

GJ Assignment

by Gabor Jonas

FILE	994_GABOR_JONAS_GJ_ASSIGNMENT_227510_1138623103.DOCX (171.5K)		
TIME SUBMITTED	23-JAN-2020 08:11PM (UTC+0000)	WORD COUNT	1324
SUBMISSION ID	119000633	CHARACTER COUNT	6961



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Network Theory

Student name: Gabor Jonas

Student number: 1705136

Module Number: ACCA6015

Module: Networked Applications

Table of Contents

1. Transmission Control Protocol	3
1.1 Connection Establishment	3
1.2 Two Generals' problem	4
2. Packet fragmentation	5
2.1 Reassembly.....	6
3. Interoperability in Networked Applications	6
4. References	7

1. Transmission Control Protocol

Transmission Control Protocol (TCP) is one of the main protocols and is implemented in the transport layer of the TCP / IP reference model. It's intended to provide a reliable, sequential transmission of a stream between applications on two devices. Most of the important services on the Internet are available through TCP. Other applications where lower latency is more important than avoiding packet loss may use the User Datagram Protocol (UDP). It's described by Vinton Cerf and Robert Kahn in 1974. [1]

1.1 Connection Establishment

The header of the TCP segment contains six 1-bit fields used to handle TCP processes:

- **SYN**: Synchronization message to establish or connect request to maintain
- **FIN**: Request to disconnect
- **ACK**: Acknowledgment message, response to SYN / FIN message indicating receipt of message

Before starting the data transfer, the connection between the two hosts must be established. Because of the maximum transportable data size (MTU) is limited in a TCP segment, the protocol must split the larger data and restore it on the other side in the same order. Therefore, it's necessary to match the sequence number of the segments. This connection process is called a three-phase handshake, with the following steps:

- Host 1 initiates the connection with destination Host 2 by sending a SYN segment in which it also sends its start sequence number ($SEQ = x$)
- Host 2 receives the segment and records the starting number of Host 1, then sends a receipt with the sequence number of the next segment ($ACK = x + 1$) and its own starting sequence number ($SEQ = y$)
- Host 1 receives the answer, which learns Host 2's starting number (y) and sends the next segment, acknowledging the request ($ACK = y + 1$).

The data transfer will then begin and the connection will remain open until either side requests to close it.

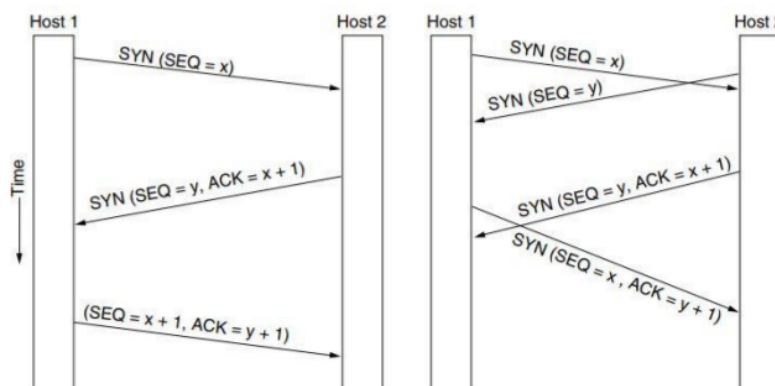


Figure 1 Three-way handshake [2]

Each step of a TCP connection is called a state:

- **CLOSED**: This is the default state from which the connection establishment process starts.
- **LISTEN**: The host (usually the server) is waiting for a synchronization request (SYN), it has not yet sent its own SYN message
- **SYN-SENT**: The host (usually the client) has sent the SYN message and is waiting for a response from the other host (server)
- **SYN-RECEIVED**: A connection request (SYN) is sent and received, waiting for the other party to acknowledge receipt (ACK)
- **ESTABLISHED**: Once both hosts are in this state, data transfer can begin and continue until either party initiates the connection termination
- **CLOSE-WAIT**: The station has received a disconnection request (FIN) from the other party. Waiting for the local application to be acknowledged before sending the appropriate response message
- **LAST-ACK**: The station has already received and acknowledged a disconnection request, has sent its own FIN message, and is waiting for the other party's receipt (ACK) of this request
- **FIN-WAIT-1**: Waiting to acknowledge the sent FIN message or to receive a disconnection request from the other party
- **FIN-WAIT-2**: Receipt received for the sent disconnection message, waiting for the other party's FIN message
- **CLOSING**: The station has received and acknowledged the other party's FIN message, but has not received a receipt for its own FIN message
- **TIME-WAIT**: Wait for all packets to die

1.2 Two Generals' problem

The basic requirement for secure communication is for the sender to make sure that the message being sent has been received by the receiving party, so that both parties are certain that the operation has been completed. The danger is that, as a result of manipulation or incorrect transmission, one of the parties believes that the operation has been successfully completed. The question is how the sending party can verify the success of the operation.

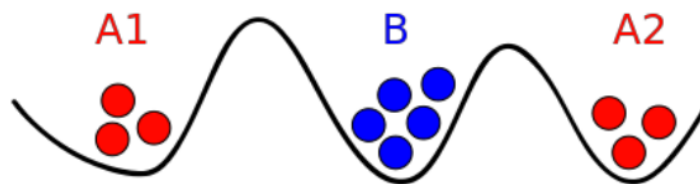


Figure 2 Two General's problem [3]

The Two Generals' Problem illustrates the difficulty of the confirmation. In this experiment two armies (A1 and A2) prepare to attack a city (B). The only way for the generals to communicate is by sending a messenger through the valley, however the message can be

captured by the city's guard. The question is how to reach agreement on the time of the attack, since none of the generals know that the other party successfully received the message.

2. Packet fragmentation

In the Internet Protocol Specification MTU is specified as *"The maximum sized datagram that can be transmitted through the next network is called the maximum transmission unit (MTU)."* [4]

IP fragmentation refers to breaking an IP data datagram into several data blocks (fragments) if the total length of the data packet is greater than the maximum transmission unit of the network interface. The maximum size of an IP datagram is 65535 bytes including 20 bytes header. However, the maximum possible packet size depends on the infrastructure components used, since different packet switching techniques allow different maximum packet sizes.

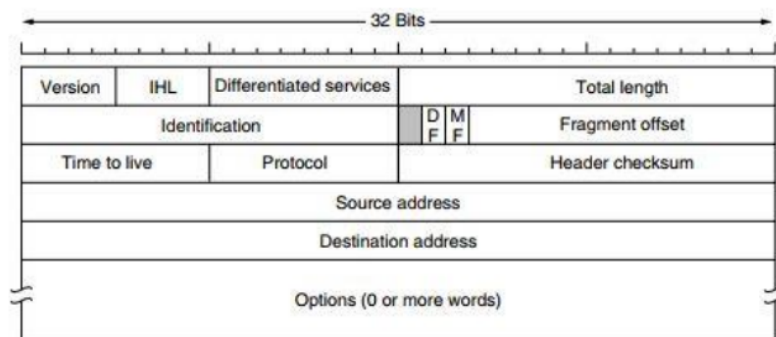


Figure 3 IPv4 Header [2]

- **Version:** This field allows different IP versions to operate on the same network, so that each migration can take place continuously, without having to migrate all the equipment on the whole network at the same time. The version field is set to 4 if IPv4, 6 if the packet belongs to IPv6.
- **IHL:** This field carries information about the length of the header in 32-bit words, ranging from 5 to 15, representing a minimum of 20 to 60 bytes in headers.
- **Differentiated services:** It's used to mark the packet with its service class.
- **Total Length:** This field contains the total length of the packet in bytes, including the header and the data portion.
- **Identification:** This field is necessary for the target host to compile chunks of higher protocols. After splitting each datagram, all pieces are transmitted with the same ID.
- **DF (Do not fragment):** Single bit indicating that the datagram cannot be fragmented.
- **MF (More Fragments):** Single bit indicating that there are more pieces of the message.

- **Fragment offset:** Specifies where the part of the fragment is in the package.
- **Time to live:** This field limits the amount of time a packet can spend on a network.
- **Protocol:** This field indicates the protocol for which the packet is being transmitted.
- **Header checksum:** The checksum is used to detect errors.

2.1 Reassembly

In this example the packet size is 5140 bytes and sent through ethernet so the MTU is 1500 bytes.

Original IP Datagram

Sequence	Identification	Total Length	MF	Fragment Offset
0	344	5140	0	0

IP Fragments

Sequence	Identification	Total Length	MF	Fragment Offset
First packet	345	1500	1	0
Second packet	345	1500	1	185
Third packet	345	1500	1	370
Fourth packet	345	700	0	555

Disadvantages of IP fragmentation [5]:

- CPU and memory overhead
- If one fragment of a datagram is dropped, the original datagram has to be dropped as well

3. Interoperability in Networked Applications

Peter Wegner defines interoperability as *“the ability of two or more software components to cooperate despite differences in language, interface and execution platform.”* [6]

4. References

- [1] V. G. Cerf and R. E. Kahn, "A Protocol for Packet Network Intercommunication," *IEEE Transactions on Communications*, vol. 22, no. 5, pp. 637-648, 1974.
- [2] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, Fifth ed., Prentice Hall, 2011.
- [3] Wikiwand, "Two Generals' Problem," Wikiwand, [Online]. Available: https://www.wikiwand.com/en/Two_Generals%27_Problem. [Accessed 20 01 2020].
- [4] I. S. Institute, "Internet Protocol," 1981. [Online]. Available: <https://www.rfc-editor.org/rfc/pdf/rfc791.txt.pdf>. [Accessed 15 01 2020].
- [5] C. Wu and E. Vyncke, "Resolve IPv4 Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPsec," Cisco, 08 01 2019. [Online]. Available: <https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html>.
- [6] P. Wegner, "Interoperability," *ACM Computing Surveys*, vol. 28, no. 1, March 1996.

GJ Assignment

GRADEMARK REPORT

FINAL GRADE

31 / 100

GENERAL COMMENTS

Instructor

Generally good sources used. Number 3 is weak and, while it's used for an image (which is fine), it's the only source in that section.

This has the makings of a good report, but sadly is clearly a week late but still a very long way from finished. There's nothing wrong with what you have - marks are simply limited through lack of depth and the incompleteness of the report. If you're having any issues which the university can help with, please don't hesitate to speak to me.

Engagement with Literature Skills (20): 11

Knowledge and Understanding Skills (30): 6

Cognitive and Intellectual Skills (30): 7

Transferable Skills for Life and Professional Practice (20): 7

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

