Institute of Computational Intelligence
Częstochowa University of Technology

ICMP in practice

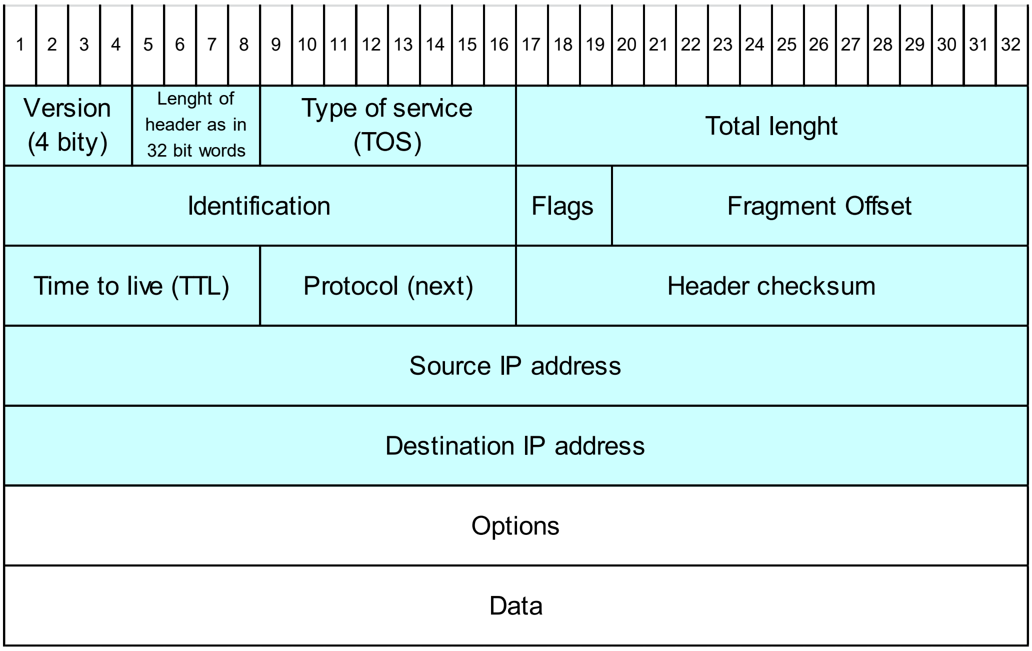
Foundations of computer networks laboratory

The objective of the exercises

The aim of the exercise is to familiarize with possibilities of Internet Control Message Protocol application.

Introduction

ICMP (Internet Control Message Protocol) has proposed to support the Internet Protocol (IP) in the case of troubles in deliver of IP datagrams. It is always encapsulated in IP. The structure of IP datagram in version 4 has shown below.



<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td></tr>
<tr><td colspan="4">Version
(4 bity)</td><td colspan="4">Lenght of header as in 32 bit words</td><td colspan="8">Type of service
(TOS)</td><td colspan="16">Total lenght</td></tr>
<tr><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td colspan="8">Time to live (TTL)</td><td colspan="8">Protocol (next)</td><td colspan="16">Header checksum</td></tr>
<tr><td colspan="32">Source IP address</td></tr>
<tr><td colspan="32">Destination IP address</td></tr>
<tr><td colspan="32">Options</td></tr>
<tr><td colspan="32">Data</td></tr>
</table>

In planned experiments the following fields of the IP header will be used:

- **Flags**
    - **reserved** – not in use,
    - **don’t fragment** – when the flag is set, the fragmentation of datagram by the routers is forbidden. In such case, when fragmentation is needed, e.g. is too long, the datagram is dropped and router sends to sender of dropped datagram the ICMP message about the occurrence.
    - **more fragments** – in the case of fragmentation, this flag is set for all parts of fragmented datagram except the last one.
- **Time to live (TTL)** – historically, every router should decrease the value of the field of the time (in seconds) spent in the routing of the datagram. Nowadays, every router decreases the field of one. When the value of field riches zero, the datagram is dropped. The router sends to sender of dropped datagram the ICMP message about the occurrence.
- **Source IP address** – the address (32 bits) of the sender.
- **Destination IP address** – the address (32 bits) of the addressee (recipient). The address consists of two parts – address of target network and address of target node (e.g. computer) in target network.

The header of ICMP includes only two information fields and the checksum of them. The fields are:

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td></tr>
<tr><td colspan="8">Type</td><td colspan="8">Code</td><td colspan="16">Header checksum</td></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td colspan="32">Data</td></tr>
</table>

- **Type** – message type (see table below – selected types),
- **Code** – reason of the issue (see table below).

Type	Code	Description	Type	Code	Description
0	0	**Echo replay**	**5**		**Redirect request**
3		**Destination unreachable**		0	for the network
	0	network unreachable		1	for teh host
	1	host unreachable		2	for the network fot TOS
	2	prtocol unreachable		3	for the host for TOS
	3	port unreachable	**8**	0	**Echo request**
	4	fragmentation required but forbidden	**9**	0	**Router advertisement**
	5	source route failed	**10**	0	**Router discovery/selection/solicitation**
	6	network unknown	**11**		**TTL expired**
	7	host unknown		0	in transit
	8	host isolated (absolete)		1	in defragmentation (one of fragment)
	9	network prohibited (by administator)	**12**		**Bad IP header**
	10	host prohibited (by administrator)		0	varius problems
	11	network unreachable for TOS		1	missing options but required
	12	host unreachable for TOS		1	bad length
	13	communication prohibited by administrator	**13**	0	**Timestamp request**
	14	host precedence violation	**14**	0	**Timestamp replay**
	15	shut down in progress	**15**	0	**Information request (absolete)**
4	0	**Bufers or queue full (absolete)**	**16**	0	**Information replay (absolete)**
			17	0	**Address mask request**
			18	0	**Address mask replay**

- **Data** – contains the first bytes (headers) of the frame, which was the cause of ICMP message.

Software and commands which applies ICMP

Ping

The application sends to selected node, e.g. computer, echo request, i.e. ICMP message type 8. The Addressee should send the answer, echo replay i.e. ICMP message type 0. It allows checking if selected node exists in the network and is available to communication. However, the echo replay can be prohibited by administrator, so the above procedure is not reliable. In default, the ping application in Windows operating systems sends 4 messages contain 32 bytes of data each. It could be changed using the options:

```
ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
```

```
       -l size        Send buffer size.
       -f             Set Don't Fragment flag in packet (IPv4-only).
       -i TTL         Time To Live.
       -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                      and has no effect on the type of service field in the IP
Header).
       -r count       Record route for count hops (IPv4-only).
       -s count       Timestamp for count hops (IPv4-only).
       -j host-list   Loose source route along host-list (IPv4-only).
       -k host-list   Strict source route along host-list (IPv4-only).
       -w timeout     Timeout in milliseconds to wait for each reply.
       -R             Use routing header to test reverse route also (IPv6-only).
       -S srcaddr     Source address to use.
       -4             Force using IPv4.
       -6             Force using IPv6.
```

Tracert

The task of the application is to show the list of routers on the path between two nodes (usually computers) in the network. Tracert sends to destination many the echo requests (ICMP type 8). However, in subsequent messages the initial TTL value is various. In the first requests TTL=1. It cause first router on the path changes TTL value to 0 and drops the message. This router sends to sender the new ICMP message type 11 (TTL expired) to inform the sender that the echo request has dropped. The type 11 ICMP message is encapsulated in IP protocol. In its header there is the IP address of the router. Then tracert sends another echo requests with higher values, i.e. TTL=2, 3, …. It allows recognizing addresses of all routers on the path. The procedure finishes when TTL value is high enough to reach the destination node, which sends echo replay message (ICMP type 0). In order to show also mnemonic addresses of the routers, tracert sends appropriate DNS queries to DNS servers. The procedure presented above can be modified by the following options:

```
tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

VisualRoute

This application works as tracert. However, the results are presented on the map of the world. The approximate localisation of the individual routers is acquired from registrators databases. See also http://en.utrace.de/. The light version of VisualRoute is free of charge for uncommercial use and available under http://www.visualroute.com/ address.

Course of exercise

Using ping application please examine the paths to the serves in various localisations and networks, e.g.

- Institute of Computational Intelligence of Częstochowa University of Technology (www.iisi.pcz.pl or www.ici.pcz.pl),

- various units of Faculty of Mechanical Engineering and Computer Science (e.g. www.wimii.pcz.pl, www.icis.pcz.pl, www.imc.pcz.pl),
- various units of Częstochowa University of Technology (www.pcz.pl, www.zim.pcz.czest.pl, www.wip.pcz.pl),
- various institution in Częstochowa, outside University,
- various institution in Poland, outside Częstochowa,
- various institution in your country,
- various institution in Europe outside Poland,
- various institutions in particular continents.

For the servers tested earlier please examine

- number of routers on the path to examined servers,
- the maximum size of frames allowed in the path to examined servers without fragmentation,
- how value of TOS field affecting communication.

Hint: Use options in ping application.

Use tracert for examination as above. Comment the various forms of results.

Try to simulate tracert operation using ping application. Hint: Use various initial values of TTL field.

Homework

Repeat the examination using VisualRoute Light.

The raport

In the report should contain the results obtained during classes and the comments. Are the paths optimal?