The internetwork layer

Goal:

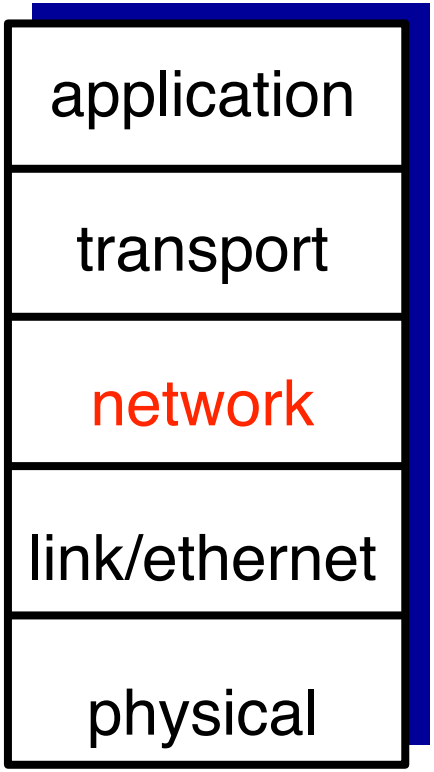
To understand the principles behind the (inter-) network layer.

Roadmap

1. the network layer
2. IP addresses
3. IP packet structure
4. Routing basics
5. Safety and security in the IP layer
6. ICMP

the network layer

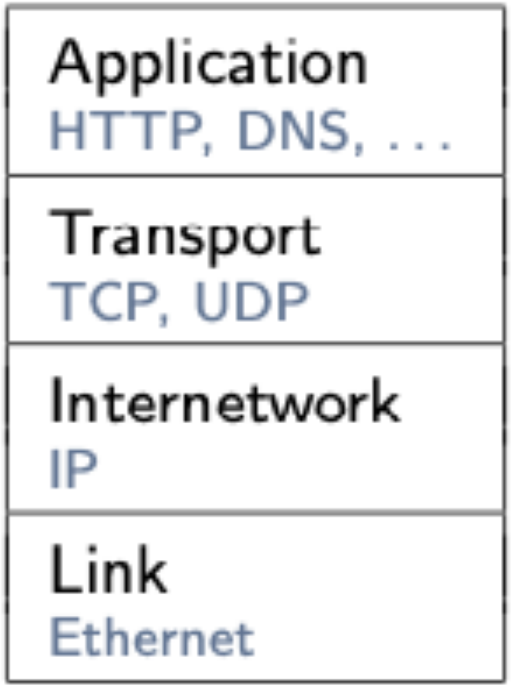
- The network layer is responsible for connecting multiple local networks.
- It makes it possible for my friend and myself to exchange messages.
- It is implemented using the IP (Internet Protocol).
- The IP layer sits on the ethernet layer, but does not depend on it.



why a new protocol?

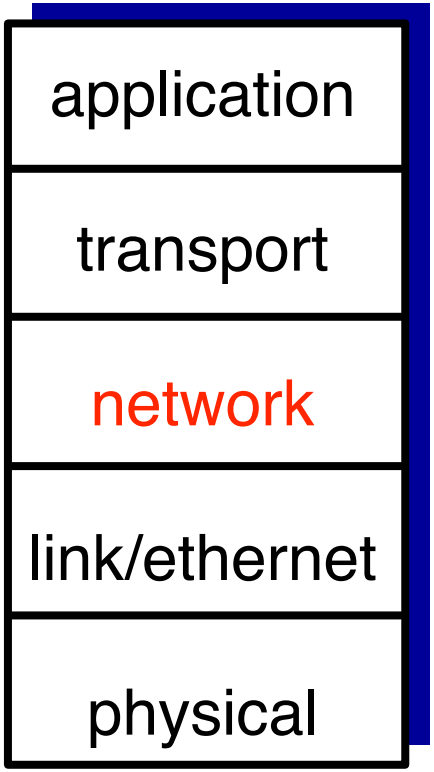
why don't we use ethernet for everything?

- Ethernet MAC addresses only contain information on the manufacturer; you have an idea of where the devices are in the network.
- To be able to send packets to the correct destination, every switch would need to manage a list of all connected devices.
- It would be like delivering a Mail only using a person's name.



Why a new protocol?

- Solution: addresses should be organised hierarchically like we already do with postcards: country, state, city, etc.
- How does the Internet Protocol (IP) fix this?
  - IP Addressing + routing



Roadmap

1. the network layer
2. IP addresses
3. IP packet structure
4. Routing basics
5. Safety and security in the IP layer
6. ICMP

IP addresses

- IP addresses are dynamically assigned to devices.
- The first parts of IP addresses are equal for all the devices in the local network.
- You are assigned a new IP address whenever you connect to a WiFi network.
- The first part of an IP address acts as a locator

Questions

Question

Check all statements that are true:

- ☐ Every router keeps track of all devices connected to the entire internet to route packets.
- ☐ A device will usually keep the same IP address over its lifetime.
- ☐ A device will usually keep the same MAC address over its lifetime.
- ☐ A routed network must not have any loops or circles.
- ☐ IP addresses can be used to implement "geo-blocking," a technique where access to content is restricted based on the user's geographical location.

what do IP addresses look like?

IPv4 addresses.

4 bytes separated by "."

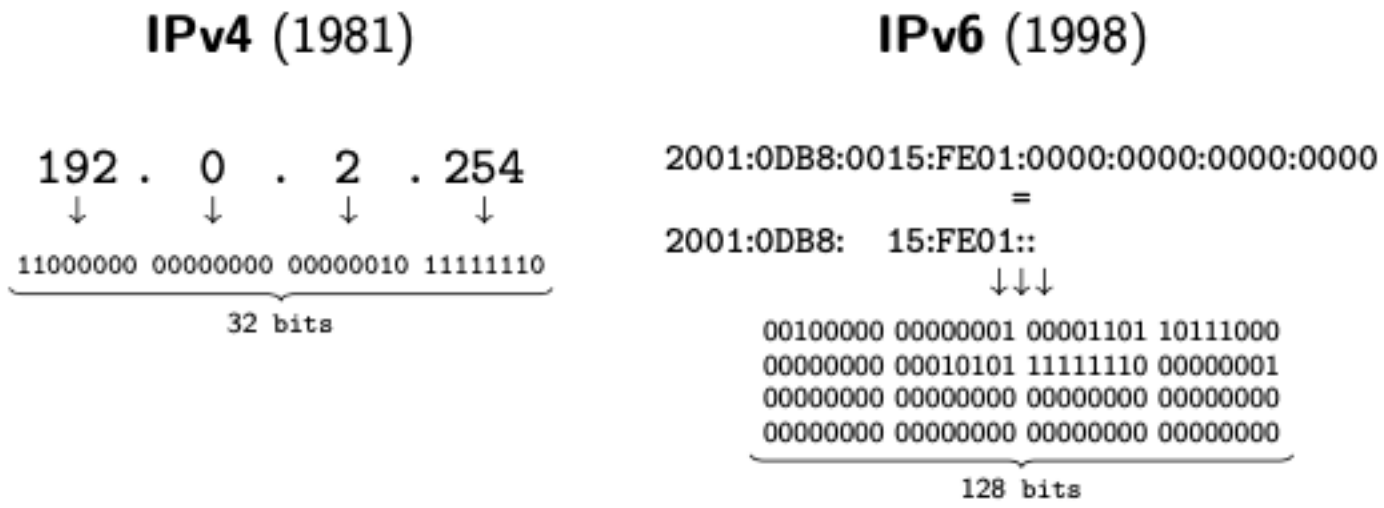
32= 8x4 bits in total

Insufficient!

IPv6 addresses

16 bytes, 8 hexadecimal numbers

128 = 16*8 bits in total



$2^{32} \approx 4$ billion addresses

$2^{128} \approx 3.4 * 10^{38}$ addresses

IPv6 - reduced versions

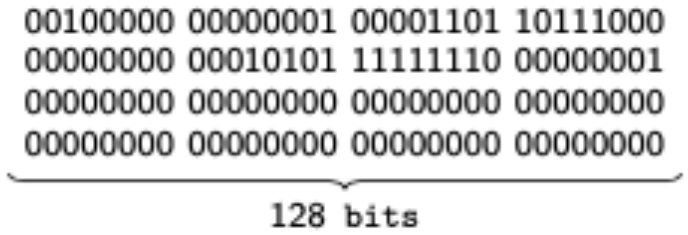
- Replace 0000 or groups of 0000: …:0000 with :
- remove leading 0s
  - 0015 becomes 15

IPv6 (1998)

2001:0DB8:0015:FE01:0000:0000:0000:0000

=

2001:0DB8: 15:FE01::



$2^{128} \approx 3.4 * 10^{38}$ addresses

Questions

Select all correct statements:

- ☐ `192.168.0.256` is a valid IPv4 address.
- ☐ `8.8.4.4` is a valid IPv4 address.
- ☐ `affe::` is a valid IPv6 address.
- ☐ `1.2.3.4` is a valid IPv6 address.
- ☐ There are strings that are both valid IPv4 and IPv6 addresses.

Answers

Questions

Reduce the following IP addresses to their shortest form:

1. 2001:0db8:0000:0000:0000:0000:0002:0001

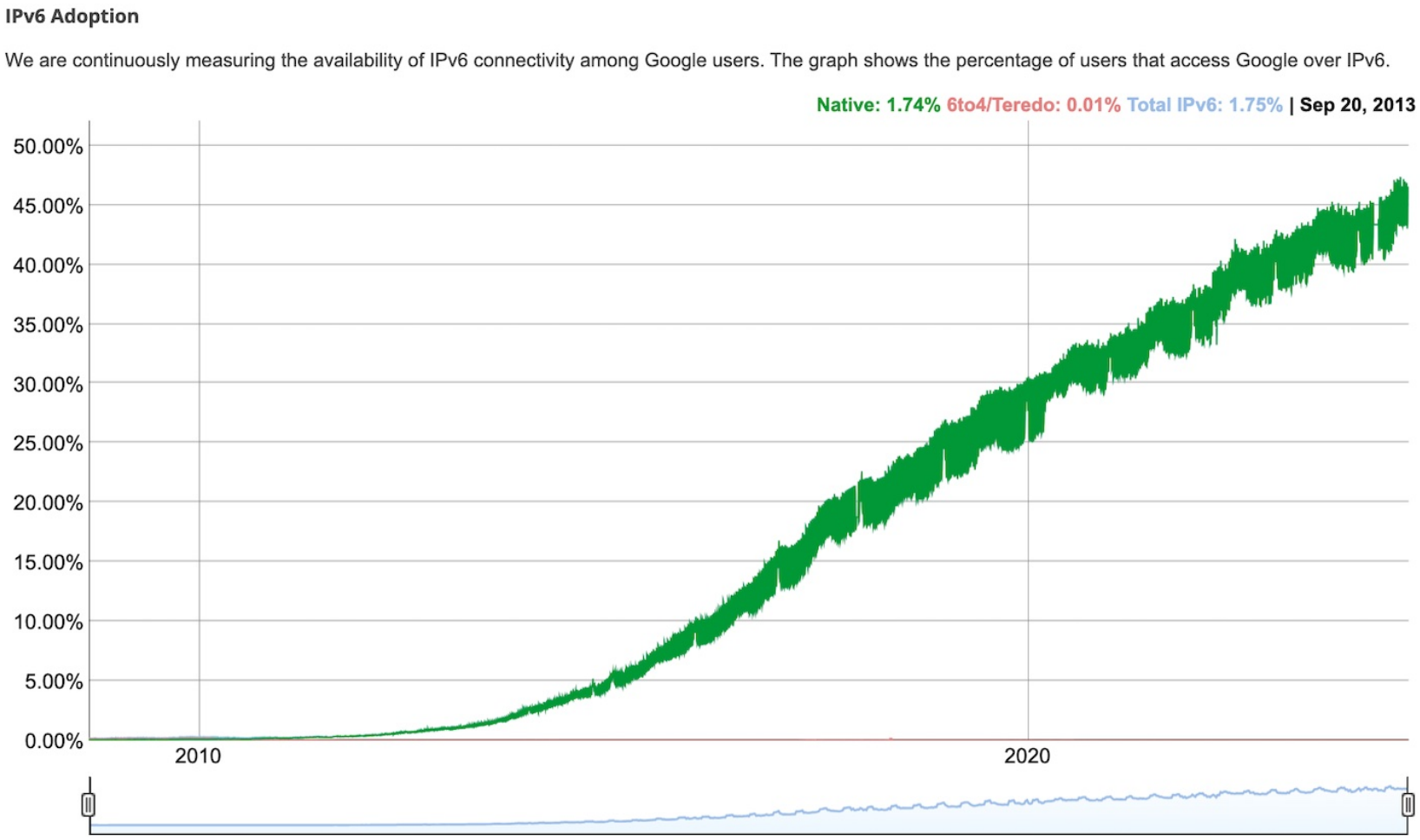
2. 0000:0000:0000:0000:0000:0000:0000:0001

3. 192.168.0.1

IPv4 vs. IPv6

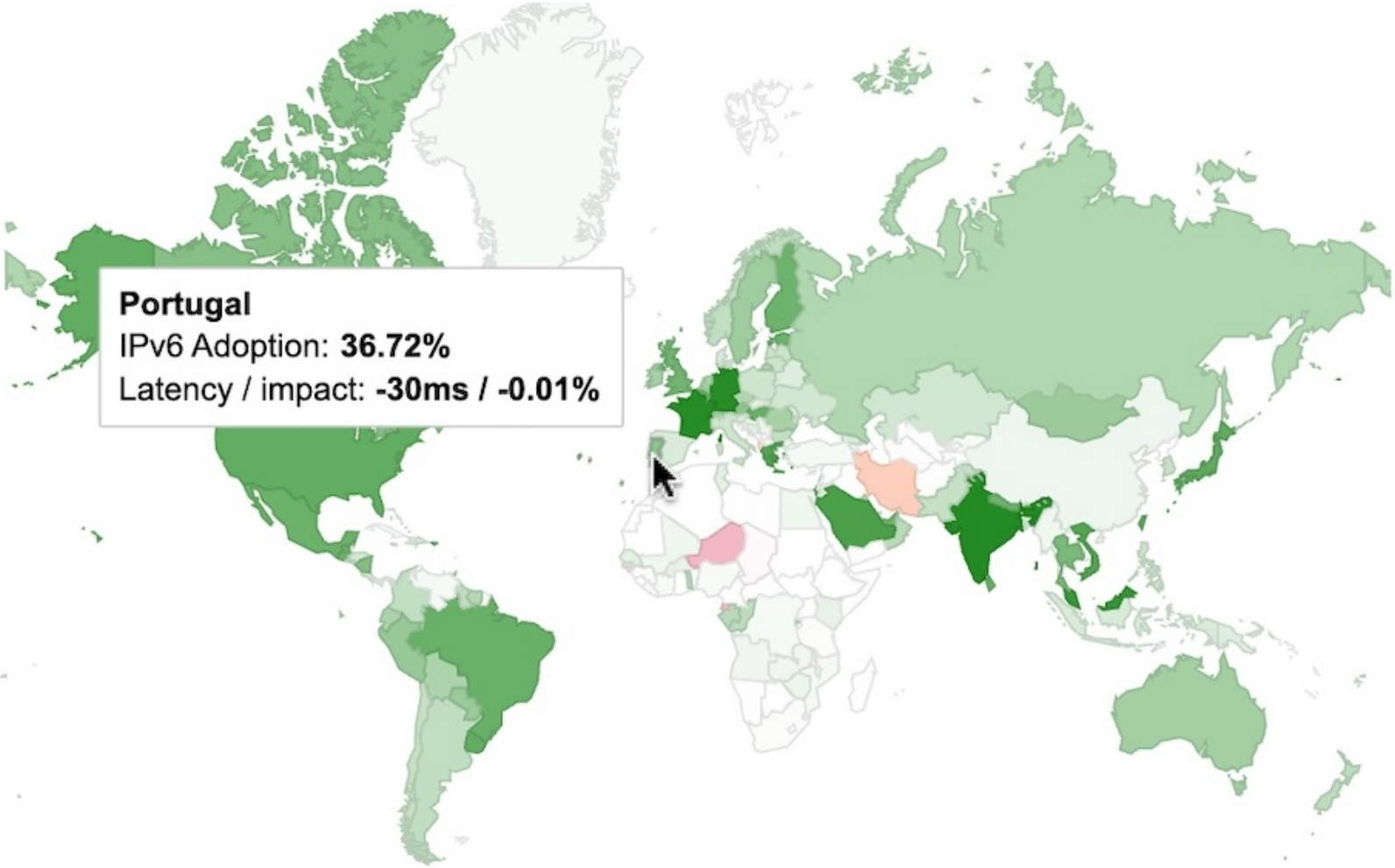
Currently, most connections are still IPv4

https://www.google.com/ipv6/statistics.html



IPv6 adoption per country

https://www.google.com/ipv6/statistics.html



Reserved IP addresses

- Loopback address (it means 'this computer')
  - 12.7.0.0.1 (IPv4)
  - ::1 (IPv6)

- Local/private addresses (IPv4): reserved for local communications between the local network only
  - 10.0.0.0 - 10.255.255.255
  - 72.16.0.0 - 72.16.255.255
  - 192.168.0.0 - 192.168.255.255

Reserved IP addresses - CIDR

- Loopback address (it means 'this computer')
  - 12.7.0.0.1 (IPv4)
  - ::1 (IPv6)

- Local/private addresses (IPv4): reserved for local communications between the local network only
  - 10.0.0.0 - 10.255.255.255 ~ 10.0.0.0/8
  - 172.16.0.0 - 172.16.255.255 ~ 172.16.0.0/16
  - 192.168.0.0 - 192.168.255.255 ~ 192.168.0.0/16

Question

Question

Check all correct statements:

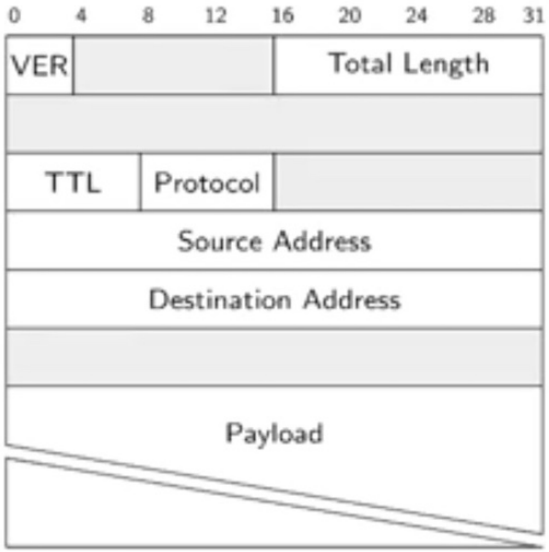
- ☐ `affe::/16` contains as many IP addresses as `beef::/16`.
- ☐ A /8 network contains twice as many addresses as a /9 network.
- ☐ `192.168.0.4/32` contains exactly one IP address.
- ☐ Hacking `127.0.0.1` and deleting all data on the machine is a bad idea.
- ☐ There are $256 * 256 = 65,536$ unique IPv4 addresses that start with `192.168`.

Roadmap

1. the network layer
2. IP addresses
3. IP packet structure
4. Routing basics
5. Safety and security in the IP layer
6. ICMP

IPv4 packet structure

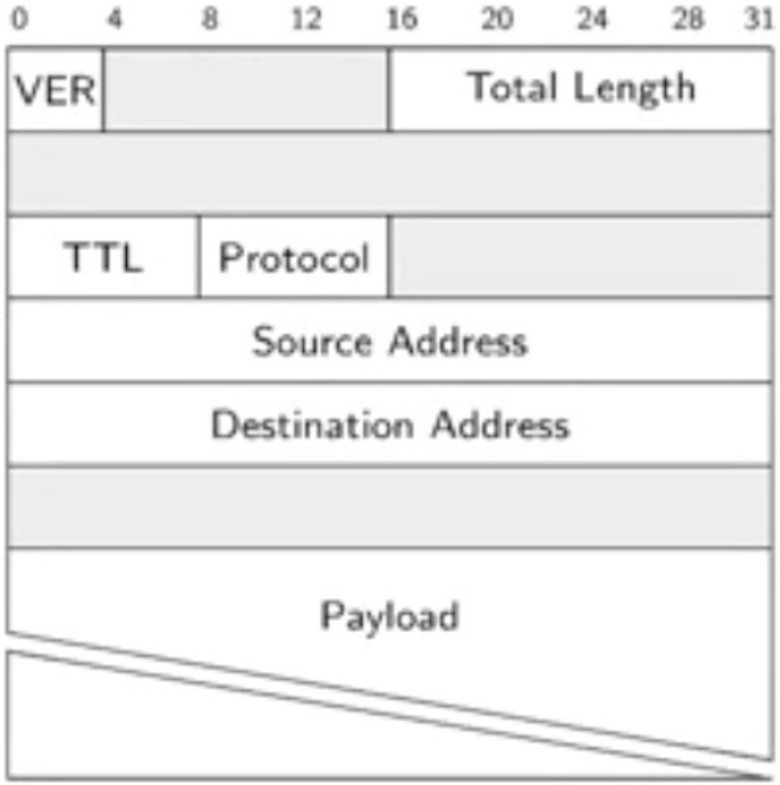
- VER: 4 bits, protocol version, 0100
- Total length: 2 bytes, total length of the packet (which sometimes is fragmented)
- TTL (Time To Live): hop limit, the maximum number of hops the package can traverse.



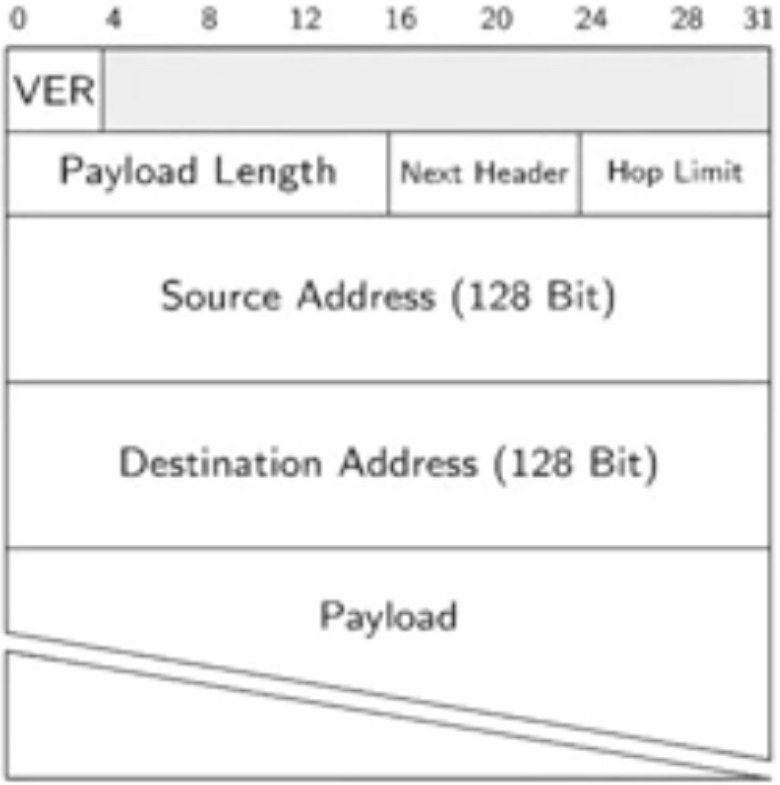
IPv4

Protocol: protocol used in the Transport Layer
Source address: where the packet is coming from
Destination address: where the packet is going to
Payload - the Transport protocol packet (remember the matryoshka image)

IPv4 vs IPv6 packet structure

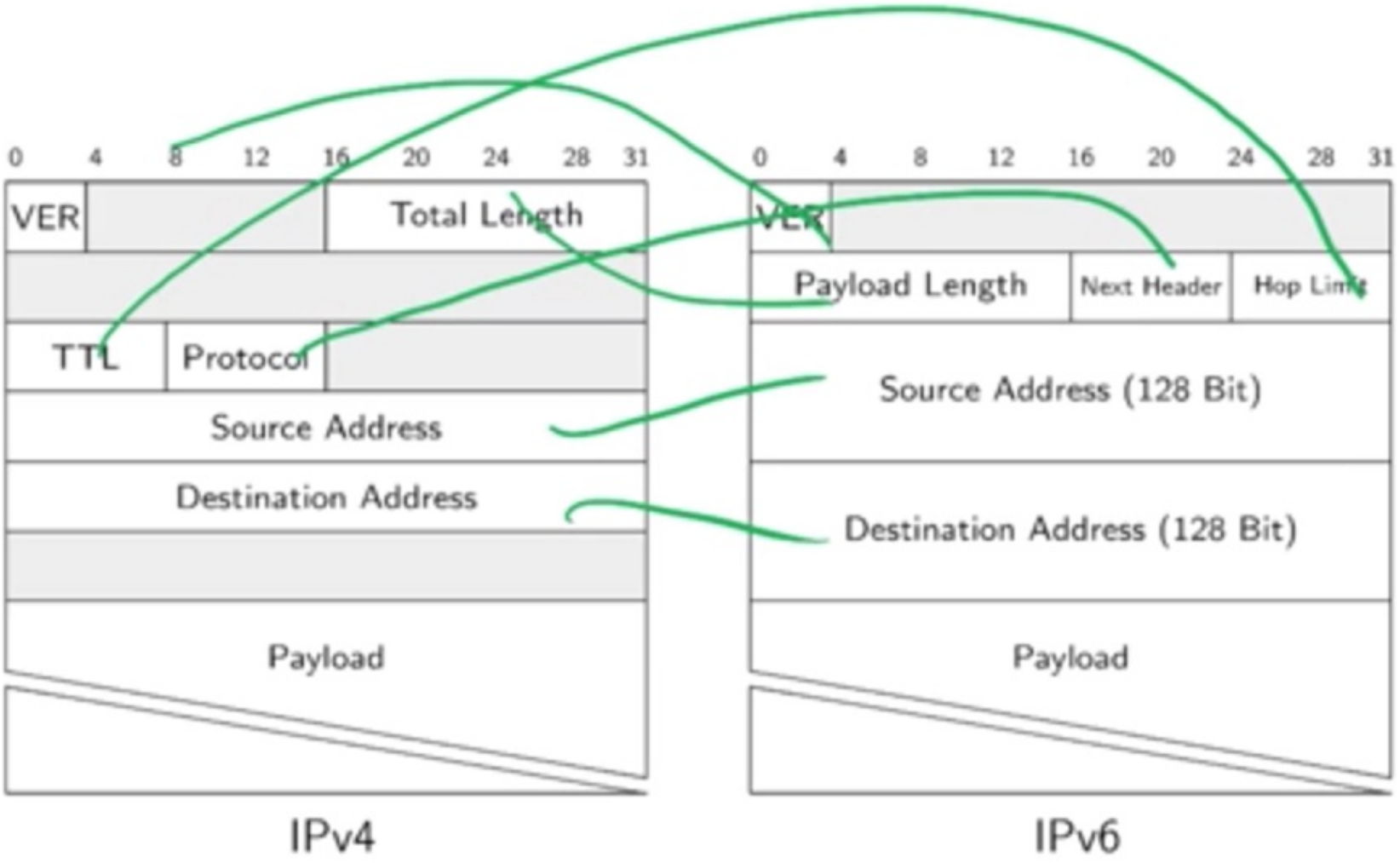


IPv4



IPv6

IPv4 vs IPv6 packet structure



The difference is Source and Destination addresses are 128 bits

Question

Question

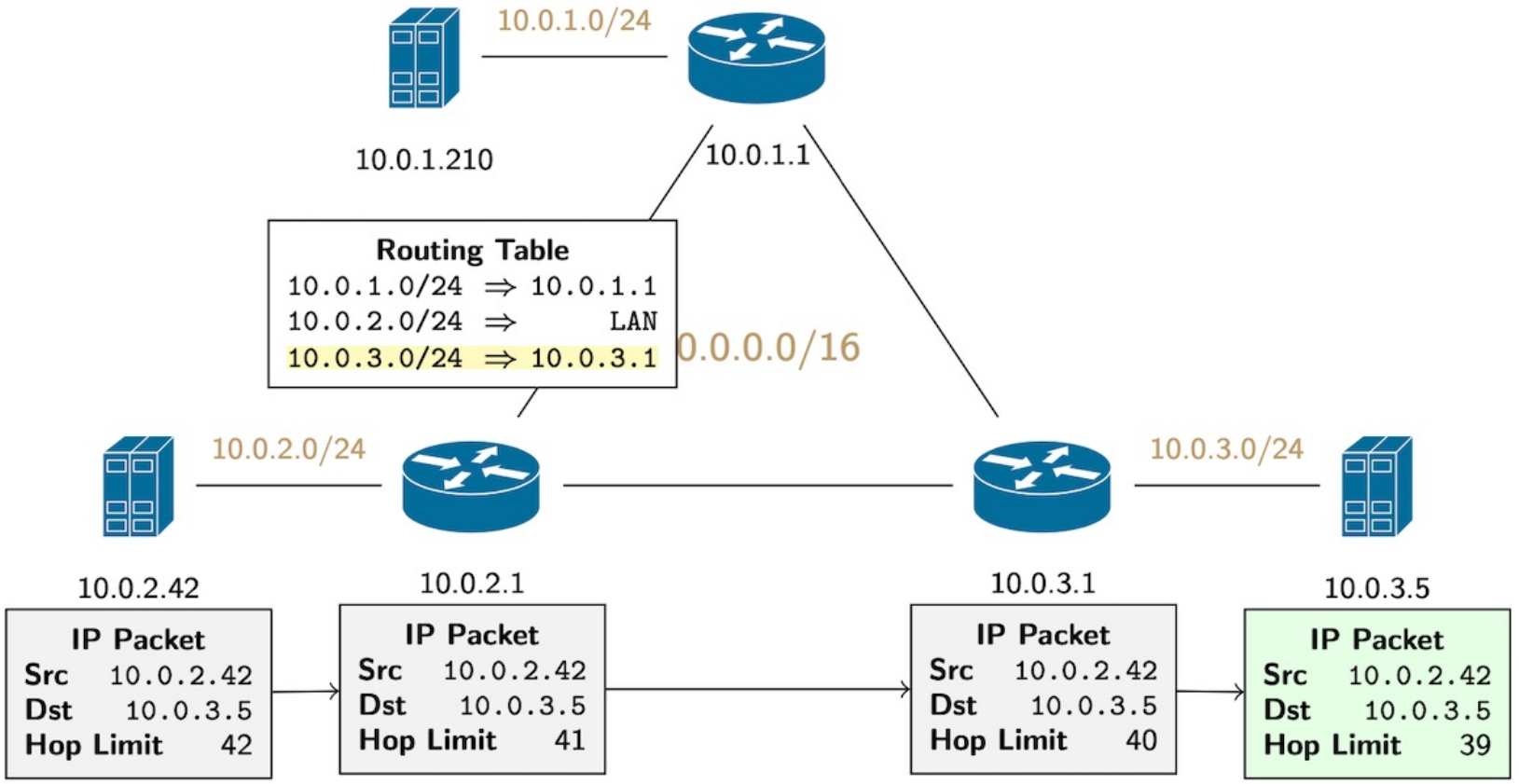
Select all correct statements:

- ☐ IP packets have a fixed length.
- ☐ The IP packet header is "sandwiched" between the link and transport layers.
- ☐ IPv6 packets contain the destination's MAC address as the destination address.
- ☐ IP packets define the transport layer protocol used in the payload.

Roadmap

1. the network layer
2. IP addresses
3. IP packet structure
4. Routing basics
5. Safety and security in the IP layer
6. ICMP

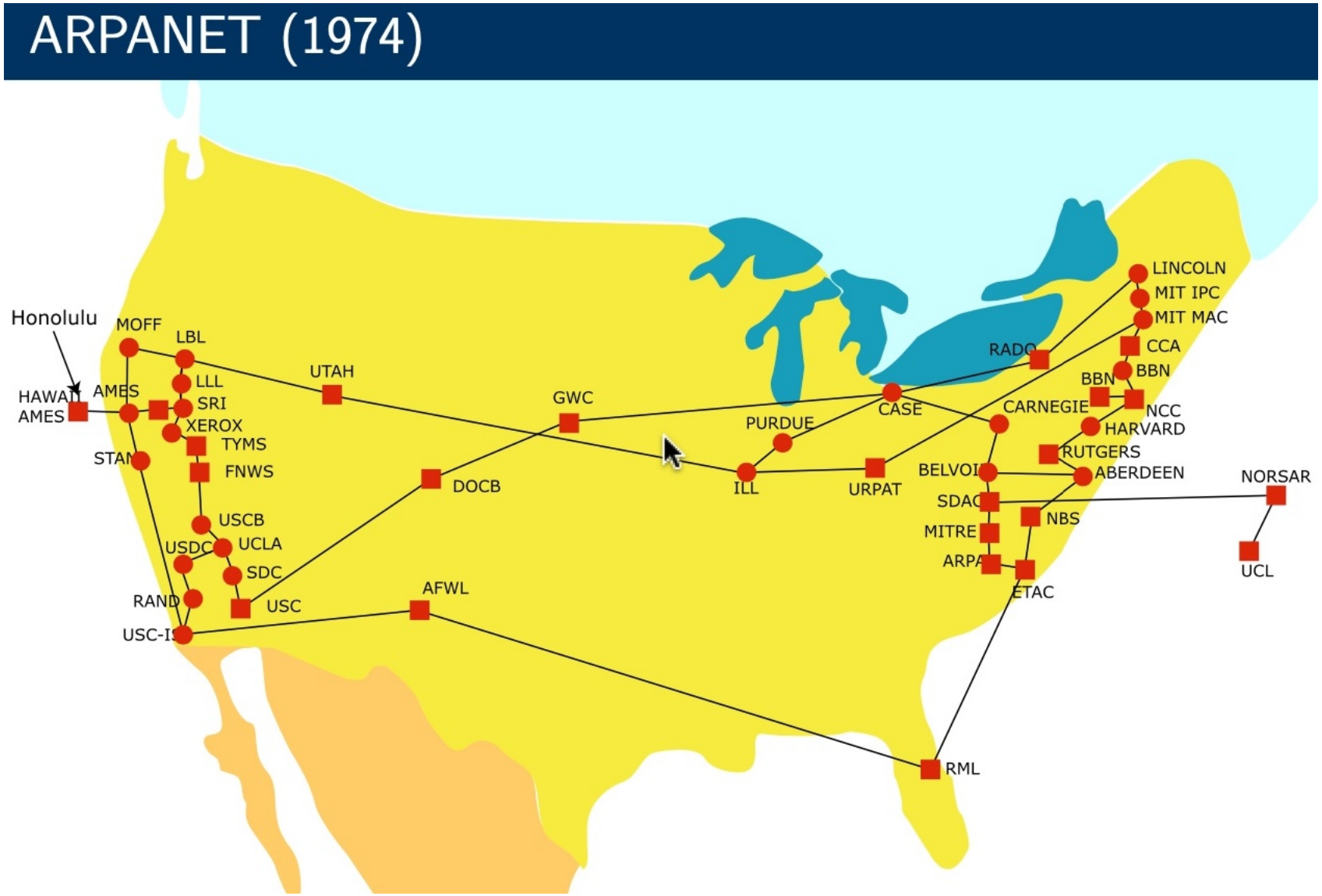
routing - basics



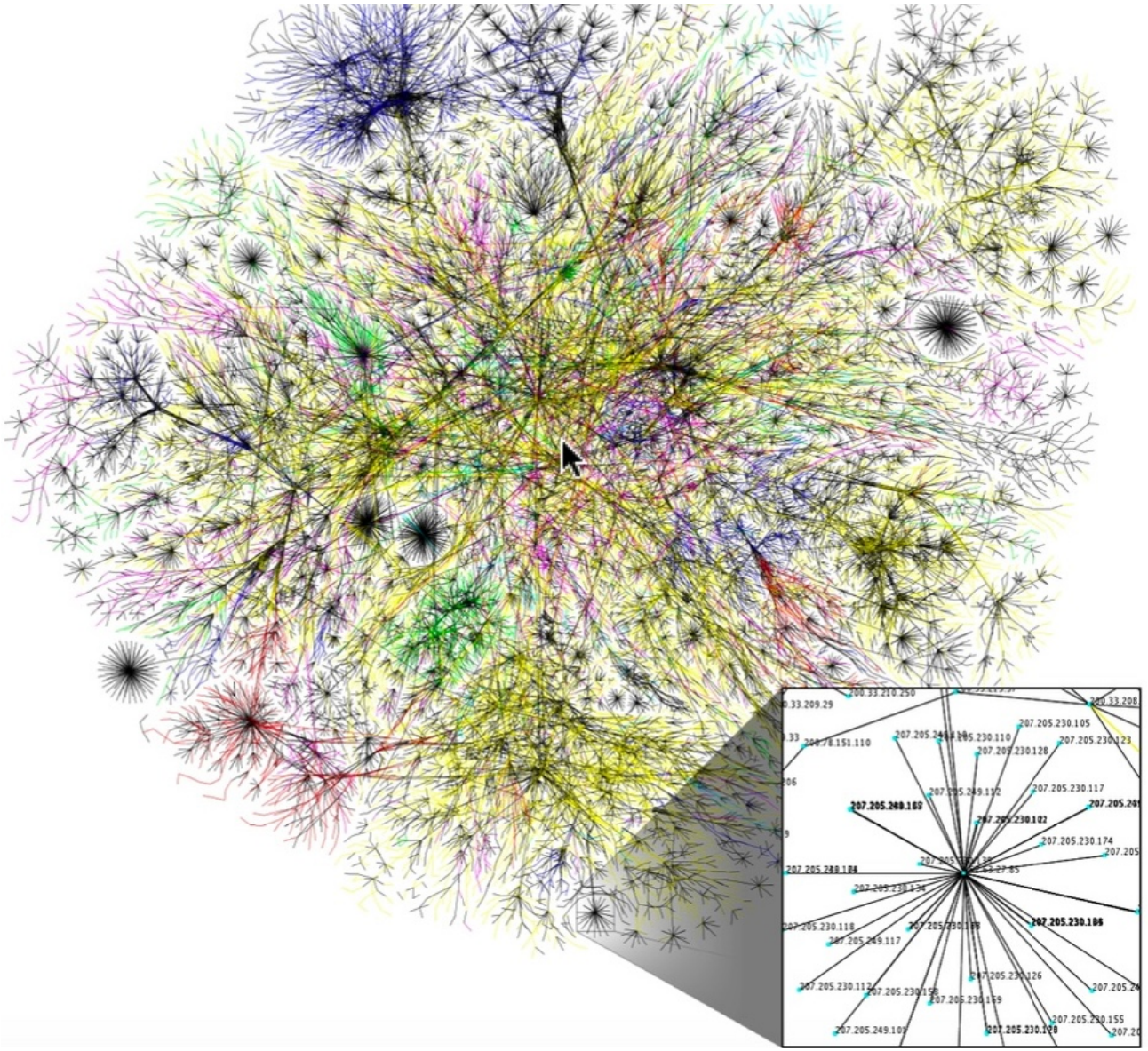
Routing Tables contain ranges of IP addresses

```
10.0.1.0/24 => 10.0.1
10.0.2.0/24 => LAN
10.0.3.0/24 => 10.0.3.1
```

Arpanet -1974



30% of Internet in 2005



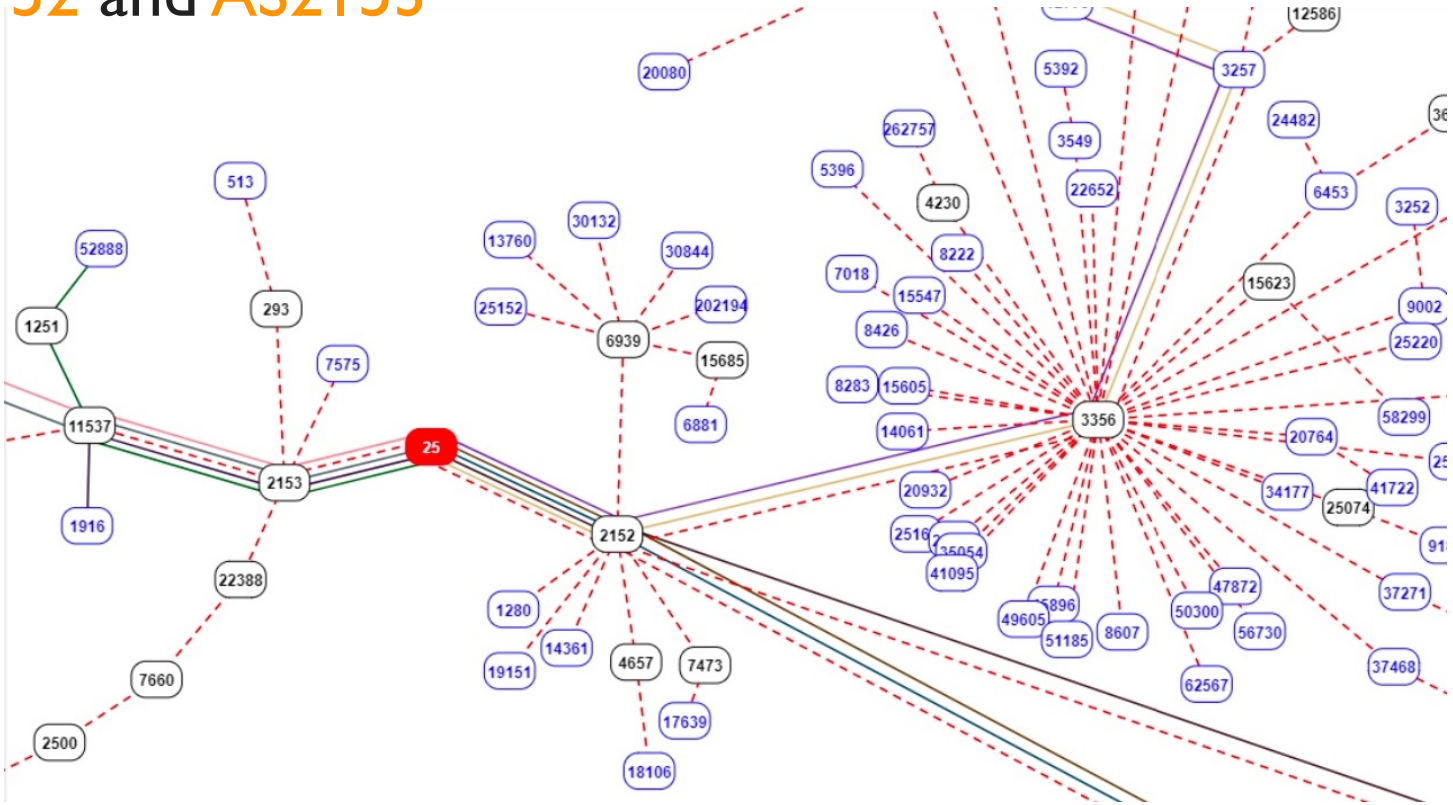
Internet

How do you maintain a routing table?

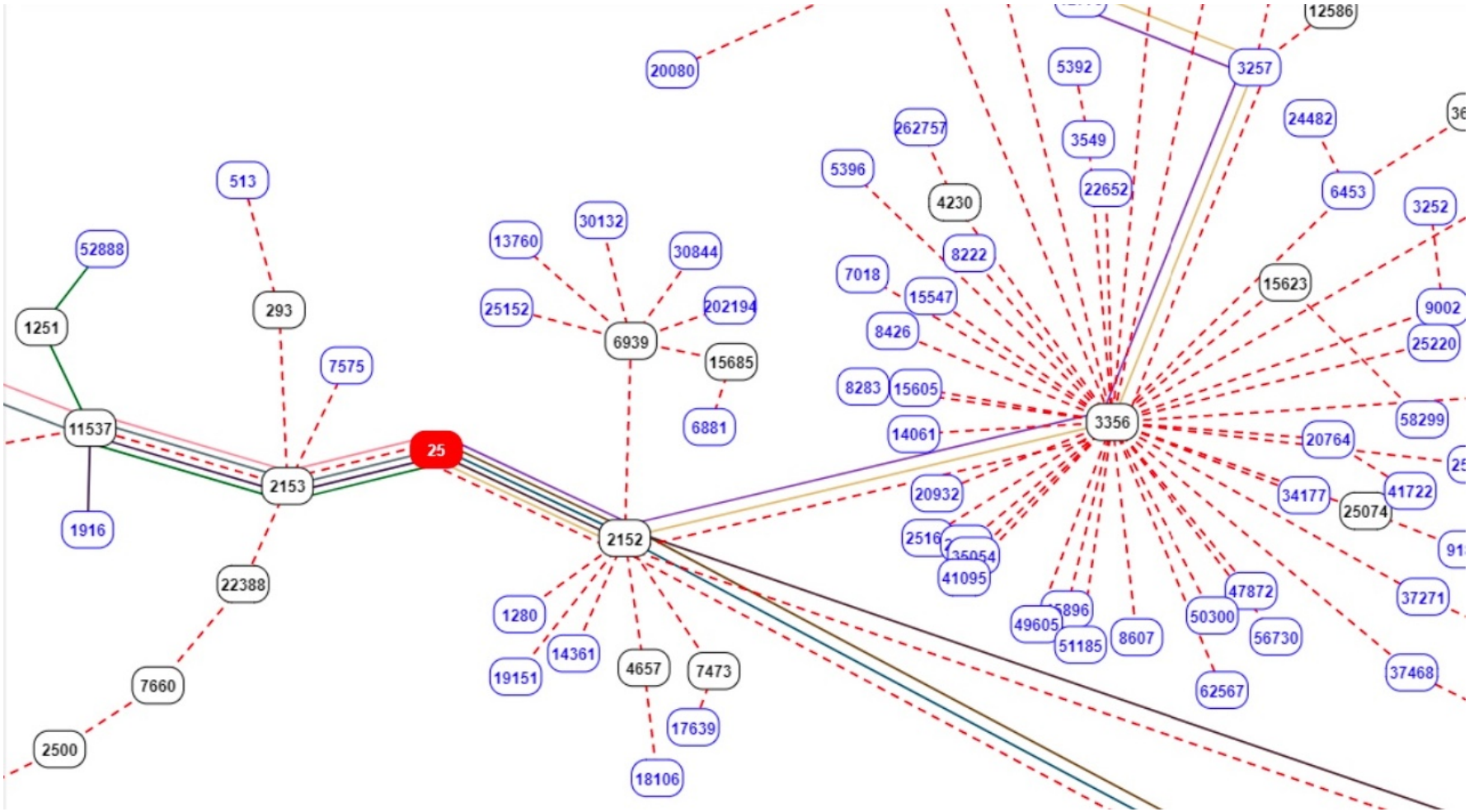
- the Internet is divided into ASs (Autonomous Systems).
  - each AS has a unique number and multiple IP ranges.
  - IGP (Interior Gateway Protocols) used for routing within ASs
- Routing: you need to take your packet to the right AS which will take care of its delivery
- BGP (Border Gateway Protocol): routing between ASs
  - BGPs are Internet Providers
- AS25 (UC Berkeley)

BGP routes for AS25

- AS25 - UC Berkeley
- Each AS owns multiple IP address ranges
  - 128.32.0.0/16 — UC Berkeley
- UC Berkeley is directly connected to 2 other systems:
  - AS2152 and AS2153



BGP routes for AS25



Questions

Check all statements that are true:

- ☐ To maximize the chances of reaching its destination, a packet should set the lowest possible hop limit.
- ☐ The destination IP address in an IP packet always points to the next router on the path.
- ☐ Having multiple submarine cables is primarily a safety measure, not a security measure.
- ☐ Many of today's internet protocols were developed for an internet with very different threat models.

Roadmap

1. the network layer
2. IP addresses
3. IP packet structure
4. Routing basics
5. Safety and security in the IP layer
6. ICMPs

safety in the IP layer

- packet delivery is not guaranteed,
- there is no confirmation that a package has been received
- package order is not guaranteed
- IP is a connectionless protocol
  - no notion of persistent connection
  - routers do not maintain a state, each packet is handled independently
  - the other delivers the packet and forgets about what it just did

security in the IP layer

- IP packets are unauthenticated plaintext
  - any router between Source and Destination can modify the contents of the exchanged packets.
  - The Source part of a packet can be faked or spoofed, e.g., I can send a postcard and sign it with someone else's name.

security in the IP layer

Spoofing or identity theft is a set of techniques that attackers use to impersonate a trusted person and trick victims into providing private information.

security in the IP layer

Confidentiality 

Integrity 

Availability 

Confidentiality and Integrity need to be addressed on higher layer

Question

Question

For their new blockchain-based cryptocurrency venture, FooBank's CTO wants to "get rid of all that old cruft" and build a revolutionary high-speed banking protocol directly on top of IP packets. They propose the following protocol for money transfers between East and West Coast branches:

> *"I first send you a packet with the receiver, then a packet with the amount, and then a packet with the recipient. Trust me, it's the best protocol we ever had!"*

What could possibly go wrong?

- ☐ Some transfers may inexplicably fail.
- ☐ Instead of sending money from Alice to Bob, FooBank may end up sending money from Bob to Alice.
- ☐ Mischievous attackers may get rich.
- ☐ Someone in Russia may get wind of it.

Roadmap

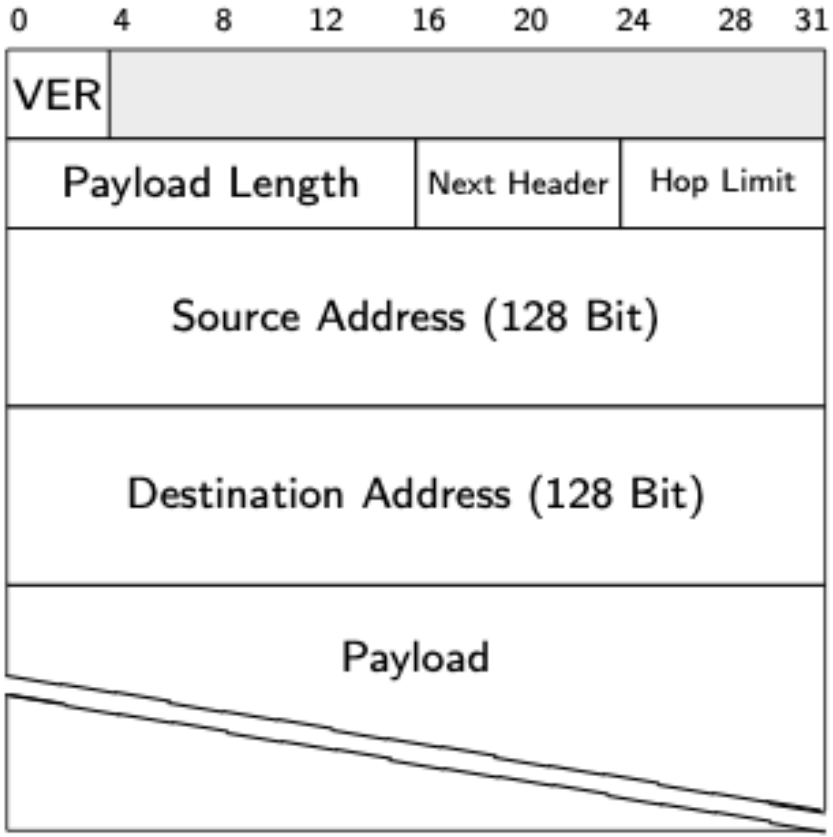
1. the network layer
2. IP addresses
3. IP packet structure
4. Routing basics
5. Safety and security in the IP layer
6. ICMP

ICMP Internet Control Message Protocol

- Why do we need ICMP?
  - Error reporting
    - Destination unreachable
    - Packet too big
  - Diagnosing
    - ping
    - traceroute

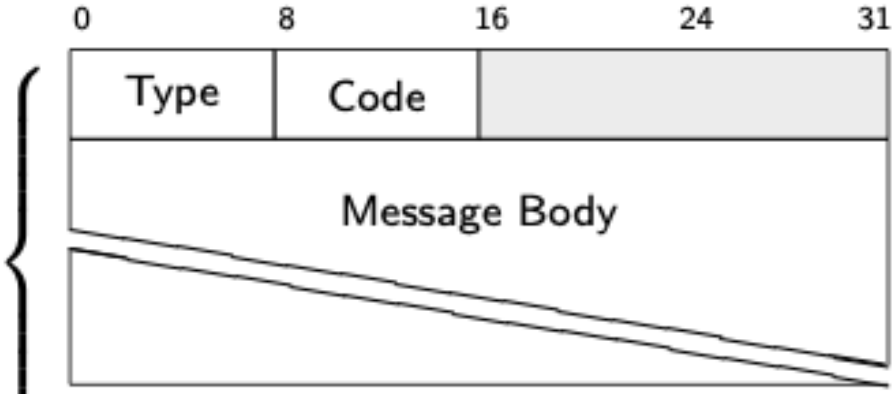
ICMP is the supporting protocol for BGP

ICMP packets



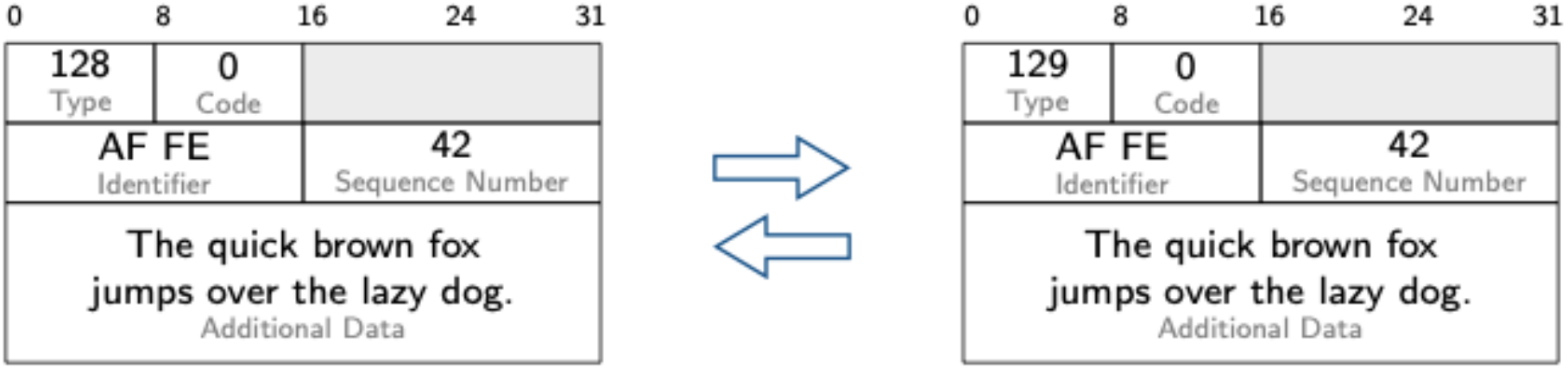
IPv6

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



ICMPv6

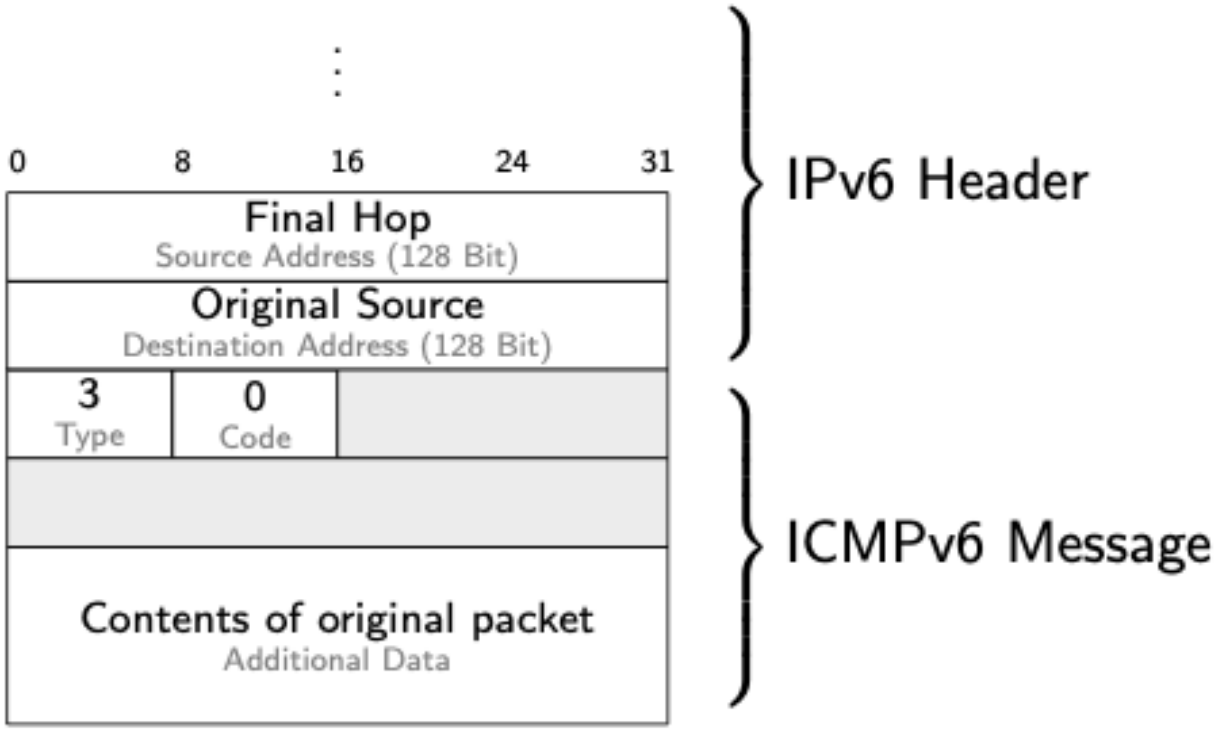
ping - can we reach another machine?




```
$ 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
```

traceroute - how do we inspect which route our packets take?

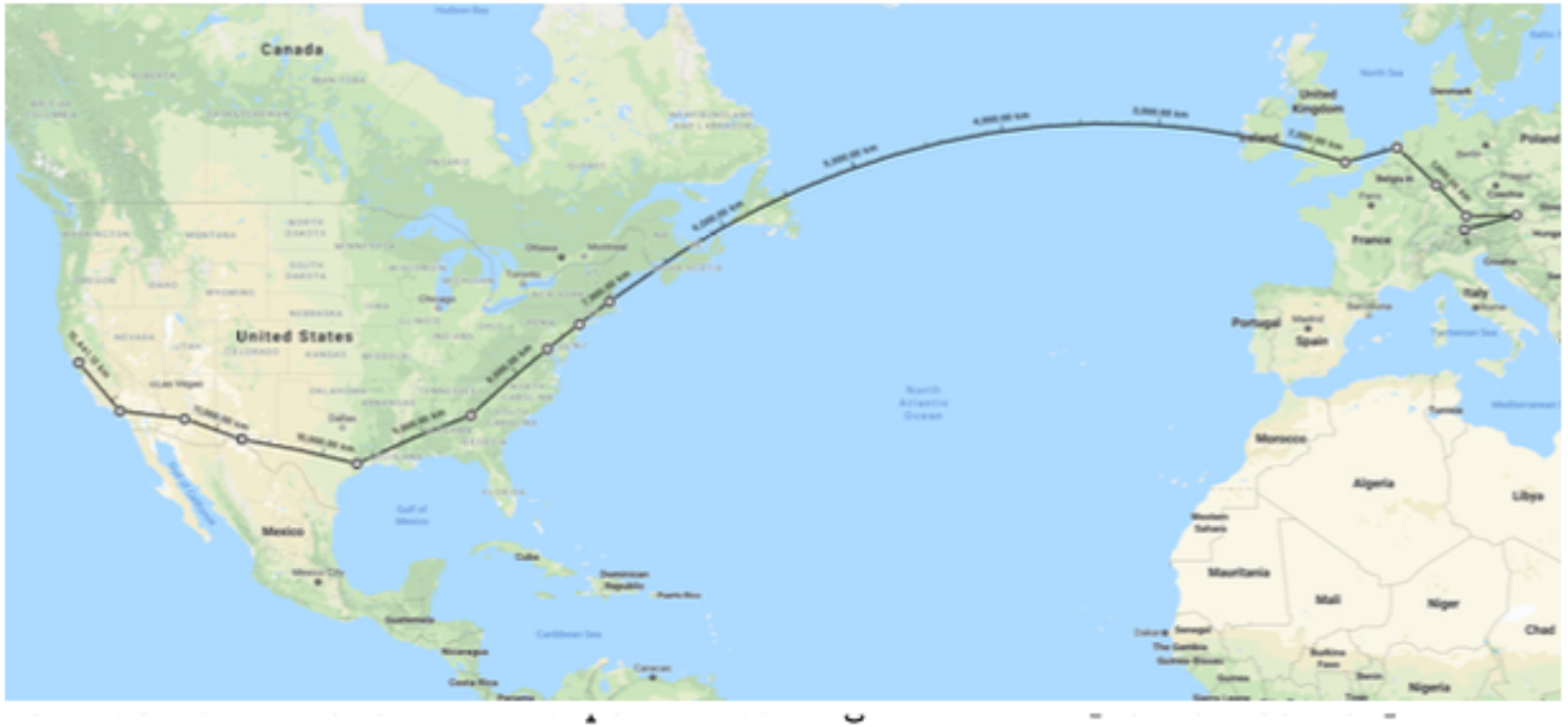
We can modify the Hop Limit and analyze ICMP errors!



ICMPv6 Time Exceeded Message

traceroute - which route our packets take?

```
$ tracert berkeley.edu
Tracing route to berkeley.edu [35.163.72.93] over a maximum of 30 hops:
```




```
16   174 ms   be2930.ccr32.phx01.atlas.cogentco.com [154.54.42.77]
17   173 ms   be2932.ccr42.lax01.atlas.cogentco.com [154.54.45.162]
18   177 ms   38.142.35.250
19     *      Timeout.
20     *      Timeout.
21   193 ms   ec2.us-west-1.amazonaws.com [35.163.72.93]
```

Internet network summary

IPv4 and IPv6

- Addressing
- Routing
- Addresses & Packets

Central Properties

- best effort
- connection-less
- unauthenticated plaintext

Security

- Eavesdropping
- BGP Hijacking

ICMP

- ping
- traceroute