The Internet Protocol

Applied Network security (comp420 –001)

Department of Computer science

Fall 2020

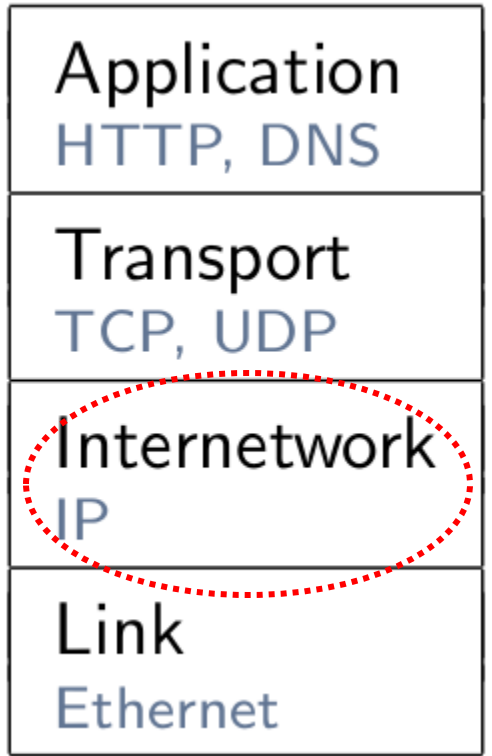
The Internet Protocol

- This layer (aka layer 3) is responsible for connecting multiple local networks. Most importantly, it forms the basis of the Internet.
- You are sitting in your local network at home. Your friend is sitting in his local network at home. The Internetwork layer (using the Internet protocol or-- short-- IP) makes it possible that both of you can exchange messages.
- One interesting thing about IP is that it almost always

sits on top of Ethernet. But it does not depend on Ethernet.

And in theory, you could replace Ethernet with something

else on the linked layer.



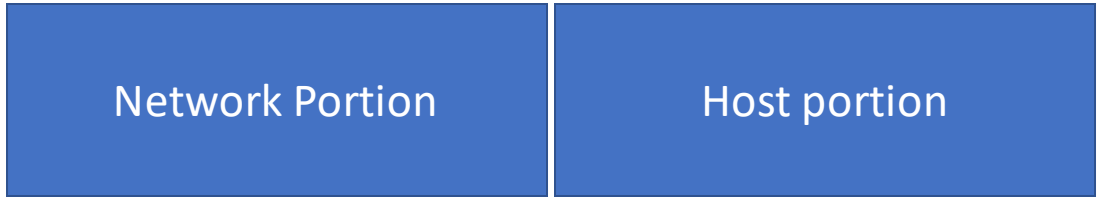
The Internet Protocol (Cont.)

- Why don't we just use Ethernet for everything? Well, the main problem is that, when you look at Ethernet addresses, they only contain information on the manufacturer. You have no idea where the device is located in the network.
- So in order to send packets to the correct port, every switch needs to manage a list of all connected devices.
- This is very much like trying to deliver mail using just a person's name. You can imagine with billions of devices on the Internet, this is impractical. So we cannot use the Ethernet for this.
- In the real world, we have solved this problem with addresses that are much more hierarchical (compared to what we have in the Ethernet).

The Internet Protocol (MAC Vs. IP)

- With the internet protocol, every device not only have a MAC address, but also it has an IP address.

- The IP address is different from a MAC address in two important ways:
  1. In contrast to a MAC address, IP addresses are not constant. So every time you join to your network, you will get a new IP address from whoever operates the network.
  2. The first part of the address will be the same for all devices in a local network. So IP addresses of every device in your local coffee shop will start with the same bytes. For MAC addresses, you can tell who manufactured the device by the first bytes of the address. For IP addresses, the first bytes act as a locator. So if I give you my current IP address, you can look up which city I'm currently in.



Each IP address has two portions

The Internet Protocol (Routing)

- Another thing the internet protocol provides is routing.
- Routing is basically the science of finding the shortest path to a destination.
- For every IP address, the router knows which of its direct neighbor routers provides the fastest route to the destination. However, instead of keeping track of every individual IP address, the router determines the route by looking at the first part of the IP address.
- This is why routers are known as layer3 devices.

Your Turn 1

Check all statements which are true:

A) Every router keeps track of all devices connected to the entire Internet.

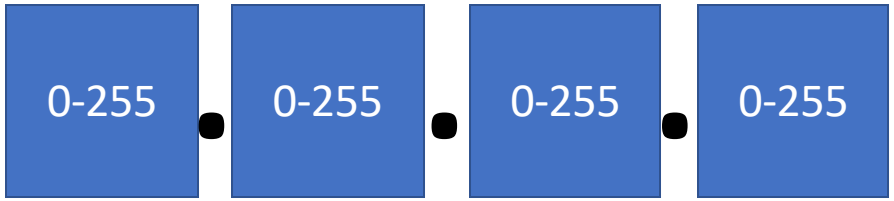
B) A device will keep the same IP address over its lifetime.

C) A device will keep the same MAC address over its lifetime.

D) IP addresses can be used to implement "Geo-blocking", a technique where access to content is restricted based on the user's geographical location.

IP Address

- There are two versions of the protocol-- the old, IPv4, and the new, IPv6.
- When we as humans talk about IPv4 addresses, we usually represent them as four numbers separated by dots.



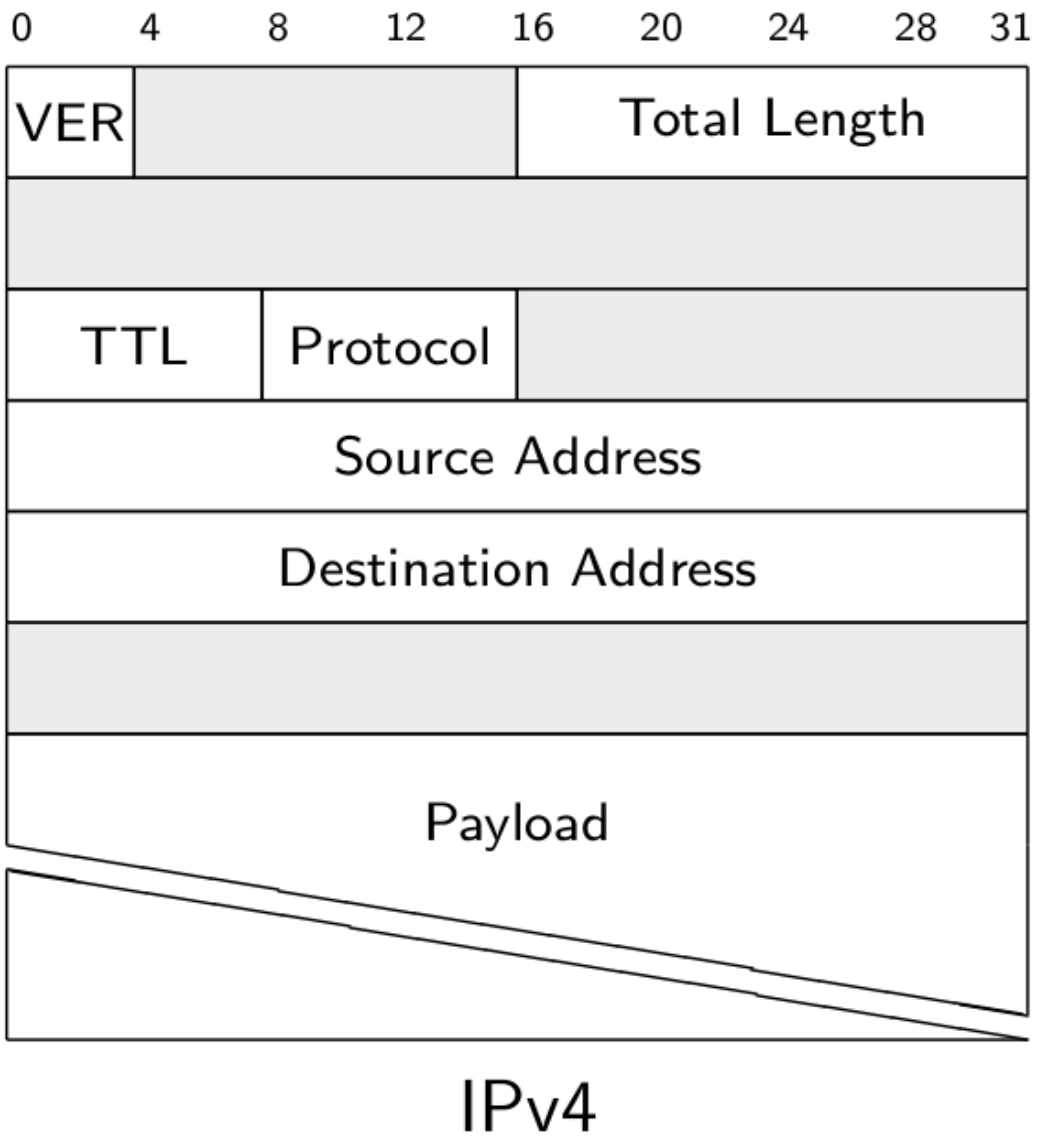
- This is called the dotted decimal notation. Each decimal is a number between 0 and 255, so they essentially represent one byte-- eight bits-- each.
- IP addresses usually come with something called subnet mask. The subnet mask has the same structure as IP address. It just define how many bits in an IP address goes for network identification and how many bits will go for host identification.

IP Address (Cont.)

- why do we even need IPv6? Well the answer is the number of available addresses in IPv4 space is a bit small for the Internet. With our 32 bits, we can represent 2 to the power of 32 devices, so that's about four billion unique IP addresses.
- IPv6 addresses are represented in hexadecimal with colons in between.
- They are much longer than IPv4 addresses. An IPv6 address is 16 bytes long.
- In total, there are 340 billion, billion, billion, billion unique addresses.

2002:0CDB:FE01:AC12:8A2E:0000:0000:0000

IPv4 Packet structure



IPv4 Packet structure (Cont.)

- We first have four bits that state protocol version. It's always 0100 which is a four in binary.
- The second important field is at offset 16, Where we have two bytes that contain the total length of the packet. This is important because an IP packet is sometimes fragmented into multiple Ethernet frame and we want to make sure that we have the full packet.
- Next, at offset 64, we have the hop limit, which is called time-to-live in IPv4. This states the maximum length of hops that the packets may traverse.
- Directly after the hop limit, we have a byte that identifies the encapsulated protocol. This tells us the protocol that is used on the next layer, the transport layer.
- Next, we get to the two most important fields, the source and destination addresses. These fields tell us where the packet is coming from and where it is going to.
- Finally, we have the packet body, containing the transport protocol packet.

Your Turn 2

Check all statements which are true:

A) IP packets have a fix length.

B) The IP packet header is "sandwiched" between the link and transport layer.

C) IP packets define the transport layer protocol used in the payload.

IP Packet Safety and Security

- **IP is a best effort protocol:**
  - Packet delivery and delivery order is not guaranteed.
  - There is no confirmation that a packet has been received on the internet web layer.
  - It happens surprisingly often that packets are delivered in a different order than they were sent because one of them is delayed and the other isn't.
  - It is the job of the layers above IP to deal with all of that.
- **IP is a connectionless protocol:**
  - Internet protocol has no concept of persistent connections.
  - Routers maintain no state;
  - each packet is handled independently.
- **IP is unauthenticated plaintext.**
  - A packet's source IP address can be spoofed.
  - Every router between you and your peer can read and modify contents of the packe syou are exchanging.

Your Turn 3

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?

1. Some transfers may inexplicably fail.
2. Instead of sending money from Alice to Bob FooBank may end up sending money from Bob to Alice.
3. Mischevious attackers may get rich.
4. Someone in Russia may get wind of it.