Phase - 1 (Initial Configuration)

Configuring Basic Devices Settings

1. Naming devices

```
Device(config)# hostname <name>
```

2. Securing privileged access

```
Device(config)# security passwords min-length 12
Device(config)# enable secret strong-PASS@2024
Device(config)# service password-encryption
```

3. Securing console line

```
Device(config)# line console 0
        Device(config-line)# password strong-conPASS@2024
Device(config-line)# exec-timeout 4 0
Device(config-line)# login
```

4. Securing VTY lines

```
Device(config)# line vty 0 4
Device(config-line)# password strong-vtyPASS@2024
Device(config-line)# exec-timeout 4 0
Device(config-line)# transport input ssh
Device(config-line)# login local
```

5. Configuring the message-of-the-day

```
Device(config)# banner motd # Unauthorized Access Is Prohibted! #
```

6. Setting the clock for the device

```
Device# clock set 14:30:00 10 Oct 2024
```

Configuring Interfaces Settings

Addressing & VLANs Table

Device	Interface	Physical port	Address	Subnet Mask	Default Gateway
Gateway	G0/0.10 G0/0.20 G0/0.50 G0/0.99 G0/0.100	G0/0	192.168.10.1 192.168.20.1 172.18.50.1 192.168.99.1 192.168.100.1	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	N/A N/A N/A N/A N/A
SW1	SVI	N/A	192.168.99.251	255.255.255.0	192.168.99.1
SW2	SVI	N/A	192.168.99.252	255.255.255.0	192.168.99.1
PC1	NIC	SW2 - Fa0/2	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	SW2 - Fa0/3	192.168.10.11	255.255.255.0	192.168.10.1
PC3	NIC	SW2 - Fa0/4	192.168.20.10	255.255.255.0	192.168.20.1
PC4	NIC	SW2 - Fa0/5	192.168.20.11	255.255.255.0	192.168.20.1
PC5	NIC	SW3 - Fa0/2	192.168.10.12	255.255.255.0	192.168.10.1
PC6	NIC	SW3 - Fa0/3	192.168.10.13	255.255.255.0	192.168.10.1
PC7	NIC	SW3 - Fa0/4	192.168.20.12	255.255.255.0	192.168.20.1
PC8	NIC	SW3 - Fa0/5	192.168.20.13	255.255.255.0	192.168.20.1
PC9	NIC	SW3 - Fa0/6	192.168.20.14	255.255.255.0	192.168.20.1
PC10	NIC	SW3 - Fa0/7	192.168.20.15	255.255.255.0	192.168.20.1
WebServer	NIC	SW3 - Fa0/8	172.18.50.50	255.255.255.0	172.18.50.1
Database	NIC	SW3 - Fa0/9	192.168.20.17	255.255.255.0	192.168.20.1

Configuring SSH For Remote Management

1. Configuring a domain name for the device

```
Device(config)# ip domain-name hostname.depi
```

2. Generating RSA keys and choosing the modulo bit size to be `2048`

```
Device(config)# crypto key generate rsa general-keys modulus 2048
```

3. Creating an SSH user with username and password

```
Device(config)# username admin secret strong-sshPASS@2024
```

4. Allowing VTY logins for two minutes if three failed login attempts occur within 60 seconds.

```
Device(config)# login block-for 120 attempts 3 within 60
```

5. Using SSH version 2

```
Device(config)# ip ssh version 2
```

Phase - 2 (Implementing VLANs)

VLANs Table

VLAN Number	VLAN Name
10	HR
20	IT
50	DMZ
99	Management
100	Native

Creating VLAN on the switches

```
Switch(config)# vlan <vlan-number>
Switch(config-vlan)# name <vlan-name>
```

Addressing Table

Device	Interface	Physical port	Address	Subnet Mask	Default Gateway
Gateway	G0/0.10 G0/0.20 G0/0.50 G0/0.99 G0/0.100	G0/0	192.168.10.1 192.168.20.1 172.18.50.1 192.168.99.1 192.168.100.1	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	N/A N/A N/A N/A N/A
SW1	SVI	N/A	192.168.99.251	255.255.255.0	192.168.99.1
SW2	SVI	N/A	192.168.99.252	255.255.255.0	192.168.99.1
PC1	NIC	SW2 - Fa0/2	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	SW2 - Fa0/3	192.168.10.11	255.255.255.0	192.168.10.1
PC3	NIC	SW2 - Fa0/4	192.168.20.10	255.255.255.0	192.168.20.1
PC4	NIC	SW2 - Fa0/5	192.168.20.11	255.255.255.0	192.168.20.1
PC5	NIC	SW3 - Fa0/2	192.168.10.12	255.255.255.0	192.168.10.1
PC6	NIC	SW3 - Fa0/3	192.168.10.13	255.255.255.0	192.168.10.1
PC7	NIC	SW3 - Fa0/4	192.168.20.12	255.255.255.0	192.168.20.1
PC8	NIC	SW3 - Fa0/5	192.168.20.13	255.255.255.0	192.168.20.1
PC9	NIC	SW3 - Fa0/6	192.168.20.14	255.255.255.0	192.168.20.1
PC10	NIC	SW3 - Fa0/7	192.168.20.15	255.255.255.0	192.168.20.1
WebServer	NIC	SW3 - Fa0/8	172.18.50.50	255.255.255.0	172.18.50.1

Device	Interface	Physical port	Address	Subnet Mask	Default Gateway
Database	NIC	SW3 - Fa0/9	192.168.20.17	255.255.255.0	192.168.20.1

Configuring access ports on the switches

```
Switch(config)# interface <interface-id>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access <vlan-number>
Switch(config-if)# no shutdown
```

Configuring the virtual management interfaces (SVIs)

```
Switch(config)# interface vlan 99
Switch(config-if)# ip address <ip-address> <subnet-mask>
```

Configuring trunk ports on the switches

```
Switch(config)# interface <interface-id>
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 100
Switch(config-if)# switchport trunk allowed vlan 10,20,50,99
Switch(config-if)# no shutdown
```

Configuring router-on-a-stick inter-VLAN routing on the router

```
Grateway(config)# interface G0/0.10
Grateway(config-subif)# description Default Gateway for VLAN 10
Grateway(config-subif)# encapsulation dot1Q 10
Grateway(config-subif)# ip add 192.168.10.1 255.255.255.0
Grateway(config-subif)# exit

Grateway(config)# interface G0/0.20
Grateway(config-subif)# description Default Gateway for VLAN 20
```

```
Grateway(config-subif)# encapsulation dot1Q 10
Grateway(config-subif)# ip add 192.168.20.1 255.255.255.0
Grateway(config-subif)# exit

Grateway(config)# interface G0/0.99
Grateway(config-subif)# description Default Gateway for VLAN 99
Grateway(config-subif)# encapsulation dot1Q 10
Grateway(config-subif)# ip add 192.168.99.1 255.255.255.0
Grateway(config-subif)# exit
```

For the native VLAN 100

```
Grateway(config)# interface G0/0.100
Grateway(config-subif)# description Default Gateway for VLAN 100
Grateway(config-subif)# encapsulation dot1Q 100 native
Grateway(config-subif)# ip add 192.168.100.1 255.255.255.0
Grateway(config-subif)# exit
```

Enabling the Physical Interface

```
Grateway(config)# interface G0/0
Grateway(config-if)# no shutdown
```

Phase - 3 (Security Measures)

Implemented features that considers security

1. Using `enable secret` instead of `enable password` for more secure password by using **md5** hashing algorithm.
2. Changing the default **native & management** VLANs from **VLAN 1** to be **VLAN 99 (Management)** and **VLAN 100 (Native)**.
3. Using **SSH version 2** instead of the legacy version 1.
4. Using a large modulus space with a 2048 bits when generating the **RSA** keys for **SSH communication encryption**.

5. Setting a password policy that restricts using a password length of min. size of **12 characters** when configuring the network devices.
6. Allowing VTY logins for two minutes if three failed login attempts occur within 60 seconds.

Implementing Port Security

1. Shutting Down Unused Ports

```
Switch(config)# interface range <interface-id>
Switch(config-if)# shutdown
```

2. Mitigating MAC Address Table Overflow Attacks

Enabling Port Security

```
Switch(config)# interface <interface-id>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```

Setting the max. number of secure MAC address to 1

```
Switch(config-if)# switchport port-security maximum 1
```

Configuring the learning process for the MAC address to sticky

```
Switch(config-if)# switchport port-security mac-address sticky
```

Setting the Port Security Violation Mode to restrict

```
Switch(config-if)# switchport port-security violation restrict
```

Mitigating VLAN Hopping Attacks

1. Disable DTP (auto trunking) negotiations on non-trunking ports by using the `switchport mode access` interface configuration command.
2. Disable unused ports and put them in an unused VLAN.
3. Manually enable the trunk link on a trunking port by using the `switchport mode trunk` command.

4. Disable DTP (auto trunking) negotiations on trunking ports by using the `switchport nonegotiate` command.
5. Set the native VLAN to a VLAN other than VLAN 1 by using the `switchport trunk native vlan vlan_number` command.

Mitigating ARP Attacks by implementing Dynamic ARP inspection (DAI)

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10,20,99,50,100
Switch(config)# ip arp inspection vlan 10,20,99,50,100
Switch(config)#
Switch(config)# ip arp inspection validate src-mac dst-mac ip
Switch(config)#
Switch(config)# interface <trunk-interface-id>
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip arp inspection trust
```

Implementing Access Control Lists (ACLs)

To achieve the two objectives with **Access Control Lists (ACLs)**, we'll need to configure **two sets of ACLs** on the router's **GigabitEthernet0/1** (Internet-facing interface) and the **GigabitEthernet0/0.x** subinterfaces (for inter-VLAN routing). Let's walk through the steps:

Objective 1: Allow Only the DMZ (VLAN 50) to Be Accessible from the Internet

For this objective, we want traffic from the Internet (on interface **G0/1**) to access only VLAN 50 (the DMZ) while denying access to other VLANs.

Step 1.1: Creating an Extended Access List

We'll create an extended access list to allow only traffic destined for **VLAN 50** (subinterface **G0/0.50**) and deny access to other VLANs.

```
Grateway(config)# access-list 100 permit ip any 172.18.50.0 0.0.0.255
Grateway(config)# access-list 100 deny ip any 192.168.10.0 0.0.0.255
Grateway(config)# access-list 100 deny ip any 192.168.20.0 0.0.0.255
Grateway(config)# access-list 100 deny ip any 192.168.99.0 0.0.0.255
```

```
Grateway(config)# access-list 100 deny ip any 192.168.100.0 0.0.0.255
Grateway(config)# access-list 100 permit ip any any
```

Step 1.2: Apply the ACL to Interface G0/1 (Internet-Facing Interface)

Next, we'll apply this ACL to the **GigabitEthernet0/1** interface to filter incoming traffic from the Internet.

```
Grateway(config)# interface GigabitEthernet 0/1
Grateway(config-if)# ip access-group 100 in
```

This applies **ACL 100** to **inbound traffic** on the Internet-facing interface.

Objective 2: Disable Communication Between the DMZ (VLAN 50) and the Other VLANs

For this objective, we need to block any communication between **VLAN 50 (DMZ)** and the other VLANs. This means preventing VLAN 50 from sending or receiving traffic to/from other VLANs.

Step 2.1: Create an ACL to Block Communication Between VLAN 50 and Other VLANs

Create an ACL to **deny traffic** between VLAN 50 and other VLANs, and then apply it to **each VLAN's subinterface**.

```
access-list 110 deny ip 172.18.50.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny ip 172.18.50.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 110 deny ip 172.18.50.0 0.0.0.255 192.168.99.0 0.0.0.255
access-list 110 deny ip 172.18.50.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 110 permit ip any any
```

- `deny ip 172.18.50.0 0.0.0.255 [other VLAN subnet]` : Denies traffic from VLAN 50 to other VLANs.
- `permit ip any any` : Allows any other traffic that is not related to VLAN 50 and the other VLANs.

Step 2.2: Apply the ACL to Each VLAN's Subinterface

You will apply **ACL 110** to the **outbound direction** of each VLAN's subinterface to block traffic from **VLAN 50** trying to communicate with other VLANs.

```
interface GigabitEthernet 0/0.10
 ip access-group 110 out
!
interface GigabitEthernet 0/0.20
 ip access-group 110 out
!
interface GigabitEthernet 0/0.99
 ip access-group 110 out
!
interface GigabitEthernet 0/0.100
 ip access-group 110 out
```

This ensures that any traffic leaving each VLAN subinterface and attempting to reach **VLAN 50** will be denied.