Structured Design

11.9.1

IPv4 Network Address Planning

Before you start subnetting, you should develop an IPv4 addressing scheme for your entire network. You will need to know how many subnets you need, how many hosts a particular subnet requires, what devices are part of the subnet, which parts of your network use private addresses, and which use public, and many other determining factors. A good addressing scheme allows for growth. A good addressing scheme is also the sign of a good network administrator.

Planning IPv4 network subnets requires you to examine both the needs of an organization's network usage, and how the subnets will be structured. Performing a network requirement study is the starting point. This means looking at the entire network, both the intranet and the DMZ, and determining how each area will be segmented. The address plan includes determining where address conservation is needed (usually within the DMZ), and where there is more flexibility (usually within the intranet).

Where address conservation is required, the plan should determine how many subnets are needed and how many hosts per subnet. As discussed earlier, this is usually required for public IPv4 address space within the DMZ. This will most likely include using VLSM.

Within the corporate intranet, address conservation is usually less of an issue This is largely due to using private IPv4 addressing, including 10.0.0.0/8, with over 16 million host IPv4 addresses.

For most organizations, private IPv4 addresses allow for more than enough internal (intranet) addresses. For many larger organizations and ISPs, even private IPv4 address space is not large enough to accommodate their internal needs. This is another reason why organizations are transitioning to IPv6.

For intranets that use private IPv4 addresses and DMZs that use public IPv4 addresses, address planning and assignment is important.

Where required, the address plan includes determining the needs of each subnet in terms of size. How many hosts there will be per subnet? The address plan also needs to include how host addresses will be assigned, which hosts will require static IPv4 addresses, and which hosts can use DHCP for obtaining their addressing information. This will also help prevent the duplication of addresses, while allowing for monitoring and managing of addresses for performance and security reasons.

Knowing your IPv4 address requirements will determine the range, or ranges, of host addresses that you implement and help ensure that there are enough addresses to cover your network needs.

11.9.2

Device Address Assignment

Within a network, there are different types of devices that require addresses:

- **End user clients** – Most networks allocate IPv4 addresses to client devices dynamically, using Dynamic Host Configuration Protocol (DHCP). This reduces the burden on network support staff and virtually eliminates entry errors. With DHCP, addresses are only leased for a period of time, and can be reused when the lease expires. This is an important feature for networks that support transient users and wireless devices. Changing the subnetting scheme means that the DHCP server needs to be reconfigured, and the clients must renew their IPv4 addresses. IPv6 clients can obtain address information using DHCPv6 or SLAAC.
- **Servers and peripherals** - These should have a predictable static IP address. Use a consistent numbering system for these devices.
- **Servers that are accessible from the internet** - Servers that need to be publicly available on the internet must have a public IPv4 address, most often accessed using NAT. In some organizations, internal servers (not publicly available) must be made available to the remote users. In most cases, these servers are assigned private addresses internally, and the user is required to create a virtual private network (VPN) connection to access the server. This has the same effect as if the user is accessing the server from a host within the intranet.
- **Intermediary devices** - These devices are assigned addresses for network management, monitoring, and security. Because we must know how to communicate with intermediary devices, they should have predictable, statically assigned addresses.
- **Gateway** - Routers and firewall devices have an IP address assigned to each interface which serves as the gateway for the hosts in that network. Typically, the router interface uses either the lowest or highest address in the network.

When developing an IP addressing scheme, it is generally recommended that you have a set pattern of how addresses are allocated to each type of device. This benefits administrators when adding and removing devices, filtering traffic based on IP, as well as simplifying documentation.

11.9.3

Packet Tracer - VLSM Design and Implementation Practice

In this activity, you are given a /24 network address to use to design a VLSM addressing scheme. Based on a set of requirements, you will assign subnets and addressing, configure devices, and verify connectivity.

📄 VLSM Design and Implementation Practice

⬇ VLSM Design and Implementation Practice