Internet Control Message Protocol

Foreword

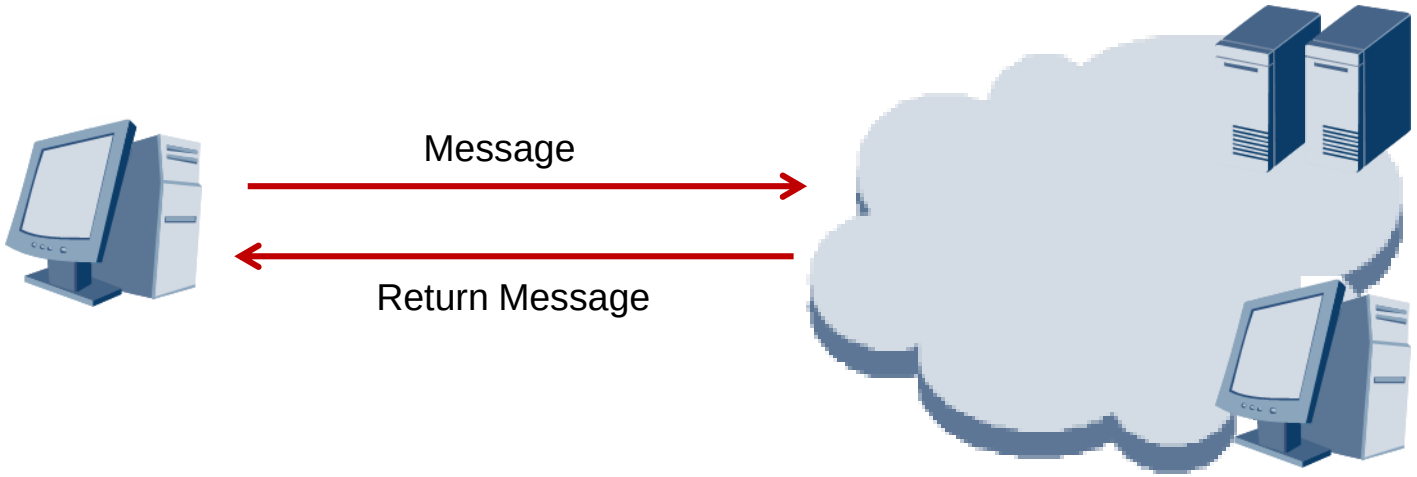
ICMP is a protocol that works alongside IP as a form of messaging protocol in order to compensate for the limited reliability of IP. The implementation of ICMP is required to be understood to familiarize with the behavior of numerous operations and applications that rely heavily on ICMP, in order to support underlying messaging, based on which further processes are often performed.

Objectives

Upon completion of this section, trainees will be able to:

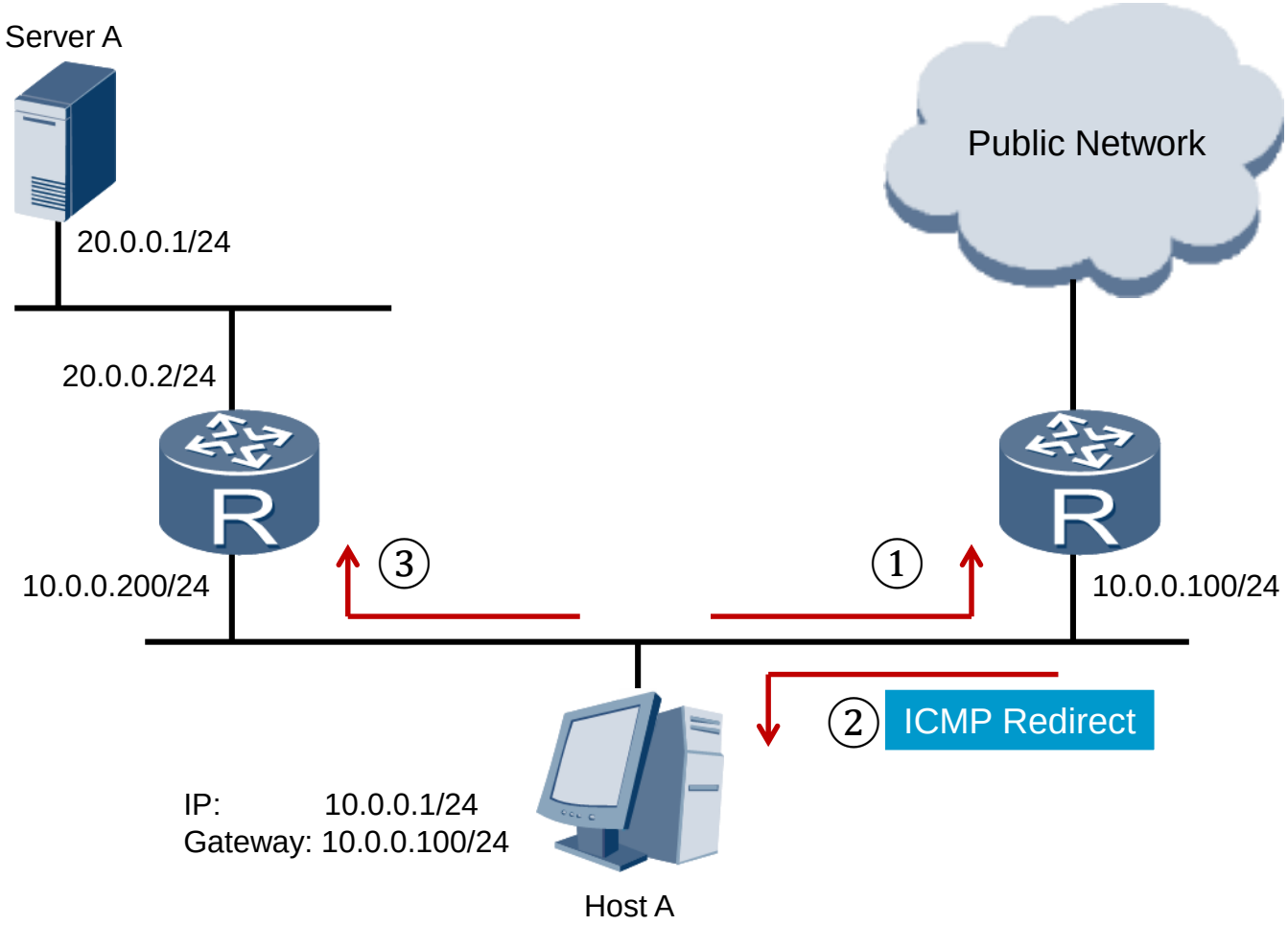
- Describe some of the processes to which ICMP is applied.
- Identify the common type and code values used in ICMP.
- Explain the function of ICMP in the ping and traceroute applications.

ICMP



- ICMP messages are used to support multiple operations including routing, diagnostics and errors.

ICMP (Routing)

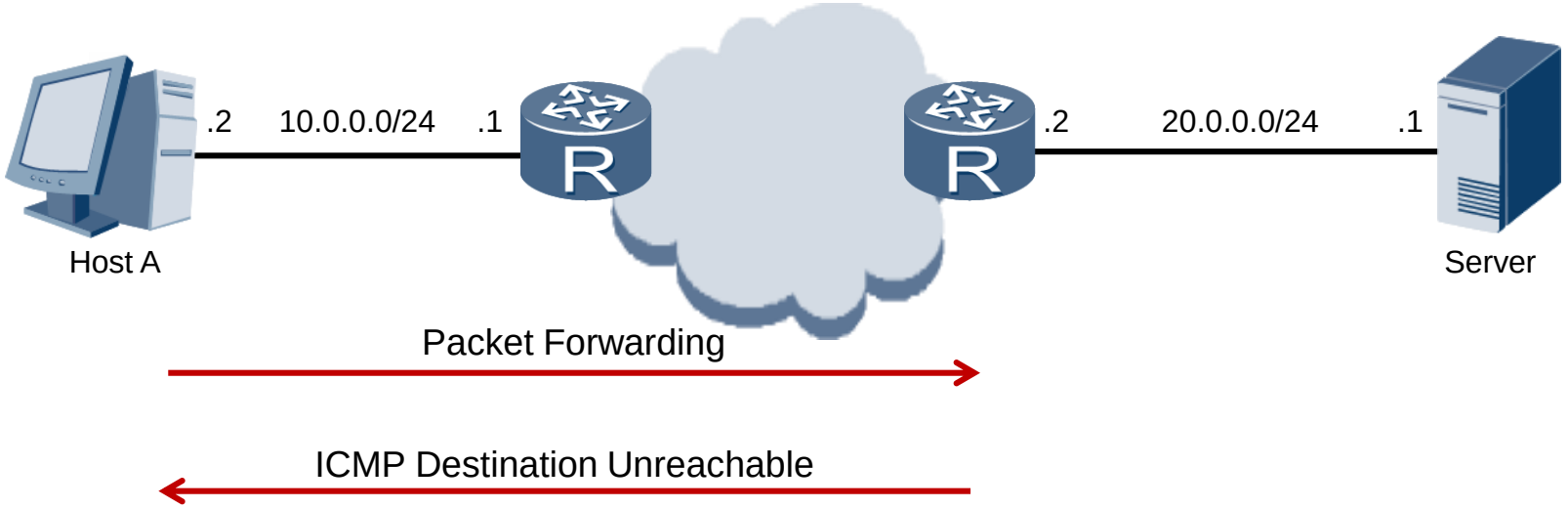


HUAWEI

ICMP (Diagnostics)

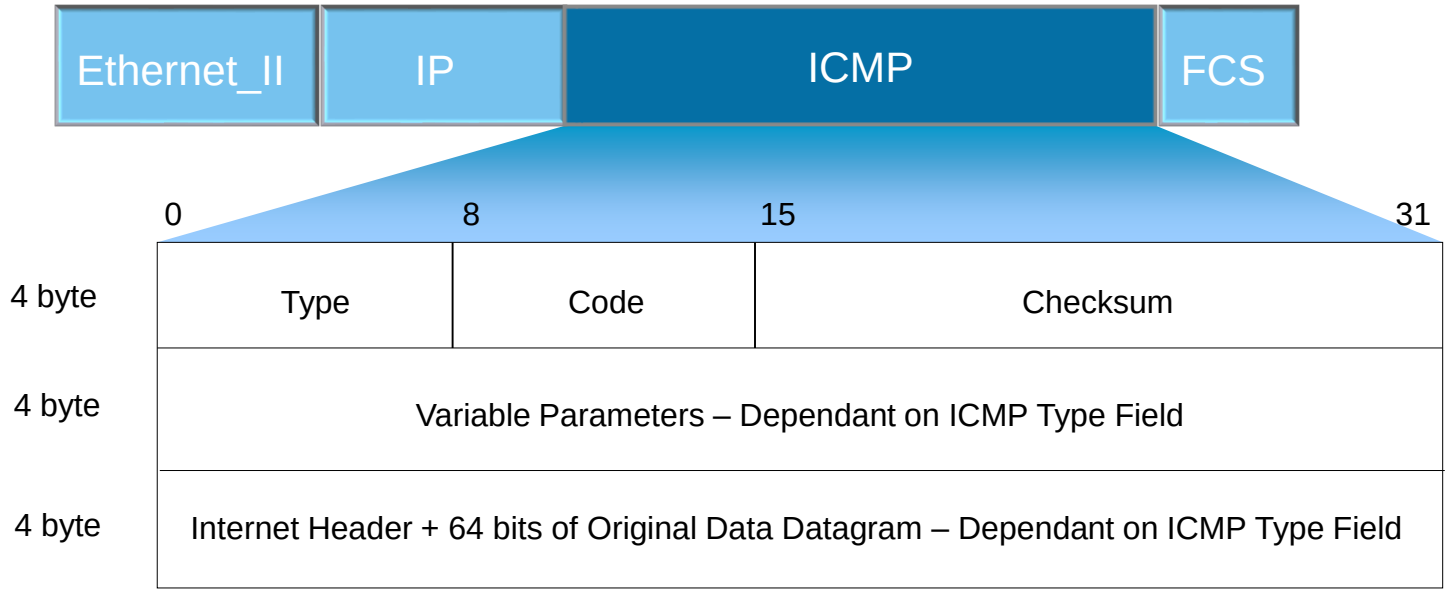
- Two separate messages are used for the request and reply.
- Commonly associated with the Ping application.

ICMP (Errors)



- Notifies the packet source of problems with packet forwarding.
- Uses the source IP address in the IP header for notification.

ICMP Format



- ICMP parameters are represented in a type/code format.
- Additional data often carried to identify the undelivered packet.

ICMP Type & Code Fields

Type	Code	Description
0	0	Echo Reply
3	0	Network Unreachable
3	1	Host Unreachable
3	2	Protocol Unreachable
3	3	Port Unreachable
5	0	Redirect Datagram for the Network
8	0	Echo Request

- The *Type* value represents the format of a message.
- The *Code* value provides a more specific message description.

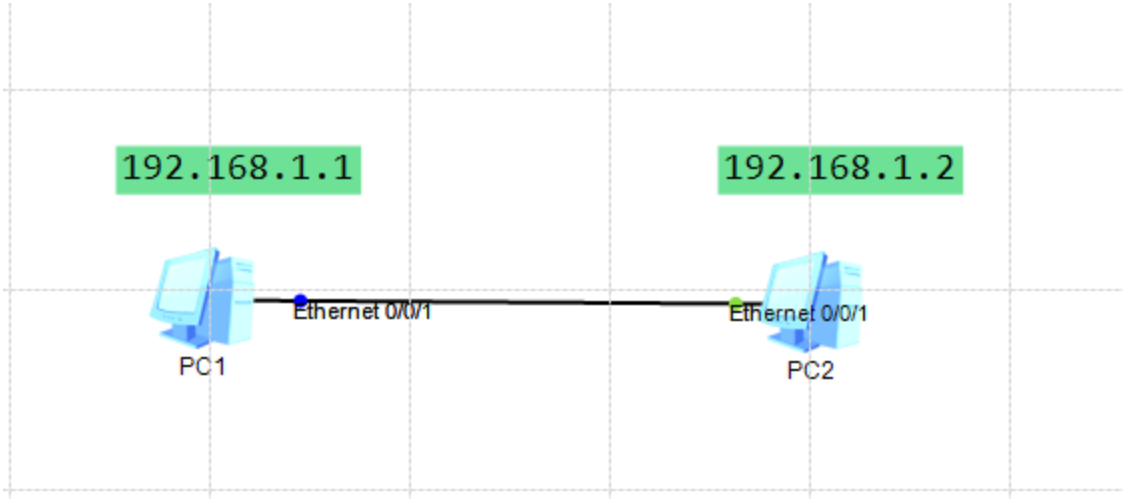
ICMP Applications - Ping


```
<RTA>ping ?
-a        Select source IP address, the default is the IP address of
          the output interface
-c        Specify the number of echo requests to be sent, the
          default is 5
-n        Numeric output only. No attempt will be made to lookup
          host addresses for symbolic names
-t        Timeout in milliseconds to wait for each reply, the
          default is 2000ms
STRING<1-255> IP address or hostname of a remote system
......
<RTA>ping 10.0.0.2
```

Ping Results

```
<RTA>ping 10.0.0.2
  PING 10.0.0.2 : 56  data bytes, press CTRL_C to break
    Reply from 10.0.0.2 : bytes=56 Sequence=1 ttl=255 time=340 ms
    Reply from 10.0.0.2 : bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 10.0.0.2 : bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 10.0.0.2 : bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.0.0.2 : bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 10.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/88/340 ms
```

Ping Results - Request



Ping Results - Request

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HuaweiTe_7f:2d:14	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
2	0.016000	HuaweiTe_0e:7a:82	HuaweiTe_7f:2d:14	ARP	60	192.168.1.2 is at 54:89:98:0e:7a:82
3	0.031000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x2ebb, seq=1/256, ttl=128 (reply in 4)
4	0.047000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x2ebb, seq=1/256, ttl=128 (request in 3)
5	1.063000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x2fbb, seq=2/512, ttl=128 (reply in 6)
6	1.063000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x2fbb, seq=2/512, ttl=128 (request in 5)
7	2.078000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x30bb, seq=3/768, ttl=128 (reply in 8)
8	2.094000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x30bb, seq=3/768, ttl=128 (request in 7)
9	3.094000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x31bb, seq=4/1024, ttl=128 (reply in 10)
10	3.110000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x31bb, seq=4/1024, ttl=128 (request in 9)
11	4.125000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x32bb, seq=5/1280, ttl=128 (reply in 12)
12	4.125000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x32bb, seq=5/1280, ttl=128 (request in 11)

```
> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: HuaweiTe_7f:2d:14 (54:89:98:7f:2d:14), Dst: HuaweiTe_0e:7a:82 (54:89:98:0e:7a:82)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
> Internet Control Message Protocol
```

```
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x57c2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 11963 (0x2ebb)
    Identifier (LE): 47918 (0xbb2e)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 4]
  v Data (32 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
      [Length: 32]
```


HUAWEI

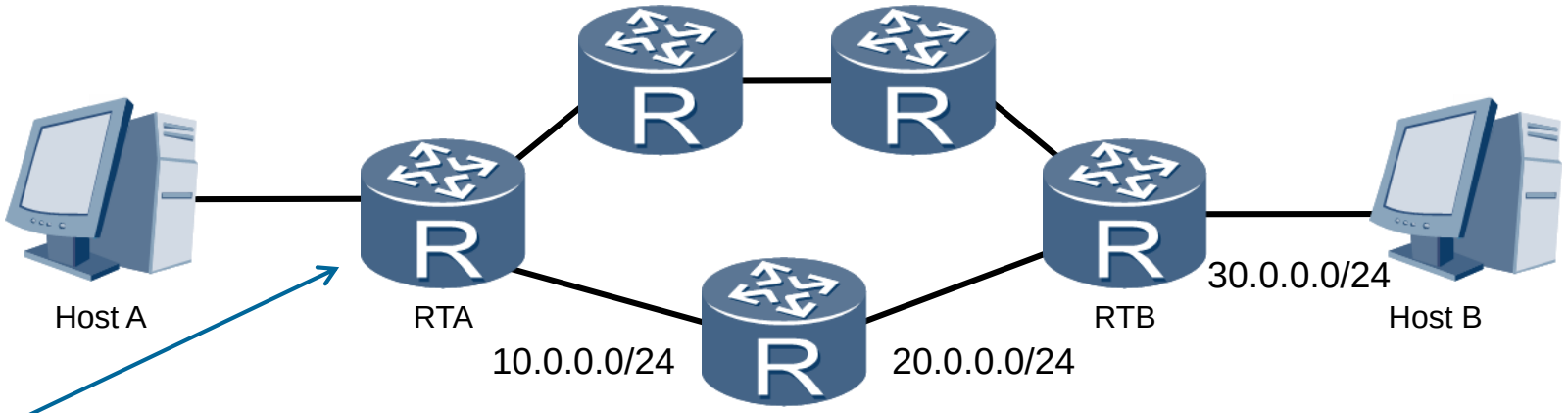
Ping Results - Reply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HuaweiTe_7f:2d:14	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
2	0.016000	HuaweiTe_0e:7a:82	HuaweiTe_7f:2d:14	ARP	60	192.168.1.2 is at 54:89:98:0e:7a:82
3	0.031000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x2ebb, seq=1/256, ttl=128 (reply in 4)
4	0.047000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x2ebb, seq=1/256, ttl=128 (request in 3)
5	1.063000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x2fbb, seq=2/512, ttl=128 (reply in 6)
6	1.063000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x2fbb, seq=2/512, ttl=128 (request in 5)
7	2.078000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x30bb, seq=3/768, ttl=128 (reply in 8)
8	2.094000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x30bb, seq=3/768, ttl=128 (request in 7)
9	3.094000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x31bb, seq=4/1024, ttl=128 (reply in 10)
10	3.110000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x31bb, seq=4/1024, ttl=128 (request in 9)
11	4.125000	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) request id=0x32bb, seq=5/1280, ttl=128 (reply in 12)
12	4.125000	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) reply id=0x32bb, seq=5/1280, ttl=128 (request in 11)

```
> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: HuaweiTe_0e:7a:82 (54:89:98:0e:7a:82), Dst: HuaweiTe_7f:2d:14 (54:89:98:7f:2d:14)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
> Internet Control Message Protocol
```

```
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5fc2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 11963 (0x2ebb)
    Identifier (LE): 47918 (0xbb2e)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 3]
    [Response time: 16.000 ms]
  v Data (32 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
      [Length: 32]
```

ICMP Application – Traceroute



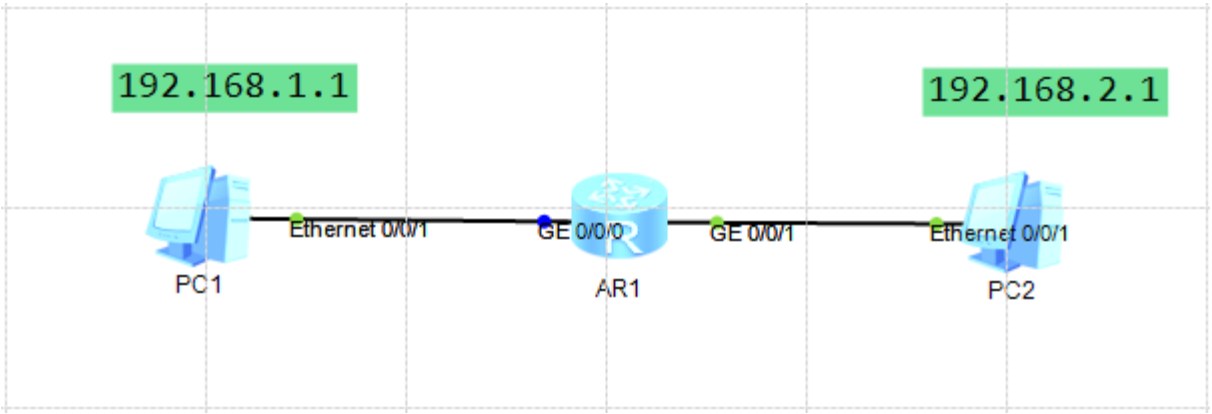

```
<RTA>tracert ?
-a        Set source IP address, the default is the IP
          address of the output interface
-f        First time to live, the default is 1
-m        Max time to live, the default is 30
-name     Display the host name of the router on each hop
-p        Destination UDP port number, the default is 33434
STRING<1-255> IP address or hostname of a remote system
......
<RTA>tracert 30.0.0.2
```

Traceroute Results

```
<RTA>tracert 30.0.0.2

traceroute to 30.0.0.2(30.0.0.2), max hops:30, packet length:40,
press CTRL_C to break

 1 10.0.0.2 130 ms  50 ms  40 ms

 2 20.0.0.2 80 ms  60 ms  80 ms

 3 30.0.0.2 80 ms  60 ms  70 ms
```

- Traceroute displays hop-by-hop transmission results.
- TTL value is used to define a hop limit for each set of results.

Traceroute Results



- Mni-Lab_basic:03-icmp_01

Traceroute Results – TTL=1

Source	Destination	Protocol	Length	Info
192.168.1.1	192.168.2.1	ICMP	106	Echo (ping) request
192.168.1.254	192.168.1.1	ICMP	70	Time-to-live exceeded
192.168.1.1	192.168.2.1	ICMP	106	Echo (ping) request

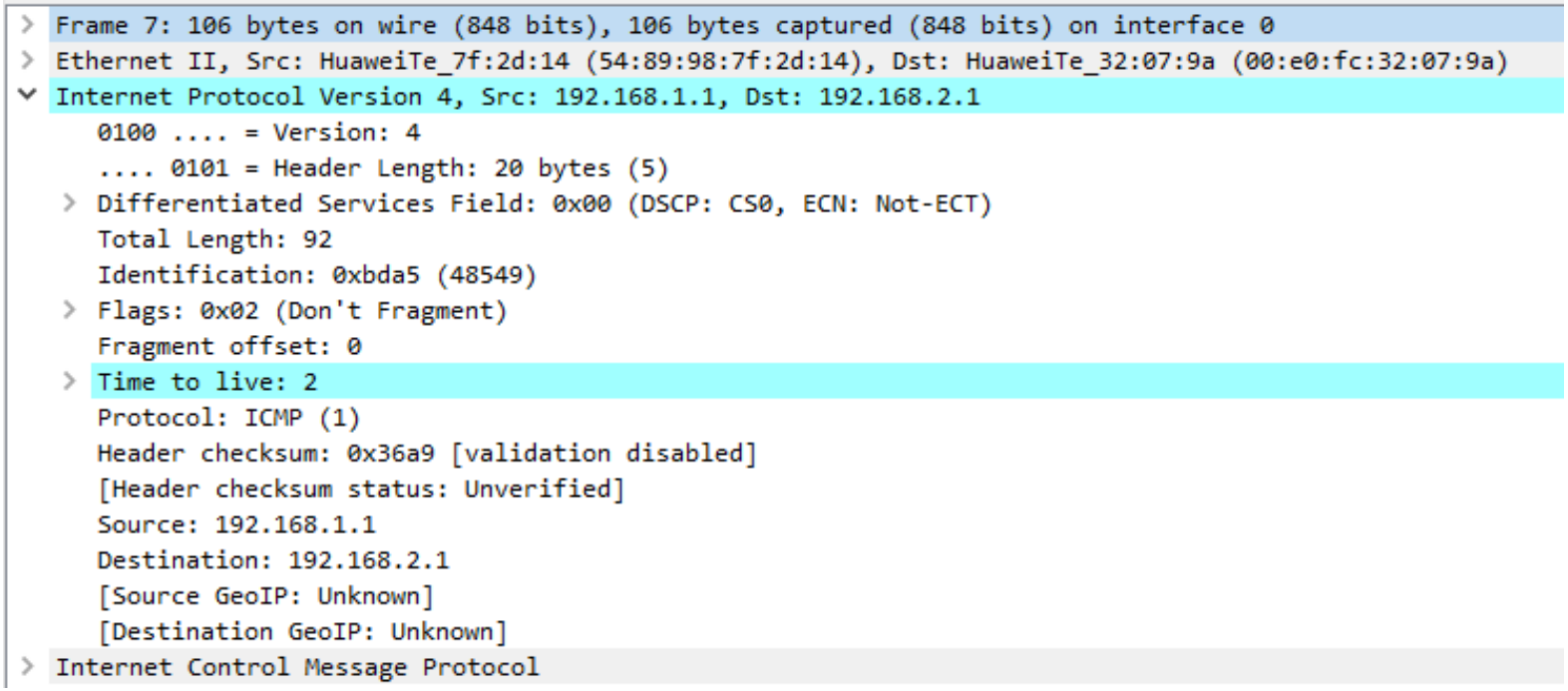
```
> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: HuaweiTe_7f:2d:14 (54:89:98:7f:2d:14), Dst: HuaweiTe_32:07:9a (00:e0:fc:32:07:9a)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
      0100 .... = Version: 4
```

```
> Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: HuaweiTe_32:07:9a (00:e0:fc:32:07:9a), Dst: HuaweiTe_7f:2d:14 (54:89:98:7f:2d:14)
> Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.1
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xda04 [correct]
    [Checksum Status: Good]
  > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
  > Internet Control Message Protocol
```

```
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
> Internet Control Message Protocol
```


HUAWEI

Traceroute Results – TTL=2



HUAWEI

Esercizi!

Con il computer che state utilizzando:

- Riconoscere ed effettuare il ping verso il default gateway;
- Effettuare il ping verso www.google.it;
- Effettuare un traceroute verso www.nasa.gov;
- Effettuare un traceroute verso 193.205.130.253;

Summary

- Which two ICMP message types are used as part of a successful Ping?
- In the event that the TTL value in the IP header of a datagram reaches zero, what action will be taken by the receiving gateway?

Thank you

www.huawei.com