**Q1. Create the following topology and ♣ Configure an ACL that will permit FTP and HTTP access on R1. ♣ Verify the ACL implementation. PC1 (Only FTP). PC2(Only HTTP)**

**🔧 Network Topology Configuration Steps**

**🖥️ PC1 Configuration:**

1. **Open Desktop > IP Configuration**
2. **Set IP Address: 172.22.34.66**
3. **Subnet Mask: 255.255.255.224**
4. **Default Gateway: 172.22.34.65**

**🖥️ PC2 Configuration:**

1. **Open Desktop > IP Configuration**
2. **Set IP Address: 172.22.34.98**
3. **Subnet Mask: 255.255.255.240**
4. **Default Gateway: 172.22.34.97**

**🖥️ Server Configuration:**

1. **Open Desktop > IP Configuration**
2. **Set IP Address: 172.22.34.62**
3. **Subnet Mask: 255.255.255.192**
4. **Default Gateway: 172.22.34.1**
5. **Enable both FTP and HTTP services from Services tab**

**📡 Router R1 Interface Configuration:**

1. **Go to CLI mode**
2. **Enter global configuration mode: conf t**
3. **Configure Interfaces:**
   * **interface gig0/0**
     + **ip address 172.22.34.65 255.255.255.224**
     + **no shutdown**
   * **interface gig0/1**
     + **ip address 172.22.34.97 255.255.255.240**
     + **no shutdown**
   * **interface gig0/2**
     + **ip address 172.22.34.1 255.255.255.192**
     + **no shutdown**

**✅ Save configuration: exit → wr**

**🔒 ACL Configuration on R1**

**🎯 Objective:**

* **PC1 should have access to FTP (port 21) only**
* **PC2 should have access to HTTP (port 80) only**

**🔧 Steps to Configure ACL:**

1. **Go to CLI mode → conf t**
2. **Create ACL:**
   * **access-list 100 permit tcp 172.22.34.66 0.0.0.0 any eq ftp**
   * **access-list 100 permit tcp 172.22.34.98 0.0.0.0 any eq www**
   * **access-list 100 deny ip any any**
3. **Apply ACL to outgoing interface towards the server:**
   * **interface gig0/2**
   * **ip access-group 100 out**

**✅ Save configuration: exit → wr**

**🧪 Verification Steps**

**🖥️ From PC1:**

* **Open web browser → Enter Server IP → ❌ Should not open HTTP**
* **Use FTP client → Connect to Server IP → ✅ FTP should work**

**🖥️ From PC2:**

* **Open web browser → Enter Server IP → ✅ HTTP should work**
* **Use FTP client → Connect to Server IP → ❌ Should be blocked**

**Q2. ♣ Configure OSPF MD5 authentication ♣ Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA. ♣ Verify local AAA authentication from the R1 console and the PC0 client and PC1 Client.**

🌐 Network Topology Setup

🖥️ PC0 Configuration:

1. Go to Desktop > IP Configuration
2. Set IP Address: 192.168.1.2
3. Set Subnet Mask: 255.255.255.0
4. Set Default Gateway: 192.168.1.1

🖥️ PC1 Configuration:

1. Go to Desktop > IP Configuration
2. Set IP Address: 192.168.1.3
3. Set Subnet Mask: 255.255.255.0
4. Set Default Gateway: 192.168.1.1

📡 Router R1 Configuration (Interface):

1. Go to CLI mode
2. Enter global config mode: conf t
3. Configure Interface:
   * interface gig0/0
   * ip address 192.168.1.1 255.255.255.0
   * no shutdown
4. ✅ Save configuration: exit → wr

🔐 OSPF MD5 Authentication Configuration

🧾 Objective: Secure OSPF using MD5 authentication.

🔧 Steps:

1. Enable OSPF:
   * router ospf 1
   * network 192.168.1.0 0.0.0.255 area 0
2. Enable MD5 authentication on the interface:
   * Go to interface gig0/0
   * Enable MD5:
     + ip ospf message-digest-key 1 md5 cisco
     + ip ospf authentication message-digest
3. ✅ Save configuration: exit → wr

👤 Local AAA User Authentication Configuration

🎯 Objective: Use a local user account for console and VTY line access.

🔧 Steps:

1. Create a local user account:
   * username Devshree privilege 15 secret Solanki
2. Enable AAA:
   * aaa new-model
3. Configure console line authentication:
   * line console 0
   * login local
   * exit
4. Configure VTY line authentication:
   * line vty 0 4
   * login local
   * exit
5. Set Enable password for AAA:
   * enable secret 123
6. ✅ Save configuration: exit → wr

🧪 Verification of Local AAA Authentication

🖥️ From Router Console (R1):

* When reconnecting via console, router should prompt for username and password.
* Enter:
  + Username: Devshree
  + Password: Solanki
* ✅ Successful login confirms AAA on console working.

🖥️ From PC0 and PC1 via Telnet:

1. Open Desktop > Terminal or use Telnet from Command Prompt.
2. Type: telnet 192.168.1.1
3. Enter credentials:
   * Username: Devshree
   * Password: Solanki
4. ✅ Access should be granted.

📝 Note: Make sure Telnet is enabled on the router if testing from PC:

* line vty 0 4
* transport input telnet

**Practical 3 1. Create the following topology and ♣ Configure an ACL that will permit one LAN to remotely access device in another LAN using SSH Protocol ♣ Besides ICMP all traffic from other network is denied. ♣ Verify the ACL implementation.**

**Part 1**

**Step 1: Create the Topology**

You need the following devices based on your addressing table:

* **Router RTA** with 3 interfaces: gig0/0, gig0/1, and gig0/2
* **PCs PCA and PCB**
* **Switches SWA, SWB, SWC**

Make sure the devices are connected according to the addressing table.

**Step 2: Configure IP addresses on RTA**

1. **Configure IP addresses on the router interfaces**:

bash

CopyEdit

RTA(config)# interface gig0/0

RTA(config-if)# ip address 10.101.117.49 255.255.255.248

RTA(config-if)# no shutdown

RTA(config-if)# exit

RTA(config)# interface gig0/1

RTA(config-if)# ip address 10.101.117.33 255.255.255.240

RTA(config-if)# no shutdown

RTA(config-if)# exit

RTA(config)# interface gig0/2

RTA(config-if)# ip address 10.101.117.1 255.255.255.224

RTA(config-if)# no shutdown

RTA(config-if)# exit

**Step 3: Configure IP addresses on PCs and Switches**

* **PCA**:
  + IP: 10.101.117.51, Subnet Mask: 255.255.255.248, Gateway: 10.101.117.49
* **PCB**:
  + IP: 10.101.117.35, Subnet Mask: 255.255.255.240, Gateway: 10.101.117.33
* **SWA**:
  + IP: 10.101.117.50, Subnet Mask: 255.255.255.248, Gateway: 10.101.117.49
* **SWB**:
  + IP: 10.101.117.34, Subnet Mask: 255.255.255.240, Gateway: 10.101.117.33
* **SWC**:
  + IP: 10.101.117.2, Subnet Mask: 255.255.255.224, Gateway: 10.101.117.1

**Part 2**

**1. ACL Configuration for SSH, ICMP**

**Router> enable  
Router# config t  
Enter configuration commands, one per line. End with CNTL/Z.  
  
! Create ACL to allow SSH, ICMP and deny other traffic  
Router(config)# access-list 100 permit tcp host 10.101.117.51 host 10.101.117.33 eq 22  
Router(config)# access-list 100 permit icmp host 10.101.117.51 any  
Router(config)# access-list 100 permit icmp host 10.101.117.35 any  
Router(config)# access-list 100 deny ip any any  
  
! Apply ACL to interfaces  
Router(config)# interface gig0/0  
Router(config-if)# ip access-group 100 in  
Router(config-if)# exit  
  
Router(config)# interface gig0/1  
Router(config-if)# ip access-group 100 in  
Router(config-if)# exit  
  
Router(config)# do wr  
Building configuration...  
[OK]  
  
Router(config)# exit**

**2. Testing the Configuration**

**PC0 (10.101.117.51):  
ssh -l Piyush 10.101.117.33 => success (SSH access allowed)  
ping 10.101.117.33 => success (ICMP allowed)  
telnet 10.101.117.33 => denied (Telnet is denied)  
  
PC1 (10.101.117.35):  
ssh -l Piyush 10.101.117.33 => denied (SSH is denied)  
ping 10.101.117.33 => success (ICMP allowed)  
telnet 10.101.117.33 => success (Telnet is allowed)  
  
! Show ACL on Router  
Router# show access-lists 100**

**Q4. Create the following topology using static routing**

**1. Configure the extended ACL**

**2. Verify the extended ACL implementation.**

**Step-by-Step CLI Commands for Full Configuration**

**PC0 Configuration (Click PC0 > Desktop > IP Configuration)**

**IP Address: 10.101.117.51**

**Subnet Mask: 255.255.255.248**

**Default Gateway: 10.101.117.49**

**PC1 Configuration (Click PC1 > Desktop > IP Configuration)**

**IP Address: 10.101.117.35**

**Subnet Mask: 255.255.255.240**

**Default Gateway: 10.101.117.33**

**SWA Configuration**

**enable**

**configure terminal**

**interface vlan 1**

**ip address 10.101.117.50 255.255.255.248**

**no shutdown**

**exit**

**ip default-gateway 10.101.117.49**

**end**

**SWB Configuration**

**enable**

**configure terminal**

**interface vlan 1**

**ip address 10.101.117.34 255.255.255.240**

**no shutdown**

**exit**

**ip default-gateway 10.101.117.33**

**end**

**SWC Configuration**

**enable**

**configure terminal**

**interface vlan 1**

**ip address 10.101.117.2 255.255.255.224**

**no shutdown**

**exit**

**ip default-gateway 10.101.117.1**

**end**

**Router RTA Configuration**

**enable**

**configure terminal**

**interface g0/0**

**ip address 10.101.117.49 255.255.255.248**

**no shutdown**

**exit**

**interface g0/1**

**ip address 10.101.117.33 255.255.255.240**

**no shutdown**

**exit**

**interface g0/2**

**ip address 10.101.117.1 255.255.255.224**

**no shutdown**

**exit**

**! Optional static routes (not needed but for exam)**

**ip route 10.101.117.48 255.255.255.248 g0/0**

**ip route 10.101.117.32 255.255.255.240 g0/1**

**ip route 10.101.117.0 255.255.255.224 g0/2**

**! ACL Configuration**

**access-list 100 permit icmp host 10.101.117.51 host 10.101.117.35**

**access-list 100 deny ip any any**

**! Apply ACL on g0/0 (inbound)**

**interface g0/0**

**ip access-group 100 in**

**exit**

**end**

**Verification Commands**

**ping 10.101.117.35 ← from PC0 ✅ should work**

**ping 10.101.117.51 ← from PC1 ❌ should fail**

**show access-lists**

**show running-config**