Network Planning and Management (PGRE)
Master in Electrical and Computers Engineering
Faculty of Engineering of University of Porto

IP Adressing and DNS Service

AFONSO QUEIRÓS UP201808903
HUGO GUIA UP201305075
JOÃO LOUREIRO UP201604453

28-03-2020

Contents

1. Introduction

In this lab work we try to understand the requirements of the IP addressing scheme of a company with several networks of different sizes and technologies. Among the challenges that come with this assignment, the DNS service plays an important role in order to resolve the domain names from the internal network (Intranet) and external (Internet), in order to avoid exposure of internal network addresses. For this purpose we used bind9 to configure the DNS service.

2. Company Addressing Schema

In the headquarters building there is an Ethernet, identified as Server's Network, 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].

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.

2.1 Addressing Values

Using the initial address, 192.168.0.0/21, for the Intranet, the addressing of the entities available on the network is built, more specifically for the DMZ, which in this case already obtains the assigned address, 20.49.51.160/28, for the Stores, Warehouse and HeadQuarters. The last one will have two different addresses, one of which refers to the network of servers included in this location. The figure below shows how the initial address was distributed, in order to address all the entities that make up the network.

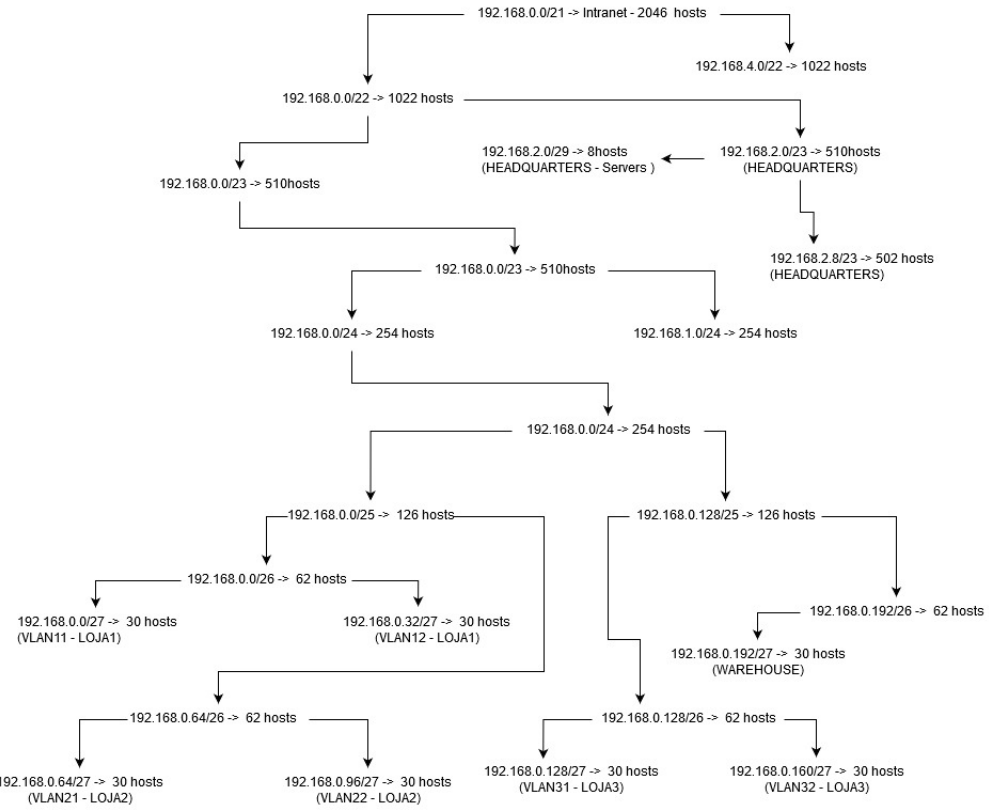

Figure 2.1: Address breakdown

For clear presentation, the following table includes the addresses assigned to network entities.

	Network	Broadcast	DNS	Gateway
Loja1.1	192.168.0.0/27	192.168.0.31	192.168.0.1	192.168.0.30
Loja1.2	192.168.0.32/27	192.168.0.63	192.168.0.33	192.168.0.62
Loja2.1	192.168.0.64/27	192.168.0.95	192.168.0.65	192.168.0.94
Loja2.2	192.168.0.96/27	192.168.0.127	192.168.0.97	192.168.0.126
Loja3.1	192.128.0.128/27	192.168.0.159	192.168.0.129	192.168.0.158
Loja3.2	192.128.0.160/27	192.168.0.191	192.168.0.161	192.168.0.190
Warehouse	192.168.0.192/27	192.168.0.223	192.168.0.193	192.168.0.222
Headquarters	192.168.2.0/23	192.168.3.255	192.168.2.1	192.168.3.254
Headquarters - SV	192.168.0.192/29	192.168.0.199	192.168.0.193	192.168.0.198

Figure 2.2: Table of Addressing Values

2.2 Network Topology

In order to put the addressing to practice and at the same time making sure that we don't lose the ssh remote access, every TUX has two different interfaces, one for remote access and the other for addressing (once we are doing this assignment remotely). The distribution of the different working stations as well as the four new VLANs, was made as follows:

Ethernet	Host	Vlan	Network	IP	Location	Gateway
Fa0/1	tux21 eth0	1	172.16.1.21			
Fa0/9	tux21 eth1	2	192.168.0.0/27	192.168.0.1	Store1	192.168.0.30
Fa0/4	tux22 eth0	1	172.16.1.22			
Fa0/15	tux22 eth1	3	192.168.0.224/27	192.168.0.225	Warehouse	192.168.0.254
Fa0/5	tux23 eth0	1	172.16.1.23			
Fa0/17	tux23 eth1	4	192.168.0.192/29	192.168.0.193	HQ	192.168.0.198
Fa0/8	tux24 eth0	1	172.16.1.24			
Fa0/19	tux24 eth1	5	20.49.51.160/28	20.49.51.161	DMZ	20.49.51.174

Figure 2.3: Selected TUX's for DMZ, Server Network, Store and Warehouse.

The Gigabit Ethernet 0/2 interface on the switch was set in trunk mode from VLAN 1 to 5. Even though we are only using VLANs 2 to 5 on this lab work, the default and first one shall also be included in order to grant the SSH access to the lab. The router GigabitEthernet 0/0 is connected to the switch in the interface previously mentioned.

```
vlan 2
    name vlan2-Store1
    exit
interface Fa0/9
    switchport access vlan 2

vlan 3
    name vlan3-Warehouse
    exit
interface Fa0/15
    switchport access vlan 3

vlan 4
    name vlan4-HQ
    exit
interface Fa0/17
    switchport access vlan 4

vlan 5
    name vlan5-DMZ
    exit
interface Fa0/19
    switchport access vlan 5

interface GigabitEthernet 0/2
    switchport trunk allowed vlan 1-5
    switchport mode trunk
```

Figure 2.4: Switch configuration.

```
interface gigabitEthernet 0/0.2

description vlan2-Store1
encapsulation dot1Q 2
ip add 192.168.0.30 255.255.255.224
shutdown
no shutdown
exit


interface gigabitEthernet 0/0.3

description vlan3-Warehouse
encapsulation dot1Q 3
ip add 192.168.0.254 255.255.255.224
shutdown
no shutdown
exit


interface gigabitEthernet 0/0.4

description vlan4-HQ
encapsulation dot1Q 4
ip add 192.168.0.198 255.255.255.248
shutdown
no shutdown
exit


interface gigabitEthernet 0/0.5

description vlan5-DMZ
encapsulation dot1Q 5
ip add 20.49.51.174 255.255.255.240
shutdown
no shutdown
exit


interface gigabitEthernet 0/0
    description switch-trunk
    no shutdown
```

Figure 2.5: Router configuration.

3. DNS Service

To set up the DNS service we installed bind9 in all three stations and automatically created the directory where the new folder /etc/bind/ would be storing the bind configuration files. In this folder there are five important files which require some explanation:

- named.conf: Includes all the configuration files. Its the main configuration file of the named daemon and the DNS server.
- named.conf.options: Has all the general configurations regarding the type of dns setup required (forwarding or caching). In this file we define who should and should not have access to the server. In this case the IP was set to 192.168.0.0/21 as we intended to give access to all the intranet and added it to the allow-query list. The recursion was also enabled in order to protect the query in case the server isn't able to respond. Finally the DMZ dns server was configured as forwarder and we also enabled public key encryption and validation in order to protect the network from outsiders from sniffing packets.
- named.conf.local: Defines the local DNS where we the servers adddressing is done, qquma.pt was defined as master and pointed to DNS tables file, and loja1.qquma.pt as a slave where we also pointed the IP address of the masters.
- named.conf.log: Configures the logging functionality as a maintenance measure. In this registry it is possible to check the date of the request, the query name, class type in addition to the IP address and client port. It is also possible to see if the the security measures were working properly and if the recursion was active or not.
- db.local: Its where the DNS tables are located and its where parameters like timeout and expire times defined as such:

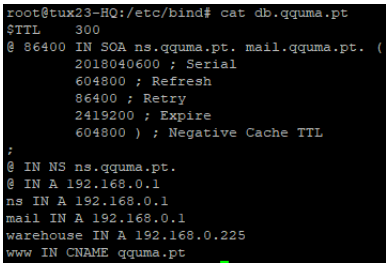

Figure 3.1: Example of db.local file.

Serial: Identifies when a new configuration version is available. Its name is the date of creation and its incremented each time the file is modified

Refresh: Its the time span before the slave verifies the existance of a new update and copies the new settings.

Retry: Its the time that the master server waits if a the slave attempts to refresh and fails. If this happens it will upadte again.

Expire: How much time the slave should wait, before verifying if an authoritative is no longer authoritative.

Minimum: Maximum valid time for a specific domain data.

3.1 NAT Configuration on DMZ

So that there can be communication between the Intranet (192.168.2.0/23), the DMZ (20.49.51.160/28) and the internet, through the network of bench 2 (172.16.2.0/24), there needs to be a translation of the addresses at the intermediate points: DMZ and Server's Network. This means that there will be an intranet translation for DMZ and another one for DMZ outside. For this to happen, the IP fowarding process will have to be activated to control the path of the packets between the LAN.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Figure 3.2: IP Fowarding.

Given this process, it is not yet possible to access the intranet or DMZ through the nodes. The next command line allows you to change and send packages outside the network, changing the internal address with a port address that communicates with the network in this case, the eth0 port address.

```
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Figure 3.3: Connection via Nodes to Intranet and DMZ.

The following command allows incoming packets to the intranet that belong to a connection already established.In this case, eth0 is the incoming port of external network, and eth1 is the connection to intranet.

```
/sbin/iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED
-j ACCEPT
```

Figure 3.4: Acceptance of already established network packets.

For redirect DMZ packets outside the intranet, this command has been executed.

```
/sbin/iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

Figure 3.5: Redirect packets to outside.

Finally, DMZ or internet access to the intranet was blocked, so that it is not possible that they have direct access to the internal servers of this network, with the following command.

```
/sbin/iptables -A FORWARD -i eth0 -o eth1 -m state --state NEW,INVALID -j REJECT
```

Figure 3.6: Blocking access from DMZ to Internal Network.

Completing these 5 processes, the network topology presents two address translations, so that there is no direct access from outside and from DMZ to the internal network.

3.2 DNS on DMZ

The qquma.pt zone was created on the server that simulates the DMZ network, which is visible from the outside. The zone was created in the named.conf.local file as type master and a zone file with the translations between site names and addresses.

```
root@tux24-DMZ:/etc/bind# cat db.qquma.pt
$TTL    300
@ 86400 IN SOA ns.qquma.pt. mail.qquma.pt. (
        2018040600 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS ns.qquma.pt.
@ IN A 20.49.51.161
ns IN A 20.49.51.161
www IN CNAME qquma.pt
```

Figure 3.7: db.qquma.pt file

```
root@tux23-HQ:/etc/bind# cat named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "qquma.pt" {
        type master;
        notify yes;
        file "/etc/bind/db.qquma.pt";
};

zone "storel.qquma.pt" {
        type slave;
        masters {192.168.0.1;};
};
```

Figure 3.8: Named.conf.local file

3.3 DNS on Servers Network

On the server that simulates the servers network, the qquma.pt type master zones and a loja1.qquma.pt type slave. This zone is notified of changes to the type slave zone. The DNS server accesses the DNS server allocated in the DMZ in forward mode to resolve names.

```
root@tux23-HQ:/etc/bind# cat named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "qquma.pt" {
        type master;
        notify yes;
        file "/etc/bind/db.qquma.pt";
};

zone "storel.qquma.pt" {
        type slave;
        masters {192.168.0.1;};
};
```

Figure 3.9: named.conf.local file

```
root@tux23-HQ:/etc/bind# cat named.conf.options
acl goodclients {
        192.168.0.0/20;
        localhost;
        localnets;
};

options {
        directory "/var/named/";

        recursion yes;
        allow-query {goodclients;};
        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                20.49.51.161;
        };

        forward only;

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================

        dnssec-enable yes;
        dnssec-validation yes;

        auth-nxdomain no;
        listen-on-v6 { any; };
};
```

Figure 3.10: named.conf.options file

```
root@tux23-HQ:/etc/bind# cat db.qquma.pt
$TTL    300
@ 86400 IN SOA ns.qquma.pt. mail.qquma.pt. (
        2018040600 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS ns.qquma.pt.
@ IN A 192.168.0.1
ns IN A 192.168.0.1
mail IN A 192.168.0.1
warehouse IN A 192.168.0.225
www IN CNAME qquma.pt
```

Figure 3.11: db.qquma.pt file

3.4 DNS on Store

The store1.qquma.pt zone was created on the server that simulates the store and it is only visible through the internal network. The zone was created as a type master and zone file. This zone notifies and transfers backups from this server to the slave which is located in the Servers Network. This DNS server access the DNS server host on the Servers network in forward mode in order to resolve hostnames.

```
tux21-Store1:/etc/bind# cat named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "store1.qquma.pt" {
        type master;
        file "/etc/bind/db.store1.qquma.pt";
        notify yes;
        allow-transfer {192.168.0.193;};
};
```

Figure 3.12: named.conf.local file

```
tux21-Store1:/etc/bind# cat named.conf.options
acl goodclients{
        192.168.0.0/21;
        localhost;

};

options {
        directory "/var/cache/bind";
        recursion yes;
        allow-query {goodclients;};
        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                192.168.0.193;
        };

        forward only;

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-enable yes;
        dnssec-validation yes;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

Figure 3.13: named.conf.options file

```
tux21-Store1:/etc/bind# cat db.store1.qquma.pt
$TTL    300
@ 86400 IN SOA ns.store1.qquma.pt. mail.store1.qquma.pt. (
        2018040600 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS ns.store1.qquma.pt.
@ IN A 192.168.0.1
ns IN A 192.168.0.1
proxy IN A 192.168.0.1
www IN CNAME store1.qquma.pt
```

Figure 3.14: db.qquma.pt file

3.5 DNS on Warehouse

On the warehouse no zone was created since this server operates in cache mode whose database is hosted on the servers' network. This DNS server accesses the DNS server hosted at said network in forward mode to resolve the hostnames.

```
root@tux22-Warehouse:/etc/bind# cat named.conf.options
acl goodclients {
        192.168.0.0/21;
        localhost;
        localnets;
};

options {
        directory "/var/cache/bind";

        recursion yes;
        allow-query {goodclients;};
        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
        192.168.0.193;
        };

        forward only;

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        auth-nxdomain no;
        listen-on-v6 { any; };
};
```

Figure 3.15: named.conf.options file

4. Conclusion

This lab work helped to understand all the different configurations that are possible while doing the IP addressing scheme of a real company with different network sizes and technologies plus some security challenges concerning the DNS service. Each department of the company ended up with its own IP network with different masks in order to waste as less resources as possible.

It was possible to understand all the different DNS configurations and typologies as well as understanding them all much clearer. It is now obvious the importance of a DNS service and its proper configuration. The DNS public key encryption and validation, along with the proper NAT settings also allowed us give the network a second layer of defense against nefarious attackers.