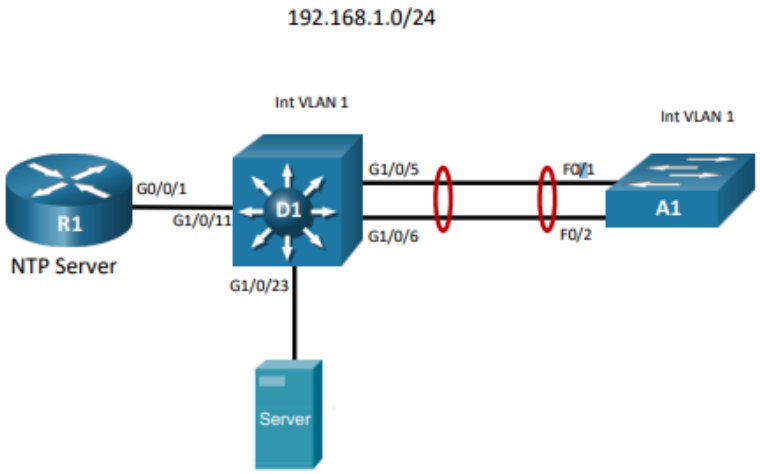


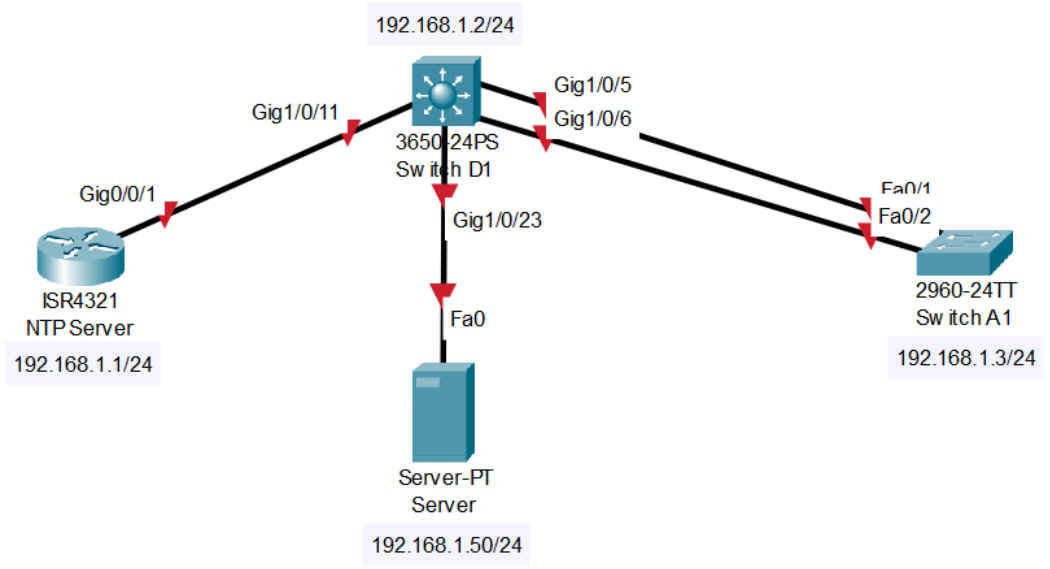
Table d'adressage :

Device	Interface	IP Adress
R1	G0/0/1	192.168.1.1/24
D1	VLAN 1	192.168.1.2/24
A1	VLAN 1	192.168.1.3/24
Server	NIC	192.168.1.50/24

Étape 1 : Construire le réseau et configurer les paramètres de base ainsi que l'adressage des interfaces.

Topologie physique :

- On connecte les appareils (routeur, switchs, et serveur) comme indiqué sur le schéma fourni.
- Utilisez les ports spécifiés dans le tableau d'adressage.



Configuration sur chaque appareil :

Accédez au mode de configuration globale en exécutant la commande suivante :

```
configure terminal
```

- **R1 (Router) :**

Définir le nom de la machine :

```
hostname R1
```

Configurez l'interface G0/0/1 avec l'adresse IP :

```
interface g0/0/1
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
```

Configurez le NTP :

```
ntp server 192.168.1.50
end
```

- **D1 (Switch 3650) :**

Configuration du nom de la machine :

```
hostname D1
```

Configurez VLAN 1 avec l'adresse IP :

```
interface vlan 1
ip address 192.168.1.2 255.255.255.0
no shutdown
exit
```

Configuration des différentes interfaces :

```
ip default-gateway 192.168.1.50
interface g1/0/23
switchport mode access
no shutdown
exit

interface g1/0/11
switchport mode access
no shutdown
exit

interface range g1/0/5-6
switchport mode trunk
channel-group 1 mode active
no shutdown
exit

interface range g1/0/1-4, g1/0/7-10, g1/0/12-22, g1/0/24, g1/1/1-4
shutdown
exit
```

Configurez le NTP :

```
ntp server 192.168.1.50
end
```

- **A1 (Switch 2960) :**

Configuration du nom de la machine :

```
hostname A1
```

Configurez VLAN 1 avec l'adresse IP :

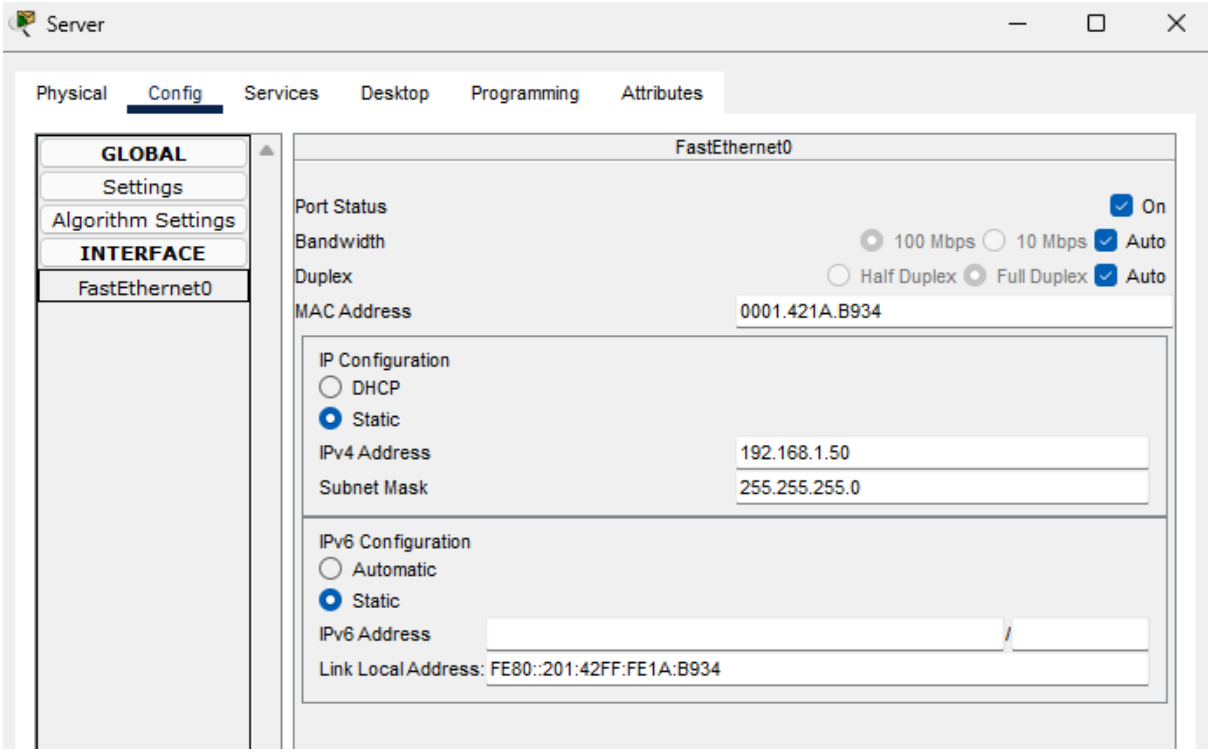
```
no ip domain lookup

interface vlan 1
ip address 192.168.1.3 255.255.255.0
no shutdown
exit

ip default-gateway 192.168.1.1
interface range f0/1-2
switchport mode trunk
channel-group 1 mode active
no shutdown
exit

interface range f0/3-24, g0/1-2
shutdown
exit
```

Configurez le NTP :

```
ntp server 192.168.1.50
end
```

- **Server :**

On s'occupe de mettre en place l'adresse IP dans l'interface graphique :



Vérification que les différents appareils peuvent ping le server sur l'adresse 192.168.1.50 :

R1 :

```
R1>ping 192.168.1.50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

D1 :

```
Switch>ping 192.168.1.50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

A1 :

```
A1>ping 192.168.1.50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Étape 2 : Configuration et vérification de SNMP

Étape 1 : Configuration des communautés SNMP

1. **Activer SNMPv2c sur les appareils** :

Accédez au mode de configuration globale sur chaque appareil (R1, D1, et A1) :

```
configure terminal
```

Configurer les chaînes de communauté :

Configurez une communauté en lecture seule (`RO`) appelée `EFREI` :

```
snmp-server community EFREI RO
```

Configurez une communauté en lecture-écriture (`RW`) appelée `EFREI-RS` :

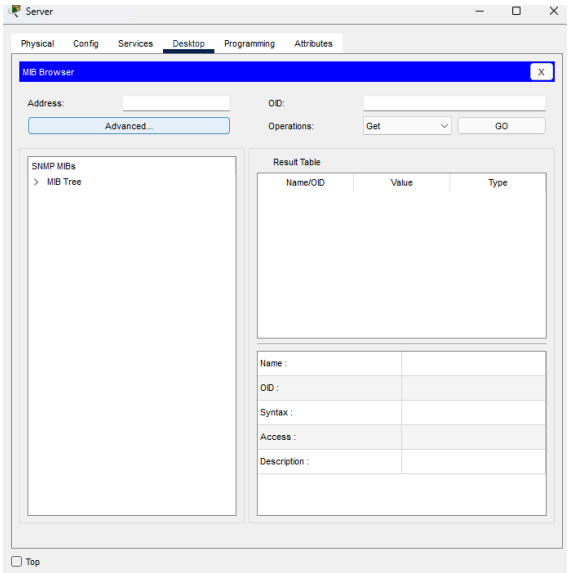
```
snmp-server community EFREI-RS RW
```

Sortir du mode de configuration :

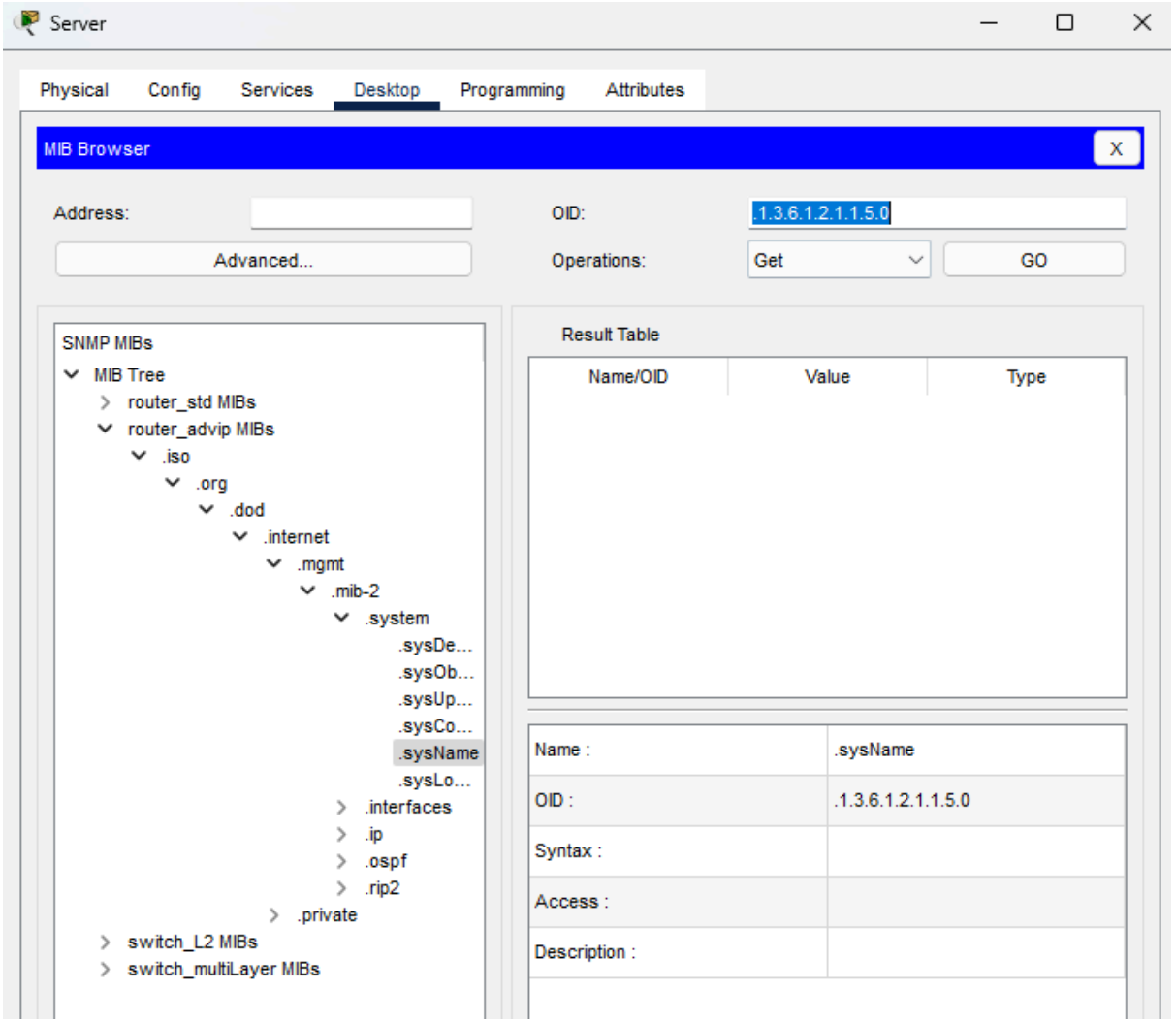
```
end
```

Étape 2 : Requêtes SNMP

1. **Sur le serveur** :
    - Accédez à l'onglet **Desktop** sur le serveur dans Cisco Packet Tracer.
2. **Lancer le navigateur MIB** :
    - Ouvrez l'application MIB Browser.



3. **Effectuer une requête SNMP** :
    - Entrez l'OID (Object Identifier) de votre choix dans la section de requête.
    - Cliquez sur **Get** pour obtenir les informations associées à l'OID.



4. **Vérification** :
    - Recherchez l'OID contenant le nom du routeur.
    - Effectuez une requête SNMP pour changer le nom du routeur via l'OID correspondant.

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>snmpget
SNMP GET Utility

Usage:
To run the command:
       snmpget /v (1|2|3) /a ADDRESS /c COMMUNITY /o OID
To display the result:
       snmpget /d

C:\>snmpget /v 2 /a 192.168.1.1 /c EFREI /o .1.3.6.1.2.1.1.5.0
C:\>snmpget /d
.1.3.6.1.2.1.1.5.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysName.0)
OctetString
R1
```

5. **Cherchez l'OID qui contient le nom du routeur, faites une requête snmpset pour changer le nom du routeur. Vérifier que ce dernier à bien changé sur le routeur.**

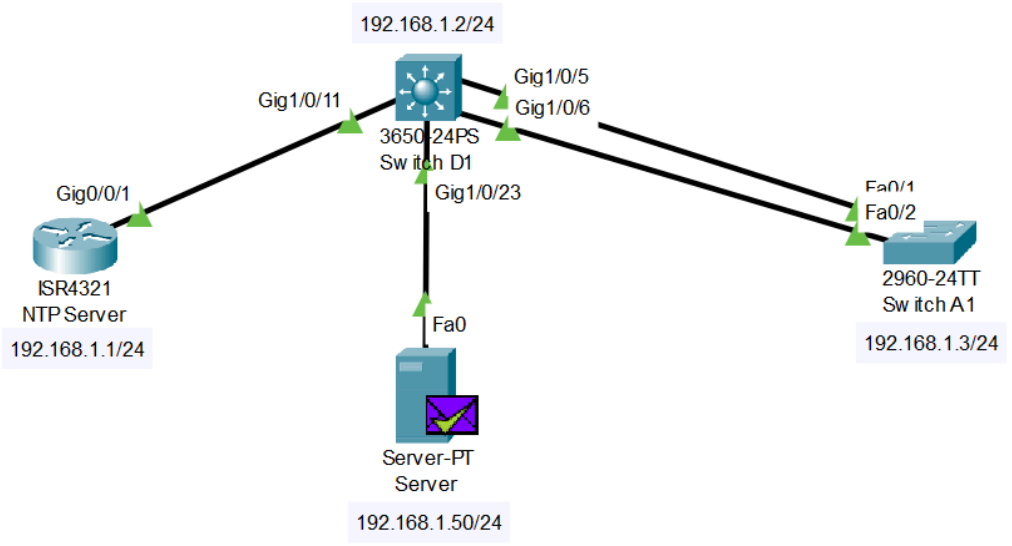
```
C:\>snmpset /v 2 /a 192.168.1.1 /c EFREI-RS /o .1.3.6.1.2.1.1.5.0 /t OctetString /v "R1-
NewName"
```

Et maintenant on vérifie que le nom a bien été changé.

```
C:\>snmpget /d
.1.3.6.1.2.1.1.5.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysName.0)
OctetString
R1-NewName
```

Étape 3 : Analyse des échanges SNMP

1. **Mode Simulation** :
    - Activez le mode simulation dans Cisco Packet Tracer pour observer les échanges SNMP entre les appareils et le serveur.
2. **Exécuter des requêtes SNMP** :
    - Effectuez des requêtes depuis le navigateur MIB en mode simulation.
    - Analysez les paquets SNMP échangés dans la fenêtre de simulation.
3. **Revenir en mode réel** :
    - Une fois l'analyse terminée, repassez en mode **Realtime** pour continuer les autres configurations.



Étape 3 : Configuration de Syslog

Step 1: buffered logging

Configurer le tampon de journalisation :

Accédez au mode de configuration globale sur chaque appareil (R1, D1, et A1) et augmentez la taille du tampon à 16 384 octets.

Commande à exécuter :

```
configure terminal
logging buffered 16384
end
```

Vérifier la configuration du tampon :
Utilisez la commande suivante pour confirmer la configuration :

```
show logging
```

Cette commande affichera les détails du tampon de journalisation et les messages enregistrés.

```
R1-NewName#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-NewName(config)#logging buffered 16384
R1-NewName(config)#end
```

Step 2: Configuration du service Syslog

On procède ensuite par la définition de l'adresse du serveur Syslog :

```
configure terminal
logging host 192.168.1.50
end
write memory
```

Step 3: Vérification de la configuration

Ensuite, on vérifie la configuration des appareils en vérifiant que les logs sont bien actifs grace a cette commande :

```
enable
show logging
```

```
R1-NewName#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 9 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 9 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  level debugging, 0 messages logged, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
    Trap logging: level informational, 9 message lines logged
        Logging to 192.168.1.50  (udp port 514,  audit disabled,
              authentication disabled, encryption disabled, link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
Log Buffer (16384 bytes):
```

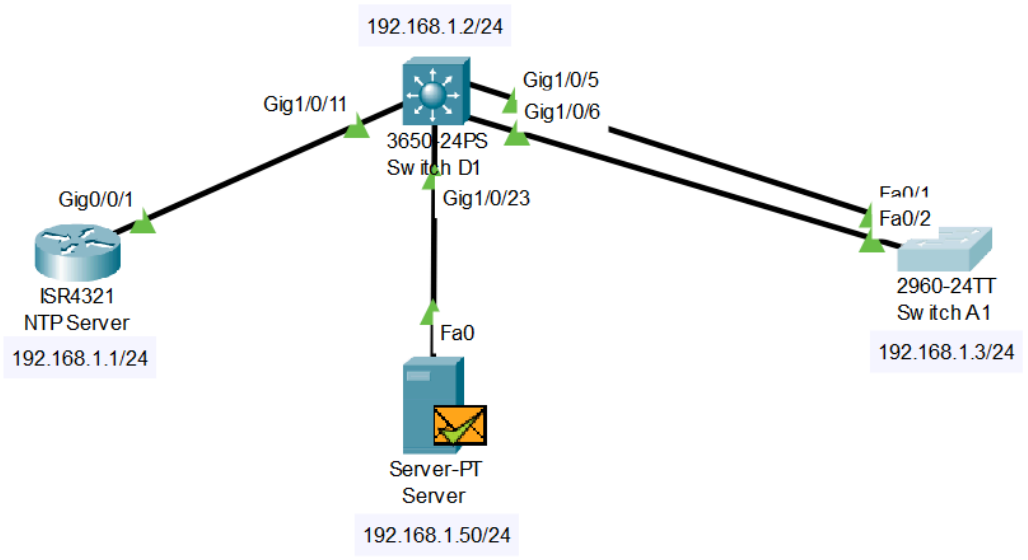
Step 4: Analyse d'échange

On réalise une action qui génère des logs pour tester. Ici, dans notre exemple on active l'interface Fa0/3 sur le switch A1 :

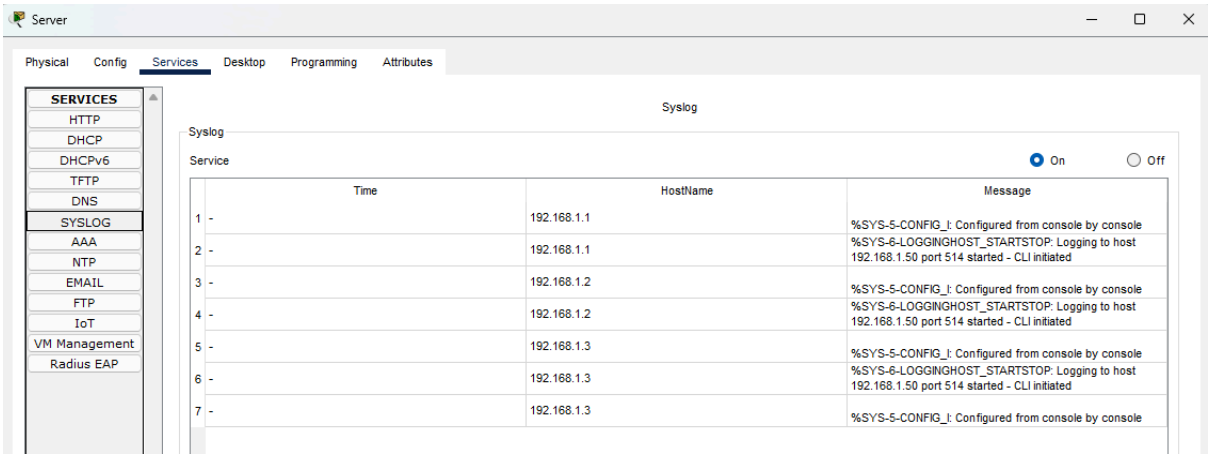
```
enable
```

```
conf t
interface Fa0/3
no shutdown
exit
write memory
```

On observe que le SYSLOG arrive bien a la machine en mode simulation :



Et quand on appuie sur le serveur on vérifie que les logs sont bien arrivés :



Step 5 : Vérification du service Syslog

On remarque qu'on ne reçoit pas les dates des logs, on active donc l'horodatage des logs sur les trois équipements avec cette commande :

```
enable
conf t
service timestamps log datetime msec
exit
write memory
```

On voit bien que les logs générés actuellement sur le R1 sonts bien horodatés :

```
R1-NewName>enable
R1-NewName#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-NewName(config)#service timestamps log datetime msec
R1-NewName(config)#exit
R1-NewName#write memory
Building configuration...
[OK]
R1-NewName#
*Mar 01, 03:05:12.055: SYS-5-CONFIG_I: Configured from console by console
```

Et on voit que sur le serveur Syslog les logs sont maintenant bien datés :

6	-	192.168.1.3	%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.50 port 514 started - CLI ...
7	-	192.168.1.3	%SYS-5-CONFIG_I: Configured from console ...
8	03.01.1993 03:05:12.413 AM	192.168.1.1	%SYS-5-CONFIG_I: Configured from console by console
9	01.27.2025 04:56:28.519 PM	192.168.1.2	%SYS-5-CONFIG_I: Configured from console by console
10	01.27.2025 04:56:40.992 PM	192.168.1.3	%SYS-5-CONFIG_I: Configured from console by console