COMPUTER NETWORKING PRIMER

By Naveen PS

MAKERDEMY
LEARN EXPLORE MAKE

The Computer Networking Primer

Chapter 1 What is a Computer Network?

The first network was directly connected with wires, thus even when half a dozen people need to be in a network, the number of wires that have to be laid increased. Thus, they had human operators that manually switched wires to enable the communication as it's impossible to put a separate line to each and every one. The outgoing messages will be stored in a queue and each will wait their turn to use the full line and sent the full message. These things worked fine as long as the network was using one brand of computers. Different companies had their own way of using telephone wires to connect other computers to the network.

As the network grew, people found a much more efficient way of sending messages over long distances, without using a single direct line. They could hop the message from one computer to another to another since it reaches the destination. This is as long as each of the computers along the route of the message agreed to store & forward the message. But the disadvantage was that a message arriving at an intermediate computer may have to be stored there and forwarded after maybe hours depending on the traffic.

Sending entire messages one at a time this way. Might take minutes, hours, or days to reach the ultimate destination. It depends on the traffic at each of the hops.

The most important innovation that allowed the message to move more quickly across a multi-hop network was to break each message into small fragments called packets and then send them individually.

When messages are broken into packets, and each packet is sent separately, as each packet is sent one after the other.
Example:
Let's say Packets needed to complete a large message is 100, and Packets for small messages is 3. As the network alternates between sending packets of small and large messages before the 4 the packet of the large message gets sent, and the whole small message would have been sent. Thus, a small message doesn't have to wait till the large message gets finished.

Another advantage of a packet-based approach is that it reduces the amount of storage needed in the intermediate computers, as it doesn't need to store entire messages, nor for a long time.

People started creating special-purpose computers that were good in moving packets, to unload the load from the computer itself. These were called Interface Message Processors; alter they were called routers because their purpose was to route the packets to the ultimate destination. Another advantage of using IMPs or routers is that it is vendor-independent, so any brand Computer can work on the same network.

Earlier along with the messages, they also add the source and destination address so that, routers can take the best path for the message to go if more than one path was available.

But when packets were sent, we also had to add offset or position info so that the destination a put back the packets in the right order to reconstruct the message. Due to traffic and routing issues, most of the cases the packets will reach the destination non sequentially.

Normally, packets would find the shortest path between source & destination, but if a node is overloaded or broken the routers can cooperate and reroute traffic along longer paths.
The core of the internet is a set of cooperating routers that move packages.

Chapter 2 Networking Basics

Any challenging problem can be split into smaller problems and solved independently and put back together. Similarly, the internet problems were split into 4 subproblems and worked on it by different groups. TCP/IP Protocol.

1. Links Layer
2. Internetwork layer
3. Transport Layer
4. Application layer

Link Layer - The Link layer is responsible for connecting your computer to its local network and moving the data across a single hop. - Wi-Fi, Cellular, Ethernet, Fibre Optics, Satellite link
The Link layer needs to solve two basic problems when dealing
with these shared local area networks.

1. How to encode & send data across the link?
2. Agree on how to cooperate with other computers that might want to send

data at the same time.

Problem 1- If the links are wired, the engineers should use a standard in which they must agree on what voltage to use on the wire and how fast the bits are sent across. If Wireless, they must create a standard, that agrees on radio frequencies to be used and encoding methods.

Problem 2- To avoid data collision, to an extent packet concept helps. One packet after the other multiple computers can take turns to send packets, to get fair access to all computers.
But how do other computers know if the other computer wants to send data at the same time?
CSMA/CD- Carrier Sense Multiple Access with Collision Detection.

How does CSMA/CD Work?

1. When a computer wants to sense the data, it listens to see if another computer is already sending data - (Carrier Sense)
2. As your computer is sending data, it listens and sees if it can receive its own data, and if it gets, it continues sending (Collision Detection)

Internetwork Layer - Once your packets have passed the link layer, it will be in the Router or internetwork layer where the Interface Message Processors uses the source address and destination address, and figure out how to best move packets toward its destination. As billions of connections are being handled, the routers can't exactly give the direct path to the destination. Each of the routers along the way does its best to get the packet closer and closer to the destination after each hop. A holiday trip is the best analogy.

Just like on a holiday trip, many things can go wrong on the way to your destination. Like a Flight delay, Or a missed train, or an accident, etc. Routers exchange special messages and compare their routing tables, to adapt and self-configure in case of network failures. Even then something can go wrong and packets can get lost. This is where the next layer comes into the picture.

Transport Layer - Two bad conditions can arise from the previous level

1. Packets are lost or delayed
2. Packets arrive out of order because later packets found a quicker way

Problem 2: As we have already seen, the second problem is solved by sending offset information along with every packet to use it to sequence the packets and reconstruct the proper output.

Problem 1- As the destination reconstructs the message, it sends an acknowledgment back to the source computer periodically indicating how much of the message it has received and reconstructed. The sending computer must keep a copy of the parts of the original messages that have been sent until the destination computer acknowledges. I have told earlier that the acknowledgment comes in periodically, but how is this set? The amount of data that the source computer sends before waiting for acknowledgment is called the window size. If the window size is too small, overall data transmission is slowed as it frequently waits for acknowledgment. Similarly, if it's too big also, it can overload routers. Thus, there should be a balance, and it's based on the network to network basis.

Application Layer

As the below layers have made it possible to quickly & reliably transfer data between computers, the next question is what kind of applications will be built to make use of these shared networks.

Initially, it was used for remote login, remote file sharing, mail, and real time chats. Then with WWW applications were able to work with images.

Any network application can be broken into two halves, Server and Client. The web browser running on your computer is a client while the document you access is from the Server which is retrieved by URLs - Uniform Resource Locators.

While we are developing the Server & Client of our network application, we must also define an application protocol that explains how the application will exchange messages over the network.
Each application protocol is dedicated to a port through which it communicates to the transport layer.

Stacking the Layers

All 4 layers run on the source computer & destination computer. The routers have no understanding of either the Transport or Application layer. The Transport & application layer only comes into play after the Internetwork layer delivers your packets to the destination computer.
A relatively good resource I have found: https://www.youtube.com/watch?v=3b_TAYtzuho

Going down the stack is encapsulating & going up the stack we call decapsulation.
Protocol Data Unit

When the application has data to send, it hands the data to the Transport layer, which has the job of delivering the data reliably to the other end. The Transport Layer sends data to the other end by handing it to the Network Layer, which has the job of breaking the data into packets, each with the correct destination address. Finally, the packets are handed to the Link Layer, which delivers the packet from one hop to the next along its path. The data makes its way, hop by hop, from one router to the next. The Network Layer forwards it to the next router, one at a time, until it reaches the destination. There, the data is passed up the layers, until it reaches the Application.

Chapter 3 - Link Layer

Transmits data using a wire, a fibre optic, or a radio signal. Regardless of the distance it is still traveling over a single link and uses packet forwarding across multiple links.

In case of a smartphone connected to a router, the first router that handles your devices packets are called gateway or base station. All devices connected inside the same network can hear all the packets sent by every other device on the network. Thus, we have to secure, which we will learn later.

Each and every radio device during the time of manufacturing has a unique serial number associated with it. Even the Wi-Fi Router’s radio chip will also have a serial number associated with it. This unique serial number is called the MAC Address

Media Access Control or MAC is a 48-bit Serial number - A MAC address is like a from or to address on a postcard. Every Packet has a source and a destination. When your computer needs to connect to the internet, it will look for a gateway by broadcasting the following message on all channels. This will happen only if the computer knows that it is not a gateway itself.

From: 0f:2a:b3:1f:b3:1a (PC)
To: ff:ff:ff:ff:ff:ff
Data: Who is the MAC-Gateway for this network?

If there is a gateway on the network, the gateway sends a message containing its serial number back to your computer.
From: 98:2f:4e:78:c1:b4
To: 0f:2a:b3:1f:b3:1a
Data: I am the gateway Welcome to my network

Once your computer receives a message with the MAC address of the gateway it sends packets that it wants the gateway to forward to the internet

When two people start talking at the same time, they are good at noticing that another person is talking and quickly stop talking. But the problem is how to restart the conversation. After a long pause, it is common that both people start talking at the exact same time again. When the WIFI radios detect a collision or garbled transmission, they compute a random amount of time to wait
before retrying the transmission

CSMA/CD- Carrier Sense Multiple Access with Collision Detection.
How does CSMA/CD Work?

1. When a computer wants to sense the data, it listens to see if another computer is already sending data - (Carrier Sense)
2. As your computer is sending data, it listens and sees if it can receive its own data, and if it gets, it continues sending (Collision Detection)

The above case is a simple example, but when the link-layer has many transmitting stations and has to operate 100% reliable/efficiently, the concept of Token is used. Instead of listening to “silence” and jumping in, each must wait their turn.

A group of people sitting around a meeting could communicate without ever interrupting each other by having a small ball that they pass around in a circle and only allowing the person who has the ball to speak. When you get the ball and have something to say you talk for a short period (transmit a packet of words) and then pass the ball on.

But the disadvantage of the token method is that if you are the only station of a dozen stations that are sending data you will need to wait quite some time before.

It all depends on the application - The token approach is best suited when using a link medium like satellite or undersea fiber-optic link where it might take too long/costly to detect collision. WiFi can use the normal CSMA/CD approach

Chapter 4 - Internetworking Layer

Now that we can move data across a single link, it’s time to figure out how to move it across the country or around the world. Some links may be fiber optic, others might be a satellite, and still, others might be wireless. The router's job is to make sure packets move through the router and end up on the correct outbound link layer. A typical packet passes through from five to 20 routers to reach destinations around the world.
The router is able to quickly determine the outbound link for your packet because every single packet is marked with its ultimate destination address. This is called the Internet Protocol Address, or IP Address for short.

IP Address
With portable computers and cell phones moving constantly, we cannot use link-layer addresses to route packets, because there is no correlation between the link-layer address (MAC) and the location of the destination.

IPv4- 212.78.1.25 - 32 bit
IPv6- 2001:0db8:85a3:0042:1000:8a2e:0370:7334 -128 bit

Network Number: 212.78
Host Identifier: 1.25

An entire college campus, school, or business could connect using a single network number, or only a few network numbers. In the example above, 65,536 computers could be connected to the network using the network number of “212.78”.

By using this approach of a network number and a host identifier, routers no longer have to keep track of billions of individual computers. Instead, they need to keep track of perhaps a million or less different network numbers.

In the simplest case, a new core router can be connected to the internet and slowly build a map of network numbers to outbound links so it can properly route packets based on the IP address for each incoming packet. We call this mapping of network numbers to outbound links the “routing table” for a particular router. Thus, it does not need to rediscover the route for the network number unless something changes or goes wrong. This means that the router does a lookup on the first packet, but then it could route the next billion packets to that network number just by using the information it already has in its routing tables.

If some broken links or errors come, the router solves this problem by going through the route discovery process again from scratch. Packets are routed more slowly for a while as routing tables are rebuilt that reflect the new network configuration
This is called Dynamic Routing

The router always compares its routing tables with other neighbours even when no data is being sent, and it improves its routing table.

Just imagine a condition where a set of routers form a closed loop, also known as Routing Vortex. This infinite packet vortex is dangerous as routers would fill up with packets waiting to be sent and all three routers will crash.

To solve this problem, the Internet Protocol designers added a number to each packet that is called the Time to Live (TTL). This number starts out with a value of about 30. Since the packet keeps getting forwarded around the loop, eventually the TTL reaches zero. And when the TTL reaches zero, the router assumes that something is wrong and throws the packet away. This approach ensures that routing loops do not bring whole areas of the network down.

The ability of computers to get different IP addresses when it changes network is called Dynamic Host Configuration Protocol (DHCP).

The devices that are connected to the router use the same Network Number Prefix, but it violates the basic concepts, right? Not necessarily. It uses something called Network Address Translation.

Multiple Networks can reuse the same Private IP Address Space. It is done by Router. It maps the Reused Private IP address and modifies it to a global single IP address. Maps between Private & Public IP addresses.

Reserved Private IP
192.168.x.x
10.x.x.x

The NAT will replace the Private IP with its own global IP, and when it receives a response it again converts and brings back the value.

Chapter 5 - The Domain Name System

The Domain Name System lets you access websites by their domain name like (makerdemy.com), so you don't have to keep a list of numeric Internet Protocol (IP) addresses like "212.78.1.25". This Global IP address is determined by the location.

The individual owners of those domains are allowed to manage their domain and create subdomains under it for their own use or use by others.

Domain Names vs IP Address
212.78.1.25 - The more specific part comes at the right end
makerdemy1.teachables.com- The more specific comes at the left end

Chapter 6 - Transport Layer

A key element of the Internetworking layer is that it does not attempt to guarantee delivery of any particular packet. The Internetworking layer is nearly perfect, but sometimes packets can be lost or misrouted.

A packet will have-

| Link header | IP header | TCP header | Data Packet |

Link header - From & To
IP header - From, To & Time To Live
TCP header - Port & Offset

As the destination computer receives the packets, it looks at the offset position from the beginning of the message so it can put the packet into the proper place in the reassembled message.

One of the Transport layer's key elements is that the sending computer must hold on to all of the data it is sending until the data has been acknowledged. Once the receiving computer acknowledges the data, the sending computer can discard the sent data.

A computer can run several types of web applications at the same time. For instance, a web client (a browser) needs to connect to the remote computer's web server. A client application needs to know which remote computer to connect to, but it also needs to choose a particular application to interact with on that remote computer.

We use a concept called “ports” to allow a client application to choose which server application it wants to interact with. **Ports are like telephone extensions**. All of the extensions have the same phone number (IP Address) but each extension (server application) has a different extension number (port number).

Default ports for various server applications:
- Telnet (23) - Login
- SSH (22) - Secure Login
- HTTP (80) - World Wide Web
- HTTPS (443) - Secure Web
- SMTP (25) - Incoming Mail
- IMAP (143/220/993) - Mail Retrieval
- POP (109/110) - Mail Retrieval
- DNS (53) - Domain Name Resolution
- FTP (21) - File Transfer

Chapter 7 - Application Layer

Client-Server Model.
The server portion of the application runs somewhere on the Internet and has the information that users want to view or interact with. The client portion of the application makes connections to the server application, retrieves information, and shows it to the user. These applications use the Transport layer on each of their computers to exchange data.

Just like people talking on telephones, each pair of network applications needs a set of rules that govern the conversation. When your phone rings and you pick up the phone you say “Hello”. Normally the person who made the call is silent until the person who picked up the phone says “Hello”.

Chapter – 8 Secure Transport Layer

Encryption & Decryption is needed.
Two kinds of secrets: -
Shared Keys vs Asymmetric Key
Shared Keys - One Private key
Asymmetric Key - Public & Private Key

Secure Transport Layer/Secure Sockets Layer/Transport Layer Security is an optional partial layer between Transport Layer & Application Layer.

There is a small overhead in setting up the https connections and a small cost to encrypt and decrypt the data that is being sent. Since https was slightly more costly, for a while it was used only for pages that contained passwords, bank account numbers, or other sensitive data.
But over time as networks have become faster and the https implementations have gotten much more efficient, there is a trend toward encrypting all web server interactions whenever you are interacting with a web server where you have an account. The current trend is towards using https for all web traffic.

There is still a problem of knowing if the public key that you received when you connected to a server is really from the organization it claims to be from.

For example, a rogue computer can phis the banking details. So, your computer needs to know who the key is actually coming from. This is achieved by sending you a public key that is digitally signed by a Certificate Authority (CA). When your computer or browser is initially installed, it knows about a number of well-known certificate authorities.

Chapter 9 - OSI Model

The other model commonly used to make sense of network design is called the **Open System Interconnection** (OSI) model. While the TCP/IP model was designed and evolved as the TCP/IP protocols were developed, deployed, and changed, the OSI model was the result of a careful design process by many networking experts who worked to develop a general approach to network models.

In today’s networked world, the OSI model and the TCP/IP model serve two different purposes.

1. The TCP/IP model is an implementation model; in that it guides those who would build TCP/IP-compatible network hardware or software.
2. The OSI model is more of an abstract model that can be used to understand a wide range of network architectures

THE END