Ahuva Miller

Media Studies 255

Assignment 1: Profile of an Internet Technology

11 September 2018

IP Addresses

Ahuva Miller

MEDST 255

11 September 2018

Assignment 1: IP Addresses

An IP address, or an Internet Protocol Address, is the representation of where you live on the internet. It’s purpose is so our browsers, and ourselves, can be reachable. Imagine sending a letter through snail mail. You send a message, and expect to get a reply. In the same way, your internet server is your address.

As an initial internetting concept, IP addresses came about by Robert E. Kahn who saw the internet as an open-architecture network environment. This idea was introduced in 1972 when he realized that a reliable end-to-end protocol that maintained effective communication could not stay local to only the packet radio network. The Network Control Protocol, or the NCP for short, would avoid having to deal with the multitude of different operating systems, however it does not have the ability to address networks and machines. “Thus, Kahn decided to develop a new version of the protocol which could meet the needs of an open- architecture network environment. This protocol would eventually be called the Transmission Control Protocol/Internet Protocol (TCP/IP). While NCP tended to act like a device driver, the new protocol would be more like a communications protocol.” (1, Leiner, Barry M)

Kahn intended for an IP address to serve four critical functions. Firstly, each distinct network would connect to the internet, without any internal changes required by it. Secondly, communications sent from its source device would always make it to its intended destination, otherwise it must be retransmitted shortly. Thirdly, he envisioned gateways and routers as the means by which networks connected. “There would be no information retained by the gateways about the individual flows of packets passing through them, thereby keeping them simple and avoiding complicated adaptation and recovery from various failure modes.” (V. G. Cerf and R. E. Kahn) Lastly, the operations level of networks would never maintain global control.

He delegated Vint Cerf in the spring of 1973 to work with him on the detailed design of the protocol. This collaboration resulted in the basic approaches to what became TCP/IP. Most importantly, the development of the unique series of numbers that are written in bytes were decided to be the mode of communication between the processes.

An IP address is a unique series of numbers that identify computers and other devices on the internet. Any action you do online needs an IP address. It is composed of numbers separated by dots.

The IP address has two parts. The first part is the Network ID and the second part is the Host ID. Picture a street lined with houses. Each house has its own address, but each address has its own two parts. The first part is the house number, and the second part is the street number, which have all the houses have in common. To address a letter to a person living on said block, you would first write the number of the house, and then write the number of the street. An IP address works in the opposite way. The identifying variables are the other way around, you have the street and then the actual house number after that.

The address format of an IP address is written in the coded language of binary. The binary-to-decimal and decimal-to-binary conversion is pretty complex, but what you see is an IP address as a 32 bit binary number. For readability, the 32 bit binary number can be divided into four 8 bit octets. Then, each octet can be converted to decimal and the IP address can be written in dotted decimal notation. For example, the binary code of 10101100010000001000000000000000 can have the first 8 digits be converted to the decimal 172, the next eight digits to 16, then 128, and lastly 17, and the IP address of 172.16.128.17. This is for the purpose of readability and understanding the ways to communicate an IP address. The periods between the decimals is for further easing the effort of understanding each digit.

Because of a limited number of IP address numbers and the growing volume of people with access to the internet around the world, a system was developed in the 1990’s to slow down the rate that addresses were being used up. The Network Address Translation, or NAT, joins more than one addresses from your network to send to the server. The server replies, and NAT can allocate back each browser’s action effectively. This reduces the number of IP addresses used. This is why addresses can be pretty similar between devices. “This allows for future internet growth and simplifies IP Address configuration and administration.” (Tsirtsis, George, and Pyda Srisuresh)

As the internet becomes increasingly important as a business infrastructure, the number of attacks on it grows. Because of IP addresses, methods of IP traceback are crucial in efforts to detect hackers and the attack source. To accomplish IP traceback, the host where the attack originated needs to be reached. Normally, by checking the source IP address field of an IP packet, the origin can be found. However, senders can forge this information by using the problem with tracing beyond corporate firewalls. “Usually, firewalls control access based on source IP address, destination IP address, protocol type, source port number, and destination port number. For example, we can configure a firewall to deny any access to a WWW server except for WWW access using HTTP (destination port number 80). If an attacker attempts to exploit the WWW server using HTTP, however, the firewall cannot prevent it.”

With forged addresses, a method of Ingress Filtering can deal with IP traceback. In this method, a router compares an incoming packet’s source IP address with a router’s routing table and discards packets with inconsistent source addresses as having been forged. “This method is effective for many spoofed DoS attacks, but it fails if an attacker changes its source IP address to one that belongs to the same network as the attacker’s host.” (5, Baba, Tatsuya and Shigeyuki Matsuda)  
 This ongoing issue will prevail with the increasingly widespread use of the internet. Various methods of blocking IP addresses and new figurations of navigating beyond it remain one of the big crises of our global digital network. The innovative and practical development of IP addresses by Kahn and Cerf are creditable for what we are familiar with as today’s internet.

Citing:

1. Leiner, Barry M., et al. "A brief history of the Internet." ACM SIGCOMM Computer Communication Review 39.5 (2009): 22-31.
2. V. G. Cerf and R. E. Kahn, "A protocol for packet network interconnection", IEEE Trans. Comm. Tech., vol. COM-22, V 5, pp. 627-641, May 1974.
3. R. Kahn, Communications Principles for Operating Systems. Internal BBN memorandum, Jan. 1972. Proceedings of the IEEE, Special Issue on Packet Communication Networks, Volume 66, No. 11, November, 1978. (Guest editor: Robert Kahn, associate guest editors: Keith Uncapher and Harry van Trees)
4. Tsirtsis, George, and Pyda Srisuresh. Network address translation-protocol translation (NAT-PT). No. RFC 2766. 2000.
5. Baba, Tatsuya, and Shigeyuki Matsuda. "Tracing network attacks to their sources." IEEE Internet Computing 6.2 (2002): 20-26.