Bialystok University of Technology

Faculty of Electrical Engineering

Course name:
Computer Networks

Course code: IS-FEE-10082S

Laboratory classes manual guide

Laboratory exercise number: **2**

Subject of the laboratory exercise:

Analysis of the operation of TCP/IP family protocols

Manual prepared by:
Andrzej Zankiewicz, PhD

Białystok 2025

1. General characteristics of the exercise

The TCP/IP family protocols are currently the most commonly used group of protocols at layers 3 and 4 of the OSI model. This group includes the basic layer 3 protocol, which is IP (Internet Protocol), and layer 4 protocols: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), as well as auxiliary protocols such as ARP (Address Resolution Protocol) and ICMP (Internet Control Message Protocol).

These protocols were designed for fault-tolerant military networks and are now widely used in the global Internet, as well as in local networks not connected to the Internet.

The aim of the exercise is to learn the properties and principles of operation of the TCP/IP family of protocols by observing and analyzing data units transmitted over the network by these protocols.

2. Preparation for classes

Before starting the exercise, you should read the following materials:

- The entire contents of this manual
- Descriptions of the IP, TCP, UDP, ICMP and ARP protocols that can be found, for example, in the textbook "TCP/IP from the inside. Protocols" [1] or in the relevant RFC documents [2]
- Wireshark documentation [3]

The above-mentioned information is the **minimum** theoretical knowledge necessary to start and properly complete the exercise.

3. Basic information about the TCP/IP family of protocols

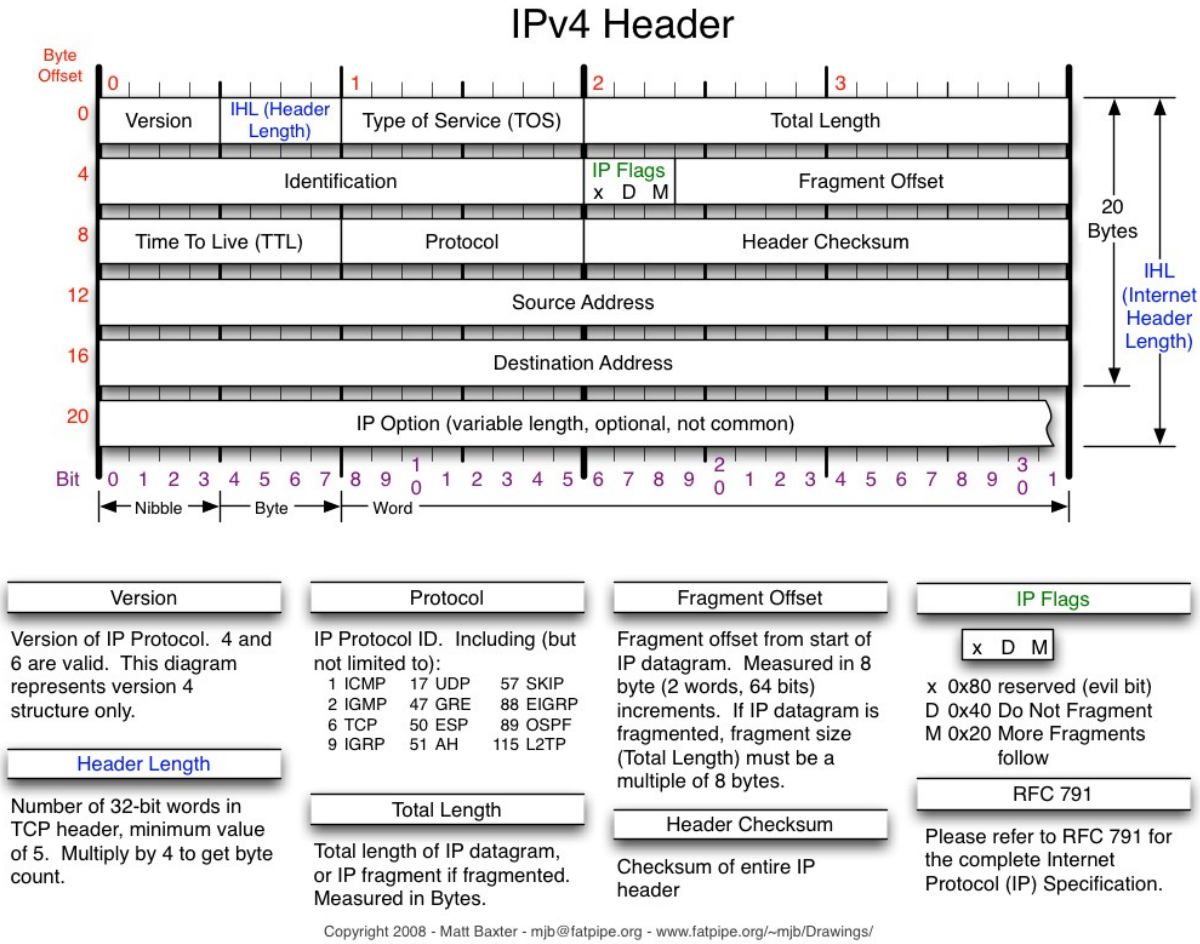
In the TCP/IP protocol family, the basic protocol operating at layer 3 of the OSI model is the IP protocol, which is a connectionless protocol that allows the transfer of data units called packets. To identify individual stations, the IP protocol uses 32-bit numbers called IP addresses or logical addresses. An IP address consists of two parts, which are the network address and the host (station) number in that network, respectively. The place where the address is divided into these parts is determined by the network mask provided when configuring the station.

Layer 4 of the OSI model can use the connection-reliable TCP protocol or the simple connectionless UDP protocol, used mainly in query-response applications. These protocols enable the simultaneous creation of multiple transport connections over a single network connection (one IP address). They use 16-bit port numbers to distinguish individual connections.

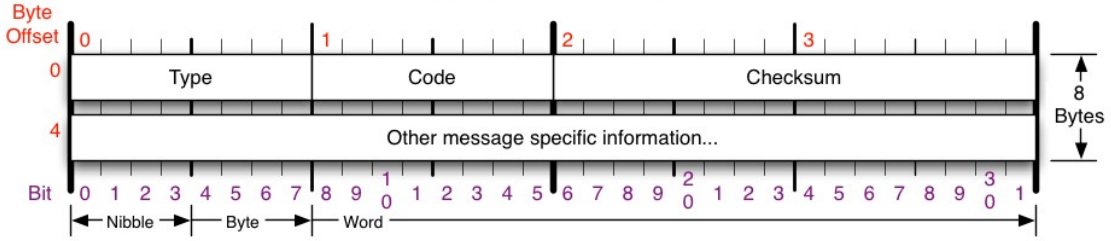
For testing purposes and error signaling in TCP/IP networks, the auxiliary ICMP protocol is used, which is an integral part of the TCP/IP protocol family. It allows, among other things, checking the availability of a given station at the layer 3 level and informing about the unavailability of destination stations.

The use of TCP/IP protocols in Ethernet local networks is enabled by the ARP auxiliary protocol used to determine the physical addresses (MAC) of stations based on their logical addresses (IP). This allows for delivery of an IP packet encapsulated in an Ethernet frame to the destination station.

4. Structure of headers of selected protocols



ICMP Header



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceeded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

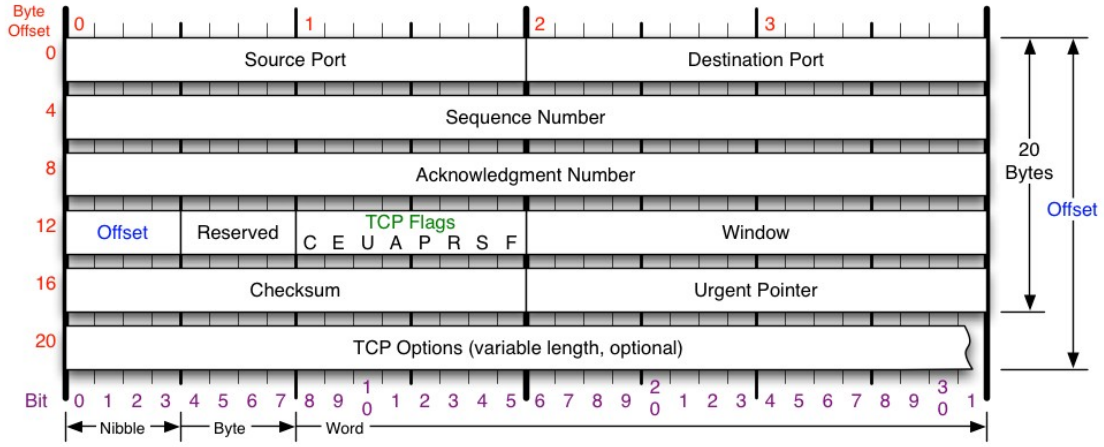
Checksum of ICMP header

RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

Copyright 2008 - Matt Baxter - mjb@fatpipe.org - www.fatpipe.org/~mjb/Drawings/

TCP Header



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

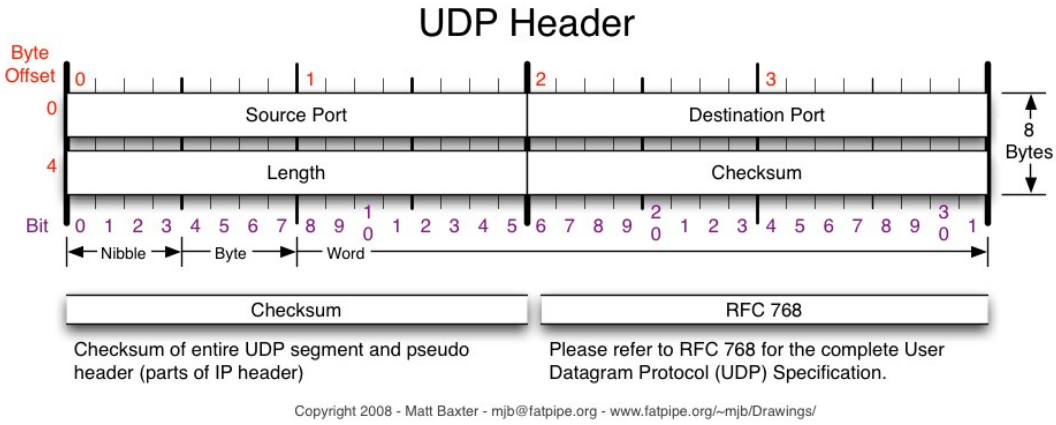
Offset

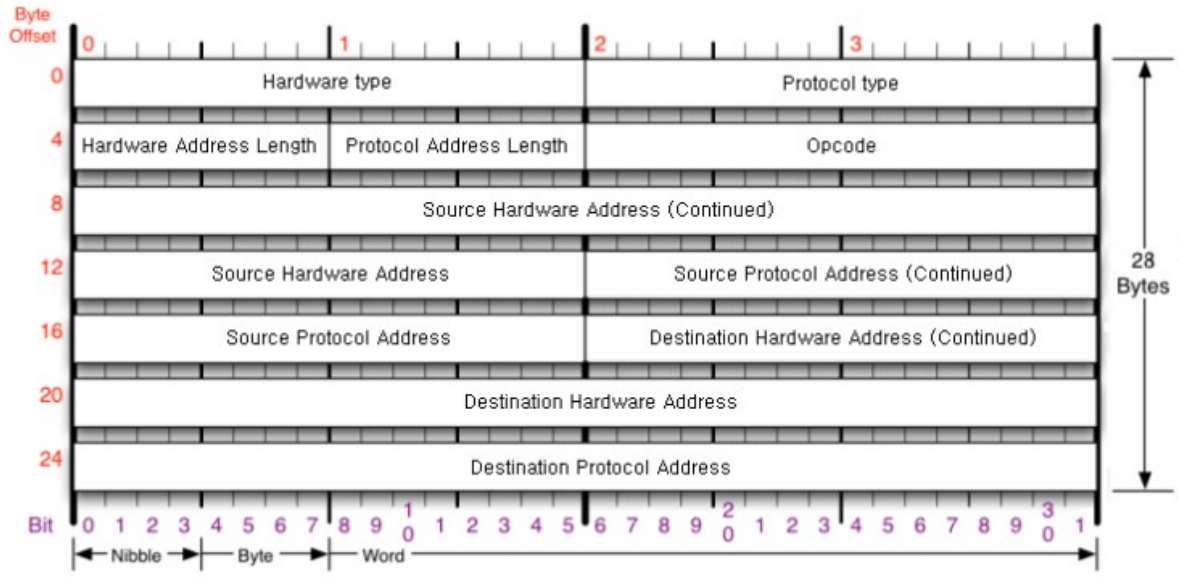
Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Copyright 2008 - Matt Baxter - mjb@fatpipe.org - www.fatpipe.org/~mjb/Drawings/





Hardware type – specifies the type of address used by the hardware. For Ethernet networks, the value of this field is 1.

Protocol type – specifies the network protocol (Layer 3) whose addresses are mapped to hardware addresses using the ARP protocol. For the IP protocol, the value of this field is 0x0800.

Hardware Address Length – specifies the size of the hardware (MAC) address that ARP finds from the network protocol address. For Ethernet, the value of this field is 6 (MAC address has 6 bytes, 48 bits).

Protocol Address Length – specifies the size of the network protocol address (layer 3) based on which the ARP protocol finds the hardware address. For networks with the IPv4 protocol, the value of this field is 4.

Opcode – The contents of this field indicate whether the message is an ARP request (value 1), an ARP reply (value 2), a RARP request (value 3), or a RARP reply (value 4).

Source Hardware Address – hardware address of the host sending the message. In the case of an ARP response, this field contains the found MAC address.

Source Protocol Address – network (IP) address of the host sending the message.

Destination Hardware Address – hardware address of the host for which the ARP message is intended. In the case of an ARP request, this field is set to zero.

Destination Protocol Address – the network (IP) address of the host for which the ARP message is intended. In the case of an ARP request, this field contains the IP number of the host whose MAC address is to be found.

5. Laboratory exercise plan

1. Specify the network configuration of the computer located at the laboratory station (IP address, subnet mask, default gateway address). Determine the IP address of the network to which this computer is connected.
2. Using Wireshark, trace the exchange of IP packets related to the execution of the ping command between two computers located in the same IP network. It is advisable to set the filters in Wireshark appropriately so that only frames from the communication of interest are recorded. Record and interpret the values contained in the individual fields of the IP and ICMP protocol headers for sent and received packets.
3. Using Wireshark, trace the IP packet exchange associated with the execution of the traceroute program to the computer indicated by the instructor. Record and interpret the values contained in the individual fields of the IP and ICMP protocol headers. Describe in detail the operation of the traceroute program using data from the captured packets.
4. Send a single ping request to a selected computer located in the same IP network with a packet size larger than the maximum transmission unit (MTU) size of the given station's interface. In Windows family systems, the default MTU value for Ethernet interfaces is 1500 bytes. The size of the packet sent with the ping command can be set using the -l option of this command. Use Wireshark to record frames with the sent query and received response. Describe the IP packet fragmentation process based on the analysis of the content of these frames. In particular, the contents of the "fragmentation offset", "identification" and tag fields in the headers of sent and received IP packets should be correctly interpreted.
5. Check the network behavior when an IP packet is sent with the DF ("do not fragment") flag set and a size larger than the smallest MTU value on the connection path. You can use the -f option of the ping command to send a packet with the DF flag set.

6. Record and analyze ARP messages exchanged during a connection attempt (e.g., ping) between two computers in the following situations:

- both computers are on the same IP network,
- one of the computers is working on a different IP network.

Before recording ARP messages, you must clear the ARP buffer by executing the `arp -d *` command.

Read the value in the Type field of Ethernet frames containing the ARP protocol request and response. What MAC addresses are these frames sent to?

7. Trace the exchange of UDP datagrams related to the use of the DNS service. For this purpose, you can use, for example, the nslookup application. Record and interpret the values contained in each header field of sent and received UDP datagrams.

8. Record a TCP connection session using the WWW service. In order for the recorded session to have an acceptable length, you should use the WWW page specially prepared for this exercise. The address of this page is http://gateway/test.asp, where gateway is the IP address of the default gateway set in the network configuration of the computer used in the exercise.

It is advisable to set the relevant filters in the Wireshark application, e.g.:

```
tcp and ip.addr==gateway_IP and ip.addr==station_IP
```

Make a diagram showing the observed process of exchanging TCP segments, including the content of the "sequence number", "acknowledgement number" fields and the TCP Flags (e.g. SYN, ACK) in the TCP header. In particular, the diagram should distinguish the phases of establishing a connection, exchanging information and terminating the connection.

Exercise report

The report should include a description of the steps performed and the results recorded at each point of the exercise, along with any necessary comments explaining the essence of the individual operations supported by appropriate data captured with Wireshark.

6. Health and safety requirements

According to the rules specified in the first class and confirmed by students held. Appropriate health and safety regulations are also posted in the laboratory room.

7. References

1. Kevin R. Fall, W. Richard Stevens: TCP/IP Illustrated. Volume 1: The Protocols. 2nd Edition, Addison Wesley, 2011.
2. RFC documents (available on the Internet: http://www.rfc-editor.org).
3. Wireshark documentation (www.wireshark.org).
4. Lecture notes.