THE UNIVERSITY OF MELBOURNE

Semester 2 Assessment, 2022

Department of Electrical and Electronic Engineering

ELEN90061 Communication Networks

Reading/ printing time: 30 minutes, Writing time: 180 minutes

Scanning and submission time: 30 minutes

This examination paper has 8 pages (including this cover page)

Authorised materials:

This is a Zoom Supervised, hand-written exam where only the following materials are permitted:

- Printed copy of this exam paper or an electronic copy on an offline electronic PDF reader.
- A4 paper, any writing materials. Electronic devices may be used for writing your answers.
- Any material in hard copy (handwritten or printed) and/or any material on a electronic device that is disconnected from all communication networks.
- Any offline calculator, including offline computational software such Matlab, Python, or Wolfram Alpha.

Instructions to students:

- Attempt **ALL** questions.
- The questions carry weight in proportion to the marks stated for each question number. These marks total **180 marks**.
- During **Reading Time**, you are **NOT PERMITTED** to do any writing of any kind. You may print out a hardcopy of the exam. Alternatively, you may download the exam to an electronic PDF reading device, which must then be disconnected from the internet.
- During **Writing Time**, you are permitted to write. You may only interact with the device running the Zoom session with supervisor permission. The printed exam paper (or offline device containing the exam paper) and any other working sheets and any offline devices must be visible to Zoom invigilators.
- Write your exam answers using pens/pencils and A4 paper, or electronic writing device. Start each question on a new page and write down the question numbers.
- During **Scan/Upload Time**, you immediately must **CEASE WRITING**, assemble your pages in question number order, and use a mobile phone or tablet to scan and combine them into a single PDF. Check that all pages are included and clearly readable.
- Submit your PDF file to the Canvas Assignment window corresponding to this exam. Confirm with your Zoom supervisor that you have received confirmation of your submission.
- Collusion is **not allowed under any circumstances**. Collusion includes, but is not limited to, talking to, phoning, emailing, texting or using the internet to communicate with other students.
- Plagiarism, through the use of sources without proper acknowledgement or referencing, **is not permitted** and can attract serious penalties. Plagiarism includes copying and pasting from the Internet without clear acknowledgement and paraphrasing or presenting someone else's work as your own.

Question 1	**30 marks**

Consider the hypothetical scenario of 10 routers sharing an incoming link as a router pool with a single queue for all the routers. The packets arrive at the router pool at a *Poisson rate of one packet per 10 milliseconds*. Packet processing at any router is assumed to be *exponentially distributed with a mean of 50 milliseconds*.

*Answer all parts of the question **in your own handwriting** and **show all your work for full marks.***

(a) [15 marks] If a packet arrives at the router pool and finds all 10 routers busy with **m** other packets waiting in the queue ahead of it, what is the average waiting time in the queue for that packet?

Solution:

When all the routers are busy, the expected time between two departures is 50/10=5 milliseconds. If a packet sees **m** packets waiting in the queue, there must be exactly **m**+1 departures from the system before the packet gets processed. Since all the routers would be busy during this whole time, the average waiting time required before **m**+1 departure is 5(**m**+1) milliseconds.

(b) [15 marks] What is the average waiting time in the queue for packets that find all routers busy on arrival?

Hint for part (b): the average number of packets in the queue (not in service) in this system is $P_Q \frac{\rho}{1-\rho}$, where P_Q is given by the Erlang C formula.

Solution:

Let X be the expected waiting time given that the routers are found busy. We have:

$\lambda = {}^{1}/_{10} \quad \mu = {}^{1}/_{50} \quad \rho = {}^{\lambda}/_{(10\mu)} = 0.5$

And by the M/M/m results

$$W = \frac{\rho P_Q}{\lambda(1-\rho)}$$

Since $W = XP_Q$, we obtain:

$X = \frac{W}{P_Q} = \frac{\rho}{\lambda(1-\rho)} = 10$ milliseconds

Question 2	**20 marks**

Consider a single server which has the capacity for **k** communication sessions. The time between session arrivals to the server is exponentially distributed with a mean of $\frac{1}{\lambda}$. The server completes a session in an exponentially distributed manner with a mean of **x**. All of these times are independent. What is the steady-state proportion of time where the server is idle (i.e., there are no sessions active)?

*Answer the question **in your own handwriting** and **show all your work for full marks**.*

Solution:

This gives a Markov chain, which is the same as an M/M/1/**k** queue with arrival rate λ and service rate 1/**x**. The required probability is simply p_0 for such a queue.

Question 3	**30 marks**

Ten firefighters respond to a bushfire in an area. Each firefighter has a walkie-talkie (handheld wireless radio). We make the following assumptions:

- The radios all use the same single channel.
- The **transmission and reception range** of the radios is larger than the deployment area.
- The radio can broadcast the owner's talk if the owner presses the send button, but the send button works only once every 20 seconds and resets (cuts off the talk of the owner) after 20 seconds.
- All radios share the same clock.
- When the send button is not pressed, which is the default case, all the radios listen to all the broadcasters in their reception range.
- When two or more walkie-talkies broadcast at the same time, their transmissions interfere with each other and get garbled, i.e., nobody understands the message sent (talk of the owner).
- Each firefighter attempts to talk to their colleagues with a fixed probability.

*Answer all parts of the question **in your own handwriting** and **show all your work for full marks**.*

(a) Analyse the described protocol by answering the following questions.

(i) [**5 marks]** Identify this communication protocol and describe two of its main properties.

(ii) **[5 marks]** State the formula for the probability of any transmitter's talk being received successfully by receivers.

(iii) **[5 marks]** Derive and compute the optimal probability of individual firefighters' attempts to talk to other firefighters.

Hint: consider the link layer protocols discussed in the subject.

Solution:

(i) Half duplex radios, slotted aloha protocol

(ii) Prob success is $Np(1-p)^{(N-1)}$

(iii) $p^*=1/10$

(b) [15 marks] Suggest a different communication protocol for the firefighting crew to improve their communication efficiency. Assume you can change the send button behaviour. Describe your protocol in sufficient detail.

Hint: there are multiple options, choose only one.

Solution:

It is possible to use CSMA/CD. Each student can use their assigned numbers over e.g. one second to ensure they obtain the channel (shorter contention window) and then talk for longer, increasing efficiency of the protocol.

Question 4	**10 marks**

Explain and briefly discuss (in around 100 words) the advantages and disadvantages of optical networking technology deployment in access and backbone networks.

Answer all parts of the question ***in your own handwriting!***

Solution:
Optical networks have the potential to provide enormous bandwidth due to fiber optic technology and wave division multiplexing when deployed in access networks. They are widely used in core networks. The main disadvantage is the wired infrastructure deployment cost. Replacing old copper (telephony) and cable TV (coaxial) access networks with fiber optic is a costly endeavour as an infrastructure deployment project.

Question 5	**10 marks**

For the graph shown in Figure 1, use Dijkstra's algorithm to find the forwarding table from U to all other nodes.
A blank table for the steps of Dijkstra's algorithm and the forwarding table, in the same format as seen in the lectures, is provided for your convenience.

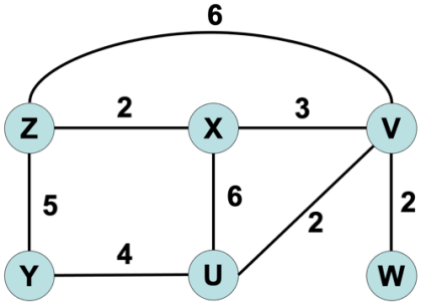


Figure 1: Graph for Question 5.

*Answer the question and **show all your work for full marks**.*

Steps of the Dijkstra algorithm:

Step	**N'**	**D(V) , p(V)**	**D(W) , p(W)**	**D(X) , p(X)**	**D(Y) , p(Y)**	**D(Z) , p(Z)**
0	U	2 , U	inf	6 , U	4 , U	inf
1	U,V		4 , V	5 , V	4 , U	8 , V
2	U,V,W			5 , V	4 , U	8 , V
3	U,V,W,Y			5 , V		8 , V
4	U,V,W,Y,X					7 , X
5	U,V,W,Y,X,Z					

Forwarding table in U:

Destination	**Link**
V	(U,V)
W	(U,V)
X	(U,V)
Y	(U,Y)
Z	(U,V)

Question 6	**15 marks**

For the graph shown in Figure 2, the Distance Vector algorithm is being used and has **converged** for the link costs shown in Figure 2. Each node uses poison reverse and the distance vectors stored by each node **at convergence** are:

```
          A    B    C    D    E
D_A = [ 0    1    3    1    2 ]
D_B = [ 1    0    2    2    3 ]
D_C = [ 3    2    0    4    5 ]
D_D = [ 1    2    4    0    1 ]
D_E = [ 2    3    5    1    0 ]
```

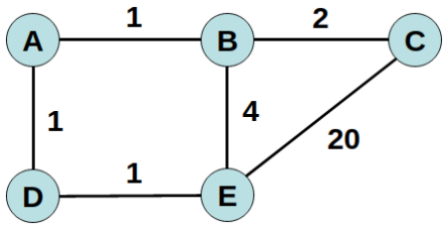


Figure 2: Graph for Question 6 corresponding to the converged distance vectors provided.

The link cost between B and C then increases to a cost of 200 as shown below in Figure 3. This causes B and C to perform an update of their distance vectors.

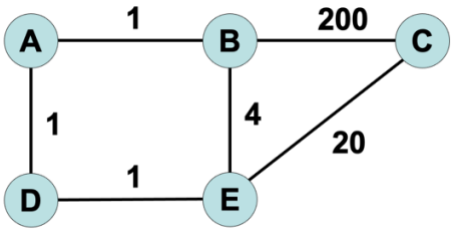


Figure 3: Graph for Question 6 after the cost increase of the B-to-C link.

*Answer all parts of the question **in your own handwriting** and **show all your work for full marks.***

(a) [5 marks] Compute the updated distance vector for B (i.e., compute D_B) after one iteration of the distance vector algorithm for B before any communication occurs.

*Hint: Due to poison reverse, when beginning its update **B has the following** distance vectors from its neighbours:*

```
          A      B      C      D      E
D_A = [ 0      inf    inf    1      2    ]
D_C = [ inf    inf    0      inf    inf  ]
D_E = [ 2      3      5      1      0    ]
```

Solution:

```
D_B = [
    min(1, 1+0   , 200+inf, 4+2) = 1    <- [1 mark]
    min(0, 1+inf, 200+inf, 4+3) = 0    <- [1 mark]
    min(2, 1+inf, 200+0   , 4+5) = 9    <- [1 mark]
    min(2, 1+1   , 200+inf, 4+1) = 2    <- [1 mark]
```

```
    min(3, 1+2  , 200+inf, 4+0) = 3   <- [1 mark]
]
```

(b) [3 marks] Based on your answer to part (a), and given that poison reverse is in operation, state the distance vectors that B communicates to its neighbours at this first iteration of the distance vector algorithm.

Solution:

To A: D_B = [inf 0 9 inf inf]
To C: D_B = [1 0 9 2 3]
To E: D_B = [1 0 inf 2 3]

(c) [7 marks] Explain whether poison reverse avoids the "count to infinity" phenomena for this example.

Solution:

[2 mark] No, the "count to infinity" phenomena is not avoided.

[2 marks] The loop B-E-D-A will count up until E finds the link (E,C) to be the lowest cost path to C.

[3 marks] This should only take two increases in the cost DE(C) (i.e., 5 to 12, then 12 to 20), but this is still the "count to infinity" phenomena of bad news taking multiple cycles to count up in increments until converging the new low-cost paths.

Question 7	**10 marks**

Provide one argument for and one argument against the use of Network Address Translation (NAT) in a network where the network layer of all devices uses IPv6 addresses, and all routers are IPv6 capable.

*Answer all parts of the question **in your own handwriting!***

Solution:
Mostly taken from link in the lecture slides:
https://blogs.infoblox.com/ipv6-coe/you-thought-there-was-no-nat-for-ipv6-but-nat-still-exists/
Arguments against:

- NAT breaks the layered internet architecture (because it changes both the IP address and socket values) and IPv6 address space is sufficient to provide every interface with a unique IP address, hence it is an unnecessary to break of the layered internet architecture.
- There is not an RFC specifying how NAT for IPv6 should operate.
- Causes problems for applications that require native connectivity and embed addresses inside the protocol payload.

Arguments for:

- For large organisation with many firewalls, NAT ensures that outgoing traffic comes back through the same firewall.
- Some small organisation have dual ISP links, a primary and a secondary, both of which are advertised router to the organisation. NAT allows the organisation to only receive traffic on the secondary link when it chooses, for example, when the primary link goes down.

[5 marks for a correct argument for]
[5 marks for a correct argument against]

Question 8	**15 marks**

Consider the graph of "congestion window size (in segments)" versus "transmission round" shown below in Figure 4, and assume the following:

- Every segment (without headers) is of size 1460 bytes.
- The headers always total size of 62 bytes.
- The round trip time (RTT) is always exactly 20ms.
- No packet loss occurs.
- TCP acknowledges every received packet (i.e., no delayed ACK mechanism).
- All acknowledgement segments are sufficiently small to ignore their transmission time.
- The link capacity is 6.088 Mbps.

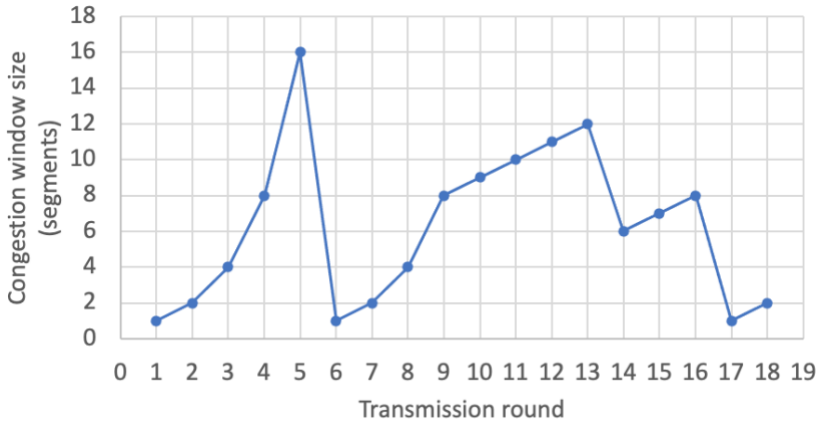


Figure 4: Graph for Question 8.

Answer all parts of the question ***in your own handwriting*** *and* ***show all your work for full marks****.*

(a) [11 marks] How long does it take for the first 10 segments to be acknowledged by the sender?

Solution:

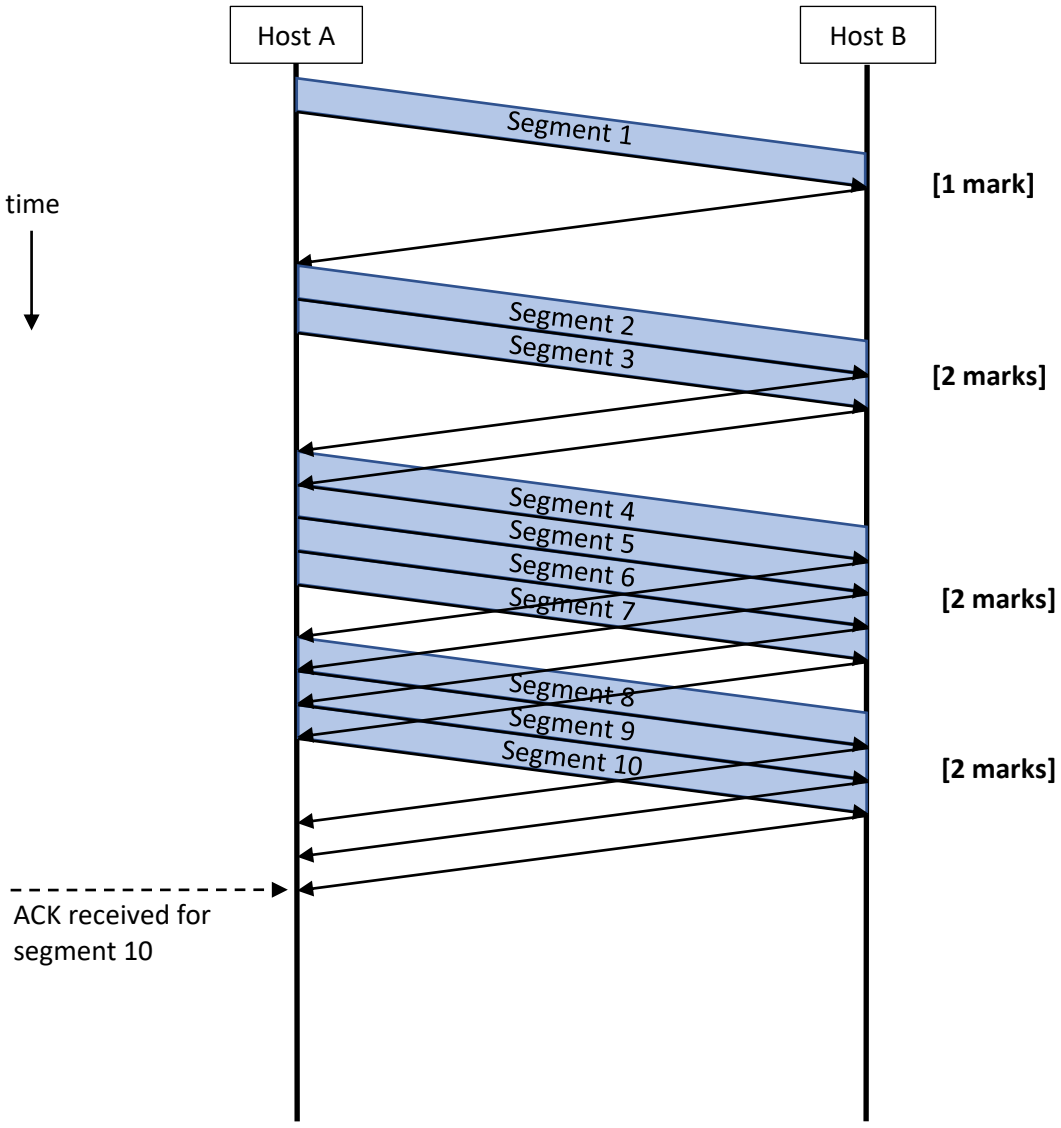
Transmission time per segments
= (1460+62) [bytes] * 8 [bits/byte] / (6.088*106 [bits/sec])
= 15.22*102*8/(6.088*106)
= 15.22*102*8/(60.88*105)
= 10-3 * 8 / 4
= 2*10-3 [seconds]
= 2 [milli-seconds]
[2 marks for working]
[2 marks for correct final value]

Sequence of pipelined transmits (assuming ACK packets of negligible size):

- Segment 1: ACK received at 22ms **[1 mark]**
- Segments {2,3}: ACK for packet 2 received at 44ms **[2 marks]**

- This allows packet 4 to be sent.
- Segments {4,5,6,7}: ACK for packet 4 received at 66ms **[2 marks]**
  - This allows packet 8 to be sent.
- Segments {8,9,10}: ACK for packet 8 received at 88ms, ACK for packet 10 received at 92ms **[2 marks]**

These numbers shown as a diagram:



(b) [4 marks] What is the utilization of the link for these first 10 segments to be acknowledged by the sender?

Solution:

Utilisation = fraction of time sender is busy = (10 [segment] * 2 [ms/segment] / (92 [ms]) = 21.7 %

[2 marks for working]

[2 marks for correct final value]

Question 9	**15 marks**

Consider the following scenario:

- You arrive at a public institution you have never visited before.
- Then you get out your smartphone and connect to the unsecured public Wi-Fi of the institution (which does not require a password and does not require you to accept terms & conditions).
- Then you open the internet browser and request a web address that has never been requested by anyone else on the network of the public institution where you are (for example, the web address www.obscure.com.au)
- You wait for the web page to load.

Describe in chronological order **ONLY** the application layer, transport layer and network layer packets that are sent-from and received-by your smartphone as this scenario unfolds (i.e., ignore link and physical layers).

*Answer all parts of the question **in your own handwriting** and **show all your work for full marks**.*

Solution:

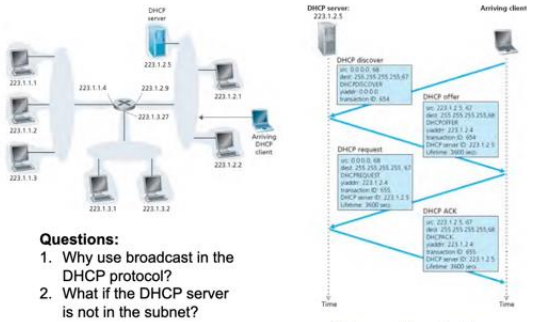
- **[4 marks]** Network layer DCHP messages to obtain an IP address. As per Mod4L1, there are 4 messages: DCHP discover, DCHP offer, DHCP request, DHCP ACK
- **[3 marks]** Application layer DNS messages to obtain IP address of webpage. As per Mod6L1, there are 2 messages from the smartphones point of view, DNS query, DNS response.
    - Other messages for the local DNS to query the {authoritative, top-level, root} DNS servers are not seen by the smartphone.
- **[3 marks]** Transport layer connection established by the browser. As per Mod5L2, this is a 3-way handshake where data may be sent from client to server with the third message, hence TCP SYN sent from the smartphone and then SYNACK received.
- **[3 marks]** Application layer request the web page of HTTP and displays the response, as per Mod6L1.
- **[2 marks]** HTTP requests sent as part of the third message of the TCP handshake.

Relevant slides from lectures:

DCHP slide:

THE UNIVERSITY OF MELBOURNE

DHCP: Dynamic Host Configuration Protocol



Questions:

1. Why use broadcast in the DHCP protocol?
2. What if the DHCP server is not in the subnet?

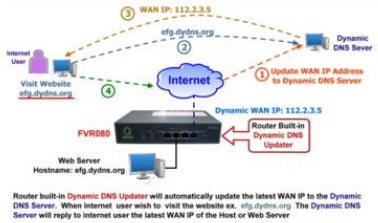
yiaddr: your internet addr

Module 4 – Lesson 1 38

DNS slide:

THE UNIVERSITY OF MELBOURNE

Dynamic DNS



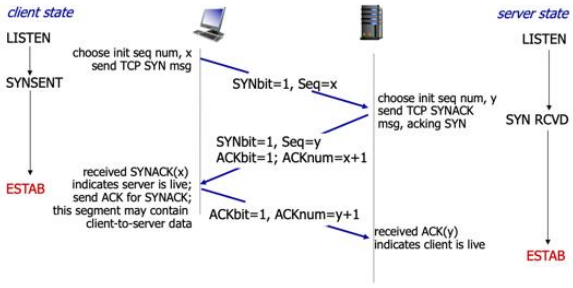
- The standardized method of dynamically updating domain name server records is prescribed by **RFC 2136**, commonly known as dynamic DNS update.
- Dynamic DNS providers offer a software client program that automates the discovery and registration of the client system's public IP addresses. The provider then might use RFC 2136 to update the DNS servers.
- Many home networking modem/routers include client applications in their firmware, compatible with a variety of DDNS providers.

Module 6 - Lesson 1 30

TCP slide:

THE UNIVERSITY OF MELBOURNE

TCP 3-way handshake



Remember that seq numbers are chosen randomly!

Module 5 - Lesson 2 29

HTTP slide:

THE UNIVERSITY OF MELBOURNE

Hyper Text Transfer Protocol (HTTP 1.1)

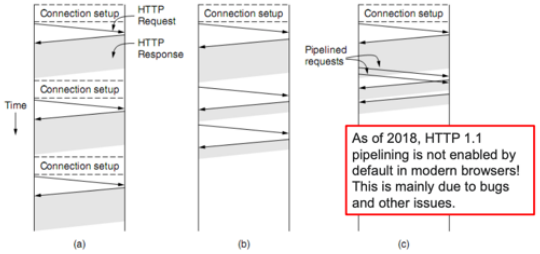
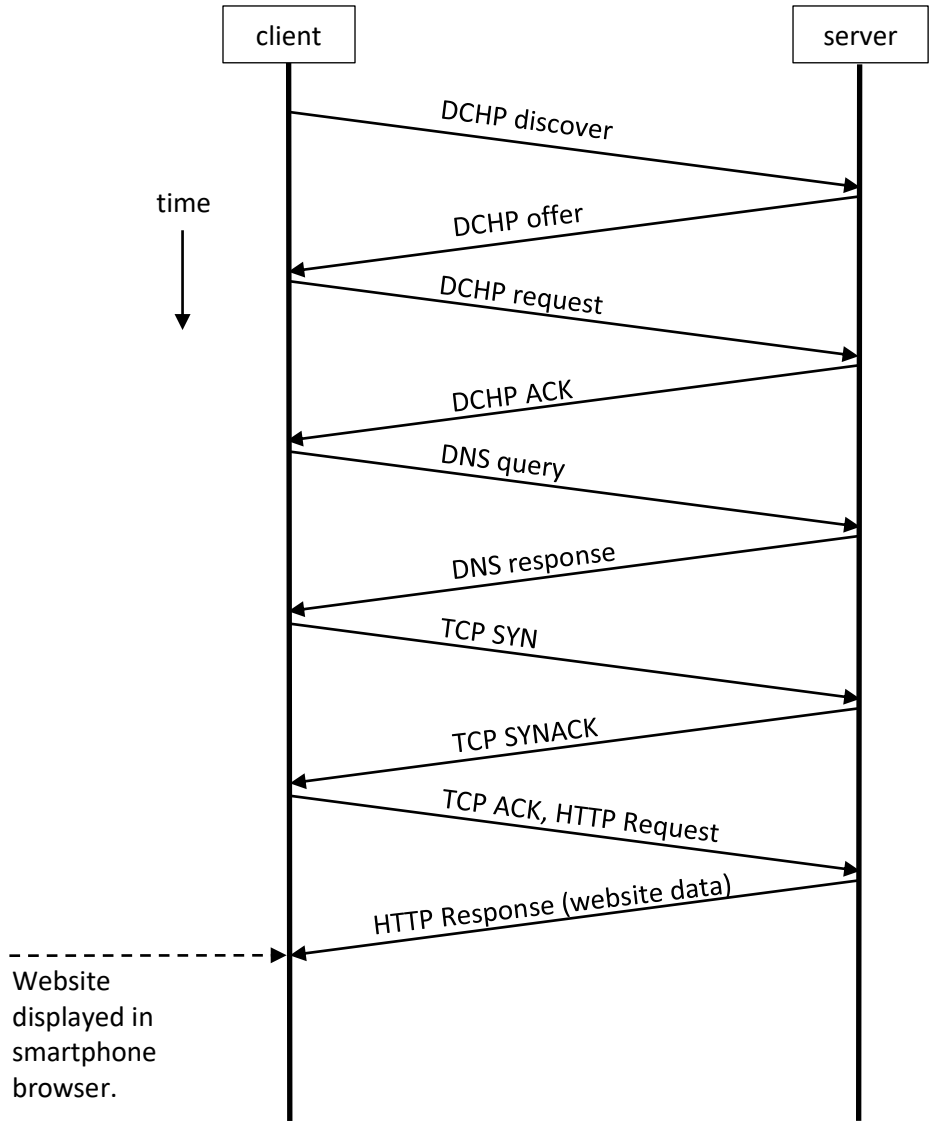


Figure 7-36. HTTP with (a) multiple connections and sequential requests. (b) A persistent connection and sequential requests. (c) A persistent connection and pipelined requests.

https://en.wikipedia.org/wiki/HTTP_pipelining

Module 6 - Lesson 1 14

Solution as a diagram:



Question 10	**25 marks**

The Remote Sensing Student Society (RSSS) of the University of Melbourne has approached you for communication networking advice with implementing their own transport layer reliable data transfer protocol, i.e., they do not want to use UDP nor TCP. They have developed a custom-made IoT device that:

- Records the 20 bytes worth of measurements every 10 seconds (which is temperature, pressure, humidity, luminosity, and time).
- Has sufficient storage for 200 sets of measurements, i.e., 2000 seconds worth of data.
- Is equipped with a cellular connection.
- Is placed in an area of outback Australia without any nearby electricity or wired internet.
- Needs to send the data to a dedicated computer with a fixed IP address in Melbourne, called the "base computer".
- Preliminary experiments indicate a round trip time (RTT) from the IoT device to the base computer in Melbourne and back of around 5 seconds.
- The power consumption of the IoT device is proportional to the amount of data that is sent and received.

The RSSS have already configured the IoT device and the base computer to connect with the network layer for sending and receiving using the IP protocol.

Advise the RSSS on the details of a reliable data transfer protocol that they could implement on the IoT device and the base computer.

*Answer all parts of the question **in your own handwriting** and **show all your work for full marks**.*

(a) [15 marks] Specify the pipelining protocol and headers for sending the data, explaining the intentions of your specifications and any assumptions that you make.

Solution:

Considerations:

- Use RDT3.0 as per lectures for handling bit errors and lost packets.
    - Only needs to be implemented as a uni-directional protocol because RSSS has not requested sending data from the base computer to the remote device.
- Stop-and-wait (ARQ) should be the smallest header as only 2 sequence number required (0 and 1).
- Stop-and-wait (ARQ) maybe not be sufficient if the cellular connection is error prone because the RTT is half of the measurement period.
- Increase utilisation by using pipelining.
- Selective Repeat pipelining preferred because:

    - Individual acknowledgement of packets reduces the number of necessary retransmissions.
    - Assume that the base computer has plenty of available memory for buffering.
    - Assume that the remote device has the capacity to run many timers.
- As can only buffer 200 measurement (i.e., messages) sequence number range of 2^8=256 is sufficient.
- Cellular link layer has its own error detection, so use simple error detection same as UDP and TCP
- Assume the remote device and base computer do now receive messages from any other sources, hence do not need message types or socket numbers.
- Keep the window size relatively small so that events where all message in a prolonged period are lost does not result in a significant amount of resending.
    - Only need the sequence number to be twice the window length.
- Could consider using the buffering on the remote device to send multiple measurements combined in one packet, this would reduce the number of acknowledgement messages.
- If the buffer on the remote device is full, then overwrite out data to be consistent with sampling at a lower frequency.
    - Assume that we can get advice from RSSS as to whether this is suits their purpose for the data.
- Key parameters:
    - Number of measurements in each segment: 2, which is 20 seconds of data
    - Window size: 4 segments, which allows 80 seconds of data in the pipeline at any one time
    - Timeout duration: keep a running estimate of the RTT and its deviation, set the timeout duration to estimate + 3*deviation, capped at a maximum of 10 seconds to match the measurement period.
- Header fields:
    - Sequence number, 4 bits long:
        - Hence 16 possible sequence numbers
        - Each number indexes a segment of 2 measurements
        - This is double what is required for a window of size 4, and hence allows for increase the window up to length 8 segments.
    - Checksum, 8 bits long, as messages are small, use a small checksum than UDP and TCP

(b) [5 marks] For the key parameters that need to be determined in your specification (e.g., window size, sequence number length, error detection approach), specify what tests you would perform during the first week of commissioning the device to determine these parameters. Explain the purpose of the tests you suggest.

Solution:

- For error detection:
  - Log on the main computer the events where corrupted data was received, logging both the corrupted data and the "correct" message that was eventually received.
  - Count on the remote device the number of corrupted ACK messages received. Logging more information about corrupt data events not feasible due to limited memory on the device.
- Log the times of received message on the main computer in an attempt to see any patterns of long period where all packets are lost.
  - It could be possible to avoid wasted transmission by increasing the window size (e.g., to 8 segments) for better utilisation and introducing a congestion window similar to TCP Reno that reduces the window to 1 segment on timeout and increase exponentially to the window size.
- Timeout duration:
  - Log any message that were received in duplicate at the base computer.
  - Count on the remote device the number timeouts that occurred.

(c) [5 marks] What diagnostic data do you recommend is collected during ongoing operation of the device? Is this data collected on the IoT device or on the base computer? Explain your answers.

Solution:

- As there is very little memory on the remote device, only consider logging what cannot be inferred from the packets received at the base computer, for example:
  - Count of corrupt ACK
  - Count of timeouts causing retransmission
  - Time when the 10 highest buffer usage levels occurred.
- On the base computer, storing "everything" could be considered wasteful. Likely RSSS is most interested in knowing the risk levels of their data is of being lost.
  - Lost data is obvious from the fact that the data is missing, so nothing extra to record.
  - Record the previous 100 message that are received in duplicate. If the cellular connection is particularly patchy, it may be worth adding 2 bits of flags for timeout and corrupt ACK so that this data is available at the base computer for ongoing monitoring and diagnosis.
  - Record details of the top 100 largest times between receiving packets at the base computer, i.e., > 10 seconds (plus buffer) means packets are not making it through to the base computer for that period.

END OF EXAM