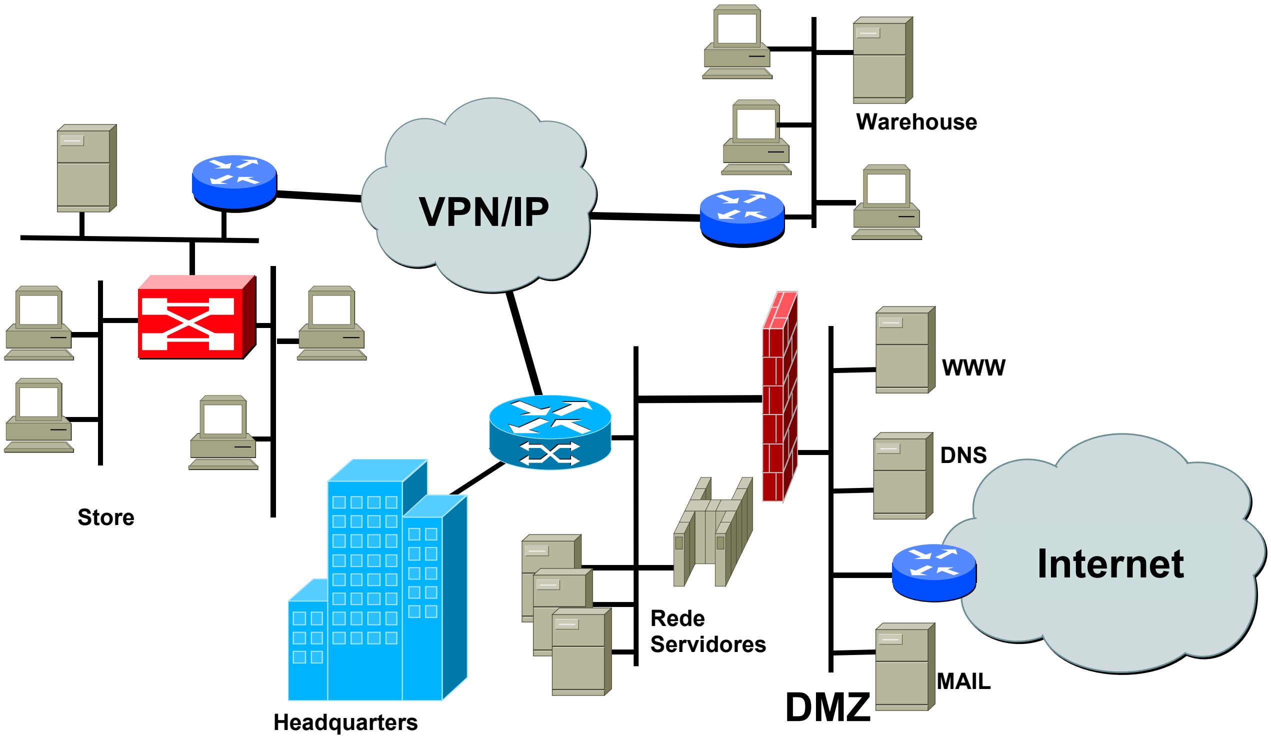
IP addressing and DNS Service

The purpose of this assignment it to help students understand the requirements of the IP addressing scheme of a company with several networks of different sizes and technologies. Then should be designed and configured the DNS service to allow resolution of names separate from the internal network (Intranet) and external (Internet), avoiding the exposure of internal network addresses.

Part 1

Design the IP addressing scheme necessary for the interconnection of QQUMA Ltd networks and enterprise systems.



The main features of the infrastructure network of the company are:

- All network services are supported in the TCP / IP protocol suite.
- The company's facilities are connected by a VPN / IP over MPLS.
- In the headquarters building there is an Ethernet, identified as "*Rede Servidores*", which links to the firewall for external access and to the router/switch to access the building's network over structured cabling (300 information outlets). The servers on this network provide essential services to the corporate network, such as the DNS server for the Intranet [ns.qquma.pt], the E-mail server [mail.qquma.pt] and the Web server [www. qquma.pt].

- There are three stores with the setting as the standard store shown. In each store there is an access router to which an Ethernet switch 10/100 Mb/s is connected, which provides two VLANs for customers with a maximum of 24 and 16 stations connected, respectively. For local network services, such as management of the DNS domain for the store and the HTTP proxy, there is a server that is seen in both VLANs and should be recognized by the names [ns.lojaX.qquma.pt] and [proxy. lojaX.qquma.pt].
- There is a warehouse with an access router and an Ethernet LAN, with a single collision domain, to which 17 stations are connected and a local server [armazem.qquma.pt], which has configured a DNS service cache server. This server forwards all DNS requests to the main server located in the headquarters.
- For direct communications with the outside, between the firewall and the router directly connected to the Internet, is a demilitarized zone of the network, the DMZ. On this network are installed only servers visible from the outside: DNS, E-mail and Web, being recognized by the names [ns.qquma.pt], [mail.qquma.pt] and [www.qquma.pt], respectively.

To solve the addressing problem, the following block of IP addresses was assigned:

192.168/21 for the Intranet and **20.49.51.160/28** for the DMZ.

1. Design the addressing scheme of the corporate network, using from the address block above only the addresses with the size needed for each network. Justify.

2. Present the multiple addresses (the network ID and broadcast) and their masks for each network.

3. Assign addresses to the servers and gateways listed in each local network. Best practices recommend that the servers have the lowest address of the network, for example, the lower is the DNS server, and the highest (pre-broadcast) is for the router.

4. Assuming the assignment of addresses that you made previously, set a bench on your network topology representing a network for the headquarters servers, the store and warehouse networks.

Part 2

Configure the DNS service for the company QQUMA Ltd, with the domain **qquma.pt**.

1. Identify in Unix systems that are available on the workbench, the location of the software required for the installation and configuration of the daemon "named".
2. If not available, create the directory `/var/named` and then put all the configuration files and data for the proper operation of "named".
3. Set up a solution of "split DNS" with a primary server for the domain qquma.pt in the Intranet and the other is what will be available for Internet information services/servers in DMZ (configure the DNS server to forward Intranet to the external DNS server with Internet connectivity, or alternatively set up a BIND server with "views").
4. Setup a DNS server to the sub-domain of a store and put the DNS server of the company's domain server as secondary (slave) of this.
5. In the warehouse network server configure a DNS cache server.
6. Intranet DNS servers make forward for the company's server in the headquarters building.
7. None of the IP networks of Intranet should have connectivity to Internet, will only have the DMZ network. Therefore, to implement this scenario in each workbench must be made NAT of the network 20.49.51.160/28 to the lab network. The network 192.168/21 should have no external connectivity.
8. Activate the generation of logs for the BIND(s) server(s) and test the settings. Present the extract from the logging of the proper functioning of the settings made.

Example configuration NAT:

```
router#conf terminal
router(config)#int fa0/0
router(config-if)#description outside access interface
router(config-if)#ip nat outside
router(config-if)#int fa0/1.10
router(config-if)#description inside access interface
router(config-subif)#ip nat inside
router(config-if)#int fa0/1.20
router(config-if)#description inside access interface
router(config-subif)#ip nat inside
router(config-if)#int fa0/1.30
router(config-if)#description inside access interface
router(config-subif)#ip nat inside
router(config-subif)#exit

router# conf terminal
! Include the VLAN10 IP network
router(config)#access-list 1 permit 172.16.1.0 0.0.0.255
! Include the VLAN20 IP network
router(config)#access-list 1 permit 172.16.2.64 0.0.0.31
! Include the VLAN30 IP network
router(config)#access-list 1 permit 172.16.2.192 0.0.0.15
router(config)#ip nat inside source list 1 interface fa0/0 overload
```

Reference Materials:

- Comer, Douglas E., *Internetworking with TCP/IP, Vol I*
- http://www.isc.org
- Online Linux man pages (local or http://www.linuxdoc.org)
- RFCs.