Internet Control Message Protocol (ICMP)

Applied Network security (comp420 –001)

Department of Computer science

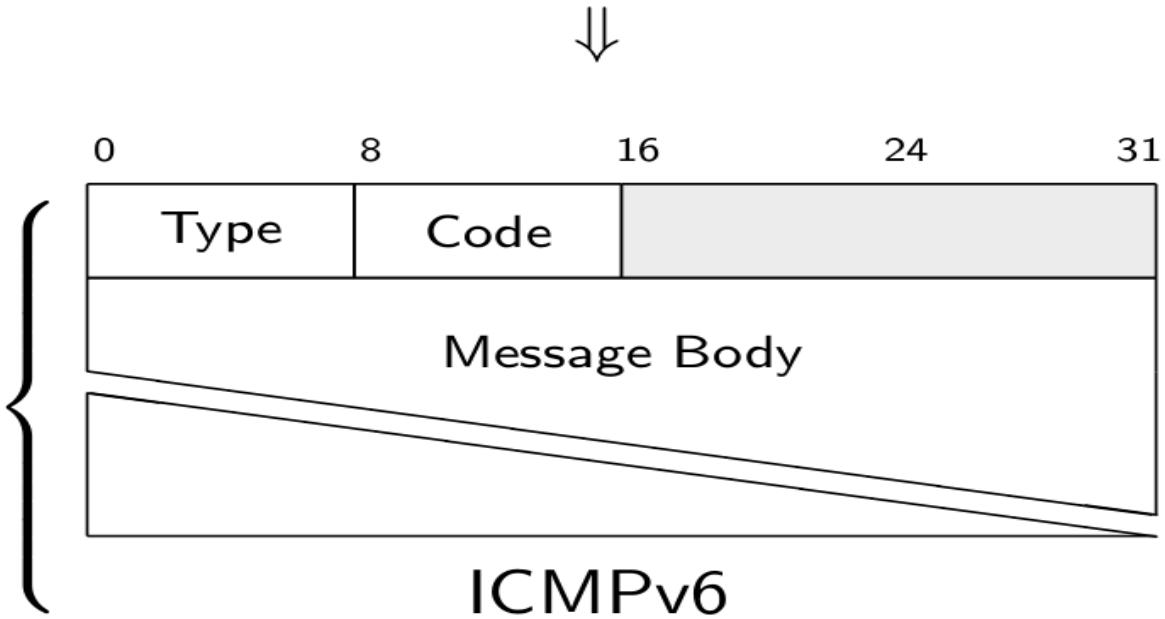
Fall 2020

Internet Control Message Protocol (ICMP)

- When we talk about IP, there's also supporting protocol we have to talk about.
- Why do we need it ICMP?
  - First, ICMP is used for **error reporting**.
    - Destination unreachable
    - Packet's too big
    - For example, if a packet is too big for a router to process, the router can send an ICMP error back to the client. Without ICMP, we'd be pretty much in the dark if we have any network issues.
  - Second, ICMP is immensely useful for **diagnostics** and probably best known for the ping utility.
    - ping
    - traceroute
    - For example, You can send a ping packet to a server and the server will reply with a pong so that we know it can be reached. That is a very good way to make sure that you have basic internet connectivity.
- long story short, ICMP is a support protocol for IP and an important part of the Inter net.

ICMP Packet

Type	Meaning
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
128	Echo Request (“ping”)
129	Echo Reply (“pong”)
...	

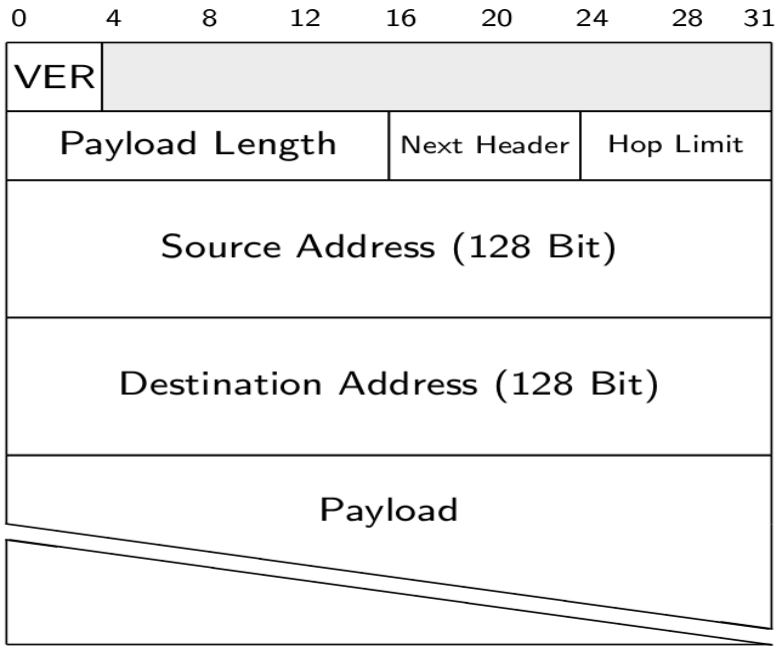


ICMP Packet (Cont.)

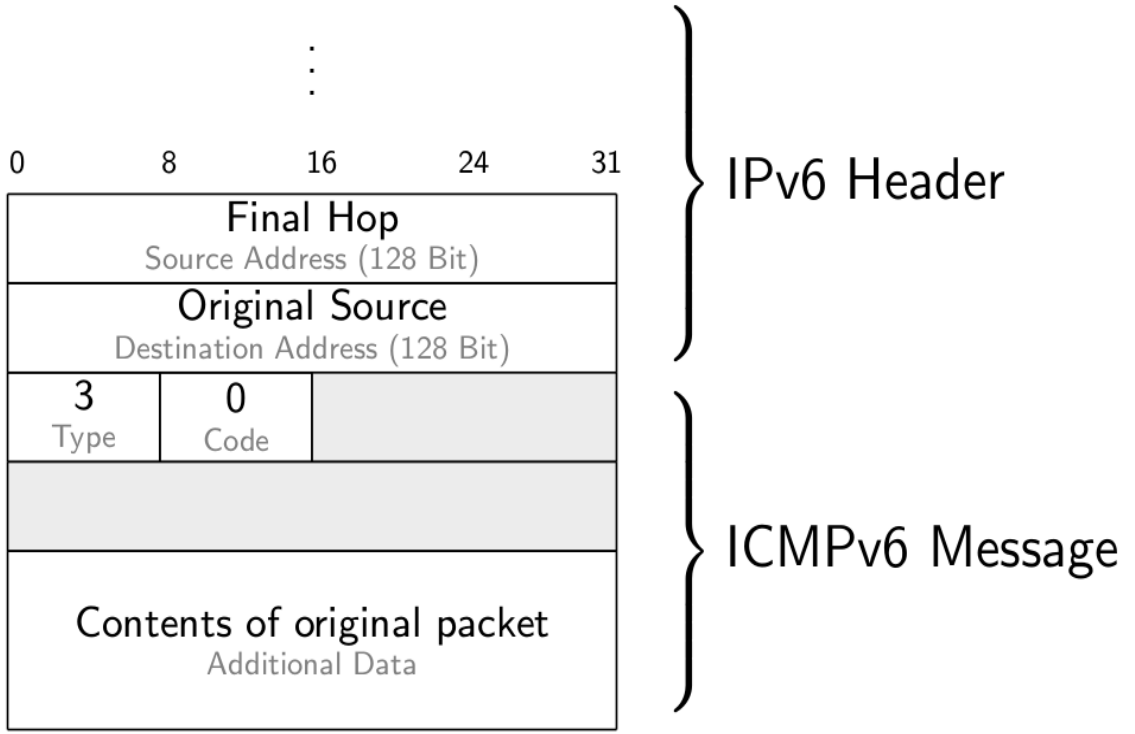
- The structure of an ICMP packet is quite simple. It consists of a type field, a code field, and an optional message body.
- An ICMP message can be an error-- for example, time exceeded when our hop limit reaches 0. Or it can be an informational message, such as a ping packet.
- The code field is used to provide a more detailed reason for the packet. For example, when we have a destination unreachable packet, the code states why the destination could not be reached. One reason could be that there is no known route. Another could be that communication with the destination is administratively prohibited.
- We have also the message body whose meaning depends on the message type.

ICMP (Cont.)

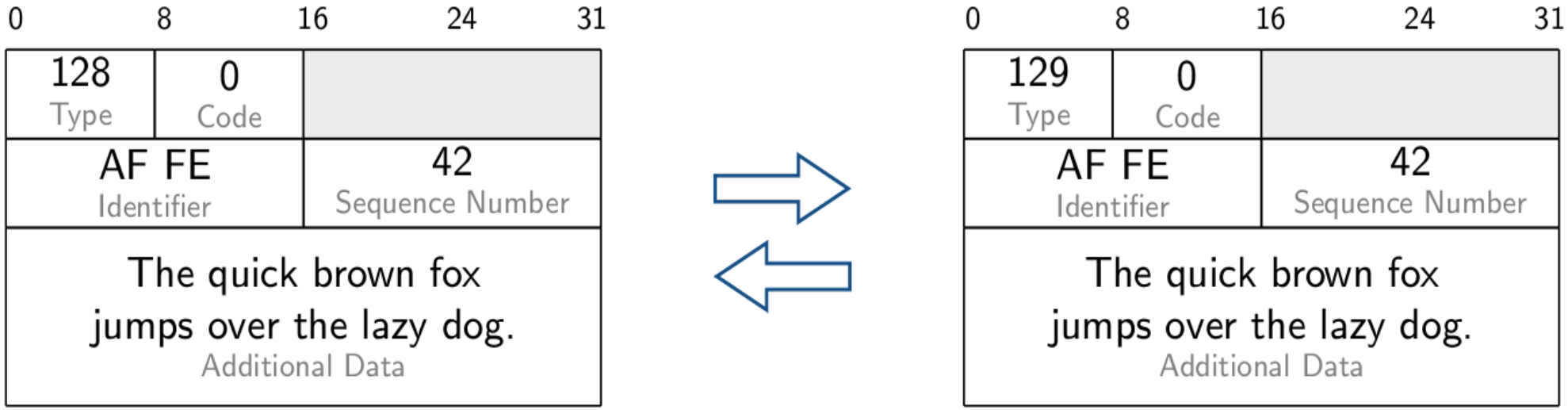
- While ICMP is technically part of IP, it is built on top of regular IP packets.
- So an ICMP message is sent as part of the body of an IP packet. If we want to send a ping message to someone, we basically enter the destination address in the IP header and then just state it's a ping request in the ICMP message.



IPv6



Ping Packet



ICMPv6 Echo Request

ICMPv6 Echo Reply

```
$ ping 8.8.8.8
PING 8.8.8.8 with 64 bytes of data.
64 bytes from 8.8.8.8: ttl=58 time=25ms
```

Ping Packet (Cont.)

- We have a message type of 128, indicating that it's a ping-- an ICMP echo request.
- For pings, the code field is always 0, as there aren't really any different codes.
- In the body, we have an identifier and a sequence number. These are basically used so it can match your pong to the right ping.
- For ping requests, we can also include an arbitrary payload, which a server will echo.
- After the ping packet reaches the server, the server crafts a pong packet, which is the same except for the ICM type. This is then sent back to the client.
- If we know the initial hop limit set by the server, we can determine how many hops away we are from the destination machine. For Linux machines, the hop limit is usually set to 64. So in the previous slide case, we are very likely six hops away from our target.

Your Turn 1

Your internet connection is lost:

```
$ ping 8.8.8.8[1]
PING 8.8.8.8 with 64 bytes of data.
no answer yet for icmp_seq=1
```

```
$ ping 10.0.0.1[2]
PING 10.0.0.1 with 64 bytes of data.
no answer yet for icmp_seq=1
```

Which of the following scenarios are likely?

- ☐ Your computer has a problem.
- ☐ Your router has a problem.
- ☐ Your internet service provider has a problem.
- ☐ Google's server has a problem.

---

[1] 8.8.8.8 is the IP address of a Google server.
[2] 10.0.0.1 is the IP address of your local router.

Your Turn 2

Dang! Your internet connection is lost *again*:

```
$ ping 8.8.8.8[3]
PING 8.8.8.8 with 64 bytes of data.
no answer yet for icmp_seq=1
```

```
$ ping 10.0.0.1[4]
PING 10.0.0.1 with 64 bytes of data.
64 bytes from 10.0.0.1: time=1ms
```

Which of the following scenarios are likely?

- ☐ Your computer has a problem.
- ☐ Your router has a problem.
- ☐ Your internet service provider has a problem.
- ☐ Google's server has a problem.

---

[3] 8.8.8.8 is the IP address of a Google server.
[4] 10.0.0.1 is the IP address of your local router.