Computer Networks

John SUM
Institute of Technology Management
National Chung Hsing University
Taichung, ROC

November 14, 2019

Contents

1 Introduction

Today, we can use desktop computers, notebooks and even smartphones to access Google searching engine, watch Youtube videos and make LINE calls. One important infrastructure for making them real is the Internet. Internet is a global network of computers and communication devices. Equivalently, Internet is a network of computer networks. Generally speaking, a computer is able to communicate with other computer as long as both computers have been connected to the Internet.

2 Computer Network

Computer network is a network of computers. It could be a private network of computers, sometimes called local area network (LAN). It could be the public network connecting all the computers in the world, called the Internet. One original purpose of a computer network is to share computational resources amongst the computers connected in the network. For instance, in a research lab located in New Mexico of US, there is a supercomputer that can do large scale scientific computation. A research team in UCLA would like to access this supercomputer for solving a research problem. Without computer network, the researchers had to take the data and drove all the way from LA to New Mexico for accessing such a computer. Clearly, it was not convenient. Thus, it came to the idea of computer network – networking computational resources for sharing. While the motivation is simple, the technologies for making it work are enormous.

Computer network embraces a collection of technologies that enable communication amongst computers. Those technologies are usually named as protocols or in more general term called standards. There protocols include the binary code of a character, to the format of an address of a computer, to the steps for making a secure connection between two computers. To start with, let us have two simple examples.

2.1 Three browsers two websites

Suppose that I have a notebook with WiFi connection. Now, I am siting in a cafe in Taipei. I open three browsers. One of them is connecting to the NCHU server browsing the latest news. One is connecting to the NCHU

server browsing seminar information. The third browser is connecting to Youtube for video watching. Technically, the action 'browse' refers to a sequence of messages passing back and forth.

1. User keys in the url `https://www.nchu.edu.tw/news/id/1` on the address bar and presses return.

2. The browser composes a request message sending to the NCHU web server asking for sending back a specific file (yet another message).

3. Once the request message has arrived the web server, the web server reads the message and figure out what action it should do.

4. The web server in response with the message (i.e. the results of the action) sending back to the browser.

5. The browser reads the message and formats the results as a webpage to the user.

The 2nd and the 4th steps will need the help of the operating system. Precisely, in the 2nd step, the browser (as an application system) requests the operating system to help sending out the message to the Internet. In the 4th step, the operating system sends the message to the corresponding browser once it has received the message.

2.2 Problems aroused and solutions

Even for this simple situation, it raises a number of problems to be solved.

Problem 1 In the cafe, there is only one access point (AP) which is connected to the Internet. There are many notebooks around. How does the access point help these notebooks to sending out the messages to the Internet?

Problem 2 Even though the URL has been keyed, how does the Internet know where the message should be sent to? In other words, which physical machine the NCHU web server is located?

Problem 3 Once the 'latest news' and the 'seminar information' have been received, how does the operating system know which browser shows 'latest news' and which browser shows the 'seminar information'?

Problem 4 Video file is usually a big file, in the order of magnitude mega bytes. So, it is inefficient to send a big file over the Internet. Not just traffic jams could be caused, it could also lead to file lost. So, how does the Internet handle the transmission of a big file?

While all these problems are essential in computer communication, the solutions for solving such problems are very intuitive.

MAC Address To solve the first problem, the solution is to assign for each notebook and the access point a unique address, the MAC address. The MAC address can allow the AP to differentiate which message is sent from which machine, and which message is sent to which machine. Once a computer has been connected to a network, either wired or wireless, the computer will have to report to the network management system its MAC address. Note that MAC address is different from IP address. MAC address, while it is called address, should better be called as a machine ID. Today, this address is assigned by the manufacturer before the mobile device has been released to the marker. This address is unique. Different devices have different MAC address. For an ad hoc wireless network of notebooks, the notebooks can then communicate each other by their MAC addresses.

IP Address To solve the second problem, the solution is to assign for each computer an IP address. The address of a computer on the Internet space. It acts like the postal address of a physical location. To send a message from one machine to another, we simply specify the sender IP address and the destination IP address. The routers in the Internet can read the IP address of the message and route it to its destination. On the other hand, the routers can route back an error message to the sender if the message is failed to be routed. Moreover, the destination server can send the reply message back to the sender computer by specifying the sender IP address.

Session ID To solve the third problem, the solution is to assign for each browser (each process)[1] a session ID. The message composed by the

[1]This technique is in fact applied in process management in an operating system. Each process running in a computer is assigned with a unique process ID. This process ID is used for assigning the file IDs of all temporary files to be accessed by the same process and the process IDs of all the background processes created by this process.

operating system will add the session ID in the message. While the web server has received the message, processed the request and then composed the reply message, the session ID will be added in the reply message. Therefore, the notebook operating system is able to differentiate which message to be shown in which browser (which process).

Sequence ID To solve the forth problem, the solution is to chop the big file into small message files. Each of these message files are then sent to the Internet with the sender and destination IP address, the receiver MAC address, the session ID. Now, one more information is added. It is the sequence ID. The sequence IDs are used for the application system to reconstruct the big file.

For some machines, it might consist of more than one server, say web server together with mail server. So, it causes another problem.

Problem 5 If a machine has more than one server, how does the network operating system know which server queue the message has to be put?

In such case, one more ID called port number is needed.

Port Number For a server machine, it could consist of many servers, like web server, mail server, FTP server and etc. Each server has its own server queue. The port number is able to let the network operating system (NOS) in the machine to efficiently pass to its corresponding server queue once the message has arrived.

These IDs are sufficient for identifying which message to be sent to which process, to which computer and to which server queue. To make it possible, two more problems have to be solved.

Problem 6 Seamlessly, the AP is connected to more than one notebooks helping them sending and receiving messages to and from the Internet simultaneously. As a matter of fact, the AP can only serve one notebook (one device) at a time. That is to say, in each moment, only one device can actually be connected with the AP sending a message to it or receiving message from it. In each moment, the AP can only connect and communicate with one notebook to send the message to. So, how does the AP manage this physical connection?

Problem 7 The routing of a message is relied on a specific network of computers. Normally, we call them routers. Each router is usually connected to at least one other network. Once a message has arrived a router, how does the router forward this message to the other routers?

Problem 6 is usually attributed as the medium access control (MAC) problem. The access point is treated as a medium for the notebooks to send and receive messages to and from the Internet. Problem 7 is attributed as the routing problem. The solutions for the MAC problem depend very much on the actual structure of the computers being connected. The solutions for the routing problem are a bit interesting. They are heuristic and sometimes designed by trial-and-error.

MAC In the WiFi environment, computers can send and receive messages via an access point (AP). In each moment, it is clear that only one machine can connect to the access point to send or receive a message. The mechanism to determine which computer is allowed to connect is defined by a medium access control (MAC) protocol. There are many MAC protocols which are developed for various local area networks (LANs) of different topologies.

For the aforementioned wireless LAN, the medium access control is based on a simple method carrier-sense multiple access with collision avoidance (CSMA/CA)[2], see Figure 1. If a notebook NB-X needs to send a frame of data to the AP (the request-for-webpage message to AP and let the AP forwards it to the Internet), it sends out a RTS (ready-to-send) message together with its MAC address (source MAC address) and the AP MAC address (destination MAC address)[3]. If the AP is idle, it responses by sending a message CTS (clear-to-send) together with its MAC address and the NB-X MAC address. Then, NB-X can send the frame of data to the AP. Once, the AP has successfully received the frame, it replies by sending acknowledgement (ACK) message to NB-X.

It is possible that NB-X does not receive any CTS message. One reason is because the AP is busy. Another reason is because another notebook,

[2]This method is applied not just to notebook-AP connection, but also notebook-notebook connection.

[3]Note that this message together with the MAC addresses is broadcasted in the air in a specific form of radio signal. Thus, all devices in the LAN are able to hear the message. However, only the device with the AP MAC address can receive.

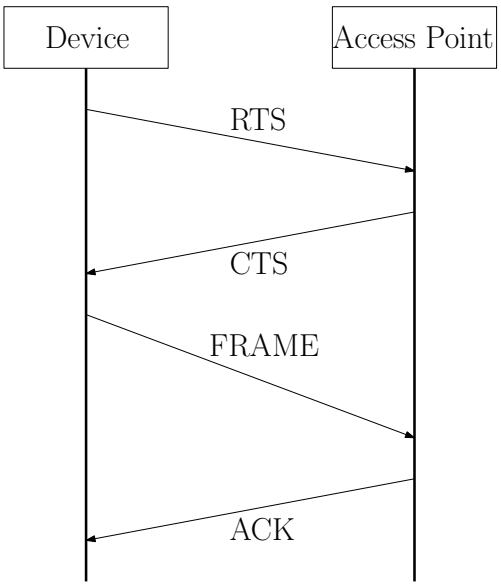


Figure 1: Carrier-sense multiple access with collision avoidance (CSMA/CA).

say NB-Y, also sends out a RTS message. Multiple RTS messages in the air will interfere each others. The resultant messy signal becomes noise. Thus, the AP does not have any response simply because it cannot sense any signal. In either case, NB-X waits for a random time and sends the RTS message again.

Suppose that the webpage has arrived the AP, the AP needs to forward it to NB-X. The AP does the same thing. It first sends out a RTS message together with its MAC address (sender MAC address) and the NB-X MAC address (destination MAC address). If NB-X is idle, NB-X responses by sending a CTS message together with its MAC address and the AP MAC address. Then, the AP sends the frame of the webpage message to NB-X. Finally, NB-X sends ACK message to the AP once the frame has been received successfully.

In fact, the request-for-webpage message to be forwarded to the Internet is an IP datagram, see Figure 2. It consists of the data (i.e. request-for-webpage message) to be sent to the NCHU web server, the sequence ID, the session ID, the source and destination port numbers, the source and destination IP addresses. This datagram is eventually routed to the NCHU web server.

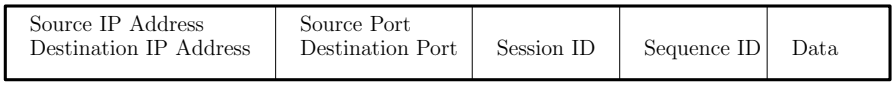


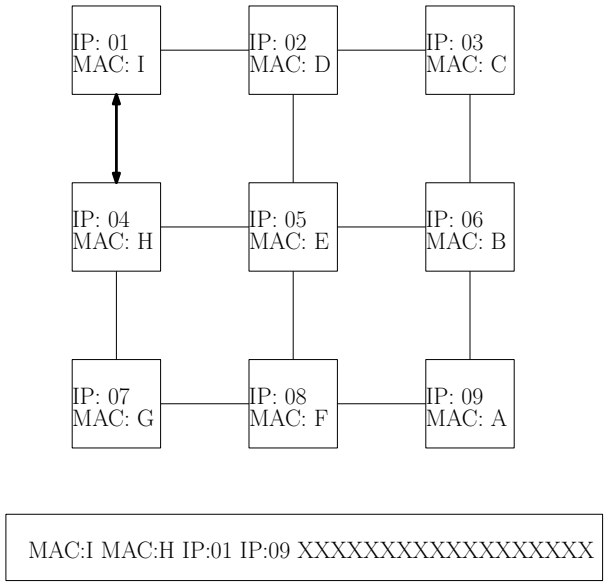
Figure 2: The IP datagram to be forwarded by the router to the Internet.

Routing Algorithms There are many routing algorithms the routers can implement. One approach is to maintain a router table. The table reveals the topology of the network of routers the router can reach. If a router needs to forward a datagram, it determines from the table the shortest path to route the datagram to its destination. By that, the router is able to determine which neighbor routers the datagram should be forwarded. If the destination IP address does not exist in the router table, the router forwards it to a higher level (domain level) router and let it forward the datagram through the network of domain routers.

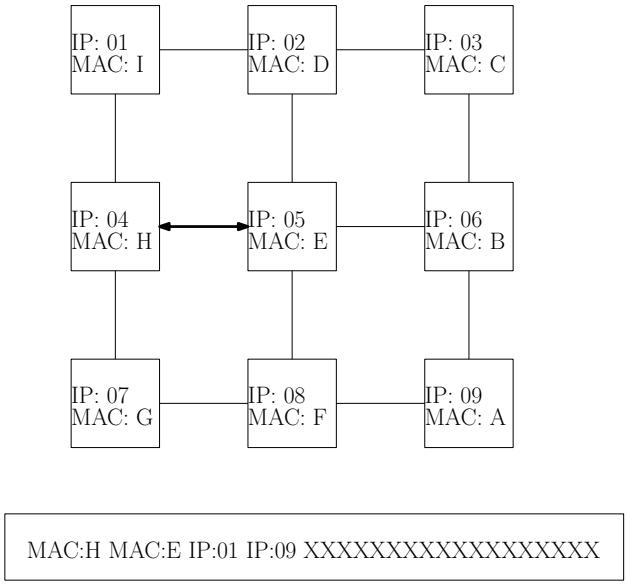
The above approach applies to a stable network with fixed topology. For a network with dynamic topology, the above routing algorithm could not be implemented efficiently. For a network of notebooks, the notebooks move arbitrarily. Due to limit of transmission range, only two notebooks within the transmission range are able to communicate. In this moment, these two notebooks are neighbors. In another moment, these two notebooks could be distance apart. Then, these two notebooks are not neighbors. The network topology changes. In this regard, the router table will have to be updated frequently if the above routing algorithm is applied. It thus leads to very high overhead is too high. To this end, another routing algorithm is more suitable for this kind of network, flooding. The datagram (resp. message) is simply forwarded to all the neighbor notebooks. Each neighbor notebook checks if its IP (resp. MAC) address is the destination IP (resp. MAC) address. If it is not, the neighbor notebook floods the datagram to all its neighbor notebooks.

2.3 IP address versus MAC address

It should be noted that routing of a datagram is based on the information of the source and destination IP addresses. Sending of a frame of message from a computer to another computer within a LAN is based on the information



(a) Packet is forwarded from IP01 to IP04.



(b) Packet is forwarded from IP04 to IP05.

Figure 3: A message is forwarded from IP01 to IP09.

of the source and destination MAC addresses. In principle, each computer in a Internet-connected LAN will be assigned with an IP address during the time it is connected to the LAN. This IP address could be a temporary IP address. The table mapping between the IP addresses and the MAC addresses is maintained by the routers in the LAN. Once the computer has been disconnected from the LAN, its IP address will be released.

If a LAN is an isolated private network and the computers have no need to access Internet, it is in principle to use their MAC addresses for communication amongst the computers. For some networks of mobile devices which are communicated by Bluetooth or Zigbee technologies, it is also possible to use the MAC addresses for communication.

Figure 3 shows an example how a packet is formated during routing. Here, device with IP:01 and MAC:I is goint to send a data to the the device with IP:09. Once it has made connection with the device (IP:04, MAC:H), it generates the following packet and then forwards it to the device.

MAC:I MAC:H IP:01 IP:09 XXXXXXXXXXXXXXXXXX

Once the IP:04 device has received the packet and checked that it is not the destination, it forwards the datagram to a neighbor device, say the one with IP:05 and MAC:E. The following packet is then sent out.

MAC:H MAC:E IP:01 IP:09 XXXXXXXXXXXXXXXXXX

So, the only change is the source and destination MAC addresses. The source and destination IP addresses have not been changed.

2.4 Network topologies

Network topology usually refers to the structure of a local network, not the structure of Internet. Figure 4 shows four examples. For the bus structure, all computers are connected to a common medium called bus. To control the medium access, one method is based on the algorithm described in Figure 1. It is also the method applied in the medium access control for sharing an access point to multiple mobile devices.

In the ring structure, the computers are connected in a ring shape. Each computer can only communicate with two neighbor computers. The MAC protocol for this structure is called token ring. Each computer is initially assigned with a number. Then, a special message with a token inside is

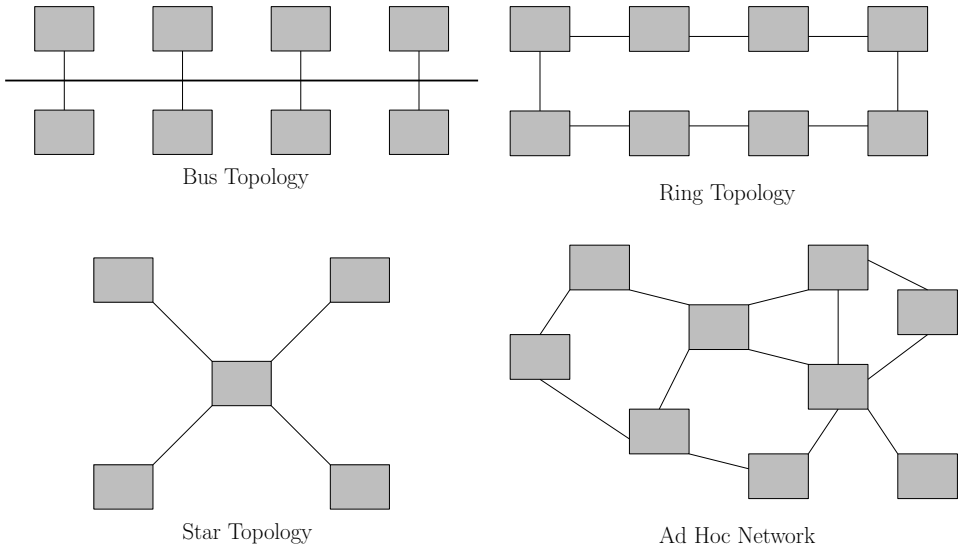


Figure 4: A few network topologies.

composed. The token is started as '1'. The number in the token indicates which computer can send message. Suppose now that C1 needs to send a message. It composes the message with the destination number, say C3, and passes it to C2. C2 checks that the token is '1' and the destination is not C2, it passes the message to C3. Now, C3 checks that it is the destination. It then downloads the message, increments the token number by one, i.e. '2'. Clearly, C3 has no right to send, it them passes the message to C4 and so on.

Nowadays, many vehicles have been equipped with a computer inside. These computers thus form a mobile ad hoc network. As the vehicles in the network are moving around, the network has no fixed structure. Communication between two computers can only be possible if they are within the transmission range. So, a computer can have many neighbor computers if there are many computers in its transmission range. In other case, it can have no neighbor computer if there is no computer in its transmission range. Routing algorithms for this kind of networks are still underway.

3 Telecommunication Network

Internet and telecommunication network are two different networks. Internet is the infrastructure for computers communication, while telecomm network is for communication amongst mobile phones and landline phones. The operation principles of computer network and telecomm network are similar but not the same. However, many technologies behind them are similar. For example, each computer connected to the Internet has a unique IP address for sending or receiving messages. Each smartphone connected to the telecomm network has a unique phone number for making phone calls. The carrier frequency in telecomm network is different from the carrier frequency in WiFi.

Today, each telecommunication firm (or operator) provides many services to her subscribers, including voice service, cellular data service and many others. Voice service and cellular data service are two important services for almost all subscribers, through the 4G/5G cellular network and the landline network.

3.1 Voice service

Voice call is the fundamental service that every telecommunication network has to support. While a caller X has to make a call to Y, the caller X simply keys in the phone number of Y. As the voice call is a real-time service, it is not allowed to have lag during the call. Thus, the switching centers of the telecommunication firm will make a dedicated path for X and Y. This dedicated path is called a circuit. Resources along the path are allocated for X and Y to ensure high quality voice call, such as zero time lag and zero noise. This method of switching is called **circuit switching**.

3.2 Data service

Sending and receiving digital data is another service provided by telecommunication firms. Sending a page of document from one facsimile machine to another facsimile machine would need to use the data service. Messaging a photo to your friend will need to use the data service. To support data service, the mechanism is based on the idea of **packet switching**.

The document or file is chopped into multiple small segments. Each segment is encapsulated in a stream of binary bits called packet. These packets

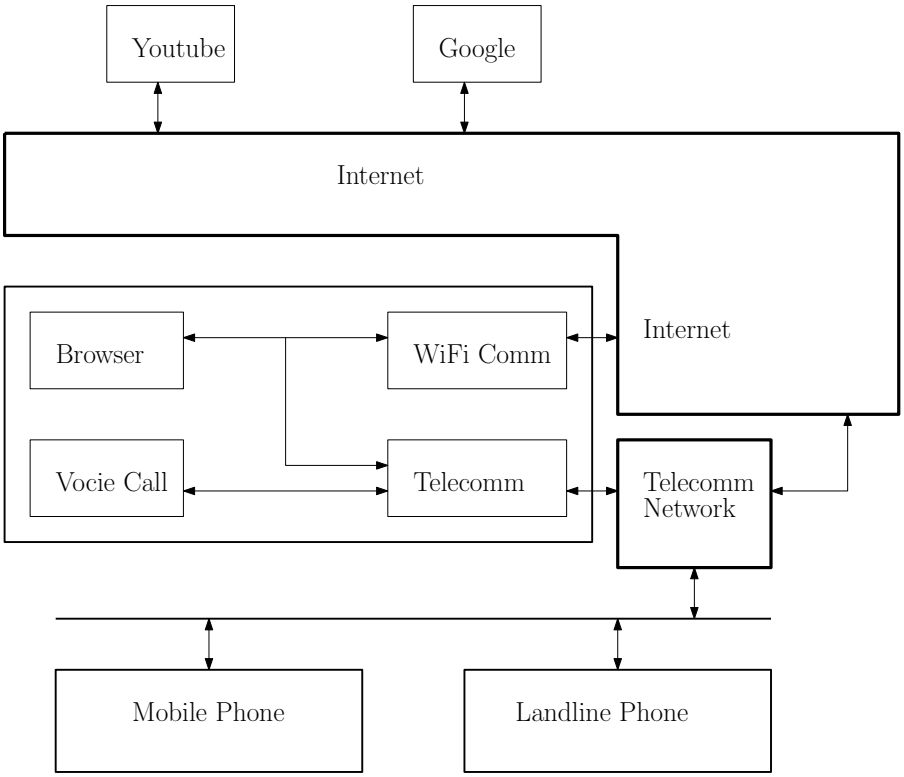


Figure 5: Smartphone is able to connect to the Internet and telecomm network.

are thus routed to the destination phone. Finally, the file is reconstructed in the receiver phone. In contrast to voice call, data service has no need to be real-time. Packet switching, instead of circuit switching, is already good enough to support such service.

Here, two points should be noted. First, the idea of packet switching is also applied in Internet. However, the industrial standard (equivalently, the technologies) for telecommunication networks supporting data services is not the same as the standard for the Internet. Second, almost all public telecommunication networks are now connected to the Internet via a machine called gateway, see Figure 5. One of its tasks is to convert the format of the packet to be passed from the telecommunication network (resp. Internet) to the Internet (resp. telecommunication network).

3.3 iPhone setting

Suppose you have subscribed both the voice service and data service from a telecommunication firm. You can set your phone as shown in the following.

```
WiFi              OFF
Bluetooth         OFF
Cellular          ON
Personal Hotspot  OFF
Carrier           ON
```

The carrier must be ON. Then, you phone can connect to the telecommunication network. To enjoy the data service, 'Cellular' has to be ON. To let the phone to connect to a WiFi network, WiFi has to be ON. It should be noted that the phone can still access to the Internet if WiFi is OFF.

3.4 Network of 2 PCs

Suppose you would like to have a network of two remote computers. One is located at home and the other is located in your office. To make communication between these two computers possible, one would need to have two modems. The modem[4] is connected on one side to the computer and the other side to the telecommunication network. In this regard, sending message from one computer to the other is possible. Before doing this, it

[4]The full name of modem is modulator-demodulator.

has to be sure that you have subscribed telecommunication services for your home and your office.

4 Switching

Switching technology refers to the method to pass a data (resp. voice) message to from one device to another. Here, a device could be a computer or a smartphone.

4.1 Circuit switching

As mentioned in the mechanism how voice is sent over the telecommunication network, the technology is based on circuit switching. Once a device X needs to send a data (resp. voice) message to another device Y, the network (resp. telecommunication network) will instruct the intermediate nodes, the routers in the network (resp. the switches in the telecommunication network), to reserve resource and then form a circuit (i.e the dedicated path) for the devices X and Y. Then, devices X and Y can communicate with each other over this circuit seemingly like no disturbance from other devices. Apart from handling voice call over the telecommunication network, circuit switching can support other real-time mission critical tasks which demand excellent quality of communication with no delay.

4.2 Message switching

In message switching, a message is forwarded from one node to another based on the idea of store-and-forward. Usually, it is assumed that the message is not a short message. Thus, the time spent on receiving a message is not instantaneously. Once a message is sent to a node, say Y, its bits will be stored in node Y. Until the complete bit stream has been received, the message is then forwarded to a neighbor node for routing. In contrast to circuit switching, there is no dedicated circuit to be set up in message switching.

As the entire message is forwarded from one node to another, the time spent on sending a message from one device to another depends on the path that the message has travelled. The message could take a long time to arrive the destination device if there are too many nodes along the path.

4.3 Packet switching

Message switching is aimed at sending the entire message from node to node. Packet switching is aimed at sending part of the message from one node to another. First, the message is chopped into small segments. Next, each segment is assigned with a sequence ID and encapsulated in a packet. Finally, these packets are sent to the network. In the receiver side, the packets are then decapsulated and the message is reconstructed.

For some applications, like streaming, the entire file is not possible to be sent from the video server to the user computer. Clearly, the video file must be chopped into segments and sent to the user computer in forms of packets. The video is thus reconstructed in the user computer and shown on the video viewer.

5 Noise

Applying which switching method is sometimes related to the channel noise. It should be noted that each packet or message is actually a stream of bits. This stream of bits will be physically embedded in a very high frequency electrical signal (resp. radio signal). This signal is called the carrier signal and the frequency is called the carrier frequency. The signal will then be transmitted through a cable (resp. the air) to the other device. If the channel is fiber optics, there is another mechanism for sending the stream of bits.

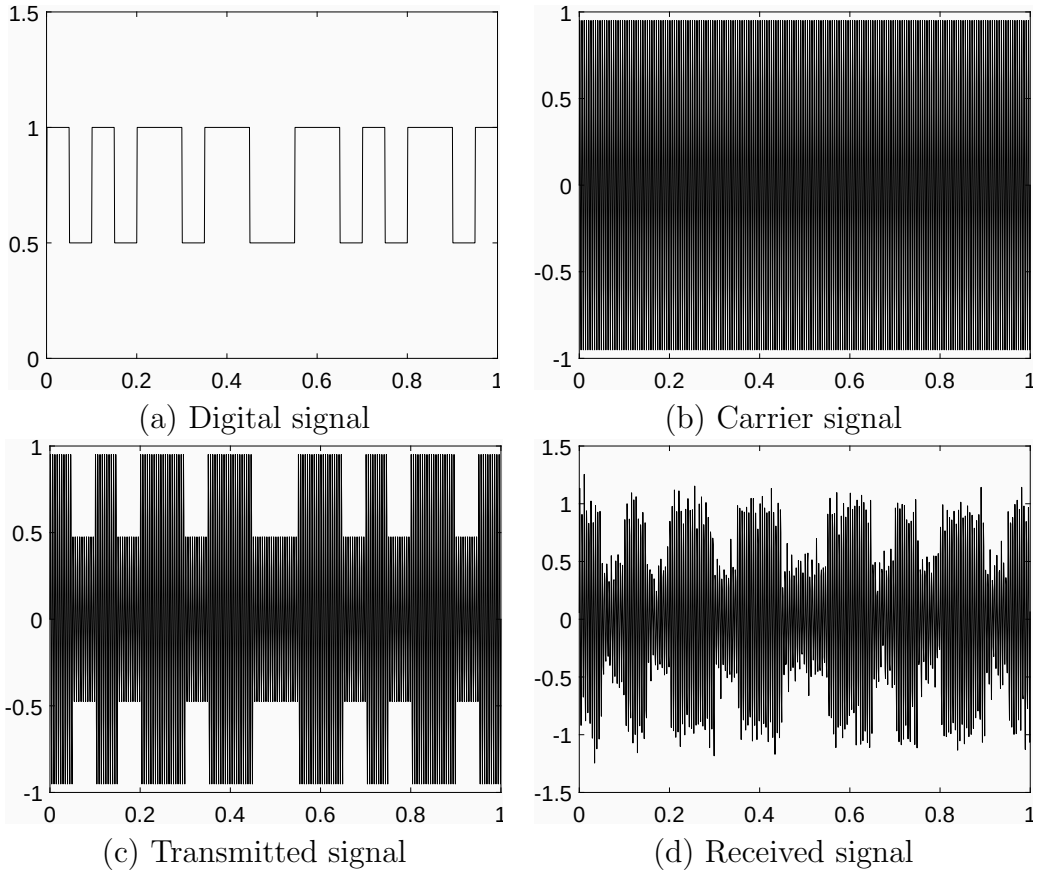
To start with, let us introduce how digital data is transmitted by radio signal. By that, some key terms are introduced. Suppose a stream of 20 bits is going to be transmitted.

Source:10101101100110101101

1. A sequence of electrical signals is generated to represent the bits, see Figure 6a.

2. The electrical signal is thus multiplied with a carrier signal as shown in Figure 6b. For illustration, the frequency of the carrier signal is 200Hz. In reality, this frequency is around 2.4 GHz or higher.

3. The radio signal (i.e. electromagnetic wave) is generated and emitted to the air, see Figure 6c.



(a) Digital signal (b) Carrier signal

(c) Transmitted signal (d) Received signal

Figure 6: Digital data transmission via radio signal.

4. In the presence of noise, the signal received is a noisy radio signal as shown in Figure 6d.

A few points should be noted. (1) The data transmission rate, i.e. say 10 mega bits per second (10 Mbps), depends partly from the carrier frequency. (2) The data transmission rate cannot be higher than the carrier frequency. (3) In wireless communication, the bit error rate (a measure of the noise effect of a channel) depends on the distance between two devices. One factor is due to the fact that particles, like water molecules and dusts, in the air could absorb the energy of the radio signal and end up with signal deterioration. Another factor is the background radiation (from microwave oven and sun light) which is a source of noise corrupting the radio signal.

As a result, the reconstructed bit stream could be erroneous. In this example, the 6th and the 13th bits are incorrect.

Source: 10101101100110101101
Destination: 10101001100100101101

Similar situation exists when the digital signal is transmitted over a cable or a fibre optic. In either cases, error detection and correction is an important problem in data transmission.

Problem 8 In the above example, as we know the correct bit stream, we know which bits are incorrect. However, the destination device cannot have such information. The stream of bits received is the only information it has. Error detection and error correction turn out to be two big problems to the engineers. Thanks to the pioneer engineers, many error detection and correction methods have been developed.

Error Detection & Correction Once a stream of bits has been received, the destination device can detect if there is any incorrect bit. If there is, the device can try to correct the error. Note that all these methods have one limitation. They can only correct erroneous bit stream with a few error bits. If there are too many error bits, the only way is to ask the source device to re-send.

To this end, one should realize that it is not recommended to apply message switching for a long data over a wireless medium. The recontructed bit stream could have too many error bits. The data transmission might not be successful even after a number re-send. Message switching is thus suitable for wired network with very low bit error rate.

6 Packet Loss

For a packet to be sent, there are at least two possible reasons making it disappear. The first one is definitely the channel noise. Suppose that a datagram is going to be sent from device X to a neighbor device Y. If the channel is too noisy, the datagram cannot be reconstructed in device Y. As a result, device X cannot receive the ACK frame. Normally, each device will set a waiting time, say 1 second. After one second, the ACK has not been received, the packet is treated as loss.

Another factor leading to packet loss is a bit funny. Let say a datagram has been routed to a router K. Router K will check the destination IP address. If the destination IP address is one of its neighbor, the router forwards the datagram to the neiighor. If it is not, teh router guesses which neighbor router is closer to the destination IP address and then the datagram is forwarded to it. For the latter case, it is not guaranteed that the guess is correct. It might happen that the guess is wrong and the datagram is again forwarded to another router which is far away from the destination IP address. In the end, the datagram could be forwarded in the Internet forever.

Owing to solve this problem, apart from the soruce IP address and the destination IP address have to be specified in the IP datagram. In fact, one more information has to be added. It is the time-to-live (TTL) information. For instance, the TTL is set to 15 by the source device. Once, the datagram has arrived a router (or other devices for doing routing), the value of TTL will be decremented by one. If the datagram has been forwarded for 15 times, the TTL will then be decremented to zero. In such case, the datagram will not be forwarded and deleted. This is the second reason leading to packet loss.

7 Protocol

Protocol refers to a collection of technologies and standards to ensure voice/data communication amongst devices connected to a network. One might also call these technologies and standards the rules or agreements.

The frequency of the carrier signal is specified in the protocol. The format of the electrical signal representing '0' and '1' singals is specified in the protocol. The method to control medium access and the format of binary stream of the packet are specified in one of the MAC protocols. The method of embedding this binary bit stream in radio signal and the method to correct erroneous bits are specified in the data-link level and physical level protocols.

Device manufacturers can thus follow these standards to design and make the communication devices, like routers, built-in network cards and the chips for WiFi communication. Today, the widely adopted protocol for Internet is called TCP/IP. TCP refers to transmission control protocol. IP refers to internetworking protocol.

There are many protocols for telecommunication networks and Internet. Earlier in the text, it is mentioned that telecommunication network and

Internet are two different networks. One reason is that the protocols for telecommunication network are not the same as the protocols for Internet. The carrier frequency for cellular networks is not the same as the carrier frequency for WiFi networks.

8 Applications

The ultimate pruposes of these protocols are developed to support 'data' communication. The source device (with a unique IP address) generates a stream of bits in which the 'Data' is encapsulated as shown in Figure 2. Once the stream of bits is received at the destination device (the device with the corresponding desintation IP address), the 'Data' is reconstructed. So, we can now use the Internet to develop applications.

8.1 Simple example: File transfer

Suppose that I want to share technical reports to my friends. The size of each technical report is over 1MByte. It is definitely larger than the size of the 'Data' that can be encapsulated in an IP datagram. So, I need to develop an application program. The program is applied to chop a report file into a number of segments. Each segment is small enough to be encapsulated in the datagram. Apart from file chopping, I also need to add extra information to let the application program running in the destination computer know what is going on with these segments. So, here is a method developed for sending large file. It is assumed that an application program named APP21 is running as a background process in both the source computer and destination computer.

Source Computer

Step 1: Chop the file into segments of no more than 512 bytes.

Step 2: Number each segment with a sequence ID, starting from 1, and a number (say APP21) representing the application program.

Step 3: Generate a summary data for the file, including (i) memory size of the file (ii) the total number of segments to be sent. Number the summary with the sequence ID 0. Again, the number APP21 is added, see Figure 7.

Summary data:

```
APP21 SID000 50KByte 100 Segments
```

Segment 001:

```
APP21 SID001 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Segment 002:

```
APP21 SID002 yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
```

Figure 7: Segments to be generated.

Step 4: Request the operating system to send out the segments.

Once the segments have be received in the destination IP address, the operating system identifies from 'APP21' that the data is sent to the background process APP21.

Destination Computer

Step 1: Puts the segments one by one in temporary memory location.

Step 2: Checks for the segment with SID000 and the information in the segment.

Step 3: Reconstructs the file in accordance with the sequence IDs.

Step 4: Generates an acknowledgement data and sends it to the source computer.

8.2 Application-layer protocols

To make the above application works, one would need to have a program (i.e. APP21) to be developed. This program must be installed and running persistently in both the source and destination computers. Together with the program, one needs to design the format of the data to be encapsulated in the datagram. Therefore, the APP21 running in the source computer can generate the right format of data to be sent. The program APP21 in the destination side is able to understand the meaning of the data received.

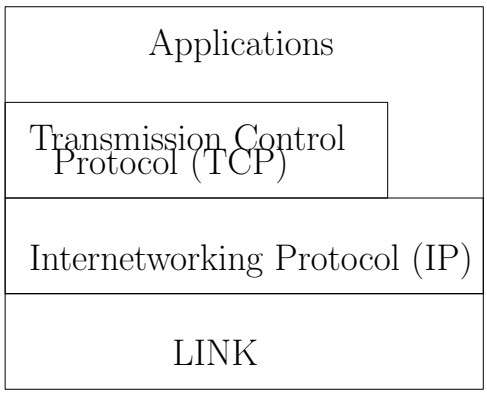


Figure 8: Protocol stack.

Nowadays, many applications have been developed by using the services provided by the Internet. Notable applications include file transfer, email, world wide web and voice transfer (LINE and Whatsapp). Their corresponing protocols are called file transfer protocol (FTP), simple mail transfer protocol (SMTP), hypertext transfer protocol (HTTP) and voice over Internet protocol (VOIP). As these protocols are developed for common applications, they are collectively called the application layer protocols, or simply application protocols. They have been filed to be standards and listed with numbers. In fact, many tehnology firms have developed their own protocols for different applications. Even though, those protocols have not been filed as standards.

Figure 8 shows the protocol stack. In the bottom layer is the LINK layer. Merdium access control, the format of the packet to be send to the destination MAC address, error detection and so on are specified in the LINK layer. The second bottom layer is the internetworking protocol (IP) layer. On top of it is the transmission control protocol layer. Applications are developed by using the services provided either or both by TCP layer and IP layer.

9 Conclusions

In simple words, computer network is simply a network for sending data from one computer to another computer. The technologies (or the protocols) developed are to ensure that the data received in the destination computer is identical to the data sent from the source computer. The global network is computer networks becomes to day Internet. Applications can thus be

developed on top of Internet for various purposes, such as file transfer and send mail.

To conclude this chapter, I must say that we should appreciate all those engineers and scientists who have involved in the development of Internet. Radio engineers, electrical engineers and even scientists developed many technologies to ensure smooth transmission of physical signals (i.e. electrical signal or radio signal). Computer scientists and mathematicians developed error detection and correction technologies. Moreover, they developed many encryption technologies to ensure network security. Building of such a extraordinary Internet is one of the mega project in the 20 century.

10 Questions

1. What is the use of IP address?
2. What is the use of MAC address?
3. What is the use of PORT ID?
4. What is the use of session ID?
5. What do TCP and IP stand for?
6. What is the use of domain name system (DNS)?
7. Once a device, like smartphone and notebook, has been manufactured, it will be assigned with unique address (or ID). What is the name of this address (or ID) and what is it used for?
8. In simple words, what is the ultimate goal of technologies developed behind TCP/IP?
9. What is the format of an IP datagram?
10. Describe the mechanism of CSMA/CA in medium access control.
11. You are now in Taiwan. You telephone service is subscribed from a Taiwan telecom firm. You have set your phone WiFi OFF but cellular ON. Describe the mechanism how the browser in your cell phone can connect to Google.

12. Imagine that you are now in HK. You telephone service is subscribed from a Taiwan telecom firm. In HK, you set your phone WiFi OFF but cellular ON. Describe the mechanism how the browser in your cell phone can connect to Google.

13. Without connecting to the Internet, is it possible to connect notebooks to form a local area network for data communication?

14. Name three application protocols and describe what applications they support.

15. Describe under what conditions, a packet can be lost.

16. Search over the Internet and find in which year the APARNET project was launched.

17. In telephone network, after a caller has dialed and connected to another phone, both phone users can talk to each other. Which switching method is applied to make this connection?

18. VOIP is a protocol (i.e. a collection of technologies) for sending voice signal from one computer to another over the Internet. Which switching method is applied to make this connection?

19. What is the key difference between message switching and packet switching?

20. Is encryption technology embraced in TCP or IP?

21. Is HTTP embraced in TCP or IP?