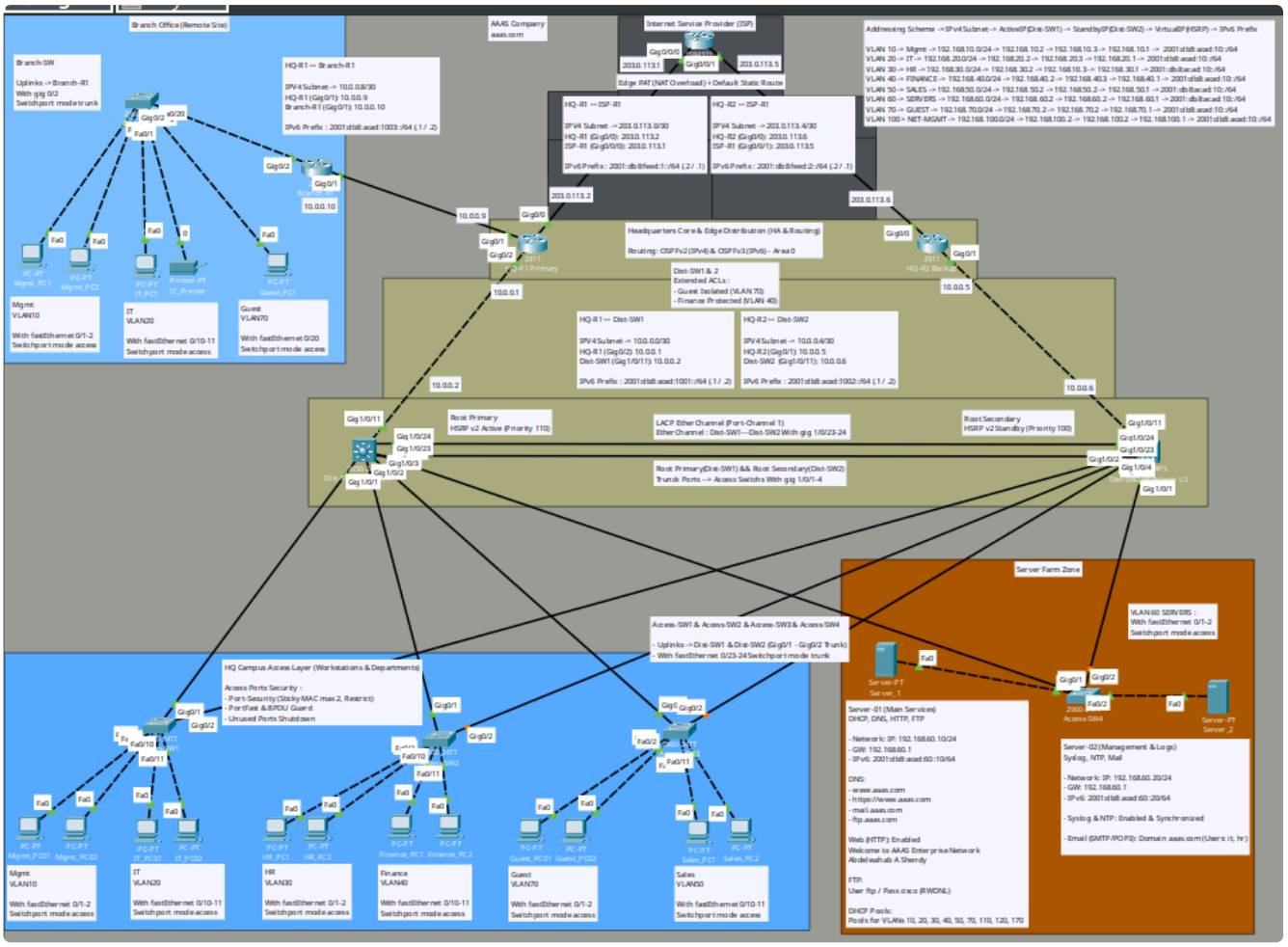
Designing & Securing an Enterprise Multi-Site Network Infrastructure (Dual-Stack IPv4, IPv6)

> Abdelwahab Ahmed Shendy
> linkedin.com/in/abdelwahab-a-shendy/
> abdelwahab-a-shendy.github.io

Project Requirements



- High Availability & Redundancy:
  - Deploy dual Distribution switches running HSRPv2 for default-gateway failover
  - LACP EtherChannel for link aggregation
  - Rapid-PVST+ for loop-free switching topology
- Dual-Stack Campus Routing:

    - Implement end-to-end IPv4 and IPv6 addressing across all VLANs, SVIs
    - Routed links using single-area dynamic routing (OSPFv2 & OSPFv3).
- Multi-Site Connectivity:
    - Connect the remote Branch Office via a routed WAN link and configure Router-on-a-Stick (802.1Q encapsulation) for local Inter-VLAN routing.
- Centralized Network Services:
    - Host dedicated infrastructure servers in a segregated Server Farm (VLAN 60) to provide DHCP Relay, Split DNS, HTTP Web, FTP file storage, local SMTP/POP3 Email, and centralized NTP & Syslog logging.
- Edge Translation & Internet Access:
    - Provide redundant ISP edge routing with static default routing and Port Address Translation (PAT / NAT Overload) for internal subnet internet access.
- Defense-in-Depth Hardening:
    - Restrict management planes with SSHv2 and session limits, enforce switchport-level Port Security (Sticky MAC) and BPDU Guard, disable unused interfaces, and enforce Extended ACLs for strict Guest isolation and Finance subnet protection.

Step 1 – Initial Device Configuration & Security Hardening

All Routers and Switchs With Change Username :

This section applies a standardized baseline configuration to all routers and switches, including device naming, local authentication, password encryption, SSHv2 secure remote access, console/VTY line security, session timeouts, and login banners :

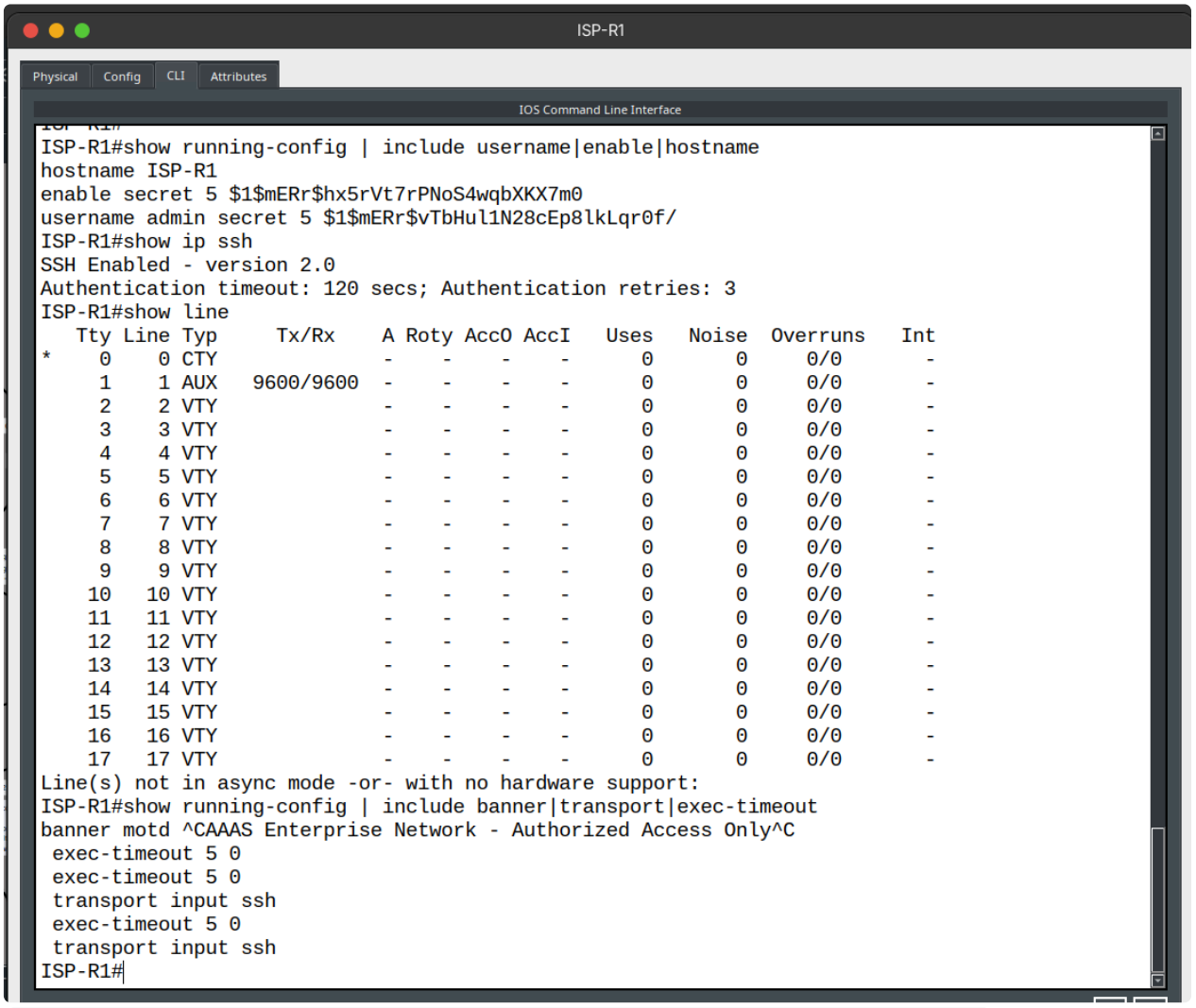
```
enable
configure terminal
```

```
//1. Hostname (Dist-SW1, Dist-SW2, HQ-R1, Access-SW1...)
hostname Dist-SW1

// Disable DNS Lookup & Set Domain Name
no ip domain-lookup
ip domain-name aaas.local

// Passwords & Local Admin User
enable secret cisco

// it depend what you want with (enable & Auth) level
username admin privilege 15 secret admin
// OR
username admin privilege 1 secret admin

service password-encryption

// SSH v2 Configuration
crypto key generate rsa general-keys modulus 2048
ip ssh version 2
ip ssh time-out 120
ip ssh authentication-retries 3

// Console Line Security
line console 0
 password ciscoline
 login local
 exec-timeout 5 0
 logging synchronous
 exit

// VTY Lines (SSH Only)
line vty 0 15
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
 exit

//Add Banner
banner motd #AAAS Enterprise Network - Authorized Access Only#
```

```
// Legal Warning Banner
end
write memory
```

Verification(On one of the devices):

- Quickly check the settings :



- `show running-config | include username|enable|hostname`
- `show ip ssh`
- `show line vty 0 15`
- `show running-config | include banner|transport|exec-timeout`

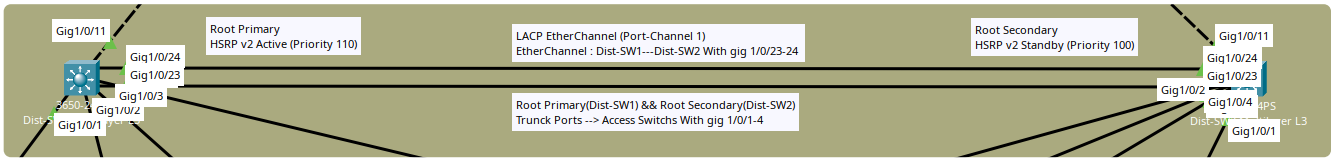
Step 2 – Layer 2 Infrastructure Configuration

VLANs Database and STP Configuration

Creates and standardizes VLANs across all switches and enables Rapid-PVST for Layer 2 loop prevention and redundancy :

```
conf t
vlan 10
 name MANAGEMENT
vlan 20
 name IT
vlan 30
 name HR
vlan 40
 name FINANCE
vlan 50
 name SALES
vlan 60
 name SERVERS
vlan 70
 name GUEST
vlan 99
 name NATIVE
vlan 100
 name NET-MGMT
exit
spanning-tree mode rapid-pvst
```

Distribution Layer Configuration :



Configures Dist-SW1 as the STP Root Primary and Dist-SW2 as the Root Secondary, with redundant trunk links and EtherChannel between the distribution switches.

- **On `Dist-SW1` (Root Primary):**

```
conf t
// Set the switch as the Root Primary for all VLANs
spanning-tree vlan 10,20,30,40,50,60,70,99,100 root primary
```

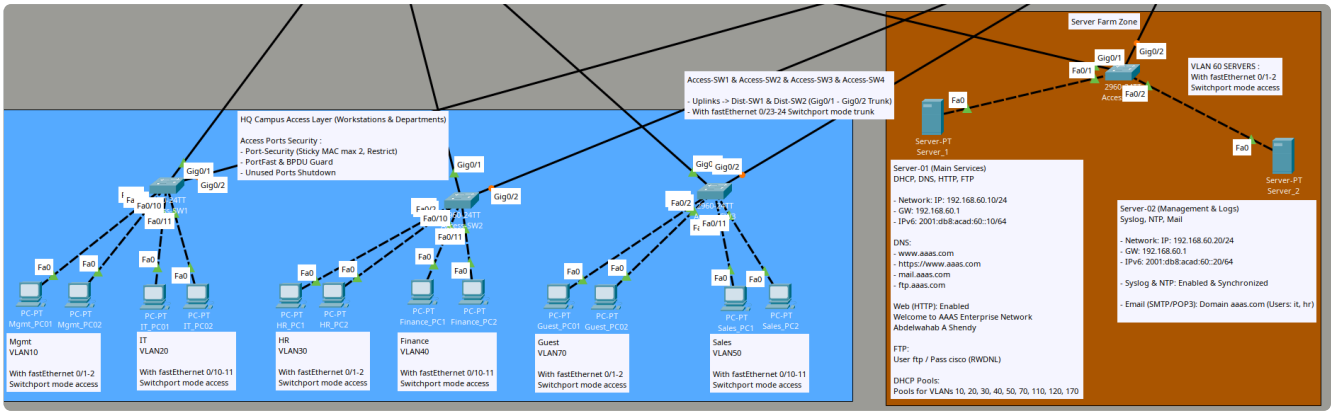
```
// EtherChannel with Dist-SW2 (Port-Channel 1)
interface range gigabitEthernet 1/0/23-24
//switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
 channel-group 1 mode active
exit

// Trunks ports leading to access switches
interface range gigabitEthernet 1/0/1-4
//switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
 no shutdown
exit
end
wr
```

- On `Dist-SW2` (Root Secondary):

```
conf t
// Set the switch as Root Secondary for all VLANs
spanning-tree vlan 10,20,30,40,50,60,70,99,100 root secondary

// EtherChannel with Dist-SW1 (Port-Channel 1)
interface range gigabitEthernet 1/0/23-24
// switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
 channel-group 1 mode active
exit

// Trunks ports leading to access switches
interface range gigabitEthernet 1/0/1-4
// switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
```

```
 no shutdown
exit
end
wr
```

Access Layer Configuration – HQ :



Configures trunk uplinks and assigns end-user and server ports to their corresponding VLANs, with PortFast and BPDU Guard enabled for edge-port protection.

- **On `Access-SW1` (Mgmt & IT):**

```
conf t
// Uplinks pointing to Dist-SW1 and Dist-SW2
interface range gigabitEthernet 0/1-2
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
 no shutdown
exit

// 10 VLAN ports (Management PCs)
interface range fa0/1 - 2
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
exit

// 20 VLAN ports (IT PCs)
interface range fa0/10 - 11
 switchport mode access
```

```
 switchport access vlan 20
 spanning-tree portfast
 spanning-tree bpduguard enable
exit
end
wr
```

- On `Access-SW2` (HR & Finance):

```
conf t
// Uplinks pointing to Dist-SW1 and Dist-SW2
interface range gigabitEthernet 0/1-2
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
 no shutdown
exit

// 30 VLAN ports (HR PCs)
interface range fa0/1 - 2
 switchport mode access
 switchport access vlan 30
 spanning-tree portfast
 spanning-tree bpduguard enable
exit

// 40 VLAN ports (Finance PCs)
interface range fa0/10 - 11
 switchport mode access
 switchport access vlan 40
 spanning-tree portfast
 spanning-tree bpduguard enable
exit
end
wr
```

- On `Access-SW3` (Guest & Sales):

```
conf t
// Uplinks pointing to Dist-SW1 and Dist-SW2
interface range gigabitEthernet 0/1-2
```

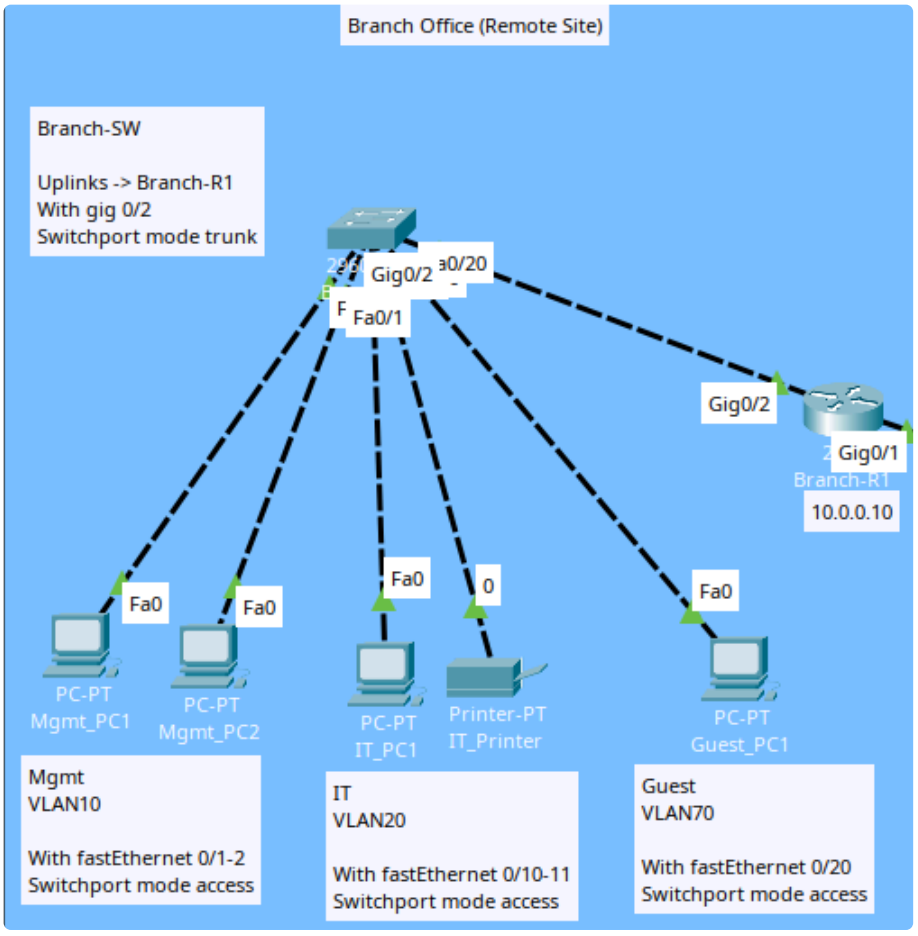
```
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
 no shutdown
exit

// 70 VLAN ports (Guest PCs)
interface range fa0/1 - 2
 switchport mode access
 switchport access vlan 70
 spanning-tree portfast
 spanning-tree bpduguard enable
exit

// 50 VLAN ports (Sales PCs)
interface range fa0/10 - 11
 switchport mode access
 switchport access vlan 50
 spanning-tree portfast
 spanning-tree bpduguard enable
exit
end
wr
```

- **On `Access-SW4` (Server Farm Switch):**

```
conf t
// Uplinks pointing to Dist-SW1 and Dist-SW2
interface range gigabitEthernet 0/1-2
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
 no shutdown
exit

// Server ports (VLAN 60)
interface range fa0/1 - 2
 switchport mode access
 switchport access vlan 60
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
exit
end
wr
```

Branch Configuration :



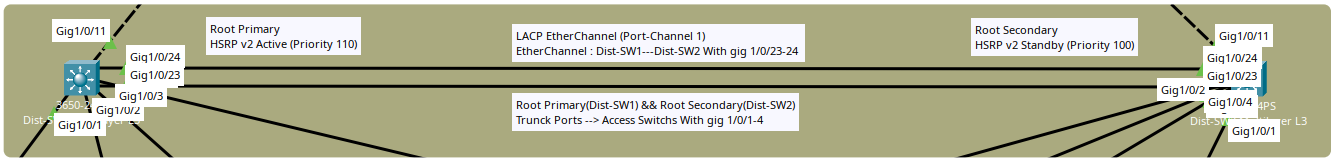
Configures the branch switch with a trunk uplink and assigns management, IT, and guest devices to their respective VLANs :

- Branch Switch Settings `Branch-SW` :

```
conf t
// Uplink directed to the router Branch-R1 (Trunk)
interface gig0/2
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
 no shutdown
exit

// Mgmt (VLAN 10)
interface range fa0/1 - 2
```

```
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
exit

// IT (VLAN 20)
interface range fa0/10 - 11
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
 spanning-tree bpduguard enable
exit

// Guest (VLAN 70)
interface fa0/20
 switchport mode access
 switchport access vlan 70
 spanning-tree portfast
 spanning-tree bpduguard enable
exit
end
wr
```

EtherChannel Configuration



Bundles multiple physical links between the distribution switches into a single logical Port-Channel using LACP for increased bandwidth and link redundancy.

- in `Dist-SW1` && `Dist-SW2` in same time :

```
interface range gigabitEthernet 1/0/23-24
switchport mode trunk
switchport trunk native vlan 99
switchport trunk allowed vlan 10,20,30,40,50,60,70,99,100
```

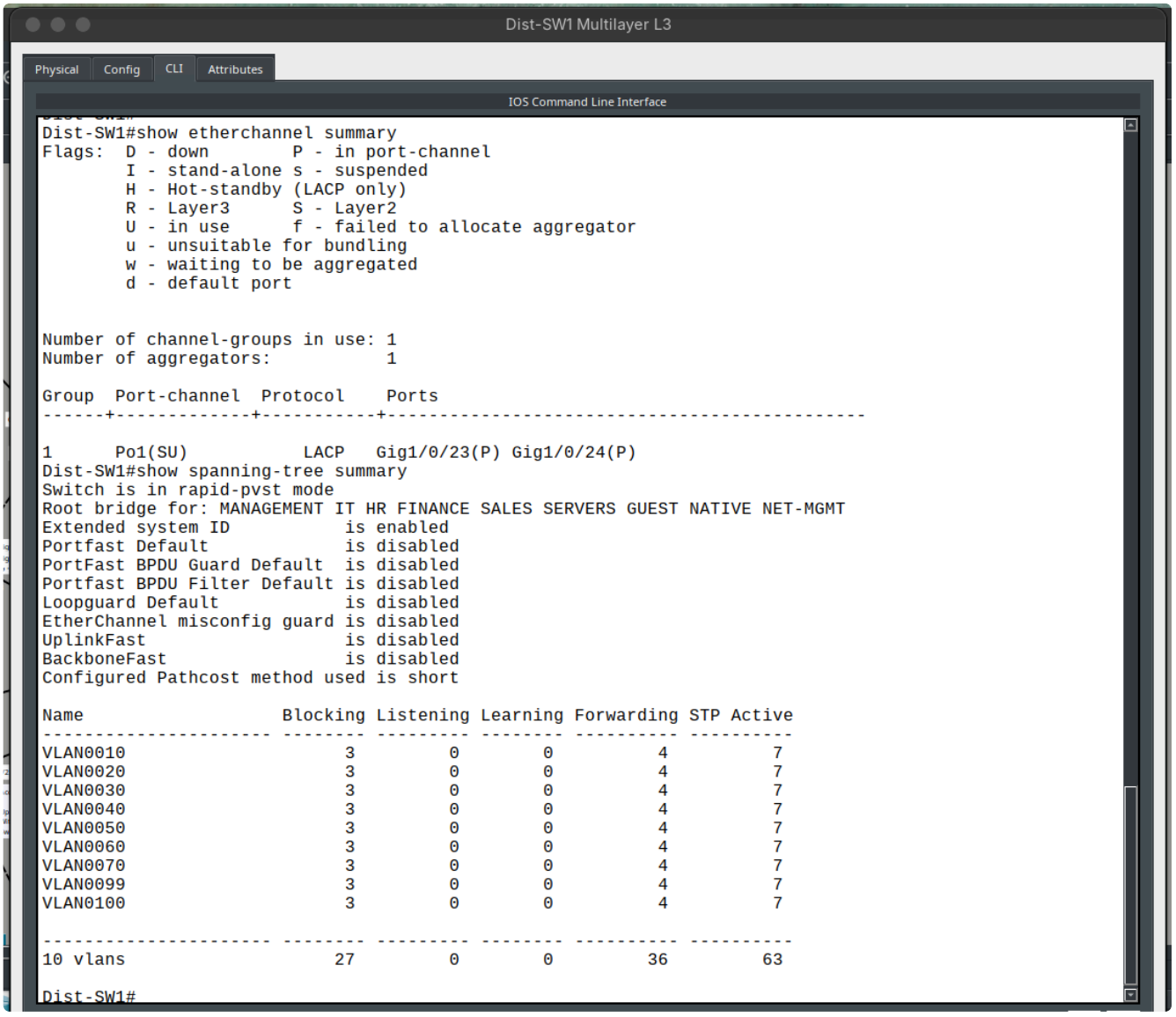
```
channel-group 1 mode active
exit
```

Layer 2 Verification :

Verifies VLAN assignments, trunk status, EtherChannel operation, and STP root placement to ensure the Layer 2 infrastructure is operating correctly.

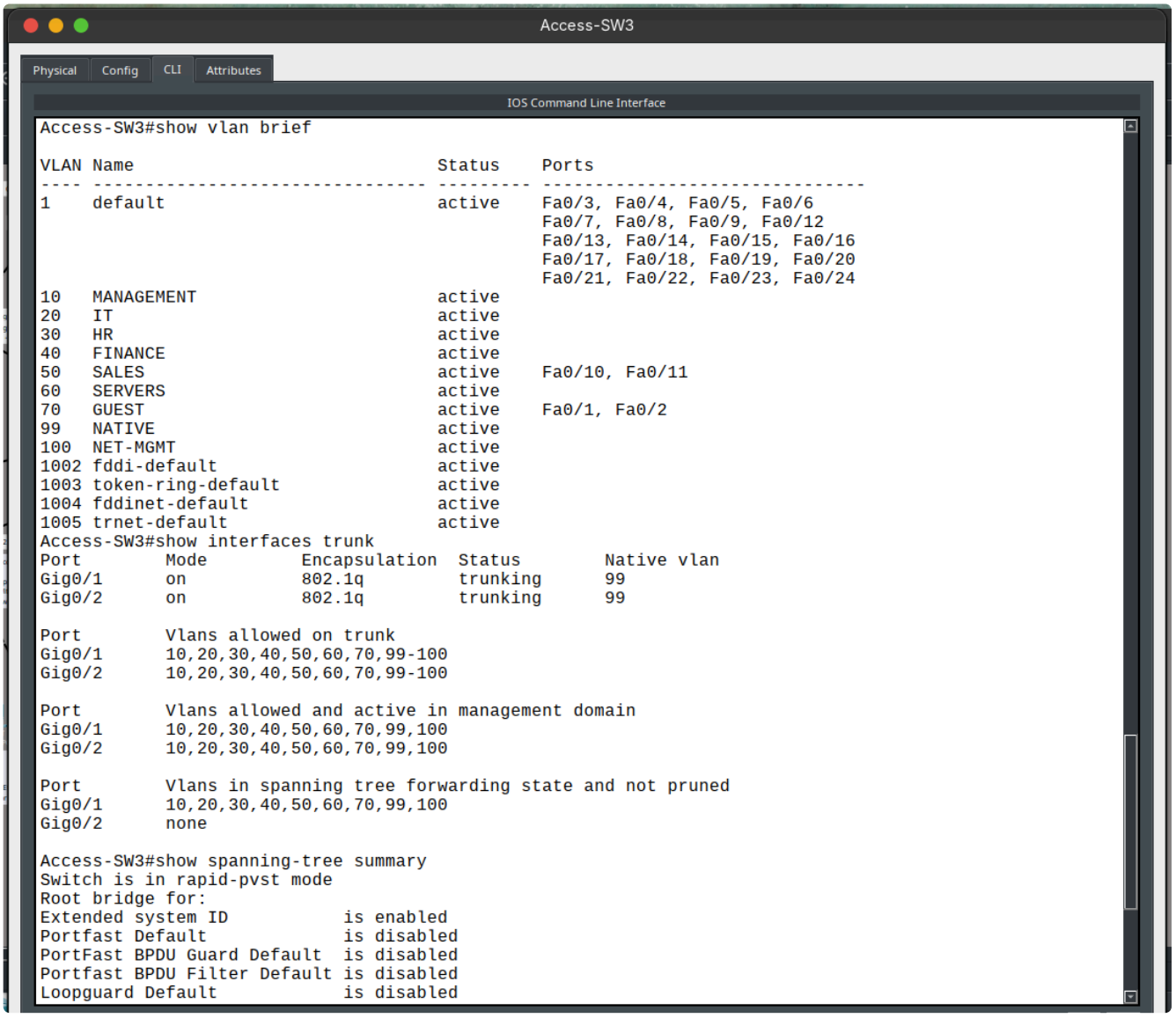
- Dist-SW1 - Root & EtherChannel Core :

```
show etherchannel summary
show spanning-tree summary
show interfaces trunk
```



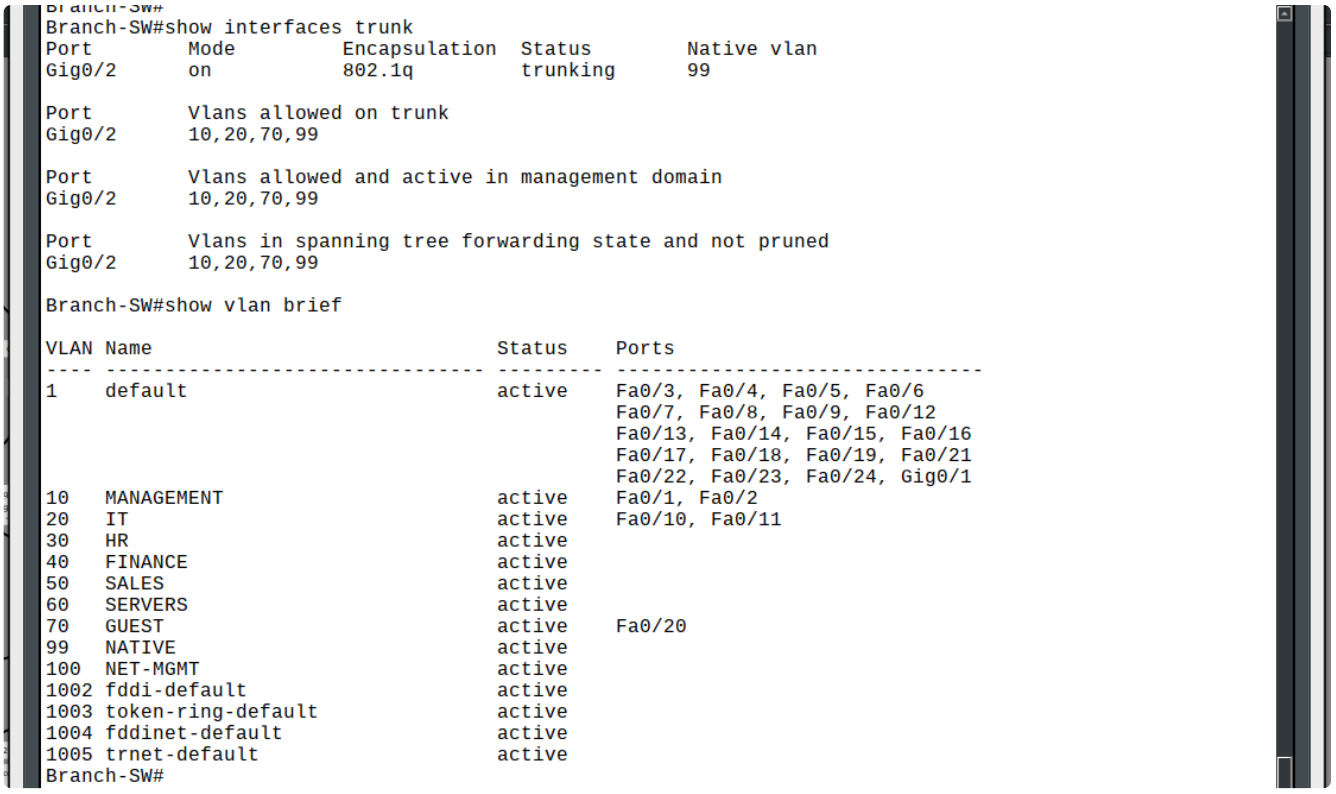
- Any Access-SW :

```
show vlan brief
show interfaces trunk
show spanning-tree summary
```



- Branch-SW - Remote Site Trunk & VLANs

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



```
Branch-SW#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/2      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig0/2      10,20,70,99

Port        Vlans allowed and active in management domain
Gig0/2      10,20,70,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/2      10,20,70,99

Branch-SW#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
10   MANAGEMENT                       active    Fa0/1, Fa0/2
20   IT                               active    Fa0/10, Fa0/11
30   HR                               active
40   FINANCE                          active
50   SALES                            active
60   SERVERS                          active
70   GUEST                            active    Fa0/20
99   NATIVE                           active
100  NET-MGMT                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Branch-SW#
```

Step 3 – Layer 3 & Gateway Redundancy Configuration (Headquarters Core)

Addressing Scheme & HSRP Design

Defines the IPv4/IPv6 addressing scheme for all VLANs and establishes HSRP virtual gateways for redundant default-gateway services

VLAN ID	Name	IPv4 Subnet	Dist-SW1 IP (Active)	Dist-SW2 IP (Standby)	Virtual IP (HSRP VIP)
VLAN 10	MANAGEMENT	192.168.10.0/24	192.168.10.2	192.168.10.3	192.168.10.1
VLAN 20	IT	192.168.20.0/24	192.168.20.2	192.168.20.3	192.168.20.1
VLAN 30	HR	192.168.30.0/24	192.168.30.2	192.168.30.3	192.168.30.1
VLAN 40	FINANCE	192.168.40.0/24	192.168.40.2	192.168.40.3	192.168.40.1
VLAN 50	SALES	192.168.50.0/24	192.168.50.2	192.168.50.3	192.168.50.1

VLAN ID	Name	IPv4 Subnet	Dist-SW1 IP (Active)	Dist-SW2 IP (Standby)	Virtual IP (HSRP VIP)
VLAN 60	SERVERS	192.168.60.0/24	192.168.60.2	192.168.60.3	192.168.60.1
VLAN 70	GUEST	192.168.70.0/24	192.168.70.2	192.168.70.3	192.168.70.1
VLAN 100	NET-MGMT	192.168.100.0/24	192.168.100.2	192.168.100.3	192.168.100.1

Dist-SW1 – HSRP Active

Enables Layer 3 routing and configures SVIs with IPv4/IPv6 addresses, making Dist-SW1 the preferred HSRP Active gateway using higher priority and preemption

- `Dist-SW1` commands (HSRP Active - Priority 110 with Preempt) :

```
conf t
// Activate Routing
ip routing
ipv6 unicast-routing

// VLAN 10 - MANAGEMENT
interface vlan 10
 ip address 192.168.10.2 255.255.255.0
 ipv6 address 2001:db8:acad:10::2/64
 standby version 2
 standby 10 ip 192.168.10.1
 standby 10 priority 110
 standby 10 preempt
 no shutdown
exit

// VLAN 20 - IT
interface vlan 20
 ip address 192.168.20.2 255.255.255.0
 ipv6 address 2001:db8:acad:20::2/64
 standby version 2
 standby 20 ip 192.168.20.1
 standby 20 priority 110
```

```
 standby 20 preempt
 no shutdown
exit

// VLAN 30 - HR
interface vlan 30
 ip address 192.168.30.2 255.255.255.0
 ipv6 address 2001:db8:acad:30::2/64
 standby version 2
 standby 30 ip 192.168.30.1
 standby 30 priority 110
 standby 30 preempt
 no shutdown
exit

// VLAN 40 - FINANCE
interface vlan 40
 ip address 192.168.40.2 255.255.255.0
 ipv6 address 2001:db8:acad:40::2/64
 standby version 2
 standby 40 ip 192.168.40.1
 standby 40 priority 110
 standby 40 preempt
 no shutdown
exit

// VLAN 50 - SALES
interface vlan 50
 ip address 192.168.50.2 255.255.255.0
 ipv6 address 2001:db8:acad:50::2/64
 standby version 2
 standby 50 ip 192.168.50.1
 standby 50 priority 110
 standby 50 preempt
 no shutdown
exit

// VLAN 60 - SERVERS
interface vlan 60
 ip address 192.168.60.2 255.255.255.0
 ipv6 address 2001:db8:acad:60::2/64
 standby version 2
```

```
 standby 60 ip 192.168.60.1
 standby 60 priority 110
 standby 60 preempt
 no shutdown
exit

// VLAN 70 - GUEST
interface vlan 70
 ip address 192.168.70.2 255.255.255.0
 ipv6 address 2001:db8:acad:70::2/64
 standby version 2
 standby 70 ip 192.168.70.1
 standby 70 priority 110
 standby 70 preempt
 no shutdown
exit

// VLAN 100 - NET-MGMT
interface vlan 100
 ip address 192.168.100.2 255.255.255.0
 ipv6 address 2001:db8:acad:100::2/64
 standby version 2
 standby 100 ip 192.168.100.1
 standby 100 priority 110
 standby 100 preempt
 no shutdown
exit
end
wr
```

Dist-SW2 – HSRP Standby

Configures redundant SVIs and HSRP standby gateways on Dist-SW2 to maintain gateway availability if Dist-SW1 fails

- `Dist-SW2` commands (HSRP Standby - Priority 100 default) :

```
conf t
// Activate Routing
ip routing
ipv6 unicast-routing
```

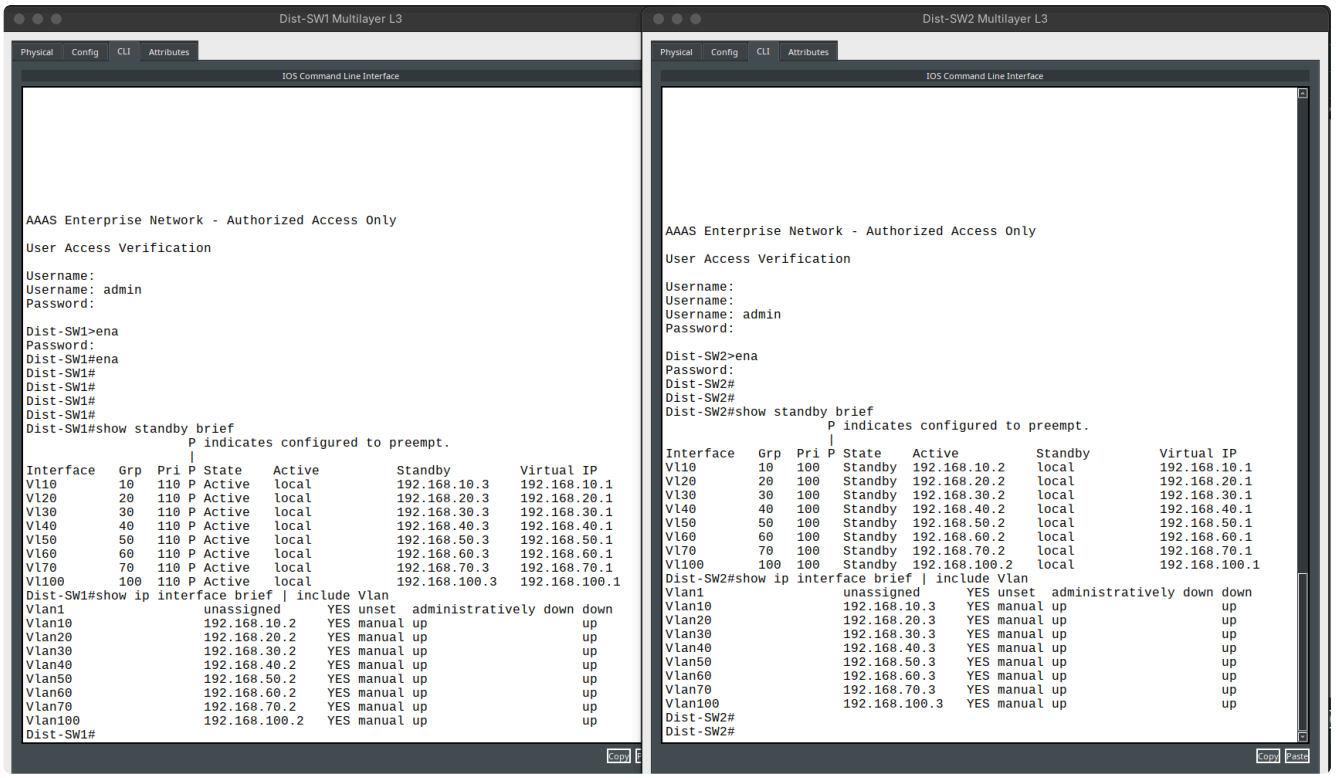
```
// VLAN 10 - MANAGEMENT
interface vlan 10
 ip address 192.168.10.3 255.255.255.0
 ipv6 address 2001:db8:acad:10::3/64
 standby version 2
 standby 10 ip 192.168.10.1
 no shutdown
exit

// VLAN 20 - IT
interface vlan 20
 ip address 192.168.20.3 255.255.255.0
 ipv6 address 2001:db8:acad:20::3/64
 standby version 2
 standby 20 ip 192.168.20.1
 no shutdown
exit

// VLAN 30 - HR
interface vlan 30
 ip address 192.168.30.3 255.255.255.0
 ipv6 address 2001:db8:acad:30::3/64
 standby version 2
 standby 30 ip 192.168.30.1
 no shutdown
exit

// VLAN 40 - FINANCE
interface vlan 40
 ip address 192.168.40.3 255.255.255.0
 ipv6 address 2001:db8:acad:40::3/64
 standby version 2
 standby 40 ip 192.168.40.1
 no shutdown
exit

// VLAN 50 - SALES
interface vlan 50
 ip address 192.168.50.3 255.255.255.0
 ipv6 address 2001:db8:acad:50::3/64
 standby version 2
```

```
 standby 50 ip 192.168.50.1
 no shutdown
exit

// VLAN 60 - SERVERS
interface vlan 60
 ip address 192.168.60.3 255.255.255.0
 ipv6 address 2001:db8:acad:60::3/64
 standby version 2
 standby 60 ip 192.168.60.1
 no shutdown
exit

// VLAN 70 - GUEST
interface vlan 70
 ip address 192.168.70.3 255.255.255.0
 ipv6 address 2001:db8:acad:70::3/64
 standby version 2
 standby 70 ip 192.168.70.1
 no shutdown
exit

// VLAN 100 - NET-MGMT
interface vlan 100
 ip address 192.168.100.3 255.255.255.0
 ipv6 address 2001:db8:acad:100::3/64
 standby version 2
 standby 100 ip 192.168.100.1
 no shutdown
exit
end
wr
```

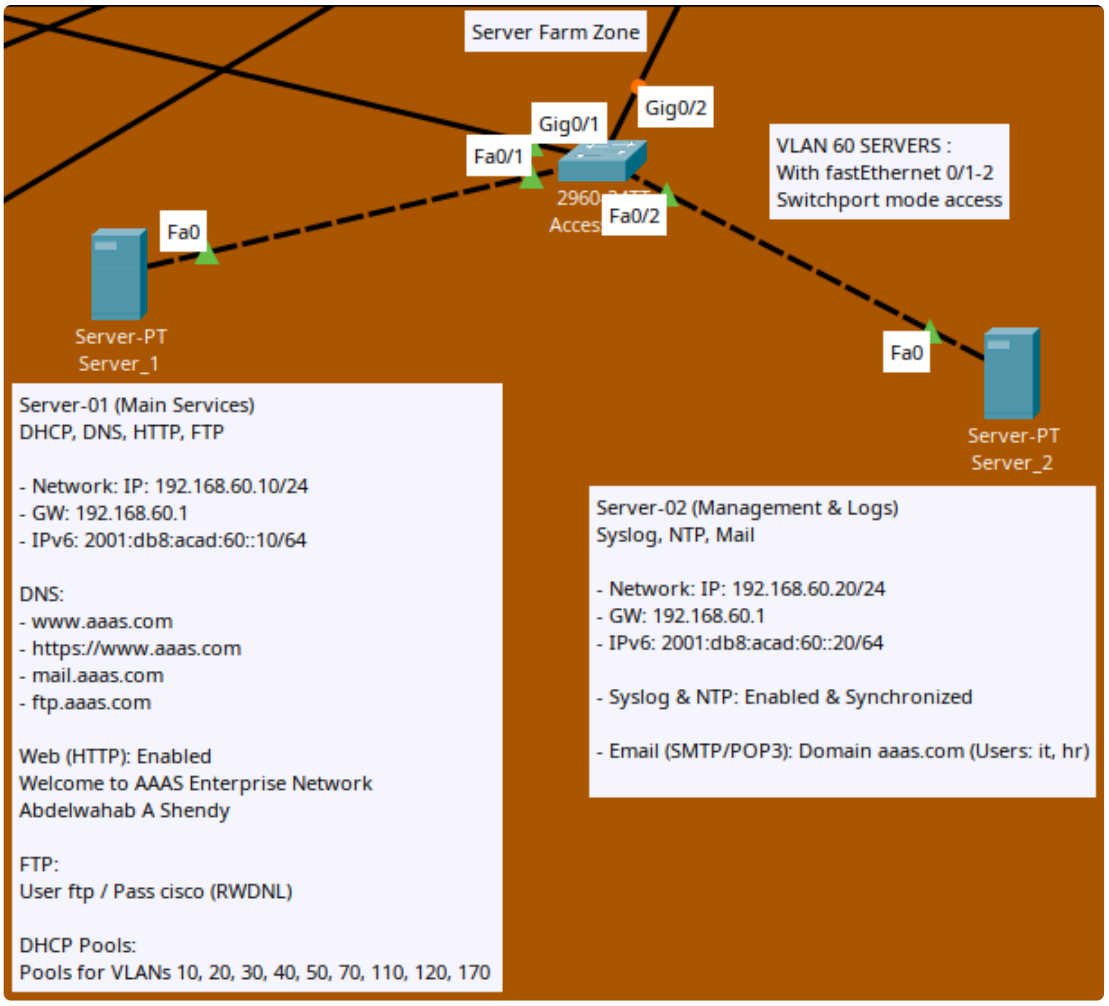
HSRP Verification :

- Execute the following command on `Dist-SW1` and `Dist-SW2` :

```
show standby brief
show ip interface brief | include Vlan
```



Step 4 – Centralized Services (Server Farm - VLAN 60) :



Server settings (Server-01 (DHCP, DNS, Web, FTP)) :

- 1. Open Server and In Desktop → IP Configuration :
  - **IPv4 Address:** `192.168.60.10`
  - **Subnet Mask:** `255.255.255.0`
  - **Default Gateway:** `192.168.60.1`
  - **DNS Server:** `192.168.60.10`
  - **IPv6 Address:** `2001:db8:acad:60::10/64`
  - **IPv6 Gateway:** `2001:db8:acad:60::1`
- 2. Configure services on `Server-01` :
- Open Services Tab on `Server-01` :
  - **HTTP Service:** Activate the service to **ON** and edit the `index.html` page to write the following:

```
<h1>Welcome to AAAS Enterprise Network</h1>
```

```
<h1>Abdelwahab A Shendy</h1>
```

- 3. **DNS Service:** Activate the service on **ON** and add the following record:
  - **DNS** Record :
    - **Name:** `www.aaas.local`
      - **Type:** A Record
      - **IP Address:** `192.168.60.10`
  - Add **Mail** record :
    - Name: `mail.aaas.com`
    - Type: A Record
    - IP Address: 192.168.60.20 (IP Address Server_2)
  - Add FTP record :
    - Name: `ftp.aaas.com`
    - Type: A Record
    - IP Address: 192.168.60.10
- 4. **DHCP Service:** Activate the service to **ON** and create the following pools, then press **Add/Save** for each pool :

POOL_GUEST	192.168.70.1	192.168.60.10	192.168.70.10	255.255.255.0	50	0.0.0.0	0.0.0.0
POOL_SALES	192.168.50.1	192.168.60.10	192.168.50.10	255.255.255.0	50	0.0.0.0	0.0.0.0
POOL_FINANCE	192.168.40.1	192.168.60.10	192.168.40.10	255.255.255.0	50	0.0.0.0	0.0.0.0
POOL_HR	192.168.30.1	192.168.60.10	192.168.30.10	255.255.255.0	50	0.0.0.0	0.0.0.0
POOL_IT	192.168.20.1	192.168.60.10	192.168.20.10	255.255.255.0	50	0.0.0.0	0.0.0.0
POOL_MGMT	192.168.10.1	192.168.60.10	192.168.10.10	255.255.255.0	50	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.60.0	255.255.255.0	512	0.0.0.0	0.0.0.0

5. Enable DHCP Relay on the Distribution Switches

Command `ip helper-address` must be written under all user SVLs interfaces to route DHCP Broadcast requests to `Server-01` :

- **Implemented on both switches (`Dist-SW1` and `Dist-SW2`):**

```
conf t
interface vlan 10
 ip helper-address 192.168.60.10
exit
```

```
interface vlan 20
 ip helper-address 192.168.60.10
exit
interface vlan 30
 ip helper-address 192.168.60.10
exit
interface vlan 40
 ip helper-address 192.168.60.10
exit
interface vlan 50
 ip helper-address 192.168.60.10
exit
interface vlan 70
 ip helper-address 192.168.60.10
exit
end
wr
```

6. Activating the **FTP** service on `Server-01` and testing file uploading and downloading from user devices:

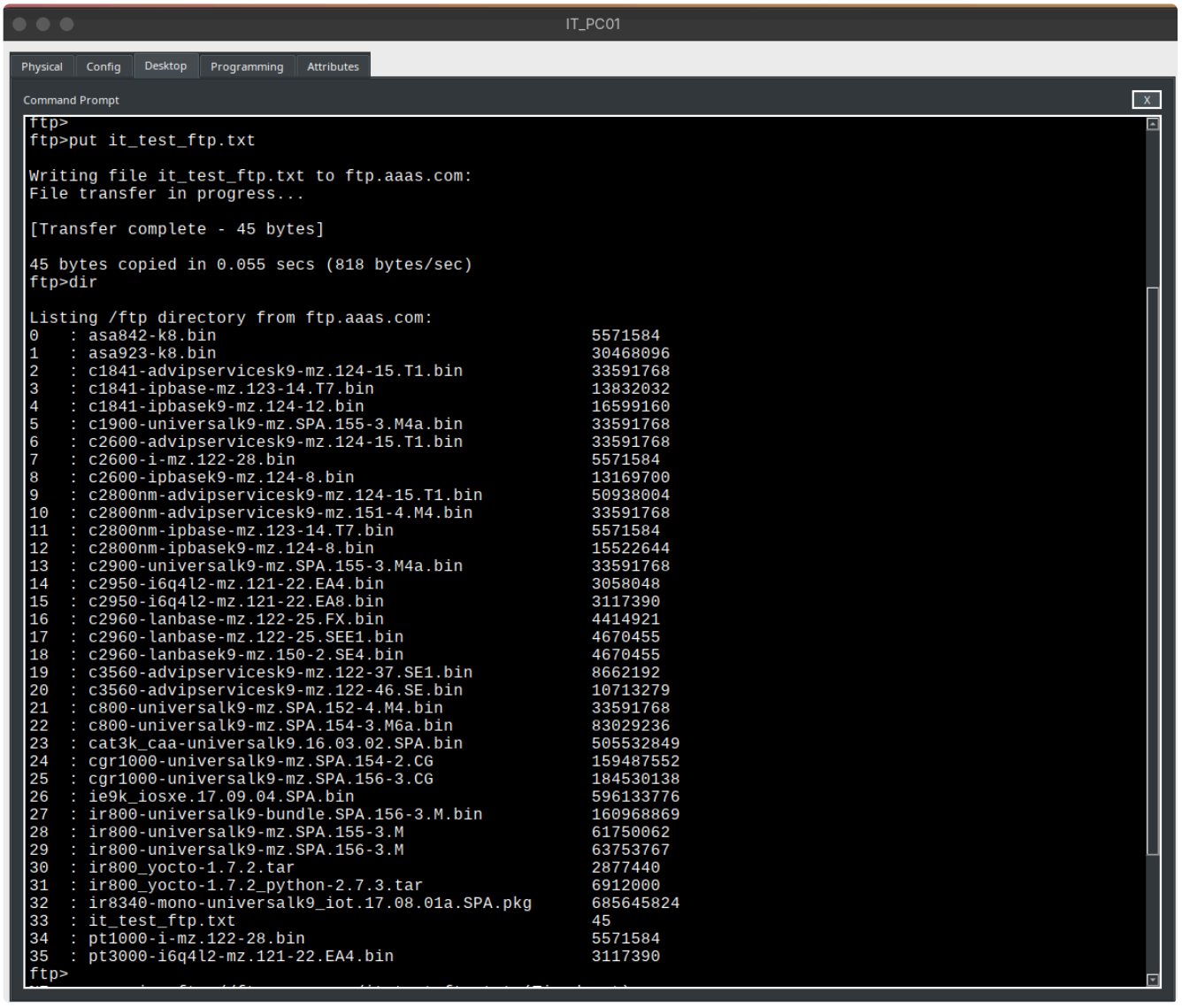
- Open **Services** Tab → Chooes FTP
- Services : ON
  - **Username:** `ftp` And **Password:** `cisco`
  - **Permissions:** Select all permissions by checking the following: `RWDNL` : `Write` , `Read` , `Delete` , `Rename` , `List`
    - And **Save**
- Service testing from any device :
  - Open `IT_PC01` → **Desktop Tab** → **Text Editor** And Add and Save : `This is a backup test file from IT department.`
  - With Name : `it_test_ftp.txt` and Save
  - Connecting to the server and uploading the file , in Same Device:

```
ftp ftp.aaas.com
```

> With User : `ftp` and Pass : `cisco`

- Upload to Server With command `put` :

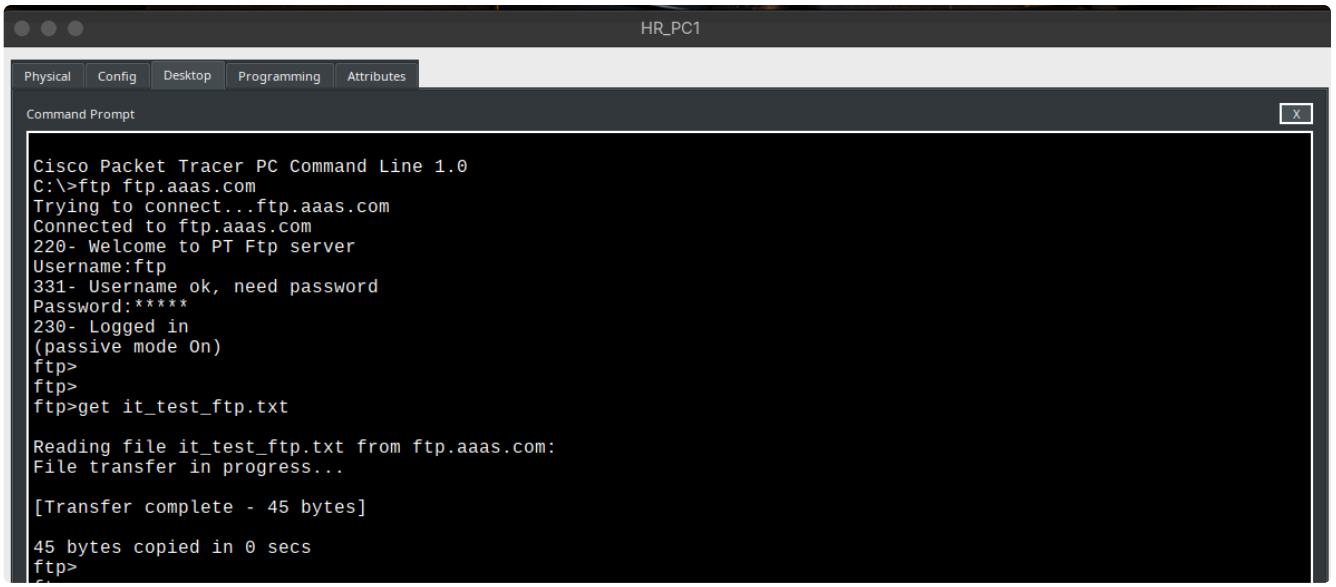
```
put it_test_ftp.txt
```



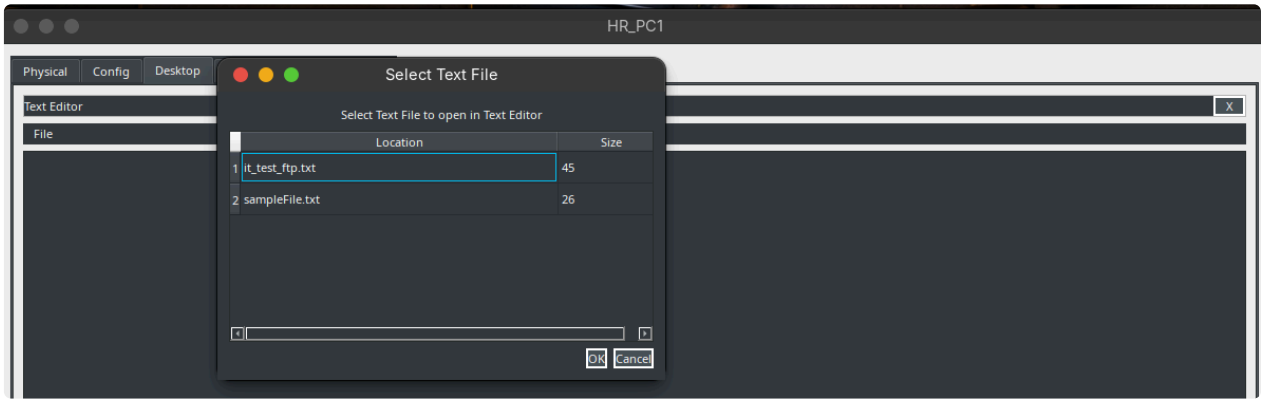
> Done

- In Anther Device Download With `HR_1` :
  - open CMD And Connection With FTP server and Get File

```
get it_test_ftp.txt
```



- i can see the file in Text Editor :



> `Server-01` Configuration is Done (DHCP, DNS, HTTP, FTP)

Server settings Server-02 (Syslog, NTP, Email) :

1. Open Server and In Desktop → IP Configuration :
   - **IPv4 Address:** `192.168.60.20`
   - **Subnet Mask:** `255.255.255.0`
   - **Default Gateway:** `192.168.60.1`
   - **DNS Server:** `192.168.60.10`
   - **IPv6 Address:** `2001:db8:acad:60::20/64`
   - **IPv6 Gateway:** `2001:db8:acad:60::1`
2. Configure the services to `Server-02` and connect the switches to it :
   - **On Server-02 (Services Tab):**
     - **Syslog:** Set the status to **ON**.
     - **NTP:** Set the status to **ON**, enter the correct date and time, and ensure that Authentication is enabled if desired, or leave it

without a key.

3. **Connecting the Switches to Server-02 (for recording and time synchronization):**
    - Apply these commands to `Dist-SW1` , `Dist-SW2` , and all Access switches :

```
conf t
// Time synchronization via NTP
ntp server 192.168.60.20

// Sending logs to Syslog Server
logging host 192.168.60.20
logging trap debugging
service timestamps log datetime msec
end
wr
```

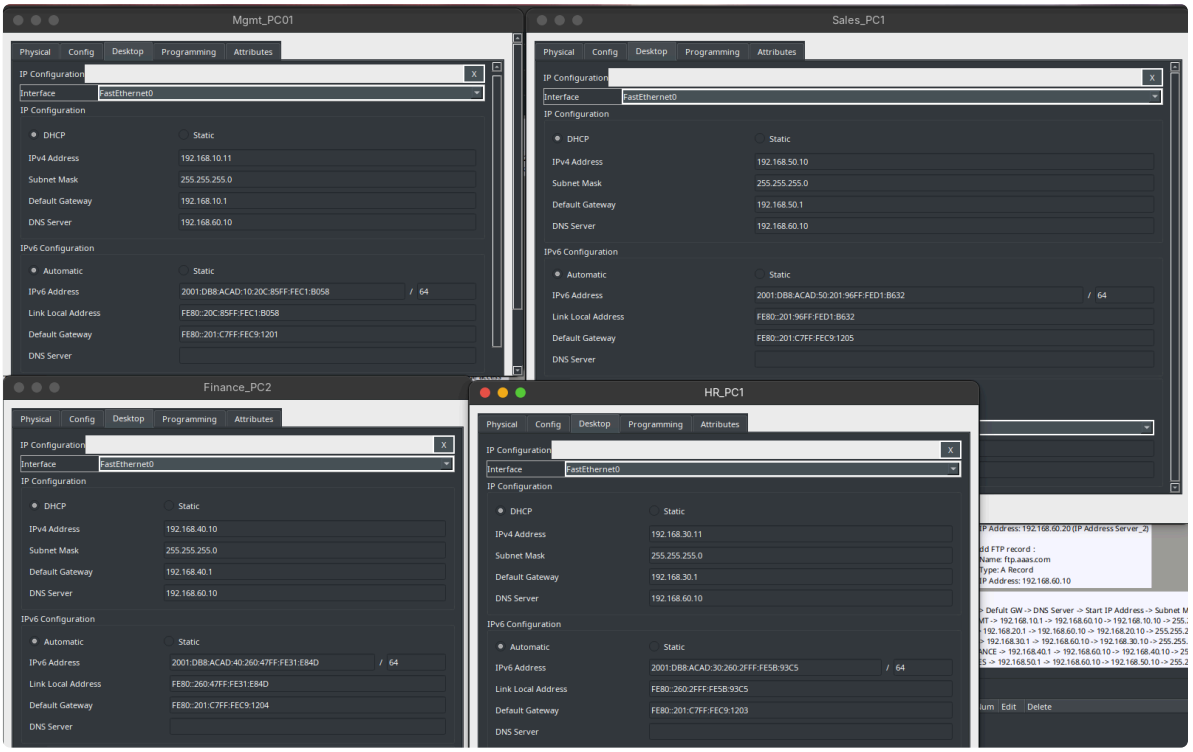
4. **EMAIL** service :
    - **Activating Services:** Make sure **ON** is selected for both `SMTP Service` and `POP3 Service` :
    - Add Domain Name :
        - In the `Domain Name` : `aaas.com` Add **Set**
    - **Add Users :**
        - **User:** `it` And **Password:** `cisco` And (`+`)
            - **User:** `hr` And **Password:** `cisco` And (`+`)
5. Configuring the email on users' devices (Clients Setup) :

- in devices (IT_1) :
    - open device and open **Desktop tab** → **Mail** and Add :
        - **Your Name:** `IT`
            - **Email Address:** `it@aaas.com`
            - **Incoming Mail Server:** `mail.aaas.com`
            - **Outgoing Mail Server (SMTP):** `mail.aaas.com`
            - **User Name:** `it`
            - **Password:** `cisco`
                - and **Save**

- in devices (HR_1) :
  - open device and open **Desktop tab** → **Mail** and Add :
    - **Your Name:** `HR`
      - **Email Address:** `hr@aaas.com`
      - **Incoming Mail Server:** `mail.aaas.com`
      - **Outgoing Mail Server (SMTP):** `mail.aaas.com`
      - **User Name:** `hr`
      - **Password:** `cisco`
        - and **Save**

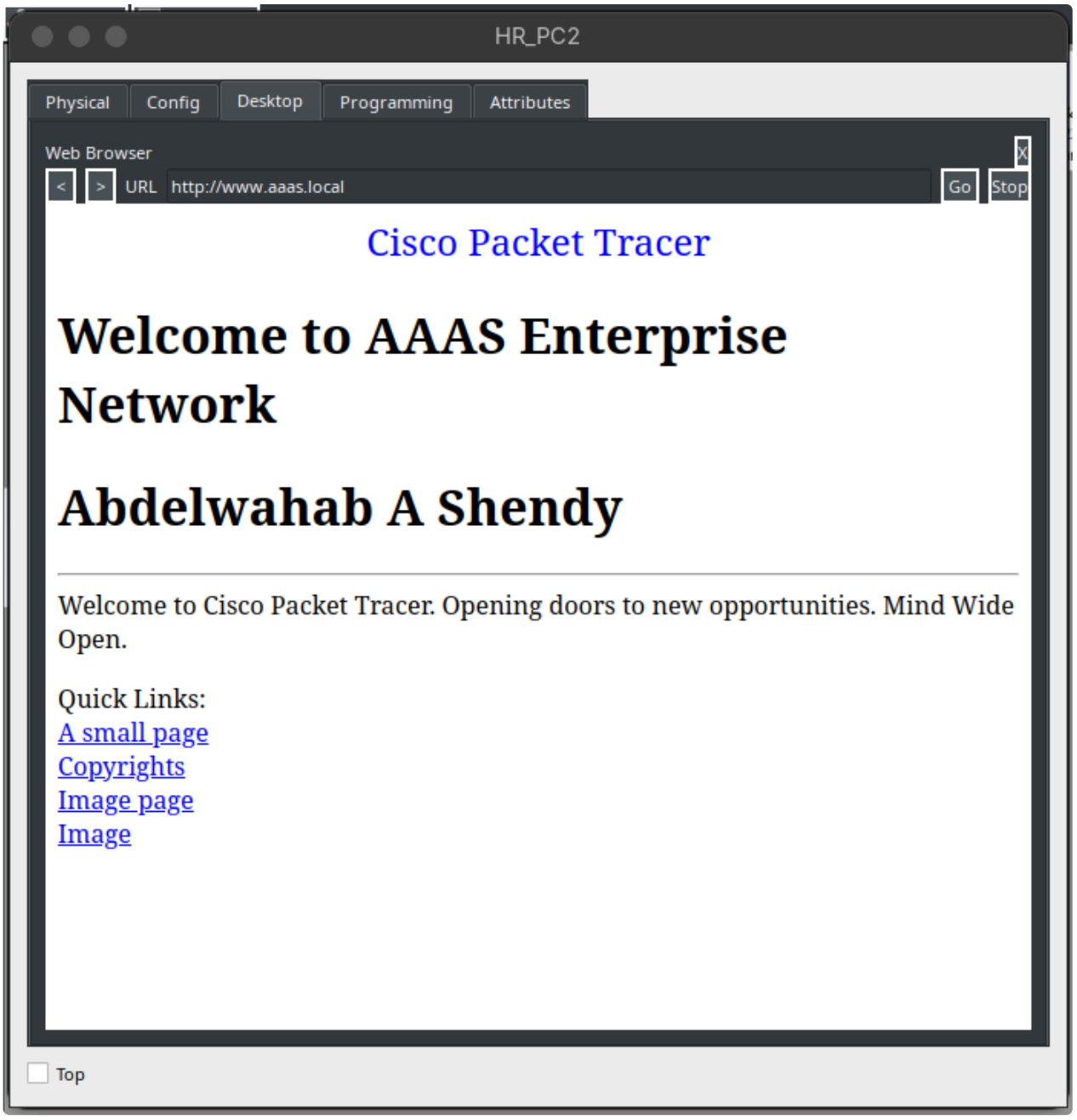
Verification Centralized Services

1. Verification **DHCP** (**Server-01**) :
   - in all devices → **IP Configuration** And choose **DHCP**



2. **Verification DNS & Web (Server-01)**:
   - **DNS & Web:** Open **Web Browser** and Write URL :

```
http://www.aaas.local
```



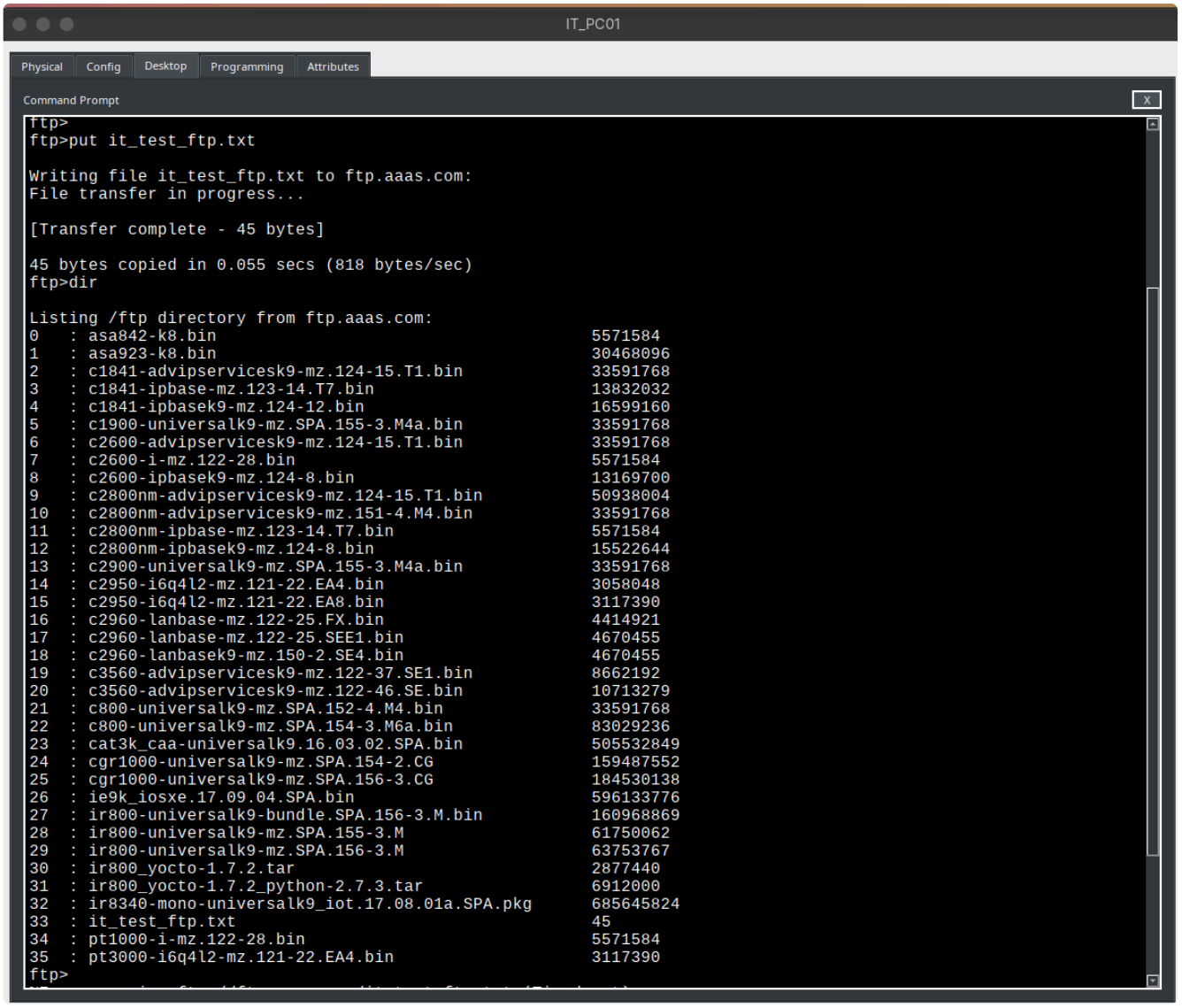
3. **Verification FTP (File Transfer) (Server-01):**

- Open `IT_PC01` → **Desktop Tab** → **Text Editor** And Add and Save : `This is a backup test file from IT department.`
  - With Name : `it_test_ftp.txt` and Save
  - Connecting to the server and uploading the file , in Same Device:

```
ftp ftp.aaas.com
```

- Upload to Server With command `put` :

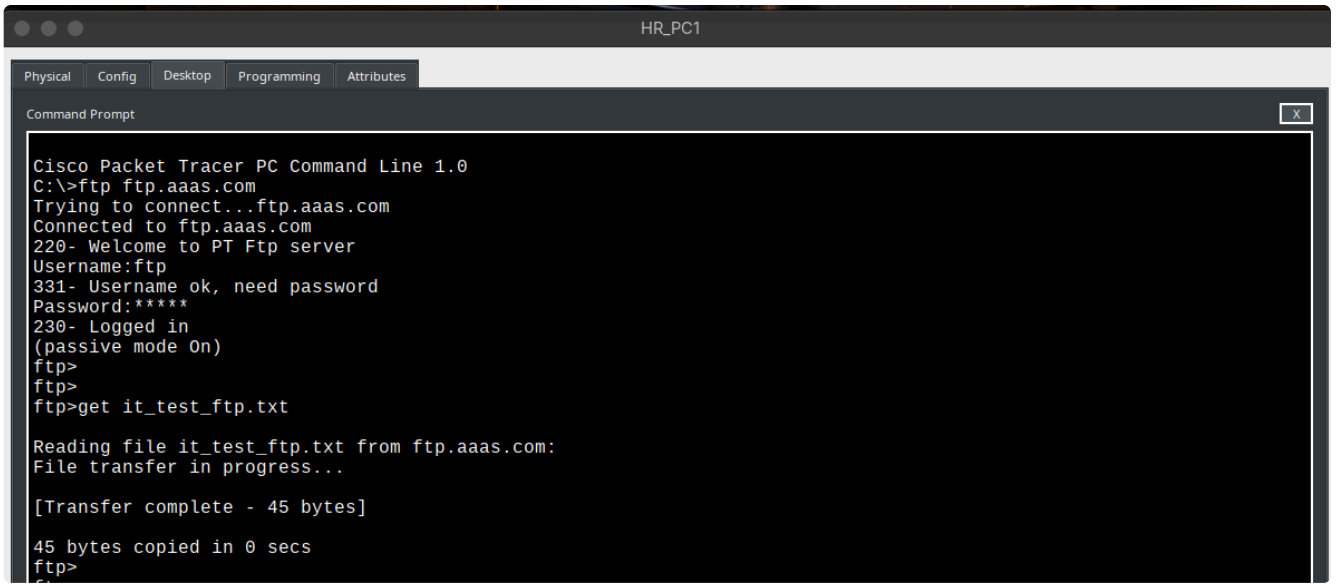
```
put it_test_ftp.txt
```



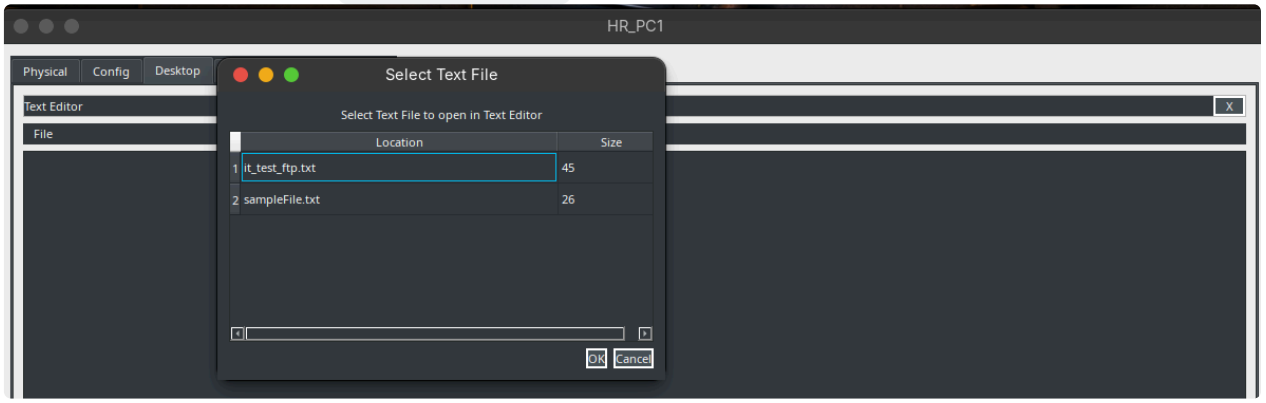
> Done

- In Anther Device Download With `HR_1` :
  - open CMD And Connection With FTP server and Get File :

```
get it_test_ftp.txt
```



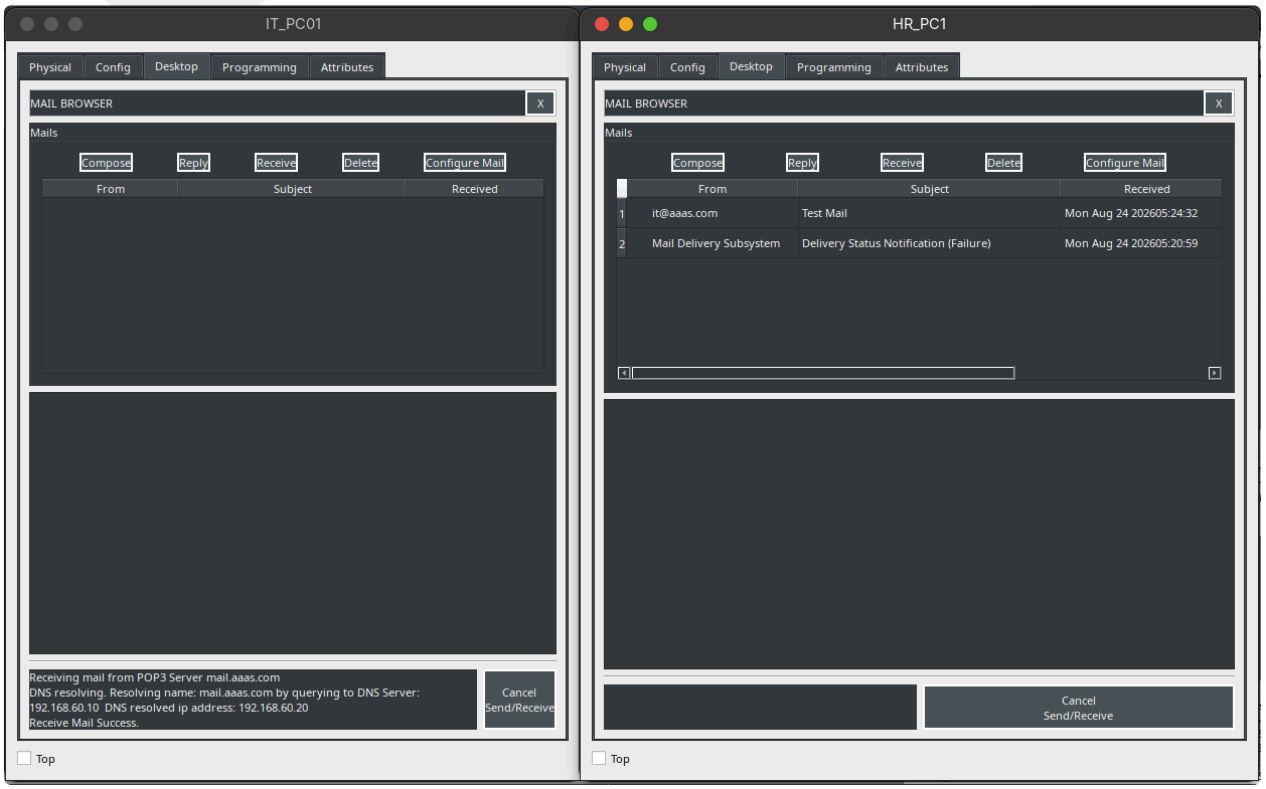
- I can see the file in `Text Editor` :



4. **Verification Email (SMTP / POP3) (Server-01)**

- From `IT_PC01` : Open **Mail**, press **Compose**, and send a message to `hr@aaas.com`

- From `HR_PC01` : Open **Mail** and press **Receive**



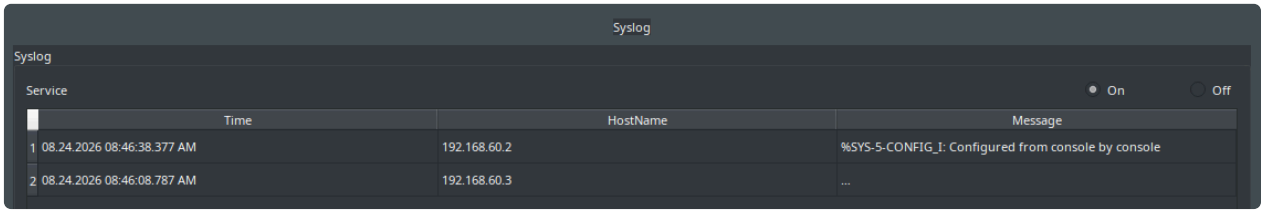
4. Verification **NTP & Syslog (Server-02)**

- In Switches (Ex : `Dist-SW1`):

```
show ntp status
show ntp associations
```

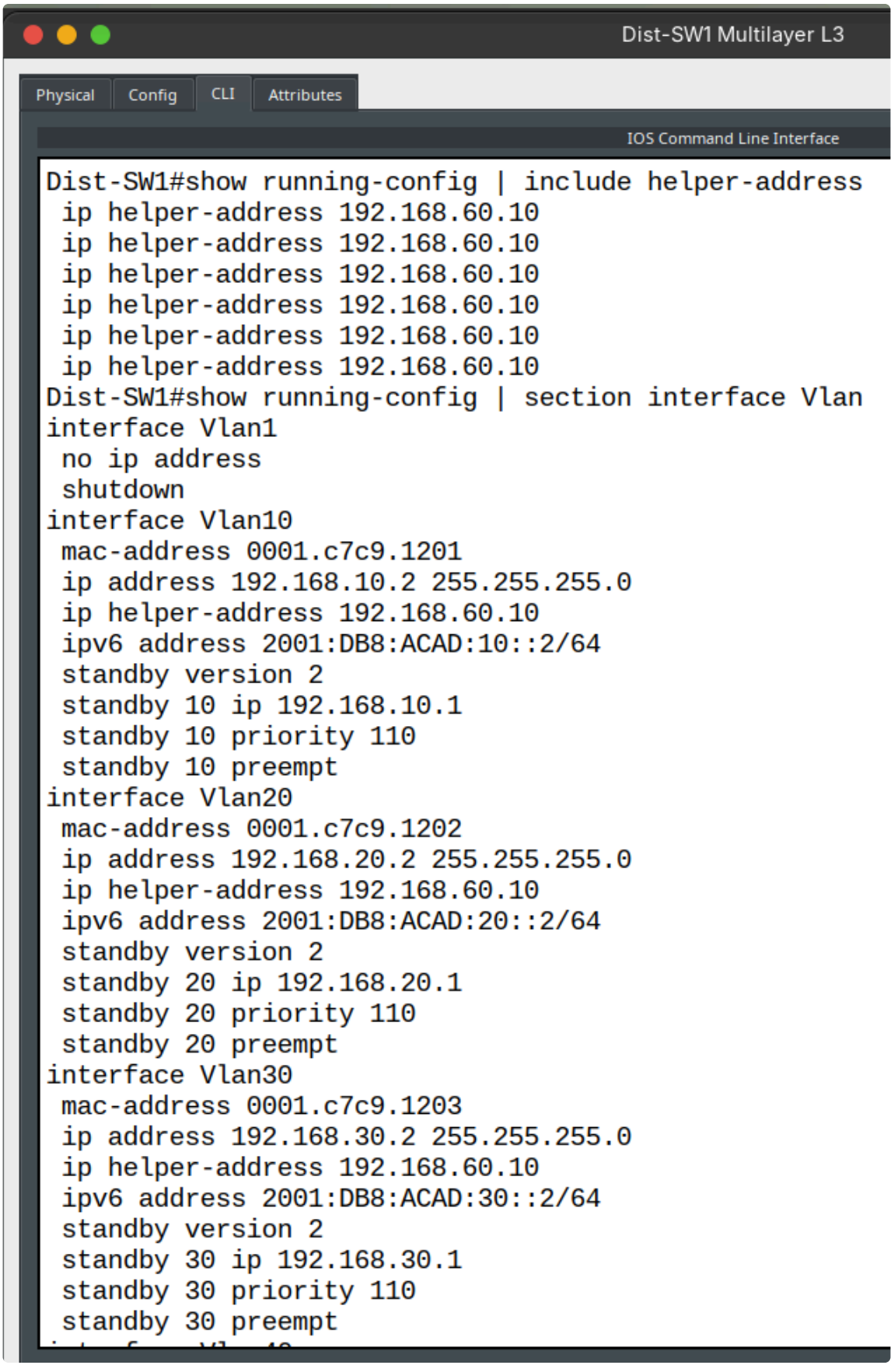
```
Dist-SW1#
Dist-SW1#
Dist-SW1#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.60.20
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is FFFFFFFFEE0B08A1.0000009F (9:15:13.159 UTC Mon Aug 24 2026)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 284.32 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll interval is 4, last update was 16 sec ago.
Dist-SW1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset           disp
*~192.168.60.20 127.127.1.1     1    87       16      240    0.00           0.00             0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Dist-SW1#
```

- Open **Services → Syslog** :

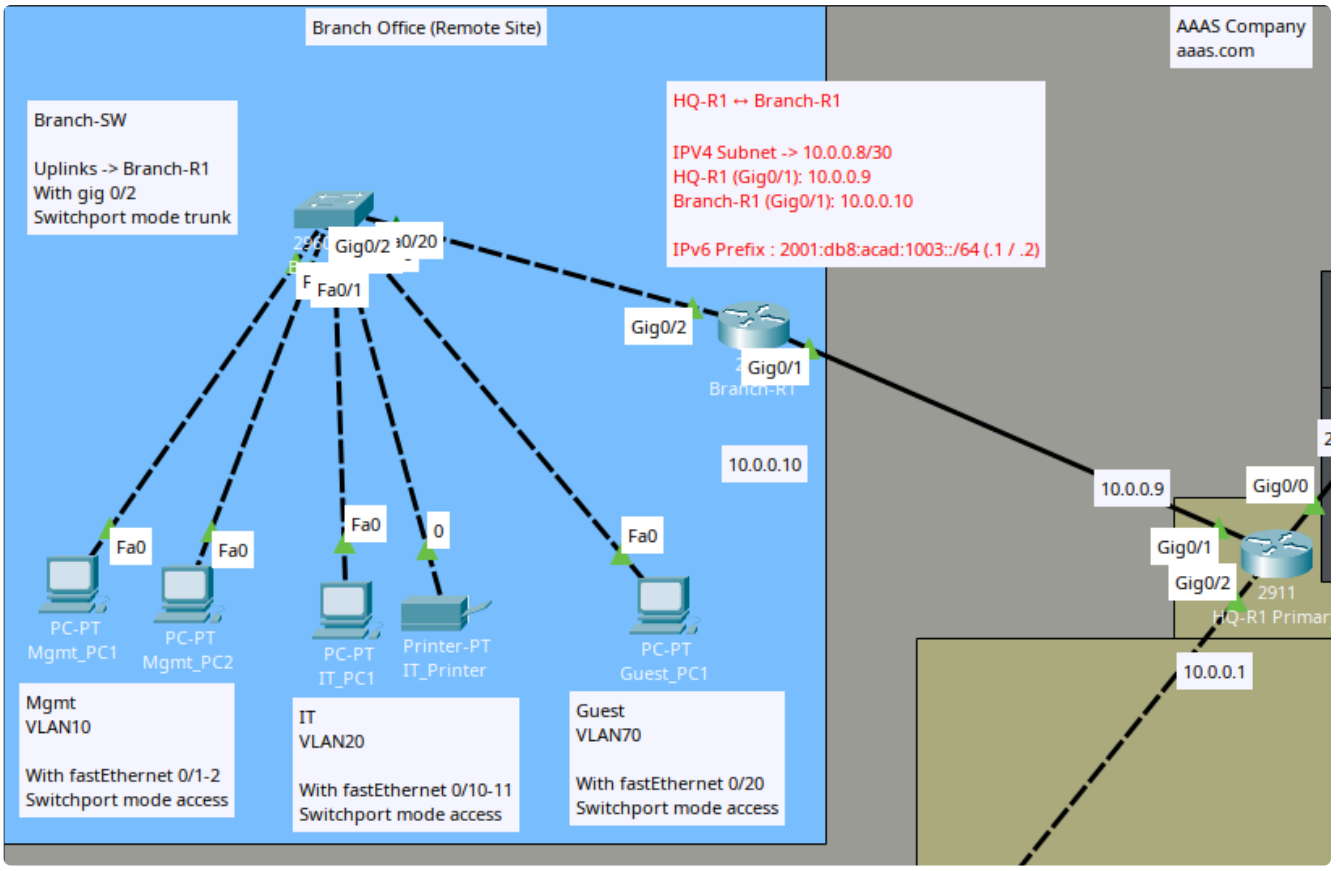


5. Verification DHCP Relay in Switch :

```
show running-config | include helper-address
show running-config | section interface Vlan
```



Step 5 – Branch Office Setup :



Branch-R1 – Router-on-a-Stick Configuration

Configures 802.1Q sub-interfaces on Branch-R1 to provide inter-VLAN routing and IPv4/IPv6 gateways for the branch VLANs.

Table of Addresses for Branch Departments :

VLAN ID	Section	IPv4 Subnet	Branch-R1 Gateway (Sub-interface IP)	IPv6 Prefix
VLAN 10	Branch Management	`192.168.110.0/24`	`192.168.110.1`	`2001:db8:acad:110::1/64`
VLAN 20	Branch IT & Printer	`192.168.120.0/24`	`192.168.120.1`	`2001:db8:acad:120::1/64`
VLAN 70	Branch Guest	`192.168.170.0/24`	`192.168.170.1`	`2001:db8:acad:170::1/64`
VLAN 99	Native VLAN	–	–	–

1. Router branch commands `Branch-R1` (Router-on-a-Stick) :

```
conf t
// Enable IPv6 Routing
ipv6 unicast-routing

// The main port leading to the switch without an IP address
interface gig0/2
 no ip address
 no shutdown
exit

// VLAN 10 (Branch Management)
interface gig0/2.10
 encapsulation dot1Q 10
 ip address 192.168.110.1 255.255.255.0
 ipv6 address 2001:db8:acad:110::1/64
 ip helper-address 192.168.60.10
 no shutdown
exit

// VLAN 20 (Branch IT & Printer)
interface gig0/2.20
 encapsulation dot1Q 20
 ip address 192.168.120.1 255.255.255.0
 ipv6 address 2001:db8:acad:120::1/64
 ip helper-address 192.168.60.10
 no shutdown
exit

// VLAN 70 (Branch Guest)
interface gig0/2.70
 encapsulation dot1Q 70
 ip address 192.168.170.1 255.255.255.0
 ipv6 address 2001:db8:acad:170::1/64
 ip helper-address 192.168.60.10
 no shutdown
exit

// VLAN 99 (Native VLAN Sub-interface)
interface gig0/2.99
 encapsulation dot1Q 99 native
 no shutdown
```

```
exit
end
wr
```

Branch-SW – Trunk & Access Configuration :

Configures the trunk link between Branch-SW and Branch-R1 and assigns branch endpoints to their respective VLANs with basic Layer 2 protection.

- Reviewing `Branch-SW` commands :

```
conf t
// The port connected to the router (Gig0/2) is 802.1Q Trunk
interface gig0/2
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,70,99
 no shutdown
exit

//  VLAN device ports 10 (Branch Mgmt PCs)
interface range fa0/1 - 2
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
exit

// VLAN device ports 20 (Branch IT & Printer)
interface range fa0/10 - 11
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
 spanning-tree bpduguard enable
exit

// VLAN device ports 70 (Branch Guest PC)
interface fa0/20
 switchport mode access
 switchport access vlan 70
 spanning-tree portfast
```

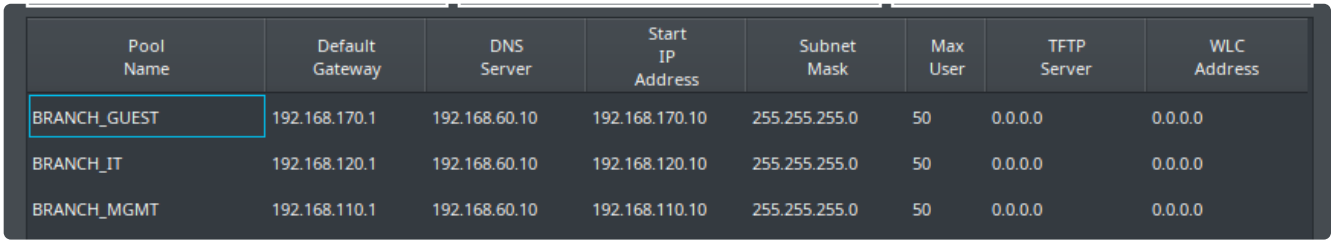
```
 spanning-tree bpduguard enable
exit
end
wr
```

Branch DHCP Configuration :

Creates dedicated DHCP pools on the HQ server to dynamically assign IP addresses, default gateways, and DNS information to branch clients.

- Add branch DHCP domains to `Server-01`
  - Open **Server-01** → **Services** → **DHCP** → Add Pools :

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Maxi Use
BRANCH_MGMT	192.168.110.1	192.168.60.10	192.168.110.10	255.255.255.0	50
BRANCH_IT	192.168.120.1	192.168.60.10	192.168.120.10	255.255.255.0	50
BRANCH_GUEST	192.168.170.1	192.168.60.10	192.168.170.10	255.255.255.0	50



Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
BRANCH_GUEST	192.168.170.1	192.168.60.10	192.168.170.10	255.255.255.0	50	0.0.0.0	0.0.0.0
BRANCH_IT	192.168.120.1	192.168.60.10	192.168.120.10	255.255.255.0	50	0.0.0.0	0.0.0.0
BRANCH_MGMT	192.168.110.1	192.168.60.10	192.168.110.10	255.255.255.0	50	0.0.0.0	0.0.0.0

Branch Connectivity Verification :

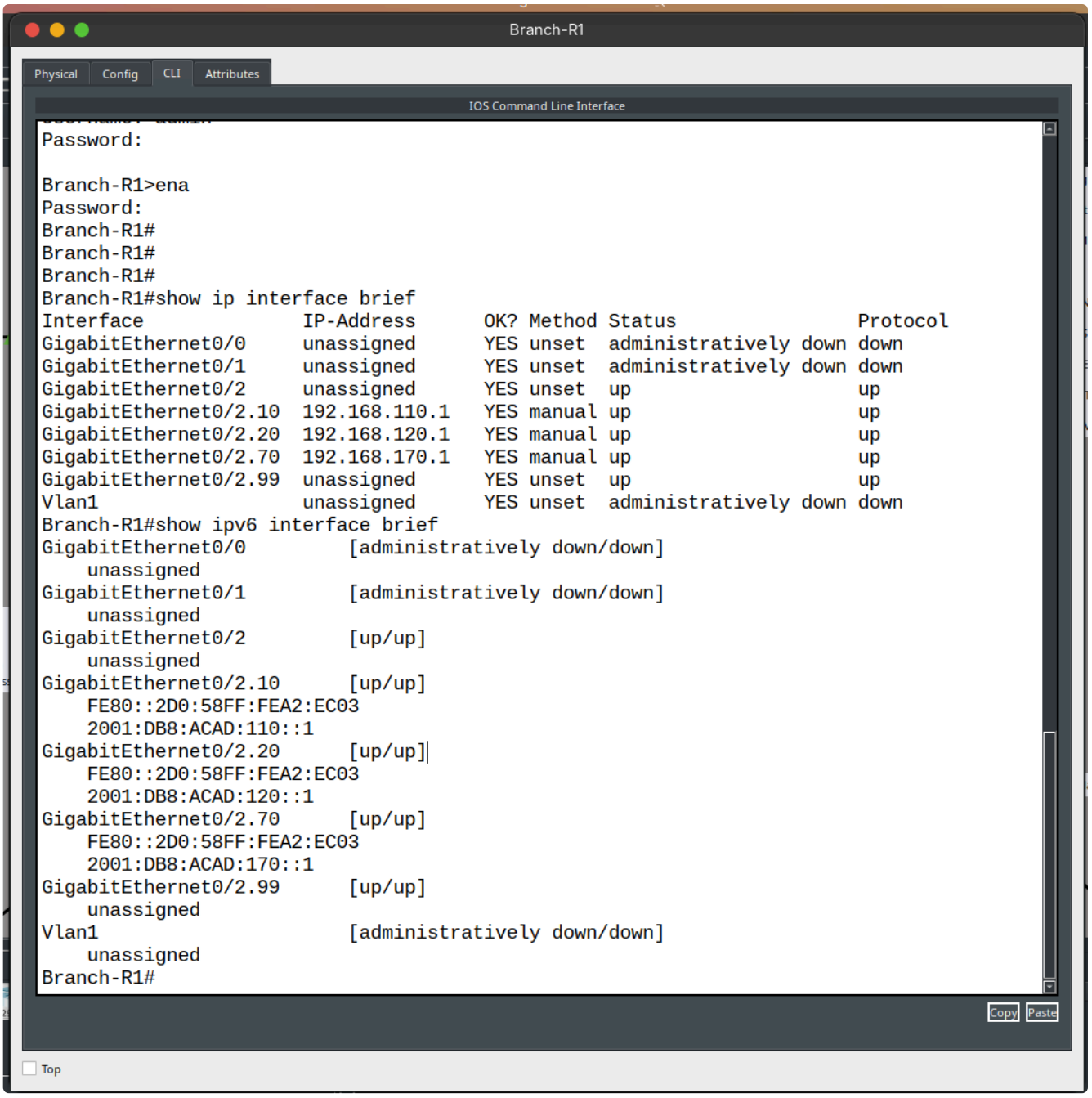
Verifies sub-interface status, gateway connectivity, and inter-VLAN communication within the branch network :

- Verification **Sub-interfaces** status :
- In `Branch-R1` :

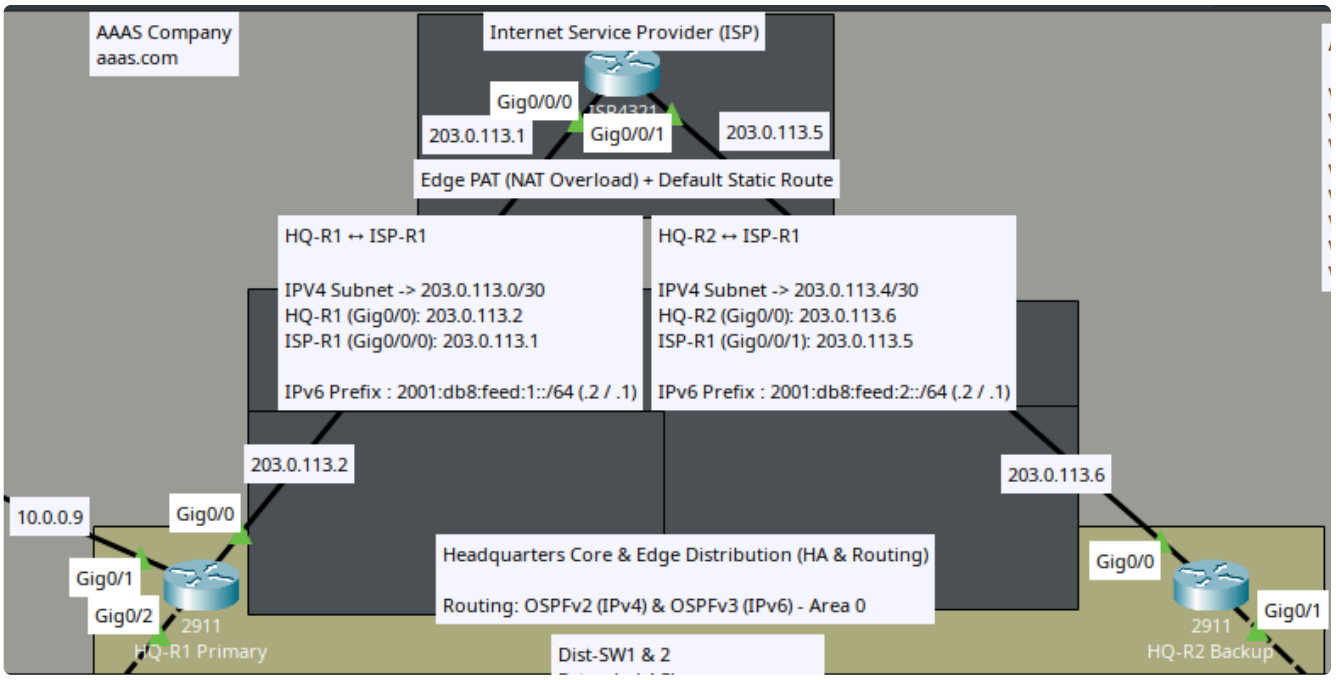
```
show ip interface brief
```

- To confirm the Dual-Stack on the branch, you can type :

```
show ipv6 interface brief
```



Step 6 – Dynamic Routing & WAN Connectivity (OSPF) :



Point-to-Point Addressing Scheme

Defines the IPv4 and IPv6 addressing for routed point-to-point links connecting the HQ, branch, and ISP infrastructure.

(Link)	IPv4 Subnet (/30)	First Device End	Second device end	IPv6 Prefix (/127 أو 64/)
HQ-R1 ↔ Dist-SW1	`10.0.0.0/30`	HQ-R1 (Gig0/2): `10.0.0.1`	Dist-SW1 (Gig1/0/11): `10.0.0.2`	`2001:db8:acad:1001::/64` (.1 / .2)
HQ-R2 ↔ Dist-SW2	`10.0.0.4/30`	HQ-R2 (Gig0/1): `10.0.0.5`	Dist-SW2 (Gig1/0/11): `10.0.0.6`	`2001:db8:acad:1002::/64` (.1 / .2)
HQ-R1 ↔ Branch-R1 (WAN)	`10.0.0.8/30`	HQ-R1 (Gig0/1): `10.0.0.9`	Branch-R1 (Gig0/1): `10.0.0.10`	`2001:db8:acad:1003::/64` (.1 / .2)
HQ-R1 ↔ ISP-R1 (Public)	`203.0.113.0/30`	HQ-R1 (Gig0/0): `203.0.113.2`	ISP-R1 (Gig0/0/0): `203.0.113.1`	`2001:db8:feed:1::/64` (.2 / .1)
HQ-R2 ↔ ISP-R1 (Public)	`203.0.113.4/30`	HQ-R2 (Gig0/0): `203.0.113.6`	ISP-R1 (Gig0/0/1): `203.0.113.5`	`2001:db8:feed:2::/64` (.2 / .1)

Distribution Layer – OSPF Configuration

Configures the distribution switches with routed uplinks and OSPFv2/OSPFv3 to exchange internal IPv4 and IPv6 routes dynamically.

- In `Dist-SW1`:

```
conf t

// Convert the port connected to HQ-R1 to a Routed Port
interface GigabitEthernet 1/0/11
 no switchport
 ip address 10.0.0.2 255.255.255.252
 ipv6 address 2001:db8:acad:1001::2/64
 no shutdown
exit

// Enable OSPFv2 (IPv4)
router ospf 1
 router-id 1.1.1.1
 passive-interface default
 no passive-interface gig1/0/11
 // no passive-interface port-channel 1
 network 10.0.0.0 0.0.0.3 area 0
 network 192.168.0.0 0.0.255.255 area 0
exit

// Enable OSPFv3 (IPv6)
ipv6 router ospf 1
 router-id 1.1.1.1
exit

interface gig1/0/11
 ipv6 ospf 1 area 0
exit

interface vlan 10
 ipv6 ospf 1 area 0
exit

interface vlan 20
 ipv6 ospf 1 area 0
exit

interface vlan 30
 ipv6 ospf 1 area 0
```

```
exit

interface vlan 40
 ipv6 ospf 1 area 0
exit

interface vlan 50
 ipv6 ospf 1 area 0
exit

interface vlan 60
 ipv6 ospf 1 area 0
exit

interface vlan 70
 ipv6 ospf 1 area 0
exit

interface vlan 100
 ipv6 ospf 1 area 0
exit

end
wr
```

- In `Dist-SW2`:

```
conf t

// Convert the port connected to HQ-R2 to a Routed Port
interface gig1/0/11
 no switchport
 ip address 10.0.0.6 255.255.255.252
 ipv6 address 2001:db8:acad:1002::2/64
 no shutdown
exit

// Enable OSPFv2 (IPv4)
router ospf 1
 router-id 2.2.2.2
 passive-interface default
```

```
 no passive-interface gig1/0/11
 // no passive-interface port-channel 1
 network 10.0.0.4 0.0.0.3 area 0
 network 192.168.0.0 0.0.255.255 area 0
exit

// Enable OSPFv3 (IPv6)
ipv6 router ospf 1
 router-id 2.2.2.2
exit

interface gig1/0/11
 ipv6 ospf 1 area 0
exit

interface vlan 10
 ipv6 ospf 1 area 0
exit

interface vlan 20
 ipv6 ospf 1 area 0
exit

interface vlan 30
 ipv6 ospf 1 area 0
exit

interface vlan 40
 ipv6 ospf 1 area 0
exit

interface vlan 50
 ipv6 ospf 1 area 0
exit

interface vlan 60
 ipv6 ospf 1 area 0
exit

interface vlan 70
 ipv6 ospf 1 area 0
exit
```

```
interface vlan 100
 ipv6 ospf 1 area 0
exit

end
wr
```

HQ-R1 – Primary Edge Router

Provides the primary WAN and ISP connectivity, advertises the default route through OSPF, and connects the HQ core with the branch and external network

- In Basis `HQ-R1` :

```
conf t
ipv6 unicast-routing

// Port directed to the ISP (Public Link)
interface gig0/0
 ip address 203.0.113.2 255.255.255.252
 ipv6 address 2001:db8:feed:1::2/64
 no shutdown
exit

// Port pointing to Branch-R1 (WAN Link)
interface gig0/1
 ip address 10.0.0.9 255.255.255.252
 ipv6 address 2001:db8:acad:1003::1/64
 no shutdown
exit

// Port pointing to Dist-SW1 (Internal Core Link)
interface gig0/2
 ip address 10.0.0.1 255.255.255.252
 ipv6 address 2001:db8:acad:1001::1/64
 no shutdown
exit

// Default Static Routes towards the ISP
```

```
ip route 0.0.0.0 0.0.0.0 203.0.113.1
ipv6 route ::/0 2001:db8:feed:1::1

// OSPFv2 with Default Route passed
router ospf 1
 router-id 11.11.11.11
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.0.8 0.0.0.3 area 0
 default-information originate
exit

// OSPFv3 with Default Route passed
ipv6 router ospf 1
 router-id 11.11.11.11
 default-information originate
exit

interface gig0/1
 ipv6 ospf 1 area 0
exit
interface gig0/2
 ipv6 ospf 1 area 0
exit
end
wr
```

HQ-R2 – Secondary Edge Router

Provides redundant WAN and ISP connectivity using a backup default route and OSPF to maintain routing availability during primary-link failure

- Backup Router Settings `HQ-R2` :

```
conf t
ipv6 unicast-routing

// Port directed to the ISP (Public Link)
interface gig0/0
 ip address 203.0.113.6 255.255.255.252
 ipv6 address 2001:db8:feed:2::2/64
 no shutdown
```

```
exit

// Port pointing towards Dist-SW2 (Internal Core Link)
interface gig0/1
 ip address 10.0.0.5 255.255.255.252
 ipv6 address 2001:db8:acad:1002::1/64
 no shutdown
exit

// Default Static Route towards the ISP with higher Metric (Floating
Backup)
ip route 0.0.0.0 0.0.0.0 203.0.113.5 10
ipv6 route ::/0 2001:db8:feed:2::1 10

// OSPFv2
router ospf 1
 router-id 22.22.22.22
 network 10.0.0.4 0.0.0.3 area 0
// default-information originate metric 20
 default-information originate
exit

// OSPFv3
ipv6 router ospf 1
 router-id 22.22.22.22
// default-information originate metric 20
 default-information originate
exit

interface gig0/1
 ipv6 ospf 1 area 0
exit
end
wr
```

Branch-R1 – WAN & OSPF Configuration

Establishes the WAN connection with HQ and advertises the branch VLAN networks through OSPF for end-to-end dynamic routing.

- In `Branch-R1` :

```
conf t

// Port connected to HQ via WAN
interface gig0/1
 ip address 10.0.0.10 255.255.255.252
 ipv6 address 2001:db8:acad:1003::2/64
 no shutdown
exit

// Enable OSPFv2
router ospf 1
 router-id 33.33.33.33
 passive-interface default
 no passive-interface gig0/1
 network 10.0.0.8 0.0.0.3 area 0
 network 192.168.110.0 0.0.0.255 area 0
 network 192.168.120.0 0.0.0.255 area 0
 network 192.168.170.0 0.0.0.255 area 0
exit

// Enable OSPFv3
ipv6 router ospf 1
 router-id 33.33.33.33
exit

interface gig0/1
 ipv6 ospf 1 area 0
exit
interface gig0/2.10
 ipv6 ospf 1 area 0
exit
interface gig0/2.20
 ipv6 ospf 1 area 0
exit
interface gig0/2.70
 ipv6 ospf 1 area 0
exit
end
wr
```

ISP-R1 – Internet Simulation

Simulates the ISP network and external Internet connectivity using public addressing and a loopback interface representing an external service.

In `ISP-R1` Simulates :

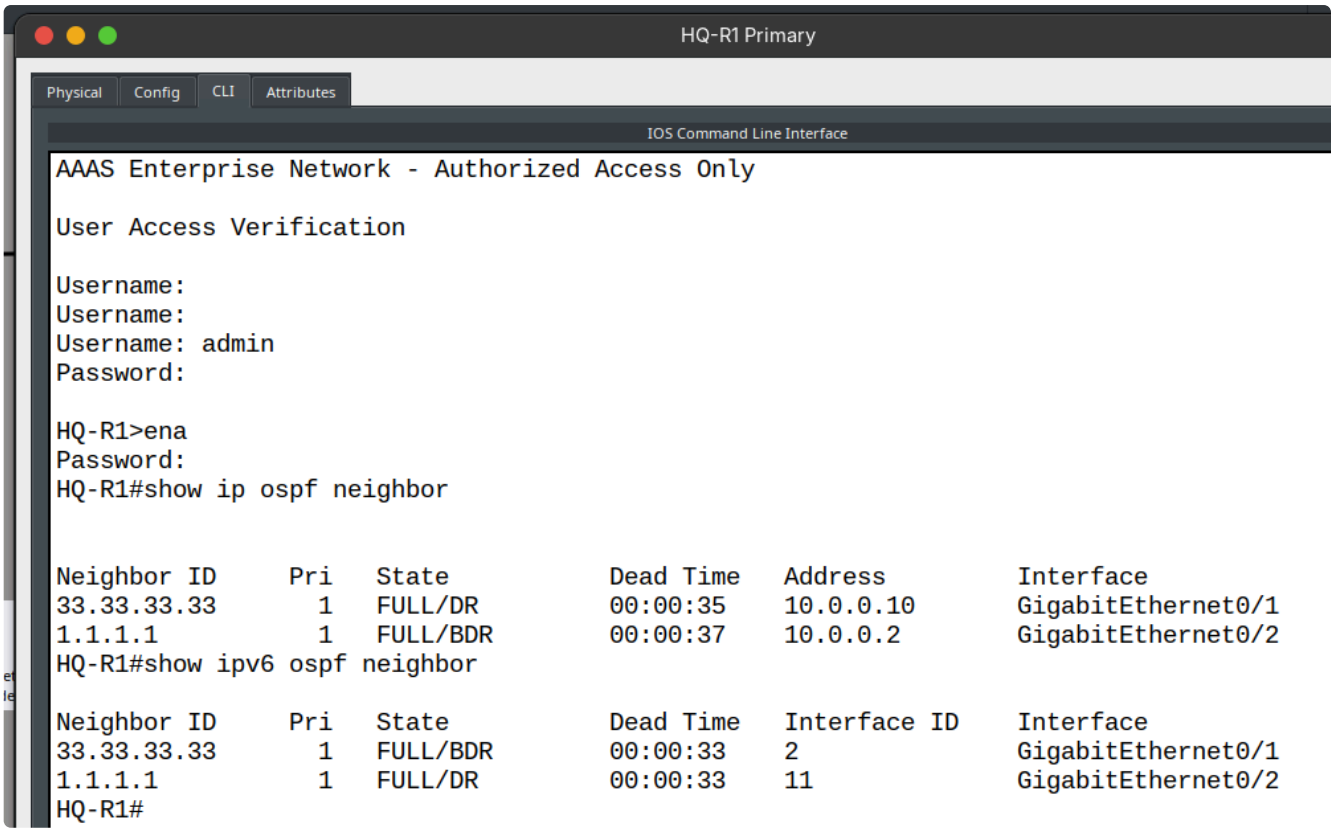
```
conf t
ipv6 unicast-routing

// Port connected to HQ-R1
interface gig0/0/0
 ip address 203.0.113.1 255.255.255.252
 ipv6 address 2001:db8:feed:1::1/64
 no shutdown
exit

// Port connected to HQ-R2
interface gig0/0/1
 ip address 203.0.113.5 255.255.255.252
 ipv6 address 2001:db8:feed:2::1/64
 no shutdown
exit

// Simulated external web server (Simulated Internet / DNS 8.8.8.8)
interface loopback 0
 ip address 8.8.8.8 255.255.255.255
 ipv6 address 2001:4860:4860::8888/128
 no shutdown
exit

// Directing Public Blocks to HQ Routers
ip route 203.0.113.0 255.255.255.0 203.0.113.2
end
wr
```

OSPF & Connectivity Verification :

Verifies OSPF neighbor relationships, learned routes, default-route propagation, and DHCP connectivity between the branch and HQ.

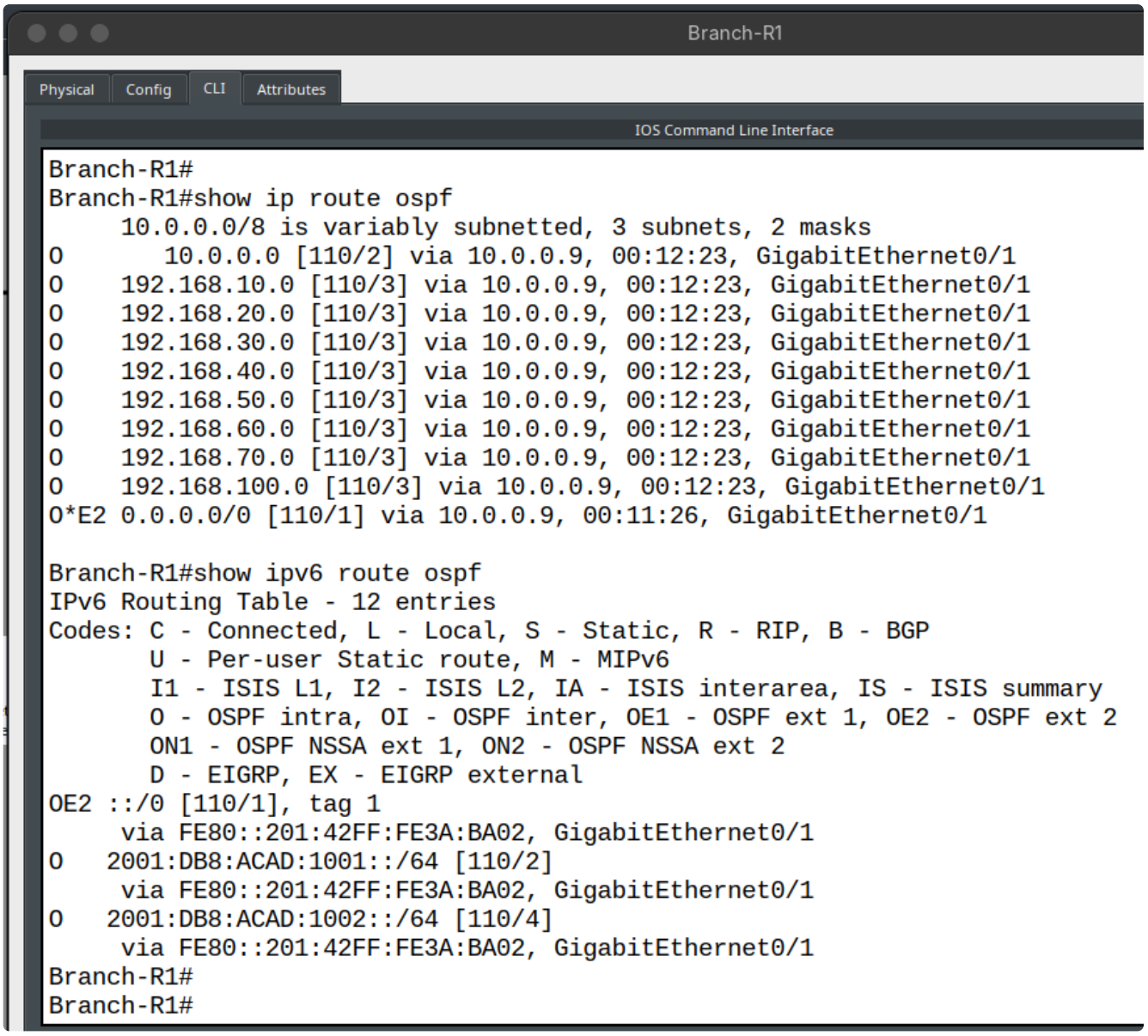
- OSPF Neighbors State In **HQ-R1** :

```
show ip ospf neighbor
show ipv6 ospf neighbor
```



- Routing Table & Default Route in **Branch-R1**:

```
show ip route ospf
show ipv6 route ospf
```

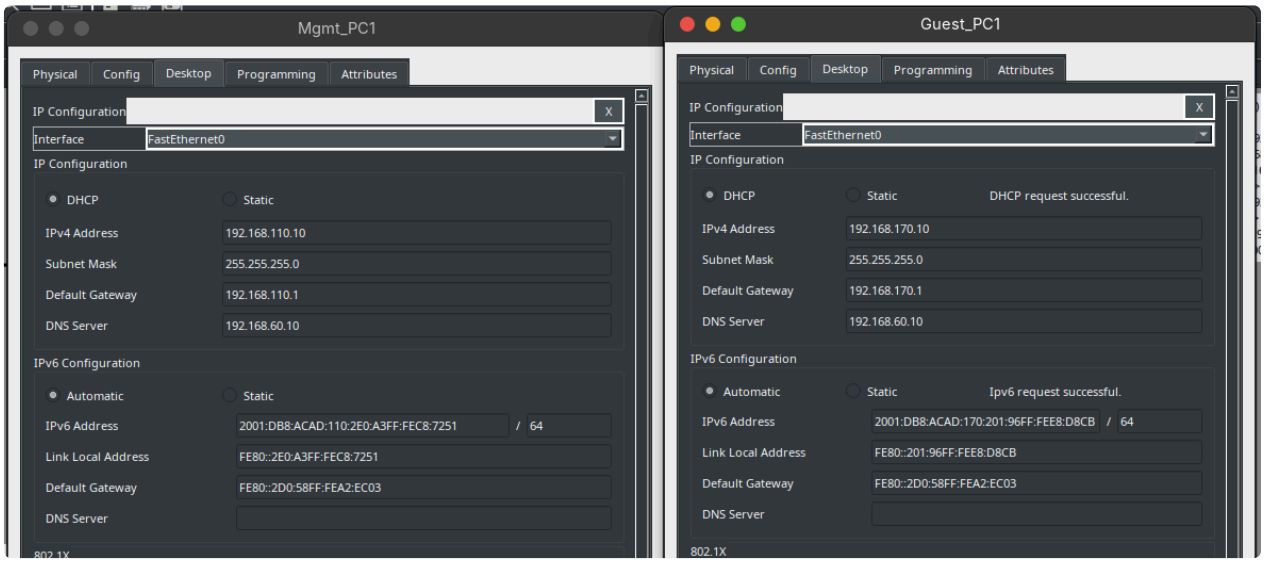


- In **Dist-SW1** :

```
show ip route ospf
```

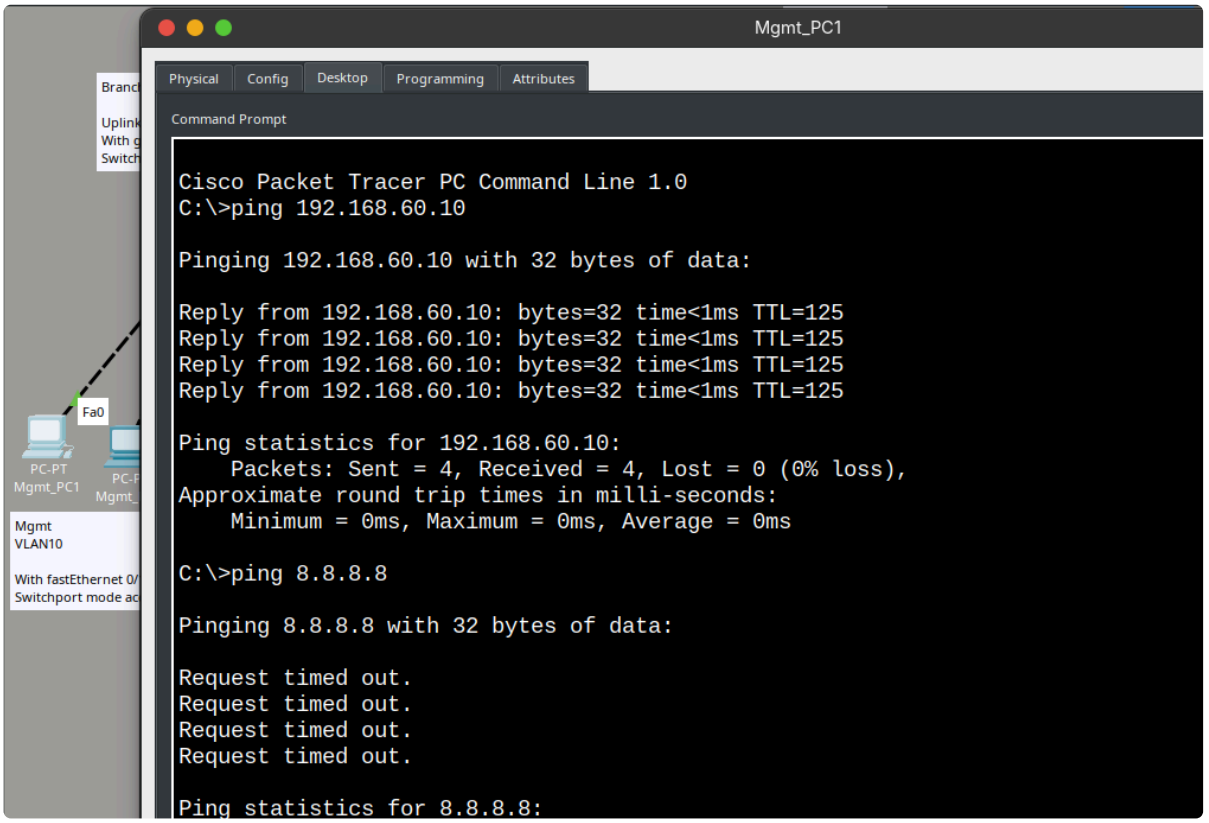
```
Dist-SW1#
Dist-SW1#
Dist-SW1#show ip route ospf
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O       10.0.0.8 [110/2] via 10.0.0.1, 00:13:05, GigabitEthernet1/0/11
O    192.168.110.0 [110/3] via 10.0.0.1, 00:12:55, GigabitEthernet1/0/11
O    192.168.120.0 [110/3] via 10.0.0.1, 00:12:55, GigabitEthernet1/0/11
O    192.168.170.0 [110/3] via 10.0.0.1, 00:12:55, GigabitEthernet1/0/11
O*E2 0.0.0.0/0 [110/1] via 10.0.0.1, 00:12:08, GigabitEthernet1/0/11

Dist-SW1#
Dist-SW1#
```

- Retracting the IP in the branch via the WAN (DHCP Relay Over WAN):



- End-to-End Dual-Stack Ping :

```
ping 192.168.60.10
ping 8.8.8.8
```



> connection to `8.8.8.8` will work after the NAT step in the next stage

---

Step 7 – Edge NAT/PAT & Internet Simulation :

PAT (NAT Overload)

- `HQ-R1` (Port Address Translation - Overload) :

```
conf t

// Defining the internal and external interfaces of the NAT
interface gig0/0
 ip nat outside
exit

interface gig0/1
 ip nat inside
exit

interface gig0/2
 ip nat inside
exit

// Create an Access Control List (ACL) to specify the networks allowed for translation
// Includes HQ networks (192.168.0.0/16), branch networks, and link networks (10.0.0.0/8)
ip access-list standard NAT_ALLOWED
 permit 192.168.0.0 0.0.255.255
 permit 10.0.0.0 0.255.255.255
exit

// Enable PAT by translating ACL to the external port IP address Gig0/0
ip nat inside source list NAT_ALLOWED interface gig0/0 overload

end
wr
```

- Add NAT in `HQ-R2` (Redundancy) :

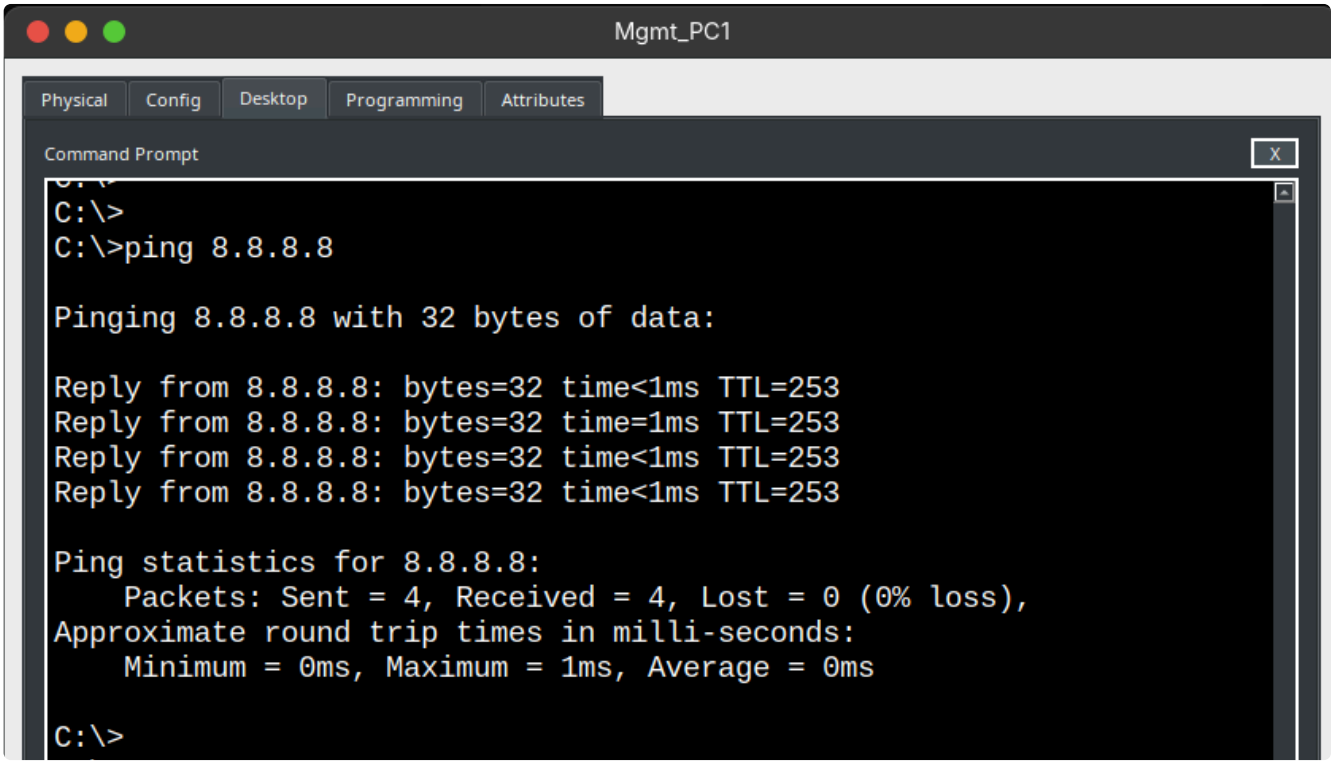
```
conf t

interface gig0/0
 ip nat outside
```

```
exit

interface gig0/1
 ip nat inside
exit

ip access-list standard NAT_ALLOWED
 permit 192.168.0.0 0.0.255.255
 permit 10.0.0.0 0.255.255.255
exit

ip nat inside source list NAT_ALLOWED interface gig0/0 overload

end
wr
```

NAT/PAT Verification :

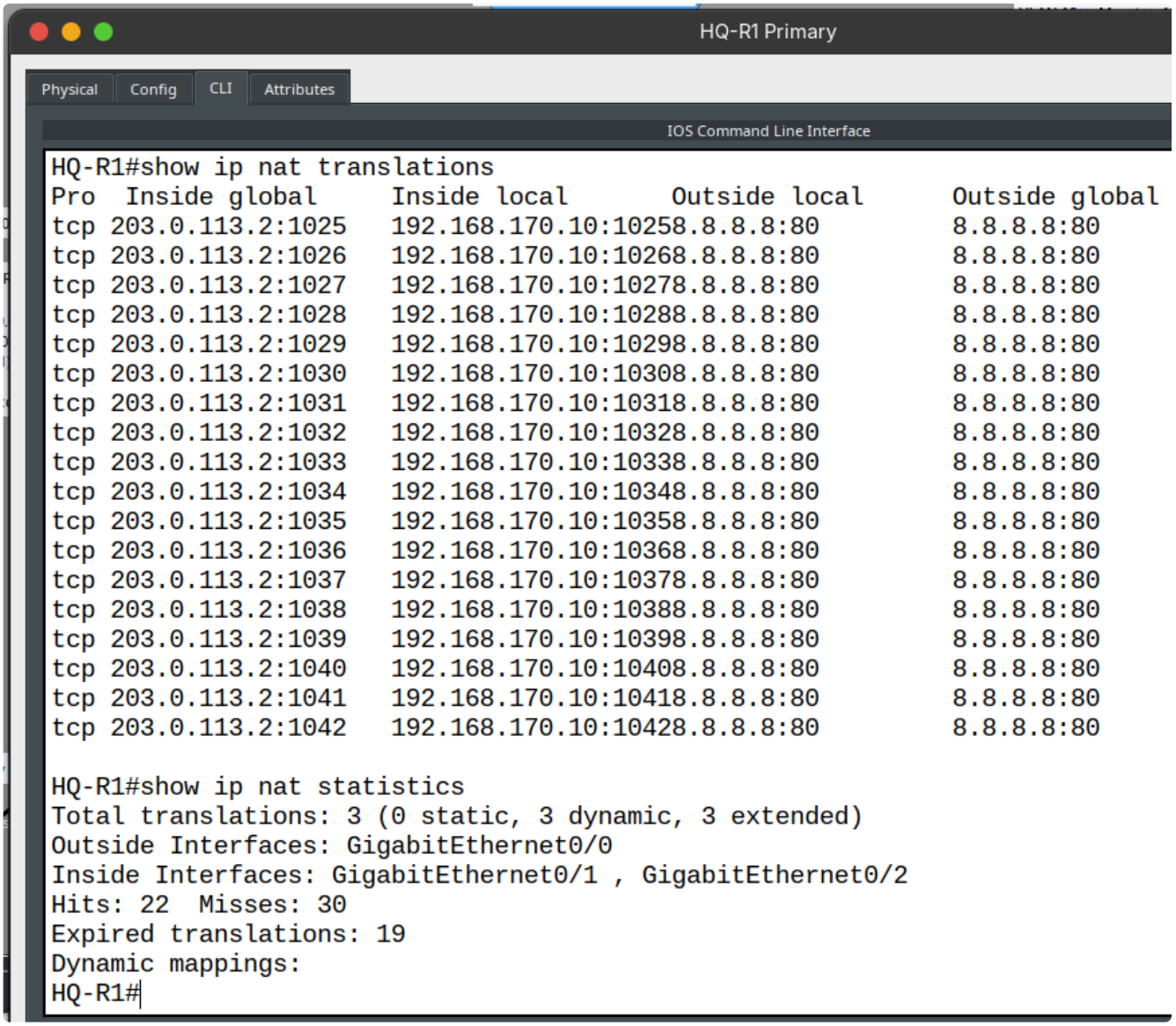
- Test connect internet (in Pc Devices) :

```
C:\>ping 8.8.8.8
```



- NAT Translations Table (in `HQ-R1`):
  - watch Translations session during make `ping` :

```
show ip nat translations
show ip nat statistics
```



Step 8 – Security Hardening & ACLs :

Extended ACLs applied to Distribution switches :

Required security rules:

- **Guest Isolation (VLAN 70):** Allow access only to DHCP, DNS, and external internet services, and block access to all internal company networks (192.168.0.0/16 and 10.0.0.0/8).
- **Finance Network Protection (VLAN 40):** Allow access only to the Management (VLAN 10) and IT (VLAN 20) departments, blocking access

to all other departments.

- **Server Farm Security (VLAN 60):** Allow all employees access to web services (HTTP/HTTPS), DNS, email, and FTP, and restrict server management (SSH/ICMP) to the IT and Management departments only.
- In `Dist-SW1` and `Dist-SW2` :

```
conf t

// 1. ACL for Guest Isolation (VLAN 70)
ip access-list extended GUEST_RESTRICTION

// Allow DHCP and DNS
 permit udp 192.168.70.0 0.0.0.255 host 192.168.60.10 eq domain
 permit tcp 192.168.70.0 0.0.0.255 host 192.168.60.10 eq domain
 permit udp any eq bootpc any eq bootps

// Block access to any internal company network
 deny ip 192.168.70.0 0.0.0.255 192.168.0.0 0.0.255.255
 deny ip 192.168.70.0 0.0.0.255 10.0.0.0 0.255.255.255

// Allow access to external internet
 permit ip 192.168.70.0 0.0.0.255 any
exit


// 2. ACL for protecting the Finance network (VLAN 40)
ip access-list extended FINANCE_PROTECTION

// Allow administration and IT access
 permit ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
 permit ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255

// Allow return traffic (Established Traffic)
 permit tcp any 192.168.40.0 0.0.0.255 established

// Prevent other departments from accessing the finance department
 deny ip any 192.168.40.0 0.0.0.255

// Allowing the rest of the normal traffic flow
 permit ip any any
exit
```

```
// 3. Applying ACLs to SVIs interfaces
interface vlan 70
 ip access-group GUEST_RESTRICTION in
exit

interface vlan 40
 ip access-group FINANCE_PROTECTION out
exit

end
wr
```

Setting up the ACL on `Branch-R1`

Required security :

- Allow DHCP and DNS (from the HQ server).
- Allow internet access only.
- Block access to local branch networks (192.168.110.0/24, 192.168.120.0/24).
- Block access to all internal HQ networks (192.168.0.0/16, 10.0.0.0/8).
- In `Branch-R1` :

```
conf t

// Create the ACL dedicated to isolating the guest in the branch
ip access-list extended BRANCH_GUEST_ACL

// 1. Allow DHCP requests from the server
 permit udp any eq bootpc any eq bootps

// 2. Allow DNS from the main server
 permit udp 192.168.170.0 0.0.0.255 host 192.168.60.10 eq domain
 permit tcp 192.168.170.0 0.0.0.255 host 192.168.60.10 eq domain

// 3. Block access to any internal network at the branch or HQ
 deny ip 192.168.170.0 0.0.0.255 192.168.0.0 0.0.255.255
 deny ip 192.168.170.0 0.0.0.255 10.0.0.0 0.255.255.255
```

```
// 4. Allow internet access
 permit ip 192.168.170.0 0.0.0.255 any
exit

// Applying the ACL to the Guest's Sub-interface
interface gig0/2.70
 ip access-group BRANCH_GUEST_ACL in
exit

end
wr
```

Enable Port Security on Access Switches

- In `Access-SW1` (Mgmt & IT):

```
conf t
interface range fa0/1 - 2 , fa0/10 - 11
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
exit
end
wr
```

- In `Access-SW2` (HR & Finance):

```
conf t
interface range fa0/1 - 2 , fa0/10 - 11
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
exit
end
wr
```

- In `Access-SW3` (Guest & Sales):

```
conf t
interface range fa0/1-2,fa0/10-11
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
exit
end
wr
```

- In `Branch-SW`:

```
conf t
interface range fa0/1-2,fa0/10-11,fa0/20
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
exit
end
wr
```

Close all unused ports (Unused Ports Shutdown)

To reduce the attack surface and prevent random delivery

- In `Access-SW1`:

```
conf t
interface range fa0/3-9,fa0/12-24
 shutdown
exit
end
wr
```

- In `Access-SW2`:

```
conf t
interface range fa0/3-9,fa0/12-24
 shutdown
```

```
exit
end
wr
```

- In `Access-SW3` :

```
conf t
interface range fa0/3 - 9 , fa0/12 - 24
 shutdown
exit
end
wr
```

- In `Access-SW4` (Server Switch) :

```
conf t
interface range fa0/3 - 24
 shutdown
exit
end
wr
```

- In `Branch-SW` :

```
conf t
interface range fa0/3 - 9 , fa0/12 - 19 , fa0/21 - 24
 shutdown
exit
end
wr
```

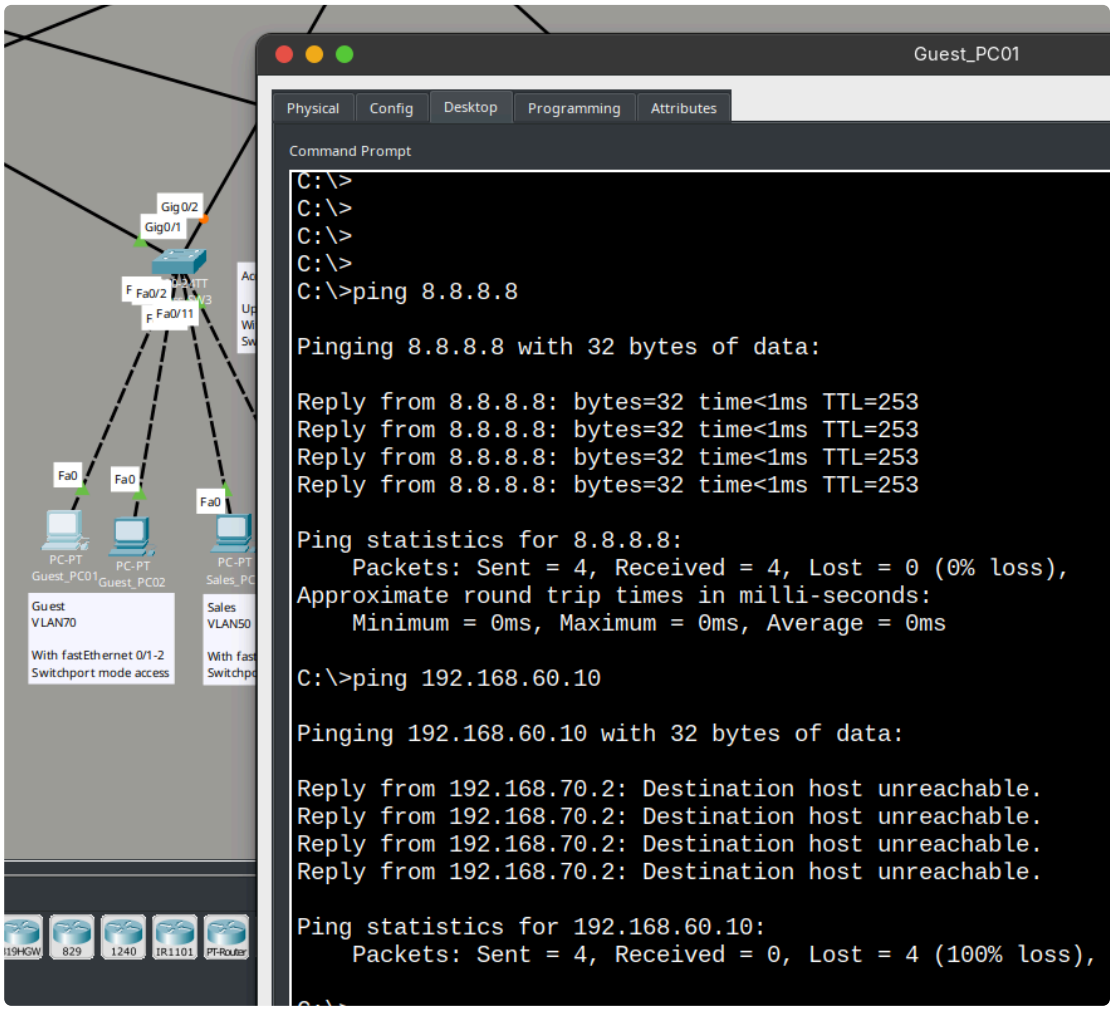
- In `Dist-SW1` and `Dist-SW2` :

```
conf t

interface range gigabitEthernet 1/0/5-10, gigabitEthernet 1/0/12-22,
gigabitEthernet 1/1/1-4

 shutdown
```

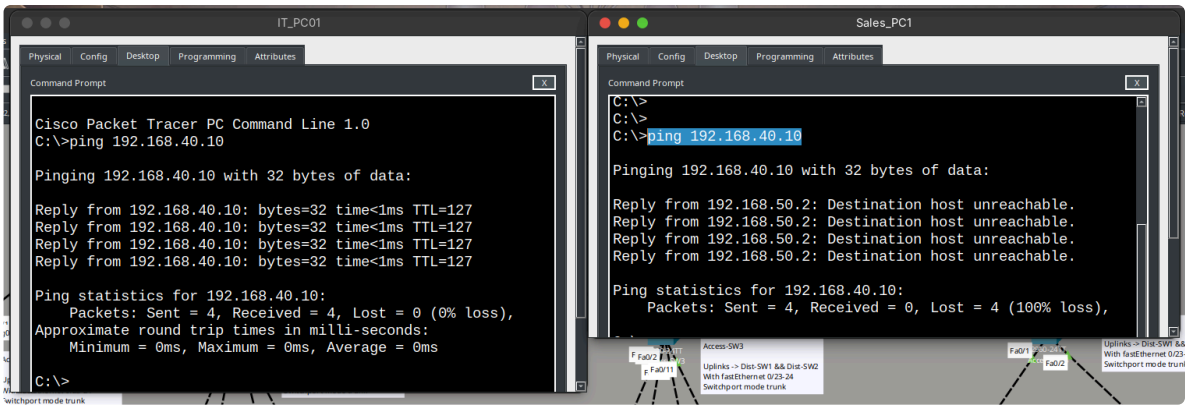
```
exit
end
wr
```

HQ Verification :

- **Guest Isolation Test:**
  - From machine `Guest_PC01`
    - execute `ping 192.168.60.10` (the ping will fail)
  - then execute `ping 8.8.8.8`
    - (the internet connection will succeed)



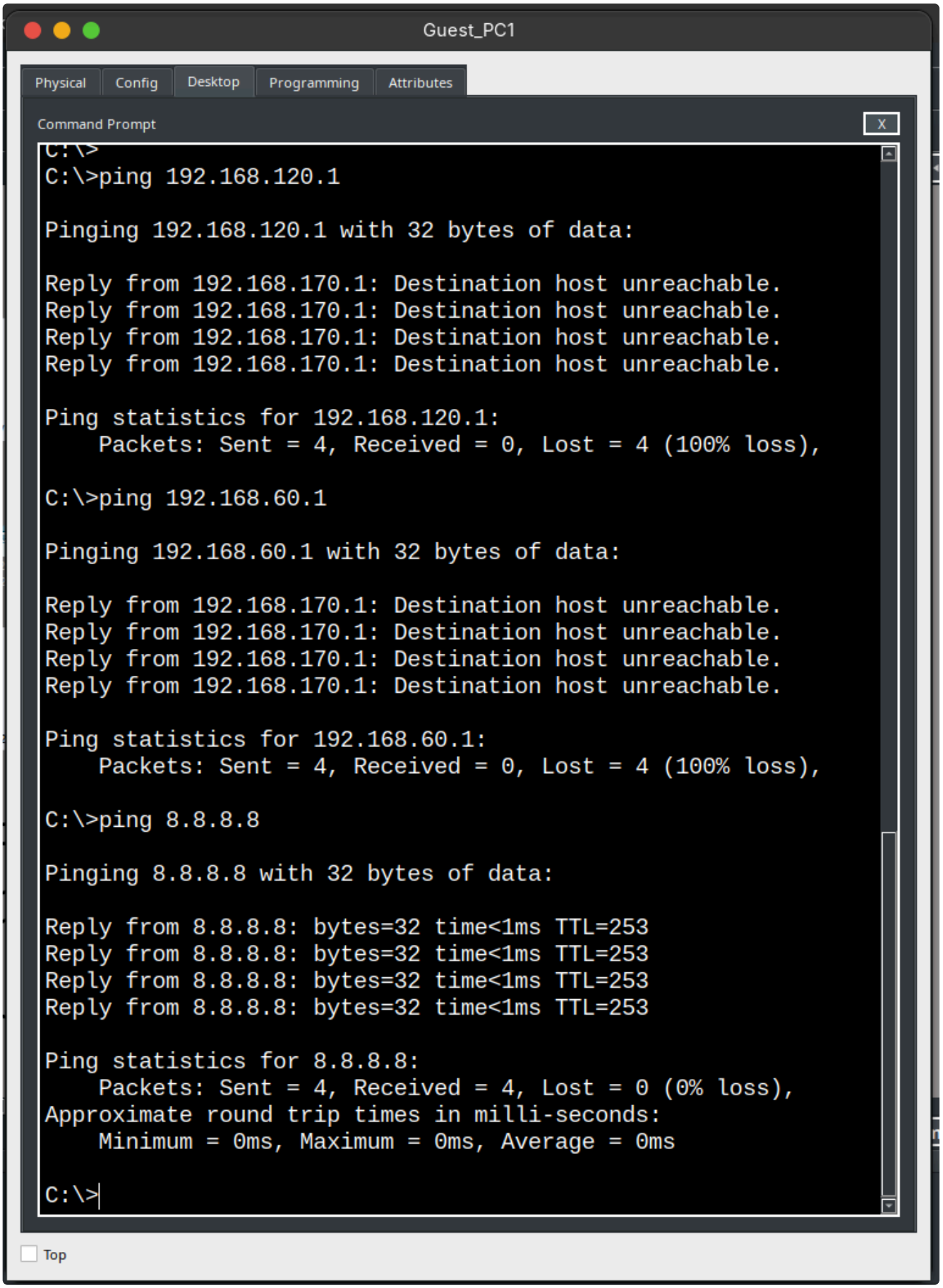
- **Financial Protection Test:**
  - From the `Sales_PC1` device, execute `ping 192.168.40.10` (will fail due to the ACL)
  - while from the `IT_PC01` device the connection to finance will succeed



- **Port Security Verification:** Execute the command `show port-security interface fa0/1` on any Access Switch to check the port status and the automatic MAC Address (`sticky`) is set.

Verifying the `Guest_PC1` device from Branch:

- **Ping to the branch printer (`192.168.120.1`):** Fails (Destination host unreachable).
- **Ping to the HQ server (`192.168.60.10`):** Fails.
- **Ping to the internet (`8.8.8.8`):** Succeeds.



- This project establishes a resilient, production-ready enterprise network architecture that balances continuous service availability with strict

access control

- By integrating Layer 2 redundancy, dynamic Dual-Stack OSPF routing, centralized services, and granular Extended ACLs, the design effectively eliminates single points of failure while securing critical enterprise assets against unauthorized internal and external access