Subnetting

Overview

A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.

What is an IP address?

In order to understand subnets, we must quickly define IP addresses. Every device that connects to the Internet is assigned a unique IP (Internet Protocol) address, enabling data sent over the Internet to reach the right device out of the billions of devices connected to the Internet. While computers read IP addresses as binary code (a series of 1s and 0s), IP addresses are usually written as a series of alphanumeric characters.

What do the different parts of an IP address mean?

This section focuses on IPv4 addresses, which are presented in the form of four decimal numbers separated by

periods, like 203.0.113.112. (IPv6 addresses are longer and use letters as well as numbers.)

Every IP address has two parts. The first part indicates which network the address belongs to. The second part specifies the device within that network. However, the length of the "first part" changes depending on the network's class.

Networks are categorized into different classes, labeled A through E. Class A networks can connect millions of devices. Class B networks and Class C networks are progressively smaller in size. (Class D and Class E networks are not commonly used.)

Let's break down how these classes affect IP address construction:

- **Class A network:** Everything before the first period indicates the network, and everything after it specifies the device within that network. Using 203.0.113.112 as an example, the network is indicated by "203" and the device by "0.113.112."
- **Class B network:** Everything before the second period indicates the network. Again using 203.0.113.112 as an example, "203.0" indicates the network and "113.112" indicates the device within that network.
- **Class C network:** For Class C networks, everything before the third period indicates the network. Using the same example, "203.0.113" indicates the Class C network, and "112" indicates the device.

Why is subnetting necessary?

As the previous example illustrates, the way IP addresses are constructed makes it relatively simple for Internet routers to find the right network to route data into. However, in a Class A network (for instance), there could be millions of connected devices, and it could take some time for the data to find the right device. This is why subnetting comes in handy: subnetting narrows down the IP address to usage within a range of devices.

Because an IP address is limited to indicating the network and the device address, IP addresses cannot be used to indicate which subnet an IP packet should go to. Routers within a network use something called a subnet mask to sort data into subnetworks.

What is a subnet mask?

A subnet mask is like an IP address, but for only internal usage within a network. Routers use subnet masks to route data packets to the right place. Subnet masks are not indicated within data packets traversing the Internet — those packets only indicate the destination IP address, which a router will match with a subnet.

Suppose Bob answers Alice's letter, but he sends his reply to Alice's place of employment rather than her home. Alice's

office is quite large with many different departments. To ensure employees receive their correspondence quickly, the administrative team at Alice's workplace sorts mail by department rather than by individual employee. After receiving Bob's letter, they look up Alice's department and see she works in Customer Support. They send the letter to the Customer Support department instead of to Alice, and the customer support department gives it to Alice.

In this analogy, "Alice" is like an IP address and "Customer Support" is like a subnet mask. By matching Alice to her department, Bob's letter was quickly sorted into the right group of potential recipients. Without this step, office administrators would have to spend time laboriously looking for the exact location of Alice's desk, which could be anywhere in the building.

For a real-world example, suppose an IP packet is addressed to the IP address 192.0.2.15. This IP address is a Class C network, so the network is identified by "192.0.2" (or to be technically precise, 192.0.2.0/24). Network routers forward the packet to a host on the network indicated by "192.0.2."

Once the packet arrives at that network, a router within the network consults its routing table. It does some binary mathematics using its subnet mask of 255.255.255.0, sees the device address "15" (the rest of the IP address indicates the network), and calculates which subnet the packet should go to. It forwards the packet to the router

or switch responsible for delivering packets within that subnet, and the packet arrives at IP address 192.0.2.15 (learn more about routers and switches).

Advantages of Subnetting

The advantages of Subnetting are mentioned below:

1. It provides security to one network from another network. e.g.) In an organization, the code of the Developer department must not be accessed by another department.
2. It may be possible that a particular subnet might need higher network priority than others. For example, a Sales department needs to host webcasts or video conferences.
3. In the case of Small networks, maintenance is easy.

Disadvantages of Subnetting

The disadvantages of Subnetting are mentioned below:

1. In the case of a single network, only three steps are required to reach a Process i.e Source Host to Destination Network, Destination Network to Destination Host, and then Destination Host to Process.
2. In the case of a Single Network only two IP addresses are wasted to represent Network Id and Broadcast

address but in the case of Subnetting two IP addresses are wasted for each Subnet.

3. The cost of the overall Network also increases. Subnetting requires internal routers, Switches, Hubs, Bridges, etc. which are very costly.

Basic Subnetting Routing