Internet Basics

**Recommended reading:** This note is based on Chapters 1-4 of the text book. You are recommended to read the chapters for more details.

**Overview of Internet**

- **Data communication**
  A data communication system is made up of a few basic components: *message*, the information to be communicated; *source*, a device which sends the message; *destination*, a device which receives the message; *transmission medium*, a physical path by which the message is transmitted; and *protocol*, a set of rules for communication.

- **Network type**
  Ideally, each source is connected directly to each destination by a physical link. However, this is impossible due to the hardware or geographical limitations. In practice, sources and destinations are connected by networks.

  Networks can be classified into the following categories:
  - Switched (packet/circuit-switched) networks provide point-to-point message delivery. Messages are transmitted through intermediate nodes.
  - Broadcast networks: there is no intermediate node; one medium is shared by all devices; and the message is broadcasted on the medium and the destination picks up the message.
  - Wide area networks (WAN) cover a large geographical area. WANs are switched networks.
  - Local area networks (LAN) cover a small area, like a building, a campus, etc. Most LANs are broadcast networks.

- **Internet**
  The Internet is a collection of networks connected by network nodes (devices) called *routers*. From the user’s point of view, the Internet is a single global network. It is a virtual global network consisting of many physical networks.

- **TCP/IP internet**
  The research funded by the US Defense Advanced Research Projects Agency (DARPA) for ARPANET results in a set of network standards that specify the details of how computers communicate and a set of conventions for interconnecting networks and routing traffic. The DARPA technology is named TCP/IP Internet Protocol Suit and can be used to communicate across any set of interconnected networks. Many other agencies in US, like National Science Foundation (NSF) etc., have participated in funding the Internet, and use TCP/IP to connect their sites. Now, the Internet, TCP/IP Internet, or ARPA/NSF Internet is used for the global Internet.

  The Internet provides two levels of services: application level services and network level services.

  The services of the Internet at application level include World Wide Web, Electronic Mail, Cloud access and remote desktop, voice and video services, etc.
The services of the Internet at network level include *connectionless packet delivery* and *reliable stream transport*.

- **Network level service property**
  
  Network Technology Independence: TCP/IP is independent of any particular vendor’s hardware.

  Universal Interconnection: In a TCP/IP internet each computer (host) is assigned a unique global address (IP address) through the internet, each process in a host is assigned a unique address (TCP port) within the host.

  End-to-End Acknowledgments: Provide acknowledgments between the original source and final destination.

  Application Protocol Standards: Include standards for applications.

- **Brief history on the Internet and TCP/IP**
  
  The Defense Advanced Research Project Agency (DARPA) of the United States Department of Defense funded a research project for a long-haul packet-switched network in 1969. The result of this project is the network called ARPANET. The original goals in designing the ARPANET include

  - Robust and reliable data delivery.
  - Communication between different computer systems
  - Interconnection between systems across long distances.

  ARPANET became the backbone of the Internet.

  The work on TCP/IP started in 1973. A major goal of this work is to allow the local area networks (LANs), like Ethernet, connected to the long-haul networks. The Internet Protocol version 4 (IPv4) appeared in 1978 and so did the TCP/IP protocols. ARPANET was used for many experiments with TCP/IP.

  The year of 1983 is important for the Internet and TCP/IP. In this year, the Defense Communication Agency (DCA) started the operation of the ARPANET (DCA is now called DISA, Defense Information Systems Agency). It was required in the same year that all computers using any other experimental protocols on the Internet switch to TCP/IP. In the same year, TCP/IP was implemented in the Berkeley’s Unix (4.2BSD) operating system which was widely used in most universities and colleges. The ARPANET was split into two parts, a research network ARPARNET and a military network MILNET in the same year as well.

  The National Science Foundation (NSF) created a new backbone NSFNET for the Internet in 1986. In 1990 the Hypertext Transfer Protocol (HTTP) and the notion of the World Wide Web (WWW) appeared. Commercial Internet Exchange (CIX) is an interexchange point for free exchanging TCP/IP traffic, including the commercial traffic. CIX was created in 1991 and an important initiative for creating the commercial internet.

  The number of devices connected to the Internet increased rapidly every year. As a result, the number of IP addresses in IPv4 became a bottleneck for the expansion of the Internet. To solve this problem, a new version of Internet Protocol, IPv6, was proposed in 1998.
• **Groups related to the Internet and TCP/IP**

The Internet Society (ISOC), the parent organization of other Internet boards and task forces. The home page of ISOC: [www.isoc.org](http://www.isoc.org).

The Internet Architecture Board (IAB), the parent organization for standards making and research groups. Those groups handle the Internet technologies, protocols, and research. The home page of IAB: [www.iab.org](http://www.iab.org).

The Internet Engineering Task Force (IETF), the group for drafting, testing, proposing, and maintaining official Internet standards. There are many areas in the IETF, each area has a manager. The IETF chairman and area managers constitute the Internet Engineering Steering Group (IESG). IETF’s home page: [www.ietf.org](http://www.ietf.org).

The Internet Research Task Force (IRTF), the group for the research and development work for future topics. Its home page: [www.irtf.org](http://www.irtf.org).

Internet Engineering Steering Group (IESG), the group for technical management of IETF activities and Internet standards process. Its home page: [www.ietf.org/iesg](http://www.ietf.org/iesg).

The Internet Corporation for Assigned Names and Numbers (ICANN) manages all Internet domain names, IP addresses, and protocol parameters and behaviors. Its home page: [www.icann.org](http://www.icann.org).

• **Internet Request for Comments (RFCs)**

Documentation of work on the Internet, proposals for new or revised protocols, and TCP/IP protocol standards all appear in a series of technical reports called Internet Request For Comments or RFCs. RFCs and Internet drafts can be obtained from [www.ietf.org](http://www.ietf.org).

**Underlying Network Technologies**

• **Network technologies**

The Internet is a virtual global network consisting of many networks. These networks can be classified into **switched networks** and **broadcast networks** based on the network technology used for communication. The networks can also be classified into **local area networks** (LAN) and **wide area networks** (WAN) according to the technologies for communication over different distances.

• **Switched networks**

In a switched network, network nodes (devices) are connected by communication links, node-to-node (point-to-point) data delivery is provided, and data are transmitted through intermediate nodes (called switches or routers).

There are two switching technologies: circuit switching and packet switching. Circuit switching: a dedicated path is set-up for the duration of data transmission. Packet switching: data are transmitted in units (packets), and packets passed from node to node from source to destination in a store-and-forward way.
• **Broadcast networks**

In a broadcast network, all network nodes are connected to a communication medium, data from a source node are broadcasted on the medium for delivery, only the destination node(s) picks up the data, and nodes other than the destination(s) ignore the data.

• **Local Area Networks (LAN)**

Most LANs are broadcast networks. Network nodes are attached to the common transmission medium. A message from one node is broadcasted on the medium, received by all nodes, and picked up by the destination node(s). The key points of LANs are protocol architecture, topologies, media access control, and logical link control.

In 1985, the Computer Society of IEEE developed Project 802 which covers the first two layers of the OSI model and part of the third layer. In IEEE 802 reference model, LAN protocols have physical layer and data link layer of OSI model.

• **Data link layer**

Data link layer provides services to LAN users. It is further divided into medium access control and logical link control sub-layers.

Medium access control (MAC): It assembles data into frame with address and error detection fields, disassembles frame, recognizes address, detects error, and controls the access to transmission medium.

Logical link control (LLC): It provides the interface to higher levels and flow/error controls. Error detection and control are handled in different sub-layers. MAC layer detects error and discards frame. LLC layer optionally retransmits frames.

• **LAN systems**

Common LAN systems include Ethernet, Token ring, FDDI, etc.

• **Ethernet**

It was originally developed by Xerox and later extended by a joint venture between Digital Equipment Corporation, Intel Corporation, and Xerox. It uses shared transmission medium and the hosts in the network access medium randomly. It uses CSMA/CD MAC technology to solve the contention for transmission medium.

CSMA/CD MAC Protocol: To send a message, a host first listens to the transmission medium. If it is idle, then the host sends the message. Otherwise, it waits for the medium idle. This is called carrier sense medium access (CSMA). After sending the message, the host listens to the medium, if there is a collision, the host stops transmission and retransmits the message with a binary exponential backoff.

The minimum time interval required for all hosts to sense a collision of two frames is determined by the LAN size (the length of transmission medium). This minimum time interval is called contention slot.

Binary exponential backoff is that at the $i$th consecutive collision, a host chooses a backoff interval at random from the range $0 \sim (2^i - 1)$ contention slots. The maximum value for the
range is set to 1023. It means that the range is limited to $2^{10} - 1$ for 10 or more consecutive collisions. In practice, the protocol gives up after 16 consecutive collisions.

CSMA/CD protocol improves the utilization of transmission medium but limits the size of the network. In CSMA/CD, the collision is detected by listen to a high signal level caused by multiple transmissions on the medium. Let $T$ be the signal propagation time in the network. $T$ is proportional to the size of the network. The collision detection is effective if the transmission time of a data frame is greater than $2T$. Once the transmission time (frame size and medium) is fixed, there is a limit on the size of Ethernet.

- **Data frame**
  
  The data frame in Ethernet has the following fields:
  
  Preamble: for synchronization, seven bytes of 1010... .
  
  Start frame delimiter, one byte of 10101011.
  
  Source address, six bytes.
  
  Destination address, six bytes.
  
  Data length(IEEE802.3)/frame type(Ethernet V2), two bytes.
  
  Data, 46-1500 bytes.
  
  Pad, to ensure frame long enough.
  
  Frame check sequence, four bytes.

- **Ethernet address**
  
  Ethernet uses 6 bytes (48 bits) to express an address. Two bits are reserved for global/local and group/individual addresses in the 1st (the most significant) byte. Each device connected to a network has a globally unique Ethernet address (also called hardware address) usually imprinted on the network interface card (NIC).

- **Evolution of Ethernet**
  
  10Base5 (thick Ethernet), bus topology, a single cable segment limited to 500m.
  
  10Base2 (thin Ethernet), bus topology, a single cable segment limited to 200m.
  
  10BaseT (twisted pair), star topology, logical bus, the distance from host to hub limited to 100m.
  
  10BaseF (optic fiber), star topology, logical bus, the distance from host to hub limited to 2000m.
  
  100BaseT4 (CAT 3 twisted pair)
  
  100BaseTX (CAT 5 twisted pair)
  
  100BaseFX (optical fiber)
  
  1000BaseSX (optical fiber)
  
  1000BaseLX (optical fiber)
  
  1000BaseT (CAT 5 twisted pair)

  Hierarchical architecture
• **Power over Ethernet**
  A technology known as *Power over Ethernet* (PoE) has been developed for sending a small amount of electrical power over the transmission medium used for Ethernet. The key point in PoE is that the presence of power does not degrade data transmission. The presence of power in an Ethernet cable makes the applications of small devices with Ethernet much easier.

• **Wireless LANs and Ethernet**
  IEEE has developed a series of standards, known as IEEE 802.11, for wireless networks that are closely related to Ethernet. The medium access control protocol in IEEE 802.11 is known as distributed foundation wireless medium control (DFWMAC) which provides a distributed access control mechanism with an optional centralized control unit. CDMA is used in the distributed access control. IEEE 802.11 also defines a frame exchange protocol to improve the reliability of data transfer.

• **Connect LANs together**
  LANs can be connected by bridges or routers to make a larger network. A bridge connects LANs with same physical/link layers protocols into one network with one network address. A bridge works at data link layer and relays MAC frames on Ethernet addresses. A router can connect LANs of different physical/link layers protocols into one network. A router works at network layer.

  Ethernets can also be connected by *Ethernet switches* which are devices incorporating and extending the concept of bridges. An Ethernet switch functions much the same as a bridge but can provide multiple connections, called *port*, into which devices connect.

• **Wide Area Networks (WAN)**
  A WAN consists of switched networks covering a large geographic area. Usually, a WAN uses routers to connect different networks. The backbone networks in the Internet are WANs, examples including ARPANET, the 1st backbone of the Internet, and NSFNET.

**Internetworking**

• **Approaches for internetworking**
  The goal of interconnection is to hide the details of underlying networks and provide universal communication services. This goal can be achieved by two approaches.

  Application level interconnection: Application programs handle details. Application programs interoperate with peers on other computers. This approach seems natural but is inefficient. Any change in functionality in the application or network hardwares results in the modification of the application program on every computer.

  Network level interconnection: This approach separates data transfer from application programs and handles communication as delivering data packets. Advantages: Efficient delivery of packets. No knowledge on application is needed for intermediate node to deliver packets. Make the systems flexible. Easy to modify the network technology without the change for applications.
The key to design universal network level interconnection is *internetworking* which separates the notions of communication from the details of network technologies and hides low-level details from users.

- **Internet architecture**
  
  Internet is a collection of networks connected by routers. In a TCP/IP internet, special computers called *IP routers* or *IP gateways* provide the interconnections among physical networks. From the user's point of view, a TCP/IP internet is a single virtual network. TCP/IP internet protocols treat networks equally. Routers operate at network layer.

  The Internet provides two levels of services: application level services and network level services.

  The services of the Internet at application level are provided by application programs. Such services include World Wide Web, Electronic Mail, Cloud access and remote desktop, voice and video services, etc.

  The services of the Internet at network level include *connectionless packet delivery* (by IP) and *reliable stream transport* (by TCP).

### Protocol Layering

- **Protocols**

  Protocols are rules for communication and specify the details of message formats, how a source sends a message, how a destination responds when a message arrives, how to deal with errors, etc. Protocols allow us to discuss data communication independent of any particular network hardware. Protocols to communication is similar as algorithms to computation.

  Protocols for computer networks are very complex. A layered structure is an efficient approach to design and implement such protocols. In his approach, a complex communication problem is partitioned into several sub-problems and protocols for the complex problem are divided into several layers, each layer handles one sub-problem.

- **Well used layered model**

  TCP/IP and OSI are well used models for protocol layering.

- **TCP/IP model**

  The TCP/IP model is a result from the research funded by the US Defense Advanced Research Projects Agency (DARPA) for ARPANET (DARPA has also been called ARPA, Advanced Research Projects Agency). Now it is used by the Internet and a de facto standard for internets. There are five layers in the model:

  Application layer, it deals with user applications

  Transport layer, it deals with end to end reliable delivery of data. Transmission Control Protocol (TCP) is used in this layer.

  Internet layer, it deals with data transmission across multiple networks. Internet Protocol (IP) is used in this layer.
Network access layer, it deals with data exchange between the end device and network.
Physical layer, it deals with the access to physical medium.

- **OSI model**
  Open System Interconnection (OSI) model is developed by International Organization for Standardization (ISO). The model is a de jure reference model and has seven layers.
  Application layer, it enables a user, human or software, to access the network. It provides user interfaces and support for services such as email, etc.
  Presentation layer, it ensures interoperability among communicating devices. It provides the necessary translation of different control codes, character sets, etc. to allow two devices to understand the transmission in the same way.
  Session layer, it establishes, maintains, and terminates connections (sessions) between cooperating applications.
  Transport layer, it provides end-to-end delivery of entire message, error recovery, and flow-control.
  Network layer, it deals with end-to-end delivery of a data packet. It handles switching and routing.
  Data link layer, it provides the reliable transfer of data across the physical link.
  Physical layer, it deals with access to physical medium.

- **Conceptual layers and protocol organizations**
  In a layered design of protocols, there can be multiple protocols in a same layer providing different types of services. For example, in the TCP/IP protocol suit, there are many application programs in the application layer for different applications, and there are TCP (for reliable transport service) and UDP (for best effort data delivery service) in the transport layer.

- **Layering principle in TCP/IP**
  One principle in applying the TCP/IP layered structure is that the data packet transmitted from layer $X$ to layer $Y$ at the source node should be identical to the data packet transmitted from layer $Y$ to layer $X$ at the destination node.

- **Protocol Data Unit (PDU)**
  A Protocol Data Unit (PDU) is the data packet which contains the data from the next higher layer and a layer head which contains the control information. For example, a PDU from the transport layer has the transport layer head which contains the information on source/destination service access points (called ports in TCP), sequence number of the packet, error-detection code, and so on.