NETWORKS REPORT

TEAM:
Majid Rahmanov (majid.rahmanov@ufaz.az)
Huseyn Naghiyev (huseyn.naghiyev@ufaz.az)
Vasif Shirinzade (vasif.shirinzade@ufaz.az)

Table of contents

Introduction

To build a network model , we should consider tons of factors such as reliability, accessibility, security , flexibility and so on.

Network Architecture should be created in a way that it can be further extended , that is where subnetting comes to the scene.

Another important point is to divide network by user groups to prevent devices overload which appear during broadcast requests. Here VLAN can be implemented.

Devices should be chosen in the right way , for example not to use an extra router where a switch can make a needed task , a router is more expensive.

Security is also crucial , as hosts on network can have different user groups and ability to access other groups on network. ACL will help us with this aspect.

Subnetting

As our network consists of 4 buildings and 3 of them contains 3 services with 250 beds and 10 doctors and nurses → we have 780 hosts per building. About the 1st building we can say that it consists of 4 services one of which is Local Server. Number of hosts in building 1 is not set , so we considered it.

Now to meet our needs , we decided to give /21 subnet mask for each building. Why? - because we took 3 bits from /18 which gave us 2 in power of $3 = 8$ subnets. 4 of them we assigned to buildings and 1 for interconnection. Other 3 subnets we will keep for future in case the network will grow.
The subnet of connection was then divided by VLSM into 5 /30 networks to connect routers with each other.

Addressing Table

Device Name	Interface	IP Address	Subnet Mask
Building 1	s0/0/0	172.16.0.2	255.255.255.252
	s0/0/1	172.16.0.5	255.255.255.252
	g0/0.2	172.16.8.1	255.255.254.0
	g0/0.3	172.16.10.1	255.255.254.0
	g0/0.4	172.16.12.1	255.255.254.0
	g0/0.5	172.16.14.1	255.255.254.0
Main Router	s0/0/0	172.16.0.6	255.255.255.252
	s0/0/1	172.16.0.9	255.255.255.252
	s0/1/0	172.217.22.1	255.255.255.252
Building 2	s0/0/0	172.16.0.13	255.255.255.252
	s0/0/1	172.16.0.10	255.255.255.252
	g0/0.2	172.16.16.1	255.255.252.0
	g0/0.3	172.16.20.1	255.255.252.0
Building 3	s0/0/0	172.16.0.1	255.255.255.252
	s0/0/1	172.16.0.17	255.255.255.252
	g0/0.2	172.16.24.1	255.255.252.0
	g0/0.3	172.16.28.1	255.255.252.0
Building 4	s0/0/0	172.16.0.14	255.255.255.252
	s0/0/1	172.16.0.18	255.255.255.252
	g0/0.2	172.16.32.1	255.255.252.0
	g0/0.3	172.16.36.1	255.255.252.0

Dividing Services to VLANs

First building has 4 services , which means 4 different groups. We decided to separate all of them into vlans , as we want our network to have high performance and be secure.

Why? - when network devices make a request to broadcast it sends it to all devices - and it is a big problem in big networks. Let's consider 780 hosts + routers and switches - it will slow down the network. Also we introduced vlan because it gives some kind of security , that is when a device sends broadcast

and multicast requests , they will reach all devices and it is a confidentiality issue.

So we have 4 vlans in building 1: IT , administration , accounting and local server vlans.

About Buildings 2-4 , we considered the building as service per floor. So services will be divided by floor , using switches. And then we introduced vlan to separate doctors from patients.

So we have 2 vlans in buildings 2-4: Doctors and Patients.

Routing

In order for buildings to access each other and hosts on all services access the internet , we need Routing.

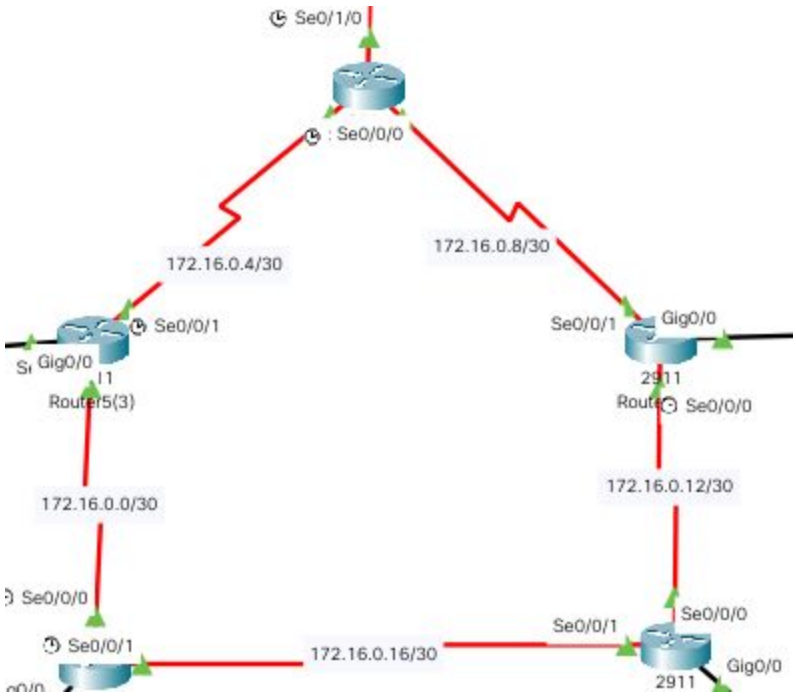
Routing is used to make networks within one router be known by networks on other routers.

Some information about our choice - there are 2 types of routing static and dynamic. Static will be very inefficient in our network , because it is big although we introduced it in some places , which we will discuss later.

Dynamic routing is the one we need , there are several Dynamic Routing Protocols , but we are familiar with RIPv2 and OSPF. We decided to use OSPF , because it is very efficient in a big network.

OSPF was introduced between routers.

Network and OSPF table



Physical Config CLI

IOS Command Line Interface

```
    172.16.0.0/16 is variably subnetted, 17 subnets, 4 masks
O      172.16.0.0/30 [110/128] via 172.16.0.5, 00:22:58, Serial0/0/0
C      172.16.0.4/30 is directly connected, Serial0/0/0
L      172.16.0.6/32 is directly connected, Serial0/0/0
C      172.16.0.8/30 is directly connected, Serial0/0/1
L      172.16.0.9/32 is directly connected, Serial0/0/1
O      172.16.0.12/30 [110/128] via 172.16.0.10, 00:22:58, Serial0/0/1
O      172.16.0.16/30 [110/192] via 172.16.0.5, 00:22:58, Serial0/0/0
                      [110/192] via 172.16.0.10, 00:22:58, Serial0/0/1
O      172.16.8.0/23 [110/65] via 172.16.0.5, 00:22:58, Serial0/0/0
O      172.16.10.0/23 [110/65] via 172.16.0.5, 00:22:58, Serial0/0/0
O      172.16.12.0/23 [110/65] via 172.16.0.5, 00:22:58, Serial0/0/0
O      172.16.14.0/23 [110/65] via 172.16.0.5, 00:22:58, Serial0/0/0
O      172.16.16.0/22 [110/65] via 172.16.0.10, 00:22:58, Serial0/0/1
O      172.16.20.0/22 [110/65] via 172.16.0.10, 00:22:58, Serial0/0/1
O      172.16.24.0/22 [110/129] via 172.16.0.5, 00:22:58, Serial0/0/0
O      172.16.28.0/22 [110/129] via 172.16.0.5, 00:22:58, Serial0/0/0
O      172.16.32.0/22 [110/129] via 172.16.0.10, 00:22:58, Serial0/0/1
O      172.16.36.0/22 [110/129] via 172.16.0.10, 00:22:58, Serial0/0/1
    172.217.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.217.22.0/30 is directly connected, Serial0/1/0
L      172.217.22.1/32 is directly connected, Serial0/1/0
S*  0.0.0.0/0 [1/0] via 172.217.22.2
```

Ctrl+F6 to exit CLI focus Copy Paste

Top

Static and Dynamic routing configuration:

```
router ospf 1
 log-adjacency-changes
 network 172.16.0.4 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
```

```
ip route 0.0.0.0 0.0.0.0 172.217.22.2
!
```

NAT

NAT is used to convert private IP addresses to public. We used it in our model as it is essential for internet access and in order to access world wide web. Also we used the ACL rule to permit all hosts access to the internet.

Configuration:

```
ip nat inside source list nat interface Serial0/1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 172.217.22.2
!
```

```
ip access-list standard nat
 permit any
!
```

ACL

We used ACL in order to permit internet access to all devices on a network. Then we used it to deny all services to ping IT service , but allow echo-reply packets to go to IT service , which allow IT hosts ping other devices. Also ACL was used to allow doctors to ping Local Server and Accounting but deny pinging of Administration. And finally ACL that denies patients from pinging all services in building 1.

Configuration:

```
ip access-list extended patient-acl
 deny ip any 172.16.10.0 0.0.1.255
 deny ip any 172.16.12.0 0.0.1.255
 deny ip any 172.16.14.0 0.0.1.255
 permit ip any any
ip access-list extended doctor-acl
 deny ip any 172.16.12.0 0.0.1.255
 permit ip any any
!
```

```
ip access-list extended it-acl
 permit icmp any any echo-reply
!
```

Conclusion

As a result we have functional model of network , see the topology: