**Project Manager**: Manzano, Nathaniel Ree M.

**Network Engineer**: Domantay, Rafael Joseph

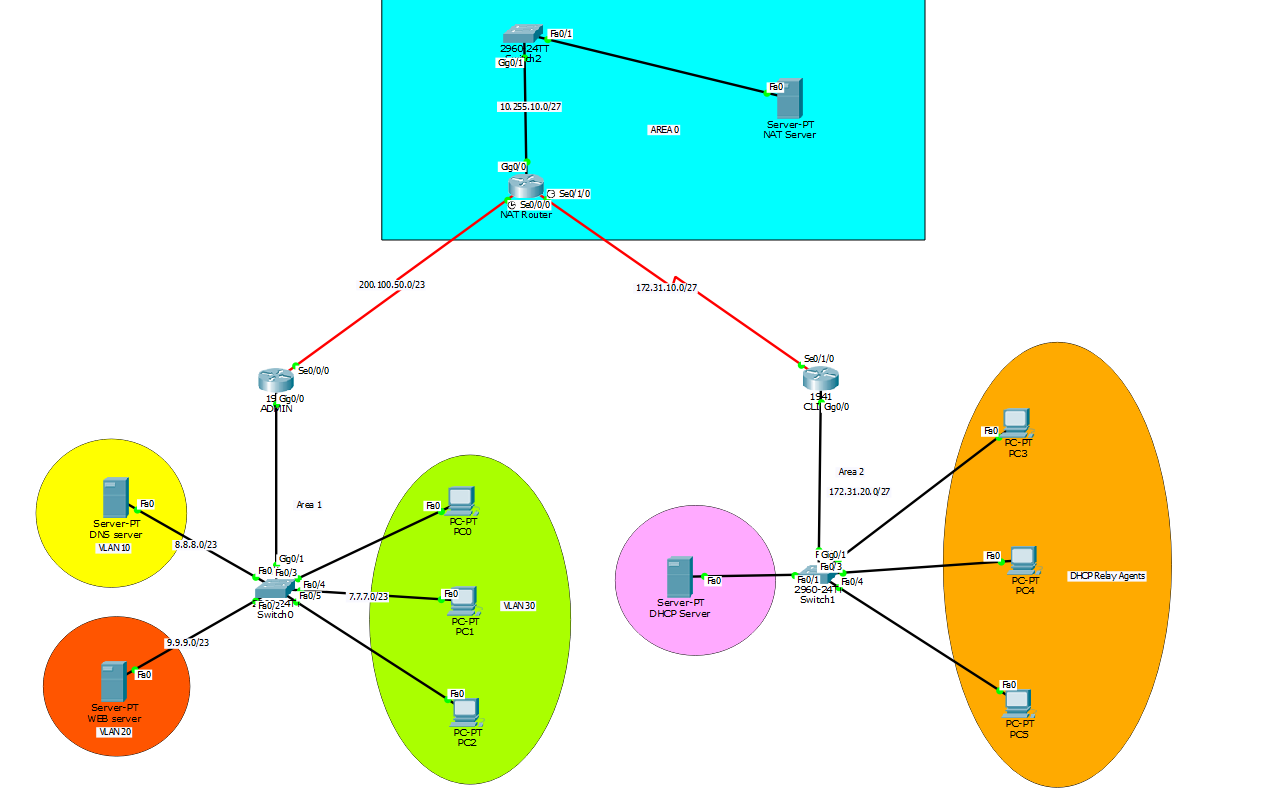
**Document Writer**: Coloma, Draven Troy

**Network design and topology diagrams**

This network setup uses a **star topology**, where all devices are connected to a central hub or router. It is segmented into different areas using both **public** and **private IP addressing**, as well as multiple **VLANs** to separate network traffic for servers and clients. The network is divided into multiple areas for routing with **OSPF (Open Shortest Path First)** as the chosen routing protocol. There are also **servers** dedicated to DNS, NAT, DHCP, and web services.

The network consists of the following key components:

* **NAT Router**: Interfaces with the internet and local networks.
* **ISP Router**: Connects the organization to the Internet Service Provider.
* **Client Router**: Manages traffic for local clients and services.
* **Servers**: Provides various services including DNS, web hosting, and DHCP.



**Configuration files for each network device**

**OSPF**

**NAT Router**:

Router>enable

Router#configure terminal

Router(config)#hostname NAT

NAT(config)#int se0/0/0

NAT(config-if)#clock rate 64000

NAT(config-if)#ip address 200.100.50.1 255.255.254.0

NAT(config-if)#no shutdown

NAT(config-if)#exit

NAT(config)#int se0/1/0

NAT(config-if)#clock rate 64000

NAT(config-if)#ip address 172.31.10.1 255.255.255.224

NAT(config-if)#no shut

NAT(config-if)#exit

NAT(config)#int gig0/0

NAT(config-if)#ip address 10.255.10.1 255.255.255.224

NAT(config-if)#no shutdown

NAT(config)#router ospf 1

NAT(config-router)#router-id 2.2.2.2

NAT(config-router)#network 10.255.10.0 0.0.0.31 area 0

NAT(config-router)#network 200.100.50.0 0.0.1.255 area 0

NAT(config-router)#network 172.31.10.0 0.0.0.31 area 0

NAT(config-router)#end

NAT(#)write memory

**ADMIN Router:**

ADMIN(config)#router ospf 1

ADMIN(config-router)#

ADMIN(config-router)#router-id 1.1.1.1

ADMIN(config-router)#network 7.7.7.0 0.0.1.255 area 1

ADMIN(config-router)#network 8.8.8.0 0.0.1.255 area 1

ADMIN(config-router)#network 9.9.9.0 0.0.1.255 area 1

ADMIN(config-router)#network 200.100.50.0 0.0.1.255 area 0

ADMIN(config-router)#end

ADMIN(#)write memory

**CLIENT Router:**

CLIENT (config)#router ospf 1

CLIENT (config-router)#router-id 3.3.3.3

CLIENT (config-router)#network 172.31.20.0 0.0.0.31 area 2

CLIENT (config-router)#network 172.31.10.0 0.0.0.31 area 0

CLIENT (config-router)#end

CLIENT (#)write memory.

The **NAT router** acts as an **ABR (Area Border Router)** because it connects **area 0** to other areas (1 and 2).

The **NAT router** connects both the **ADMIN** and **CLIENT** routers, serving as the gateway between different areas (0, 1, and 2)

**INTER-VLAN**

Assign IP address every Server

For DNS server:

IP ADDRESS: 8.8.8.8

SUBNETMASK: 255.255.254.0

DEFAULT GATEWAY: 8.8.8.1

DNS Server: 8.8.8.8

For WEB server:

IP ADDRESS: 9.9.9.9

SUBNETMASK: 255.255.254.0

DEFAULT GATEWAY: 9.9.9.1

DNS Server: 8.8.8.8

**Device: Switch 0**

Command in use:

**Switch**>enable

**Switch**# configure terminal

**Switch**(config)#vlan 10

**Switch**(config-vlan)#name DNS

**Switch**(config-vlan)#exit

**Switch**(config)#vlan 20

**Switch**(config-vlan)#name WEB

**Switch**(config-vlan)#exit

**Switch**(config)#vlan 30

**Switch**(config-vlan)#name PC’s

**Switch**(config-vlan)#exit

**Switch**(config)#int range fa0/1

**Switch**(config-if-range)#switchport mode access

**Switch**(config-if-range)#switchport access vlan 10

**Switch**(config-if-range)#exit

**Switch**(config)#int range fa0/2

**Switch**(config-if-range)#switchport mode access

**Switch**(config-if-range)#switchport access vlan 20

**Switch**(config-if-range)#exit

**Switch**(config)#int range fa0/3-5

**Switch**(config-if-range)#switchport mode access

**Switch**(config-if-range)#switchport access vlan 30

**Switch**(config-if-range)#exit

**Switch**(config)#int g0/1

**Switch**(config-if)#switchport mode trunk

**Switch**(config-if)#switch trunk allowed vlan 10,20,30

**Switch**(config-if)#end

**Switch**(#)write memory

VLAN 10: DNS server

VLAN 20: Web Server

VLAN 30: PC’s

This configuration segregates network traffic based on user roles, enhancing security and network management.

**Device: ADMIN Router**

Command in use:

**Router**>enable

**Router** #configure terminal

**Router** #hostname **ADMIN**

**ADMIN** (config)#int g0/0

**ADMIN** (config-if)#no shutdown

**ADMIN** (config-if)#exit

**ADMIN** (config)#int g0/0.10

**ADMIN** (config-subif)#encapsulation dot1Q 10

**ADMIN** (config-subif)#ip address 8.8.8.1 255.255.254.0

**ADMIN** (config-subif)#exit

**ADMIN** (config)#int g0/0.20

**ADMIN** (config-subif)#encapsulation dot1Q 20

**ADMIN** (config-subif)#ip address 9.9.9.1 255.255.254.0

**ADMIN** (config)#int g0/0.30

**ADMIN** (config-subif)#encapsulation dot1Q 30

**ADMIN** (config-subif)#ip address 7.7.7.1 255.255.254.0

**ADMIN** (config-if)#end

**ADMIN** (#)write memory

This configuration on the ISP router enables inter-VLAN routing by creating subinterfaces for VLAN 10 and VLAN 20, allowing devices in different VLANs to communicate through the router.

**DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP)**

**Configure IP address for DHCP server**

IP ADDRESS: 172.31.20.2

SUBNETMASK: 255.255.255.224

DEFAULT GATEWAY: 172.31.20.1

DNS Server: 8.8.8.8

Add Services for DHCP Pool

Switch on the DHCP pool

Pool Name: dhcpPool

Default Gateway: 172.31.20.1

DNS Server: 8.8.8.8

Start IP Address: 172.31.20.3

SubnetMask: 255.255.255.224

Host: 29

Click Add

Click Save

**Configure Client Router**

**Router**>enable

**Router** #configure terminal

**Router** #hostname Client\_Router

**Client\_Router** (config)#int g0/0

**Client\_Router** (config-if)#no shutdown

**Client\_Router**(config)#int gig0/0

**Client\_Router**(config-if)#ip address 172.31.20.1 255.255.255.224

**Client\_Router**(config-if)#ip helper-address 172.31.20.2

**Client \_Router** (config-if)#end

**Client \_Router** (#)write memory

Every PC connected to the gig0/0 interface with the network 172.31.20.0/27 will automatically switch to dynamic IP configuration and receive an IP address from the DHCP server.

**NAT Configuration**

**NAT ROUTER:**

NAT (config)# access-list 1 permit 172.31.20.0 0.0.0.31

NAT (config)# ip nat pool DYNAT 200.100.50.1 200.100.50.255 netmask 255.255.254.0

NAT(config)#ip nat inside source list 1 pool DYNAT overload

NAT(config)#int  se0/0/0

NAT(config)#ip nat outside

NAT(config)#exit

NAT(config)#int  se0/1/0

NAT(config)#ip nat inside

NAT(config)#exit

This configuration allows internal devices on the network 172.31.20.0/26 to communicate with external networks by translating their internal IP addresses to a pool of public IPs (200.100.50.1 - 200.100.50.255).

**Configuring SSH**

NAT (config)# hostname NAT

NAT (config)# ip domain-name cisco.com

NAT (config)# crypto key generate rsa

How many bits in the modulus [512]: 1024

NAT (config)# username admin secret cisco

NAT (config)# ip ssh version 2

NAT (config)# access-list 10 permit ip 10.255.10.1 0.0.0.31 any

NAT (config)# line vty 0 4

NAT (config-line)# login local

NAT (config-line)# transport input ssh

NAT (config-line)# access-class 100 in

NAT (config-line)# exit

This configuration ensures that only authorized users from specified networks can access the NAT Router via SSH.

**IP addressing scheme and subnetting details**

This document outlines the IP addressing scheme and routing setup for the network infrastructure, including NAT, ISP, and Client routers, as well as the DNS, Web, DHCP servers, and DHCP relay agents. Each device is configured with its respective IPv4 address, subnet mask, default gateway, wildcard mask, and OSPF area.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IPv4 Address** | **Subnet Mask** | **Default Gateway** | **Wildcard Mask** | **Area** |
| **NAT Router** | Gig0/0 | 10.255.10.1/27 | 225.255.255.224 | 10.255.10.1 | 0.0.0.31 | Area 0 |
| Se0/1/0 | 172.31.10.1/27 | 255.255.255.224 | 172.31.10.1 | 0.0.0.63 |
| Se0/0/0 | 200.100.50.1/23 | 255.255.254.0 | 200.100.50.1 | 0.0.1.255 |
| **ADMIN Router** | Se0/0/0 | 200.100.50.2/23 | 255.255.254.0 | 200.100.50.2 | 0.0.1.255 | Area 0 |
| Gig0/0 | VLAN | VLAN | VLAN | VLAN | Area 0 |
| **Client Router** | Se0/1/0 | 172.31.10.2/26 | 172.31.10.0/26 | 172.31.10.2 | 0.0.0.63 | Area 0 |
| Gig0/0 | 172.31.20.0/27 | 255.255.255.224 | 172.31.20.1 | NA | Area 2 |
| **DNS Server** | Fa0/0 | 8.8.8.0/23 | 255.255.254.0 | 8.8.8.1 | NA | Area 1 |
| **WEB server** | Fa0/0 | 9.9.9.0/23 | 255.255.254.0 | 9.9.9.1 | NA | Area 1 |
| **DHCP server** | Fa0/0 | 172.31.20.2/27 | 255.255.255.224 | 172.31.20.1 | NA | Area 2 |
| **DHCP relay agents** | Fa0/0 | 172.31.20.3 –  172.31.20.62 | 255.255.255.224 | 172.31.20.1 | NA | Area 2 |
| **NAT server** | Fa0/0 | 10.255.10.2/27 | 225.255.255.224 | 10.255.10.1 | NA | Area 0 |
| **VLAN 10**  **VLAN20**  **VLAN30** | Fa0/1 | 8.8.8.0/23 | 255.255.254.0 | 9.9.9.1 | NA | Area 1 |
| Fa0/2 | 9.9.9.0/23 | 255.255.254.0 | 8.8.8.1 | NA | Area 1 |
| Fa0/3 - 5 | 7.7.7.0/23 | 255.255.254.0 | 7.7.7.1 | NA | Area 1 |

**Troubleshooting steps and resolutions**

**1. OSPF (Open Shortest Path First)**

**Troubleshooting Steps:**

* **Check OSPF Configuration:**
  + Verify that OSPF is enabled on the correct interfaces.
  + Ensure that the OSPF area configuration is consistent across routers.
* **Verify OSPF Neighbors:**
  + Use the command show ip ospf neighbor to check neighbor status.
  + Ensure that the OSPF Hello and Dead intervals match between routers.
* **Check Network Statements:**
  + Confirm that the correct networks are included in OSPF using the command show running-config.

**Resolutions:**

* Update OSPF configuration if discrepancies are found.
* Restart OSPF process with clear ip ospf process if necessary.

**2. DNS (Domain Name System)**

**Troubleshooting Steps:**

* **Check DNS Configuration:**
  + Verify the DNS server IP addresses in the network settings.
  + Use lookup or dig to test DNS resolution.
* **Review DNS Server Logs:**
  + Check logs for errors or misconfigurations.
* **Test Connectivity:**
  + Ensure that the DNS server is reachable via ping.

**Resolutions:**

* Update DNS server IPs if they are incorrect.
* Consider caching issues or update DNS entries as necessary.

**3. DHCP (Dynamic Host Configuration Protocol)**

**Troubleshooting Steps:**

* **Check DHCP Server Status:**
  + Ensure the DHCP service is running.
  + Use show ip dhcp binding to check assigned IPs.
* **Examine Network Configuration:**
  + Verify that DHCP scopes are correctly configured and not exhausted.
* **Review Client Configuration:**
  + Use ipconfig /release and ipconfig /renew on Windows to refresh DHCP lease.

**Resolutions:**

* Expand the DHCP scope or remove unused bindings.
* Ensure that the DHCP relay agent is configured if needed.

**4. SSH (Secure Shell)**

**Troubleshooting Steps:**

* **Check SSH Configuration:**
  + Verify the SSH version and authentication settings in the router/switch.
* **Examine Access Control Lists (ACLs):**
  + Ensure that the ACLs permit SSH traffic.
* **Test Connectivity:**
  + Confirm that the device is reachable via ping.

**Resolutions:**

* Update SSH configuration as necessary.
* Reset passwords or authentication methods if needed.

**5. ACL (Access Control Lists)**

**Troubleshooting Steps:**

* **Review ACL Configuration:**
  + Use show access-lists to review rules and their order.
* **Test Connectivity:**
  + Use ping and traceroute to identify where packets are being dropped.
* **Check Interface Assignments:**
  + Verify that ACLs are applied to the correct interfaces.

**Resolutions:**

* Modify or reorder ACL entries based on troubleshooting results.

**6. VLAN (Virtual Local Area Network)**

**Troubleshooting Steps:**

* **Check VLAN Configuration:**
  + Use show vlan brief to ensure VLANs are created and active.
* **Verify Trunking:**
  + Ensure that trunk ports are configured properly on switches.
* **Examine Port Assignments:**
  + Confirm that switch ports are assigned to the correct VLAN.

**Resolutions:**

* Update VLAN assignments or configurations as needed.
* Ensure correct trunk configurations to allow VLAN traffic.