Lab 6

IPSec VPN

**Lab Instructions:**

Before connecting any routers, ensure that the IOS version on each one supports

encryption. This can be done by running the following command:

Router# show version

The IOS name in the output must contain “K9”.

**Objective 1: Site to Site VPN**

Make changes to the previous lab and create the following network

A picture containing indoor, green, skiing, table

Description automatically generated

Create the following loopbacks:

R3: 20.20.10.2/24 (PC1)

R7: 20.20.20.2/24 (PC2)

R4: 50.50.50.2/24

20.20.40.2/24

R6: 20.20.30.2/24 (PC3)

Objective 1:

1. Create an IPSec tunnel between the following routers (Attach a screenshot of the configuration and the Security Associations)

R3 – R7

R7-R6

R3-R6

R6 – R4

1. Achieve full network connectivity. (Each loopback should be able to ping every other loopback in the network)
2. Traffic between routers which are connected through a VPN tunnel should go encrypted (e.g. When pinging the loopback on R7 from loopback on R3, traffic should go encrypted but when pinging the loopback on R4, traffic should go cleartext)

For part 3, attach a screenshot showing that traffic is going encrypted

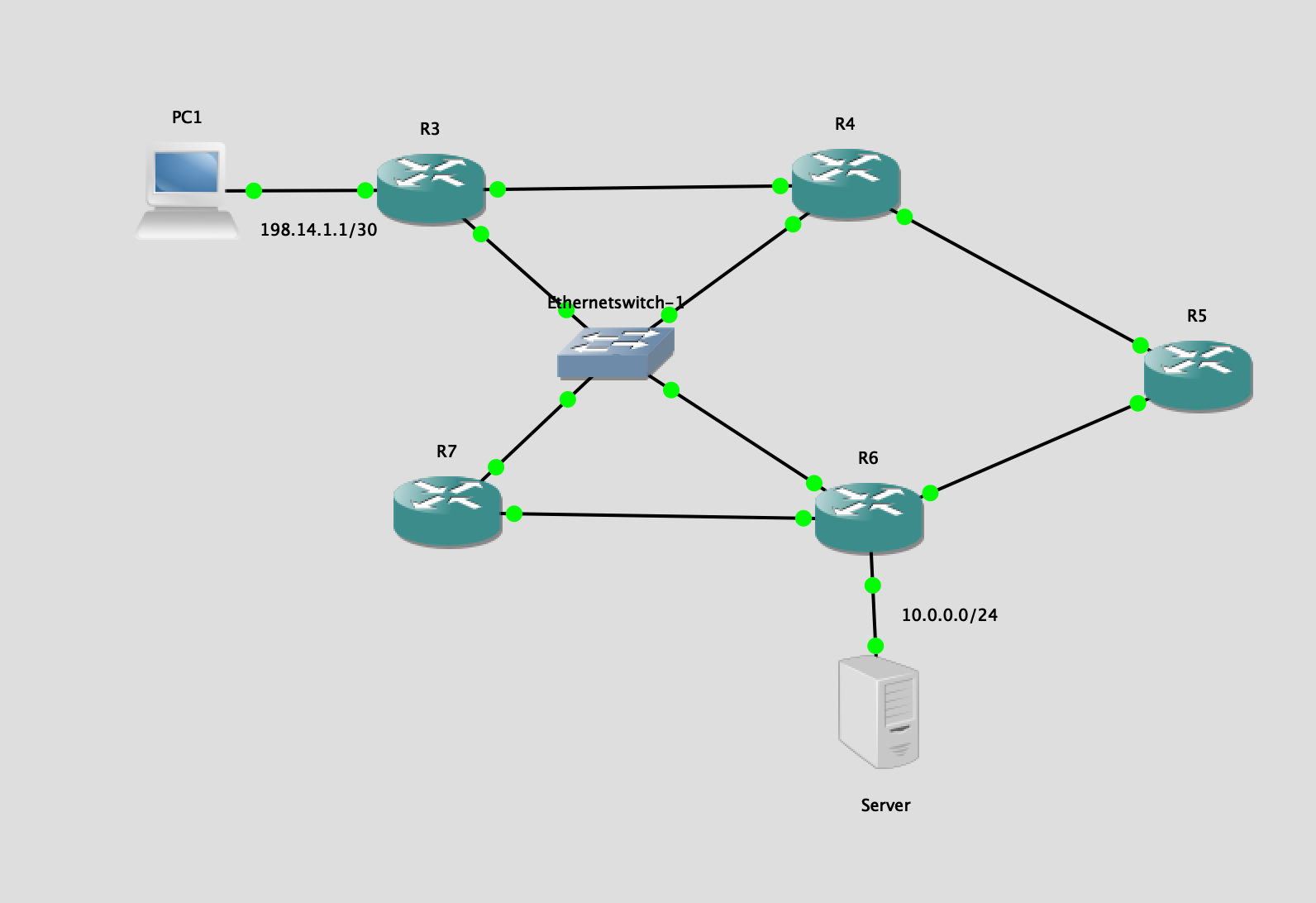
1. Run a capture on the switch and see the packets that are exchanged before and after the VPN is established. Include in your report the Wireshark captures.

**Objective 2: Remote VPN**

In this part you need to create a “Remote VPN” or “Easy VPN”. The client (PC1) needs to access the server. PC1 is a windows VM that has a Cisco VPN client installed on it.

Users belonging to the public network 178.168.1.16/30 should be able to

remote VPN into the 10.0.0.0 network



**Objective 3: DMVPN**

1. Clear configurations from the previous objective.
2. Consider R4 as the hub router and R3, R5 and R7 as the spoke routers.
3. Configure the crypto and tunnel on the Spoke router & HUB router, which effectively deploys DMVPN between the Spoke and Hub.
4. Attach the crypto and NHRP configurations, and various

“show” commands to troubleshoot and verify Spoke-Hub connectivity & tunnel

formation.

Following are some of the helpful ‘show’ commands:

showdmvpn

showipnhrp

showip route

show crypto isakmpsa

show crypto ipsecsa

Refer the following link for DMVPN configurations:

<https://www.gns3.com/marketplace/lab/dmvpn-ipsec>