Computer Networks (UE18CS301)

Unit 1

Aronya Baksy

August 2020

1 Introduction

Definition 1. A **Computer Network** can be defined as ≥ 2 computing devices connected to each other capable of sharing information between them.

2 The Internet

The internet is a network of computer networks. It consists of traditional devices (PCs, Workstations, servers) and non-traditional IoT devices (TVs, gaming consoles, home security appliances, cars, smart speakers etc.) connected to each other via a well-defined communication protocol called TCP/IP.

2.1 The nuts-and-bolts description

The following components comprise the internet according to the nuts and bolts description:

1. **End Systems:**
   (a) These are also known as **Edge Systems** or **hosts**.
   (b) They run network applications at the end points/edges of the internet
   (c) eg: PCs, smartphones, Servers, IoT devices
2. **Packet Switches:**
   (a) Forward packets, ie. chunks of data from one point in the internet to the next
   (b) **Routers** are Level 3 communication devices, as they act on level 3, ie. the **network** layer of the TCP/IP model. They are used in the network core.
   (c) **Switches** are Level 2 communication devices, as they act on level 2, ie. the **data link** layer of the TCP/IP model. They are used in access networks.
3. **Communication Links:**
   (a) The hardware media needed to transfer data between end systems and the packet switches
   (b) These comprise of cables (copper/fiber optic), radio and satellite communication
4. **ISPs**
   (a) ISPs provide connections between end systems and the internet
   (b) An ISP in itself is a network of packet switches and communication links.
5. **Protocols:**
   (a) A protocol can be defined as a set of rules or standards used to define the methods and formats for sending/receiving of messages.
   (b) The 2 most common protocols in use as part of the internet are **TCP** (Transmission Control Protocol) and **IP** (Internet Protocol)
   (c) The IP protocol specifies the format of the packets that are sent and received among routers and end systems.

(d) Other protocols in use by the internet are FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol), UDP (User Datagram Protocol)

6. **Internet Standards:**

   (a) These are the definitions for the protocols that define the functioning of the internet.

   (b) They are defined in the form of documents called **RFCs** (Request for Comments) that are sent out by the **IETF** (Internet Engineering Task Force)

   (c) The IETF is responsible for defining protocols such as TCP, IP, SMTP, HTTP etc.

   (d) Other bodies such as the **IEEE** (International association for Electrical and Electronics Engineers) define standards for communication protocols like WiFi and Ethernet (IEEE 802)

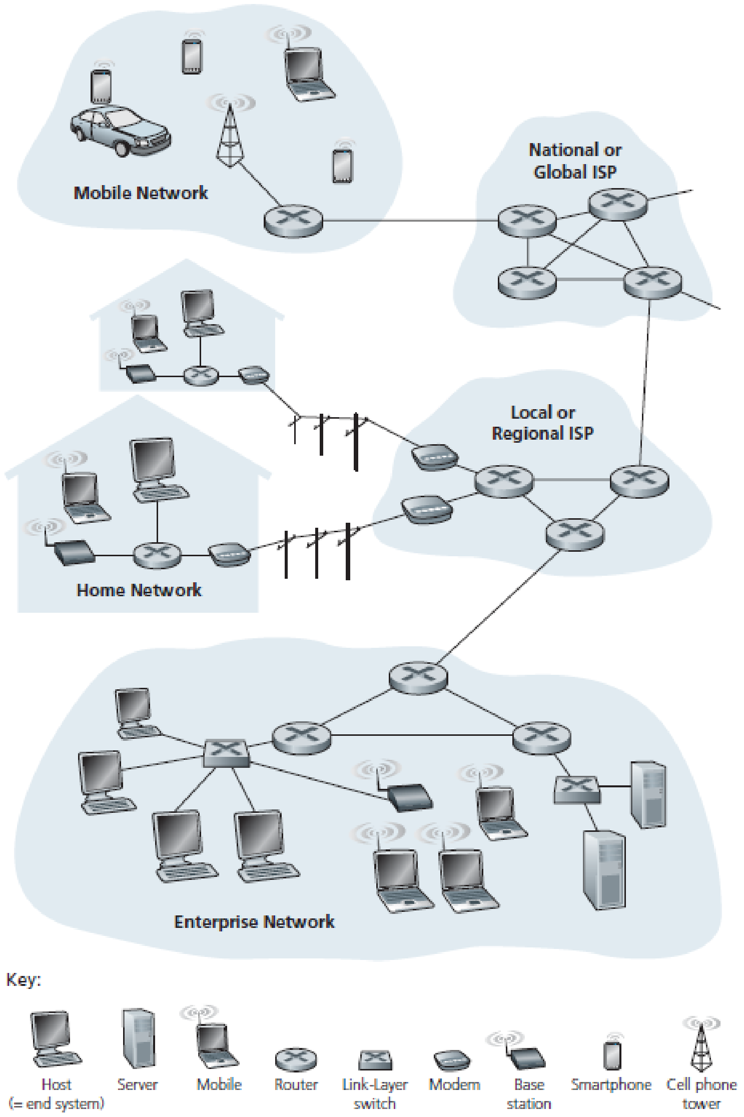


Figure 1: A schematic computer network

2.2 The services description

- The internet may also be viewed from the application programmer's point of view as a service, that offers methods to transmit user data from one end system to another.

- The end systems offer **APIs** (Application Programming Interfaces) as **Hooks** into the internet ecosystem. The application developer can use these hooks to plug their application into the internet, and use the internet to transfer data.
- The internet API is a standard that specifies how a program running on one end system asks the Internet infrastructure to deliver data to a specific destination program running on another end system.
- The internet, in this point of view, can be considered to be analogous to a postal system, where the sender of the letter (the programmer) can use the post office (the API) as a **hook** into the postal service that transfers the letter to the final receiver.

3 Protocols

Definition 2. A protocol defines the format and order of messages sent and received between two or more communicating entities, as well as the action to be taken on the transmission and/or the receipt of messages or any other event.

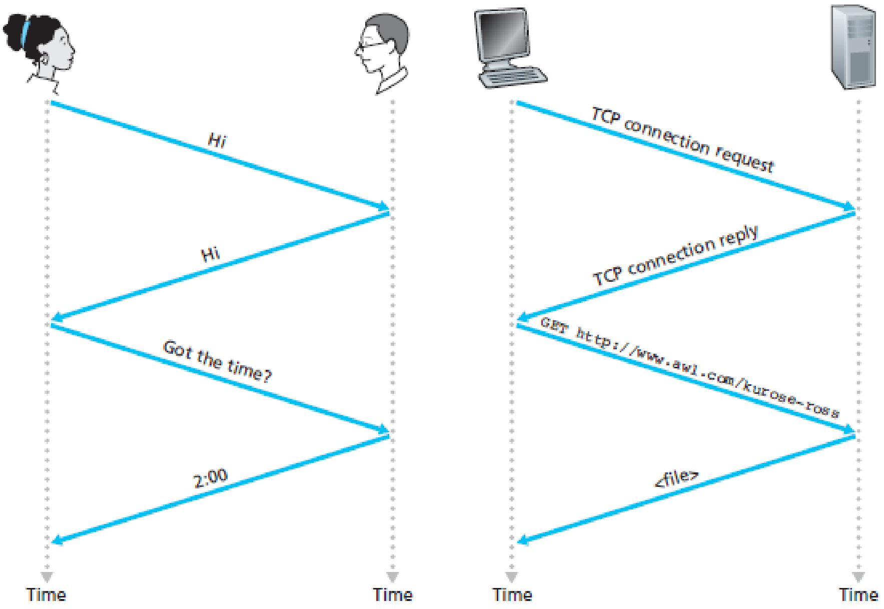


Figure 2: Human communication protocol and HTTP Protocol

Some of the protocols are listed below along with the layers of the 7-layer OSI Reference Model in which they function.

1. **Application Layer:** DNS, WWW/HTTP, P2P, email/POP, SMTP, FTP, telnet
2. **Presentation Layer:** HTML, DOC, JPEG, AVI, Socket
3. **Session Layer:** Session establishment in TCP, SIP, UDP
4. **Transport Layer:** TCP, UDP, SSL, TLS, SCTP
5. **Network Layer:** IP, ARP, IPSec, ICMP, IGMP, OSFP
6. **Data Link Layer:** Ethernet, IEEE 802.11, MAC/LLC
7. **Physical Layer:** RJ45, RS-232

4 The Network Edge: client-server architecture

- The network edge is primarily comprised of end systems (see above for definition of an end system).
- End systems are also referred to as **hosts** as they are responsible for *hosting* the application software that communicates with the internet
- End systems (or hosts) may be further subdivided into **client** and **server** machines.
- Informally, a client machine is one that requests data that is stored on a server. Client machines are low performance machines like PCs, mobiles, tablets, and non-traditional IoT devices.
- A server, in comparison, is a more powerful machine that is capable of servicing multiple client requests and handling very complicated processing of queries, while storing large amounts of data.
- Servers today appear in large clusters called **data centers**. (`https://cloud.google.com/about/locations` gives a rough idea about the number of Google Data Centers)

4.1 Access Networks

Definition 3. An **access network** is a network that connects an edge system to the first router in the path from that end system to any other distant system, also called the *edge router*

4.1.1 Home Connection: DSL

- **DSL** (Digital Subscriber Line) is one of the most popular methods for homes to connect to the internet. This service is provided by telephone companies.
- Each customer's DSL Modem uses the same cable as the telephone line (twisted pair copper cable) to exchange data with a DSL Access Multiplexer (**DSLAM**)
- The DSL modem converts digital data (represented as 0/1) into high frequency tones that can be transferred over the telephone line. The residential telephone line carries both data and traditional telephone signals simultaneously, which are encoded at different frequencies:
  - A high-speed downstream (internet to home) channel (50kHz - 1MHz band)
  - A medium-speed upstream (home to internet) channel (4kHz - 50kHz band)
  - An ordinary two-way channel (0-4kHz)
- On the customer side, a splitter separates the data and telephone signals arriving to the home and forwards the data signal to the DSL modem.
- On the telephone operator's side, in the Central Office, the DSLAM separates the data and phone signals and sends the data into the Internet.

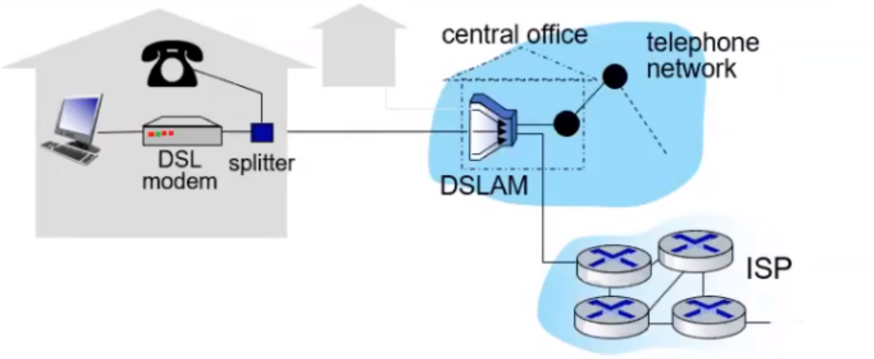


Figure 3: DSL Internet Access

4.1.2 Home Connection: Cable

- Cable internet shares IP data and cable television data over a common channel.
- Fiber optics connect the cable head end to neighborhood-level junctions, from which traditional coaxial cable is then used to reach individual houses and apartments.
- At the Cable head end, the CMTS (Cable Modem Termination System) serves the role of turning the analog signal sent from the cable modems in many downstream homes back into digital format.
- One important characteristic of cable Internet access is that it is a shared broadcast medium. In particular, every packet sent by the head end travels downstream on every link to every home and every packet sent by a home travels on the upstream channel to the head end.

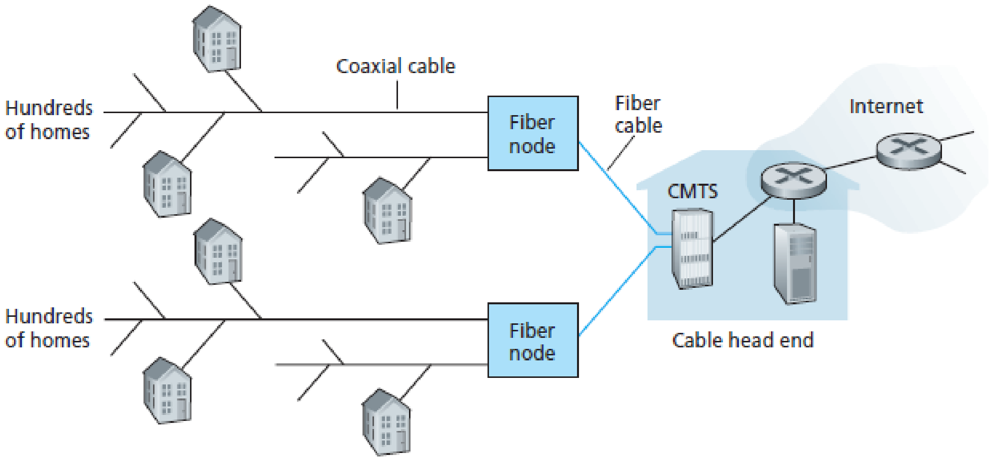


Figure 4: Cable Internet Access

- One common feature of Cable and DSL is the asymmetric access, where the download and upload speeds are different.
- For DSL, 24 Mbps downstream, 2.5 Mbps upstream
- For Cable, 42.8 Mbps downstream, 30.7 Mbps

4.1.3 Enterprise connection: Ethernet and WiFi

- In corporate/educational settings, LAN (Local Area Network) is used to connect the end systems to the edge routers.
- **Ethernet** users use twisted pair copper wire to connect to an Ethernet switch, which in turn connects to the larger internet.
- Ethernet offers users 100 Mbps access to the internet, while servers have 1-10 Gbps access.
- **WLAN (Wireless LAN)** is a method for wirelessly connecting mobile devices in an enterprise environment.
- A WLAN user must be within a few tens of meters from a WLAN access point. Wireless access is based on the IEEE 802.11 b/g/n/ac protocols, commonly called WiFi.
- WiFi offers transmission rates of 11, 54 or 450 Mbps.
- Outside the enterprise context, many homes combine broadband residential access (that is, cable modems or DSL) with these inexpensive wireless LAN technologies to create powerful home networks.

- This home network consists of a roaming laptop as well as a wired PC; a base station (the wireless access point), which communicates with the wireless PC; a cable modem, providing broadband access to the Internet; and a router, which interconnects the base station and the stationary PC with the cable modem.

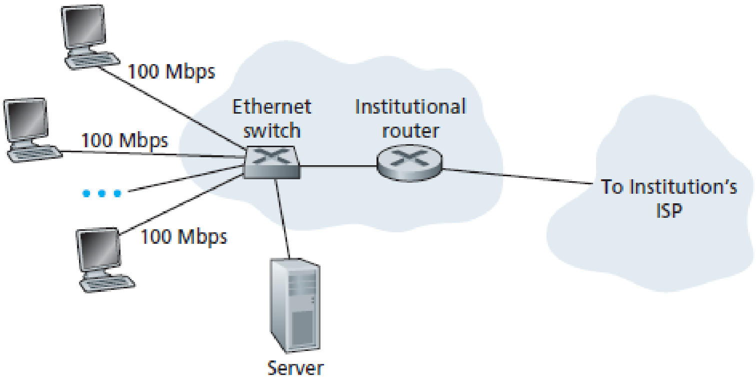


Figure 5: Ethernet Internet Access

5 Physical Communication Media

- For each transmitter-receiver pair, the bit is sent by propagating electromagnetic waves or optical pulses across a physical medium. The physical medium can take many shapes and forms and does not have to be of the same type for each transmitter-receiver pair along the path.
- Physical media fall into two categories: guided media and unguided media.
- With **guided media**, the waves are guided along a solid medium, such as a fiber-optic cable, a twisted-pair copper wire, or a coaxial cable.
- With **unguided media**, the waves propagate in the atmosphere and in outer space, such as in a wireless LAN or a digital satellite channel.

5.1 Twisted Pair Copper Wire

- Twisted pair consists of two insulated copper wires, each about 1 mm thick, arranged in a regular spiral pattern.
- The wires are twisted together to reduce the electrical interference from similar pairs close by.
- One pair constitutes one communication link. A number of pairs are typically bundled together in a protective shield (**Shielded Twister Pair** Cable)
- LANs use **Unshielded Twisted Pair (UTP)** cables, for intra building communication as an example. Shielded Twisted Pair cables are more expensive and have less attenuation rate.
- Cat 5: upto 100 Mbps, or 1 Gbps over an Ethernet connection
- Cat 6: upto 10 Gbps over Ethernet

5.2 Coaxial Cable

- Concentric (not parallel, as in the case of twisted pair) copper conductors.
- With special insulation, shielding and this construction, coaxial cables achieve high data transmission rates.

- They are used primarily in cable TV systems, and can be coupled with cable modems to provide residential internet access at tens of Mbps.
- The transmitter shifts the digital internet signal to a specific frequency band, which is sent to one or more receivers.
- Coaxial cables can also be used as a shared medium, with a number of end systems conneced to the same cable.

5.3 Fiber Optic Cable

- A thin flexible medium that conducts data via pulses of light, with each pulse representing one bit of information.
- A single fiber can support upto 100s of gigabits per second (Gbps).
- They are immune to electromagnetic interference, have very low signal attenuation upto 100km, and are almost impossible to tap.
- The high cost of fiber optic network devices (transmitters, receivers, switches) has meant reduced adoption for short haul networks like LAN or residential access networks.
- The OC-n (Optical Carrier) standards define the link speeds for certain standard fiber optic configurations; the link speed is calculated as $n \times 51.8$ Mbps. Standards in use today include OC-1, OC-3, OC-12, OC-24, OC-48, OC-96, OC-192 and OC-768.

5.4 Terrestrial Radio Channels

- Radio waves carry signals in the radio part of the electromagnetic spectrum.
- Radio communication does not need a physical medium to be installed, can penetrate walls, can provide connectivity to mobile users and can carry signals for large distances.
- Radio wave characteristics are significantly influenced by the environmental factors. These are parameterized by the **path loss** and **shadow fading** (reduce signal strength as the signal travels over or around objects), **multi-path fading** (due to signal reflection) and **interference** (due to other EM signals and transmissions).

5.5 Satellite Radio Channels

- A communication satellite links two or more Earth-based microwave transmitter/ receivers, known as ground stations.
- The satellite receives transmissions on one frequency band, regenerates the signal using a repeater (discussed below), and transmits the signal on another frequency.
- Two types of satellites are used in communications: **geostationary** satellites and **low-earth orbiting** (LEO) satellites.

6 The Network Core

6.1 Packet Switching

- To send a message from a source end system to a destination end system, the source breaks the message into well-formatted chunks called **packets**.
- Each packet travels through several communication links, and **packet switches** (ie. routers, link-layer switches).
- The packets are transmitted at the *full* transmission rate of the link, hence for an end system/switch transmitting packets of length L bits at a rate of R bits/sec, the time to transmit the packet would be

$$T_{transmit} = \frac{L}{R} \tag{1}$$

6.1.1 Store-and-Forward Transmission

- Most packet switches use store-and-forward transmission at the inputs to the links.
- Store and forward transmission means that the entire packet must be received at the input before it can be propagated to the next element in the network.
- The packet bits that a router receives are stored in the router's **buffer** until the entire packet is received, then the packet can be transmitted and the buffer can be cleared.

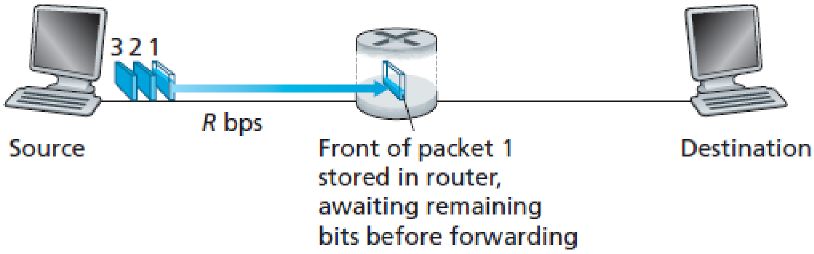

3 2 1
R bps
Source
Front of packet 1 stored in router, awaiting remaining bits before forwarding
Destination

Figure 6: Store-and-Forward Packet Switching

- In the example above, when packet 1 is completely received by the router, it can be forwarded and simultaneously the bits of packet 2 start getting transmitted by the router. By the time packet 1 fully reaches the destination, packet 2 is fully at the router.
- For a single packet of length L bits, travelling over N communication links (hence $N-1$ routers), each having a transmission rate of R bits/sec, the end to end delay between source and destination is
$$d_{end-to-end} = N\frac{L}{R} \tag{2}$$
- Generalizing this to P packets being transmitted, we have
$$d_{end-to-end} = (N+P-1)\frac{L}{R} \tag{3}$$
In the given example, we have $N=2$ and $P=3$, hence the end to end transmission delay is $4\frac{L}{R}$.

6.1.2 Queuing delays and Transmission Loss

- For each input link into a router, the router maintains an **output buffer** (or an output queue) that stores the the packets that the router is about to send into the output link.
- If an arriving packet arrives while the link is already busy transmitting another packet, then it must wait until the link is free.
- This leads to an addition **queuing delay** in addition to the store and forward delay described above.
- If the arriving packet finds that the buffer is full, then either the arriving packet or one of the packets in the queue must be dropped to make space. This leads to **packet loss**.
- This situation normally occurs when the speed of the input links are higher than the speed of the output link, as shown in the figure below (Figure 7).

6.1.3 Forwarding tables and Routing Protocols

- When a router arrives at a packet, the router consults its forwarding table using a part of the destination address of the packet (its **IP Address**) to direct the packet to its appropriate outbound communication link.
- Forwarding tables are set using an automated approach that uses a routing algorithm (static or dynamic) to determine the shortest path between a given source and a destination. (eg: Dijkstra's Algorithm)

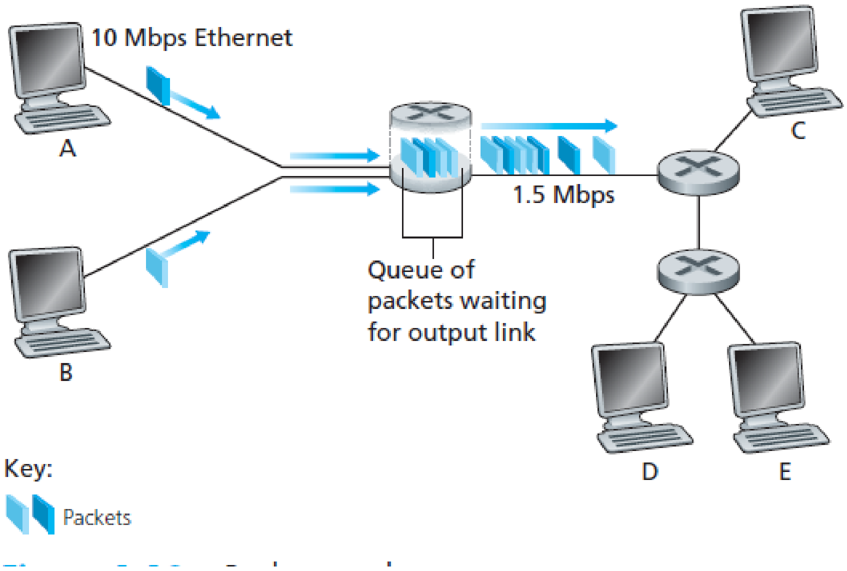


Figure 7: Queuing delay in Packet Switching

6.2 Circuit Switching

- In a circuit-switched network, all resources (buffers, link transmission rate) along a path are allocated and **reserved** for the entire duration of the communication between source and destination.
- In packet-switched networks, by contrast, these resources are used on demand, and hence packets may have to wait until the resource is available to actually make use of it (leading to queuing delays and end-to-end transmission delays as described above).
- Before any communication can happen, a connection must be established between the two parties. This is a *bonafide* connection, meaning that all the network devices along the connection must maintain the same state for the entire duration of the communication.
- In the parlance of telephone networks, such an end-to-end connection is called a *circuit*, hence the name circuit switching is given to such a system.
- Along with the path and the network devices, a constant fraction of the transmission link's capacity must also be reserved for the duration of the connection. This guarantees the data transfer at a *guaranteed* constant rate for the entire communication.
- The splitting of the link capacity between each circuit is achieved using either **Time Division Multiplexing (TDM)** or **Frequency Division Multiplexing (FDM)**.

6.2.1 Frequency Division Multiplexing (FDM)

- The frequency spectrum of a link is split up for each connection across that link.
- The link dedicates a frequency band to each connection for the duration of the connection.

6.2.2 Time Division Multiplexing (TDM)

- Time is divided into frames, and each frame is subdivided into slots.
- When the network establishes a connection across a link, the network dedicates one time slot in every frame to this connection. These slots are dedicated for the sole use of that connection, with one time slot available for use (in every frame) to transmit the connection's data.

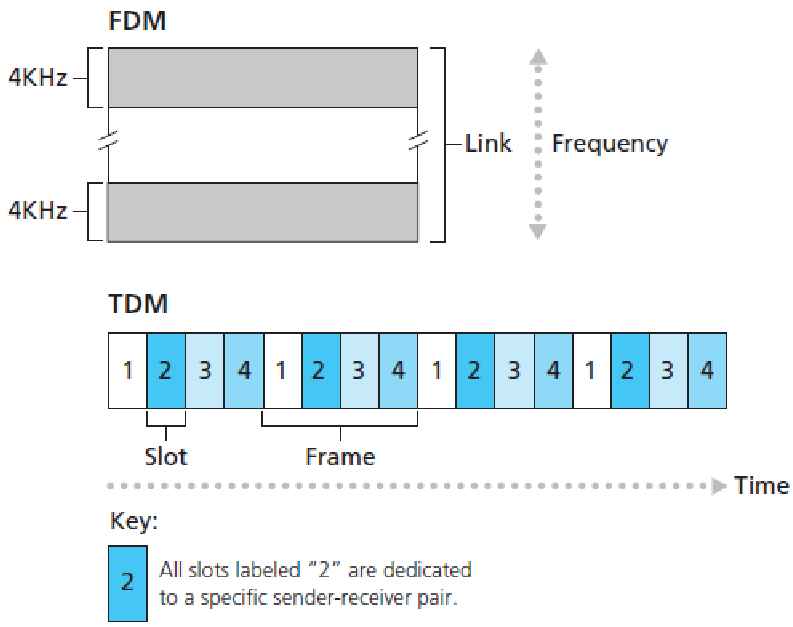


Figure 8: FDM and TDM in a circuit-switched network

6.3 Comparison between Packet and Circuit Switching

- Circuit Switching may lead to under utilization of resources during silent periods.
- For example, if one person on a telephone call stops talking, the idle resources (time/freq bands) cannot be used by any other connections along the same link.
- Establishing end-to-end circuits and reserving end-to-end transmission capacity is complicated and requires complex signaling software to coordinate the operation of the switches along the end-to-end path.
- Suppose users share a 1 Mbps link, and users are active for 10% of time, and inactive for 90% of time. While the user is active, the user generates data at a rate of 100 kbps.
- In a circuit switched network, 100 kbps of link capacity must be reserved for all users at all points in time. This implies that with a total link capacity of 1 Mbps as mentioned, only 10 users can simultaneously use a circuit switched network.
- In a packet switched network, assuming that the total number of users is 35, the probability of having 10 simultaneous active users on the network is 0.9996, and the network functions exactly at the same performance as a circuit switched network.
- When there are 11 or more active users, the router buffer queue begins to expand as the aggregate arrival rate of packets exceeds the output capacity of the link, and the output queue will begin to grow (it grows until the aggregate input arrival rate of packets drops below 1 Mbps). However with 35 total users, the probability of having ≥ 11 users is only 0.0004, which is very small.
- In conclusion, the packet switched network offers similar performance to a circuit switched network while allowing almost thrice as many total users.

7 Network of Networks: Interconnection of ISPs

7.1 Network Structure 1

- This is a global ISP that connects all the individual access networks. This network would span the entire globe and contain at least one router near each access network.

- This single global ISP would charge each local access ISP according to the volume of traffic in the link between the global and local ISPs. The access ISP is called a **customer** and the global ISP is called the **provider**.

7.2 Network Structure 2

- This consists of multiple global ISPs that connect a large number of local access ISPs. These multiple global ISPs must themselves be connected to ensure full connectivity among all the local access ISPs.
- This structure is more favourable for local access ISPs as they can choose between these global ISPs based on their pricing and infrastructure plans.

7.3 Network Structure 3

- Network Structure 2, just described, is a two-tier hierarchy with global transit providers residing at the top tier and access ISPs at the bottom tier.
- In any given region, there may be a **regional ISP** to which the access ISPs in the region connect. Each regional ISP then connects to **tier-1 ISP**s.
- There may be multiple competing networks at each level of this hierarchy (regional, tier-1), and there may be further subdivisions of this hierarchy, such a country-wide larger regional ISP that connects multiple regional ISPs, and itself connects to the tier-1 ISP (eg: in China).
- Such a multi-tier architecture is Network Structure 3. At each level there is a customer-provider relationship where the customer pays the provider for the service they provide.

7.4 Network Structure 4

- To the idea of network structure 3, some devices, namely **PoP**s (Points of Presence), **multi-homing**, **peering** and **IXP**s (Internet eXchange Points) must be added to make it more accurate to the structure of the current internet.
- A PoP is a group of one or more routers (at the same location) in the provider's network where customer ISPs can connect into the provider ISP. For a customer network to connect to a provider's PoP, it can lease a high-speed link from a third-party telecommunications provider to directly connect one of its routers to a router at the PoP
- Multi homing is a facility that allows a customer ISP to connect to multiple providers in the level immediately above, or even levels above that. (eg: an access ISP cann connect to multiple regional ISPs, or multiple regional ISPs along with a direct link to a tier-1 ISP). This is a method of building fault tolerance into an access network.
- Peering is a method of directly connecting two ISPs which are at the same level of the hierarchy, instead of connection via a higher level provider. This connection is commonly done out of mutual interest and no ISP pays the other for a peering link.
- An IXP is an infrastructure built by a third-party company. It is a meeting point where multiple ISPs can peer together, and it consists of multiple link-layer switches connected within a single building.

7.5 Network Structure 5

- In addition to the structure defined in Network Structure 4, the modern internet contains one final piece, the **content delivery netowrk**.
- Such networks are maintained by content providers (such as Google and its related services like YouTube, Drive, Google Office Suite, etc.)
- A CDN has its own internal network by which all the data centers and servers in the CDN can communicate with each other.

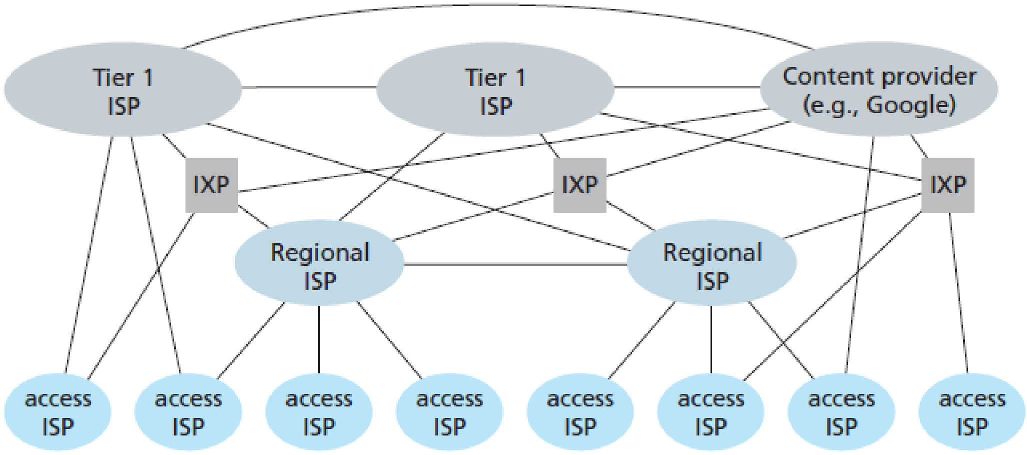


Figure 9: Interconnection of ISPs

- CDNs connect to the rest of the internet either by directly connecting to tier-1 ISPs or directly peering with the lower levels using peering networks or at IXPs.

8 Delay, Loss and Throughput in Computer Networks

As a packet travels from one node (router) to the next in the network, it faces 4 main types of delays: **nodal processing delays**, **queuing delay**, **transmission delay** and **propagation delay**.

8.1 Types of Delays

8.1.1 Nodal Processing Delay

- This is the delay involved in reading the packet header, and routing the packet to its appropriate link, as well as the delays involved in checking for bit-level errors in the packet.

- After the nodal processing, the packet is directed to a queue where it waits for transmission.

- In a modern router, this delay is on the order of microseconds.

8.1.2 Queuing Delay

- The queuing delay is the time spent by the packet inside the router buffer, waiting to be transmitted on the outbound link.

- If the queue is empty and no other packets are transmitted on the link, the queuing delay is 0. If incoming traffic is heavy, and lots of packets are waiting to be transmitted, this leads to significant queuing delays.

- Queuing delays are on the order of micro or milliseconds.

8.1.3 Transmission Delay

- This is the time taken to push all the bits of the packet from the router onto the link.

- If the packet is L bits long, and R is the transmission rate of the link (in bps), then the transmission delay is given by

$$d_{trans} = \frac{L}{R} \tag{4}$$

- Transmission delays are on the order of micro or milliseconds.

8.1.4 Propagation Delay

- The delay involved in propagating all the packet bits from the beginning of the link to the next router.
- This is given by

$$d_{prop} = \frac{d}{s} \tag{5}$$

  Where d is the length of the link, and s is the propagation speed of the link (in m/s)
- These are on the order of milliseconds.

8.2 Queuing Delay and Packet Loss

- The queuing delay, unlike the other three types of delays, may vary from packet to packet, depending on the prevailing conditions of the queue and the outbound link.
- Let a denote the rate of packet arrival at the router buffer, and L denote the packet length in bits. Therefore the rate of arrival of bits at the router buffer is La bps.
- If R is the link transmission rate in bps, then the ratio La/R, called the **traffic intensity** is a good estimate of the queuing delay.
- If $La/R > 1$ then the rate of incoming bits exceeds the rate of outgoing bits. Thus the queue grows without bound, and the queuing delay approaches infinity.
- If $La/R \leq 1$ then the nature of packet arrival affects the queuing delay. Uniform rate of packet arrival leads to zero queuing delay, but packet arrival in large bursts may lead to large avg queuing delays.

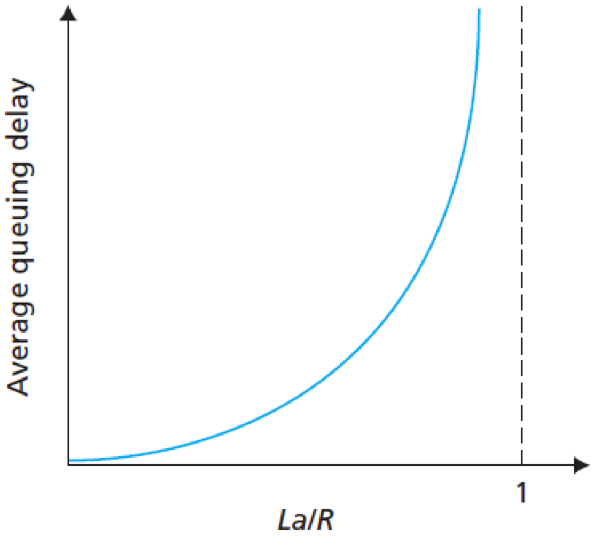
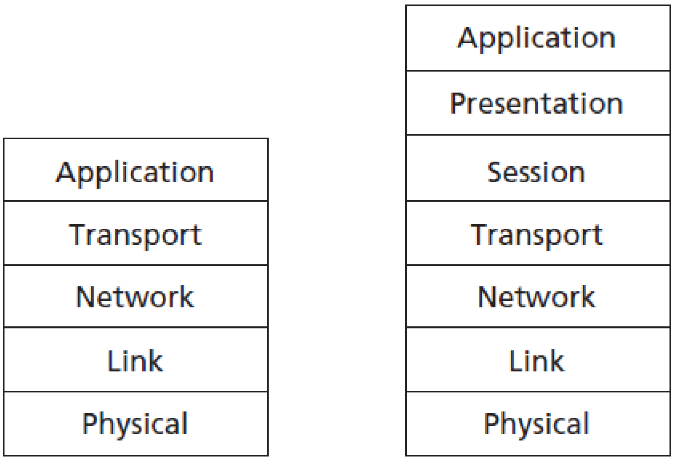


Figure 10: Dependence of avg queuing delay on traffic intensity

9 Protocol Layers and Layered Architecture of the Internet

- The internet and its associated hardware infrastructure are organized as layers so that they can be easily understood and studied.



a. Five-layer Internet protocol stack

b. Seven-layer ISO OSI reference model

- These protocol **layers** are organized in a stack, with each layer providing service to the layers above it, and being independent of the layers below it.
- Layering offers the advantages of **modularity** (which helps in isolating faults and updating hardware) and a clear **standard structure** for vendors to implement.
- The disadvantages of layering are **duplication** of services in more than one layer, and the possible **dependence** of layers on information from other layers.

9.1 Internet Protocol Stack

9.1.1 Layer 5: Application Layer

- **Network applications** and their associated protocols reside in this layer.
- Application layer protocols include **HTTP** (to receive and transfer web documents across the internet), **SMTP** (e-mail transfer), **FTP** (file transfer between end systems) and **DNS** (translation of human-readable web addresses to 32-bit IPv4 addresses).
- End systems use the application layer to exchange information in the form of **messages**.

9.1.2 Layer 4: Transport Layer

- This layer provides support to transfer messages between application endpoints.
- The primary protocols in this layer are **TCP** (a connection oriented service that guarantees reliable data transfer, offers congestion and flow control, along with the breaking of large messages into shorter blocks), and **UDP** (a connectionless, no frills service without congestion/flow control and no guarantee of reliable tranmission, but high speed and stateless).
- Transport layer protocols break the messages from the application layer into smaller blocks called **segments**.

9.1.3 Layer 3: Network Layer

- The network layer consists primarily of the IP protocol, that takes in a transport layer segment along with a destination IP Address, and encapsulates this information into a structure called a **datagram**.

- The IP protocol defines the structure and format of the datagrams, as well as many different routing protocols that determine the routes to be followed by datagrams from source to destination.

9.1.4 Layer 2: Data Link Layer

- Also simply called the link layer, this layer moves datagrams between consecutive routers on the path defined by the network layer protocols.
- Protocols acting in this layer include IEEE 802.11, Ethernet, and PPP. A datagram may pass through many different protocols on each router-router link through its route.
- Link layer packets are called **frames** and they contain additional information in the form of the MAC Address or the hardware address of the destination router.

9.1.5 Layer 1: Physical Layer

- This layer deals with bit level transfer of frames between network devices, across the different types of physical media present on these links.
- The protocols on this layer are dependent on the link medium, eg: Ethernet has separate sub protocols for twisted-pair, coaxial and fiber optic cable media.

9.2 OSI 7-layer Reference Model

The 7 layer model refers to two additional layers which are not part of the internet protocol. In the Internet protocol, these services are commonly wrapped into the application layer and are implemented only if needed.

9.2.1 Presentation Layer

- This layer allows application layer services to interpret the meaning of data and take appropriate actions.
- Services like encryption, compression and description (to aid in conversion between hardware formats) of data fall into this layer.

9.2.2 Session Layer

- This layer offers services for synchronization and delimiting data exchange, including checkpointing and recovery.
- It allows information of different streams, perhaps originating from different sources, to be properly combined or synchronized.

9.3 Encapsulation

- All network devices organize their hardware into layers, but not all devices implement all the layers in the Internet Protocol stack.
- Link-layer switches implement only layers 1 and 2, while routers implement layers 1,2 and 3 only.
- Each layer adds some information to the packet coming from the layer below it, and while going down the layers, this information is removed and used.
- Every packet has a **header** and a **payload**. The header consists of the new information being added, and the payload is the packet from the previous layer.

- The application layer message M is passed to the transport layer at the source
- The transport layers adds the information that is needed by the receiver side transport layer in the **transport layer header** H_t (The port number). The combination of M and H_t is called the transport-layer **segment**.

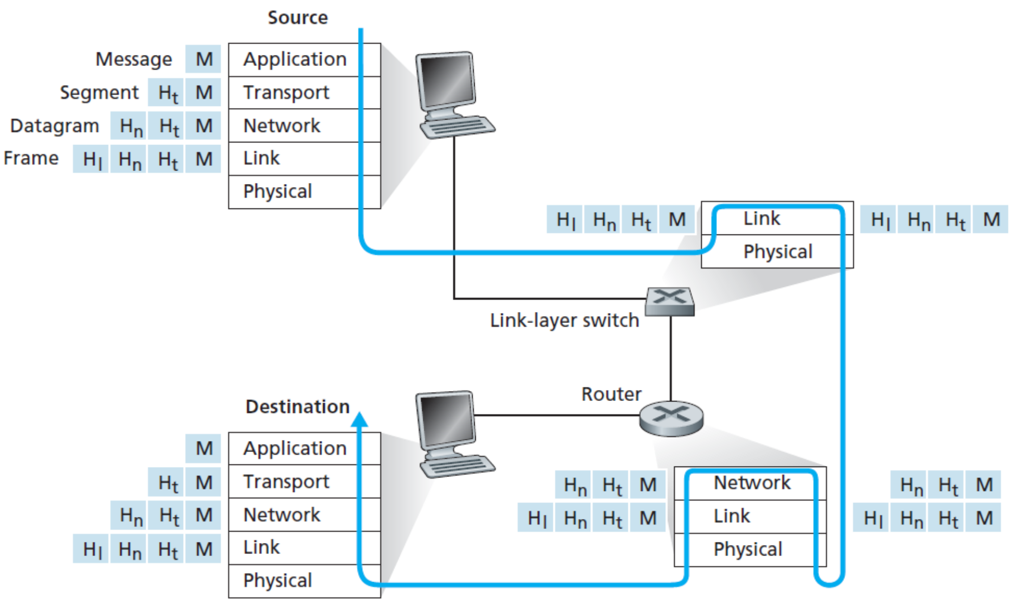


Figure 11: Protocol Stacks on host systems, routers and link-layer switches

- The transport-layer segment enters the network layer and the network-layer header H_n is added to the segment (the IP Address of source and destination), making up the network-layer **datagram**.
- The datagram enters the link layer and the MAC address of the destination (contained in the header H_l) is added to it, turning it into the link-layer **frame**.
- The frame is then transmitted over the physical layer.