Xi Liu, xl3504

Assignment 1

1.

(a)

circuit switching requires two nodes to have a communication circuit before communication.

packet switching does not an establishment of dedicated path between two nodes.

Let d\_{end - end}: end to end delay

d\_{proc}: processing delay

d\_{queue}: queuing delay

d\_{trans}: transmission delay

d\_{prop}: propagation delay

N: number of routers

L: packet size (bits)

R: transmission rate of link between two routers (bits / second)

D: distance between nodes (meters)

S: propagation speed (meters / second)

d\_{trans} = L / R

d\_{prop} = D / S

circuit switching:

delay = N (d\_{proc} + D / S) + L / R

packet switching:

delay = N (d\_{proc} + d\_{queue} + d\_{trans} + d\_{prop}) = N (d\_{proc} + d\_{queue} + L / R + D / S)

N \* L / R since packet switches use store and forward transmission, in which router must receive all bits of a packet before transmitting it, and a packet has to go through N links.

(b)

(1) layering nature of internet protocol stack is unlikely to change, since modularity makes system component update to be easier so that update of one component of a layer does not affect the service of another layer. a significant change of this layering structure requires big and expensive modifications of operating system software and related hardware.

the internet protocol stack is:

application layer of network applications that uses application layer protocols such as hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

transport layer that transports application layer messages using protocols such as connection-oriented transmission control protocol (TCP) that guarantees the correct ordering of reassembling segment (transport layer packets), connectionless user datagram protocol (UDP) that have no reliability.

network layer that moves datagrams (network layer packets) between hosts. network layer services deliver segments to transport layer in destination host. network layer uses internet protocol (IP) that defines fields in datagram and how routers and end systems need to act on them. network layer include routing protocols that find routes for datagrams.

link layer contains protocols for links that hosts are connected to. link layer protocols include Ethernet, WiFi, data over cable service interface specification (DOCSIS). link layer packets are called frames.

physical layer is for moving individual bits within frame. protocols are dependent on link and transmission medium. Ethernet has physical layer protocols for copper wire, coaxial cable, and fiber.

(2) what each field represents in the header of a datagram used in internet protocol (IP) and how they are interpreted. since each field is useful for the transmission of the datagram. for example, source and destination address fields must be present so that the packet can reach where its designated destination. A checksum field can be used to check the integrity of the data.

(3) link layer protocols such as Ethernet or WiFi are likely to continue to be valid protocols and well supported in the future. Ethernet connection is usually faster and more reliable than WiFi. whereas WiFi enables multiple users to be connected simultaneously.

(4) orbital height of a geostationary satellite or a satellite used in global positioning system (GPS) is likely to be same. if the satellite is too close to earth, not enough area of the earth can be seen, and air friction became influential. if the satellite is too far, then it might be harder to detect a location of an object on earth and more time delay in transmission.

2.

(a)

advanced message queuing protocol (AMQP)

constrained application protocol (CoAP)

data distribution service (DDS)

message queuing telemetry transport (MQTT)

extensible messaging and presence protocol (XMPP)

(b)

internet of things (IoT) protocols and devices currently lack interoperability between different technologies and have platform segmentation. to solve the problem, more standardization and documentation of IoT protocols are needed.

3.

(a)

open systems interconnection (OSI) model has 7 layers: application, presentation, session, transport, network, link, and physical. whereas transmission control protocol/internet protocol (TCP/IP) network model has 4 layers: application, transport, network, and link.

OSI model development is earlier then TCP/IP development, but OSI’s development is more theoretical whereas TCP/IP model has a more practical answer to concrete engineering problems.

TCP/IP is incorporated into the operating system compatible with Berkeley Software Distribution (BSD) sockets, Linux has its internet protocol implementation of sys/socket.h, netined/in.h, and netinet/ip.h where TCP socket is socket(AF\_INET, SOCK\_STREAM, 0), UDP socket is socket(AF\_INET, SOCK\_DGRAM, 0), and raw socket is socket(AF\_INET, SOCK\_RAW, protocol), in which AF\_INET stands for internet protocol address family.

early implementations of OSI model had poor performance, whereas TCP/IP model was connected with uniplexed information computing system (UNIX) that take advantage of the operating system and its popularity. OSI model was not well designed since session and presentation layers are almost empty.

(b)

advantage: network layers in architecture provides abstraction that reduce complexity of development. It defines a model that encapsulates important components of the system and provide an interface that can be useful for other components of the system. problem of building a network is divided into more smaller and manageable sections, each layer target one type of problem. more modularity is provided, if want to update functionality of a service in one layer, need not update implementation of the services in other layers.

disadvantages: if a developer of one layer is not aware of the service in another layer, functionalities might be duplicated if that developer reinvent that functionality. making a new protocol that need to be compatible with protocols in other layers might be tedious. performance might be better if an operation on data that need to be performed through multiple layers can be potentially reduced into an operation in one layer.

4.

(a)

internet protocol (IP) segmentation is a process that breaks packets into smaller pieces so that the maximum transmission unit (MTU, maximum data size that a link layer frame can carry) is smaller. different link layer protocols can have different MTUs, so fragment the data when a link layer frame is too big.

(b)

after segmentation, data is broken into 2 or more IP datagrams, each needs to be attached with a header (encapsulated). the header contains information such as destination address. fragments need to be reassembled before reaching transport layer of end host. the reassemble task can introduce more complication.

(c)

decreased throughput since data need to be reassembled, additional processing time of dealing with identification, flag, and fragmentation offset fields, and more storage space needed.

if 1 or more fragments is lost, original IP datagram is discarded and must be resent and fragmented again, taking more time.

5.

(a)

request for comments (RFC) is a series of memorandum published by internet engineering task force (IETF) that describes methods and research regarding internet and networked systems. It documents stages of standardization process of procedures and protocols.