CS 88: Security and Privacy

18: PKI and Introduction to Networking

04-09-2024

slides adapted from Dave Levine, Jim Kurose

SWARTHMORE COLLEGE

Reading Quiz

Network Security!

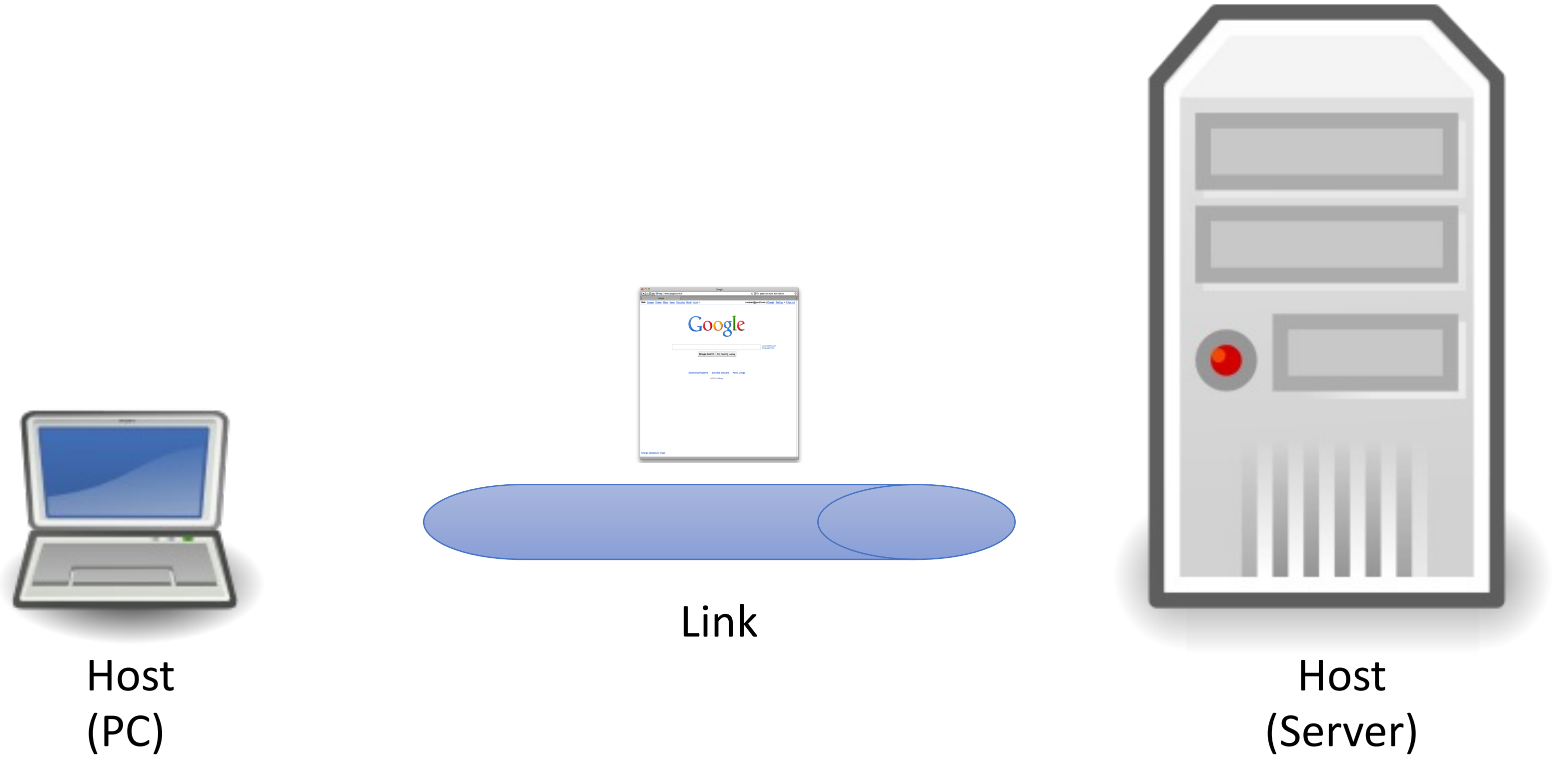
What is the goal of a network?

- Allow devices communicate with one another and coordinate their actions to work together.

- Piece of cake, right?

A “Simple” Task

Send information from one computer to another



Host
(PC)

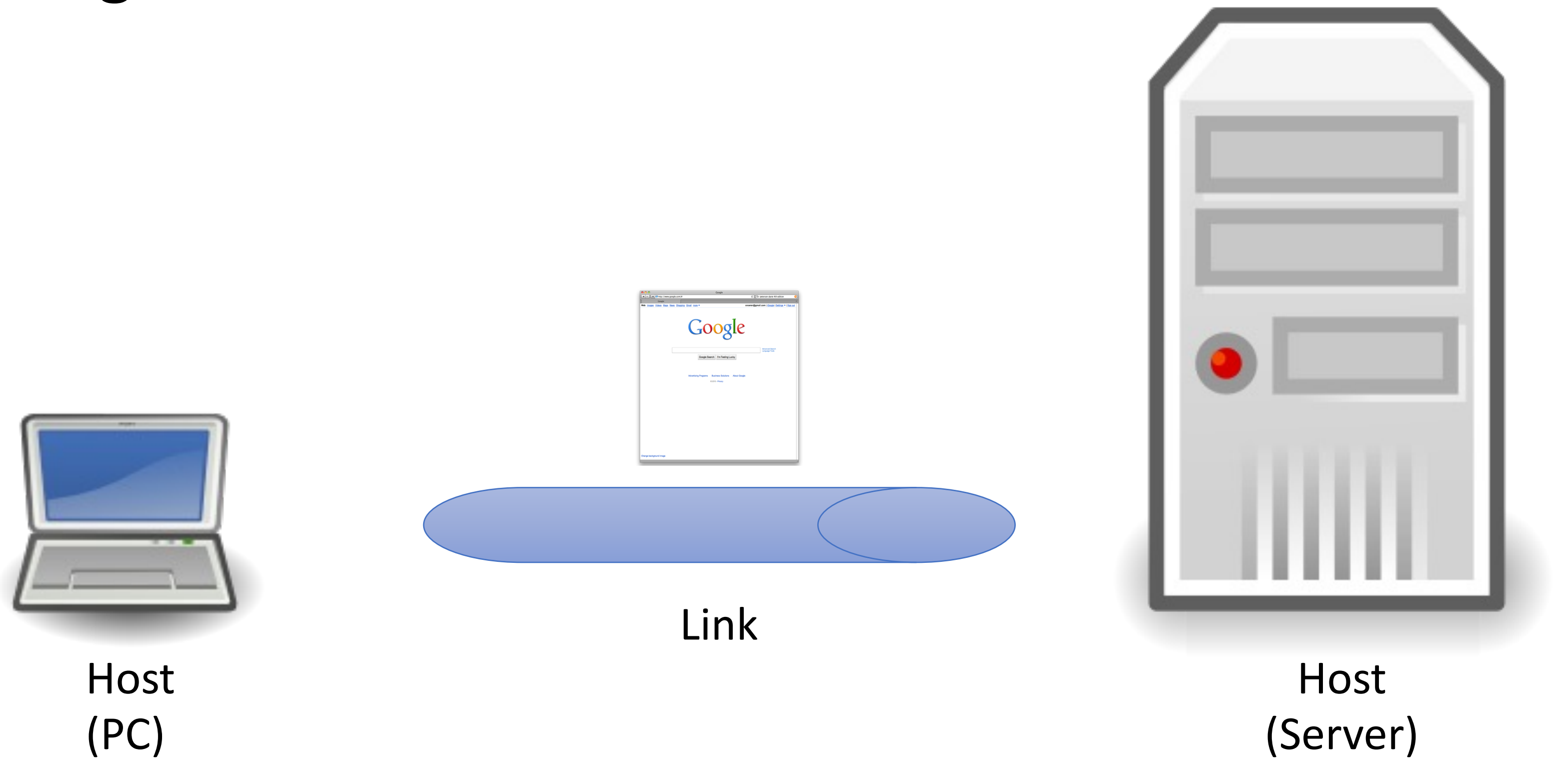
Link

Host
(Server)

A "Simple" Task

Send information from one computer to another

- hosts: endpoints of a network
- The plumbing is called a link.

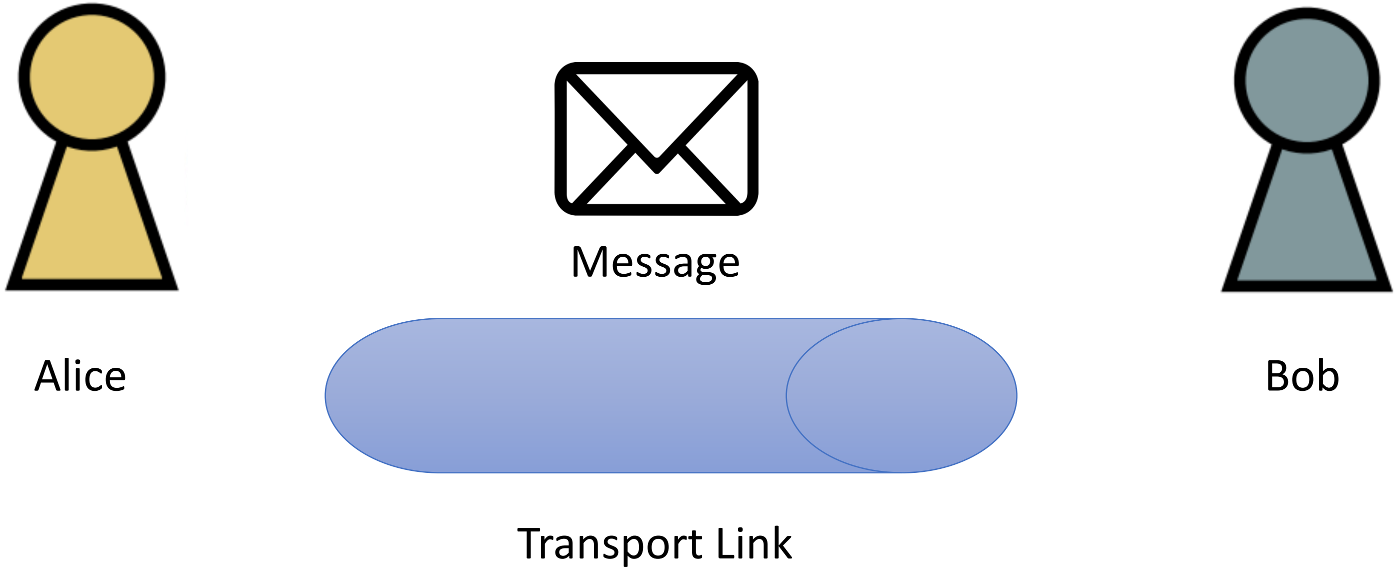


A "Simple" Task: Sending a message from host to destination

But first... let's try the postal system, something we are all (still!) familiar with and address a couple of key challenges..

A “Simple” analogous task: Post-it Note

Alice and Bob are Swatties starting out their semester and are roommates. Alice wants to give Bob a reminder to get milk.



A “Simple” analogous task: Post-it Note

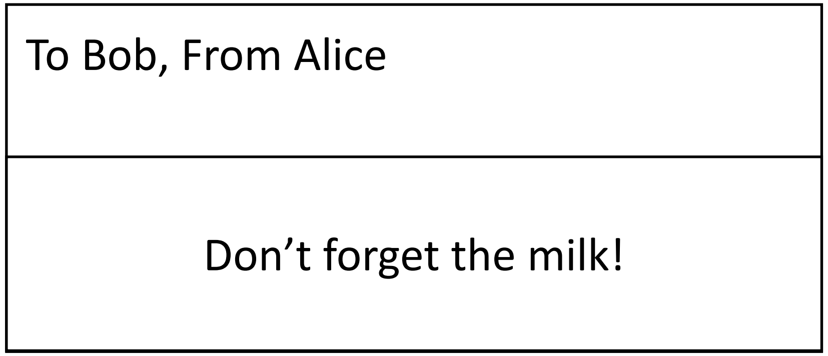
Alice and Bob are roommates, Alice wants to give Bob a reminder to get milk.
Figure out some key tasks:

1. **Structure of the message:**
    - Construct the message that Alice posts to Bob.
2. **Organizing a drop-off point.**
    - Who chooses the drop-off point?
3. **Write a protocol to write a note /post—it to your housemate**

A “Simple” analogous task: Post-it Note

Alice and Bob are roommates, Alice wants to give Bob a reminder to get milk.

1. **Structure of the message: (Alice to Bob)**



To Bob, From Alice

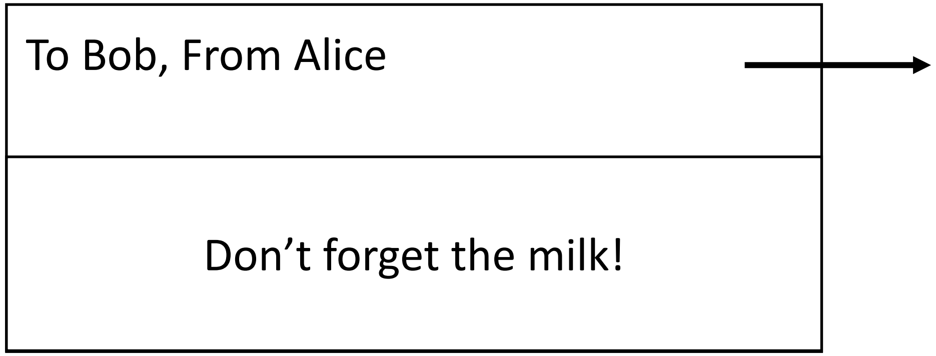
Don’t forget the milk!

Irrespective of the source and destination, the format of the message stays the same.

A “Simple” analogous task: Post-it Note

Alice and Bob are roommates, Alice wants to give Bob a reminder to get milk.

1. **<u>Structure of the message: (Alice to Bob)</u>**



To Bob, From Alice

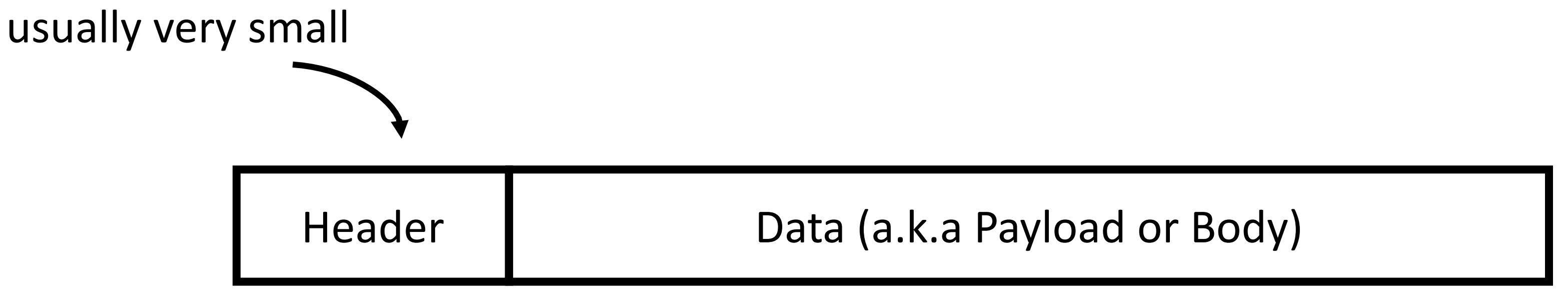
Don’t forget the milk!

Header: contains sender/receiver information
+ additional state

- timestamp
- urgent! (priority)
- ordering of messages (1 of 10..)
- error control..

<u>Irrespective of the source and destination, the format of the message stays the same.</u>

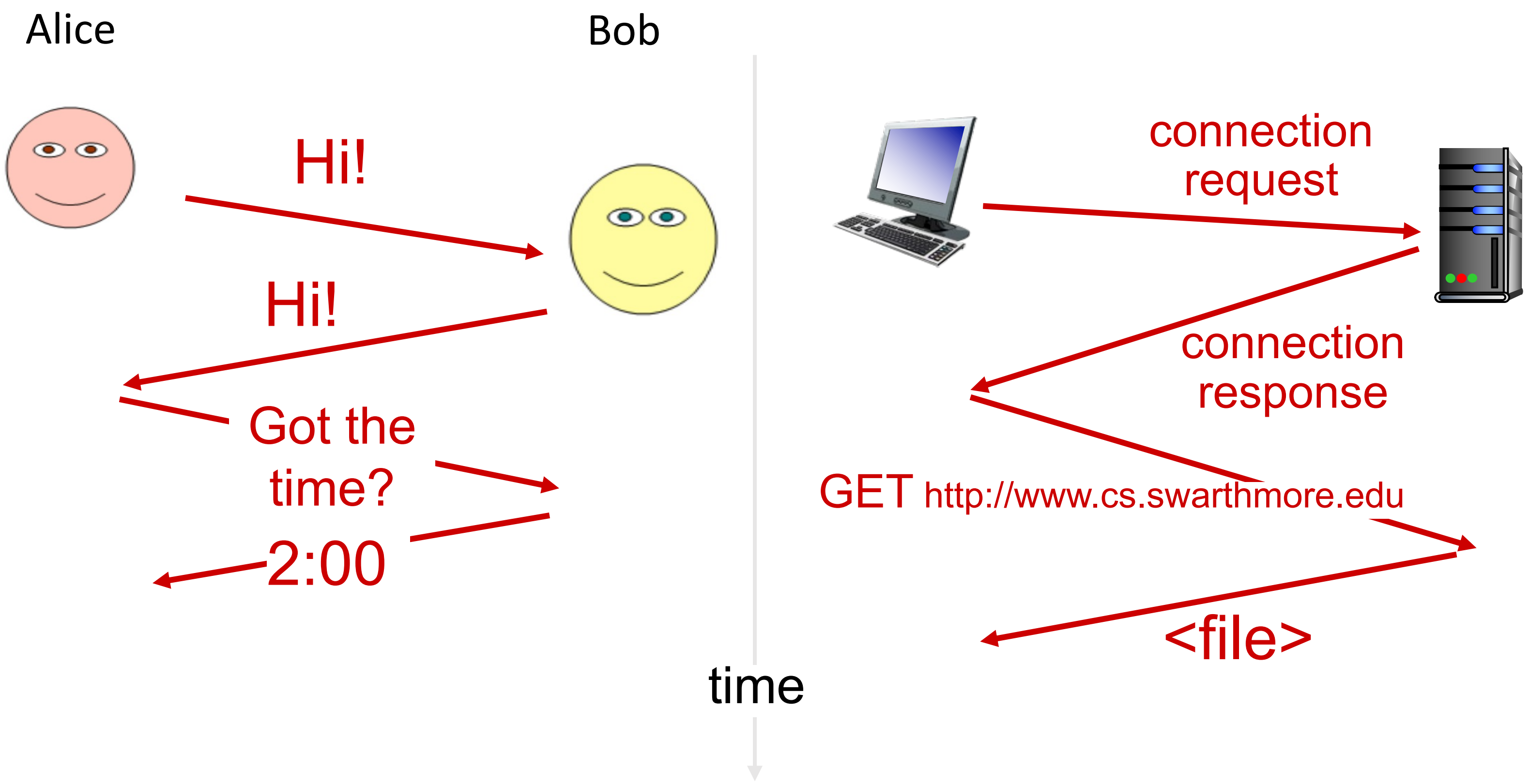
Network Packet



- Message: Header + Data
- Data: what sender wants the receiver to know
- Header: information to support protocol
  - Source and destination addresses
  - State of protocol operation
  - Error control (to check integrity of received data)

What is a protocol?

Protocol: message format + transfer procedure



Human Protocol

Network Protocols
(defined in RFCs)

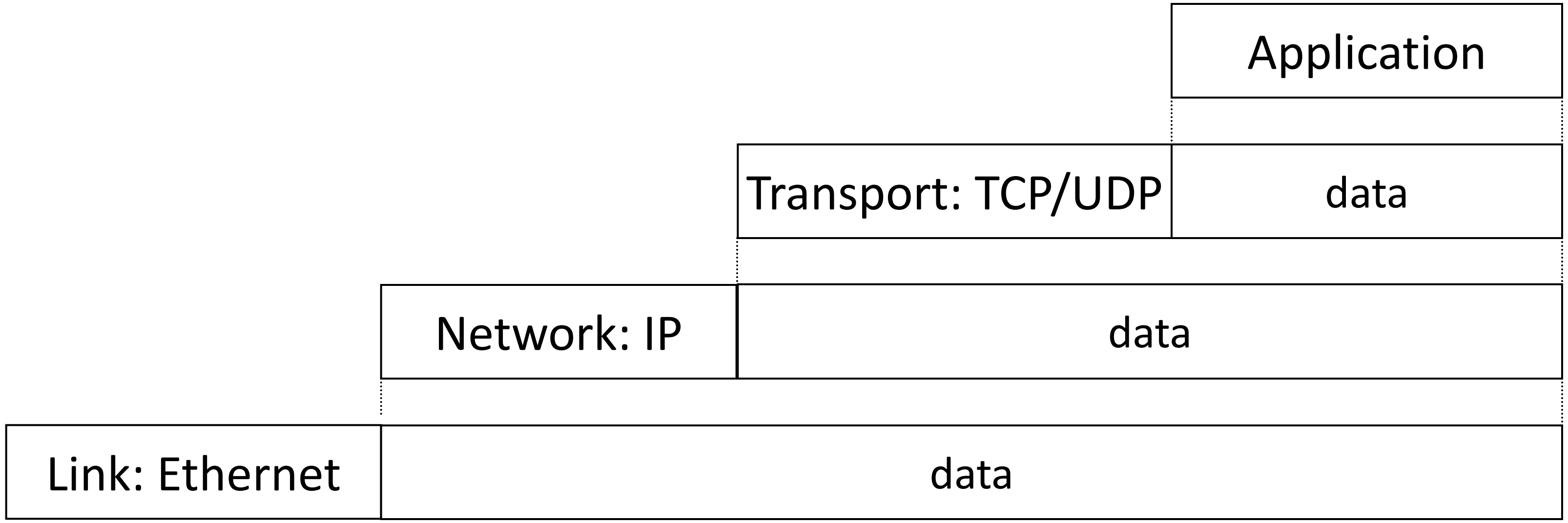
What is a protocol?

Goal: get message from sender to receiver

Protocol: message format + transfer procedure

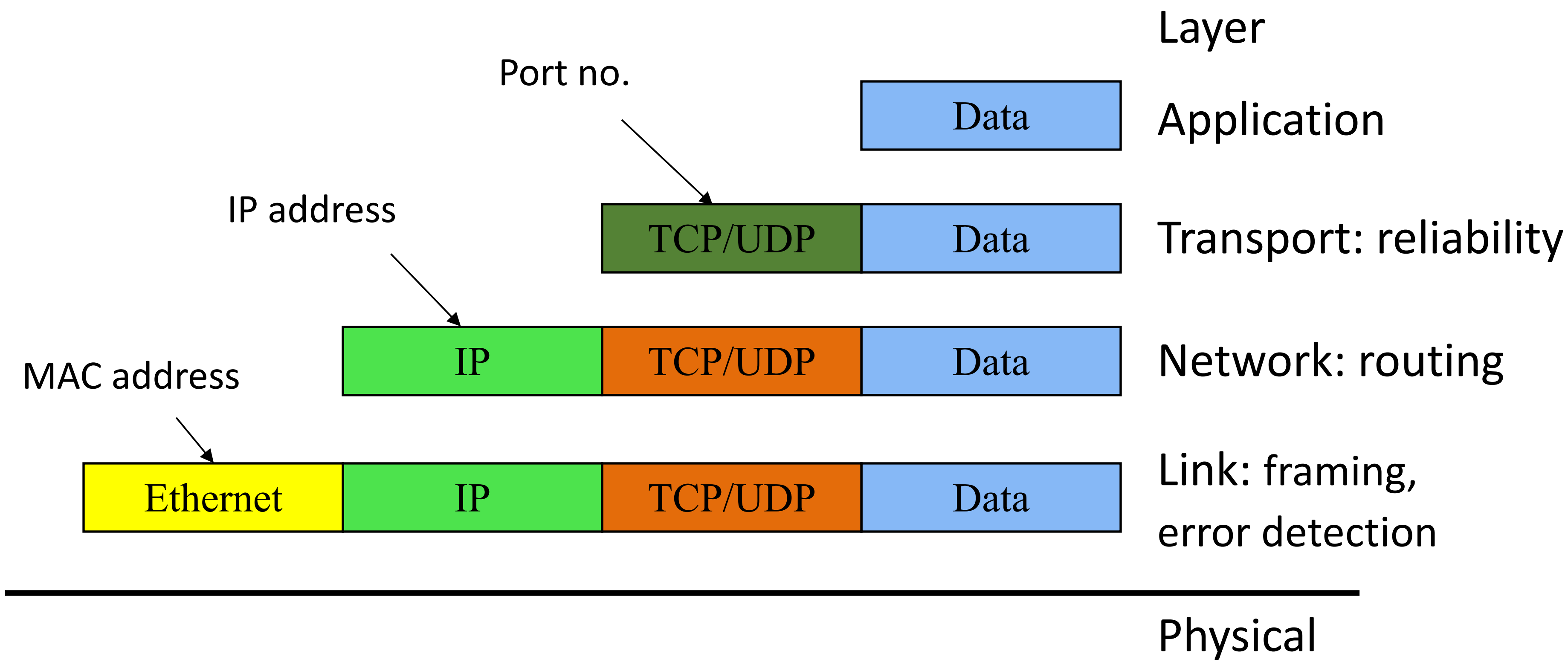
- Expectations of operation
  - first you do x, then I do y, then you do z, ...
- Multiparty! so no central control
  - sender and receiver are separate processes

Message Encapsulation



- Higher layer within lower layer
- Each layer has different concerns, provides abstract services to those above

Layering and encapsulation



A “Simple” analogous task: Postal Mail

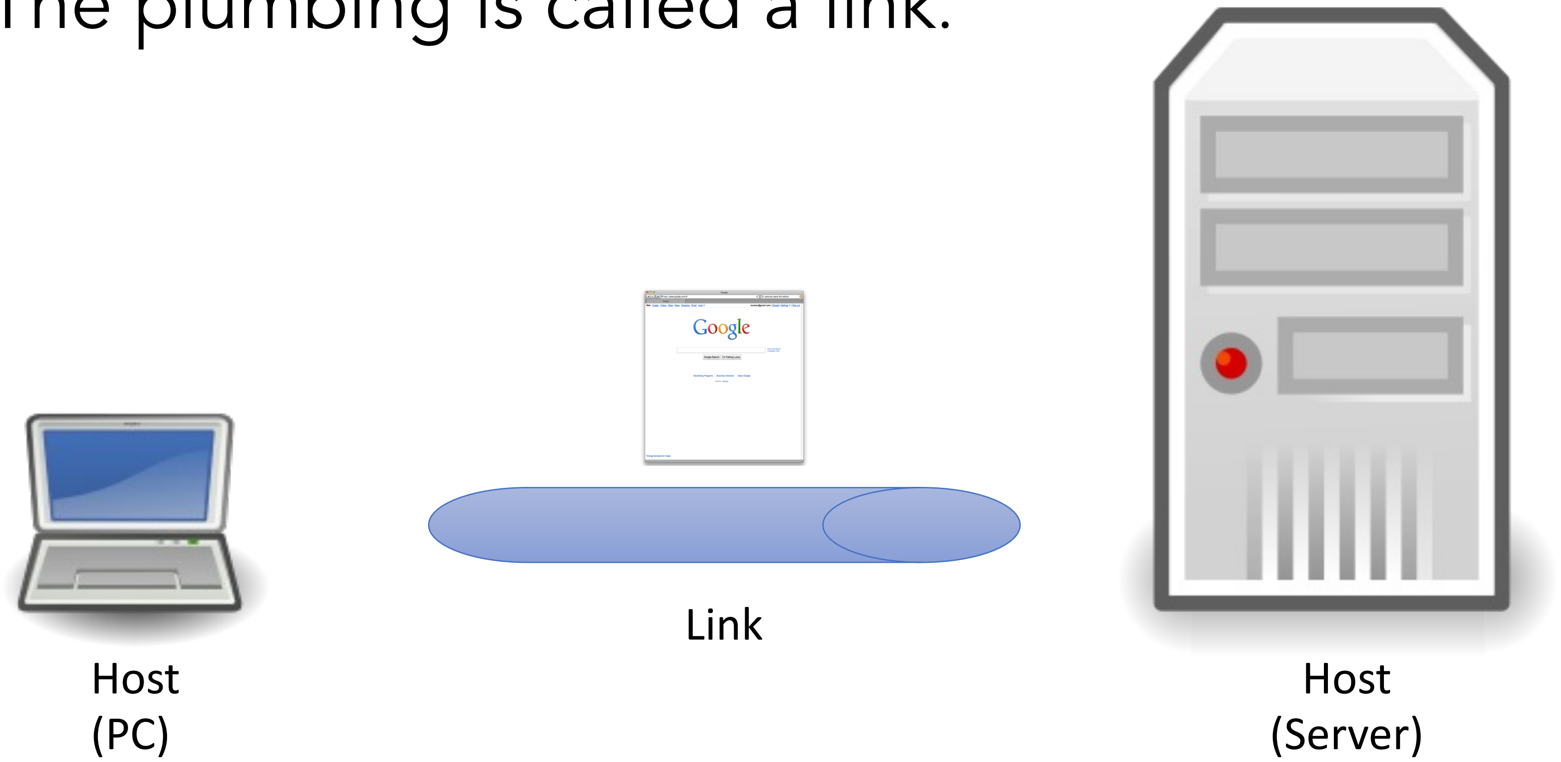
Many more considerations:

- Who decides the the sender and receiver addresses? Does someone maintain a mapping peoples’ names to addresses?
- Can Bob always be guaranteed of this delivery date? What factors influence delivery ?
- What if the mail gets lost – who’s responsibility is it? Alice, Bob or someone else?
- What about security? privacy?

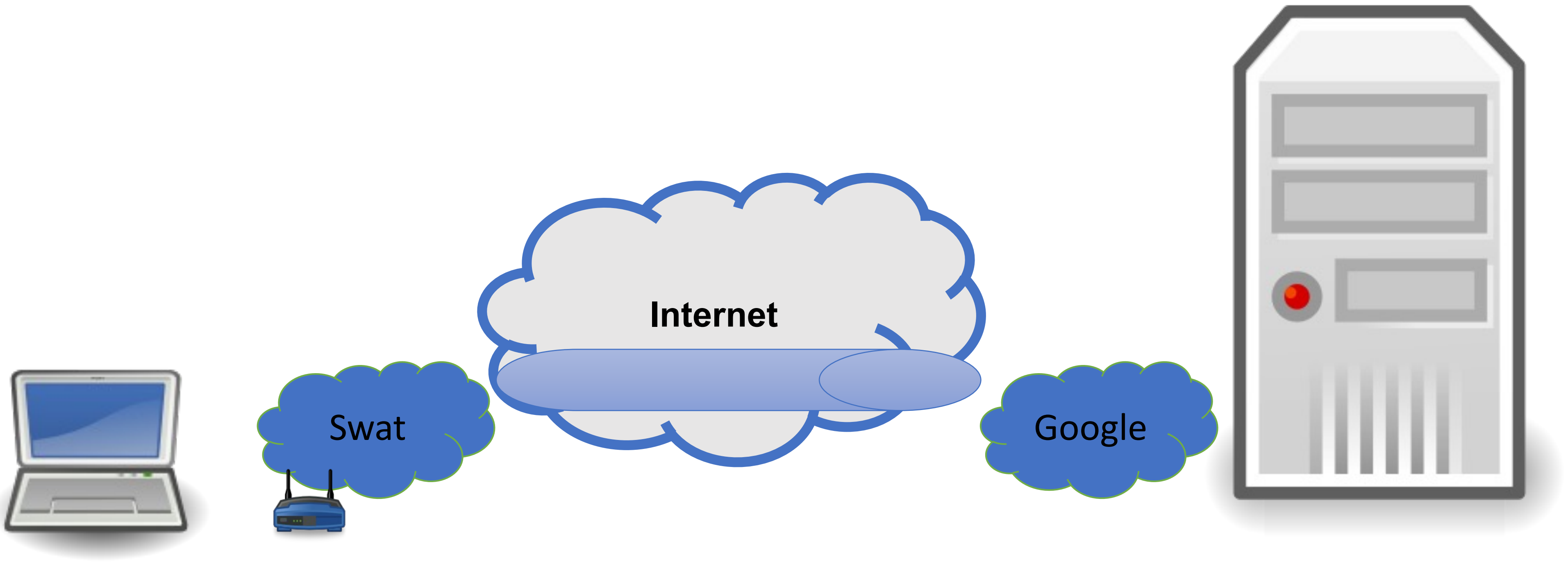
A “Simple” Task

<u>Send information from one computer to another</u>

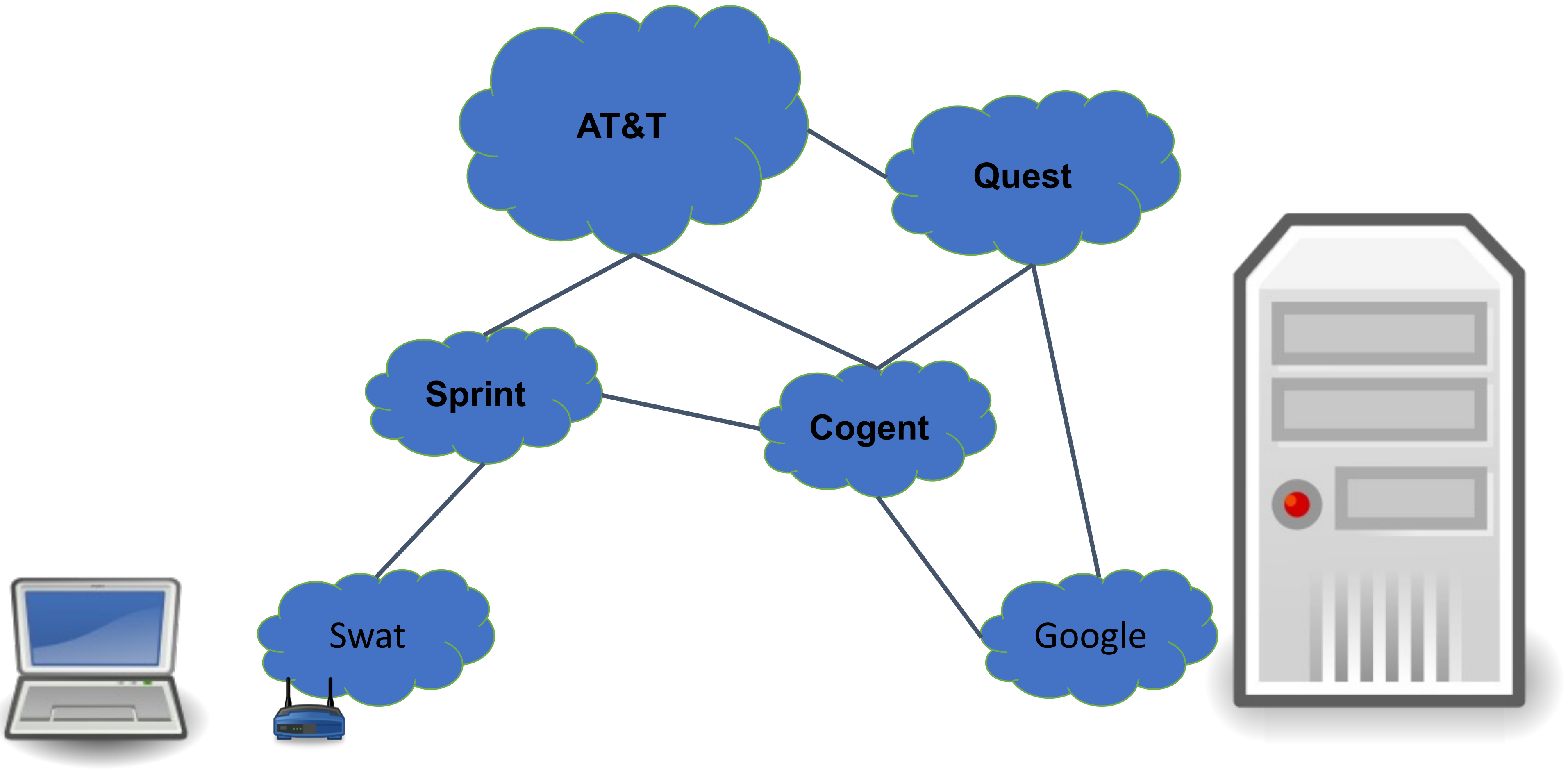
- hosts: endpoints of a network
- The plumbing is called a link.



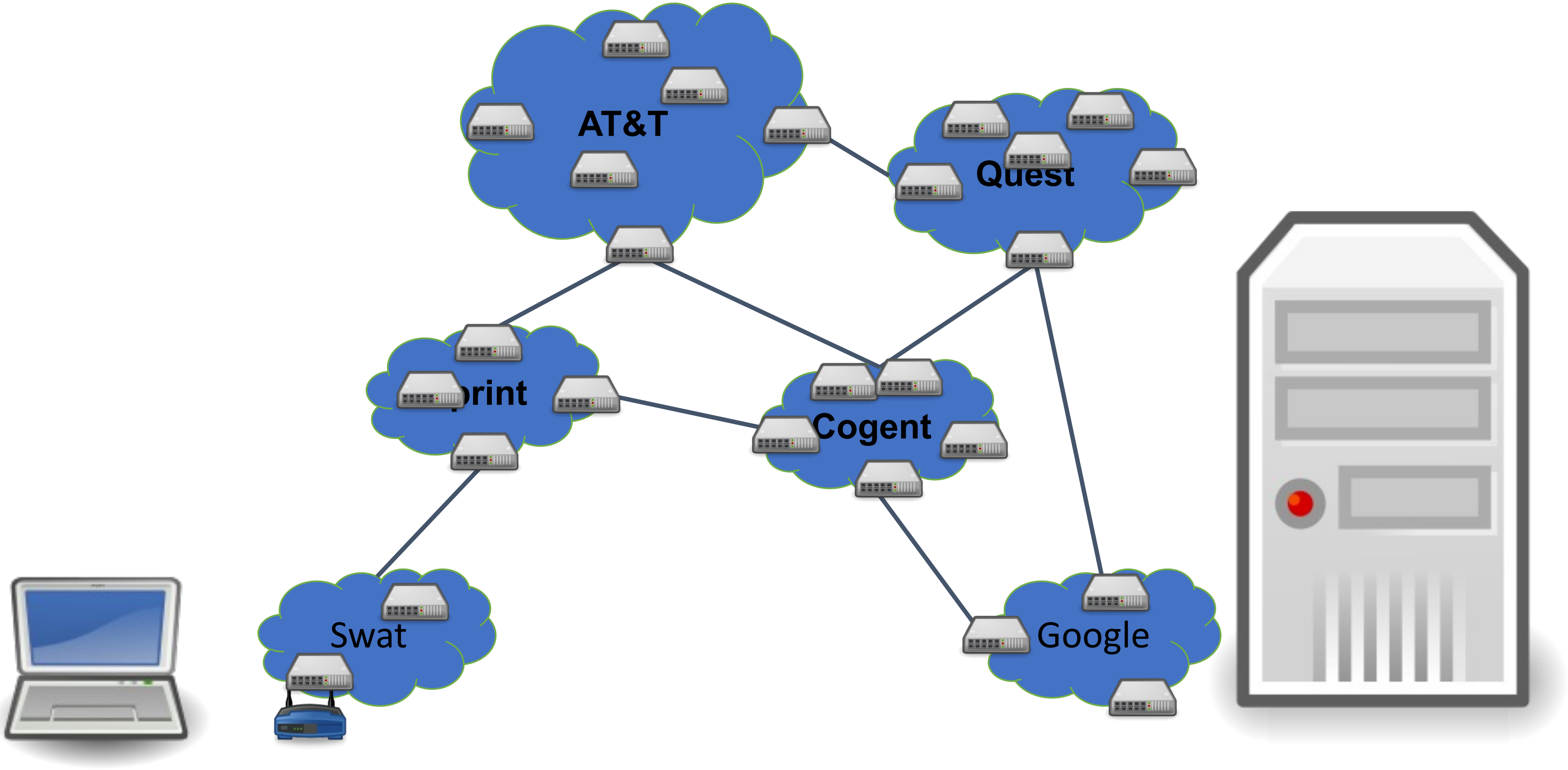
Not really so simple…



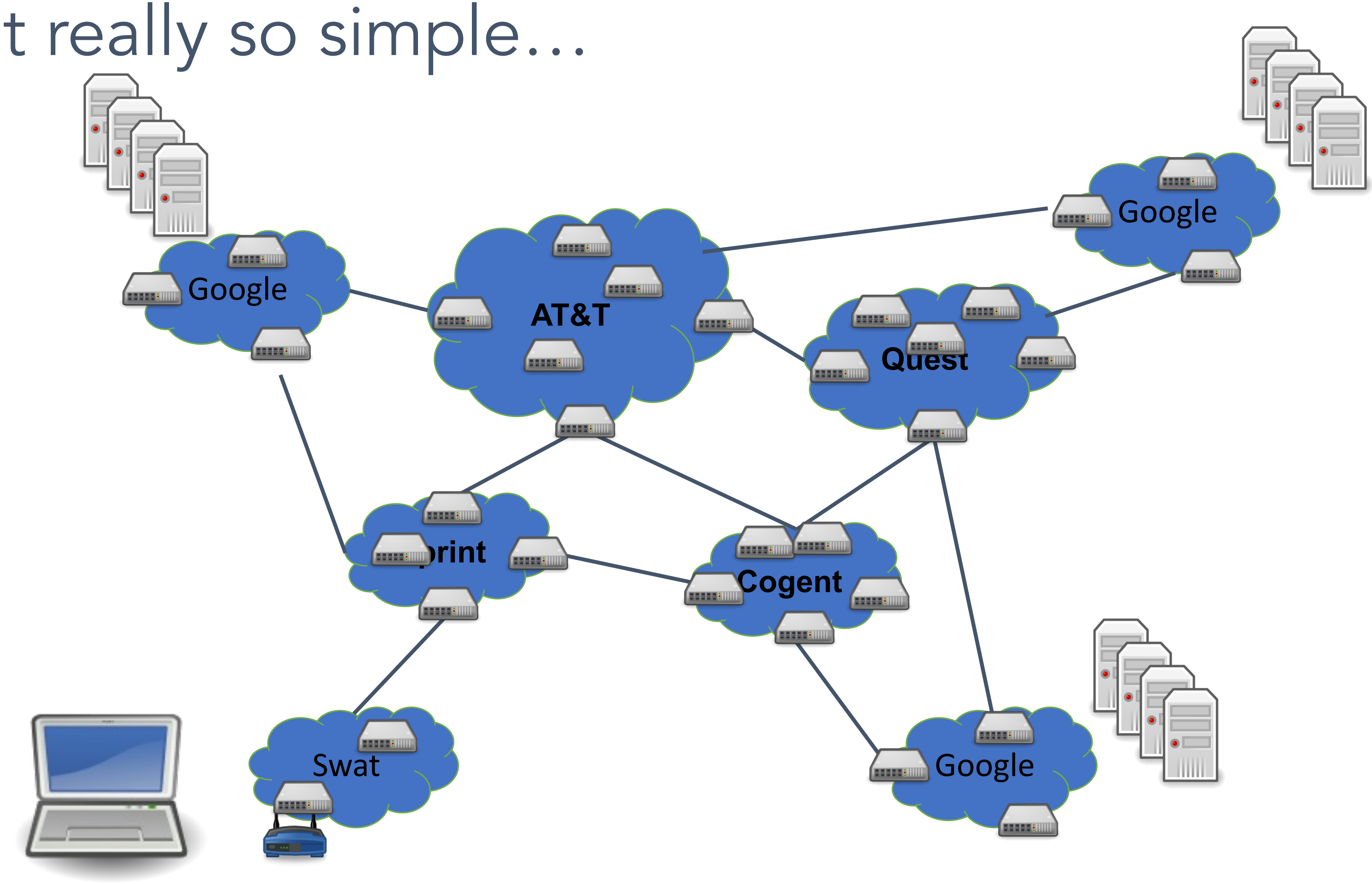
Not really so simple…



Not really so simple…



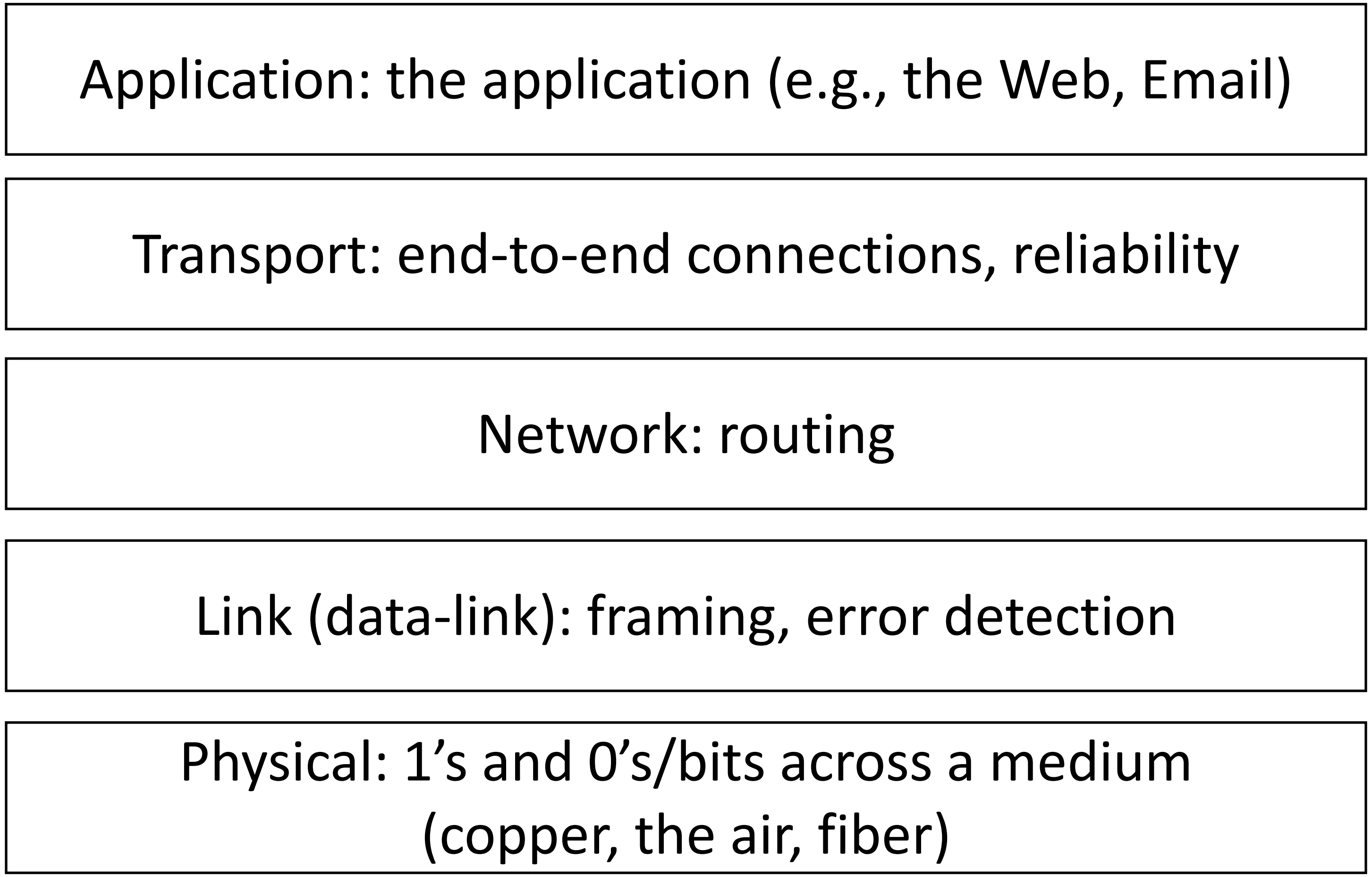
Not really so simple…



We only need…

- Manage complexity and scale up
- Naming and addressing
- Moving data to the destination
- Reliability and fault tolerance
- Resource allocation, Security, Privacy..

Five-Layer Internet Model



Application: the application (e.g., the Web, Email)

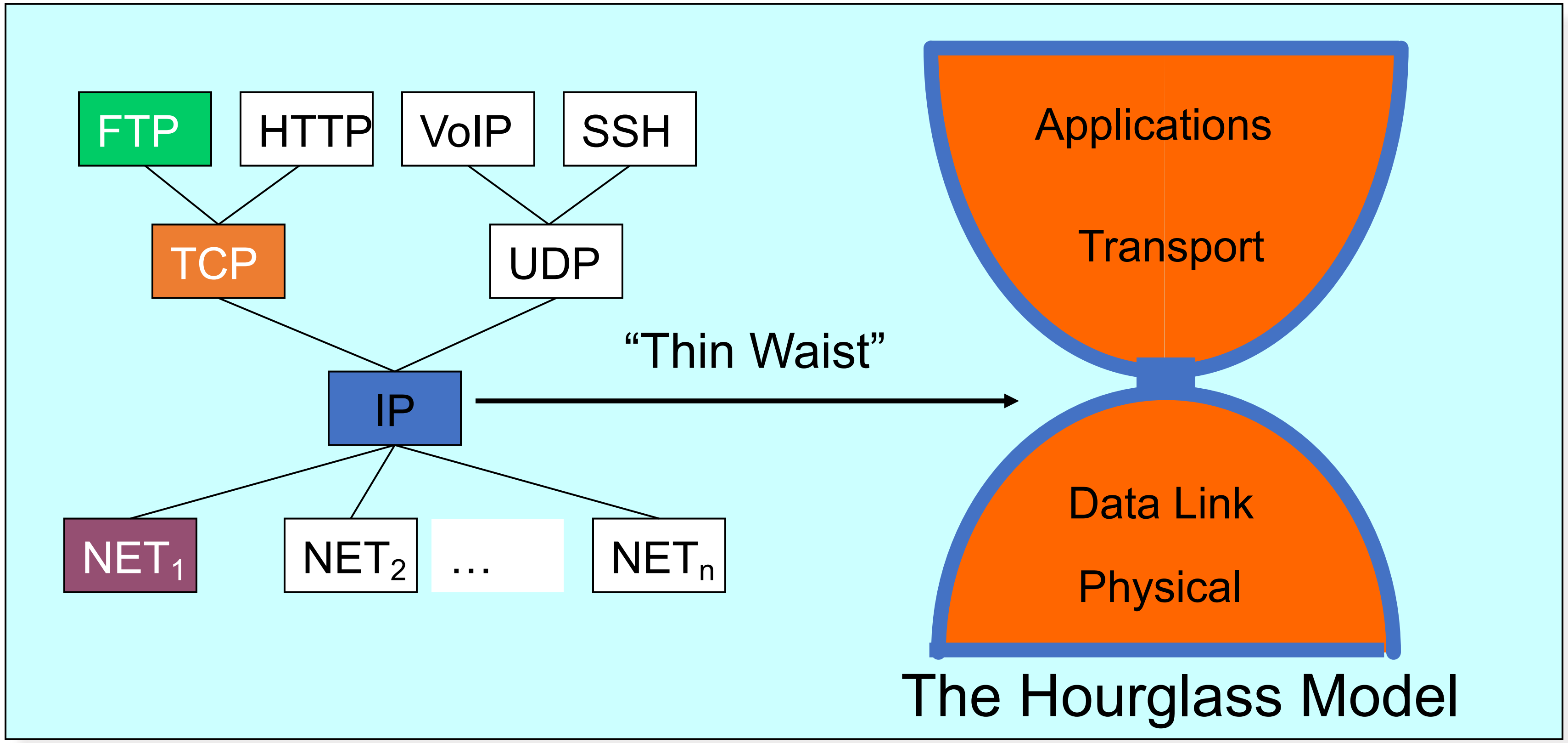
Transport: end-to-end connections, reliability

Network: routing

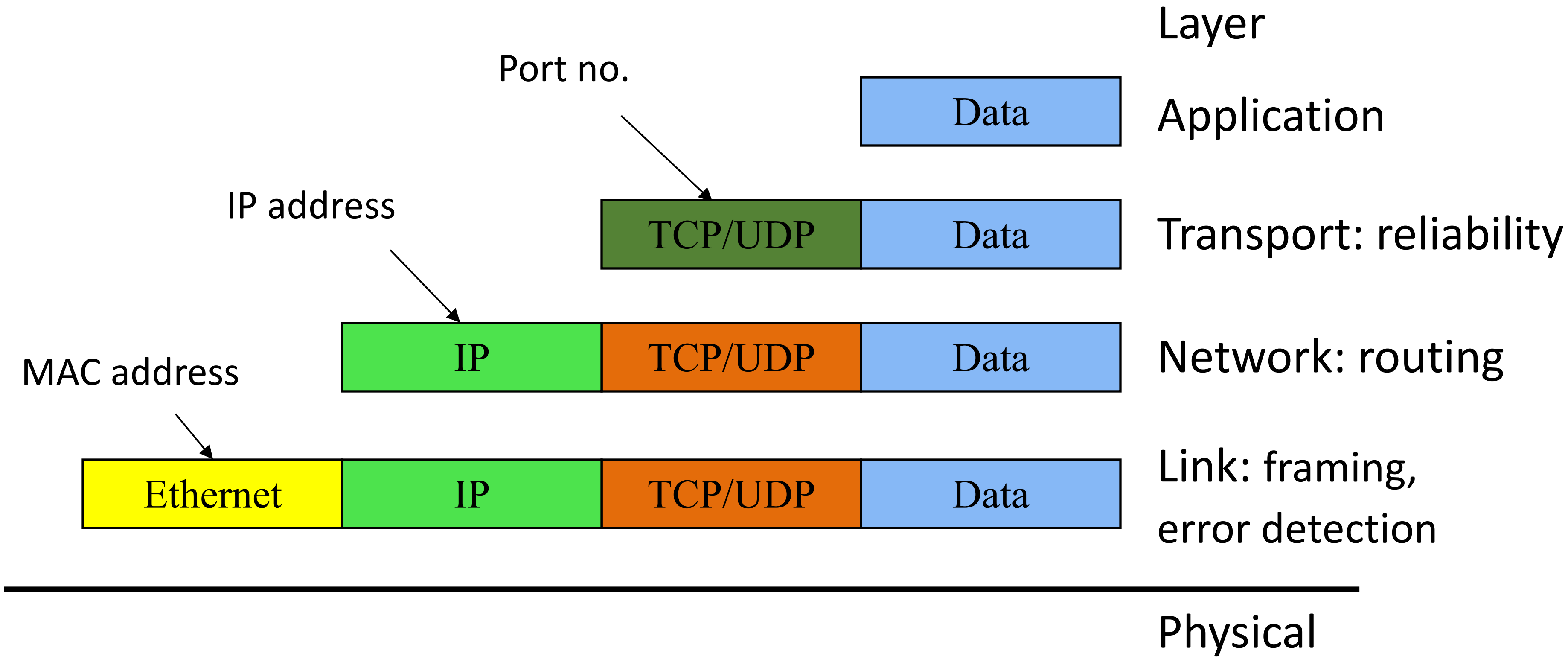
Link (data-link): framing, error detection

Physical: 1’s and 0’s/bits across a medium
(copper, the air, fiber)

Internet Protocol Suite



Layering and encapsulation



Layering: Separation of Functions

- Explicit structure allows identification, relationship of complex system’s pieces
  - layered reference model for discussion
  - reusable component design
- Modularization eases maintenance
  - change of implementation of layer’s service transparent to rest of system,
  - e.g., change in postal route doesn’t effect delivery of letters

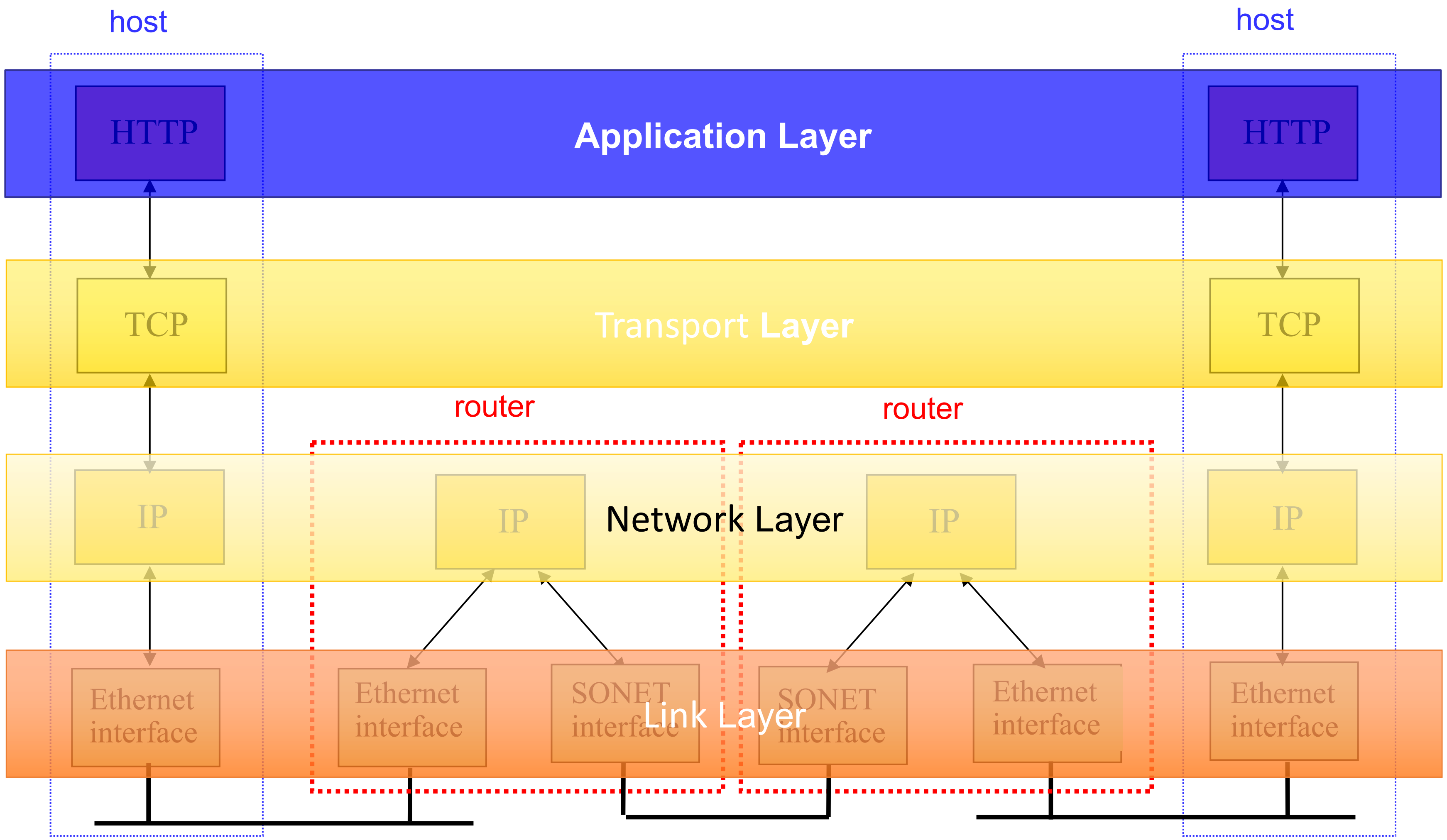
Abstraction!

- Hides the complex details of a process

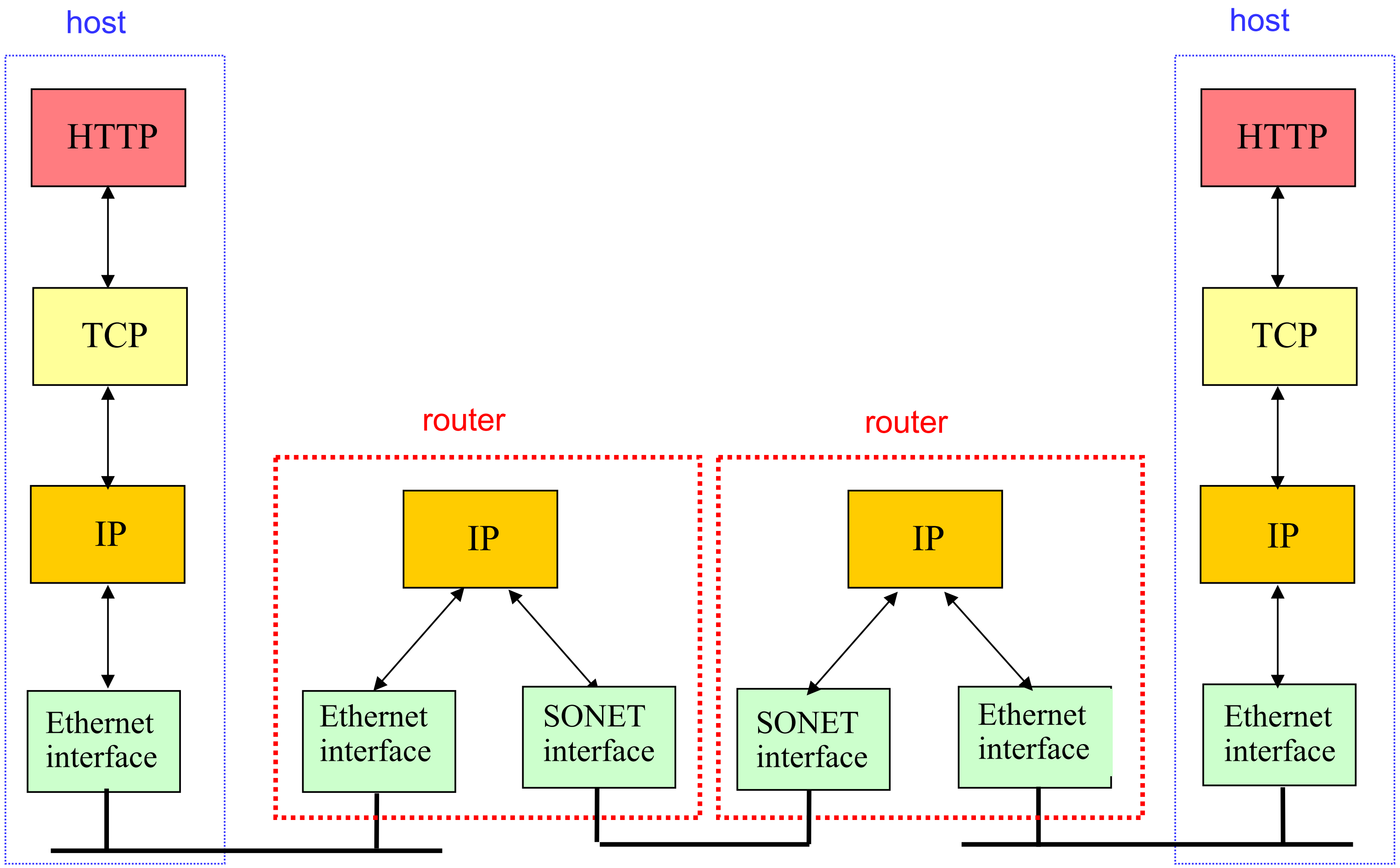
- Use abstract representation of relevant properties make reasoning simpler

- Ex: Alice and Bob’s knowledge of postal system:
  - Letters with addresses go in, come out other side

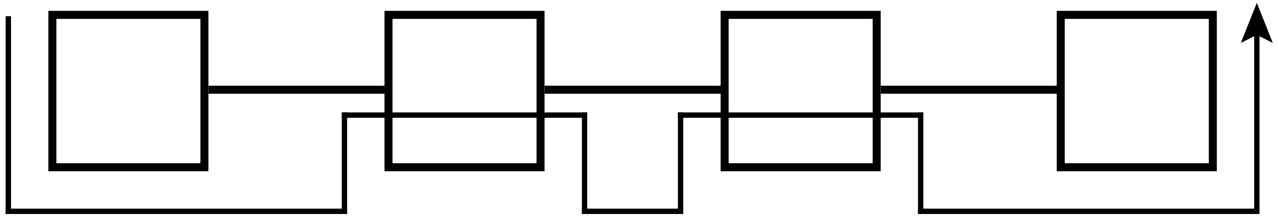
TCP/IP Protocol Stack



TCP/IP Protocol Stack



The "End-to-End" Argument



Don't provide a function at lower layer if you have to do it at higher layer anyway ...

... unless there is a very good performance reason to do so.

Examples: error control, quality of service

Reference: Saltzer, Reed, Clark, "End-To-End Arguments in System Design," ACM Transactions on Computer Systems, Vol. 2 (4), pp. 277-288, 1984.

The Internet

Global network of networks that ..

provides **best-effort** delivery of **packets** between connected hosts

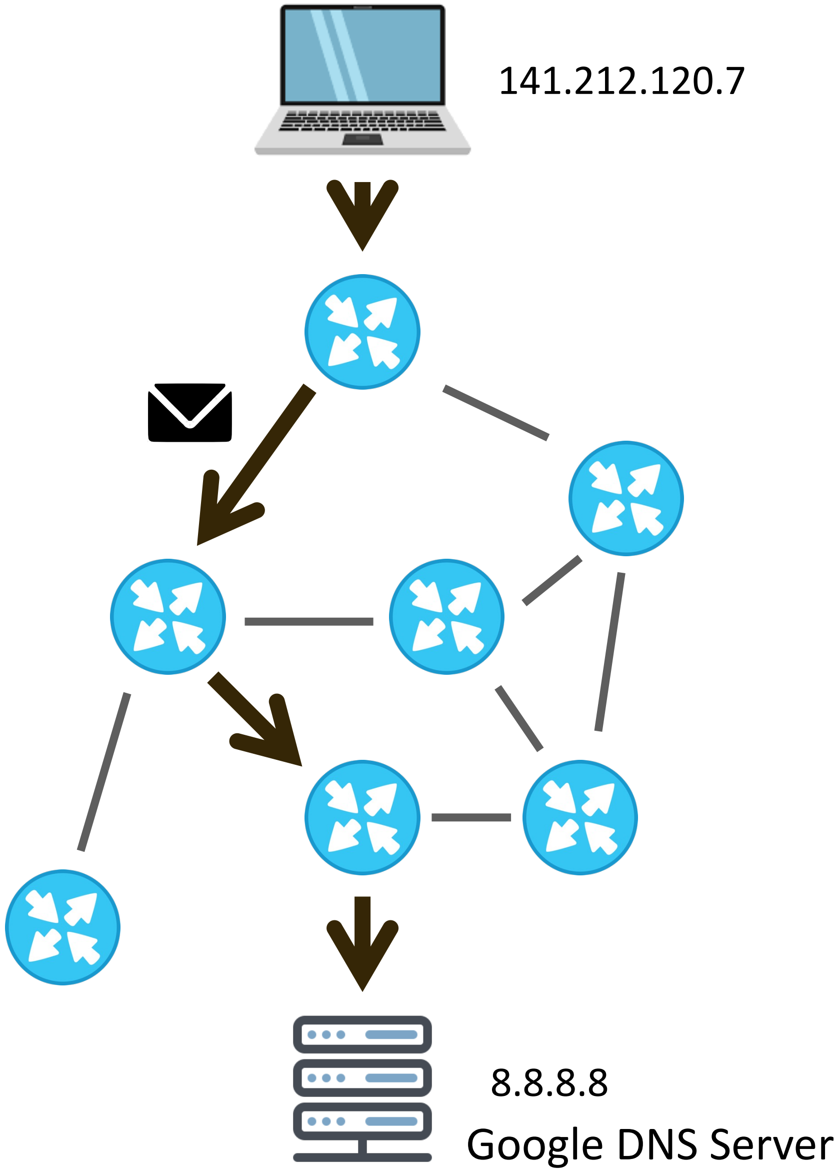
Packet: a structured sequence of bytes

Header: metadata used by network

Payload: user data to be transported

Every host has a unique identifier — IP address

Series of routers receive packets, look at destination address on the header and send it one hop towards the destination IP address

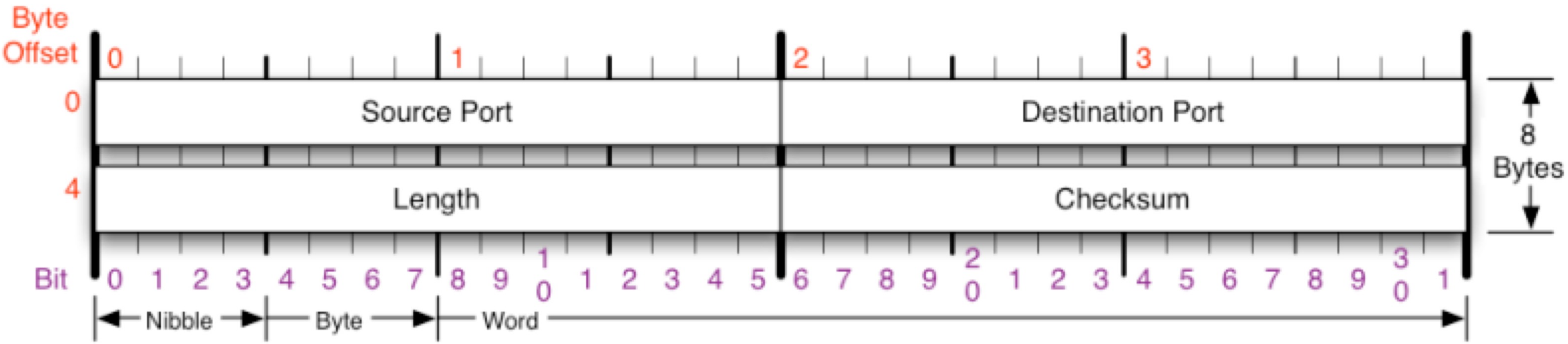


Network Protocols

We define how hosts communicate in published network protocols

Syntax: How communication is structured (e.g., format and order of messages)

Semantics: What communication means. Actions taken on transmit or receipt of message, or when a timer expires. What assumptions can be made.



Example: What bytes contain each field in a packet header

Threat modeling for network attacks

Basic security goals:

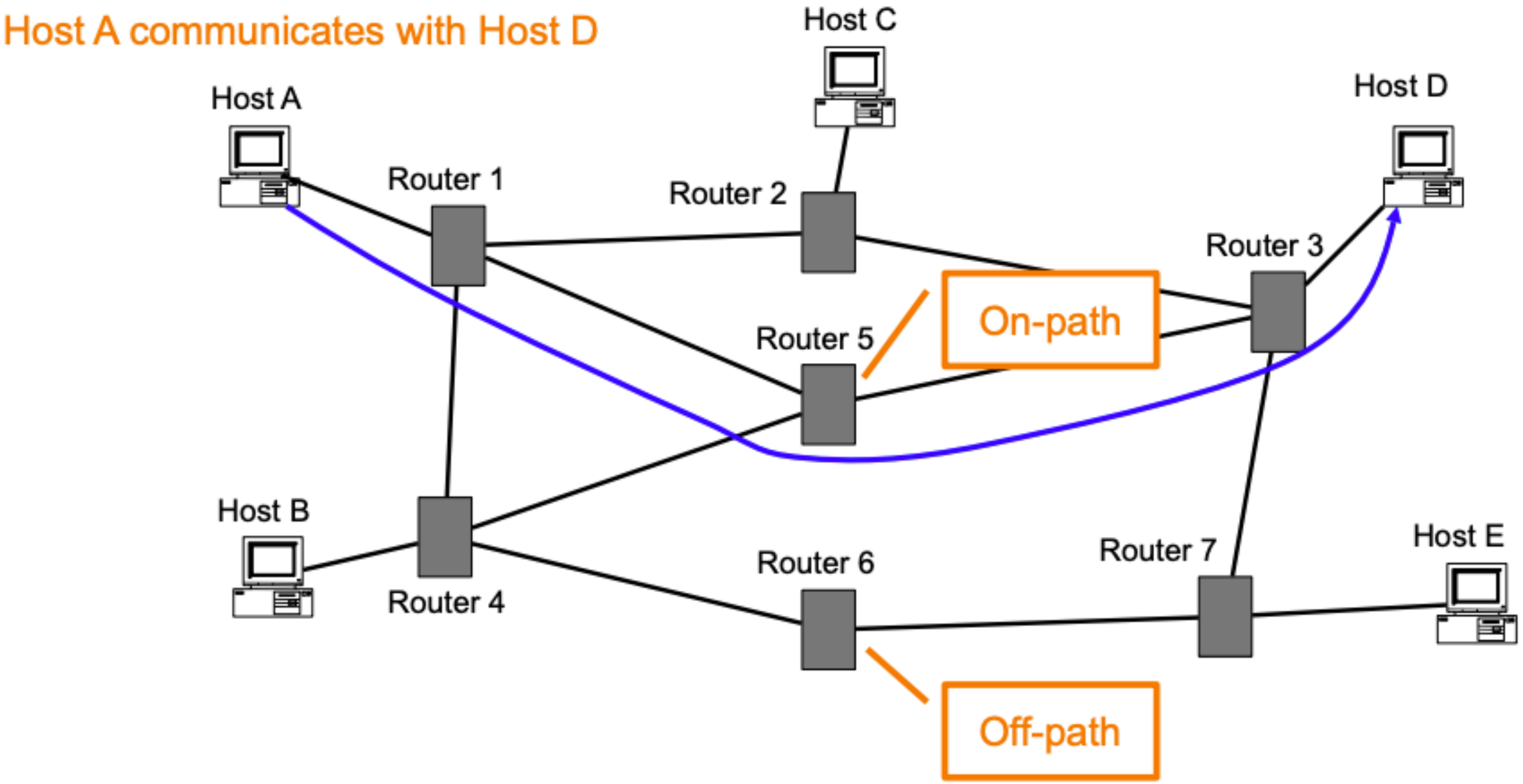
- **Confidentiality:** No one should be able to read our data/communications unless we want them to.
- **Integrity:** No one can manipulate our data/communications unless we want them to.
- **Availability:** We can access our data/communication capabilities when we want to.

Threat modeling for network attacks

- **Physical access:** Attacker has physical access to the network infrastructure.
- **In path/Meddler in the middle:** Attacker can see, add, and block packets.
- **Passive:** Attacker can see victim’s network traffic, but cannot add or modify packets.
- **Off path:** Attacker cannot see network traffic of the victim.

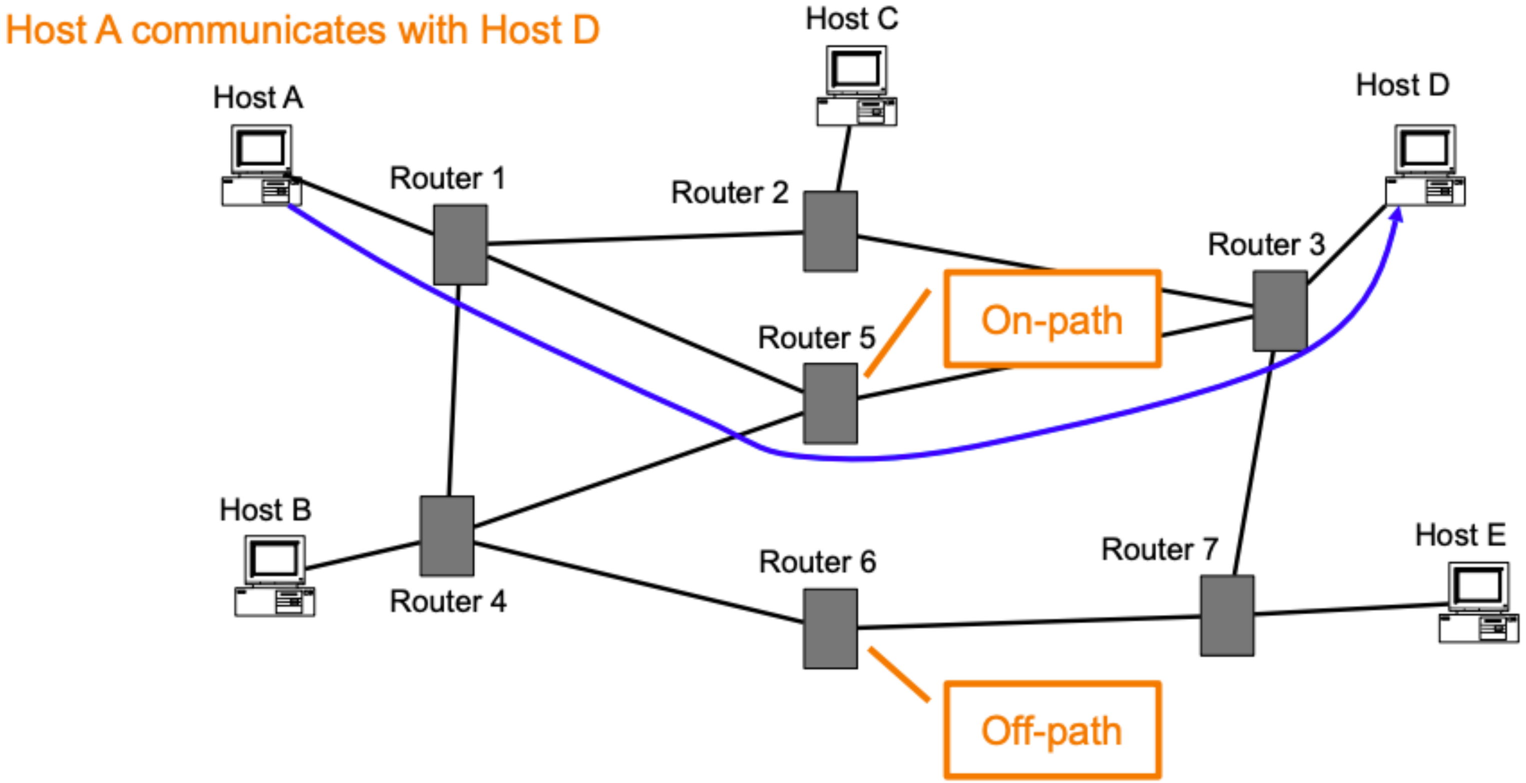
Network Attacks: Classes of Attackers

- MiTM: Can see packets, and can modify and drop packets
- On-path: Can see packets, but can’t modify or drop packets
- Off-path: Can’t see, modify, or drop packets



Network Attacks: Classes of Attackers

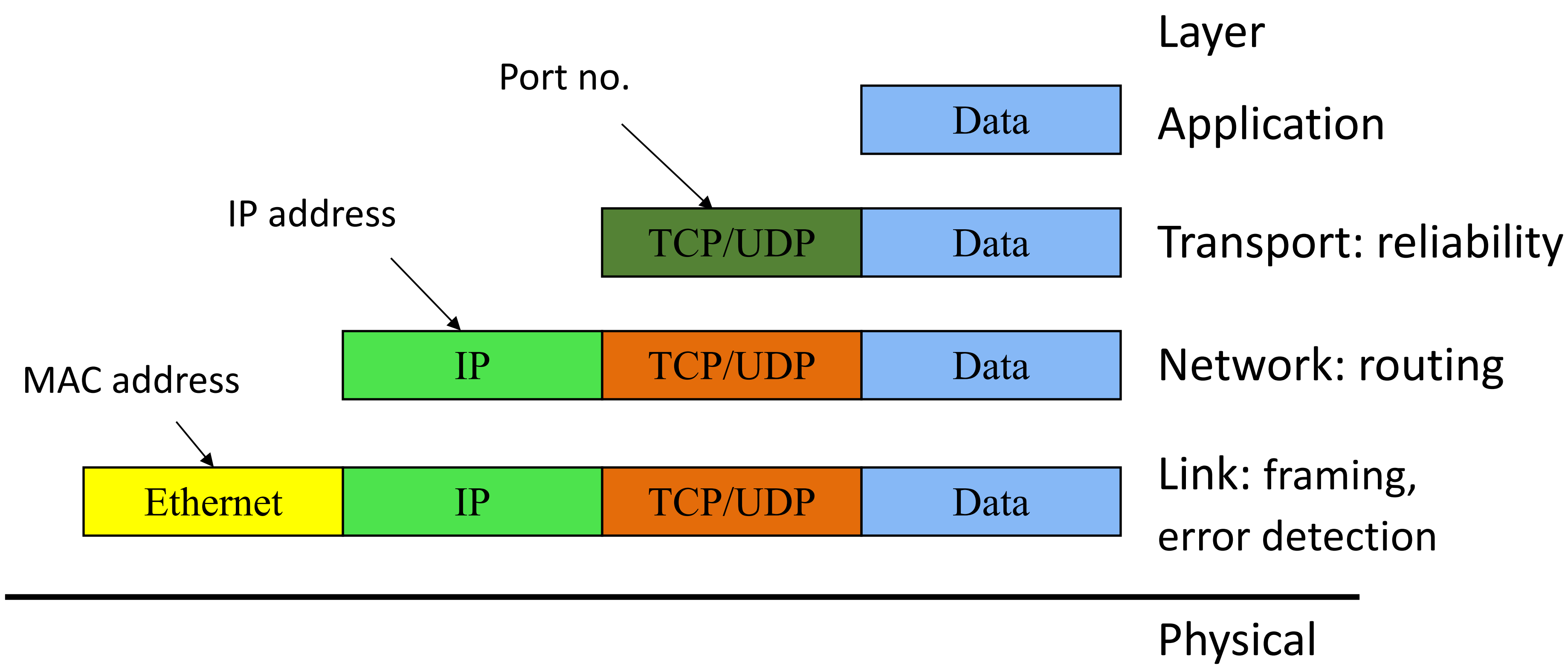
- MiTM: Can see packets, and can modify and drop packets
- On-path: Can see packets, but can’t modify or drop packets
- Off-path: Can’t see, modify, or drop packets



Which type of attacker is more powerful?

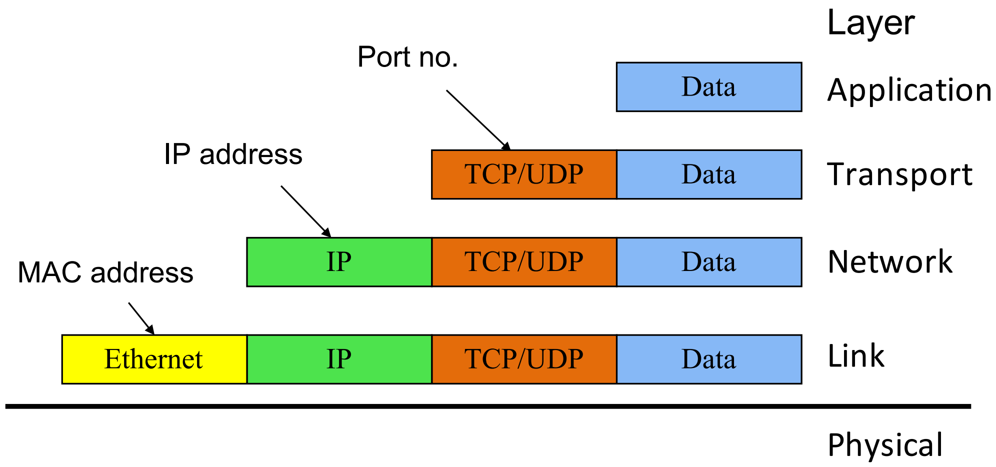
A. on-path
B. off-path
C. neither is strictly stronger than the other

Layering and encapsulation



Application Layer
(HTTP, FTP, SMTP, Skype)

- Does whatever an application does!



Layer

Port no.

Data — Application

IP address

TCP/UDP | Data — Transport

MAC address

IP | TCP/UDP | Data — Network

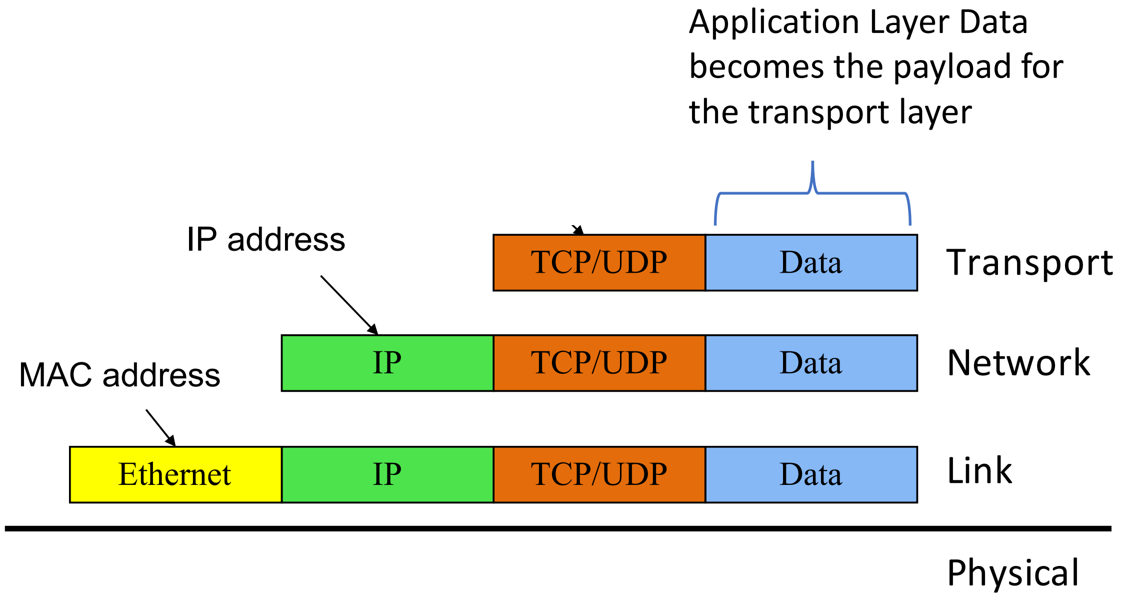
Ethernet | IP | TCP/UDP | Data — Link

Physical

Transport Layer (TCP, UDP)

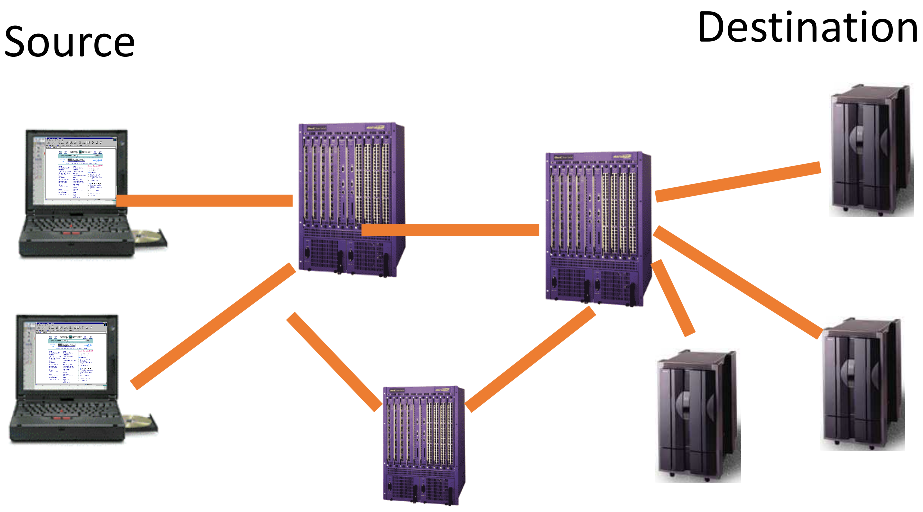
- Provides
  - Ordering
  - Error checking
  - Delivery guarantee
  - Congestion control
  - Flow control

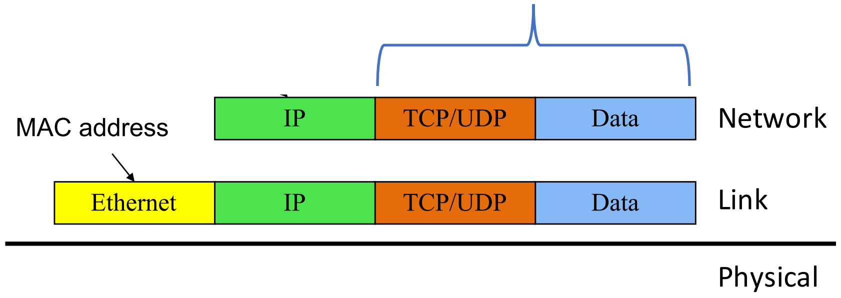
- Or doesn't!



Network Layer (IP)

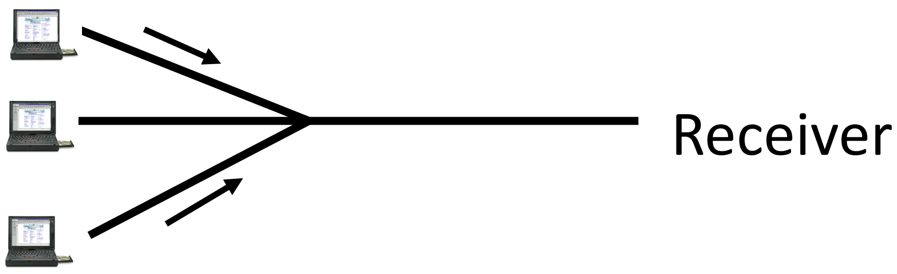
- **Routers**: choose paths through network




Transcript layer data + header becomes payload for the network layer

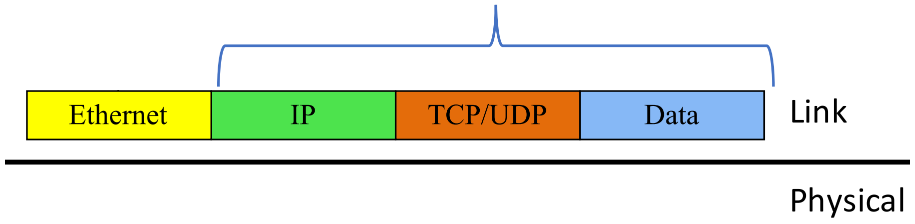
Link Layer (Ethernet, WiFi, Cable)

- Who’s turn is it to send right now?
- Break message into frames
- Media access: can it send the frame now?

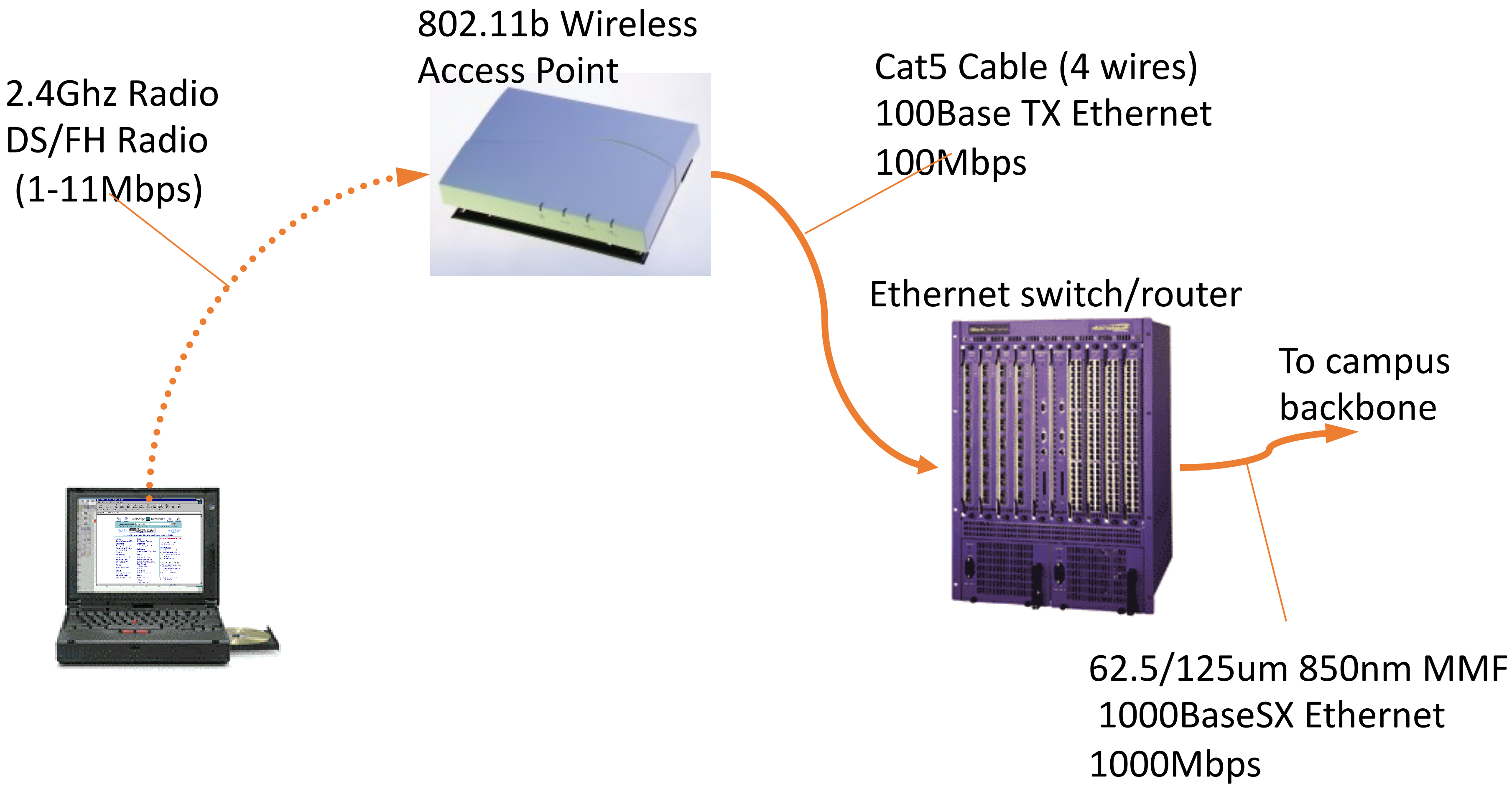


- Send frame, handle “collisions”

Network layer data + header becomes payload for the link layer



Physical layer – move actual bits!
(Cat 5, Coax, Air, Fiber Optics)



2.4Ghz Radio
DS/FH Radio
(1-11Mbps)

802.11b Wireless
Access Point

Cat5 Cable (4 wires)
100Base TX Ethernet
100Mbps

Ethernet switch/router

To campus
backbone

62.5/125um 850nm MMF
1000BaseSX Ethernet
1000Mbps