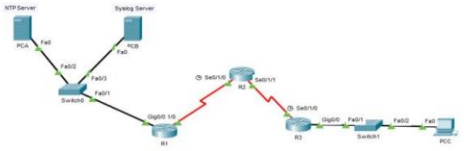
Seat No: _____ Max. Marks: 50

1. Create the following topology and — 40
   - Configure OSPF MD5 authentication.
   - Configure NTP and configure routers to log messages to the Syslog Server



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1

Here's a **step-by-step guide** to perform the tasks shown in the PDF.

✅ Task 1: Configure OSPF MD5 Authentication

Step 1: Assign IP Addresses to Interfaces

R1 Configuration:

enable

conf t

interface gig0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.1.1.1 255.255.255.252

no shutdown

exit

R2 Configuration:

enable

conf t

interface se0/1/0

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

interface se0/1/1

ip address 10.2.2.2 255.255.255.252

no shutdown

exit

R3 Configuration:

enable

conf t

interface gig0/0

ip address 192.168.3.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.2.2.1 255.255.255.252

no shutdown

exit

Step 2: Enable OSPF and Set MD5 Authentication

R1 Configuration:

enable

conf t

router ospf 1

network 192.168.1.0 0.0.0.255 area 0

network 10.1.1.0 0.0.0.3 area 0

exit

interface se0/1/0

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 password123

exit

R2 Configuration:

enable

conf t

router ospf 1

network 10.1.1.0 0.0.0.3 area 0

network 10.2.2.0 0.0.0.3 area 0

exit

interface se0/1/0

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 password123

exit

interface se0/1/1

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 password123

exit

R3 Configuration:

enable

conf t

router ospf 1

network 192.168.3.0 0.0.0.255 area 0

network 10.2.2.0 0.0.0.3 area 0

exit

interface se0/1/0

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 password123

exit

✅ **Task 2: Configure NTP and Syslog**

Step 1: Configure NTP on All Routers

R1, R2, R3 Configuration:

enable

conf t

ntp server 192.168.1.5

exit

- **192.168.1.5** is the IP of the NTP server.

Step 2: Configure Syslog Logging

R1, R2, R3 Configuration:

enable

conf t

logging host 192.168.1.10

logging trap informational

exit

- **192.168.1.10** is the IP of the Syslog server.

✅ **Task 3: Configure PCs with IP and Gateway**

PC-A:

- IP: 192.168.1.5
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.1.1

PC-B:

- IP: 192.168.1.6
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.1.1

PC-C:

- IP: 192.168.3.5
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.3.1

✅ **Verification**

Check OSPF Neighbors:

show ip ospf neighbor

Check Routing Table:

show ip route

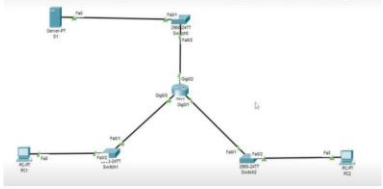
Verify NTP:

show ntp status

Verify Syslog:

show logging

Let me know if this works or if you need any troubleshooting assistance!

1.	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)  **Addressing Table** **Device** / **Interface** / **IP Address** / **Subnet Mask** / **Default Gateway** R1 / gig0/0 / 172.22.34.65 / 255.255.255.224 / N/A R1 / gig0/1 / 172.22.34.97 / 255.255.255.240 / N/A R1 / gig0/2 / 172.22.34.1 / 255.255.255.192 / N/A Server / NIC / 172.22.34.62 / 255.255.255.192 / 172.22.34.1 PC1 / NIC / 172.22.34.66 / 255.255.255.224 / 172.22.34.65 PC2 / NIC / 172.22.34.98 / 255.255.255.240 / 172.22.34.97	40
2.	Viva	5
3.	Journal	5

Here's a **step-by-step guide** to perform the tasks shown in the new PDF.

✅ Task 1: Configure IP Addresses on Interfaces

R1 Configuration:

enable

conf t

interface gig0/0

ip address 172.22.34.65 255.255.255.224

no shutdown

exit

interface gig0/1

ip address 172.22.34.97 255.255.255.240

no shutdown

exit

interface gig0/2

ip address 172.22.34.33 255.255.255.192

no shutdown

exit

✅ **Task 2: Configure ACL to Permit FTP and HTTP**

Step 1: Define Access Control List (ACL) on R1

Permit FTP for PC1:

enable

conf t

ip access-list extended FTP_HTTP_ACL

permit tcp host 172.22.34.66 any eq ftp

deny tcp host 172.22.34.66 any eq http

Permit HTTP for PC2:

permit tcp host 172.22.34.98 any eq http

deny tcp host 172.22.34.98 any eq ftp

Apply ACL to the Interfaces:

interface gig0/0

ip access-group FTP_HTTP_ACL in

exit

interface gig0/1

ip access-group FTP_HTTP_ACL in

exit

✅ **Task 3: Configure and Verify FTP and HTTP on the Server**

Step 1: Enable FTP and HTTP Services on the Server

- Go to **Server**.
- Enable **FTP** and **HTTP** services.

✅ **Task 4: Configure IP and Gateway on PCs**

PC1:

- IP: 172.22.34.66
- Subnet Mask: 255.255.255.224
- Gateway: 172.22.34.65

PC2:

- IP: 172.22.34.98
- Subnet Mask: 255.255.255.240
- Gateway: 172.22.34.97

✅ Task 5: Verification

Check ACL Configuration:

show access-lists

Check Interface Status:

show ip interface brief

Test FTP and HTTP Access:

- **PC1:** Test FTP by opening the FTP client and accessing the server.
- **PC2:** Test HTTP by using a browser or HTTP client.

Verify ACL Logs:

show ip access-list

🔍 Troubleshooting Tips:

1. Check if ACL is applied correctly to the interfaces:

show run interface gig0/0

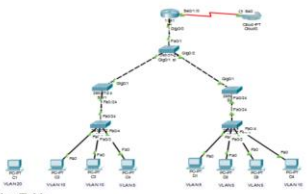
show run interface gig0/1

2. Make sure FTP and HTTP services are running on the server.
3. Use ping to test connectivity between PCs and the server.

Let me know if this works or if you need help troubleshooting!

1. Create the following topology and **40**

- Connect a new redundant link between SW-1 and SW-2.
- Enable trunking and configure security on the trunk link.
- Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
- Verify connectivity of the management PC to all switches.
- Implement an ACL to prevent outside users from accessing the management VLAN



Addressing Table

Devices	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/1			
	se0/0/0	209.165.200.1	255.255.255.0	N/A
C2	NIC	192.168.10.1	255.255.255.0	192.168.10.100
C3	NIC	192.168.10.2	255.255.255.0	192.168.10.100
C4	NIC	192.168.5.1	255.255.255.0	192.168.5.100
D1	NIC	192.168.5.2	255.255.255.0	192.168.5.100
D2	NIC	192.168.5.3	255.255.255.0	192.168.5.100
D3	NIC	192.168.5.4	255.255.255.0	192.168.5.100
D4	NIC	192.168.10.3	255.255.255.0	192.168.10.100

Here's a **step-by-step guide** to perform the tasks described in your latest PDF.

✅ Task 1: Connect a Redundant Link Between SW-1 and SW-2

Step 1: Configure Trunking Between Switches

On **SW-1**:

enable

conf t

interface range gig0/1 - 2

switchport mode trunk

switchport trunk allowed vlan all

exit

On **SW-2**:

enable

conf t

interface range gig0/1 - 2

switchport mode trunk

switchport trunk allowed vlan all

exit

✅ Task 2: Enable Trunking and Configure Security on Trunk Link

Step 1: Configure Native VLAN and Security

On both SW-1 and SW-2:

interface gig0/1

switchport trunk native vlan 99

switchport trunk allowed vlan all

switchport mode trunk

exit

Step 2: Secure the Trunk Link

interface gig0/1

switchport nonegotiate

spanning-tree portfast trunk

exit

✅ **Task 3: Create Management VLAN (VLAN 20) and Assign Management PC**

Step 1: Create VLAN 20

enable

conf t

vlan 20

name Management

exit

Step 2: Assign Management PC to VLAN 20

On the appropriate switch port:

interface gig0/3

switchport mode access

switchport access vlan 20

exit

✅ **Task 4: Verify Connectivity of Management PC to All Switches**

Step 1: Assign IP Address to Management Interface

On **SW-1 and SW-2**:

interface vlan 20

ip address 192.168.10.1 255.255.255.0

no shutdown

exit

Step 2: Configure Default Gateway

ip default-gateway 192.168.10.100

Step 3: Verify Connectivity

- Ping from the management PC to all switch IPs:

ping 192.168.10.1

✅ **Task 5: Implement ACL to Prevent Outside Users from Accessing VLAN 20**

Step 1: Define ACL on R1

enable

conf t

ip access-list extended BLOCK_MGMT

deny ip any 192.168.10.0 0.0.0.255

permit ip any any

exit

Step 2: Apply ACL to the Interface

interface gig0/1

ip access-group BLOCK_MGMT in

exit

✅ **Task 6: Assign IP and Gateway to PCs**

C2, C3, C4:

- IP: 192.168.10.x

- Subnet Mask: 255.255.255.0
- Gateway: 192.168.10.100

D1, D2, D3, D4:

- IP: 192.168.5.x
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.5.100

🔍 Verification and Testing

1. Check VLANs and Trunking

show vlan brief

show interfaces trunk

2. Check ACL

show access-lists

3. Ping to Test Connectivity

ping 192.168.10.1

ping 192.168.5.1

Let me know if this works or if you encounter any issues during the setup!

Seat No: _____ Max. Marks: 50

1.	Create the following topology using static routing and ▪ Configure, apply and verify an ACL that will block ICMP access on R3	40
2.	Viva	5
3.	Journal	5

Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
PC1	NIC	2001:DB8:1:10::10/64	FE80::1
PC2	NIC	2001:DB8:1:11::11/64	FE80::1
R1	gig0/0	2001:DB8:1:10::1/64	FE80::1
	gig0/1	2001:DB8:1:11::1/64	FE80::1
	se0/1/0	2001:DB8:1:1::1/64	FE80::1
R2	se0/1/0	2001:DB8:1:1::2/64	FE80::2
	se0/1/1	2001:DB8:1:2::2/64	FE80::2
R3	gig0/0	2001:DB8:1:30::1/64	FE80::3
	se0/1/0	2001:DB8:1:2::1/64	FE80::3
Server	NIC	2001:DB8:1:30::30/64	FE80::3

Here's a **step-by-step guide** to perform the tasks described in your latest image:

✅ Task 1: Create the Topology Using Static Routing

Step 1: Assign IPv6 Addresses to Interfaces

On PC1:

ipv6 address 2001:DB8:1:10::10/64

ipv6 default-gateway FE80::1

On PC2:

ipv6 address 2001:DB8:1:11::11/64

ipv6 default-gateway FE80::1

Step 2: Configure IPv6 on Routers

On R1:

enable

conf t

interface gig0/0

ipv6 address 2001:DB8:1:10::1/64

ipv6 enable

exit

interface se0/1/0

ipv6 address 2001:DB8:1:1::1/64

ipv6 enable

exit

interface se0/1/1

ipv6 address 2001:DB8:1:2::1/64

ipv6 enable

exit

ipv6 route 2001:DB8:1:30::/64 2001:DB8:1:1::2

ipv6 route 2001:DB8:1:11::/64 2001:DB8:1:2::2

exit

On R2:

enable

conf t

interface se0/1/0

ipv6 address 2001:DB8:1:1::2/64

ipv6 enable

exit

interface se0/1/1

ipv6 address 2001:DB8:1:2::2/64

ipv6 enable

exit

interface gig0/0

ipv6 address 2001:DB8:1:30::1/64

ipv6 enable

exit

ipv6 route 2001:DB8:1:10::/64 2001:DB8:1:1::1

ipv6 route 2001:DB8:1:11::/64 2001:DB8:1:2::1

exit

On R3:

enable

conf t

interface gig0/0

ipv6 address 2001:DB8:1:30::30/64

ipv6 enable

exit

interface se0/1/0

ipv6 address 2001:DB8:1:2::1/64

ipv6 enable

exit

ipv6 route 2001:DB8:1:10::/64 2001:DB8:1:2::2

ipv6 route 2001:DB8:1:11::/64 2001:DB8:1:2::2

exit

✅ **Task 2: Configure and Apply ACL to Block ICMP on R3**

Step 1: Create an ACL to Block ICMP Traffic

enable

conf t

ipv6 access-list BLOCK_ICMP

deny icmp any any

permit ipv6 any any

exit

Step 2: Apply ACL to the Interface

interface gig0/0

ipv6 traffic-filter BLOCK_ICMP in

exit

✅ **Task 3: Verify and Test**

Step 1: Check Routing

show ipv6 route

Step 2: Verify ACL

show ipv6 access-list

Step 3: Ping Test

- Try to **ping R3** from PC1 and PC2:

ping 2001:DB8:1:30::30

- ICMP traffic should be **blocked**.

🔍 **Troubleshooting (if needed)**

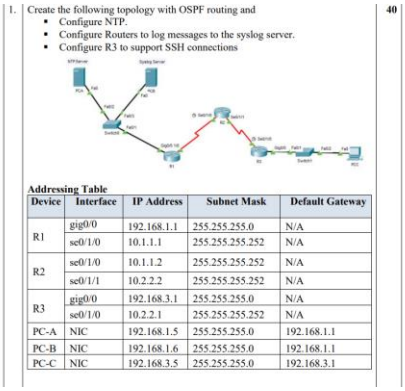
- Check interface status:

show ipv6 interface brief

- Verify connectivity:

ping FE80::1

Let me know if this works or if you encounter any issues!



1. Create the following topology with OSPF routing and
   - Configure NTP.
   - Configure Routers to log messages to the syslog server.
   - Configure R3 to support SSH connections

40

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1

Here's a **step-by-step guide** to perform the tasks described in your latest image:

✅ Task 1: Create the Topology with OSPF Routing

Step 1: Assign IP Addresses to Interfaces

On PC-A:

ip address 192.168.1.5 255.255.255.0

default-gateway 192.168.1.1

On PC-B:

ip address 192.168.1.6 255.255.255.0

default-gateway 192.168.1.1

On PC-C:

ip address 192.168.3.5 255.255.255.0

default-gateway 192.168.3.1

Step 2: Configure IPs and OSPF on Routers

On R1:

enable

conf t

interface gig0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.1.1.1 255.255.255.252

no shutdown

exit

router ospf 1

network 192.168.1.0 0.0.0.255 area 0

network 10.1.1.0 0.0.0.3 area 0

exit

On R2:

enable

conf t

interface se0/1/0

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

interface se0/1/1

ip address 10.2.1.2 255.255.255.252

no shutdown

exit

router ospf 1

network 10.1.1.0 0.0.0.3 area 0

network 10.2.1.0 0.0.0.3 area 0

exit

On R3:

```
enable
conf t
interface gig0/0
ip address 192.168.3.1 255.255.255.0
no shutdown
exit

interface se0/1/0
ip address 10.2.1.1 255.255.255.252
no shutdown
exit

router ospf 1
network 192.168.3.0 0.0.0.255 area 0
network 10.2.1.0 0.0.0.3 area 0
exit
```

✅ **Task 2: Configure NTP on Routers**

On All Routers:

```
enable
conf t
ntp server 192.168.1.3
exit
```

✅ **Task 3: Configure Routers to Log Messages to the Syslog Server**

On All Routers:

```
enable
conf t
```

logging host 192.168.1.4

logging trap informational

exit

✅ **Task 4: Configure SSH on R3**

Step 1: Create SSH User and Set Domain

enable

conf t

hostname R3

ip domain-name example.com

username admin privilege 15 secret cisco123

Step 2: Enable SSH

crypto key generate rsa

1024

Step 3: Enable SSH on VTY Lines

line vty 0 4

transport input ssh

login local

exit

✅ **Verification and Testing**

Step 1: Check OSPF Neighbors

show ip ospf neighbor

Step 2: Verify NTP

show ntp status

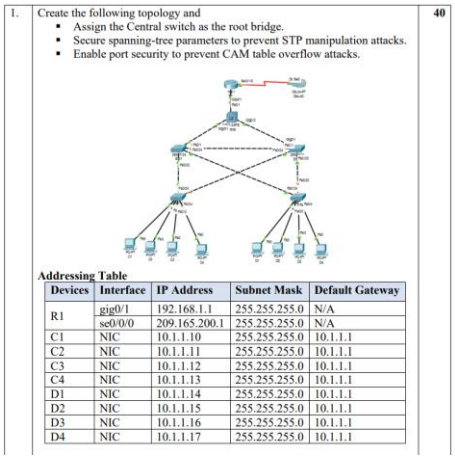
Step 3: Verify Syslog Messages

show logging

Step 4: Test SSH to R3

ssh -l admin 192.168.3.1

Let me know if this works or if you encounter any issues!



1. Create the following topology and — 40
   - Assign the Central switch as the root bridge.
   - Secure spanning-tree parameters to prevent STP manipulation attacks.
   - Enable port security to prevent CAM table overflow attacks.

Addressing Table

Devices	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/1	192.168.1.1	255.255.255.0	N/A
	se0/0/0	209.165.200.1	255.255.255.0	N/A
C1	NIC	10.1.1.10	255.255.255.0	10.1.1.1
C2	NIC	10.1.1.11	255.255.255.0	10.1.1.1
C3	NIC	10.1.1.12	255.255.255.0	10.1.1.1
C4	NIC	10.1.1.13	255.255.255.0	10.1.1.1
D1	NIC	10.1.1.14	255.255.255.0	10.1.1.1
D2	NIC	10.1.1.15	255.255.255.0	10.1.1.1
D3	NIC	10.1.1.16	255.255.255.0	10.1.1.1
D4	NIC	10.1.1.17	255.255.255.0	10.1.1.1

Here's a step-by-step guide to perform the tasks described in the latest image:

✅ Task 1: Create the Topology and Assign IP Addresses

Step 1: Assign IP Addresses to PCs

For each PC, assign the IP address and gateway as per the addressing table:

- **On C1:**

ip address 10.1.1.10 255.255.255.0

default-gateway 10.1.1.1

- **On C2:**

ip address 10.1.1.11 255.255.255.0

default-gateway 10.1.1.1

- **On C3:**

ip address 10.1.1.12 255.255.255.0

default-gateway 10.1.1.1

- **On D1, D2, D3, D4:**

ip address <respective IP> 255.255.255.0

default-gateway 10.1.1.1

Step 2: Configure IPs on R1

- **On R1:**

enable

conf t

interface gig0/1

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface se0/0/0

ip address 209.165.200.1 255.255.255.0

no shutdown

exit

✅ **Task 2: Assign the Central Switch as the Root Bridge**

Step 1: Set Priority on Central Switch

enable

conf t

spanning-tree vlan 1 root primary

exit

✅ **Task 3: Secure Spanning Tree Parameters**

Step 1: Enable BPDU Guard and Root Guard

enable

conf t

interface range gig0/1 - 24

spanning-tree bpduguard enable

exit

Step 2: Configure Root Guard on Uplink Ports

interface gig0/1

spanning-tree guard root

exit

✅ **Task 4: Enable Port Security to Prevent CAM Table Overflow**

Step 1: Enable Port Security

enable

conf t

interface range gig0/1 - 24

switchport mode access

switchport port-security

switchport port-security maximum 2

switchport port-security violation restrict

switchport port-security aging time 2

exit

✅ **Verification and Testing**

Step 1: Check Spanning Tree Configuration

show spanning-tree

Step 2: Verify Port Security

show port-security

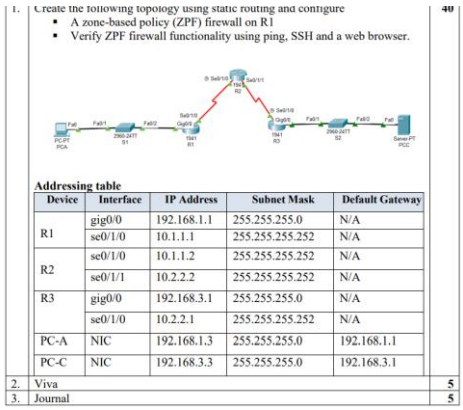
Step 3: Verify Root Bridge

show spanning-tree root

Step 4: Check Interface Status

show interfaces status

Let me know if this works or if you encounter any issues!



1. Create the following topology using static routing and configure — 40
   - A zone-based policy (ZPF) firewall on R1
   - Verify ZPF firewall functionality using ping, SSH and a web browser.

Addressing table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

2. Viva — 5
3. Journal — 5

Here's a detailed step-by-step guide to perform the tasks mentioned in the latest image:

✅ Task 1: Create the Topology with Static Routing

Step 1: Configure IP Addresses on the Routers

On R1:

enable

conf t

interface gig0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.1.1.1 255.255.255.252

no shutdown

exit

On R2:

enable

conf t

interface se0/1/0

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

interface se0/1/1

ip address 10.2.2.2 255.255.255.252

no shutdown

exit

On R3:

enable

conf t

interface gig0/0

ip address 192.168.3.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.2.2.1 255.255.255.252

no shutdown

exit

Step 2: Configure Static Routes on the Routers

On R1:

ip route 192.168.3.0 255.255.255.0 10.1.1.2

On R2:

ip route 192.168.1.0 255.255.255.0 10.1.1.1

ip route 192.168.3.0 255.255.255.0 10.2.2.1

On R3:

ip route 192.168.1.0 255.255.255.0 10.2.2.2

✅ **Task 2: Configure a Zone-Based Policy Firewall (ZPF) on R1**

Step 1: Define Security Zones

enable

conf t

zone security INSIDE

exit

zone security OUTSIDE

exit

zone security DMZ

exit

Step 2: Assign Interfaces to Zones

interface gig0/0

zone-member security INSIDE

exit

interface se0/1/0

zone-member security OUTSIDE

exit

Step 3: Create Class Maps

class-map type inspect match-any INSIDE-TO-OUTSIDE

match protocol http

match protocol https

match protocol icmp

exit

Step 4: Create Policy Maps

policy-map type inspect INSIDE-OUT-POLICY

class type inspect INSIDE-TO-OUTSIDE

inspect

exit

Step 5: Create Zone Pair and Apply Policy

zone-pair security INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect INSIDE-OUT-POLICY

exit

✅ **Task 3: Verify ZPF Firewall Using Ping, SSH, and Web Browser**

Step 1: Verify Connectivity with Ping

- From PC-A (192.168.1.3), ping PC-C (192.168.3.3).

ping 192.168.3.3

Step 2: Verify SSH Connection to R3

- Use SSH to access R3 from PC-A.

ssh 192.168.3.1

Step 3: Verify Web Access

- Open a browser on PC-A and access any web service hosted on PC-C.

✅ Verification Commands

Check Static Routes

show ip route

Verify Zone-Based Firewall Configuration

show zone security

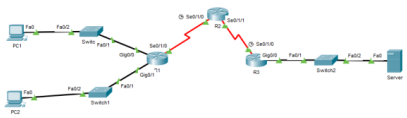
show policy-map type inspect

show zone-pair security

Check Interface Status

show ip interface brief

Let me know if you encounter any issues while performing these steps!

1.	Create the following topology using static routing and ▪ Configure, apply and verify an ACL that will block HTTP access on R1 ▪ Configure, apply and verify an ACL that will block HTTPS access on R1  **Addressing Table** **Device** / **Interface** / **IPv6 Address/Prefix** / **Default Gateway** PC1 / NIC / 2001:DB8:1:10::10/64 / FE80::1 PC2 / NIC / 2001:DB8:1:11::11/64 / FE80::1 R1 / gig0/0 / 2001:DB8:1:10::1/64 / FE80::1 R1 / gig0/1 / 2001:DB8:1:11::1/64 / FE80::1 R1 / se0/1/0 / 2001:DB8:1:1::1/64 / FE80::1 R2 / se0/1/0 / 2001:DB8:1:1::2/64 / FE80::2 R2 / se0/1/1 / 2001:DB8:1:2::2/64 / FE80::2 R3 / gig0/0 / 2001:DB8:1:30::1/64 / FE80::3 R3 / se0/1/0 / 2001:DB8:1:2::1/64 / FE80::3 Server / NIC / 2001:DB8:1:30::30/64 / FE80::3	**40**
2.	Viva	**5**
3.	Journal	**5**

Here's a step-by-step guide to perform the tasks from the latest image:

✅ Task 1: Create the Topology Using Static Routing

Step 1: Configure IPv6 Addresses on the Routers

On R1:

enable

conf t

interface gig0/0

ipv6 address 2001:DB8:1:10::1/64

no shutdown

exit

interface se0/1/0

ipv6 address 2001:DB8:1:1::1/64

no shutdown

exit

On R2:

enable

conf t

interface se0/1/0

ipv6 address 2001:DB8:1:1::2/64

no shutdown

exit

interface se0/1/1

ipv6 address 2001:DB8:1:2::2/64

no shutdown

exit

On R3:

enable

conf t

interface gig0/0

ipv6 address 2001:DB8:1:30::1/64

no shutdown

exit

interface se0/1/0

ipv6 address 2001:DB8:1:2::1/64

no shutdown

exit

Step 2: Configure Static Routes

On R1:

ipv6 route 2001:DB8:1:30::/64 2001:DB8:1:1::2

On R2:

ipv6 route 2001:DB8:1:10::/64 2001:DB8:1:1::1

ipv6 route 2001:DB8:1:30::/64 2001:DB8:1:2::1

On R3:

ipv6 route 2001:DB8:1:10::/64 2001:DB8:1:2::2

✅ **Task 2: Configure, Apply, and Verify ACL to Block HTTP (Port 80) on R1**

Step 1: Create and Apply IPv6 ACL to Block HTTP

enable

conf t

ipv6 access-list BLOCK-HTTP

deny tcp any any eq 80

permit ipv6 any any

exit

Step 2: Apply the ACL to an Interface

Apply on R1:

interface gig0/0

ipv6 traffic-filter BLOCK-HTTP in

exit

Step 3: Verify the ACL

show ipv6 access-list

✅ Task 3: Configure, Apply, and Verify ACL to Block HTTPS (Port 443) on R1

Step 1: Create and Apply IPv6 ACL to Block HTTPS

enable

conf t

ipv6 access-list BLOCK-HTTPS

deny tcp any any eq 443

permit ipv6 any any

exit

Step 2: Apply the ACL to an Interface

Apply on R1:

interface gig0/0

ipv6 traffic-filter BLOCK-HTTPS in

exit

Step 3: Verify the ACL

show ipv6 access-list

✅ Verification Steps

Verify HTTP and HTTPS Blocking

- From PC1, try to access the HTTP and HTTPS service on the server.

ping 2001:DB8:1:30::30

- Try to access HTTP and HTTPS using a web browser on PC1 or PC2.
- Verify that HTTP and HTTPS traffic is blocked.

Check Routing Table

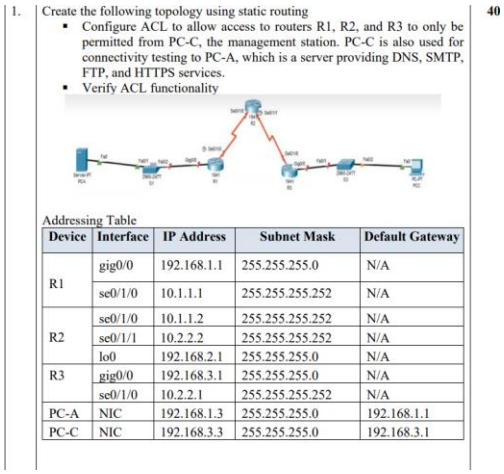
show ipv6 route

Check ACL Statistics

show ipv6 access-list BLOCK-HTTP

show ipv6 access-list BLOCK-HTTPS

Let me know if you encounter any issues while performing these tasks!



1. Create the following topology using static routing
   - Configure ACL to allow access to routers R1, R2, and R3 to only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, which is a server providing DNS, SMTP, FTP, and HTTPS services.
   - Verify ACL functionality

40

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
	lo0	192.168.2.1	255.255.255.0	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Here's a step-by-step guide to perform the tasks from the provided images:

✅ Task 1: Configure ACL to Allow Access to Routers R1, R2, and R3 Only from PC-C

Step 1: Configure IP Addresses

On R1:

enable

conf t

interface gig0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.1.1.1 255.255.255.252

no shutdown

exit

interface se0/1/0

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

On R2:

enable

conf t

interface se0/1/0

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

interface se0/1/1

ip address 10.2.2.2 255.255.255.252

no shutdown

exit

interface lo0

ip address 192.168.2.1 255.255.255.0

no shutdown

exit

On R3:

enable

conf t

interface gig0/0

ip address 192.168.3.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.2.2.1 255.255.255.252

no shutdown

exit

Step 2: Configure Static Routing

On R1:

ip route 192.168.2.0 255.255.255.0 10.1.1.2

ip route 192.168.3.0 255.255.255.0 10.1.1.2

On R2:

ip route 192.168.1.0 255.255.255.0 10.1.1.1

ip route 192.168.3.0 255.255.255.0 10.2.2.1

On R3:

ip route 192.168.1.0 255.255.255.0 10.2.2.2

ip route 192.168.2.0 255.255.255.0 10.2.2.2

Step 3: Configure ACL to Allow Only PC-C to Access Routers

On R1:

access-list 101 permit ip host 192.168.3.3 any

access-list 101 deny ip any any

interface gig0/0

ip access-group 101 in

exit

On R2:

access-list 102 permit ip host 192.168.3.3 any

access-list 102 deny ip any any

interface lo0

ip access-group 102 in

exit

On R3:

access-list 103 permit ip host 192.168.3.3 any

access-list 103 deny ip any any

interface gig0/0

ip access-group 103 in

exit

✅ **Task 2: Verify ACL Functionality**

Verification Steps:

1. **Ping Routers from PC-C**

ping 192.168.1.1

ping 192.168.2.1

ping 192.168.3.1

2. **Ping from Any Other PC**

- Should be denied by ACL.

3. **Check ACL Hits on R1, R2, and R3:**

show access-list

✅ **Task 3: Enable IOS IPS, Configure Logging, and Verify**

Step 1: Enable IPS and Configure Basic Setup

On R1:

enable

conf t

ip ips name MY_IPS

ip ips signature-category

category all

retire false

exit

interface gig0/0

ip ips MY_IPS in

exit

Step 2: Configure Logging and Alerts

conf t

ip ips notify SDEE

logging buffered 51200 warnings

logging console critical

logging monitor informational

logging trap debugging

exit

Step 3: Verify IPS and Logging

1. **Check IPS Status**

show ip ips interfaces

2. **Check SDEE Alerts**

show ip ips all

show ip ips signatures

✅ **Task 4: Modify IPS Signature and Verify**

Step 1: Modify Signature (Example: ICMP Echo)

conf t

ip ips signature-definition 2004 0

status disabled

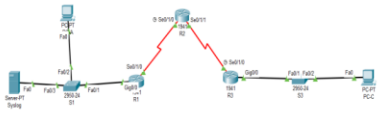
exit

Step 2: Verify Signature

show ip ips signatures

Let me know if you encounter any issues or need further assistance!

1. Create the following topology and
   - Enable IOS IPS
   - Configure logging and verify IPS
   - Modify signature and verify again



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1

Here's a step-by-step guide to perform the tasks in the latest image:

✅ Task: Enable IOS IPS, Configure Logging, and Verify

Step 1: Configure IP Addresses

On R1:

enable

conf t

interface gig0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.1.1.1 255.255.255.252

no shutdown

exit

interface se0/1/1

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

On R2:

enable

conf t

interface se0/1/0

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

interface se0/1/1

ip address 10.2.2.2 255.255.255.252

no shutdown

exit

interface lo0

ip address 192.168.2.1 255.255.255.0

no shutdown

exit

On R3:

enable

conf t

interface gig0/0

ip address 192.168.3.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.2.2.1 255.255.255.252

no shutdown

exit

Step 2: Configure Static Routing

On R1:

ip route 192.168.2.0 255.255.255.0 10.1.1.2

ip route 192.168.3.0 255.255.255.0 10.1.1.2

On R2:

ip route 192.168.1.0 255.255.255.0 10.1.1.1

ip route 192.168.3.0 255.255.255.0 10.2.2.1

On R3:

ip route 192.168.1.0 255.255.255.0 10.2.2.2

ip route 192.168.2.0 255.255.255.0 10.2.2.2

✅ **Step 3: Enable IOS IPS on R1**

Step 1: Enable IPS

enable

conf t

ip ips name MY_IPS

ip ips signature-category

category all

retire false

exit

interface gig0/0

ip ips MY_IPS in

exit

Step 2: Configure Logging and Alerts

conf t

ip ips notify SDEE

logging buffered 51200 warnings

logging console critical

logging monitor informational

logging trap debugging

exit

Step 3: Verify IPS and Logging

1. **Check IPS Status**

show ip ips interfaces

2. **Check SDEE Alerts**

show ip ips all

show ip ips signatures

✅ **Step 4: Modify Signature and Verify Again**

Step 1: Modify Signature (Example: ICMP Echo)

conf t

ip ips signature-definition 2004 0

status disabled

exit

Step 2: Verify Signature

show ip ips signatures

✅ Verification Steps

---

1. **Ping Test:**

ping 192.168.1.1

ping 192.168.3.1

2. **Check IPS and Logging:**

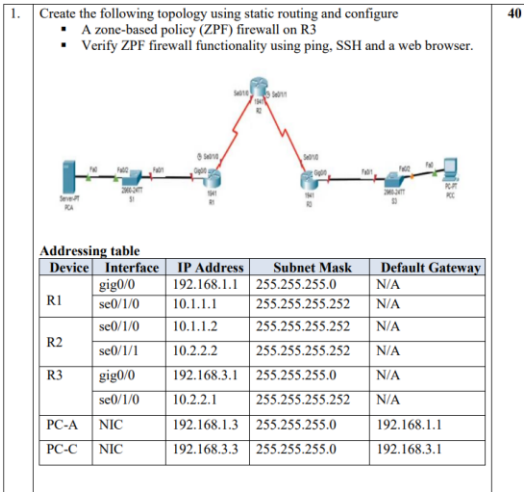
show ip ips statistics

show logging

3. **Check Modified Signature:**

show ip ips signatures

Let me know if you encounter any errors or need further assistance!



1. Create the following topology using static routing and configure — 40
   - A zone-based policy (ZPF) firewall on R3
   - Verify ZPF firewall functionality using ping, SSH and a web browser.

Addressing table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	se0/1/0	10.1.1.2	255.255.255.252	N/A
	se0/1/1	10.2.2.2	255.255.255.252	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	se0/1/0	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Here's a step-by-step guide to perform the tasks shown in your image:

✅ Task: Create Topology, Configure ZPF on R3, and Verify Firewall

---

Step 1: Configure IP Addresses

On R1:

enable

conf t

interface gig0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.1.1.1 255.255.255.252

no shutdown

exit

interface se0/1/1

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

On R2:

enable

conf t

interface se0/1/0

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

interface se0/1/1

ip address 10.2.2.2 255.255.255.252

no shutdown

exit

On R3:

enable

conf t

interface gig0/0

ip address 192.168.3.1 255.255.255.0

no shutdown

exit

interface se0/1/0

ip address 10.2.2.1 255.255.255.252

no shutdown

exit

Step 2: Configure Static Routing

On R1:

ip route 192.168.3.0 255.255.255.0 10.1.1.2

ip route 192.168.2.0 255.255.255.0 10.1.1.2

On R2:

ip route 192.168.1.0 255.255.255.0 10.1.1.1

ip route 192.168.3.0 255.255.255.0 10.2.2.1

On R3:

ip route 192.168.1.0 255.255.255.0 10.2.2.2

ip route 192.168.2.0 255.255.255.0 10.2.2.2

✅ **Step 3: Configure ZPF (Zone-Based Policy Firewall) on R3**

Step 1: Define Security Zones

conf t

zone security INSIDE

zone security OUTSIDE

exit

Step 2: Assign Interfaces to Zones

interface gig0/0

zone-member security INSIDE

exit

interface se0/1/0

zone-member security OUTSIDE

exit

Step 3: Define Class Maps

class-map type inspect match-all ALLOW_TRAFFIC

match protocol tcp

match protocol icmp

match protocol udp

exit

Step 4: Define Policy Maps

policy-map type inspect MY_POLICY

class type inspect ALLOW_TRAFFIC

inspect

exit

Step 5: Create Zone-Pair and Apply Policy

zone-pair security ZP-INSIDE-OUTSIDE source INSIDE destination OUTSIDE

service-policy type inspect MY_POLICY

exit

✅ **Step 4: Verify ZPF Configuration**

Step 1: Verify Zone and Zone-Pair Configuration

show zone security

show zone-pair security

show policy-map type inspect zone-pair

Step 2: Test Connectivity

- **Ping from PC-A to PC-C:**

ping 192.168.3.3

- **SSH to PC-C (If configured):**

ssh 192.168.3.3

- **Test Web Browser Access:** Open a browser and try accessing web services.

✅ **Step 5: Additional Verification**

---

1. Check Log for Matches and Dropped Packets

show policy-map type inspect MY_POLICY

show conn

2. Check Interface Zone Membership

show zone-member security
