Faculty of Informatics and Computer Science
Dr. Marwa Zamzam
Eng. Salma Abou Bakr

Network Security, ICS 605
Spring Semester 2024
Assignment 1

Network Security |Assignment 1
Deadline: April 15, 2024
Team of 3

Deliverables:

1. Report: This should include a screenshot of the **Whole WINDOW** displaying all of your configurations along with all the commands.
2. You are required to save and upload the **Packet Tracer File** named **"yourname.pka".**
3. Evaluation will occur during Lab 7
4. Submission should be made through this link: **https://forms.gle/gnykx5EUb32Shkp8A**

Question 1: Inter-LAN Connectivity Setup with Enhanced Security Measures.

The aim is to establish connectivity between two PCs located in different LANs while implementing enhanced security measures to ensure secure access and communication. Each PC will be connected to a separate router, and the routers will be configured to facilitate communication between the PCs. The following security configurations will be applied to both routers:

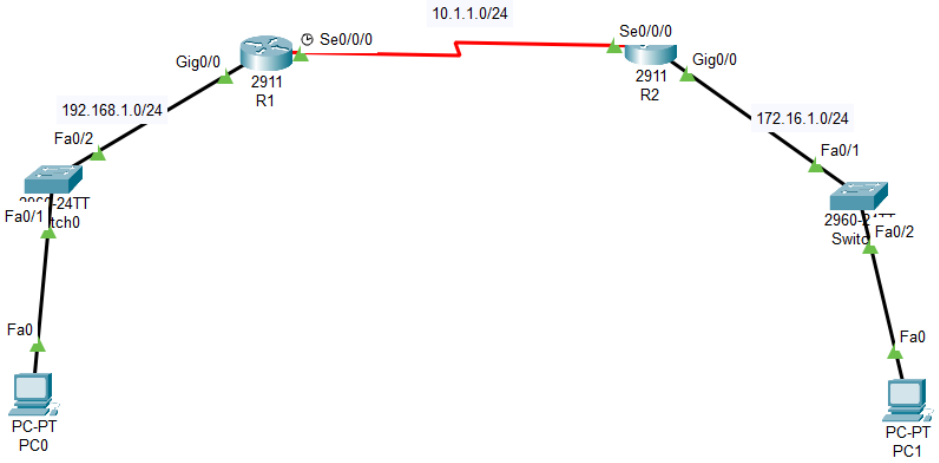


Figure 1: Topology 1

1. **Set Minimum Password Length on R1 and R2:**
   - Configure routers to enforce a minimum password length of 10 characters.

2. **Assign and Encrypt Privileged EXEC Password on R1 and R2:**
   - Set the privileged EXEC password to "cisco12345" and encrypt it to ensure secure access to privileged mode.

3. **Add User in Local Database on R1 and R2 for Administrator Access:**
    - Create a user named "admin01" with privilege level 15 and set the password to "admin01pass" to provide administrator access.
    - Create a user named "admin02" with privilege level 15 and set the password to "admin02pass" to provide administrator access.

4. **Configure SSH:**
    - Enable IP addresses (as shown in Figure 1) for PCs and configure SSH to provide secure remote access.
    - Set the domain name to "netsec.com" and generate RSA keys with a size of 1024 bits on R1 and R2.
    - Configure SSH timeout to 90 seconds and authentication retries to 2 for enhanced security on R1 and R2.

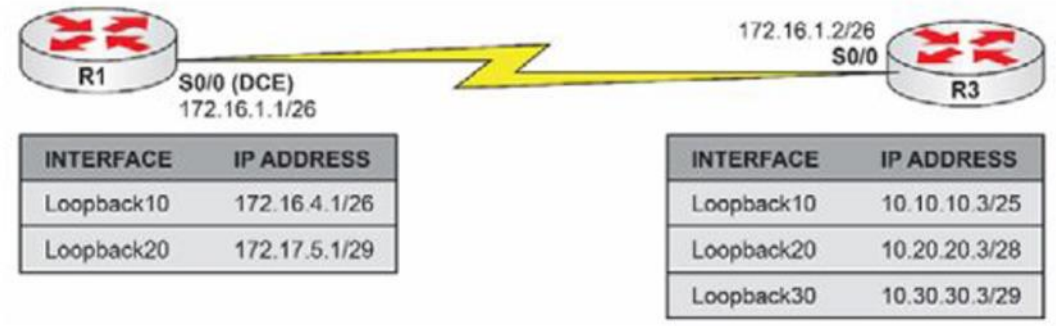
5. **Configure AAA Authentication Settings on R1 and R2:**
    - Enable AAA authentication.
    - Use the local database as the default authentication method.
    - Enable case-sensitive local username authentication for added security.
    - Implement enhanced login settings to block access for three minutes after four failed attempts within a two-minute period.

6. **Encrypt All Passwords on R1 and R2:**
    - Ensure all passwords are encrypted to prevent unauthorized access to sensitive information.

7. **Configure VTY Lines for SSH Access on R1 and R2:**
    - Configure access to routers' VTY lines to allow SSH access only.

8. **Verify SSH Access to Routers from PCs:**
    - Test SSH access from each PC to their respective routers (R1 and R2) to ensure successful connectivity and authentication.

Question 2 (Bonus): Create and apply extended numbered access control lists. Please use the following topology to complete the following tasks:



INTERFACE	IP ADDRESS
Loopback10	172.16.4.1/26
Loopback20	172.17.5.1/29

INTERFACE	IP ADDRESS
Loopback10	10.10.10.3/25
Loopback20	10.20.20.3/28
Loopback30	10.30.30.3/29

a) Configure the host names on routers R1 and R3 as illustrated in the topology.

b) Configure R1 serial port, which is a DCE, to provide a clock rate of 768 Kbps to R3.

c) Configure a static default route on R1 pointing to R3 over the Serial connection between the two routers. Also, configure a static default route on R3 pointing to R1 via the Serial connection between the two routers. Configure the IP addresses on the Serial interfaces of R1 and R3 as illustrated in the topology.

d) Configure the IP addresses on the Loopback interfaces specified in the diagram on R1 and R3.

e) Configure both R1 and R3 to allow SSH connections. The password *CISCO* should be used for SSH access.

f) Configure a numbered extended ACL on R3 to allow Telnet from R1 Loopback10 to R3 Loopback20 and Loopback30. Add another line to the extended ACL to only allow ping traffic from R1 Loopback20 to R3 Loopback10. Apply this ACL inbound on R3 Serial port.

g) Test your Telnet ACL configuration, telnet from R1 Loopback10 to R3 Loopback10, Loopback20, and Loopback30.

h) Test your ping ACL configuration, ping from R1 Loopback20 to R3 Loopback10, Loopback20, and Loopback30.