**MULTILAYER CORE SWITCH (L3) — FULL CLI CONFIG**

| Config Area | Description |
| --- | --- |
| VLANs | Created VLANs 10 (Admin), 20 (HR), 30 (IT), 99 (Guest) |
| SVIs | Assigned IPs for each VLAN to act as gateways |
| Inter-VLAN Routing | Enabled ip routing |
| Trunk Ports | Trunked Gig1/0/1–4 to dist switches (allowed 10,20,30,99) |
| ASA1 Trunk Port | Trunked Gig1/0/5 to ASA1 (allowed VLAN 30, native 99) |
| DHCP Relay | Added ip helper-address to SVIs pointing to DHCP server |

enable

configure terminal

! Step 1: Create VLANs

vlan 10

name VLAN\_ADMIN

vlan 20

name VLAN\_HR

vlan 30

name VLAN\_IT

vlan 99

name VLAN\_GUEST

! Step 2: Create SVI interfaces for inter-VLAN routing

interface Vlan10

ip address 192.168.10.1 255.255.255.0

no shutdown

exit

interface Vlan20

ip address 192.168.20.1 255.255.255.0

no shutdown

exit

interface Vlan30

ip address 192.168.30.1 255.255.255.0

no shutdown

exit

interface Vlan99

ip address 192.168.99.1 255.255.255.0

no shutdown

exit

! Step 3: Enable routing on the switch

ip routing

! Step 4: Configure trunk ports to distribution switches

interface range GigabitEthernet1/0/1 - 1/0/4

description Trunk to Dept Distribution Switches

switchport mode trunk

switchport trunk native vlan 99

switchport trunk allowed vlan 10,20,30,99

no shutdown

exit

! Step 5: Trunk port to ASA1 (inside interface)

interface GigabitEthernet1/0/5

description Trunk to ASA1 Inside Interface

switchport mode trunk

switchport trunk native vlan 30

switchport trunk allowed vlan 30,99

no shutdown

exit

interface Vlan10

ip helper-address 192.168.50.10

interface Vlan20

ip helper-address 192.168.50.10

interface Vlan30

ip helper-address 192.168.50.10

interface Vlan99

ip helper-address 192.168.50.10

end

write memory

**DIST SWITCH CONFIGS — FULL CLI BY SWITCH**

| **Config Area** | **Description** |
| --- | --- |
| VLANs | Defined all VLANs (10, 20, 30, 99) for tag recognition |
| Trunk Port | Fa0/1 trunked to Core Switch |
| Access Ports | Fa0/2–5 assigned per VLAN: Switch0 → Admin (10) Switch1 → HR (20) Switch2 → IT (30) Switch3 → Guest (99) |
| Native VLAN | Trunks use VLAN 99 as native |

**🔹 Switch 0 – Admin Department (VLAN 10)**

enable

configure terminal

! VLANs

vlan 10

name VLAN\_ADMIN

vlan 20

name VLAN\_HR

vlan 30

name VLAN\_IT

vlan 99

name VLAN\_GUEST

! Trunk to multilayer switch (F0/1)

interface FastEthernet0/1

description Trunk to Core Switch

switchport mode trunk

switchport trunk native vlan 99

switchport trunk allowed vlan 10,20,30,99

no shutdown

exit

! Access ports for Admin PCs (F0/2 to F0/5)

interface range FastEthernet0/2 - 5

description Admin PCs

switchport mode access

switchport access vlan 10

no shutdown

exit

end

write memory

**🔹 Switch 1 – HR Department (VLAN 20)**

enable

configure terminal

! VLANs

vlan 10

name VLAN\_ADMIN

vlan 20

name VLAN\_HR

vlan 30

name VLAN\_IT

vlan 99

name VLAN\_GUEST

! Trunk to multilayer switch (F0/1)

interface FastEthernet0/1

description Trunk to Core Switch

switchport mode trunk

switchport trunk native vlan 99

switchport trunk allowed vlan 10,20,30,99

no shutdown

exit

! Access ports for HR PCs (F0/2 to F0/5)

interface range FastEthernet0/2 - 5

description HR PCs

switchport mode access

switchport access vlan 20

no shutdown

exit

end

write memory

**🔹 Switch 2 – IT Department (VLAN 30)**

enable

configure terminal

! VLANs

vlan 10

name VLAN\_ADMIN

vlan 20

name VLAN\_HR

vlan 30

name VLAN\_IT

vlan 99

name VLAN\_GUEST

! Trunk to multilayer switch (F0/1)

interface FastEthernet0/1

description Trunk to Core Switch

switchport mode trunk

switchport trunk native vlan 99

switchport trunk allowed vlan 10,20,30,99

no shutdown

exit

! Access ports for IT PCs (F0/2 to F0/5)

interface range FastEthernet0/2 - 5

description IT Support PCs

switchport mode access

switchport access vlan 30

no shutdown

exit

end

write memory

**🔹 (Bonus) Switch 3 – Guest VLAN (VLAN 99)**

(If you used a separate switch for Guest Wi-Fi)

enable

configure terminal

! VLANs

vlan 10

name VLAN\_ADMIN

vlan 20

name VLAN\_HR

vlan 30

name VLAN\_IT

vlan 99

name VLAN\_GUEST

! Trunk to multilayer switch (F0/1)

interface FastEthernet0/1

description Trunk to Core Switch

switchport mode trunk

switchport trunk native vlan 99

switchport trunk allowed vlan 10,20,30,99

no shutdown

exit

! Access ports for Guest PCs (F0/2 to F0/5)

interface range FastEthernet0/2 - 5

description Guest Wi-Fi Clients

switchport mode access

switchport access vlan 99

no shutdown

exit

end

write memory

**ASA1 – COMPLETE CLI CONFIGURATION**

| **Config Area** | **Description** |
| --- | --- |
| Inside Interface | Gig1/1 → 192.168.30.254 (connected to Core Switch) |
| Outside Interface | Gig1/3 → 100.100.100.1 (connected to Router) |
| NAT | PAT for all internal subnets to 100.100.100.1 |
| Default Route | Forwarded to 100.100.100.2 (Router) |
| Hostname & Save Config | Set hostname to ASA1 and saved config |

enable

configure terminal

! Step 1: Set hostname (optional)

hostname ASA1

! Step 2: Configure inside interface (to Multilayer Switch)

interface GigabitEthernet1/1

nameif inside

security-level 100

ip address 192.168.30.254 255.255.255.0

no shutdown

exit

! Step 3: Configure outside interface (to Internet Router)

interface GigabitEthernet1/3

nameif outside

security-level 0

ip address 100.100.100.1 255.255.255.0

no shutdown

exit

! Step 4: Default route to simulated internet (Router)

route outside 0.0.0.0 0.0.0.0 100.100.100.2

! Step 5: NAT internal network to external IP (Dynamic PAT)

object network INSIDE-NET

subnet 192.168.0.0 255.255.0.0

nat (inside,outside) dynamic interface

end

write memory

**ASA2 – COMPLETE CONFIGURATION**

| **Config Area** | **Description** |
| --- | --- |
| Outside Interface | Gig1/1 → 10.0.0.2 (to ASA1) |
| Inside Interface | Gig1/2 → 192.168.50.1 (to DMZ switch) |
| Honeynet Interface | Gig1/3 → 10.0.1.1 (to ASA3) |
| Default Route | Points to ASA1 (10.0.0.1) |
| Static Route to ASA3 | Routes 192.168.60.0/24 to 10.0.1.2 |
| NAT | NAT for DMZ subnet |
| ACL | Only allows Admin/IT to DMZ server (HTTP), blocks others |
| Access Group | Applied ACL on inside interface |

enable

configure terminal

! Step 1: Set hostname

hostname ASA2

! Step 2: Outside interface (connected to ASA1)

interface GigabitEthernet1/1

nameif outside

security-level 0

ip address 10.0.0.2 255.255.255.0

no shutdown

exit

! Step 3: Inside interface (connected to DMZ switch)

interface GigabitEthernet1/2

nameif inside

security-level 100

ip address 192.168.50.1 255.255.255.0

no shutdown

exit

! Step 4: Honeynet interface (to ASA3)

interface GigabitEthernet1/3

nameif honeynet

security-level 50

ip address 10.0.1.1 255.255.255.0

no shutdown

exit

! Step 5: Route to internet via ASA1

route outside 0.0.0.0 0.0.0.0 10.0.0.1

! Step 6: Route to honeypot subnet via ASA3

route honeynet 192.168.60.0 255.255.255.0 10.0.1.2

! Step 7: NAT for DMZ

object network DMZ-NET

subnet 192.168.50.0 255.255.255.0

nat (inside,outside) dynamic interface

! Step 8: ACL to restrict DMZ access

access-list LAN\_TO\_DMZ extended permit tcp 192.168.10.0 255.255.255.0 host 192.168.50.10 eq 80

access-list LAN\_TO\_DMZ extended permit tcp 192.168.30.0 255.255.255.0 host 192.168.50.10 eq 80

access-list LAN\_TO\_DMZ extended deny ip 192.168.0.0 255.255.0.0 host 192.168.50.10

access-list LAN\_TO\_DMZ extended permit ip any any

access-group LAN\_TO\_DMZ in interface inside

end

write memory

**SWITCH CONNECTED TO ASA2 – DMZ SWITCH CONFIG (2960)**

| **Config Area** | **Description** |
| --- | --- |
| VLAN 50 | Created for DMZ subnet |
| ASA2 Connection | Fa0/1 connected to ASA2 Gig1/2 |
| Server Connection | Fa0/2 connected to DMZ web server |
| Access Port Config | Mode access, VLAN 50 |

enable

configure terminal

! Step 1: Create VLAN for DMZ

vlan 50

name VLAN\_DMZ

exit

! Step 2: ASA2 connection (Fa0/1 → Gig1/2 of ASA2)

interface FastEthernet0/1

description Link to ASA2

switchport mode access

switchport access vlan 50

no shutdown

exit

! Step 3: Server connection (Fa0/2)

interface FastEthernet0/2

description DMZ Web Server

switchport mode access

switchport access vlan 50

no shutdown

exit

end

write memory

**ASA3 – COMPLETE CONFIGURATION (HONEYPOT FIREWALL)**

| **Config Area** | **Description** |
| --- | --- |
| Outside Interface | Gig1/1 → 10.0.1.2 (to ASA2) |
| Inside Interface | Gig1/2 → 192.168.60.1 (to honeypot switch) |
| Default Route | Points to ASA2 (10.0.1.1) |
| NAT | NAT for Honeypot subnet (optional) |
| ACL | Allows only Guest VLAN (192.168.99.0/24) to access honeypot |
| Access Group | Applied ACL on outside interface |

enable

configure terminal

! Step 1: Set hostname

hostname ASA3

! Step 2: Outside interface (connects to ASA2)

interface GigabitEthernet1/1

nameif outside

security-level 0

ip address 10.0.1.2 255.255.255.0

no shutdown

exit

! Step 3: Inside interface (connects to honeypot switch)

interface GigabitEthernet1/2

nameif inside

security-level 100

ip address 192.168.60.1 255.255.255.0

no shutdown

exit

! Step 4: Default route to ASA2 (for internet path)

route outside 0.0.0.0 0.0.0.0 10.0.1.1

! Step 5: NAT configuration (if needed)

object network HONEYPOT-NET

subnet 192.168.60.0 255.255.255.0

nat (inside,outside) dynamic interface

! Step 6: ACL to restrict honeypot access

access-list FROM\_INSIDE extended permit tcp 192.168.99.0 255.255.255.0 host 192.168.60.10 eq 80

access-list FROM\_INSIDE extended deny ip 192.168.0.0 255.255.0.0 host 192.168.60.10

! Step 7: Apply ACL to outside interface

access-group FROM\_INSIDE in interface outside

end

write memory

**SWITCH CONNECTED TO ASA3 – HONEYPOT SWITCH (2960)**

| Config Area | Description |
| --- | --- |
| VLAN 60 | Created for Honeypot subnet |
| ASA3 Connection | Fa0/1 connected to ASA3 Gig1/2 |
| Honeypot Server | Fa0/2 connected to server |
| Access Port Config | Mode access, VLAN 60 |

enable

configure terminal

! Step 1: Create VLAN for Honeypot zone

vlan 60

name VLAN\_HONEYPOT

exit

! Step 2: ASA3 connection (Fa0/1 → Gig1/2 of ASA3)

interface FastEthernet0/1

description Link to ASA3

switchport mode access

switchport access vlan 60

no shutdown

exit

! Step 3: Honeypot server connection (Fa0/2)

interface FastEthernet0/2

description Honeypot Server

switchport mode access

switchport access vlan 60

no shutdown

exit

end

write memory

**Router (2911) – Internet Simulation Config**

| **Config Area** | **Description** |
| --- | --- |
| Interface | Gig0/0 → 100.100.100.2 (to ASA1 outside) |
| Optional Static Route | Route back to ASA1 (ip route 0.0.0.0 0.0.0.0 100.100.100.1) |
| Optional Services | Can simulate web, DNS, FTP for testing (optional) |

enable

configure terminal

! Step 1: Configure Gig0/0 with public-facing IP

interface GigabitEthernet0/0

description Link to ASA1 (Internet-facing)

ip address 100.100.100.2 255.255.255.0

no shutdown

exit

! Step 2: (Optional) Add a static default route

! Not required unless you expand the topology

ip route 0.0.0.0 0.0.0.0 100.100.100.1

! Step 3: (Optional) Enable services like HTTP, DNS, etc.

! To simulate a public website or DNS server

end

write memory