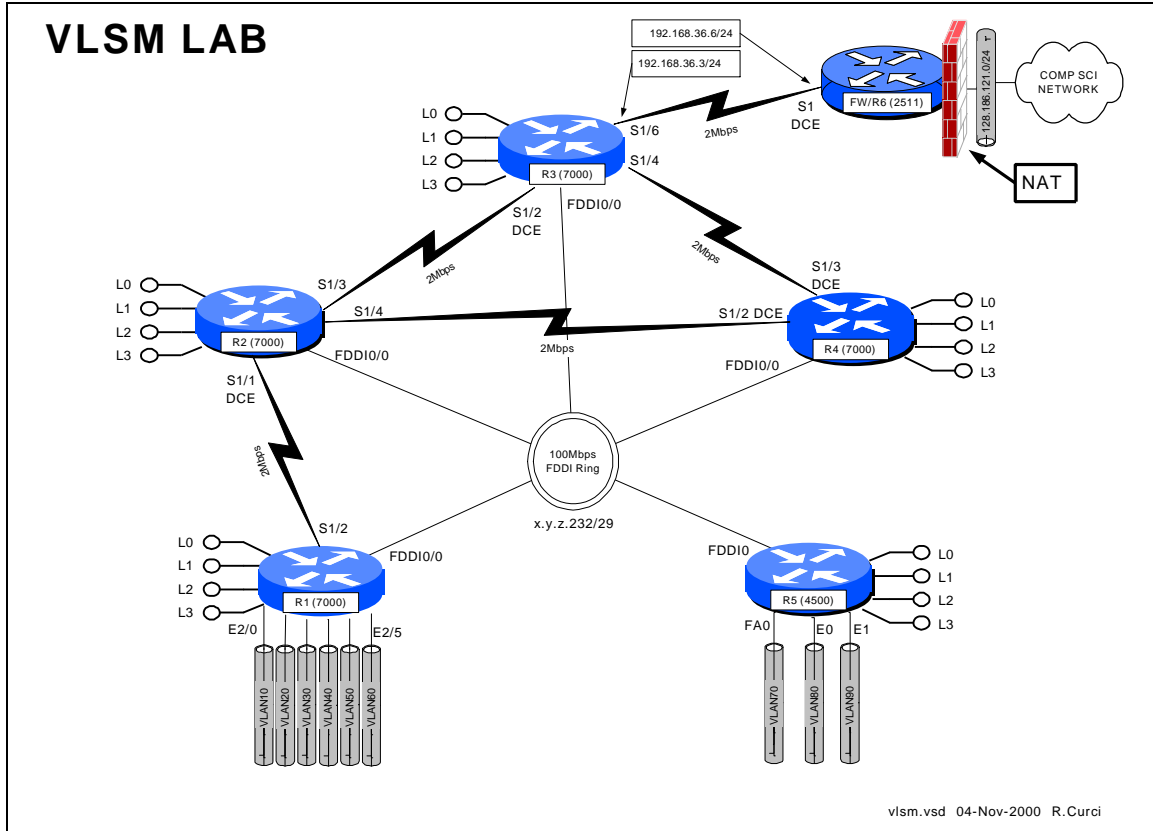INTERNET TEACHING LAB: VLSM LAB

Overview

The Internet is running out of IP address space and your network addressing scheme with all /24 subnets is wasteful.   Configure routers R1,R2,R3,R4, and R5 as shown above. Create a new IP addressing scheme for the network that efficiently utilizes class C network 192.168.100.0/24. Do not worry about router R6 or the R3-R6 serial link which can be numbered as shown in the diagram. You will need to use a technique called "variable length subnet masking" (VLSM) where you subdivide your network address space into subnetworks of different sizes. When you have finished this exercise, capture the output of the following commands to prove you completed the assignment.

-   show running-config
-   show ip interface brief
-   show cdp neighbors
-   show ip ospf neighbor
-   show ip route
-   show ip protocol

PART 1 – IP Addressing

On each router R1 through R5, create four loopback interfaces that will support the following number of hosts.

INTERFACE	# HOSTS
loopback0	14 hosts
loopback1	6 hosts
loopback2	2 hosts
loopback3	2 hosts

Begin by looking at each network and deciding how many host addresses must be supported to figure out the size of each subnet. You must do this with maximum efficiency as there no extra addresses, only exactly enough to solve this problem. For each of the five routers, select the loopback subnets such that they can be summarized. If you do not understand the concept of summarization, read up on CIDR – Classless Internet Domain Routing. You will need to use the command "ip classless" on your router to make it ignore the classfull (i.e. Class A, B, C) network mask assumptions. Since we will be using all subnets including subnet zero, you will also need the command "ip subnet-zero" in your configuration.

PART 2 – OSPF Routing

When using variable length subnet masks in your network, you will need an IP routing protocol that supports VLSM such as OSPF (Open Shortest Path First). Configure OSPF as your only routing protocol. All FDDI, Ethernet, FastEthernet, and Serial interfaces should be in area 0. Place the loopback addresses on each of the five routers in a separate area corresponding to the router identifier. For example, the loopback addresses on router 3 should be in area 3. You may wish to use the following commands to help debug your OSPF configuration:

- show ip ospf neighbor
- show ip ospf database
- show ip ospf database-summary
- show ip ospf interface
- show ip route
- show ip route ospf
- show ip protocol

PART 3 – Address Summarization

In large networks like the Internet, the number of network routes that fit in the routing table becomes a limiting factor. In the mid 1980s with the exponential growth of the Internet, many predicted the collapse of the Internet backbone due to the growing size of

the routing tables. This problem was helped by the creation of CIDR – Classless Internet Domain Routing, which summarizes network blocks without regard to the classfull network designations. As of this writing, there are approximately 90,000 routes on the Internet, a number that would be much higher without CIDR. Routing protocols like OSPF are very scalable when used with hierarchical network addressing schemes that support summarization. Your routers should be advertising their loopback addresses as individual routes, each creating its own routing table entry in the routing tables of the other routers. For each of the five routers, reconfigure OSPF to advertise a single summary route for all four loopback addresses instead of advertising them individually. Because each router is participating in more than one OSPF area, it is an autonomous system boundary router (ASBR). ASBRs can summarize the routes within their non-zero areas into the core area zero to reduce the number of routes the core area zero routers must keep in their tables. Verify everything is working by studying the output of the commands "show ip route", "show ip protocol", "show ip ospf neighbor", "show ip ospf database database-summary", "show ip ospf interface", etc. If you simply type "show ip ospf ?" you will see the various options available.

PART 4 – Network Assurance

Assign new IP addresses for your PCs using the new IP address scheme. Note that not only your IP address, but also your gateway, broadcast address, netmask, and network addresses have changed. Verify everything is reachable by scanning the lab network from a UNIX PC using the NMAP utility. This utility can be found at www.insecure.org/nmap. Be sure to only scan within the lab network because probes outside the lab will cause firewalls and intrusion detection systems to complain and are presently treated by law enforcement as attempted unauthorized access.

PART 5 – GateD / Extra Credit

Configure your Linux system to use GateD by modifying file /etc/gated.conf. Configure your system to use the OSPF routing protocol on its ethernet port which should be in area zero. Use the command "netstat –rn" to display your routing table. You should see routes for all networks in area zero plus the summary routes for non-area zero networks. You should also see a default route sometimes listed as '0.0.0.0'. Be sure to remove any static default route on your system, as you should learn the default dynamically from OSPF.