Very quick intro for IP networking

Or how to survive ELEC-E7130 network technology

Markus Peuhkuri

2023-09-01 (9ebe47a17e)

Abstract

This material is a **living document** for a part of Internet Traffic Measurements and Analysis course at Aalto University. Feedback and comments are appreciated via email or via course forum.

This material provides the reader a basic knowledge on IP networks and Internet with some pointers

Contents

1 Introduction to IP networking

This material is a **living document** for a part of Internet Traffic Measurements and Analysis course at Aalto University. Feedback and comments are appreciated via email or via course forum.

This material provides the reader a basic knowledge on IP networks and Internet with some pointers

1.1 Why there are packets?

In old telephone networks, a call occupied one physical cable for the duration of the call. Nobody other could use that. Later it was learnt to use e.g. carrier signal to transmit several calls over same cables, a bit like FM radio works. Later with digital technology, a resource could be shared by multiplexing over time with fixed time slots. But still, a limited resource was reserved for the duration of the call.

Data could be transmited over telephone wires but the usage was similar to phone calls: one connection reserved it from start to end. Of course, a connection could be taken down while a user was thinking what to do next (or computer processing data), but establishing connection was slow taking tens of seconds.

Even if the connection establishment would be a fast, it would be annoying not to be able to send a short message because the connection would be occupied for tens of minutes to transfer a data file for a movie.

To avoid large delays, a large file would be cut into pieces and these transmitted individually as “packets”. Now a small message could be interleaved among the packets of large file and would arrive to destination much earlier.

1.2 Addressing

In an old telephone, there was basically only one service: voice call. So a phone number, like 68 131, was sufficient to address. But then telefax and data modems were developed and if they shared the same line and number, one might end hearing modulated data.

Like a telephone, a computer in IP network typically has one IP address it can be addressed with a numeric value, like `192.0.2.42`. Quite often it is a dynamic one for your laptop or phone, i.e. you get one more or less random one every time you connect to network. The servers, however do typically have a permanent address.

For each IP packet, the sender puts its own IP address as a source address and the destination address is the address for the remote end. The remote address is learnt using method like a domain name service (DNS).

In computers, and in smartphones, one needs to know to which program the received data is to be delivered. Here comes the port numbers into play. Both TCP and UDP have port numbers for source and destination.

A HTTPS server listens on TCP port 443 for incoming connections, this is a *well-known port*. Now the web browser on a laptop has find out that the web server IP address is `192.0.2.80`. Its own address is `10.8.2.37` which it received when connecting to WiFi network. What is still missing is the local port number within the laptop. The browser might select one but it can set it initially as 0 in which case the operating system picks one that is vacant, like 48~092. That is a *dynamic port* number.

Now the operating system can establish a TCP connection from `10.8.2.37:48092` to `192.0.2.80:443`. The server responds and the systems perform a three-way handshake to create TCP connection. A TLS connection is then established with its own handshakes and finally the browser is able to send request, like `GET / HTTP/1.1` asking for the main page of the site. The request might fit into one packet, but if not, then additional packets are sent as needed. The response from the server most likely needs many packets, each with size of 1500 bytes carrying about 1440 bytes of application data.

In above examples, IP version 4 addresses were used but the basic functionality is the same with IP version 6; just addresses are much longer and written in colon-separated hexadecimal format instead of dottted decimal. Example of IPv6 addresses would be `2001:db8:0000:0000:0000:0000:0000:0001` that can be shortened as `2001:db8::1`, `2001:db8:12:48:ab:cdef:8765:4321`, or `ff01::1`.

1.3 How packets find towards destination?

Each address includes also an network-dependent netmask that will tell which part is *network part* and which is *host part*. Typically indicated as slash-number notation. For example, if you have a WiFi router at home, your laptop might receive address `192.168.1.100/24` and the WiFi router has address `192.168.1.1/24`. The number `24` will tell that 24 most significant bits are for the network and `32-24 =8` bits for the host. The 24 fits conviently for the dotted notation boundary, so we can say the network address is `192.168.1.0` and the host part is `1` and `100` for the router and the laptop respectively.

As the router and the laptop share the same network, they are able to communicate directly. The laptop just needs to broadcast an address resolution query (ARP) *Who has address 192.168.1.1?* and the router will answer with its own MAC (link) address. After that they can communicate with eachother.

If the laptop wants to communicate to an address `192.0.2.80`, it will compare it own address and the destination address with netmask. It will found out that these do not match. It needs to send packets via *default router* which then will forward the information towards destination. Also your WiFi router has typically a default route towards which it will send all non-local destination packets.

In the Internet routers exchange routing information using routing protocols that include BGP, OSPF and IS-IS. With these protocols a router knows to which neighbour router they need to send a packet with a specific destination address.

For the IPv6 the netmask is normally 64 bits while the point-to-point links between routers might have longer (e.g. 126).

2 Other sources

Aalto University course ELEC-C7241 (in Finnish) and ELEC-C7420 have additional source material for deeper understanding.

2.1 Notes

2.1.1 Phone call or a fax

Some devices actually answered call automatically and listened call to identify if it was fax or data modem. If not, forwarded to answering machine or ringed the phone.

2.1.2 How many IP address

An IP host can have many addresses, not just one. As of this writing, I have a test setup where a single virtual machine has more than 20~000 different IP addresses. In IP version 4, a host typically has just one IP address (e.g. 192.0.2.123) but with IP version 6, multiple addresses are typical to e.g. protect privacy as there is no shortage of IP addresses.

3 References