Mini Project Report: SSH, SNMP, Syslog and NTP Configuration on Cisco Router

Student: Hassi Imad-Eddine

Course: SSH&SNMP / Mini Proiject

Tool: Cisco Packet Tracer

1. Project Objective

The objective of this mini project is to build a simple LAN in Cisco Packet Tracer and configure secure and monitored access to a Cisco router using:

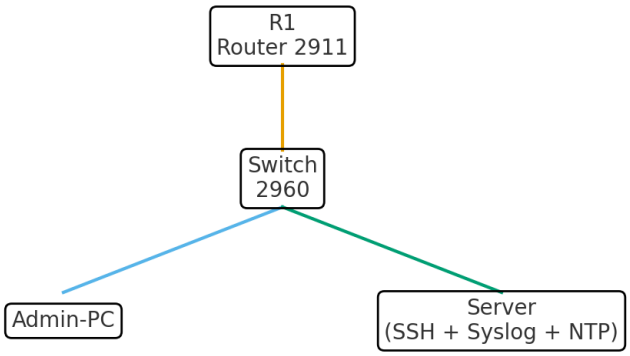
- SSH (Secure Shell) for remote management
- SNMP for monitoring and traps
- Syslog for centralized logging
- NTP for time synchronization

2. Network Topology and IP Plan

Devices used in Packet Tracer:

- Router: Cisco 2911 (R1)
- Switch: Cisco 2960
- PC: Admin-PC
- Server: Multi-service server (Syslog + NTP + SSH)

Figure 1 – Logical Network Topology



(Figure 1: Network topology in Packet Tracer showing R1, Switch, Admin-PC, and Server connected in a LAN)

2.1 IP Addressing Plan

- **R1 G0/0:** 192.168.1.1 / 255.255.255.0
- **Admin-PC Fa0:** 192.168.1.10 / 255.255.255.0, Gateway 192.168.1.1
- **Server Fa0:** 192.168.1.20 / 255.255.255.0, Gateway 192.168.1.1

3. Router Basic Configuration

Commands on R1:

```
enable
configure terminal
hostname R1
no ip domain-lookup
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
exit
enable secret imad1234
service password-encryption
end
write memory
```

Explanation:

Set the hostname, disable DNS lookup, configure the LAN interface with IP 192.168.1.1, enable the interface, configure an encrypted enable password and encrypt all plain-text passwords.

4. SSH Configuration with Access Restriction

Commands on R1:

```
enable
configure terminal
ip domain-name imadhassi.com
crypto key generate rsa modulus 1024
ip ssh version 2
username hassi privilege 15 secret imadhassi123
access-list 1 permit host 192.168.1.10
line vty 0 4
 transport input ssh
 login local
 access-class 1 in
 exec-timeout 10 0
exit
end
```

```
write memory
```

Explanation:

Define a domain name and generate RSA keys for SSH, force SSH version 2, create a local admin user, create ACL 1 to permit only Admin-PC (192.168.1.10), and configure VTY lines to use SSH only, use local login, apply ACL 1 and an idle timeout.

5. SNMP Configuration on R1

Commands on R1:

```
enable
configure terminal
snmp-server community Cisco1 RO
snmp-server community Cisco2 RW
snmp-server host 192.168.1.20 Cisco1
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps config
snmp-server enable traps snmp authentication
end
write memory
```

Explanation:

Enable SNMP on the router by creating two communities: Cisco1 (read-only) and Cisco2 (read-write), define the server (192.168.1.20) as the SNMP trap receiver using community Cisco1, and enable traps for interface up/down, configuration changes, and SNMP authentication failures.

Note: In Packet Tracer, the generic Server does not provide an SNMP Manager GUI. SNMP is therefore validated using router show commands such as 'show snmp' and 'show snmp community'.

6. Syslog Configuration

On the Server (192.168.1.20):

Enable the Syslog service from the Services tab.

On R1:

```
enable
configure terminal
logging 192.168.1.20
logging trap 4
service timestamps log datetime msec
end
write memory
```

Explanation:

The router sends log messages to 192.168.1.20. 'logging trap 4' sets the severity level to 4 (warnings) and above, and timestamps are added to each log message.

7. NTP Configuration (Time Synchronization)

On the Server:

Enable the NTP service from the Services tab so it acts as an NTP server.

On R1:

```
enable
configure terminal
clock timezone CET 1 0
ntp server 192.168.1.20
ntp update-calendar
end
write memory
```

Explanation:

Set the timezone to CET (UTC+1), use the server 192.168.1.20 as the NTP server, and update the router hardware calendar from NTP.

8. Testing and Verification

Main tests performed:

- Ping between Admin-PC and Router, and between Admin-PC and Server.
- SSH from Admin-PC to R1 using the local user 'hassi'.
- SSH from Admin-PC to the Server (if SSH is enabled on the server).
- Use 'show snmp' and 'show snmp community' on R1 to verify SNMP.
- Generate interface up/down events to see Syslog messages on the Server.
- Use 'show clock' on R1 to check that time is synchronized with the NTP server.

9. Conclusion

This mini project shows how to build a small network in Cisco Packet Tracer and configure secure remote access with SSH, monitoring with SNMP, centralized logging with Syslog and accurate time with NTP.