PT CONFIG

- Floors VLAN 10–60 → `192.168.10.0/24` … `192.168.60.0/24`
- NAS VLAN 70 → `192.168.70.0/24`
- MGMT VLAN 80 → `192.168.80.0/24` (DHCP server = `192.168.80.10`)
- IDS VLAN 90 → `192.168.90.0/24`
- DMZ VLAN 100 → `192.168.100.0/24` (DMZ server = `192.168.100.10`)
- Router↔ASA transit → `10.0.0.0/30` (Router=`10.0.0.1`, ASA inside=`10.0.0.2`)
- ASA outside↔ISP → `209.165.200.224/29` (ISP=`209.165.200.225`, ASA=`209.165.200.226`, DMZ public=`209.165.200.227`)

---

0) Context and design goal (for the report)

Goal: implement an enterprise-style network in Packet Tracer that:

- uses **one switch per floor** (access layer) and a **core switch** (distribution),
- segments users and services with **VLANs**,
- provides IP addressing via a **central DHCP server** for floor VLANs,
- routes internal VLANs using **Router-on-a-Stick (ROAS)**,
- enforces perimeter security by placing an **ASA firewall between internal router and Internet**,
- hosts a **DMZ** behind the firewall with a web service exposed to the Internet,
- uses a router as an **ISP simulation**.

Rationale: Star topology + VLAN segmentation improves availability, fault isolation, and security boundaries. The ASA provides a true perimeter firewall consistent with the assignment requirement (“firewall between internal router and Internet”; DMZ for public services).

---

1) Physical topology connections (documented)

Core and access layer

- Floor PC(s) → Floor switch access ports

- Floor switch uplink (trunk) → Core switch trunk port
- Core switch trunk port → Internal router trunk interface `Gi0/0/0`

Perimeter and DMZ

- Internal router `Gi0/0/1` → ASA **inside**
- ASA **outside** → ISP router
- ASA **dmz** → DMZ switch → DMZ web server

---

2) Switch configuration

2.1 SW-CORE (2960-24TT)

Step 1 — Create VLANs

```
enable
conf t
vlan 10
 name FLOOR1
vlan 20
 name FLOOR2
vlan 30
 name FLOOR3
vlan 40
 name FLOOR4
vlan 50
 name FLOOR5
vlan 60
 name FLOOR6
vlan 70
 name NAS
vlan 80
 name MGMT
vlan 90
 name IDS_IPS
vlan 100
 name DMZ
end
wr
```

Expected: `show vlan brief` lists VLANs 10–100.

Step 2 — Trunk to internal router (example: `Gi0/1`)

```
conf t
interface gi0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100
 no shutdown
end
wr
```

Step 3 — Trunks to floor switches (example: `Fa0/1–Fa0/6`)

```
conf t
interface range fa0/1 - 0/6
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100
 no shutdown
end
wr
```

Step 4 — DHCP server access port (example: `Fa0/10` in VLAN 80)

```
conf t
interface fa0/10
 switchport mode access
 switchport access vlan 80
 spanning-tree portfast
 no shutdown
end
wr
```

Rollback (example port back to VLAN1):

```
conf t
interface fa0/10
 switchport mode access
 switchport access vlan 1
end
wr
```

2.2 SW-FLOORx (2960-24TT) – repeat per floor

Step 1 — Create needed VLANs (safe to create all)

```
enable
conf t
vlan 10,20,30,40,50,60,70,80,90,100
end
wr
```

Step 2 — Uplink trunk to core (example: `Gi0/1`)

```
conf t
interface gi0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100
 no shutdown
end
wr
```

Step 3 — Access ports for that floor (example FLOOR1 uses VLAN 10)

```
conf t
interface range fa0/1 - 0/22
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 no shutdown
end
wr
```

For each floor:

- FLOOR2: replace VLAN with `20`
- FLOOR3: `30`
- …
- FLOOR6: `60`

---

3) Internal router configuration (ROAS + DHCP relay + ASA uplink)

You configured the ROAS subinterfaces successfully (confirmed via `show ip int brief`).

3.1 ROAS trunk interface

```
enable
conf t
interface gi0/0/0
 no shutdown
end
wr
```

3.2 VLAN subinterfaces + gateways + DHCP relay (floors)

```
conf t
interface gi0/0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.80.10

interface gi0/0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip helper-address 192.168.80.10

interface gi0/0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip helper-address 192.168.80.10

interface gi0/0/0.40
 encapsulation dot1Q 40
 ip address 192.168.40.1 255.255.255.0
 ip helper-address 192.168.80.10

interface gi0/0/0.50
 encapsulation dot1Q 50
 ip address 192.168.50.1 255.255.255.0
 ip helper-address 192.168.80.10
```

```
interface gi0/0/0.60
 encapsulation dot1Q 60
 ip address 192.168.60.1 255.255.255.0
 ip helper-address 192.168.80.10
end
wr
```

3.3 Infrastructure VLANs (no DHCP relay required)

```
conf t
interface gi0/0/0.70
 encapsulation dot1Q 70
 ip address 192.168.70.1 255.255.255.0

interface gi0/0/0.80
 encapsulation dot1Q 80
 ip address 192.168.80.1 255.255.255.0

interface gi0/0/0.90
 encapsulation dot1Q 90
 ip address 192.168.90.1 255.255.255.0
end
wr
```

3.4 Router ↔ ASA transit interface + default route (Point A)

```
conf t
interface gi0/0/1
 ip address 10.0.0.1 255.255.255.252
 no shutdown
end
wr

conf t
ip route 0.0.0.0 0.0.0.0 10.0.0.2
end
wr
```

Rollback:

conf t
no ip route 0.0.0.0 0.0.0.0 10.0.0.2
end
wr

3.5 Verification on router

show ip interface brief
ping 192.168.80.10
ping 10.0.0.2
show ip route

---

4) DHCP Server configuration (central DHCP in VLAN 80)

4.1 Static IP settings

Desktop → IP Configuration:

- IP: `192.168.80.10`
- Mask: `255.255.255.0`
- Gateway: `192.168.80.1`
- DNS: optional (e.g., `8.8.8.8` for lab testing)

4.2 DHCP pools for floors (VLAN 10–60)

Services → DHCP → ON
Create one pool per floor:

Example **FLOOR1 (VLAN10)**

- Default Gateway: `192.168.10.1`
- Start IP: `192.168.10.100`
- Subnet Mask: `255.255.255.0`
- Max Users: e.g. `100`

Repeat:

- FLOOR2: `192.168.20.100`, GW `192.168.20.1`
- …
- FLOOR6: `192.168.60.100`, GW `192.168.60.1`

---

5) ASA firewall configuration (perimeter firewall + DMZ)

5.1 ASA interfaces (inside/dmz/outside)

```
enable
conf t

interface ethernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.2 255.255.255.252
 no shutdown

interface ethernet0/2
 nameif dmz
 security-level 50
 ip address 192.168.100.1 255.255.255.0
 no shutdown

interface ethernet0/0
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
 no shutdown

end
write memory
```

Verification:

```
show interface ip brief
```

5.2 ASA routing

Default route to ISP:

```
conf t
route outside 0.0.0.0 0.0.0.0 209.165.200.225
end
write memory
```

Route back to internal networks:

```
conf t
route inside 192.168.0.0 255.255.0.0 10.0.0.1
end
write memory
```

Verification:

```
show route
ping 10.0.0.1
ping 209.165.200.225
```

5.3 NAT

Inside → Internet (PAT):

```
conf t
object network INSIDE-NETS
 subnet 192.168.0.0 255.255.0.0
 nat (inside,outside) dynamic interface
end
write memory
```

Publish DMZ web server (static NAT):

```
conf t
object network DMZ-WEB
 host 192.168.100.10
 nat (dmz,outside) static 209.165.200.227
end
write memory
```

Verification:

show nat

5.4 Outside ACL (only allow HTTP/HTTPS to DMZ)

conf t
access-list OUTSIDE_IN extended permit tcp any host 209.165.200.227 eq 80
access-list OUTSIDE_IN extended permit tcp any host 209.165.200.227 eq 443
access-group OUTSIDE_IN in interface outside
end
write memory

Verification:

show access-list

Rollback (remove outside filter):

conf t
no access-group OUTSIDE_IN in interface outside
clear configure access-list OUTSIDE_IN
end
write memory

---

6) DMZ Server configuration

Desktop → IP:

- IP: `192.168.100.10`
- Mask: `255.255.255.0`
- Gateway: `192.168.100.1`

Services:

- HTTP ON (and HTTPS optional)

---

7) ISP router configuration (Internet simulation)

7.1 Interface to ASA

```
enable
conf t
interface gi0/0/0
 ip address 209.165.200.225 255.255.255.248
 no shutdown
end
wr
```

7.2 Optional “Internet” loopback for ping testing

```
conf t
interface loopback0
 ip address 8.8.8.8 255.255.255.255
end
wr
```

---

8) End-to-end verification tests (what we checked / should check)

8.1 Switches

```
show interfaces trunk
show vlan brief
```

8.2 Internal router

```
show ip int brief
```

ping 192.168.80.10
ping 10.0.0.2
show ip route

8.3 ASA

show interface ip brief
show route
show nat
show access-list
ping 10.0.0.1
ping 209.165.200.225
ping 192.168.100.10

8.4 PCs (per floor)

Desktop → IP Configuration → DHCP
Expected:

- VLAN10 PC gets `192.168.10.x` GW `192.168.10.1`
- VLAN20 PC gets `192.168.20.x` GW `192.168.20.1`
- …

8.5 Outside/Internet test

From an outside host (behind ISP):

- Browse to `http://209.165.200.227` (should reach DMZ web)
- Attempt access to internal VLAN IPs (should fail / be blocked)

---

9) Notes / design decisions recorded

- **Star topology** chosen over daisy-chain to reduce failure blast radius and simplify troubleshooting.
- **ROAS** used to route VLANs efficiently with one router interface + subinterfaces.
- **DHCP centralized** on a dedicated server (MGMT VLAN), using router **DHCP relay** (`ip helper-address`) for each floor VLAN.

- **ASA** used as a real perimeter firewall to meet assignment wording (“between internal router and Internet”) and to host the **DMZ** properly.
