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.

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.