

## Introduction

Can you explain the **TCP/IP stack**?

TCP – Transmission Control Protocol (Reliable)

The TCP/IP Stack, or the internet protocol suite, is a set of communication protocols used by the Internet or similar networks.

### TCP/IP Stack

- Application (e.g. FTP, SMTP, HTTP)
- Transport (TCP, UDP)
- Network (IP, routing protocols)
- Link (e.g. Ethernet, 802.111 (wifi), PPP)
- Physical (bits 'on the wire')
- Alternate: OSI model adds Presentation and Session layers between Application and Transport
- Data is encapsulated (message, segment, datagram, frame)

Can you compare the **packet switching** and **circuit switching** networks with a number of users?

**packet-switching**: hosts break application-layer messages into packets.

- forward packets from one router to the next, across links on path from source to destination
- each packet transmitted at full link capacity
- packet switching allows more users to use network!

**circuit switching**: end-end resources allocated to, reserved for "call" between source & destination.

- dedicated resources: no sharing
- circuit segment idle if not used by call (no sharing)

**Circuit switching** has fixed number of potential users, packet switching can have more users so long as they aren't all communicating at once.

### Packet switching:

- Better for 'bursty data'
- Can share resources
- Simpler (no call setup)
- Congestion is a problem (packet delay and loss)
- Protocols needed for reliable data transfer and congestion control

Can you calculate **various delays**?

## Application layer

Can you find and explain detailed information on a given **application message** (e.g., HTTP request/response, DNS request/response, DHCP)?

message formats:

- headers: fields giving info about data
- data: info(payload) being communicated

DHCP: Dynamic Host Configuration Protocol overview:

- host broadcasts "DHCP discover" msg [optional]
- DHCP server responds with "DHCP offer" msg [optional]
- host requests IP address: "DHCP request" msg
- DHCP server sends address: "DHCP ack" msg

Can you explain the request and response of **application messages**?

typical request/reply message exchange:

- client requests info or service
- server responds with data, status code

## Transport layer

The **TCP sliding windows** are byte oriented. What does this mean?

It means that the sequence and acknowledgement numbers refer to bytes instead of segments. For example, the value of the ack-field in a segment defines the number of the next byte a party expects to receive.

Can you explain the differences between **UDP and TCP**?

TCP is reliable between sending and receiving process, has flow control (won't overwhelm receiver), congestion control (throttle sender when network overloaded)

- Does not provide latency, minimum throughput guarantees or security
- 'Connection-oriented' – requires setup between client and server processes

UDP is unreliable between sending and receiving process

- Does not provide reliability, flow control, congestion control, throughput guarantee, security, connection setup

Security can be done at app layer using SSL/TLS

Give examples of applications where it is good to use **UDP and TCP** respectively.

UDP is a very simple protocol with minimal overhead. If a process wants to send a small message and does not care much about reliability, it can use UDP. Sending a small message using UDP takes much less interaction between sender and receiver than using TCP. UDP is used in multimedia and multicast applications, such as multiplayer games. If reliability is wanted on the other hand, TCP should be chosen. FTP and Telnet use TCP as transport layer protocol.

How does **TCP support reliable delivery of packets**? Briefly explain three mechanisms.

- SEQ & ACK
  - Messages can be confirmed as arrived safely
  - Resend if not!
- Checksum
  - Check that bits haven't been flipped
- Handshake
  - Check that server/host can facilitate comm.
- Window size
  - Advertise acceptable receive length! Don't overflow!

Can you explain how to guarantee **reliable delivery of application messages**?

- Deals with bit errors using checksums, and ACKs and possibly NAKs to ask for retransmission of erroneous packets
- Adds sequence number to deal with duplicates
- Deals with loss by waiting for a 'reasonable' time for the ACK, retransmitting if no ACK

Can you find information (port number, direction, application protocol etc) given **transport layer protocol header** (TCP or UDP) dump?

TCP Segment structure

- 16-bit source port #
- 16-bit dest port #
- 32-bit sequence #
- 32-bit ack #
- 16-bit flagset: header length, unused padding, URG, ACK valid, PSH, RST, SYN, FIN
- 16-bit receive window
- 16-bit internet checksum
- 16-bit URG data pointer
- Variable length options
- Variable length data

Can you calculate **checksum** and verify it?

UDP Checksum

- Goal: detect 'errors' (e.g., flipped bits) in transmitted segment
- Sender treats segment contents (inc. header fields) as sequence of 16-bit numbers
- Sender **calculates checksum by addition (one's complement sum) of segment contents**
- Sender puts the value into the checksum field
- Receiver computes checksum of segment
- Checks if computed checksum equals the checksum field value
- If not, errors detected
- If yes, no error detected (though errors could still have occurred)

Can you explain the differences between **flow control** and **congestion control**?

Flow control makes sure that the receive buffers aren't getting full, Congestion Control makes sure that the connection isn't getting full.

Flow control implements throttling the speed to prevent application buffer overflow

Congestion Control throttles speed to prevent the loss of packets in a congested network

What is the main **mechanism** used to implement TCP **flow control**?

Flow control mechanism is the receive window that the sender maintains for the receiver.

Describe one of the **mechanisms** that is used to implement TCP **congestion control**.

Congestion control mechanism is the congested packet telling not to send any more.

What is the difference between **connectionless** and **connection-oriented** transport layer protocols?

Connectionless: UDP: just send packets without init a connection, which is fast

Connection-oriented: TCP: handshake, agree on terms, reliable, slow

Mechanism or Protocol for **connectionless** transport?

UDP

Mechanism or Protocol for **connection-oriented** transport?

TCP

What is the difference between **confidentially** and **authentication** in secure data transport?

Confidentially: cannot determine who sent / who will recv / what data details.

Authentication: producing a certificate to allow for confidential transport -> is the person who they say they are.

Mechanism for **Confidentially**?

TLS/SSL

Mechanism for **Authentication**?

TLS/SSL (RSA checks)

## Network layer

Can you explain the **packet scheduling** in a router?

Can you explain the **packet fragmentation** and how it works?

Can you explain the differences between the **operation of distance vector and link-state routing algorithms**?

Link state routing protocols	Distance vector routing protocols
All routers have complete topology, link cost information	Routers know only physically connected neighbours and the link cost to them
The link costs are broadcast to all the routers in the network from a single controller	Requires an iterative process of computation, exchange of information with neighbours

In Distance-Vector, each node tells its neighbours everything it knows about the network. In Link-State, each router broadcasts the state of its own links to the entire network. Leaving each router to build up a graph of the network.

Describe one advantage of **link-state routing**.

LS has the advantage that it updates router's graphs quicker across the network because it broadcasts changes.

Describe one advantage of **distance-vector routing**.

DV advantage is that it uses less memory and CPU by not having to build up graphs, only populate a routing table

Given a network graph, can you make a table that contain the **minimum-cost routes** from a source node to all other nodes using **Dijkstra's algorithm** and **Distance Vector algorithm (Bellman-Ford algorithm)**, respectively?

Can you explain **NAT**?

NAT: network address translation

motivation: local network uses just one IP address as far as outside world is concerned:

- range of addresses not needed from ISP: just one IP address for all devices
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local net not explicitly addressable, visible by outside world (a security plus)

Can you explain the difference between **IPv4** and **IPv6**?

no fragmentation/reassembly allowed at intermediate routers:

- These operations can be performed only the source and destination.

ICMPv6:

- new version of ICMP
- additional message types, e.g. "Packet Too Big"
- multicast group management functions

Header checksum:

- removed entirely to reduce processing time at each hop
  - Since the IPv4 header contains a TTL field, the IPv4 header checksum needed to be recomputed at every router, a costly operation

options:

- No longer a part of the standard IP header.
- cf. IPv4 option: used for network testing, debugging, security, and more. This field is usually empty.

## Link layer

Can you explain how **odd/even parity bit** works? Can you find parity bit given binary digits? Can you explain the **2-D parity and its limitation**?

A parity bit is a check bit, which is added to a block of data for error detection purposes. It is used to validate the integrity of the data. The value of the parity bit is assigned either 0 or 1 that makes the number of 1s in the message block either even or odd depending upon the type of parity. Parity check is suitable for single bit error detection only.

The two types of parity checking are

Even Parity – Here the total number of bits in the message is made even.

Odd Parity – Here the total number of bits in the message is made odd.

**Two-Dimensional Parity** can detect as well as correct one or more-bit errors. If a one or more-bit error takes place then the receiver will receive the message with the changed parity bit. It indicates that some error has taken place which means the error is detected.

## DRAWBACKS

In some cases, an only odd number of bit errors can be detected and corrected but even number of errors can only be detected but not corrected.

In some cases, this method is not able to detect even no bit error.

Can you calculate/show how **CRC is used to detect error(s)**?

In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.

At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.

A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

Can you explain why **forward error correction (FEC)** is used? Can you show how **FEC is used to detect and/or correct error(s)**?

Forward Error Correction (FEC) is a technique used to minimize errors in data transmission over communication channels. In real-time multimedia transmission, re-transmission of corrupted and lost packets is not useful because it creates an unacceptable delay in reproducing: one needs to wait until the lost or corrupted packet is resent. Thus, there must be some technique which could correct the error or reproduce the packet immediately and give the receiver the ability to correct errors without needing a reverse channel to request re-transmission of data.

- **Reduce retransmission on error**
- **Increase reliability of wireless systems**

Using Hamming Distance:

For error correction, the minimum hamming distance required to correct  $t$  errors is:

$$d_{\min} = 2t + 1$$

For example, if 20 errors are to be corrected then the minimum hamming distance must be  $2 \times 20 + 1 = 41$  bits. This means, lots of redundant bits need to be sent with the data. This technique is very rarely used as we have large amount of data to be sent over the networks, and such a high redundancy cannot be afforded most of the time.

Can you explain **MAC address**? Can you find relevant information given **MAC address**?

MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers

- Logical Link Control (LLC) Sublayer
- Media Access Control (MAC) Sublayer

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is worldwide unique, since millions of network devices exists, and we need to uniquely identify each. Function: used 'locally' to get frame from one interface to another physically connected interface (same network, in IP-addressing sense)

The first six digits (called the "prefix") represent the adapter's manufacturer, while the last six digits represent the unique identification number for that specific adapter. The MAC address contains no information about which network a device is connected to.

Can you explain how **MAC addresses/IP addresses** are used in a **LAN** and between different LANs?

MAC addresses are the low-level basics that make your local ethernet based network work. Local means that the network devices are either directly connected through a cable or by WiFi or over a network hub or network switch.

Network cards each have a unique MAC address. Packets that are sent on the ethernet are always coming from a MAC address and sent to a MAC address. If a network adapter is receiving a packet, it is comparing the packet's destination MAC address to the adapter's own MAC address. If the addresses match, the packet is processed, otherwise it is discarded.

How do IP addresses and MAC addresses work together?

IP is a protocol that is used on a layer above ethernet. Another protocol for example would be IPX. IP allows connecting of different local networks and thus forming a corporate network or the global internet.

When your computer wants to send a packet to some IP address  $x.x.x.x$ , then the first check is if the destination address is in the same IP network as the computer itself. If  $x.x.x.x$  is in the same network, then the destination IP can be reached directly, otherwise the packet needs to be sent to the configured router.

Up to now things seem to have gotten worse, because now we have two IP addresses: one is the original IP packet's target address, the other is the IP of the device to which we should send the packet (the next hop, either the final destination or the router).

Since ethernet uses MAC addresses, the sender needs to get the MAC address of the next hop. There is a special protocol ARP (address resolution protocol) that is used for that. Once the sender has retrieved the MAC address of the next hop, he writes that target MAC address into the packet and sends the packet.

Can you explain the **MAC protocols** and their differences (e.g., CSMA)?

channel partitioning, by time, frequency, or code

- Time Division, Frequency Division

random access (dynamic),

- ALOHA, S-ALOHA, CSMA, CSMA/CD
- carrier sensing: easy in some technologies (wire), hard in others (wireless)
- CSMA/CD used in Ethernet
- CSMA/CA used in 802.11

taking turns

- polling from central site, token passing
- Bluetooth, FDDI, token ring

Describe the key difference between **CSMA/CD** and **CSMA/CA** media access protocols.

Key	CSMA/CA	CSMA/CD
Effectiveness	CSMA/CA is effective before a collision.	CSMA/CD is effective after a collision.
Network Type	CSMA/CA is generally used in wireless networks.	CSMA/CD is generally used in wired networks.
Recovery Time	CSMA/CA minimizes the risk of collision.	CSMA/CD reduces recovery time.
Conflict Management	CSMA/CA initially transmits the intent to send the data, once an acknowledgment is received, the sender sends the data.	CSMA/CD resends the data frame in case a conflict occurs during transmission.
IEEE Standards	CSMA/CA is part of the IEEE 802.11 standard.	CSMA/CD is part of the IEEE 802.3 standard.
Efficiency	CSMA/CA is similar in efficiency as CSMA.	CSMA/CD is more efficient than CSMA.

Give an example of a link layer protocol that uses **CSMA/CD (carrier sense multiple access with collision detection)**.  
802.3 (Ethernet)

Give an example of a link layer protocol that uses **CSMA/CA (carrier sense multiple access with collision avoidance)**.  
802.11 (wireless) since we cannot be fully sure of collisions

Can you explain how **VLAN** is working?

switch(es) supporting VLAN capabilities can be configured to define multiple virtual LANS over single physical LAN infrastructure.

Can you explain how **MPLS** is working?

is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows.

What is difference between **collision detection** and **collision avoidance** in link layer protocols?

CD: detect collision and stop transmission algorithmically (CSMA/CD)

CA: check channel clear before transmission

Mechanism for **Collision Detection**?

CSMA/CD

## Relevant questions in the past final exam

- 2020 final exam
  - Q4, Q5, Q12,
- 2019 final exam
  - Q4, Q6, Q7, Q9
- The past exams are available at:
  - 2018 final exam: Q2(a), Q3, Q5
  - 2017 final exam: Q1(a), Q2, Q4(e)&(f)

Minus:  $15 - (40 - (59/100 * 20 + 80.7647/100 * 20)) = 2.95294$

Minus In final:  $(15 - (40 - (59/100 * 20 + 80.7647/100 * 20))) / 60 * 100 = 4.92156666667$

## Mock - COMS3200 Semester One Final Examination 2021

**QUESTION 1 {Transport layer}** The following is a dump (contents) of a **UDP header** in hexadecimal format.

E555 0015 0040 3A6B

(a) What is the **source port** number in decimal form? Show your working in the working sheet.  $E555_{16} = 58709$

(b) What is the **destination port** number? Show your working in the working sheet.  $0015_{16} = 21$

(c) What the **total length of the user datagram** in bits? Show your working in the working sheet.

$0040_{16} = 64 \text{ bytes} = 64 * 8 = 512 \text{ bits}$

(d) What is the **length of the data** in bytes? Show your working in the working sheet.

Since the header is 8 bytes the data length is  $64 - 8 = 56 \text{ bytes}$ .

(e) What is the **checksum value** in hexadecimal form? 3A6B

(f) Is this packet directed from a client to a server or vice versa? A client to a server

(g) What is the **application-layer protocol**? DNS

The following is a dump (contents) of a **TCP header** in hexadecimal format.

a      b      c      d      e      f      g

E293 0017 00000001 00000000 5 002 07FF ...

(a) What is the **source port** number?  $(E293)_{16} = 58,003$

(b) What is the **destination port** number?  $(0017)_{16} = 23$

(c) What is the **sequence number**?  $(00000001)_{16} = 1$

(d) What is the **acknowledgment number**?  $(00000000)_{16} = 0$

(e) What is the **length** of the header? The HLEN = 5. The header is  $5 \times 4$  (scaling factor) = 20 bytes long

(f) What is the **type of the segment**?

$(002)_{16} = (000000000010)_2$  the right most 6 bits are 000010, which means only the SYN bit is set. This is the SYN segment used for connection establishment.

g. What is the **window size**?  $(07FF)_{16}$  or 2047 in decimal. The window size is 2047 bytes.

## QUESTION 3 {Quantitative Comparison of Packet Switching and Circuit Switching}

Consider the two scenarios below: a circuit-switching scenario in which **Ncs** users, each requiring a bandwidth of **10 Mbps**, must share a link of capacity **50 Mbps**. A packet-switching scenario with **Nps** users sharing a **50 Mbps** link, where each user again requires **10 Mbps** when transmitting, but only needs to transmit 30 percent of the time.

(a) When **circuit switching** is used, what is the maximum number of circuit-switched users that can be supported?



### (Circuit users can't share bandwidth)

For each of the user is allocated 10mbps bandwidth and given link capacity is 50mbps.  $50/10 = 5$

For the remainder of this problem, suppose packet switching is used.

(b) Suppose there are 10 packet-switching users (i.e.,  $N_{ps} = 10$ ). What is the probability that a given (specific) user is transmitting, and the remaining users are not transmitting? **(How much bandwidth does each user need? Is this less than the total bandwidth?)**

The probability that a specific user is transmitting,  $p$ , is the percent of the time it is transmitting, i.e. 0.3.

The probability that a specific user is not busy is  $(1 - p)$ .

The probability that the  $N_{ps} - 1$  users are not transmitting is  $(1-p)^{N_{ps}-1}$ .

Thus, the probability that one user is transmitting, and the other users are not transmitting is,  $p^1(1-p)^{10-1}=0.3 \times 0.7^9=0.0121060821$

(c) What is the probability that one user (any one among the 10 users) is transmitting, and the remaining users are not transmitting?

The probability that exactly one (any one) of the  $N_{ps}$  users is busy is  $N_{ps}$  times the probability that a given specific user is transmitting and the remaining users are not transmitting (our answer to (c) above), since the one transmitting user can be any one of the  $N_{ps}$  users.

Therefore, the fraction of the link used when a user is using the link (and the remaining users aren't transmitting) is,  $N_{ps} * p^1 * (1-p)^{N_{ps}-1} = 10 \times 0.3^1 \times 0.7^9 = 0.121060821$

(d) What is the probability that any 6 users (of the total 10 users) are transmitting and the remaining users are not transmitting? ( $C(n, k) = n! / [(n-k)! k!]$ )

Using the formula  $p^n(1-p)^{N_{ps}-n}$  we can find the probability that  $n$  specific users are transmitting and  $N_{ps} - n$  users are not.

To find the probability that any  $n$  (6 in this case) out of the 10 possible users, are transmitting is choose  $(10, n) * p^n(1-p)^{N_{ps}-n}$

$C(10, 6) * p^6(1-p)^{10-6} = 10! / ((10-6)! \times 6!) \times 0.3^6 \times 0.7^4 = 0.036756909$

(e) What is the probability that more than 4 users are transmitting?

The probability that more than 4 users are transmitting is

$$\sum_{n=5}^{10} \binom{10}{n} p^n (1-p)^{N_{ps}-n} = \sum_{n=5}^{10} \frac{10!}{((10-n)! * n!)} * 0.3^n * 0.7^{10-n} = 0.15026833$$

### QUESTION 4 {HTTP GET}

Suppose that a server receives the following **HTTP GET** message from a client browser:

```
GET /main/test1.html HTTP/1.1 \r\n
Host: www.uq2.edu.au \r\n
User-agent: Firefox/3.6.12 \r\n
Accept: text/html, application/xhtml+xml \r\n
Accept-language: en, fr; q = 0.8, en-nz; q = 0.5 \r\n
Accept-Encoding: gzip, deflate \r\n
Connection: close \r\n
\r\n
```

(a) What is the **name of the file** that is being retrieved in this GET message? Please use file name only.

test1.html (location: /main/)

(b) What **version of HTTP protocol** does the browser use? Please use only number.

1.1

(c) What is the **language preference** of the browser user mostly preferring to use?



English

(d) Does the browser want to have **persistent connections**? Answer Yes, No or Undecidable.

No

(e) Assume that the browser has received "internal server error" from the web server. What is response code for it? Please provide the numerical value.

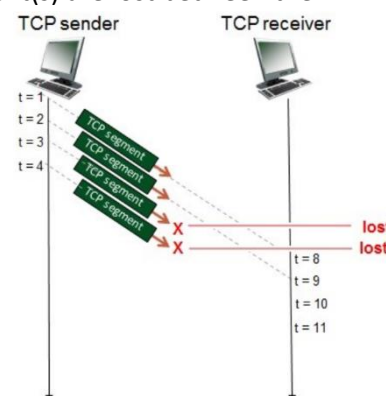
500 (<https://dynamapper.com/blog/254-the-6-types-of-http-status-codes-explained>)

**QUESTION 5** Consider a scenario that TCP a sender and receiver communicate over a connection in which the sender-to-receiver segments may be lost in Figure 1. The TCP sender sends initial window of four segments at  $t=1,2,3,4$ , respectively. Suppose the initial value of the sender-to-receiver sequence number is 116 and the **first four segments each contain 502 bytes**. The **delay between the sender and the receiver is 7-time units**, and so the first segment arrives at the receiver at  $t=8$ . As shown in the figure, two of the four segment(s) are lost between the sender and the receiver.

Figure 1. TCP sequence and ACK numbers with segment loss

Answer the following questions (2 marks each) in the table below:

- Fill in the sequence numbers associated with the segments sent by the sender.
- Fill in the time the segments were received.
- Fill in the acknowledgment field of each receiver-to-sender acknowledgment and give a brief explanation as to why that particular acknowledgment number value is being used.



Sender-to-Receiver	Time segment sent	Sender-to-receiver segment sequence number field value	Time segment received, and ACK segment sent	Receiver-to-sender ACK field value
Segment 1	1	116	8	618
Segment 2	2	618	9	1120
Segment 3	3	1120	-	No ACK is sent, since this segment was lost
Segment 4	4	1622	-	No ACK is sent, since this segment was lost

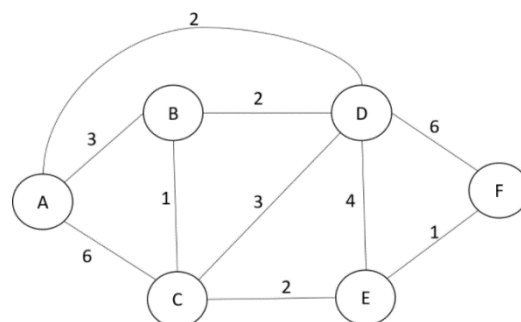
## QUESTION 6

Figure 2. An example network 1

(a) (10 marks total) Apply the **Dijkstra algorithm** on the example network 1 in Figure 2 to find the minimum-cost routes from **station A** to all other stations. Please make a table for the final value. S is the set of stations whose least-cost path is known;  $D(v)$  is the current cost of path from source (i.e., station 1) to station  $v$ ;  $p(v)$  is the predecessor station along path from source to  $v$ , that is next to  $v$ .

Please use "inf" to specify an infinite cost and "-" to specify no predecessor respectively.

The following table has not been completed filled on purpose. 'X' is used to indicate that that cell will be filled with information.



Step	S	D(B), p(B)	D(C), p(C)	D(D), p(D)	D(E), p(E)	D(F), p(F)
0	A	3, A	6, A	2, A	inf,-	inf,-
1	X	3, A	5, D	X	X	X
2	X	X	4, B	X	6, D	X
3	X	X	X	X	X	X
4	X	X	X	X	X	7, E
5	ABCDEF	X	X	X	X	X

**(b)** Apply the **Bellman-Ford algorithm** on the example network 1 given in Figure 2 to find the minimum-cost routes from **station B** to all other stations.

Please use "inf" to specify an infinite cost and "-" to specify no next hop respectively.

The following table has not been completed filled on purpose. 'X' is used to indicate that that cell will be filled with information.

Dest.	Hop 1		Hop 2		Hop 3		Hop 4		Hop 5	
	cost	hop	cost	hop	cost	hop	cost	hop	cost	hop
A	3	A	X	X	X	X	X	X	X	X
C	1	C	X	X	X	X	X	X	X	X
D	2	D	X	X	X	X	X	X	X	X
E	inf	-	3	C	X	X	X	X	X	X
F	inf	-	8	X	4	X	X	X	X	X

**QUESTION 789** [IP/subnet] Please choose which **class** the following IPv4 Address belongs to.

192.168.1.2 - **Class C**

2.2.2.2 - **Class A**

223.265.200.1 - **invalid IP address**

**QUESTION 10** Suppose an ISP owns the block of addresses of the form for IP address 224.1.1.1/24. Suppose it wants to create four subnets from this block, with each block having the same number of IP addresses. What is the **total number of usable hosts**? Show your works on the working sheet.

224.1.1.1: 11100000.00000001.00000001.00000001

The first 24 bits are fixed, and last bit is also fixed as 1, so only  $2^7$  total number of available hosts and 2 is 2 reserved addresses. the **total number of usable hosts is therefore  $2^7(128) - 2 = 126$**

**QUESTION 11** Your company wants to utilize the private **class C** IP Address of 192.164.1.0. You are tasked with subnetting the address to get the most networks with at least 30 hosts per subnet. How many networks will be created after you complete subnetting?

<https://www.calculator.net/ip-subnet-calculator.html?cclass=c&subnet=27&ip=192.164.1.0&ctype=ipv4&printit=0&x=62&y=20>

192.164.1.0 = 11000000.10100100.00000001.00000000

Bits needs for 30 hosts = 5 =  $2^5 = 32-2=30$  possible hosts.

Bits left for subnets = 3 =  $2^3 = 8$  possible subnets.

**QUESTION 12** Your company wants to utilize the private **class C** IP Address of 192.164.1.0. You are tasked with subnetting the address to get the most networks with at least 30 hosts per subnet.

What is the first usable IP Address in the 1st Network range?

Our second step will be to calculate the new subnet mask, our previous subnet mask was 255.255.255.0 or 11111111.11111111.11111111.00000000 in binary. Since we have borrowed 3 bits from the host portion our new subnet mask will be 11111111.11111111.11111111.11100000 which is 255.255.255.224 when converted to decimal notation.

First network .0 to .31 first useable .1

Second network .32 to .63 first useable .33

192.164.1.1

**QUESTION 13** Figure 3 shows a Wireshark screen shot that analyses the trace of a TCP segment sent and received directly by uploading a 150KB text file from a computer to a remote server.

The six segments sent by the client (192.168.1.102) to the server (128.119.245.12) are No. 4, 5, 7, 8, 10, and 11 (these are marked in a red highlighted box).

Figure 3. a Wireshark screenshot

1	0.000000	192.168.1.102	128.119.245.12	TCP
2	0.023172	128.119.245.12	192.168.1.102	TCP
3	0.023265	192.168.1.102	128.119.245.12	TCP
4	0.026477	192.168.1.102	128.119.245.12	TCP
5	0.041737	192.168.1.102	128.119.245.12	TCP
6	0.053937	128.119.245.12	192.168.1.102	TCP
7	0.054026	192.168.1.102	128.119.245.12	TCP
8	0.054690	192.168.1.102	128.119.245.12	TCP
9	0.077294	128.119.245.12	192.168.1.102	TCP
10	0.077405	192.168.1.102	128.119.245.12	TCP
11	0.078157	192.168.1.102	128.119.245.12	TCP
12	0.124085	128.119.245.12	192.168.1.102	TCP
13	0.124185	192.168.1.102	128.119.245.12	TCP
14	0.169118	128.119.245.12	192.168.1.102	TCP
15	0.217299	128.119.245.12	192.168.1.102	TCP
16	0.267802	128.119.245.12	192.168.1.102	TCP
17	0.304807	128.119.245.12	192.168.1.102	TCP
18	0.305040	192.168.1.102	128.119.245.12	TCP

(a) Considering the difference between when each TCP segment was transmitted and when its acknowledgement was received, what is the **Round-Trip Time (RTT)** value of the second of the six segments?

$0.077294(\text{no.9}) - 0.041737(\text{no.5}) = 0.035557$

(b) What is the EstimatedRTT of the second segment after receiving the ACK? Assume that the EstimatedRTT equal to the measured the **Round-Trip Time (RTT)** for the first segment.

$\text{EstimatedRTT} = (1 - \alpha) * \text{EstimatedRTT} + \alpha * \text{SampleRTT}$  with  $\alpha$  is 0.125

$= 0.875 \times (0.053937 - 0.026477) + 0.125 \times 0.035557$

$= 0.028472125$

**QUESTION 14 {Error detection and correction}**

(a) What is the Internet checksum value for these two 16-bit words (use one's compliment addition).

Answer it without space between binary digits.

1000 0110 0101 1110  
1010 1100 0110 1000

Step 1. Add the two numbers

$= (+1) 0011 0010 1100 0110$

Step 2. Carry over the overflow

$= 0011 0010 1100 0111$

Step 3. Compute one's complement

$= 1100 1101 0011 1000$

(b) What is the parity bit for 0100111 when the **odd** one-dimensional parity scheme?

1

(c) What is the parity bit of 1100110 when the **even** one-dimensional parity scheme?

0

(d) The two-dimensional (2D) **even** parity scheme is used for the following data:

01110 01010 01001 11001

Suppose that 5 bits are used in one row for the 2D parity. What are the first four parity bits in the column only?

011101

010100

010010

110011

101000

For  $k=2$  and  $n=4$ , we can make the following assignment.

No	Data Block	Codeword
1	00	0001
2	01	0011
3	10	1000
4	11	1110

(e) What is the **minimum Hamming distance** when a codeword block is received with the bit pattern 1001?

1

(f) Can the error be detected (Yes or no) when the received codeword is 1101? Choose one: Yes, No or Undecidable.

Yes, the error can be detected since 1101 is not a valid codeword.

To guarantee the detection of up to  $s$  errors in all cases, the minimum Hamming distance in a block code must be  $d_{\min} = s + 1$ .

(g) Can the error be corrected when the received codeword is 1001? Choose one: Yes, No or Undecidable.

No. If flip one bit, it could be case 1 or 3.

To guarantee correction of up to  $t$  errors in all cases, the minimum Hamming distance in a block code must be  $d_{\min} = 2t + 1$ .

## 2019 Q1 [HTTP GET]

*GET /kurose\_ross/interactive/quotation4.htm HTTP/1.1*

*Host: www.univ1.edu.au*

*Accept: text/plain, text/html, image/jpeg, image/gif, audio/mp4, audio/vnf.wave, video/mp4, video/mpeg, application/\*, \*/\**

*Accept-Language: en-us, en-gb;q=0.5, en;q=0.4, fr, fr-ch, zh, fi*

*If-Modified-Since: Thu, 25 April 2019 15:20:19 -0700*

*User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_7\_3) AppleWebKit/534.53.11 (KHTML, like Gecko)*

*Version/5.1.3 Safari/534.53.10*

Q1-1. What is the name of the file that is being retrieved in this GET message? [quotation4.htm](#)

Q1-2. What formats of text, images, audio, and video does the client browser prefer to receive?

[Plaintext, HTML text, jpeg, gif, mp4 of video and audio, vnf.wave, mpeg, any application, anything of any type](#)

Q1-3. Does the browser sending the HTTP message prefer Swiss French over traditional French? Explain

[No. both have equal q values \(none supplied\) default =1. So, both are accepted](#)

Q1-4. Does the client already have a (possibly out-of-date) copy of the requested file? Explain. If so, approximately how long ago did the client receive the file, assuming the GET request has just been issued?

[Yes, presence of if-modified-since indicates that file already present. So, received on 25<sup>th</sup> April 2019.](#)

## Question 2. [HTTP Response]

*HTTP/1.1 404 Not Found*

*Date: Mon, 24 Sep 2018 22:23:34 +0000*

*Server: Apache/2.2.3 (CentOS)*

*Content-Length: 74396*

*Keep-Alive: timeout=39, max=82*

*Connection: Keep-alive*

*Content-type: image/html*

Q2-1. Was the server able to send the document successfully? Explain.

[No. 404 error indicates of resource requested not existing without the server.](#)

Q2-2. When was the file last modified on the server? [Never, it doesn't exist / has no memory.](#)

Q2-3. What is the type of file being sent by the server in response? [Image/html](#)

Q2-4. What is the default mode of connection for HTTP protocol? Is the connection in the reply persistent or non-persistent? Explain. [1.1/persistence is default. Connection is persistent we have keep-alive message, which means multiple objects sent over 1 TCP connections/handshake.](#)

**Question 5. [IP/subnet]** Suppose an ISP (internet service provider) owns the block of addresses of the form 101.101.128/17. Suppose it wants to create **four subnets** from this block, with each block having the same number of IP addresses.

Q5-1. What is the **maximum number of hosts** can be connected to each subnet? Show your works.

[101. 101. 128/17](#)

[01100001.01100101.10000000.00000000](#)

[So, 15 bits for hosts for 4 groups equally sized](#)

[2<sup>15</sup> IP = 32768 machines](#)

[/4 = 8192 machines per group – 2 \(broadcast, gateway\), so, 8190 hosts on each subnet](#)

Q5-2. What are the prefixes (of the form a.b.c.d/x) for the four subnets?

[101.101.128.0/19](#)

[101.101.160.0/19](#)

101.101.192.0/19

101.101.224.0/19

#### Question 6. [Checksum]

Q6-1. If the Internet **checksum** method is adopted, what message will be sent if data is 5AD3EE35? If the message received is 59D4 EF35 B6F6, will the message be accepted? (Show your workings.)

Data = 5AD3 EE35 (16 bits 1s comp sum) 00014908 -> 4909 flip: B6F6

Sent: 5AD3 EE35 B6F6

Recv: 59D4 EF35 B6F6

Not same. Not accepted

**Question 9. [MAC address]** The following is an example MAC address. 00: A0:C9:14:C8:29

Q9-1. Write down the part in hexadecimal indicating the adapter's manufacturer.

00: A0:C9

Q9-2. What protocol is used to find an IP address given a MAC address of a device?

ARP

#### 2017 Q2

The following table describes the **purpose of different networking protocols**. For each of these protocols, give the acronym (abbreviated name) of the relevant protocol, and the relevant layer of the Internet protocol stack. If more than once correct answer is possible, then any correct answer will be accepted.

Purpose of the Protocol	Name	Layer
To request and receive web pages from a server	HTTP	Application
Convey network management control and information messages	SNMP	Application
Send email messages to mail server	SMTP	Application
Download email messages from a mail server	IMAP/POP3	Application
Used by hosts and routers to communicate network-level information	ICMP	Network
Convert a hostname to an IP address	DNS	Application
get the MAC address corresponding to an ID -> next to forward to!	ARP	Link
7. Sending intra-AS link-state routing messages	OSPF/IS-IS	Link
8. Setting up multimedia data stream connections	TCP	Transport
9. Providing connectivity between hosts and access points in WiFi networks	802.11?	Link/Physical?
An enhanced version of connection-oriented stream transport which adds security	QUIC	Transport
Communication security. Privacy for data.	SSL	Application
Exchange routing info between AS	BGP	Application
Ethernet – physical conn between hubs, switches & routers	IEEE 802.3	Physical

## Tutorial questions for Chapter 1.

Expected time to complete: 2 weeks or less.

Simple questions:

Please answer the following questions:

1. What is internet? Briefly define it with one or two sentences.

The internet is a **network of networks**, where billions of hosts are connected to networks, which are connected to ISPs. These ISPs are interconnected to form the internet as we know it.

2. What are the examples of hosts? List 3-4 examples of hosts.

A host is an end system, that may be a computer or a device which communicates with other hosts over a network. Ex: computers, smartphones, IoT devices, routers, servers (basically any device on the network that has an IP)

3. Briefly define the meaning of a protocol in computer network.

Protocols define **the format, order of messages sent and received** among network entities, and **actions taken on message transmission, receipt, errors or other states** (for example congestion, loss, disconnect).

4. What are the differences between packet switching and circuit switching? Explain at least two differences between them.

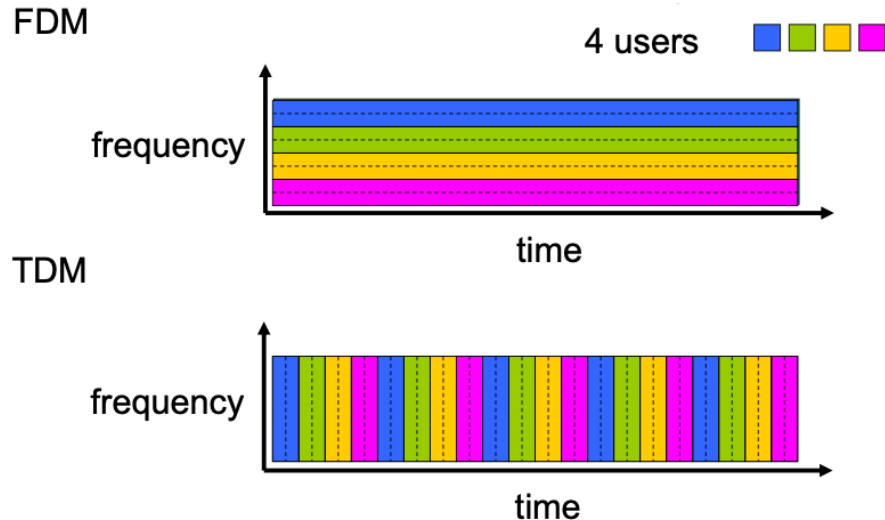
Packet switching	Circuit Switching
A block of data is split into pieces (packets) and addressed individually and switched at routers to the final destination where they are assembled into the original data block.	The circuit pathways are connected from sender to receiver to form a dedicated reserved pathway for the data similar to a pipeline. The data block flows along this pipeline.
<ul style="list-style-type: none"><li>• Packets arrive out of order</li><li>• Uses less resources</li><li>• Is more resilient as it can take least congested pathways</li><li>• Lost packets require smaller re-transmissions</li><li>• Can result in high jitter</li></ul>	<ul style="list-style-type: none"><li>• Packets come in order</li><li>• The whole pathway is reserved</li><li>• A broken pathway results in the whole connection needing to be re-established</li><li>• Path establishment is an expensive (time, cpu)</li><li>• Very little jitter and guaranteed performance</li></ul>

5. What is the difference between FDM and TDM?

Frequency Division Multiplexing – The available bandwidth is separated into frequency bands (slots) that do not overlap, each carrying an individual signal. (All senders get a smaller separate sub range to use simultaneously)



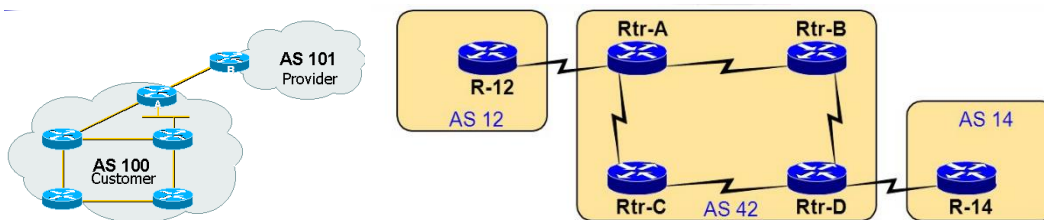
Time Division Multiplexing – The signals are sent over the available bandwidth according to time divisions, that dictate when to start sending and stop sending a signal. (The whole channel is allocated fully to each sender for a small time slice, over and over)



6. What are the three types of autonomous systems in computer networking?

AS : is a portion of a large internetwork that is under a given administrative authority ( Ex: UQ)

- Stub AS : AS is connected to only one other AS. (Ex: AS100)
- Transit AS : Connected to more than one other AS. Can be used for transit traffic between autonomous systems (Ex: AS42)
- Multi-homed AS : Connected to more than one other AS but does not let transit traffic from another AS pass through itself. An example might be a corporate network with several Internet connections to different ISPs.



7. What are the reasons to use layering for Internet protocol stack (e.g., TCP/IP)? Briefly discuss how (in)efficient it will be if the information represented in internet protocol stack (TCP/IP) stack is represented in one layer.

In TCP/IP each layer is defined according to a specific function to perform. All layers work collaboratively to transmit the data from one layer to another. Thus, layers facilitate :

- Understanding and dealing with well-defined, specific part of a large and complex system
- One or more protocol standards can be developed at each layer

- As the functions of each layer are well defined, standards can be developed independently and simultaneously for each layer. This speed up the standards-making process
- Simplification for modularity for vendors, developers and users and
- Interoperability ( ex: TCP or UDP, Fibre or Cable)
- Ease of changing implementation of the service provided by the layer
- Ease of Incorporation of new technologies (such as Wi-Fi when they arrive) and standards
- As long as the layer provides the same service to the layer above it and uses the same services from the layer below it, the remainder of the system remains unchanged when a layer's implementation is changed."

Calculation questions:

8. Please show an example of how to calculate packet transmission delay with your own numbers.

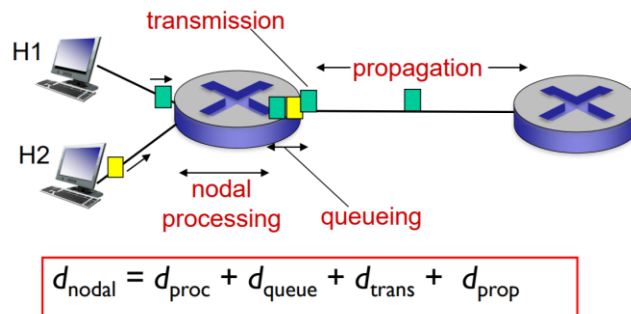
Packet transmission delay is the

$$d_{trans} = \text{time needed to transmit } L - \text{bit packet into link} = \frac{L \text{ (bits)}}{R \text{ (bits/sec)}} = \frac{8 * 2}{5} = 3.2 \text{ s}$$

Therefore, for a packet of 2 bytes (16 bits) to be sent on a link of rate 5 bits/sec, 3.2 sec would be the resulting packet transmission delay.

[Based on **Introduction 1-18** in "Chap1 - Computer Networks & the Internet"]

9. Define a nodal delay with four sources of packet delay in an equation; show an example with numbers that generated by your own.



If

$d_{proc}$ , time taken by the first router to process each packet, is 2 secs.  
 $d_{queue}$ , is not applicable since there is no queueing at the out link of the first router.

$L$ , packet size, 8 bits

$R$ , rate of transmission, is 4 bits/sec

$$d_{trans} = \frac{L}{R} = \frac{8 \text{ bits}}{4 \text{ bits/sec}} = 2 \text{ secs}$$

$d$ , length of the link between the two routers is, 2000m  
 $s$ , propagation speed is,  $2 \times 10^8 \text{ m/s}$

$$d_{proc} = \frac{d}{s} = 1 \times 10^{-5} \text{ s}$$

$$\text{Therefore, } d_{nodal} = 2 + 0 + 2 + 0.00001 = 4.00001 \text{ s}$$

The nodal delay may be different if there are more packets to be sent across the link ( this may result in packets waiting their turn to be put on the link, this  $d_{queue} \neq 0$  ), between the two routers, but for one packet under those conditions,  $d_{nodal}$  is 4.00001 seconds.

#### 10. Quantitative Comparison of Packet Switching and Circuit Switching

(Refer to the slide [01\_COMNET1\_Chap1 – sup]):

Consider the two scenarios below: A circuit-switching scenario in which  $N_{cs}$  users, each requiring a bandwidth of 15 Mbps, must share a link of capacity 250 Mbps. A packet-switching scenario with  $N_{ps}$  users sharing a 250 Mbps link, where each user again requires 12 Mbps when transmitting, but only needs to transmit 25 percent of the time.

- a. When circuit switching is used, what is the maximum number of circuit-switched users that can be supported? Explain your answer.

When circuit switching is used,  $\frac{250 \text{ Mbps}}{15 \text{ Mbps}} = 16.6667 \approx 16$  users can be supported at a time.

- b. For the remainder of this problem, suppose packet switching is used. Suppose there are 45 packet-switching users (i.e.,  $N_{ps} = 45$ ). Can this many users be supported under circuit-switching? Explain.

No, because under circuit switching, each one of the 45 users will need to be allocated 15Mbps, or an aggregate of 675 Mbps (much more than 250 Mbps link size).

- c. What is the probability that a given (specific) user is transmitting, and the remaining users are not transmitting?

- The probability that a specific user is transmitting,  $p$ , is the percent of the time it is transmitting, i.e. 0.25.
- The probability that a specific user is not busy is  $(1 - p)$ .
- The probability that the  $N_{ps} - 1$  users are not transmitting is  $(1 - p)^{N_{ps}-1}$ .
- Thus, the probability that one user is transmitting, and the other users are not transmitting is,  $p^1(1 - p)^{45-1} = 0.25 * 0.75^{44} = 7.954916e - 7$

Ans -  $7.954916e-7$

- d. What is the probability that one user (any one among the 45 users) is transmitting, and the remaining users are not transmitting? When one user is transmitting, what fraction of the link capacity will be used by this user?

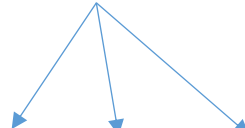
- The probability that exactly one (*any* one) of the  $Nps$  users is busy is  $Nps$  times the probability that a given specific user is transmitting and the remaining users are not transmitting (our answer to (c) above), since the one transmitting user can be any one of the  $Nps$  users.
  - Therefore, the fraction of the link used when a user is using the link (and the remaining users aren't transmitting) is,
    - $Nps \cdot \rho^1 \cdot (1 - \rho)^{Nps-1} = 45 * 0.25^1 * 0.75^{44} = 0.00003579712$
- e. What is the probability that any 25 users (of the total 45 users) are transmitting and the remaining users are not transmitting? (Hint: you will need to use the binomial distribution).
- Using the formula  $\rho^n (1 - \rho)^{Nps-n}$  we can find the probability that  $n$  specific users are transmitting and  $Nps - n$  users are not.
  - To find the probability that any  $n$  (25 in this case) out of the 45 possible users, are transmitting is  $\text{choose}(45, n) * \rho^n (1 - \rho)^{Nps-n}$ 
    - $c(45, 25) * \rho^{25} (1 - \rho)^{45-25} = c(45, 25) * 0.25^{25} * 0.75^{20} = 0.00000892826$
- f. What is the probability that more than 25 users are transmitting?  
The probability that more than 25 users are transmitting is
- $$\sum_{i=26}^{45} \text{choose}(45, n) * \rho^n (1 - \rho)^{Nps-n} = 0.0000029686$$
- g. Comment on what this implies about the number of users supportable under circuit switching and packet switching.
- With packet switching, more than thrice the number of users can be accommodated on the same link (with capacity of 250Mbps) as compared to circuit switching, with a small probability of collisions. This is given that packet switching users are using 12 Mbps of the link 25% of the time and circuit switching users are using 15Mbps.
  - In packet switching 26-45 users may transmit at the same time with a probability of  $2.9686 \times 10^{-6}$ . In circuit switching, only 16 users may be accommodated at a time.

## Practice questions

11. Run a traceroute program (Windows or linux) for a specific site (e.g., google.com) and find the information highlighted on the page 1-49 of the slide [01\_COMNET1 Chap1].

Traceroute: [www.telstra.net](http://www.telstra.net) to [www.tum.de](http://www.tum.de)

3 delay measurements from telstra.net to  
gigabitethernet3-3...melbourne.telstra.net



```
1  gigabitethernet3-3.exi1.melbourne.telstra.net (203.50.77.49)  0.302 ms  0.266 ms  0.244 ms
2  bundle-ether3-100.exi-core10.melbourne.telstra.net (203.50.80.1)  2.987 ms  1.418 ms  2.242 ms
3  bundle-ether12.chw-core10.sydney.telstra.net (203.50.11.124)  14.107 ms  14.410 ms  12.359 ms
4  bundle-ether1.oxf-gw11.sydney.telstra.net (203.50.6.93)  13.608 ms  12.286 ms  13.109 ms
5  bundle-ether1.sydo-core03.sydney.reach.com (203.50.13.98)  13.359 ms  14.286 ms  12.734 ms
6  i-10403.sydo-core04.telstraglobal.net (202.84.222.130)  14.361 ms  12.407 ms  12.735 ms
7  i-10604.1wlt-core02.telstraglobal.net (202.84.141.225)  155.528 ms  154.704 ms  153.903 ms
8  i-93.tlot02.bi.telstraglobal.net (202.84.253.86)  154.526 ms  153.705 ms  153.779 ms
9  8-3-2.edge1.LosAngeles6.Level3.net (4.68.70.69)  153.277 ms
10 ae-1-5.bar1.Hamburg1.Level3.net (4.69.142.209)  297.623 ms  297.578 ms  297.562 ms
11 195.122.181.62 (195.122.181.62)  298.318 ms  298.619 ms  297.946 ms
12 cr-han2-be3.x-win.dfn.de (188.1.144.38)  302.434 ms  302.236 ms  302.312 ms
13 cr-fra2-be12.x-win.dfn.de (188.1.144.133)  307.188 ms  307.345 ms  307.565 ms
14 cr-gar1-be6.x-win.dfn.de (188.1.145.230)  316.055 ms  315.608 ms  315.932 ms
15 kr-gar188-0.x-win.dfn.de (188.1.37.90)  316.178 ms  315.728 ms  316.056 ms
```

Trans-oceanic link



Note: (via <https://www.tolaris.com/2008/10/09/identifying-undersea-fibre-and-satellite-links-with-traceroute/>)

1 ms – within your LAN

25 ms – cable service in Telstra to servers located in Sydney

90 ms – typical home DSL in the US to google.com

100-150 ms – transoceanic cable

600-2000 ms – typical VSAT remote to hub link

You are encouraged to bring up any problems and discuss on Piazza.

## Tutorial questions for Chapter 2.

Expected time to complete: 1 or 2 week(s).

Simple questions: Please answer the following questions:

1. Define the following terms:
  - a. process in a server or client: **program running within a host**. More precisely, a process is the instance of a computer program that is being executed. For example, Firefox is a web browser program. There can be multiple instances of Firefox running in a computer. Each of them is an independent process. Stopping one process will not affect the other.
  - b. sockets: **A socket is one endpoint of a two-way communication link between two processes running on the network**. A socket is bound to a port number (0 to 64k) so that the TCP layer can identify the application that data is destined to be sent to. An endpoint is a combination of an IP address and a port number.
  - c. HTTP: **hypertext transfer protocol**. A set of rules (protocol) for transmitting hypermedia (for example graphics, audio, video, plain text and hyperlinks) documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes (API, SOAP messages)
  - d. DNS: **Domain Name System**. A hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It maps easy to remember (domain) names to the numerical IP addresses.
  - e. CDN: **Content distribution networks**. A geographically distributed network of proxy servers that provides high availability and performance. They allow faster web objects (text, graphics and scripts), downloadable objects (media files, software, documents), applications (e-commerce, portals), live streaming media, on-demand streaming media, and social media site content access.
2. What are the differences between the following?
  - a. Client-server architecture and P2P  
Client server: dedicated server and specific clients  
P2P: each node can act as both server and client
  - b. TCP and UDP  
TCP: connection-oriented protocol. It establishes a connection between a sender and receiver before data can be sent. This takes time but has good error and flow control.  
UDP: connectionless protocol. It's simple but fast as packets are simply "sent"
  - c. Persistent HTTP and non-persistent HTTP  
Persistent HTTP: multiple objects can be sent over single TCP connection between client, server. This means there is only one handshake overhead even if multiple images and files are contained in a HTML page.  
non-persistent HTTP: Each object (image, file) results in a new connection with a handshake.

d. HTTP/1.0, HTTP/1.1 (You may compare them with HTTP/2)

HTTP/1.0	HTTP/1.1	HTTP/2
GET, POST, HEAD	GET, POST, HEAD PUT, DELETE	
Stateless	Stateful	
Connectionless	persistent and pipelined connections	
Not supported	chunked transfers, compression/decompression	
	multiple languages	
	textual	binary
	fully multiplexed	fully multiplexed
		one connection for parallelism
		header compression
		Server Pushing

Source and more explanation:

HTTP/1 vs HTTP/1.1 : <http://www.ra.ethz.ch/cdstore/www8/data/2136/pdf/pd1.pdf>

HTTP/2 : <https://www.thewebmaster.com/hosting/2015/dec/14/what-is-http2-and-how-does-it-compare-to-http1-1/>

e. SMTP, POP3 and IMAP

SMTP: Simple Mail Transfer Protocol: Protocol used by the sender to **send** an email to an email server (SMTP server).

*POP3 and IMAP are protocols for receiving emails at the client side.*

POP3: Post Office Protocol – version 3: downloads the email from a server to a single computer, then deletes the email from the server

IMAP: Internet Message Access Protocol: stores the message on a server and synchronizes the message across multiple devices

f. Iterative query and (all) recursive query in DNS

Iterative query: must be supported by all DNS. May give the answer (IP) or a referral to another DNS that can give an answer.

recursive query: Will give a final answer (IP). It will recursively follow up and query other DNS server's in the internet on your behalf for the answer.

3. List at least three protocols that adopt the following protocols, which are not listed on the lecture slides:

- a. TCP
- b. UDP

Refer to [https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers) for the complete list of protocols and associated port numbers.

4. Is it reasonable to use UDP for the following protocols; briefly discuss.

- a. HTTP



- HTTP, as an application protocol, can be transferred over UDP transport protocol. services that use UDP and an underlying protocol for transferring HTTP data and streaming it to the end-user:
  - XMPP's Jingle Raw UDP Transport Method
  - A number for services that use UDT --- UDP-based Data Transfer Protocol, which is a superset of UDP protocol.
  - The Transport Layer Security (TLS) protocol encapsulating HTTP as well as the above mentioned XMPP and other application protocols does have an implementation that uses UDP in its transport layer; this implementation is called Datagram Transport Layer Security (DTLS).
  - Push notifications in GNTella are HTTP requests sent over UDP transport.
- QUIC protocol (which is more strictly a pseudo-transport or a session layer protocol) does use UDP for carrying HTTP/2.0 traffic and much of Google's traffic already uses this protocol. It's currently progressing towards standardization as HTTP/3.
- Also see : <https://thenewstack.io/http-3-replaces-tcp-with-udp-to-boost-network-speed-reliability/>
- There are more in favor in using UDP

#### b. telnet

- The standard telnet allows to telnet to services running on TCP ports only.
- However, the utility Netcat can be used for working with UDP ports in a very similar manner.
  - <https://en.wikipedia.org/wiki/Netcat>
  - Netcat site: <https://nc110.sourceforge.io/>
- Telnet uses small packets, typically interactively
- If the higher-level protocol can handle the errors, packet loss and security UDP can be used.
- There would be no "connection" with the end point established. This means data needs to be sent to know the end point exists.
- It is possible to use UDP.

5. How can a host (e.g., PC, laptop) be uniquely identified in a network? IP address is a 32-bit number that uniquely identifies a host (computer or another device, such as a printer or router) on a TCP/IP network

6. How a process (e.g., a web browser) is uniquely identified in a host?  
Process generally have a unique process id for the OS to keep track, schedule and manage.

7. How is a socket associated with a process? A process can bind itself to an available socket. The communication (transport) protocols will deliver any (data) packets to the appropriate port number, which then becomes available to the process which has bound to the port.

8. What is an advantage to use cookies for HTTP?

Cookies are small text files stored on the user's computer, allowing websites to track the visitors and provide a more customized experience.

- Cookies are domain specific i.e. a domain cannot read/write cookies created by another domain.
- Cookies are browser specific.

- Cookies are profile specific.

#### Advantages for HTTP

- Store session state: simple to use and implement, occupies less memory, do not require any server resources. Stored on the user's computer so no extra burden on server
- Transparent: Cookies work transparently without the user being aware that information needs to be stored.
- personalized content: User preferences, themes, and other settings
- Tracking: User preferences, themes, and other settings

Additional reading : [https://en.wikipedia.org/wiki/HTTP\\_cookie#Uses](https://en.wikipedia.org/wiki/HTTP_cookie#Uses)

9. What is the reason to disable cookies? (**How are cookies related to tracking?**)

Ability to track user actions and preferences.

Ability to profile a user

10. In what cases web caching is useful or not?

Useful	Not useful
Static data immutable web resources (movies, data dumps) Data accessed by many (either public or internal users) Eliminate lag time	Dynamic data

Calculation questions:

Please solve the following questions (which were the Q1, Q2 and Q3 in the 2019 final exam).

11. [HTTP GET] Suppose that a server receives the following HTTP GET message from a client browser:

```
GET /kurose_ross/interactive/quotation4.htm HTTP/1.1
Host: www.univ1.edu.au
Accept: text/plain, text/html, image/jpeg, image/gif, audio/mp4, audio/vnf.wave, video/mp4,
video/mpeg, application/*, */*
Accept-Language: en-us, en-gb;q=0.5, en;q=0.4, fr, fr-ch, zh, fi
If-Modified-Since: Thu, 25 April 2019 15:20:19 -0700
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_3) AppleWebKit/534.53.11
(KHTML, like Gecko) Version/5.1.3 Safari/534.53.10
```

a. What is the name of the file that is being retrieved in this GET message?

The full path to the resource is: [kurose\\_ross/interactive/quotation4.htm](#)

The file name is quotation4.htm located in the /kurose\_ross/interactive subdirectory of the server web root.

b. What formats of text, images, audio, and video does the client browser prefer to receive?

The client's format list is : text/plain, text/html, image/jpeg, image/gif, audio/mp4, audio/vnf.wave, video/mp4, video/mpeg, application/\*, \*/\*

However as \*/\* denotes any content, and format this accepts all formats. For example, application/xhtml+xml is also accepted.

- c. Does the client already have a (possibly out-of-date) copy of the requested file? Explain. If so, approximately how long ago did the client receive the file, assuming the GET request has just been issued?

Yes. The "If-Modified-Since:" implying there is a copy already in the Browser cache.

When the original copy was fetched, the Server has indicated that the file was last modified at Thu, 25 April 2019 15:20:19 -0700. This does not give a direct indication when the client downloaded the file.

However, if we assume that file was created at the moment it was originally downloaded (i.e. Thu, 25 April 2019 15:20:19 -0700) we can compute how long ago it was downloaded by  
Age = current time - Thu, 25 April 2019 15:20:19 -0700

12. [HTTP Response] Suppose the server-to-client HTTP response message is the following:

```
HTTP/1.1 404 Not Found
Date: Mon, 24 Sep 2018 22:23:34 +0000
Server: Apache/2.2.3 (CentOS)
Content-Length: 74396
Keep-Alive: timeout=39, max=82
Connection: Keep-alive
Content-type: image/html
```

- a. Was the server able to send the document successfully? Explain.

No.

Response was a 404, File not found

- b. What is the type of file being sent by the server in response?

image/html

- c. What is the default mode of connection for HTTP protocol? Is the connection in the reply persistent or non-persistent? Explain.

Default connection for HTTP

- HTTP 1.0 – Non persistent OR
- HTTP 1.1 – Persistent

Since this is HTTP 1.1. There also the keep-alive directive. Either of this implies a Persistent connection

13. [Transport layer] Suppose that nodes A and B want to establish a TCP connection via the three-way handshake. A sent the following TCP segment to B. The following is a dump (contents) of the TCP header in hexadecimal format. Ignore the space between hexadecimal numbers.

```
D201 0043 0000 2711 0000 0000 4002 06EE ...
```

- a. What is the destination port number? Show your working.

```
D201 0043 0000 2711 0000 0000 4002 06EE OR
0043 (hex), leading 0 optional
```

port number as 67 (base 10)
-----------------------------

- b. What is the sequence number? Show your working.

D201 0043 <b>0000 2711</b> 0000 0000 4002 06EE OR
0000 2711 (hex), leading 0 optional
seq number as 10001 (base 10)

- c. What is the length of header? Show your working.

D201 0043 0000 2711 0000 0000 <b>4</b> 002 06EE OR
4 (hex)
4 x 4 (scaling factor) = 16 bytes
NOTE that the smallest header size is 20 bytes which is also valid

- d. What is the window size? Show your working.

D201 0043 0000 2711 0000 0000 4002 <b>06EE</b> OR
06EE (hex), leading 0 optional
Indicating windows size as 1774 (base 10) bytes

#### Practice questions

14. Please try to find and run an existing socket program with both UDP and TCP. This will be useful for you to do the assignment.

You are encouraged to bring up any problems and discuss on Piazza.

## Tutorial questions for Chapter 3.

Expected time to complete: 1-2 week(s).

Simple questions: Please answer the following questions:

1. Briefly define the following terms/concepts:

a. Multiplexing

Multiplexing is the process of directing the packet from the source host by attaching a relevant transport header.

b. Demultiplexing

Demultiplexing is the process of directing received packets to the correct destination socket by using the transport header information.

c. UDP

UDP, User Datagram Protocol, is a transport layer protocol that offers datagram-based packet-switched communication without establishing connections.

d. TCP

TCP, Transmission Control Protocol, is a transport layer protocol that offers reliable host-to-host communication on a packet-switched network.

e. TCP congestion control: slow start

Slow start begins initially with a small congestion window size (CWND), increasing the CWND by one SMSS (sender maximum segment size) with each ACK received until a loss is detected or the receiver window size (RWND) is reached.

f. TCP congestion control: congestion avoidance

Congestion avoidance extends the slow start algorithm beyond ssthresh (slow start threshold). The difference is that congestion avoidance MUST NOT increase the CWND by more than SMSS bytes for every RTT (compared to 1 SMSS per ACK for slow start).

g. TCP congestion control: fast recovery

With fast recovery and retransmit, the receiver will send a duplicate ACK when a packet is lost. When the sender receives 3 duplicate ACKs, the data segment indicated by the ACKs is then immediately retransmitted (in contrast to waiting for a timeout).

2. What are the 4-tuple used to identify a TCP socket?

(Source IP address, Source port number, Destination IP address, Destination port number)

3. What information does a UDP segment include?

UDP segment consists of the header and payload. The header includes source port, destination port, length (of the entire packet, i.e. the header length + payload length) and the checksum.

4. What is stop-and-wait operation in rdt3.0?

The sender sends the packet and waits for the ACK (acknowledgement) of the packet. Once the ACK reaches the sender, it transmits the next packet in row. If the ACK is not received by the time the countdown timer has expired, it re-transmits the previous packet again.

5. What are the differences between the following?

a. Go-Back-N and selective repeat in pipelined protocols

Go-Back-N	Selective Repeat
<u>Sender sends a chunk of packets</u> and waits for a cumulative ACK.	<u>Sender sends packets</u> and waits for individual ACKs.
<u>In case of loss or damage to packets</u> , the entire chunk (of N packets) must be retransmitted.	<u>In case of loss or damage to packets</u> , only the packets in question must be retransmitted.
If retransmission occurs, it will occupy more <u>bandwidth</u> . Conversely, it saves bandwidth in terms of acknowledgements sent.	If retransmission occurs, it will occupy less <u>bandwidth</u> . Conversely, it expends more bandwidth in terms of acknowledgements sent.

b. TCP retransmission and TCP 'fast' retransmit

TCP retransmission	TPC Fast retransmit
TCP retransmission occurs when a packet is damaged (verifiable by the checksum) or lost (when there is a timeout).	Occurs when the sender receives three duplicate ACKs before a timeout. In such a case, the packet with the next higher sequence number is immediately retransmitted and the timeout is also reset.

6. What are the fields that are not included in UDP segment but included in TCP segment?

In addition to the fields contained in a UDP segment, TCP segments also contain

- 32 bit "Sequence number" and "Acknowledgment number" fields,
- 16 bit "Window", "Checksum" and "Urgent Pointer" fields,
- 6 bit "Reserved" and "Flags" fields,
- 4 bit "Data offset" field, and
- Variable size "Options" field

Calculation questions:

Please solve the following questions.

7. Consider the two 16-bit words (shown in binary) below. Recall that to compute the Internet checksum of a set of 16-bit words, we compute the one's complement sum [1] of the two words. That is, we add the two numbers together, making sure that any carry into the 17th bit of this initial sum is added back into the 1's place of the resulting sum); we then take the one's complement of the result. Compute the Internet checksum value for these two 16-bit words:

- a.      10010111 00011101              this binary number is 38685 decimal (base 10)  
           11110000 10010111              this binary number is 61591 decimal (base 10)

Step 1. Add the two numbers

$$\begin{array}{r} 1001011100011101 \\ + 1111000010010111 \\ \hline = (+1) 1000011110110100 \end{array}$$

Step 2. Carry over the overflow

$$= 1000011110110101$$

Step 3. Compute one's complement

$$= 0111100001001010$$

- b.      11110000 1001111  
           10010000 1001110

Step 1. Add the two numbers

$$\begin{array}{r} 111100001001111 \\ + 100100001001110 \\ \hline = (+1) 100000010011101 \end{array}$$

Step 2. Carry over the overflow

$$= 100000010011110$$

Step 3. Compute one's complement

$$= 011111101100001$$

8a. Fill out the table below indicating (i) the state of the sender and the receiver just after the transmission of a new packet in response to the received packet at time  $t$ , (ii) the sequence number associated with the data packet or the ACK number associated with the ACK packet sent at time  $t$ .



t	Sender state	Receiver state	Packet type sent	Seq# or Ack# sent
0	Wait for ACK 0	Wait 0 from below	data	0
1	Wait for ACK 0	Wait 0 from below	ACK	1
2	Wait for ACK 0	Wait 0 from below	data	0
3	Wait for ACK 0	Wait 1 from below	ACK	0
4	Wait for ACK 1	Wait 1 from below	data	1
5	Wait for ACK 1	Wait 0 from below	ACK	1
6	Wait for ACK 0	Wait 0 from below	data	0

b. How many times is the payload of the received packet passed up to the higher layer at the receiver in the above example? At what times is the payload data passed up?

The payload data is passed up to the higher level at the receivers end exactly two times,  
i.e.  $t = \{3,5\}$  (when data packets are sent to the receiver and received without corruption).

9. TCP sequence and ACK numbers with segment loss:

a. Give the sequence numbers associated with each of the three segments sent by the sender.

First segment seq# = 101

Second segment seq# = first segment seq# + first segment size = 101 + 450 = 551

Third segment seq# = second segment seq# + second segment size = 551 + 450 = 1001

b. List the sequence of acknowledgements transmitted by the TCP receiver in response to the receipt of the segments actually received. In particular, give the value in the acknowledgement field of each receiver-to-sender acknowledgement, and give a brief explanation as to why that particular acknowledgement number value is being used.

First segment's acknowledgment # = first segment seq# + first segment size = 551

Second segment is lost, so there is no ack for it.

Third segment arrives at the receiver end and when a seq# equal to the last ack# is expected, instead 1001 is received as seq# (1001 > 551). Therefore, the sender sends a duplicate ack (ack# = 551) to the sender to alert them of the missing segment.

10. Computing TCP's RTT and timeout values.

Suppose that TCP's current estimated values for the round-trip-time (estimatedRTT) and deviation in the RTT (DevRTT) are 315 msec and 36 msec, respectively (see Section 3.5.3 for a discussion of these variables). Suppose that the next three measured values of the RTT are 240, 300, and 380 respectively.

Compute TCP's new value of estimatedRTT, DevRTT, and the TCP timeout value after each of these three measured RTT values is obtained. Use the values of  $\alpha = 0.125$  and  $\beta = 0.25$ .

Using the formulas below to answer the following questions:

$$\text{EstimatedRTT}^0 = (1 - \alpha) * \text{EstimatedRTT} + \alpha * \text{SampleRTT}$$

$$\text{DevRTT}^0 = (1 - \beta) * \text{DevRTT} + \beta * (\text{abs}(\text{SampleRTT} - \text{EstimatedRTT}^0))$$

$$\text{TimeoutInterval} = \text{EstimatedRTT}^0 + 4 * \text{DevRTT}^0$$

a. After the first RTT estimate is made

- $\text{estimatedRTT} = 0.875 * 315 + 0.125 * 240 = 305.625$
- $\text{DevRTT} = 0.75 * 36 + 0.25 * (\text{abs}(240 - 305.625)) = 43.40625$
- $\text{TimeoutInterval} = 305.625 + 4 * 43.40625 = 479.25$

b. After the second RTT estimate is made

- $\text{estimatedRTT} = 0.875 * 305.625 + 0.125 * 300 = 304.9219$
- $\text{DevRTT} = 0.75 * 43.40625 + 0.25 * (\text{abs}(300 - 304.9219)) = 33.78516$
- $\text{TimeoutInterval} = 304.9219 + 4 * 33.78516 = 440.0625$

c. After the third RTT estimate is made

- $\text{estimatedRTT} = 0.875 * 304.9219 + 0.125 * 380 = 314.3067$
- $\text{DevRTT} = 0.75 * 33.78516 + 0.25 * (\text{abs}(380 - 314.3067)) = 41.7622$
- $\text{TimeoutInterval} = 314.3067 + 4 * 41.7622 = 481.3555$

## Tutorial questions for Chapter 4.

Expected time to complete: 1-2 weeks.

1. Briefly define/explain the following terms/concepts:

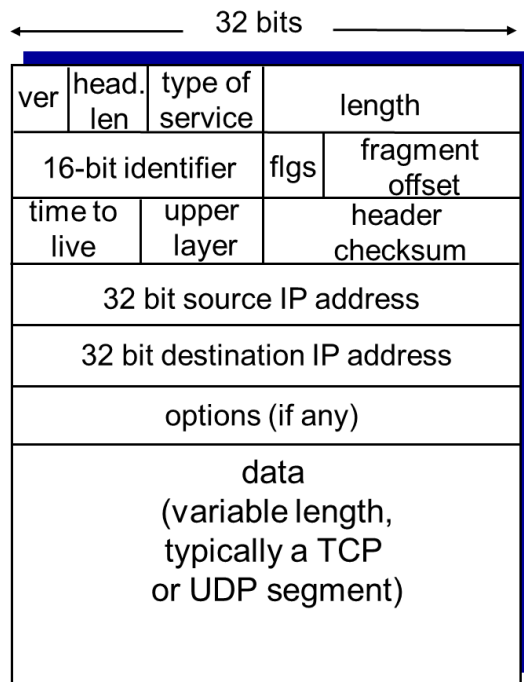
- a. Data plan
- b. Control plan
- c. Routing algorithm
- d. Forwarding table
- e. Link interface
- f. Routing protocol
- g. MTU
- h. CIDR
- i. DHCP
- j. NAT

2. IP datagram format. Fill the following fields (a-l).

← 32 bits →			
a	b	c	d
d		e	f
g	h	i	
j			
j			
k			
l			

- a.
- b.
- c.
- d.
- e.
- f.
- g.
- h.
- i.
- j.
- k.
- l.

Answer:



3. IP address classes of IPv4: Determine which class the following IP Address belongs to.

[Answers: class A, B, C, D, E, none, invalid IP address, For loopback or localhost only]

- a. 172.16.1.20: class B
- b. 192.168.1.1: belongs to class C of IPv4 addresses;
- c. 0.0.0.0: none
- d. 1.1.1.1: class A
- e. 190.0.0.0: class B
- f. 223.200.200.1: class C
- g. 127.0.0.1: local host
- h. 111.111.111.1: class A
- i. 224.0.0.0: class D

Answers:

The IP address number 0.0.0.0 is a non-routable IPv4 address with several uses, primarily as a default or placeholder.

Ranges 127.x.x.x are reserved for the loopback or localhost, for example, 127.0.0.1 is the loopback address.

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.

<b>Class B</b>	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
<b>Class C</b>	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
<b>Class D</b>	224.0.0.0 to 239.255.255.255	Reserved for <u>multicast</u> groups.
<b>Class E</b>	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

#### 4. Subnet mask questions:

- a. What is the total number of usable hosts for IP address 224.1.1.1/24?
- b. What is the total number of usable hosts for IP address 224.1.1.1/27?
- c. Subnet the Address 160.30.0.0 into networks supporting 500 Hosts each. What is the New Subnet Mask and the IP Address Range of the first Network?
- d. Your company wants to utilize the private Class C IP Address of 192.168.1.0. You are tasked with Subnetting the Address to get the most networks with at least 30 Hosts per Subnet. How many Networks will be created after you subnet? What is the first usable IP Address in the Second Network range?
- e. Subnet the IP Address 210.30.12.0 so there are 60 Hosts in each network. What are the Broadcast Addresses of each Network?

Answers:

- a. What is the total number of usable hosts for IP address 224.1.1.1/24?

IP address: 224.1.1.1

Network address: 224.1.1.0

Usable host IP range: 224.1.1.1 – 224.1.1.254

Broadcast address: 224.1.1.255

Number of hosts: 256

Number of usable hosts: 254

b. What is the total number of usable hosts for IP address 224.1.1.1/26?

<https://www.calculator.net/ip-subnet-calculator.html?cclass=c&csubnet=26&cip=224.1.1.1&ctype=ipv4&printit=0&x=42&y=28>

IP address: 224.1.1.1

Network address: 224.1.1.0

Usable host IP range: 224.1.1.1 – 224.1.1.62

Broadcast address: 224.1.1.63

Number of hosts: 64

Number of usable hosts: 62

All 4 of the Possible /26 Networks for 224.1.1.\*

Network Address	Usable Host Range	Broadcast Address:
224.1.1.0	224.1.1.1 - 224.1.1.62	224.1.1.63
224.1.1.64	224.1.1.65 - 224.1.1.126	224.1.1.127
224.1.1.128	224.1.1.129 - 224.1.1.190	224.1.1.191
224.1.1.192	224.1.1.193 - 224.1.1.254	224.1.1.255

c. Subnet the Address 160.30.0.0 into networks supporting 500 Hosts each. What is the New Subnet Mask and the IP Address Range of the first Network?

<https://www.calculator.net/ip-subnet-calculator.html?cclass=b&csubnet=23&cip=160.30.0.0&ctype=ipv4&printit=0&x=66&y=19>

All 128 of the Possible /23 Networks for 160.30.\*.\*

Network Address	Usable Host Range	Broadcast Address:
160.30.0.0	160.30.0.1 - 160.30.1.254	160.30.1.255
160.30.2.0	160.30.2.1 - 160.30.3.254	160.30.3.255

- d. Your company wants to utilize the private Class C IP Address of 192.168.1.0. You are tasked with Subnetting the Address to get the most networks with at least 30 Hosts per Subnet. How many Networks will be created after you subnet? What is the first usable IP Address in the Second Network range?

<https://www.calculator.net/ip-subnet-calculator.html?cclass=c&csubnet=27&cip=192.168.1.0&ctype=ipv4&printit=0&x=87&y=25>

### All 8 of the Possible /27 Networks for 192.168.1.\*

Network Address	Usable Host Range	Broadcast Address:
192.168.1.0	192.168.1.1 - 192.168.1.30	192.168.1.31
192.168.1.32	192.168.1.33 - 192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65 - 192.168.1.94	192.168.1.95
192.168.1.96	192.168.1.97 - 192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
192.168.1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
192.168.1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

- e. Subnet the IP Address 210.30.12.0 so there are 60 Hosts in each network. What are the Broadcast Addresses of each Network?

<https://www.calculator.net/ip-subnet-calculator.html?cclass=any&csubnet=26&cip=210.30.12.0+&ctype=ipv4&printit=0&x=76&y=3>

### All 4 of the Possible /26 Networks for 210.30.12.\*

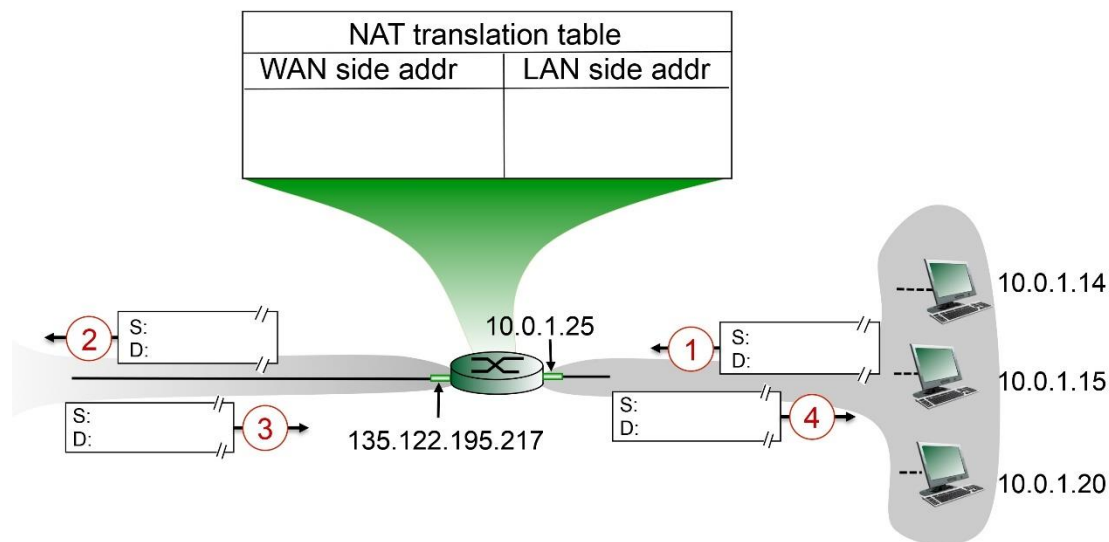
Network Address	Usable Host Range	Broadcast Address:
210.30.12.0	210.30.12.1 - 210.30.12.62	210.30.12.63
210.30.12.64	210.30.12.65 - 210.30.12.126	210.30.12.127
210.30.12.128	210.30.12.129 - 210.30.12.190	210.30.12.191
210.30.12.192	210.30.12.193 - 210.30.12.254	210.30.12.255



## 5. NAT question.

Consider the scenario below in which three hosts, with private IP addresses 10.0.1.14, 10.0.1.15, 10.0.1.20 are in a local network behind a NATted router that sits between these three hosts and the larger Internet. IP datagrams being sent from, or destined to, these three hosts must pass through this NAT router. The router's interface on the LAN side has IP address 10.0.1.25, while the router's address on the Internet side has IP address 135.122.195.217.

Before doing this problem, you might want to reread the section on the NAT protocol in section 4.3.4 in the text.



Suppose that the host with IP address 10.0.1.14 sends an IP datagram destined to host 128.119.165.188. The source port is 3481, and the destination port is 80.

- Consider the datagram at step 1, after it has been sent by the host but before it has reached the NATted router. What are the source and destination IP addresses for this datagram? What are the source and destination port numbers for the TCP segment in this IP datagram?
- Now consider the datagram at step 2, after it has been transmitted by the NATted router. What are the source and destination IP addresses for this datagram? What are the source and destination port numbers for the TCP segment in this IP datagram? Identify the differences in datagram's IP addresses and port numbers between step 1 and step 2. Specify the entry that has been made in the router's NAT table.

- c. Now consider the datagram at step 3, just before it is received by the NATted router. What are the source and destination IP addresses for this datagram? What are the source and destination port numbers for the TCP segment in this IP datagram?
- d. Last, consider the datagram at step 4, after it has been transmitted by the NATted router but before it has been received by the host. What are the source and destination IP address for this datagram? What are the source and destination port numbers for the TCP segment in this IP datagram? Identify the differences in datagram's IP addresses and port numbers between step 3 and step 4. Has a new entry been made in the router's NAT table, or removed from the NAT table? Explain your answer.

### Solution:

#### At Step 1:

source address of the IP datagram: 10.0.1.14

destination address of the IP datagram: 128.119.165.188

source port number for the TCP segment of the IP datagram: 3481

destination port number for the TCP segment of the IP datagram: 80

Host 10.0.0.14 has assigned an arbitrary source port number 3481 and sends the datagram to LAN. The datagram is received at the NAT router's right port.

#### At Step 2:

source address of the IP datagram: 135.122.195.217

destination address of the IP datagram: 128.119.165.188

source port number for the TCP segment of the IP datagram: 5116

destination port number for the TCP segment of the IP datagram: 80

After receiving the datagram from host 10.0.0.14, the NAT router generates a new source port number 5116 (not already in use within the NAT table) for the datagram and replaces the original source port number 3481 with the new source port number 5116. The traffic leaving the home router for the larger internet has the source IP of the NAT router which is 135.122.195.217, and thus the datagram's source IP address now changes to 135.122.195.217. The destination address and the port number remain the same. The NAT table, after step 2, looks like (see Figure 4.25 in text):

WAN-side address	LAN-side address
135.122.195.217, 5116	10.0.1.14, 3481

#### At Step 3:

source address of the IP datagram: 128.119.165.188

destination address of the IP datagram: 135.122.195.217

source port number for the TCP segment in the IP datagram: 80

destination port number for the TCP segment in the IP datagram: 5116

This arriving datagram was sent by remote host 128.119.165.188 in response to the datagram sent by this NAT router in Step 2 above.

At Step 4:

source address of the IP datagram: 128.119.165.188

destination address of the IP datagram: 10.0.1.14

source port number for the TCP segment of the IP datagram: 80

destination port number for the TCP segment of the IP datagram: 3481

When this datagram arrived at NAT router's left port from the Internet, the router indexed the NAT translation table using the destination IP address and destination port number to obtain the appropriate IP address(10.0.1.14) and destination port (3481) for the destination host in the home network. The router then rewrites the datagram's destination address and destination port number, and forwards the datagram into the home network.

## Tutorial questions for Chapter 5.

### Network Layer: The control plane

Expected time to complete: 1 week.

Simple questions: Please answer the following questions:

1. Briefly define/explain the following terms/concepts:

a. Routing protocols

~ determine good paths (equivalently, routes), from sending hosts to receiving hosts, through network of routers.

b. Routing algorithms

~ is an algorithm that calculates the least cost path/route that a packet can take from a sending host to a receiving host through a network of routers.

c. The differences between link state and distance vector routing protocols

Link state routing protocols	Distance vector routing protocols
All routers have complete topology, link cost information	Routers know only physically connected neighbours and the link cost to them
The link costs are broadcast to all the routers in the network from a single controller	Requires an iterative process of computation, exchange of information with neighbours

d. The differences between intra-AS routing and inter-AS routing

Intra-AS Routing	Inter-AS routing
Routing among hosts, routers in the same Autonomous System (AS)	Routing among AS'es

e. Count to infinity

~ An important issue in distance vector routing that occurs when a connecting interface goes down or link cost increases. This results in a loop that is unnecessarily expensive (what would take 2 iterations will take orders more).

f. BGP (Border Gateway Protocol):

~ the de facto inter-domain routing protocol

g. OSPF (Open Shortest Path First):

~ it is the de facto intra-AS routing protocol that uses a link state routing algorithm.

h. RIP (Routing Information Protocol):

~ it is intra-AS protocol that precedes OSPF, using a distance vector routing algorithm instead.

- i. What is ICMP?  
~ (Internet Control Message Protocol): it is used to send messages between routers, typically in case of errors.
- j. What is SNMP?  
~ (Simple Network Management Protocol): it is an Internet Standard protocol for collection and organizing information about managed devices on IP networks and for modifying that information to change device behaviour.

## 2. Routing algorithms

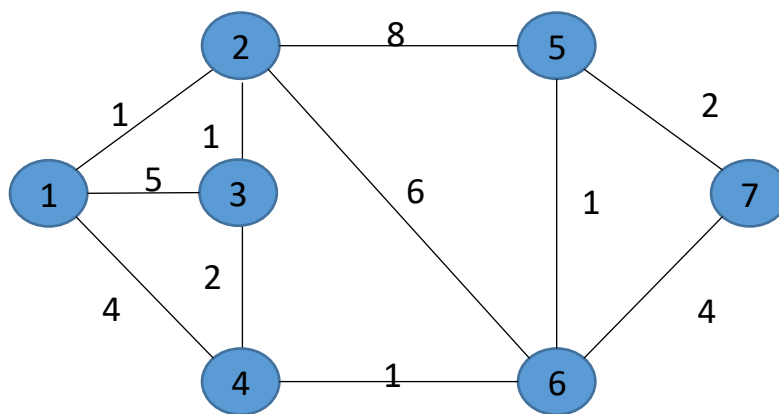


Figure 1. An example network 1

2-1. Apply the Bellman-Ford algorithm on the example network 1 given in Figure 1 to find the minimum-cost routes from station 1 to all other stations. Please make a table containing all the values. Please use "inf" to specify an infinite cost and "-" to specify no next hop respectively.

Step	1 (cost, next hop)	2	3	4
dest				
1	0, 1	0, 1	0, 1	0, 1
2	1, 2	1, 2	1, 2	1, 2
3	5, 3	2, 2	2, 2	2, 2
4	4, 4	4, 4	4, 4	4, 4
5	∞, -	9, 2	6, 4	6, 4
6	∞, -	5, 4	5, 4	5, 4
7	∞, -	∞, -	9, 4	8, 4

2-2. Apply the Dijkstra algorithm on the example network 1 in Figure 1 to find the minimum-cost routes from station 1 to all other stations. Please make a table for the final value. S is the set of stations whose least-cost path is known; D(v) is the current cost of path from source (i.e., station 1) to station v; p(v) is the predecessor station along path from source to v, that is next to v. Please use "inf" to specify an infinite cost and "-" to specify no predecessor respectively.

Step	D(1), p(1)	D(2) ,p(2)	D(3) ,p(3)	D(4) ,p(4)	D(5) ,p(5)	D(6) ,p(6)	D(7) ,p(7)	S
0	0, -	Inf, -	Inf, -	Inf, -	Inf, -	Inf, -	Inf, -	-
1	0, -	1, 1	5, 1	4, 1	Inf, -	Inf, -	Inf, -	1
2	0, -	1, 1	2, 2	4, 1	9, 2	7, 2	Inf, -	1,2
3	0, -	1, 1	2, 2	4, 1	9, 2	7, 2	Inf, -	1,2,3
4	0, -	1, 1	2, 2	4, 1	9, 2	5, 4	Inf, -	1,2,3,4
5	0, -	1, 1	2, 2	4, 1	6, 6	5, 4	9, 6	1,2,3,4,6
6	0, -	1, 1	2, 2	4, 1	6, 6	5, 4	8, 5	1,2,3,4,6,5
7	0, -	1, 1	2, 2	4, 1	6, 6	5, 4	8, 5	1,2,3,4,6,5,7

## Tutorial questions for Chapter 6

### The Link Layer and LANs

Expected time to complete: 1 week.

1. Briefly define/explain the following terms/concepts:

- a. Parity bit – the bit after a binary sequence that must, in conjunction with the preceding bits, have an even/odd sum.
- b. CRC (Cyclic Redundancy Check) – It is a form of error detection coding that is more powerful than checksum.
- c. FEC (Forward Error Correction) - is an error correction technique to detect and correct a limited number of errors in transmitted data without the need for retransmission.
- d. ALOHA – it is a random access MAC protocol that sends the data if there is data to send, and if there is an incoming message while the data is being sent, then a message collision is said to have occurred. Transmitting stations will need to transmit after an interval.
- e. CSMA/CD (Carrier Sense Multiple Access/Collision Detection) - it is a random-access MAC protocol where collisions are detected within a short time and uses carrier-sensing to defer transmissions until no other stations are transmitting.
- f. ARP (Address Resolution Protocol) – It is a communication protocol used for discovering the link layer address, i.e. MAC address, associated with a given internet layer address, i.e. typically IPv4 address.
- g. MAC (Media Access Control) – It is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable.
- h. Physical topology (bus, star)
  - i. Bus topology – All nodes connected to a single medium/channel where it is possible for collisions to occur.
  - ii. Star topology – All nodes are connected to a central switch where each spoke runs a separate ethernet protocol (nodes do not collide with each other).
- i. Ethernet switch – Link layer device that stores and forwards ethernet frames.
- j. VLAN (Virtual Local Area Network) – any switch with VLAN capabilities can be configured to define multiple virtual LANs over a single physical infrastructure.
- k. MPLS (Multiprotocol Label Switching) - is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows.

2. MAC address

The following is an example MAC address.

00:A0:C9:14:C8:29

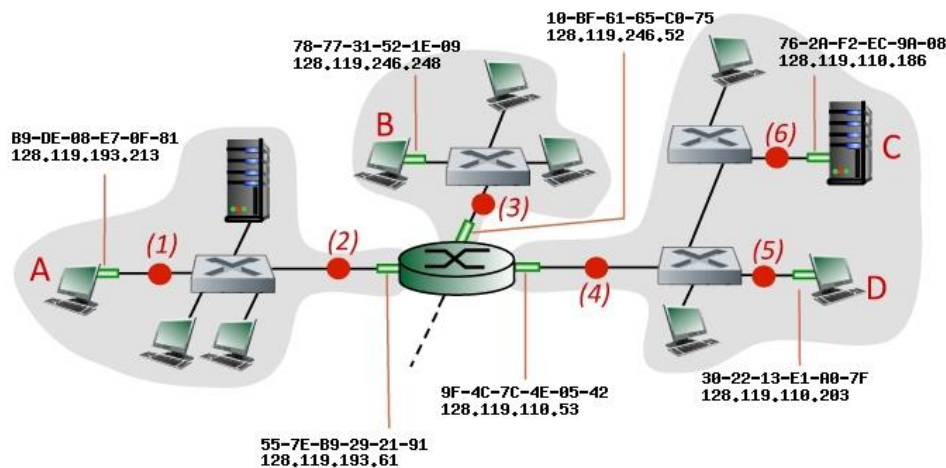
- a. Write down the part in hexadecimal indicating the adapter's manufacturer. 00:A0:C9

b. What is the identification number of the given MAC address? 14:C8:29

3. Link Layer (and network layer) addressing and forwarding:

Consider the figure below. The IP and MAC addresses are shown for nodes A, B, C and D, as well as for the router's interfaces.

[https://gaia.cs.umass.edu/kurose\\_ross/interactive/link\\_layer\\_addressing.php](https://gaia.cs.umass.edu/kurose_ross/interactive/link_layer_addressing.php)



Consider an IP datagram being sent from node **B** to node **D**. Give the source and destination Ethernet addresses, as well as the source and destination addresses of the IP datagram encapsulated within the Ethernet frame at points (1), (3), (4), and (5) in the figure above.

At point (3):

Ethernet source, destination address: 78-77-31-52-1E-09, 10-BF-61-65-C0-75

IP source, destination address: 128.119.246.248, 128.119.110.203

At point (4):

Ethernet source, destination address: 9F-4C-7C-4E-05-42, 30-22-13-E1-A0-7F

IP source, destination address: 128.119.246.248, 128.119.110.203

At point (5):

Same as point (4)



#### 4. Parity bit

The two-dimensional 'odd' parity scheme is used for the following data:

01110 01010 01001 11001.

4.1. Show how one-bit error can be detected using the two-dimensional parity scheme.

The correct odd block parity is in green

0	1	1	1	0	0
0	1	0	1	0	1
0	1	0	0	1	1
1	1	0	0	1	0
0	1	0	1	1	1

Assuming one bit changed from 1 to 0

0	0	1	1	0	0
0	1	0	1	0	1
0	1	0	0	1	1
1	1	0	0	1	0
0	1	0	1	1	1

Here it can be seen that row 1 column 2 is the wrong bit, as the parity bits are incorrect. Flipping the bit at the intersection will correct the error.

4.2. Show one example of un-correctable error pattern.

0	0	1	0	0	0
0	1	0	1	0	1
0	1	0	0	1	1
1	1	0	0	1	0
0	1	0	1	1	1

In addition to part 4.1, if row 1 column 4 is also flipped, the first row fulfills the 'odd' parity scheme. But columns 2 and 4 will have bad parity, which is detectable but not correctable.

#### 5. Cyclic Redundancy Check

Suppose we chose to send 16-bit sequence "0001 0010 0011 0100" over the Bluetooth channel. In order to enhance communication reliability, we chose to attach the CRC code using CRC-8-AUTOSAR scheme, which is commonly used in automotive integration applications. It is defined as  $x^8 + x^5 + x^3 + x^2 + x + 1$ .

5.1. How many CRC bits are added? And, what is the total number of bits to be sent?

n-k: 8 bit(s), k (data): 16 bits. Therefore, n (total) is 24 bits.

5.2. What is the CRC value? Show all your works.

1. 0001 0010 0011 0100 is multiplied by  $2^8$ , yielding 0001 0010 0011 0100 0000 0000

2.  $\text{remainder} \left( \frac{000100100011010000000000}{100101111} \right) = 10111001$

<http://www.ee.unb.ca/cgi-bin/tervo/calc.pl?num=000100100011010000000000&den=100101111&f=d&e=1&m=1>

3. Therefore, CRC value is 0001 00010 0011 0100 10111001

## 6. FEC

For  $k=2$  and  $n=4$ , we can make the following assignment.

No	Data Block	Codeword
1	00	0000
2	01	0010
3	10	1000
4	11	1110

Suppose that a codeword block is received with the bit pattern 1001.

6.1. Can the error be detected?

Yes, the error can be detected since 1001 is not a valid codeword.

6.2. Can the error be corrected? (Calculate the Hamming distance  $d$ .)

The error can be corrected by flipping the least significant bit of 1001 to turn it to 1000.

This means that the Hamming distance is 1.