Chapter 01: Computer Networks and the Internet

Table of Contents

[1.1 What is the Internet? 2](#_Toc99598477)

[1.1.1 A Nuts-and-Bolts Description 3](#_Toc99598478)

[1.1.2 A Services Description 4](#_Toc99598479)

[1.1.3 What is a Protocol? 4](#_Toc99598480)

[1.2 The Network Edge 5](#_Toc99598481)

[1.2.1 Access Networks 5](#_Toc99598482)

[1.2.2 Physical Media 6](#_Toc99598483)

[1.3 The Network Core 7](#_Toc99598484)

[1.3.1 Packet Switching 7](#_Toc99598485)

[1.3.2 Circuit Switching 7](#_Toc99598486)

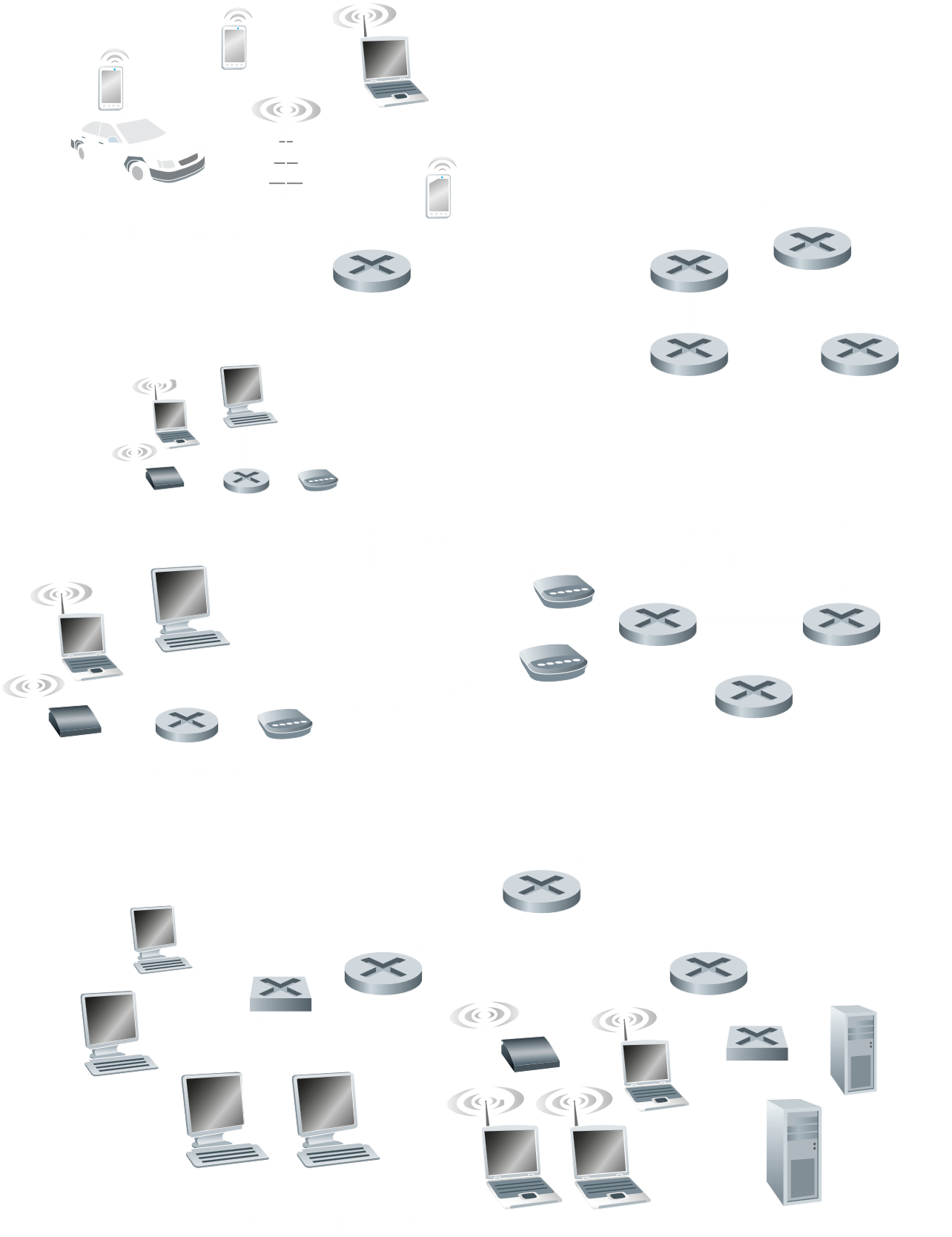
[1.4 Delay, Loss and Throughput in Packet-Switched Networks 9](#_Toc99598487)

[1.4.1 Overview of Delay in Packet-Switched Networks 9](#_Toc99598488)

[Throughput in Computer Networks 10](#_Toc99598489)

## What is the Internet?

The Internet can be described in two ways, in terms of the basic hardware and software components that make it up, or in terms of a networking infrastructure that provides services to distributed applications. We will be looking into both descriptions.



### A Nuts-and-Bolts Description

Firstly, in terms of the basic hardware and software components. The Internet is a computer network that interconnects millions of computing devices throughout the world. The devices being connected are called **hosts** or **end systems**. These hosts are connected via many different types of **communication links** and **packet switches**, which are responsible for transmitting **packets** of data. The packet switches are usually either **routers** or **link-layer switches**, with the former primarily used in the **network core** and the latter primarily used in **access networks**. The sequence of communication links and packet switches traversed by a packet from the sender to the receiver is called its **route** or **path**.

However, end-systems don’t just directly connect to the network core. They do so via an **Internet Service Provider** (ISP). An ISP is also a network of packet switches and communication links that provides access to a wide variety of networks, such as local cables to homes, corporate networks, university networks and networks in other public places. Since the Internet is all about connecting end-devices, the ISPs themselves are also connected. Low-tier ISPs to which end-devices are connected go on to connect with upper-tier ISPs like national or international ISPs, which also go on to connect to even higher tier ISPs and so on.

To regulate how all these networks send and receive information, certain protocols are used, such as the **Transmission Control Protocol** (TCP) and the **Internet Protocol** (IP). How these protocols work are defined by **Internet Standards** from the **Internet Engineering Task Force** (IETF).

### A Services Description

Now we will be looking at the Internet as an infrastructure that provides services to applications. Generally, we are running different applications and services on end devices. These applications need to communicate via the internet. However, to be able to successfully communicate, the data being sent out needs to follow a specific format, defined by an **Application Programming Interface** (API).

### What is a Protocol?

Consider a human analogy. When talking to another human being, we initiate the conversation by offering a greeting (‘Hello!’) to which the other person also responds with a greeting. This indicates to us that we can go ahead with the conversation. If instead we receive a negative response (‘Go Away!’), it is an indication that we should not continue the conversation. Critically, in order for things to work smoothly, we must both be on the same page about how our protocols work, e.g., we both understand English.

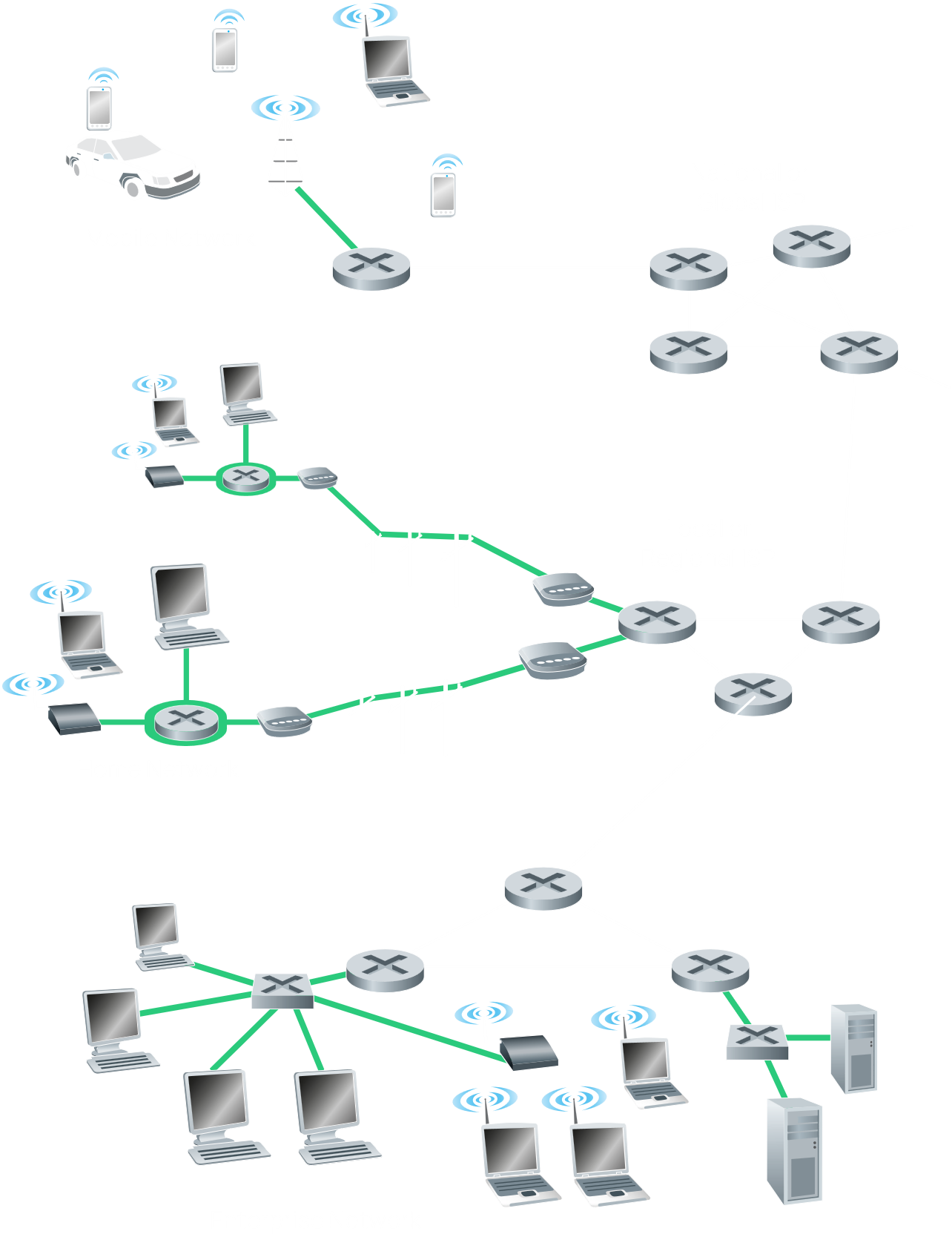
**Network Protocols** are the same. There is a connection request and a response. After this, there is a request for a document from the client, to which the server responds with the document requested.

## The Network Edge

Host devices are often called **end-systems** because they sit at the edge of the Internet. They are called **hosts** because they host applications. Note that hosts/end-systems can refer to either clients or servers.

### Access Networks

A group of end-systems connect to a single router, called the **edge router**, forms an **access network**. The edge router is what will connect this group to the rest of the internet.



Notice that an access network can be of many different types, such as:

* Traditional Home Networks like DSL, Cable and FTTH
* Enterprise Networks, which are also increasingly used as Home Networks, like LAN and Wi-Fi
* Mobile Networks, like 3G and LTE

### Physical Media

The communication links that transfer data can be of many different types, or **physical mediums**. These include:

* Twisted-Pair Copper Wire
* Coaxial Cable
* Multimode Fibre-Optic Cable
* Terrestrial Radio Spectrum
* Satellite Radio Spectrum

These media fall into two categories, **guided media** and **unguided media**, which basically refer to wired and wireless media respectively.

## The Network Core

### Packet Switching

When sending messages from one end system to another, the message is typically broken into smaller chunks of data called **packets**. In its route, the packet must pass through several packet switches. A packet switch must receive all the bits for a packet before it can begin retransmitting the packet, which means the received bits must be stored. This is called **store and forward transmission**.

### Circuit Switching

In Packet Switching, we saw that each packet of data is received by a packet switch and forwarded appropriately. In Circuit Switching, by contrast, the entire path from source to destination is reserved for the duration of the communication.

Circuit switching employs **multiplexing**, which can be of two types, Time Division Multiplexing (TDM) or Frequency Division Multiplexing (FDM).

At first sight, **Circuit Switching** may seem like the better choice. Afterall, it provides a dedicated path with a **constant data rate**. The same is not true for **Packet Switching**.

Consider a situation where we have several customers who need to be served by a single router. This router will send the data to another router using a link of . Each customer expects a constant data rate of . This is perfectly doable by dividing the link using TDM or FDM.

Sadly, circuit switching has a major limitation. For each customer, resources are **reserved**. This means that, for the above example, we can only serve a maximum of customers.

**Packet switching** on the other hand, will be able to serve as many customers as it needs to. However, the **speed** the customers get would begin to suffer. Given this limitation, why is it that packet switching is used worldwide?

In a real-life scenario, a single customer does not actually **constantly** need of speed. Suppose a customer uses the link for of the time. The other of the time, they are **inactive**. Under circuit switching, this wastes a huge amount of resources.

Given this information, let us consider the same example as above, with a link of , this time using packet switching. We can still support up to customers without any issues, exactly like circuit switching can. For more customers, speeds may begin to suffer. But what is the probability that we have more than customers?

Long story short, for customers, the probability is . For , this value is approximately . Thus, the probability that any customer will face speed issues is . Thus, packet switching can serve way more customers than circuit switching before there are any noticeable drops in speed.

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

### Overview of Delay in Packet-Switched Networks

Packets of data may face several types of delay at a router:

1. **Nodal Processing Delay** – This is the delay caused by administrative processing at the router when the packet first arrives. It includes the time taken to check for errors, process the header information, find the correct route in the routing table, modify the header information and place the packet in the correct queue. The Nodal Processing Delay depends on the routers processing power.
2. **Queuing Delay** – This is the delay as a packet waits for the output transmission medium to become empty. It depends on the traffic intensity. The queueing delay varies from packet to packet, unlike the other delays. If the queue is full, routers will drop incoming packets. This is known as **packet loss**. It is a sign of severe network congestion.
3. **Transmission Delay** – A single packet can be divided into bits. Some time will be required to push all bits of the packet into the link, i.e. for the entire packet to leave the router. This is the transmission delay. It depends on the packet size, which is standardized, and the transmission rate or bandwidth of the link.
4. **Propagation Delay** – This is the time required for one bit to physically get from one router to the next. This depends on the propagation speed of the medium. For example, fibre optic has a higher propagation speed than copper wire.

### Throughput in Computer Networks

Another critical performance measure is the **end-to-end throughput**. Consider that we are transferring a large file from one device to another. The **instantaneous throughput** at any time is the rate in bits/s at which the receiver is receiving the file. The **average throughput** is the average rate in the total time taken to receive the whole file.

The throughput of a link depends on its bandwidth as well as congestion delays.

If the path from the sender to the receiver contains multiple links, and one of the links has a lower bandwidth, then the throughput of the entire path will fall to match that bandwidth. This link is the **bottleneck link**.