HACETTEPE UNIVERSITY

COMPUTER ENGINEERING DEPARTMENT

BBM 453 LAB EXPERIMENT 6 (ICMP)

Group No: 41

Yiğit Emir İşıkçı: 2200356028

Ahmet Eren Akbaş: 21945757

1) Introduction to ICMP Wireshark Lab

The Internet Control Message Protocol, or ICMP for short, is super important for keeping computer networks running smoothly. It helps figure out if there are any issues with the connection and how data gets from one computer to another. In this Wireshark Lab about ICMP, we get to really see how ICMP works by doing some hands-on activities.

We're going to look closely at messages that come from two important tools we use in networks: Ping and Traceroute. Ping is a tool that helps us see if another computer on the network can be reached and how long it takes to get a message to it and back. If any messages get lost on the way, Ping will tell us. Traceroute is another tool that shows us the path messages take to reach another computer and helps us see where delays happen.

2) Part 1: Ping

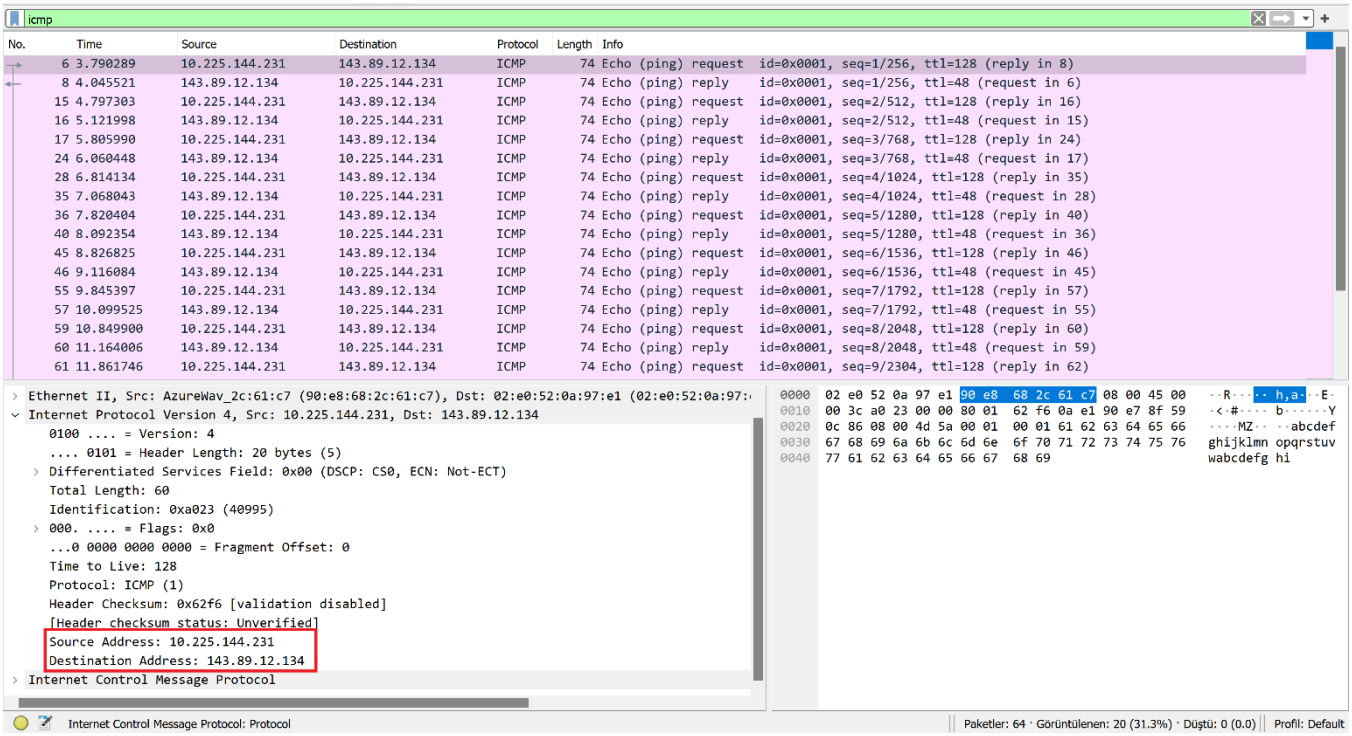
```
C:\Windows\System32>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=255ms TTL=48
Reply from 143.89.12.134: bytes=32 time=324ms TTL=48
Reply from 143.89.12.134: bytes=32 time=254ms TTL=48
Reply from 143.89.12.134: bytes=32 time=254ms TTL=48
Reply from 143.89.12.134: bytes=32 time=272ms TTL=48
Reply from 143.89.12.134: bytes=32 time=289ms TTL=48
Reply from 143.89.12.134: bytes=32 time=254ms TTL=48
Reply from 143.89.12.134: bytes=32 time=314ms TTL=48
Reply from 143.89.12.134: bytes=32 time=326ms TTL=48
Reply from 143.89.12.134: bytes=32 time=341ms TTL=48

Ping statistics for 143.89.12.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 254ms, Maximum = 341ms, Average = 288ms
```

- The Ping program successfully reached the host www.ust.hk with the IP address 143.89.12.134, indicating that the host is live and responding.
- The round-trip times (RTT) fluctuated between 254ms and 341ms. This variability in RTT could be due to network congestion, routing paths changes, or the load on the host server.
- All ten ICMP packets sent received a reply, which shows there was no packet loss during this particular ping session.

2.1) What is the IP address of your host? What is the IP address of the destination host?



The IP address of my host, from which the ping was initiated, is 10.225.144.231. This can be seen as the source address in the IP header for the echo request packets.

The IP address of the destination host, to which the ping was sent, is 143.89.12.134. This is shown as the destination address in the IP header for the echo request packets.

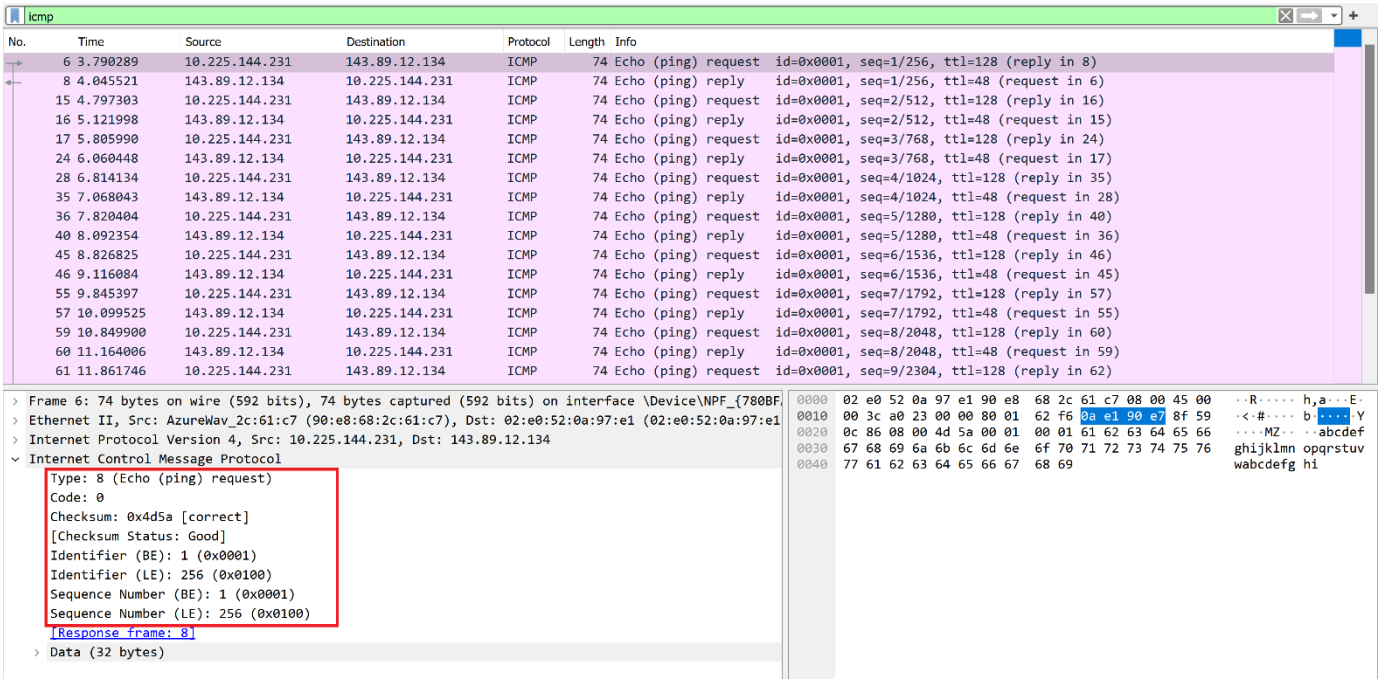
2.2) Why is it that an ICMP packet does not have source and destination port numbers?

An ICMP packet does not have source and destination port numbers because it is not designed to carry application-level data, which is what ports are generally used for.

Instead, ICMP is used for sending error messages and operational information pertaining to IP operations. Port numbers are associated with the Transport layer protocols like TCP and UDP, which facilitate application data transfer.

ICMP operates at the network layer and serves different purposes, such as diagnosing network communication issues or reporting about unreachable hosts or networks. This distinction is why ICMP packets are structured without port numbers, unlike TCP or UDP packets.

2.3) Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

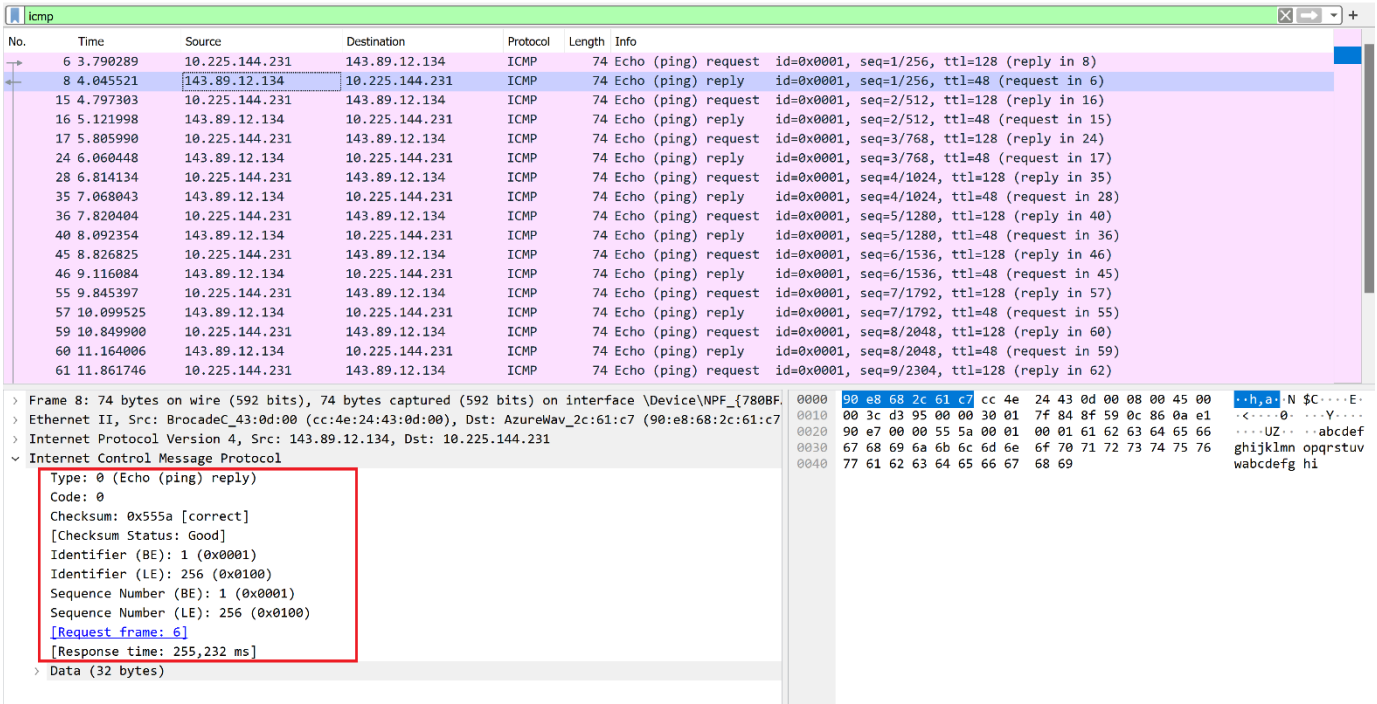


The ICMP type is 8, which indicates an echo (ping) request. The code for this type of ICMP packet is 0, which is standard for echo requests.

Other Fields:

- The Checksum is 0x4d5a, which indicates that the packet is valid and is 2 bytes long
- The Identifier (BE) is 0x0001 and in Little-Endian (LE) is 256 (0x0100). This identifier helps in matching echo requests with their corresponding replies. This field is also 2 bytes long.
- The Sequence Number (BE) is 0x0001 and in LE is 256 (0x0100). This number increments with each new echo request sent. This field is also 2 bytes long as we can see from the hexadecimal format.

2.4) Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?



The ICMP type for the reply is 0, which indicates an echo reply, and the code is 0. This is typical for ICMP echo replies, confirming that the destination has received the echo request and is responding back.

Other Fields:

- The Checksum for this packet is 0x555a, and it is marked as correct, indicating no corruption in the packet data during transit.
- The Identifier (BE) is 0x0001 and in Little-Endian (LE) is 256 (0x0100). This matches the identifier in the echo request, confirming that this reply corresponds to the initial request.
- The Sequence Number (BE) is 0x0001 and in LE is 256 (0x0100). This, too, matches the sequence number in the request, helping to match each reply to its corresponding request.

The bytes of these fields are 2, same as the request packet.

3) Part 2: Traceroute

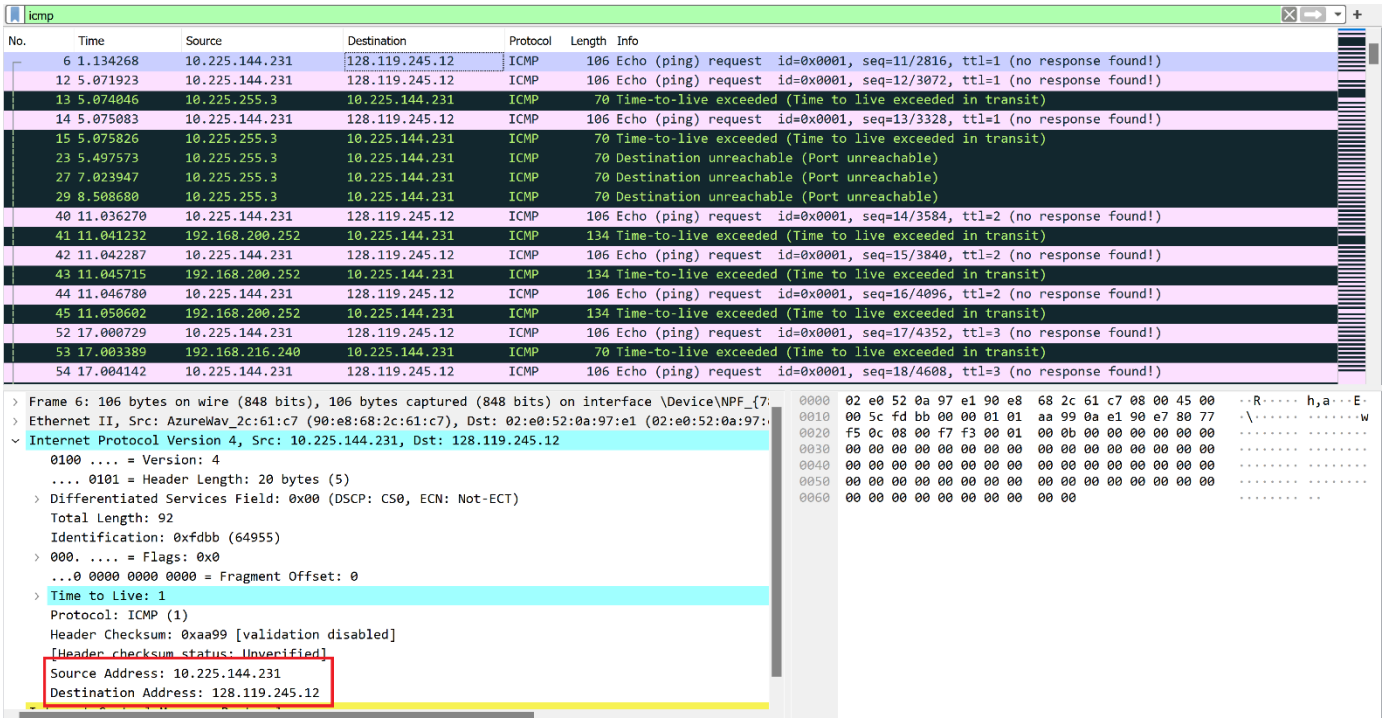
```
C:\Windows\System32>tracert gaia.cs.umass.edu

Tracing route to gaia.cs.umass.edu [128.119.245.12]
over a maximum of 30 hops:

  1     *        2 ms    <1 ms  10.225.255.3
  2     5 ms     3 ms     3 ms  192.168.200.252
  3     2 ms     3 ms     2 ms  192.168.216.240
  4     *        *        *     Request timed out.
  5     8 ms     8 ms     9 ms  193.140.0.150
  6     *       29 ms    31 ms  ulakbim.mx1.bud.hu.geant.net [62.40.125.129]
  7    56 ms    56 ms    74 ms  ae9.mx1.vie.at.geant.net [62.40.98.45]
  8    57 ms    56 ms    56 ms  ae5.rt1.pra.cz.geant.net [62.40.98.242]
  9    99 ms    44 ms    44 ms  ae6.rt1.fra.de.geant.net [62.40.98.158]
 10    55 ms    55 ms    56 ms  ae3.mx1.lon.uk.geant.net [62.40.98.179]
 11   144 ms   164 ms   141 ms  internet2-gw.mx1.lon.uk.geant.net [62.40.124.45]
 12   170 ms   237 ms   141 ms  fourhundredge-0-0-0-0.4079.core1.ashb.net.internet2.edu [163.253.1.118]
 13   149 ms   156 ms   142 ms  fourhundredge-0-0-0-1.4079.core1.newy32aoa.net.internet2.edu [163.253.1.117]
 14   140 ms   153 ms   141 ms  fourhundredge-0-0-0-20.4079.core2.newy32aoa.net.internet2.edu [163.253.1.43]
 15   144 ms   177 ms   144 ms  nox300gw1-i2-re.nox.org [192.5.89.221]
 16   146 ms   167 ms   153 ms  192.5.89.58
 17   148 ms   150 ms   146 ms  nox-mghpcc-gw1-umassnet-re2.nox.org [18.2.8.90]
 18   173 ms   236 ms   147 ms  69.16.1.0
 19   175 ms   146 ms   146 ms  core1-rt-et-8-3-0.gw.umass.edu [192.80.83.109]
 20   148 ms   151 ms   146 ms  n1-rt-1-1-et-0-0-0.gw.umass.edu [128.119.0.216]
 21   147 ms   234 ms   147 ms  128.119.7.74
 22     *      147 ms   150 ms  128.119.7.66
 23   148 ms   168 ms   147 ms  core1-rt-et-7-2-1.gw.umass.edu [128.119.0.217]
 24   147 ms   168 ms   149 ms  n5-rt-1-1-xe-2-1-0.gw.umass.edu [128.119.3.33]
 25   147 ms   260 ms   151 ms  cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]
 26   149 ms   266 ms   148 ms  nscs1bbs1.cs.umass.edu [128.119.240.253]
 27   148 ms   147 ms   147 ms  gaia.cs.umass.edu [128.119.245.12]

Trace complete.
```

3.1) What is the IP address of your host? What is the IP address of the target destination host?



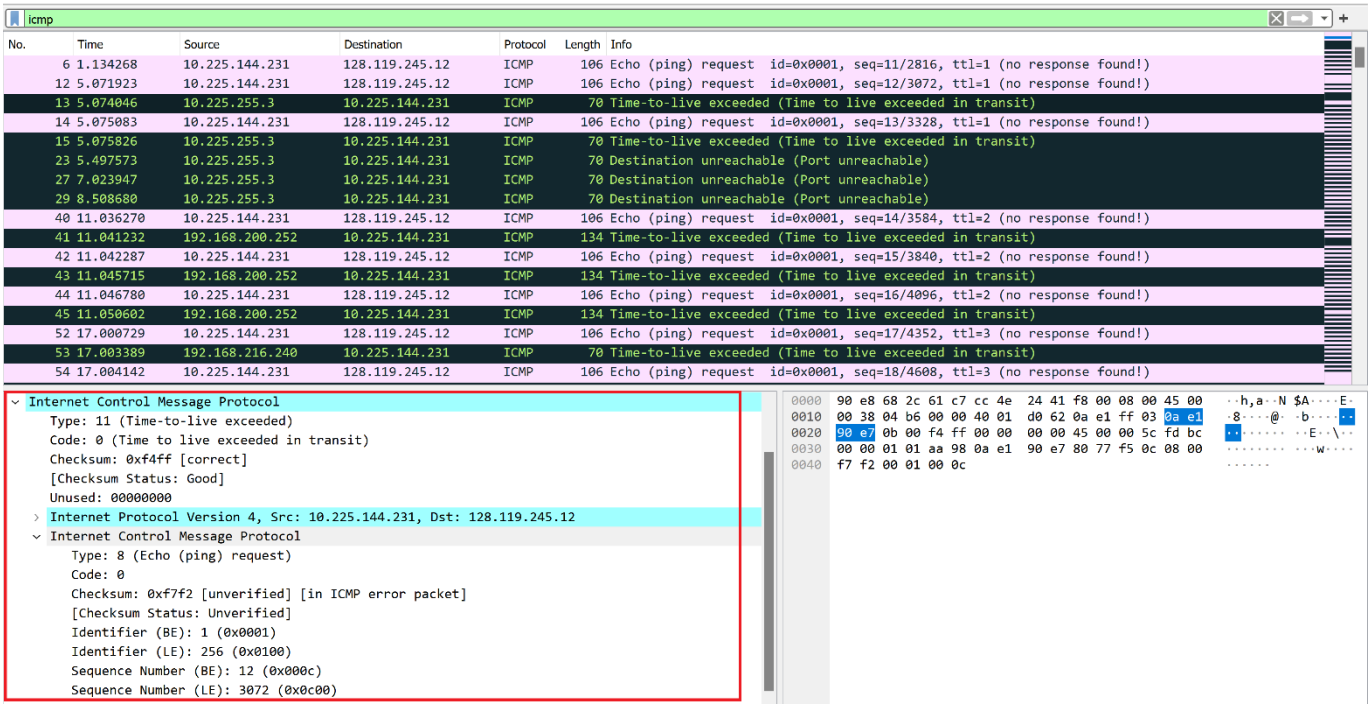
The IP address of my host, from which the ICMP packets are being sent, is 10.225.144.231. This is visible in the 'Source Address' field of the IP header for the ICMP echo (ping) request highlighted in the screenshot.

The IP address of the target destination host, to which the ICMP packets are being sent, is 128.119.245.12. Which is the ip address of the hostname “gaia.cs.umass.edu”.

3.2) If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

No, the IP protocol number would not be 01 if ICMP used UDP packets for the probes. The protocol number for ICMP is 01, but for UDP, it is 17.

3.3) Examine the ICMP error packet in your screenshot. It has more fields than the ICMP ping packet. What is included in those fields?



The ICMP error packet includes the original IP header and the first 8 bytes of the ICMP payload that triggered the error.

It includes original IP header because it provides context for the error message, indicating the source and destination IP addresses of the packet that encountered the error. This is

crucial for the sender to understand which packet was affected and to which destination it was headed.

It includes first 8 bytes of the ICMP payload because these bytes help to uniquely identify the original ICMP request that triggered the error message.

3.4) Within the traceroute measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in your figure, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

```
C:\Windows\System32>tracert gaia.cs.umass.edu

Tracing route to gaia.cs.umass.edu [128.119.245.12]
over a maximum of 30 hops:

  1     *        2 ms    <1 ms  10.225.255.3
  2     5 ms     3 ms     3 ms  192.168.200.252
  3     2 ms     3 ms     2 ms  192.168.216.240
  4     *        *        *     Request timed out.
  5     8 ms     8 ms     9 ms  193.140.0.150
  6     *       29 ms    31 ms  ulakbim.mx1.bud.hu.geant.net [62.40.125.129]
  7    56 ms    56 ms    74 ms  ae9.mx1.vie.at.geant.net [62.40.98.45]
  8    57 ms    56 ms    56 ms  ae5.rt1.pra.cz.geant.net [62.40.98.242]
  9    99 ms    44 ms    44 ms  ae6.rt1.fra.de.geant.net [62.40.98.158]
 10    55 ms    55 ms    56 ms  ae3.mx1.lon.uk.geant.net [62.40.98.179]
 11   144 ms   164 ms   141 ms  internet2-gw.mx1.lon.uk.geant.net [62.40.124.45]
 12   170 ms   237 ms   141 ms  fourhundredge-0-0-0-0.4079.core1.ashb.net.internet2.edu [163.253.1.118]
 13   149 ms   156 ms   142 ms  fourhundredge-0-0-0-1.4079.core1.newy32aoa.net.internet2.edu [163.253.1.117]
 14   140 ms   153 ms   141 ms  fourhundredge-0-0-0-20.4079.core2.newy32aoa.net.internet2.edu [163.253.1.43]
 15   144 ms   177 ms   144 ms  nox300gw1-i2-re.nox.org [192.5.89.221]
 16   146 ms   167 ms   153 ms  192.5.89.58
 17   148 ms   150 ms   146 ms  nox-mghpcc-gw1-umassnet-re2.nox.org [18.2.8.90]
 18   173 ms   236 ms   147 ms  69.16.1.0
 19   175 ms   146 ms   146 ms  core1-rt-et-8-3-0.gw.umass.edu [192.80.83.109]
 20   148 ms   151 ms   146 ms  n1-rt-1-1-et-0-0-0.gw.umass.edu [128.119.0.216]
 21   147 ms   234 ms   147 ms  128.119.7.74
 22     *      147 ms   150 ms  128.119.7.66
 23   148 ms   168 ms   147 ms  core1-rt-et-7-2-1.gw.umass.edu [128.119.0.217]
 24   147 ms   168 ms   149 ms  n5-rt-1-1-xe-2-1-0.gw.umass.edu [128.119.3.33]
 25   147 ms   260 ms   151 ms  cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]
 26   149 ms   266 ms   148 ms  nscs1bbs1.cs.umass.edu [128.119.240.253]
 27   148 ms   147 ms   147 ms  gaia.cs.umass.edu [128.119.245.12]
```

The link between 10th and 11th hop has a significantly longer delay. But we could not guess the locations of these routers. It is not written explicitly.