Simple Business Setup

Description:

It is a network infrastructure for a small Computer Training Business named Alpha-Tech, which plans to open a training center located in Largo. The training center will serve students preparing to acquire IT industry certifications by taking on-site classes. The network infrastructure at the site will be able to serve the different vlans for students, faculty, administration and IT staff, as well as, all the computing resources and intermediary devices required to support the training center.

VLANS:

- Student (VLAN 10)
- Instructor (VLAN 20)
- Admin (VLAN 30)
- IT (VLAN 40)
- Printers (VLAN 50)
- Servers (VLAN 60)

IP Addresses:

Here router act as a DHCP server, assigning Ips to all devices.

ACL:

An Access Control List (ACL) is an ordered set of rules for filtering traffic based on conditions like IP addresses, ports, and protocols. Here, Student (VLAN 10) are restricted to use staff printer and admin server. Instructors (VLAN 20) are restricted to use Student printer and admin server. IT (VLAN 30) has only access to staff printer.

Network Security:

In network security, adding passwords for Console and VTY (Virtual Terminal) access is essential to ensure unauthorized users cannot gain access to a network device, such as a router or switch. These access controls help protect the device from potential attacks, accidental configurations, and unauthorized access.

Console Access Password:

- **Role:** The **Console** port allows direct access to the device physically via a serial cable. This is typically the first point of access when setting up or troubleshooting a network device.

VTY Access Password (Virtual Terminal):

- **Role: VTY (Virtual Terminal)** access allows users to remotely access a device over the network. This is useful for administrators to manage devices without being physically present at the location.

1. Hardware Setup

Routers and Multi-Layer Switch Configuration

1. **Add Hardware Components:**
   - **Router1 (HWIC-2T)**: Add a HWIC-2T module to Router1.
   - **Router2 (HWIC-2T)**: Add a HWIC-2T module to Router2.
   - **Multi-Layer Switch**: Add the multi-layer switch and connect to power using the AC supply.

---

2. Router Configuration

Router Configuration:

1. **Activate the Interfaces:**
   - Router1 (gig 0/0 to Multi-Layer Switch):

     ```
     Router1> enable
     Router1# configure terminal
     Router1(config)# interface gig0/0
     Router1(config-if)# no shutdown
     ```

   - Router1 (serial 0/1/0 to Router2):

     ```
     Router1(config)# interface serial 0/1/0
     Router1(config-if)# no shutdown
     Router1(config-if)# clock rate 64000
     ```

---

3. Switch Configuration (6 Switches)

Port Configuration on Switches:

1. **Configure Switch1 (VLAN 10, connected to Student PCs):**

   ```
   Switch1> enable
   Switch1# configure terminal
   Switch1(config)# interface range fa0/1-24
   Switch1(config-if-range)# switchport mode access
   Switch1(config-if-range)# switchport access vlan 10
   ```

   Repeat the above step for **Switch2, Switch3, Switch4, Switch5, and Switch6**, but change the VLAN number for each.

---

4. Multi-Layer Switch Configuration

1. **Assign VLANs to Ports on Multi-Layer Switch:**

   ```
   Multi-Layer Switch> enable
   Multi-Layer Switch# configure terminal
   Multi-Layer Switch(config)# interface gig1/0/1
   Multi-Layer Switch(config-if)# switchport mode access
   Multi-Layer Switch(config-if)# switchport access vlan 10
   ```

   Repeat for the other ports:

   - **gig1/0/2** for VLAN 20
   - **gig1/0/3** for VLAN 30
   - **gig1/0/4** for VLAN 40
   - **gig1/0/5** for VLAN 50
   - **gig1/0/6** for VLAN 60
2. **Configure Trunk Port (to Router1):**

   ```
   Multi-Layer Switch(config)# interface gig1/0/7
   Multi-Layer Switch(config-if)# switchport trunk encapsulation
   dot1q
   Multi-Layer Switch(config-if)# switchport mode trunk
   ```

---

5. IP Configuration

Router1 Configuration (Subinterfaces for VLANs):

1. **Configure IP Addresses for VLAN Subinterfaces:**

   ```
   Router1(config)# interface gig0/0.10
   Router1(config-if)# encapsulation dot1Q 10
   Router1(config-if)# ip address 192.168.1.1 255.255.255.0
   ```

   Repeat for the remaining VLANs:

   - **gig0/0.20** for VLAN 20 (IP: 192.168.2.1)
   - **gig0/0.30** for VLAN 30 (IP: 192.168.3.1)
   - **gig0/0.40** for VLAN 40 (IP: 192.168.4.1)
   - **gig0/0.50** for VLAN 50 (IP: 192.168.5.1)
   - **gig0/0.60** for VLAN 60 (IP: 192.168.6.1)

Router2 Configuration:

1. **Assign IP Addresses:**

   ```
   Router2(config)# interface serial 0/1/0
   Router2(config-if)# ip address 10.10.10.6 255.255.255.252

   Router2(config)# interface gig0/0
   Router2(config-if)# ip address 20.0.0.1 255.255.255.252
   ```

2. **Server Configuration (connected to Router2):**
   - IP Address: **20.0.0.2**
   - Subnet Mask: **255.255.255.252**
   - Default Gateway: **20.0.0.1**
3. **Ping Test:**
   - On the server, run:

     ```
     ping 20.0.0.1
     ```

---

6. DHCP Configuration

Router DHCP Pools Configuration:

1. **Create DHCP Pools for Each VLAN:**

   ```
   Router1(config)# service dhcp
   Router1(config)# ip dhcp pool student-pool
   Router1(dhcp-config)# network 192.168.1.0 255.255.255.0
   Router1(dhcp-config)# default-gateway 192.168.1.1
   Router1(dhcp-config)# dns-server 192.168.1.1
   ```

   Repeat for the remaining VLANs:

   - **instructor-pool** for VLAN 20
   - **admin-pool** for VLAN 30
   - **it-pool** for VLAN 40
   - **printers-pool** for VLAN 50
   - **servers-pool** for VLAN 60

---

8. Testing and Validation

1. **Check DHCP Lease:**
   - Ensure that DHCP assignments are working properly by checking the IP addresses on the PCs.
2. **RIP Routing Check:**
   - Use `show ip route` on both routers to confirm that RIP is properly propagating routes.

9. Router Configuration - Adding Passwords for Console and VTY Access

Router Configuration (Include Password Steps)

After configuring the interfaces on Router1 (as shown in your setup), you need to secure the console and VTY lines with a password. Repeat the same process for all switches.

1. **Configure Console Password**:

```
Router1> enable
Router1# configure terminal
Router1(config)# line console 0
Router1(config-line)# password cisco
Router1(config-line)# login
Router1(config-line)# exit
```

2. **Configure VTY Password** (for remote access via Telnet or SSH):

```
Router1(config)# line vty 0 15
Router1(config-line)# password cisco
Router1(config-line)# login
Router1(config-line)# exit
```

3. **Enable Secure Access** for the privileged EXEC mode:

```
Router1(config)# enable secret cisco
```

4. **Save the Configuration**:

```
Router1(config)# write memory
```

10. Configuration with ACLs

1. Router ACLs

- To block traffic of **VLAN 10** from using **Staff printer** and **Admin Server** while allowing all other traffic:

```
int gig0/0.10
ip access-group 101 in
access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.5.2
access-list 101 deny ip 192.168.1.0 0.0.0.255 host 192.168.5.3
access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.6.2
access-list 101 deny ip 192.168.1.0 0.0.0.255 host 192.168.6.3
access-list 101 permit ip any any
```

- To block traffic of **VLAN 20** from using **Student printer** and **Admin Server** while allowing all other traffic:

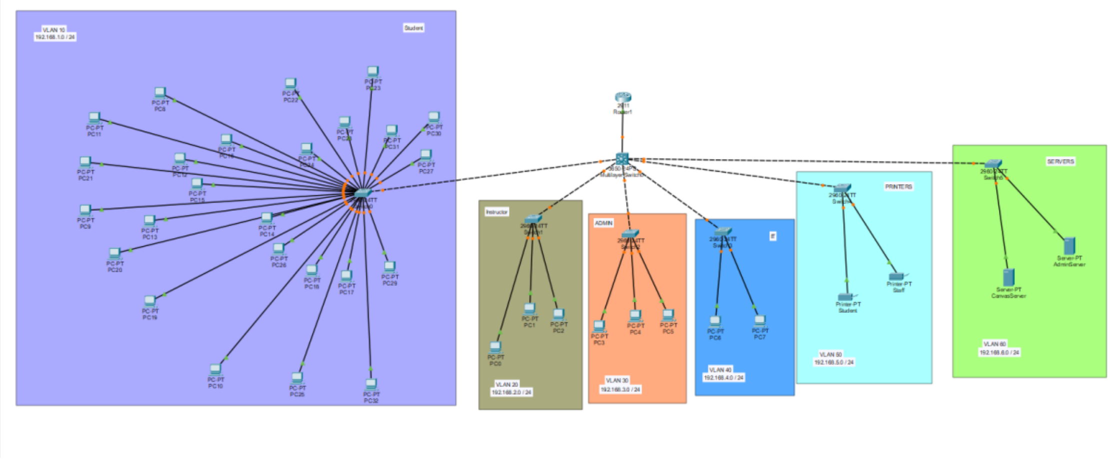
```
int gig0/0.20
ip access-group 102 in
access-list 102 deny ip 192.168.2.0 0.0.0.255 host 192.168.5.2
access-list 102 permit ip 192.168.2.0 0.0.0.255 host 192.168.5.3
access-list 102 permit ip 192.168.2.0 0.0.0.255 host 192.168.6.2
access-list 102 deny ip 192.168.2.0 0.0.0.255 host 192.168.6.3
access-list 102 permit ip any any
```

- To block traffic of **VLAN 30** from using **Student printer** while allowing all other traffic:

```
int gig0/0.30
ip access-group 103 in
access-list 103 deny ip 192.168.3.0 0.0.0.255 host 192.168.5.2
access-list 103 permit ip 192.168.3.0 0.0.0.255 host 192.168.5.3
access-list 103 permit ip 192.168.3.0 0.0.0.255 host 192.168.6.2
access-list 103 permit ip 192.168.3.0 0.0.0.255 host 192.168.6.3
access-list 103 permit ip any any
```

- To block traffic of **VLAN 40** from using **Student printer** and both **servers** while allowing all other traffic:

```
int gig0/0.40
ip access-group 104 in
access-list 104 deny ip 192.168.4.0 0.0.0.255 host 192.168.5.2
access-list 104 permit ip 192.168.4.0 0.0.0.255 host 192.168.5.3
access-list 104 deny ip 192.168.4.0 0.0.0.255 host 192.168.6.2
access-list 104 deny ip 192.168.4.0 0.0.0.255 host 192.168.6.3
access-list 104 permit ip any any
```


VLAN 10
192.168.1.0 / 24
Student
PC-PT PC8
PC-PT PC22
PC-PT PC23
PC-PT PC11
PC-PT PC16
PC-PT PC28
PC-PT PC31
PC-PT PC30
PC-PT PC21
PC-PT PC12
PC-PT PC24
PC-PT PC27
PC-PT PC15
PC-PT PC9
PC-PT PC13
PC-PT PC14
PC-PT PC20
PC-PT PC26
PC-PT PC18
PC-PT PC17
PC-PT PC29
PC-PT PC19
PC-PT PC10
PC-PT PC25
PC-PT PC32
2911 Router1
3650-24PS Multilayer Switch0
Instructor
2960-24TT Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
VLAN 20
192.168.2.0 / 24
ADMIN
2960-24TT Switch2
PC-PT PC3
PC-PT PC4
PC-PT PC5
VLAN 30
192.168.3.0 / 24
IT
2960-24TT Switch3
PC-PT PC6
PC-PT PC7
VLAN 40
192.168.4.0 / 24
PRINTERS
2960-24TT Switch4
Printer-PT Student
Printer-PT Staff
VLAN 50
192.168.5.0 / 24
SERVERS
2960-24TT Switch5
Server-PT CanvasServer
Server-PT AdminServer
VLAN 60
192.168.6.0 / 24