01. Computers Networks and the Internet

1.1 What is the Internet?

The internet consists of millions of machines that are connected through various communication links and packet switches. Links transmit data over the wire at a speed of some bits per second. Packet switches are network switches that accept and forward packets to a different destination. End systems and applications communicate over the network using a set of protocols. These programs communicate over the network using network sockets.

1.2 The Network Edge

The network edge denotes hosts or systems at the end of the network, the machines that we interact with. These hosts are typically PCs, mobile phones, and servers. Hosts connect to the network using different methods. When stationary, you will typically connect to WiFi or Ethernet, whilst on the move, you might use DSL (digital subscribe line) to access LTE, 3G, or 4G network. These are used when on the move, as they have larger ranges than WiFi. It is also possible to access networks over satellite.

1.3 The Network Core

The network core denotes the mesh of packet switches and links that connect the end systems. When a packet travels across the network it uses packet switching, a routing system which means the packet travels through multiple links, finding the most effective route. This means that multiple packets from the same program do not necessarily travel the exact same route.

The packet travels at the full transmission rate of the link. A link with the transmission rate R will take $\frac{L}{R}$ seconds to transmit a packet of size L. Store-and-forward transmission means that a packet switch must receive the entire package before forwarding the packet to the outbound link. This results in an $(N-1)\frac{L}{R}$ transmission delay for N links.

Once a packet arrives at a router, it uses a forwarding table that maps destination addresses to that router’s outbound links. To find the right outbound link, one simply looks up in this table.

Circuit switching is the other fundamental approach to transmitting packets across a network. Circuit switching differs in the way that you reserve the entire line for the transmission. This has the benefit that the connection is kept and the sender is guaranteed a constant transmission rate, but it also occupies the line and can easily waste bandwidth.

1.4 Delay, Loss, and Throughput in Packet-Switched Networks

There are multiple types of delay we face when transmitting packets over a packet-switched network. Among these are node processing delay, queuing delay, transmission delay and propagation delay.

Processing delay is the time required to decode the packet’s header and determine where to redirect the packet. Processing delays on modern routers are typically in the order of microseconds. After this processing is done, the router redirects the packet into the queue that precedes the link to the target destination.

Queuing delay is time the packet spends waiting in queue to be transmitted onto the link. If the queue is empty, the queuing delay is zero. If there is heavy traffic, we might expect delays between microseconds and milliseconds. Traffic intensity is the relation of a packets where $\frac{La}{R} > 1$. At this point, the delay can become gigantic due to the loads of packets ending up in queue. It is therefore a goal to design routers that keep traffic intensity below 1.

Transmission delay is the same as described in section (1.3). $\frac{L}{R}$

Propagation delay is time required to propogate from the beginnin`g of the link to the destination. It is the time it takes for the packet to travel from one node to another, denotes in distance in meters d over propagation speed of the line s, $\frac{d}{s}$

That means that the total end-to-end delay is determine by:

$$d_{end-to-end} = N(d_{process} + d_{transmission} + d_{queuing} + d_{propagation})$$

1.5 Protocol Layers and Their Service Models

The internet protocol (IP) is split up into five protocols, each at different layers. Each layer has a set of protocols which are used to work on said level. There also exist other protocol stacks such as the OSI model.

Layer name	Description	Example protocols	Unit
Application	Top-level protcols working with software	HTTP, SFTP, DNS	message
Transport	Responsible for end-to-end communication	TCP, UDP	segment
Network	Responsible for determining where a packet is supposed to go	IP	datagram
Link	Responsible for determining how the packet is moved onto the phyical layer	Ethernet	frame
Physical	Responsible for actually transmitting over the wire	Satelitte, Fiber, Twisted-pair cable	bit

1.6 Networks Under Attack

Because the Internet has become mission critical today, there is also need to protect services through cybersecurity. We typically face a few common types of attack vectors:

- Malware: software with the intention to do harm on one’s computer
- Botnet: thousands of comprimised machines used to leverage spam or denial-of-service
- Viruses: seemingly innocent programs that actually contain malware
- Worms: malware that enters a computer without explicit user interaction

It’s also possible for attackers to sniff packets that travel across the network. That’s why it’s important for websites to communicate over HTTPS which encrypts all data traveling across the wire. Wireshark is a program that can be used to sniff packets.

Attackers may also act as a trusted actor through spoofing IP-addresses or email addresses.

1.7 History of Computer Networking and the Internet

This chapter is less relevant to the course. The following is a tiny timeline of important events in the evolution of the Internet.

- 1972-1980: Internetworking: new and proprietary networks
- 1980-1990: New protocols such as TCP/IP, SMTP, DNS, FTP
- 1990, 2000s: Commercialization of the internet, the wide-world-web, instant messaging and social networks
- 2010+: Software as a service, streaming, cloud services