IP Subnetting

Brian Bergstrom

ITCO 251 Network Infrastructure Basics

AIU Online

Michael Pry

IP Subnetting

The IP address is an important part of networking. This tells the network where a computer or device is on a network, kind of like a street address. IP stands for Internet protocol and is in the Internet layer of the OSI Model (Dean, 2013, p.148). The packets that are sent on this layer are divided into 4 octets which can be binary or decimal. Depending on how these numbers are arranged tells you information about the host computer. There are two types of IP addressing, IPv4 and IPv6. The IPv4 is not used very often anymore, because of the wide implementation of IPv6. However, it is still important to note that both still do exist.

Subnetting is a technique used in IP addressing that that a single class of networks and divides them into a bunch of more logical, smaller networks (Dean, 2013, p. 157). This becomes useful for managing network traffic to make sure network traffic flows smoothly and not everyone is using the same lane. Dividing things up frees up more lanes so even more network traffic can get through.

There are a few types of addresses that exist that determine how data is sent and received across network devices. The first type is a unicast address which is simply used to communicate from one device like a server to your company laptop. It uses only one interface that would be assigned to something like a network adapter (Dean, 2013, p. 159). Multicast addresses represent multiple interfaces and can be on multiple devices across a network. IPv6 allows for several types of multicast groups and directs data to all reachable nodes. In IPv4, computers must share the same link in order to communicate in the transmitting mode. (Dean, 2013). The third type is really handy to get multiple devices to transmit the data quickly. Anycast addressing borrows multiple devices to help transmit data in case one is backlogged in traffic. This way things can get done much quicker without depending on one device to send or receive the message (Dean, 2013). For a large company I would say anycast addressing is most efficient because if there are problems, other devices can pick up the slack.

As mentioned before, IP addresses are presented in octets. There are three different network classes an IP address can have and the octet gives us a clue about which class the IP is under. Class A has a beginning octet between the range of 1 and 126. Fr example, 23.78.110.109 is an example of a Class A network ID. Class B falls between 128 and 191. Class C lies between 192 and 223. Some addresses are reserved addresses for performing special functions. For example, 127 is a special one that is used for loopback addresses. Loopback addressing is when you attempting to reach your own network and check its connectivity (Dean, 2103, p.155).

Assigning everyone an IP address on a large network can be quite the task. That is why they have Dynamic Host Configuration Protocol or DHCP. This automated process assigns IP addresses to devices on the network. The application layer of the OSI model is where this occurs (Dean, 2013, p.160). With this method is saves a lot of time and headaches for the IT staff. With humans, there is always a chance a mistake can be made. With DHCP, the server knows which IP addresses are available and which are not. It’s also more convenient because users can move to multiple workstations without having to reconfigure their settings each time (Dean, 2013). This is useful for internal management of IP addresses, but what about across a global network such as the internet?

Domain name servers help associate domain names with an IP address on a network. The DNS service does not rely on just one server like with DHCP, but instead relies on many computers across the globe. The application layer of the OSI model is where this all takes place (Dean, 2013, p. 169). Most people know what a domain name is like yahoo.com, but eaxch domain isn linked to a IP address on a server somewhere. The DNS cache stores any information about a site you have looked up before on your computer so it will load faster the next time you visit.

There are a few types of network protocols that exist that allow you to communicate with the network you are on and troubleshoot. ”Telnet is a terminal protocol used to log on to remote hosts using the TCP/IP suite” (Dean, 174). This method is known to be unsecure. FTP or file transfer protocol is a popular way of transferring files onto a server or site from a computer. The application layer handles this sort of protocol. This can be done via the command line or via graphical software such as CuteFTP or WS\_FTP\_LE. SFTP is a more secure version of FTP that has been released.

IP subnetting and managing IP addresses is important to understand when dealing with networks. One must understand which IP addresses are for which classes and the different functions they provide and serve. Communication between computers is difficult to understand in general, but understanding how IP addresses work will help you understand how to communicate with both computers and networks, helping your company save both time and money in the long and short term.

Works Cited

Dean. (2013). *Network+ Guide to Networks*, 6th Edition.

[Bookshelf Online]. Retrieved from https://online.vitalsource.com/#/books/9781133608196/