

I. Introduction: roadmap

I.1 what *is* the Internet?

I.2 network edge

- end systems, access networks, links

I.3 network core


- packet switching, circuit switching, network structure

I.4 delay, loss, throughput in networks

I.5 protocol layers, service models

I.6 networks under attack: security

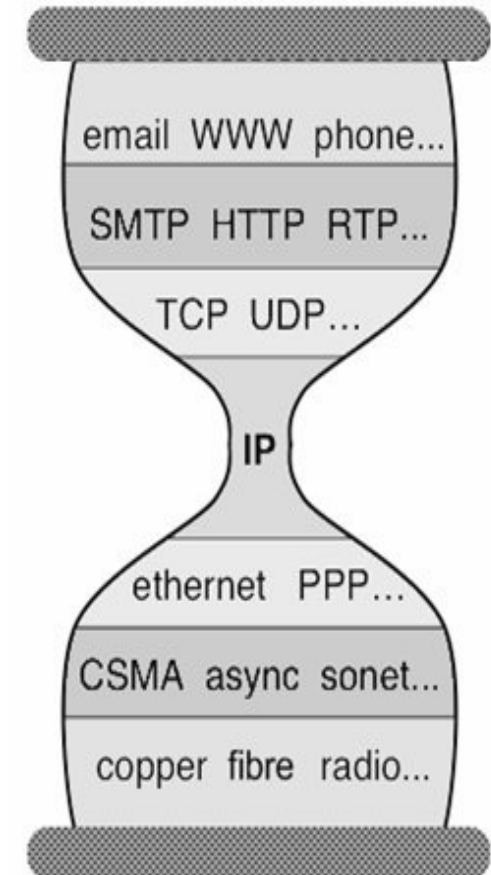
I.7 history



Self study

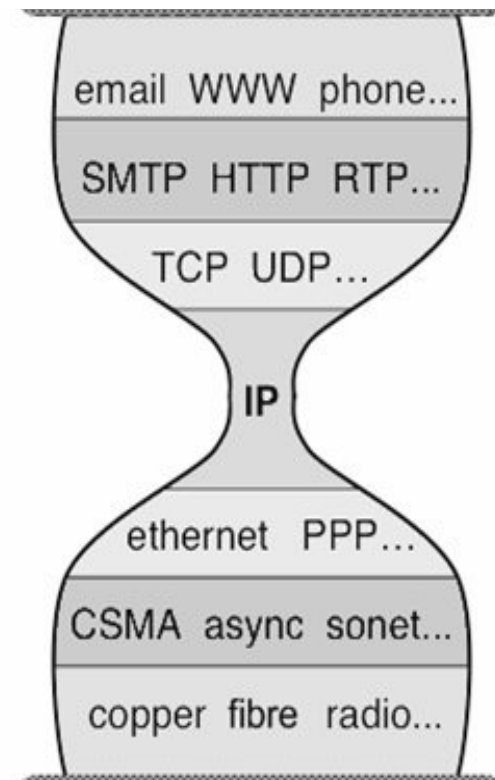
Internet protocol stack

- ❖ *application*: supporting network applications
 - FTP, SMTP, HTTP, Skype, ..
- ❖ *transport*: process-process data transfer
 - TCP, UDP
- ❖ *network*: routing of datagrams from source to destination
 - IP, routing protocols
- ❖ *link*: data transfer between neighboring network elements
 - Ethernet, 802.11 (WiFi), PPP
- ❖ *physical*: bits “on the wire”

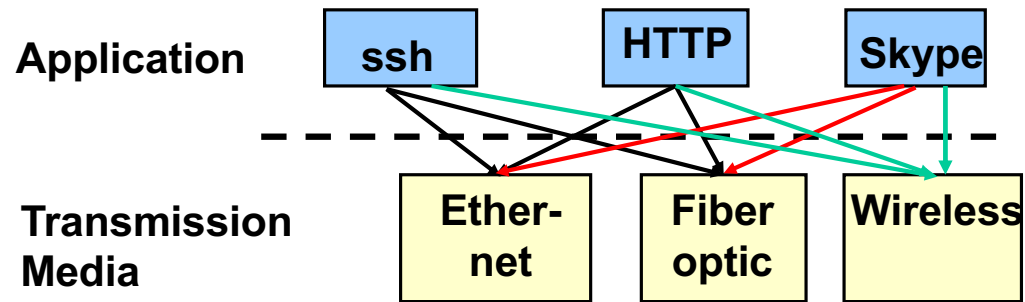


Three Observations

- ❖ Each layer:
 - Depends on layer below
 - Supports layer above
 - Independent of others
- ❖ Multiple versions in layer
 - Interfaces differ somewhat
 - Components pick which lower-level protocol to use
- ❖ But only one IP layer
 - Unifying protocol



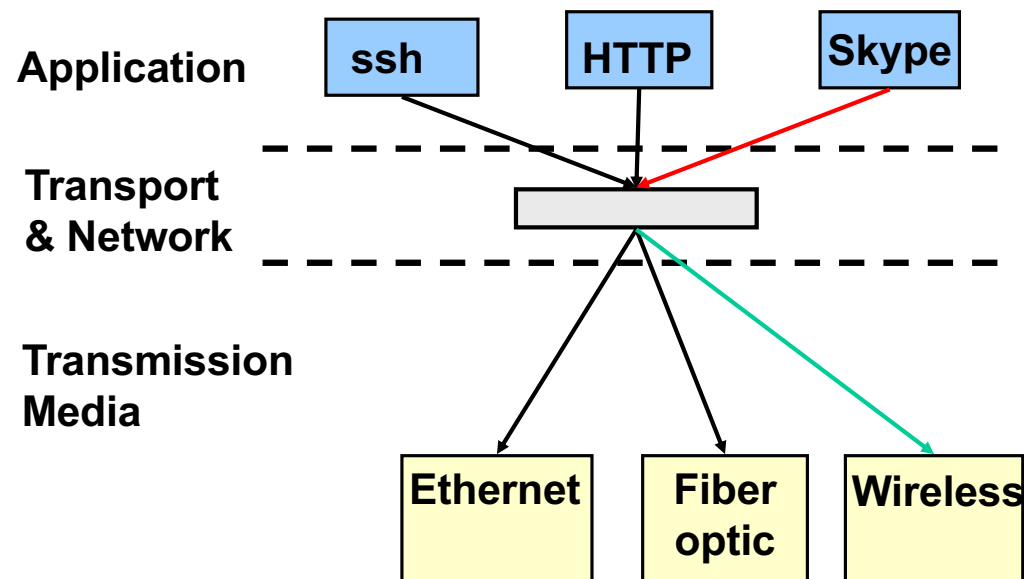
An Example: No Layering



- ❖ No layering: each new application has to be **re-**implemented for every network technology !

An Example: Benefit of Layering

- ❖ Introducing an intermediate layer provides a **common** abstraction for various network technologies



Is Layering Harmful?

- ❖ Layer N may duplicate lower-level functionality
 - E.g., error recovery to retransmit lost data
- ❖ Information hiding may hurt performance
 - E.g., packet loss due to corruption vs. congestion
- ❖ Headers start to get large
 - E.g., typically, TCP + IP + Ethernet headers add up to 54 bytes
- ❖ Layer violations when the gains too great to resist
 - E.g., Network Address Translation (NAT – to be covered in Network Layer)
- ❖ Layer violations when network doesn't trust ends
 - E.g., Firewalls (Security)

Distributing Layers Across Network

- ❖ Layers are simple if only on a single machine
 - Just stack of modules interacting with those above/below
- ❖ But we need to implement layers across machines
 - Hosts
 - Routers
 - Switches
- ❖ What gets implemented where?

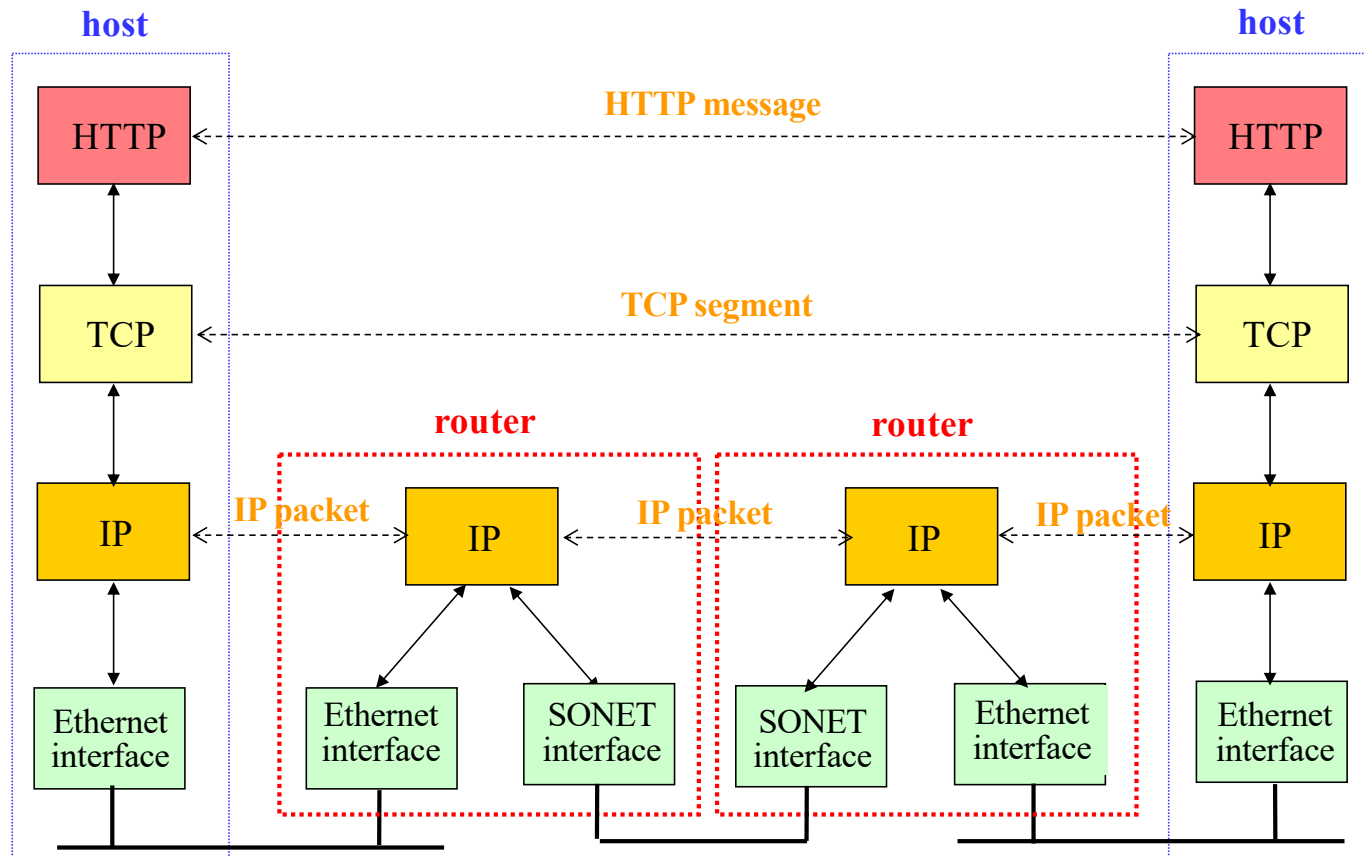
What Gets Implemented on Host?

- ❖ Hosts have applications that generate data/messages that are eventually put out on wire
- ❖ At receiver host bits arrive on wire, must make it up to application
- ❖ Therefore, all layers must exist at host!

What Gets Implemented on Router?

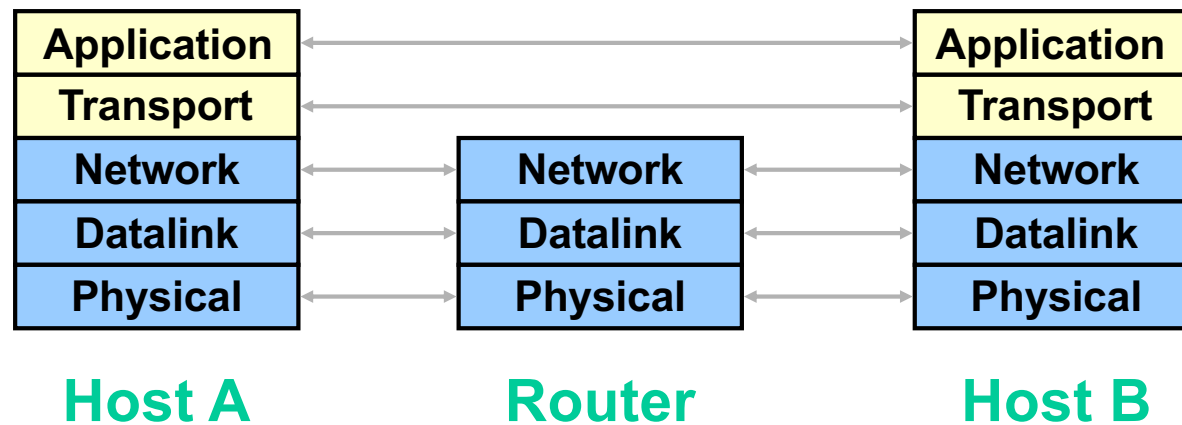
- ❖ Bits arrive on wire
 - Physical layer necessary
- ❖ Packets must be delivered to next-hop
 - datalink layer necessary
- ❖ Routers participate in global delivery
 - Network layer necessary
- ❖ Routers don't support reliable delivery
 - Transport layer (and above) **not** supported

Internet Layered Architecture



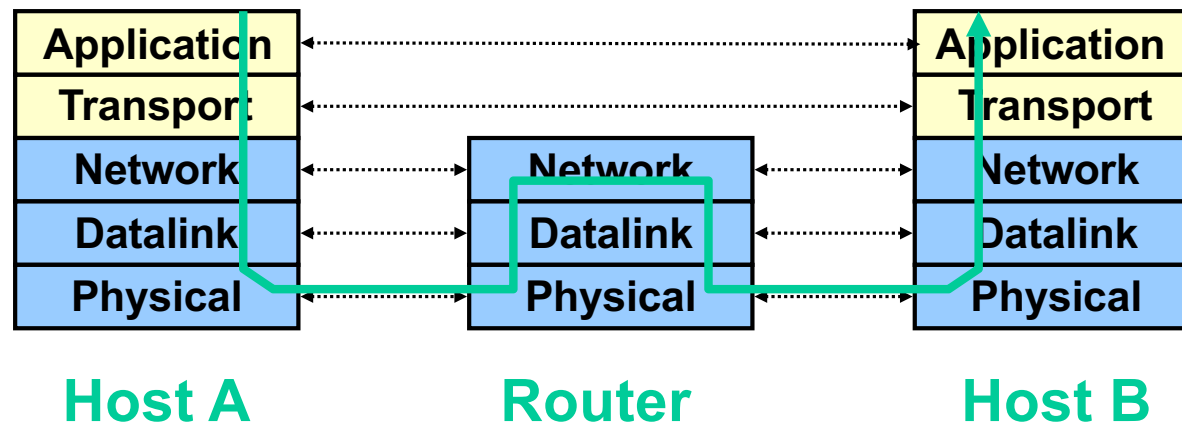
Logical Communication

- ❖ Layers interacts with peer's corresponding layer

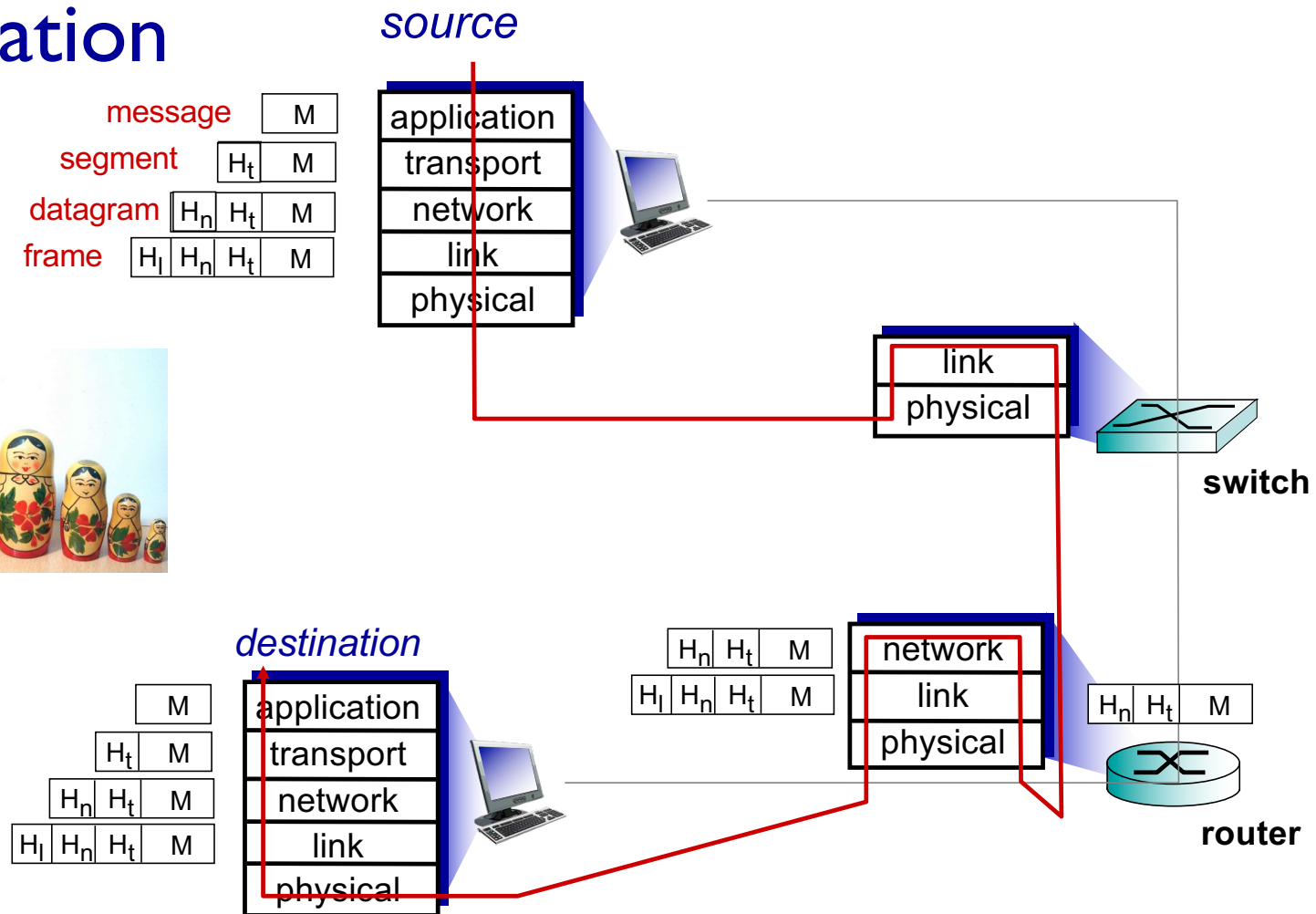
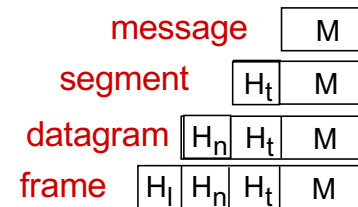


Physical Communication

- ❖ Communication goes down to physical network
- ❖ Then from network peer to peer
- ❖ Then up to relevant layer



Encapsulation



Quiz: Layering



What are two benefits of using a layered network model ? (Choose two)

- A. It makes it easy to introduce new protocols
- B. It speeds up packet delivery
- C. It allows us to have many different packet headers
- D. It prevents technology in one layer from affecting other layers
- E. It creates many acronyms

I. Introduction: roadmap

I.1 *what is the Internet?*

I.2 network edge

- end systems, access networks, links

I.3 network core


- packet switching, circuit switching, network structure

I.4 delay, loss, throughput in networks

I.5 protocol layers, service models

I.6 networks under attack: security

I.7 history



Self study

We have now completed Chapter 1 from the textbook