Network and Cybersecurity

Kristoffer Klokker

2022

Contents

1 Computer networks

A system connected to the internet is called a **host / end system**. This is done thorugh a **communication link** and **packet switch**. By this it has a **transmission rate** which describe the speed measured in bits/second.
When data is send it is done through **packets** which consist of a data header and including data. A packet is send first to the packet switch often taking form of a router or link-layer-switch. Which then sends it further to the communication link.
ISP then interconnect the communication links and connects to a higher up ISP or between higher up IPS. The highest tier is tier 1 of which other ISP connect with, even multiple such a **multi-home** setup is done in case of failure. An ISP may alos connect to a **PoP** which simply are a group of routers from another ISP.
ISPS may also peer between eachother to reduce exhange with higher tier ISP and reduce cost. Most often are peering free and third party companies may even create a IXP where multiple ISP can connect and peer to each other.
Big companies like Google also has their own private network infrastructure, which spans the globe between their datacenters. They are therefore peering between same tier ISPs and are also connected to 1 tier ISP but with reduced exhange.
Edge network refers to the connections to all the end host.

1.1 Different types of connections

Home access can be done in different ways:

- DSL - Digital subscriber line is done through a telephone lines in higher frequencies such phone and network can coincide. Current max limit of downstream is 1 Gbps, but the whole system require small distance to the telco provider 8 - 16 km.

- Cable internet access - Internet done through the existing television coax cable or hybrid fiber coax (HFC), a modem is then used to translate the analog signal to digital signal. This allows up to 1.2 Gbps downstream.

- FTTH - Fiber to the home is a direct connection from the cable office to the home. Here are two types active optical network (AON) and passive optical network (PON), PON works such a netowk teminator at the home goes through a splitter between up to 100 homes into the terminator at the telco.

- 5G fixed wireless - This is a wireless solution which are beginning to gather popularity in cities.

At the home a Local Access Network is then created, and most often extended to a Wireless Local Access Network using a router usin the WiFi protocol.

1.2 Mediums of signals

When a signal is sent through a physical media it is called guided media whereas over a wireless media it is called unguided.
Example of mediums are:

- Twisted cobber wire - used for telephone connections an still in use, for ethernet and more. A communication link done with this is called unshielded twisted pair (UTP). Modern cables of category 6a can transfer up to 10 Gbps over hundreds of meters.

- Coaxial cable - much like the twisted cobber cable, but the two copper condctors work concentric rather than parallel.

- Fiber Optics - Works by sending light insted of electricity, can have speeds in up to hundreds of Gbps over distances up to 100km due to no electromagnetic interference.

- Terrestrial Radio Channels - radio signals which characteristics depend a lot on enviremental factors. Can be found in three categories, short distance up to 2 meters, medium distance up to a few hundred meters and long distance spanning tens of kilometers.

- Satellite Radio Channels - Works as a transmitter receiver between two points on earth. Either in a geostationary orbit or low-earth orbit. geostationary eliminate the need of always finding the optimal satelite but at consequence of 280 ms delay.

1.3 Packet switching

Most packet switches use **store-and-forward transmission**, such before forwarding a transmittion all packages has to be obtained and proccessed before transmissioning.
This therefore extend the tranmission time according to package number and

speed.
When the router has processed all packages they can be send as one unit. This therefore can be described with:

$$d_{end-to-end} = N\frac{L}{R}$$

Where N is number of links, L is number of bits in a package and R is the speed.

In case of a package is alreadyu being sent the new package is sent to the **output buffer**, and in case of a full buffer **packet loss** will occur.
A packet switch most often have multiple queues for different forwarding packages. The packages are placed based on a forwarding map, using the packages IP addres.

1.4 Circuit switching

A circuit switch networks works on reservations. Instead if queues, a reservation is made to the receiver in both bandwith and that a port is open for the package.
This also has the advantage that the number of links can be ignored, in transmission time.
In this way a package can be guranteed to come at a specific time and no lost of any package.
To route more connections either **frequency-division multiplexing** or **time-division multiplexing** can be used.
FDM splits the avaliable frequecies into smaller bandwith of which data can be sent through.
TDM splits up the full bandwith into frames which are reserved with a number a number of slots for data. Therefore the speed is dependent on frame rate multipled by number of bits in a slot.
The downside of circuit switching compared to package switching, is the need for allocated sapce for every user, even in inactivity whereas package switching can work with changing demand.

1.5 Delay

There are different kind og delays the most important are:

- Nodal processing delay - delays in the router such as determine package header or bit error correction (μs)

- Queuing delay - delays in case of heavy traffic and non empty buffers (μs - ms)
- Transmission delay - delays that occur when waiting for a whole package and transmission rate is low (μs - ms)
- Propagation delay - delays from the actual bit transportation limit by medium (ms)

These in total are the total nodal dealy.

1.6 Protocols

A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.

Protocols are therefore used everywhere, such everything works as expected in between the layers of the network.
When different layers of protocols work together it is called a protocol stack, this may be for the internet:

- Application - These are protocols which are sent pr apllication such as HTTP, SMTP, DNS and such, refered as message
- Transport - These protocols are for sending application messages, here TCP and UDP, refered as segment
- Network - Protocols for distributing the segments using IP protocols or other routing protocols therefore refered as IP layer
- Link - Protocols here are used for the IP layer to transmit to until reaching the physical layer, this is protocols such as Ethernet and WiFi, refered as frames
- Physical - Protocols for transmitting frames, here protocols depend on medium such as for fiber

When data goes through each layer, a new header is added and previus layer data is used as payload.

1.7 Network attacks

Some of the different kind of internet attacks include:
Denial of service attacks (DoS) which prevent access to network host or infrastructure.
It can work by 3 ways:

- Vulnerability attack - Few messages which use a exploit such the host either stops or crashes
- Bandwith flooding - A large amount of packages is sent to the host resulting in overfilled buffers
- Connection flooding - A large number of open TCP connections are made such every entry is occupied

For flooding attacks they may also be a distributed Dos (DDoS) attack thorugh multiple devices often in a botnet.

A packet sniffer is a type of passive attack of which a device will listen for packages and possibly find sensitive information in packages sent through it.
IP Spoofing is a package which source address is spoofed, and therefore faked to look as a different source.

2 Protocol layers

For an application communicates to network layer, a socket is setup, which indentifies by a port. An app-layer protocol defines

- Messages exchanges - requst, resonse,...
- Message syntax - what fields are in a message
- Message sematics - Meaning of fields
- Rules for send and reponds

Transport service requirements - The different requirements an application may set for the transport of data
The different types of requirements an application may set

- Data loss - May be strictly no loss or just some percentage
- Throughput - May need a constant throughput or can be elastic

- Time sensitive - May need a minimum latency for data
- Security - Some data may be more sensitive than other

2.1 Client server architecture

The server side is on a always on host, with permanent ip, which handles backend stuff.
Ex. are hosting api and database.
The client in this architecture communicates via HTTP protocols are some alike.
The clients are the dynamic part, may not be on same ip, or connect with each other

2.2 P2P

No host involved but clients communicating directly between each other.
Are scaled based on number of users.

2.3 TCP Service

Reliable transport with flow control to not overwhelm receiver
Able to throttle sender in an overloaded network.
Does not provide: timing, min. througput guarantee or security
Need a setup between client and server established before use.

2.4 UDP

Unreliable data transfer.
Does not provide: reliability, flow control, congestion control, timing, throughput guarantee, security
Smarter for data which can handler larger loss.
TCP may get stuck on a packet whereas UDP would simply skip the package and go forward for the next package.

2.5 Domain name system

DNS binds name/string to an ip address.
This also includes alias names for mail server or sub domains.

Usefull for more dynamic ip setup and readability
Implemented via a distributed database.
The databases stores resource records (RR) in the format (name,value,type,ttl)
The DNS is implemented in a tree structure.
First are the root DNS which contains addresses of top level domain severs like .com, .org, .dk
They then contain then the DNS servers for domain such as google.com, which itself contains addresses for subdomain.
So when a request is made first, the cache is checked, then a request to a preinstalled root such as 1.1.1.1 is made.
This then returns a top level address for a DNS server, which a request is made to.
This is repeated until an ip matching the request is returned.
This is the itterative method.
The recursive query find the ip via the DNS servers which contacts eachother putting the burden on them
Local DNS servers does not belong to hierarchy but is hosted by an ISP.
TTL (time-to-live) is a numerical value representing the amount of server hops a packet can make before being outdated.
The local DNS handles the requesting and caching for an IP to the hiarachy DNS servers.

2.5.1 Types of resource records

To do a lookup the dig tool can be used

- Type=A - name: hostname, value: ip-address
- Type=NS - name: domain, value: nameserver
- Type=CNAME - name: alias, value: hostname
- Type=MX: name: '@', value: mail server

2.5.2 DNS protocol

Query and reply are in the form Message, header
The header consist 12 bytes dedicated to

- 16 bit identificaiton
- 16 bit flags
  - Query (0) or reply (1)

  - 4 bit opcode: standard query (0), domain name form ip (1), status request of server (2), (3) is reserved for status an not used
  - AA: The server is authoritative (1), non authoritative/cache (2)
  - TC: the message exceeds 512 bytes and are truncated (1)
  - RD: Recursion desired (1)
  - RA: Recursion avaliable from server (1)
  - Zero: 3 bits of zeros reserved
  - rCode: Respnse code, no error (0), format error (1), server failure (2), did not find name (3), request is supported (4), policy denies execution of query (5)

- 16 bit Number of questions in body
- 16 bit Number of answers RRs and is 0 from client and set by server
- 16 bit Number of authority RRs and is likewise 0 from client
- 16 bit Number of additional RRs

The body then cosist of

- Questions - query from client
- Answers RRs- Response to query from non authority
- Authority RRs - Response to query from authority
- Additional information

2.5.3 Security

A person could bombard the DNS servers with traffic and deny other trafffic in form of DDoS.
Not successful to date on root server but TLD (top-level domain) has successed
NXDOMAIN attack is requesting non existing domains and spending the DNS server ressources to find non valid addresses.
Random subdomain attack are like NXDOMAIN attack but with subdomains to target the namespace rather than root or TLD.
Phantom domain attack is setting up DNS servers which does not respond or very slow responses, such in a recursive lookup the TLD will have to wait for response.

TCP SYN is the attack of which a bunch of TCP request are opened but never used.
DNS domains lock-up is an extended TCP SYN attack where after a connection is established random packages is sent to the server, and the server will wait for a correct response.
DNS rebinding attack is used to get past browsers same-origin policy, this is done by first the user lands on a shady website, the website then make a request to itself, but the dns record is updated to point at a new site which the script now can be run upon.
DNS cache poisoning is where an attacker imposes as a nameserver, and then creates a request for the nameserver and answers before the real nameserver and thereby creating a fake lookup in the cache.

3 Web and HTTP

3.1 HTTP

A HTTP request is sent by the client, and server sends using HTTP protocol an object in response
The request is sent at port 80 using a TCP request.
Non-persistent HTTP sendt a single object and then closes
Persisten HTTP can send multiple files between client and server
Repsonse time RTT is the time for a small packet to travel from client to server and back.
Persistent has longer open connection but every referenced object can be sent at as little as one RTT
Non-persisten requires 2 RTT atleast pr referenced object, and looses alot of time to OS overhead for each established connection.

The general request consist of: method, url, protocol, headers
The general response consit of: protocol, status code, status phrase, headers, data
There is 4 method types for HTTP/1.1

- GET - get ressource
- POST - send ressource
- HEAD - meta data to check for updates
- PUT - Uploads file in entity body to url field

- DELETE - delete file in the url field

The most common response status codes

- 200 OK
- 301 Moved Permanently - object is moved to new location given in message
- 400 Bad Request - not understood by server
- 404 Not Found - Fil not found on server
- 505 HTTP version not supported
- 418 I'm a teapot - When a teapot is requested to bre coffee

3.2 Cookies

Cookies are the solution for http being stateless.
Cookies allows to store files in the browser of the user.
This can be used for saved storage like shopping cart or authority like a session cookie.

3.3 HTTP/2.0

Problem in 1.0 was request was treated in order, 1.1 made it a little better using pielining which allowed for multiple sequential request.
2.0 introduced streams, where request are numbered in odds and responses are given in even numbers.

3.4 Electronic mail

Electronic mail consist of 3 major components: User agents, Mail servers and Simple mail transfer protocol (SMTP)
User agents are essentially mail clients which allows for creation and reading of emails.
Mail servers have a mailbox for incomming messages and a message queue for outgoing mails
SMTP uses TCP on port 25 to transfer emails.
The protocol work on command response, where command are in ASCII 7

bit and reponse are status codes.
The mail message consist of header (To, from, subject), blank line and body (Only ASCII)
The user agents access the mail server via the IMAP protocol or HTTP

3.5 Video streaming and content delivery networks

To reduce the amount of data, coding is used on the data, spatial (groups pixels together) and temporal (only send difference of video frames)
CBR - constant bit rate
VBR - variable bit rate
DASH - Dynamic, Adaptive Streaming over HTTP
DASH divides video files into chunks, with each having different rates.
All chunks are managed in the manifest file which provides URL to each chunk.
The client then handles, when to get chunks, at what encoding rate and which server to request chunks.
CDN networks work by distributing the content to multiple servers around the globe.
To find the best server in a CDN preiod tests are made in the network of which speeds are in between each server.

3.6 P2P

No need for an always on server
End systems directly communicate.
Is more scaleable than a server setup.
For n clients on a server the sever time will be $D_{Client-Server} > max(NF/u_s, F/d_{min})$, it will therefore scale linearly.
Whereas in P2P the time will be $D_{P2P} > max(F/u_s, F/d_{min}, NF/(U_s + \sum u_i))$
Where U_s is the central server speed, u_i is user upload speed, d_i user download speed and F is filesize.
A torrent is a group of peers exchaning files divided into chunks of 256Kb.
The peers are then managed in a tracker, which also participate in the torrent.
A torrent client then uses those peers, request which chunks they have and missing chunks are downloaded from fastest connection.