CS 250: Foundations of Computer Systems [Networking]

Layering Complexity

Layers at the top
Depend on the ones below

The higher you are
The more you leverage the ones below

Transport	for ports
IP	for addresses and routing
Link	for local communications

Guest Lecture:
Shrideep Pallickara
Computer Science
Colorado State University

1

Frequently asked questions from the previous class survey

- Layering and encapsulation …
- Why are packets dropped?

2

Topics covered in this lecture

- Networking Stack

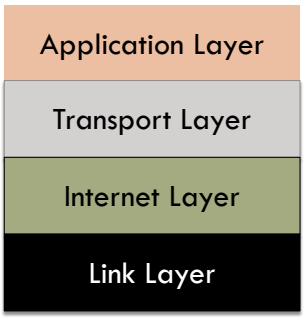
Run, rabbit, run
Dig that hole, forget the sun
And when at last the work is done
Don't sit down, it's time to dig another one
Breathe; Waters, Gilmour, Wright; Pink Floyd

THE INTERNET PROTOCOL SUITE

The internet protocol suite is designed around a four-layer model

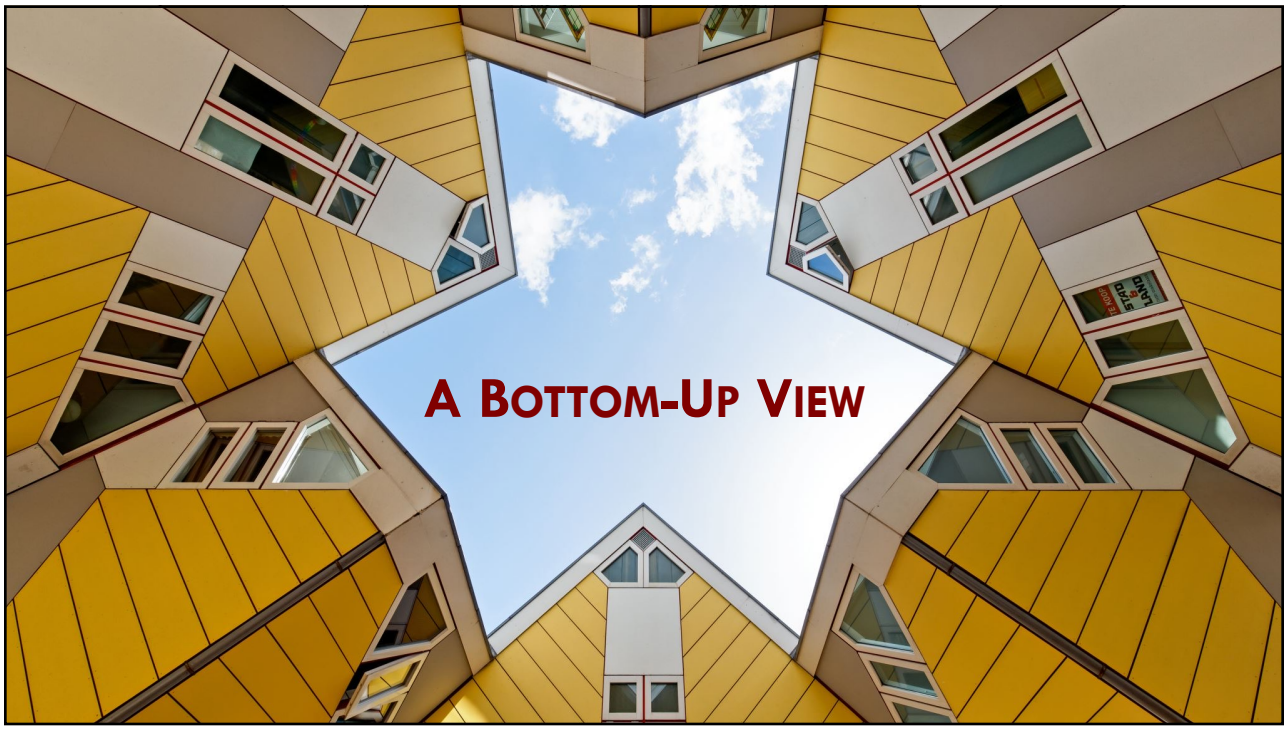
- This is sometimes called the **TCP/IP model**
- The four layers of the protocol suite:
  - The link layer
  - The internet layer
  - The transport layer
  - The application layer

The Internet Layered Protocol Stack



Not every device is interested in using all 4 layers

- Network hosts (such as a client or server) make use of protocols from all four layers
- Other types of networking hardware (such as switches and routers) only use protocols associated with lower layers
  - Such devices can perform their jobs without bothering to examine the higher layer protocol data contained in a network transmission



Link Layer [1/2]

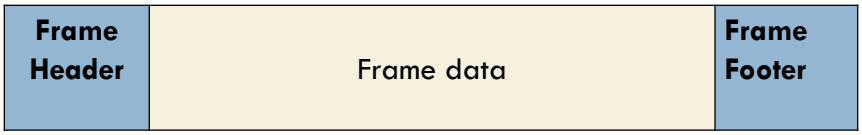
- The lowest level of the internet protocol suite is the link layer
- The physical and logical connections between hosts are known as network links
- Link layer protocols are used by **devices on the same network** to communicate with each other

Link Layer [2/2]

- Each device on a link has a network **address that uniquely identifies** it
- For many link layer protocols, this address is known as a **media access control address (MAC address)**
  - 6-byte identifier burned into every NIC [allows 2^{48} different devices]
- Link layer data is divided into small units known as **frames**
- Each frame includes
  - A **header** describing the frame
  - A **payload** of data, and finally
  - A frame **footer** used to detect errors

Link layer frame

- **All devices** connected to the internet participate in the link layer
- This is required, since it's the link layer that provides connectivity (either wired or wireless) to a local network



The Link Layer and MAC Addresses

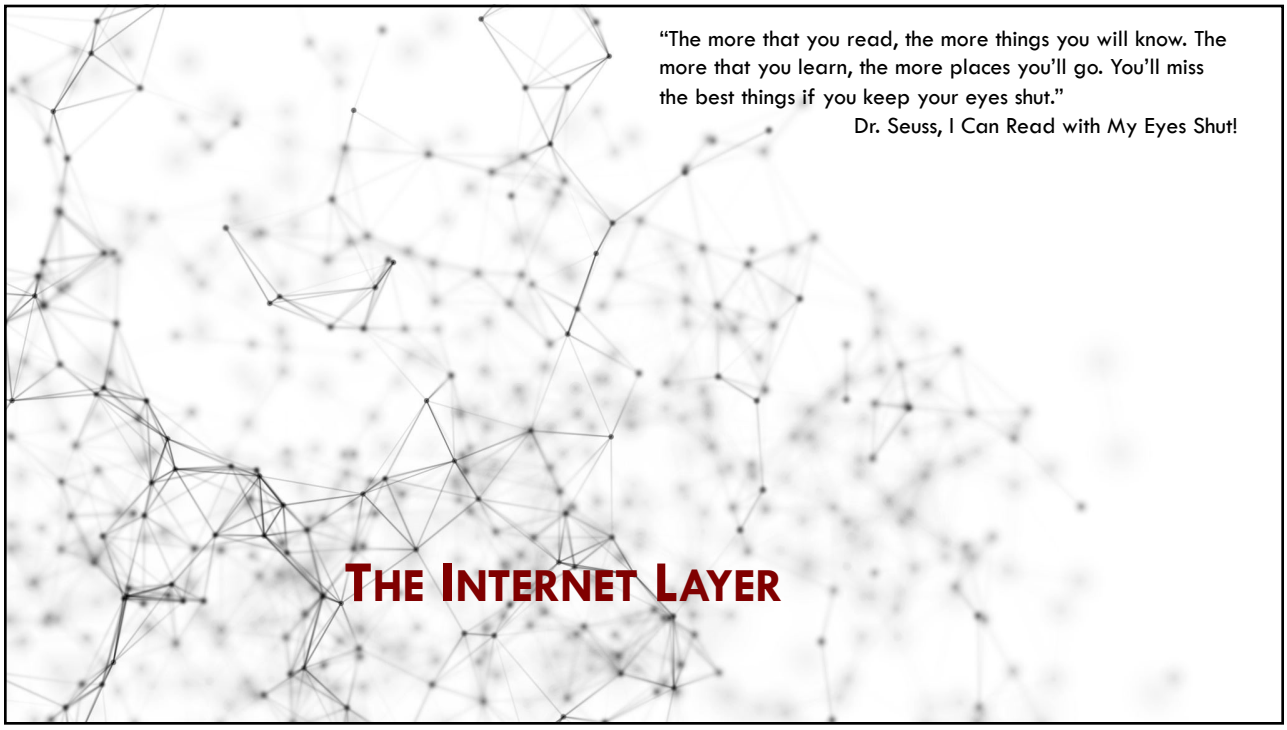
- The frame header contains source and destination MAC addresses
- MAC addresses are **only useable on a local network**
  - A computer on a remote network cannot directly send data to a MAC address on your local network
- The header also includes a descriptor of the type of data carried in the frame data section

MAC Addresses

- If your home has a Wi-Fi network, Wi-Fi is the link between the hosts on your network
  - Wi-Fi protocol, defined by the IEEE 802.11 specifications, doesn't know or care what type of data is being sent over the wireless network
- Another notable link layer technology is Ethernet, used for **wired** physical connections
  - Ethernet is defined by the IEEE 802.3 standards
  - Ethernet typically uses a cable with pairs of copper wires inside that ends in a connector commonly known as **RJ45**

Payload size within the Link Layer frame

- Ethernet
  - 1500 bytes
- WiFi
  - 2304 bytes
- FDDI
  - 4352 bytes



15

Internet Layer

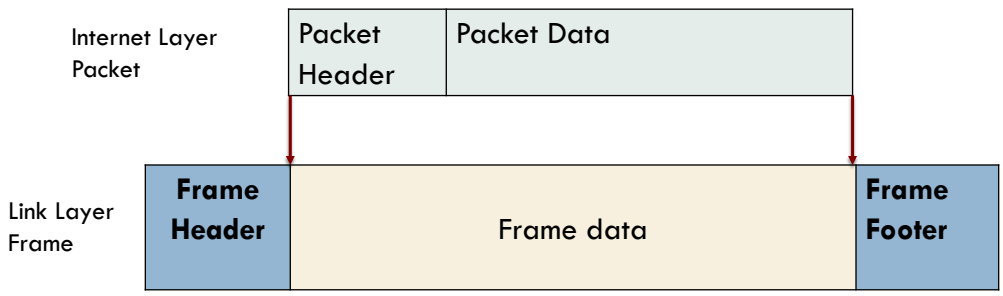
- The internet layer allows data to **travel beyond the local network**
- The primary protocol used in this layer is the **Internet Protocol (IP)**
  - Enables **routing**: the process of determining a path for data that's transmitted between networks

16

IP Addresses

- Every host on the internet is assigned an **IP address**
  - A number that *uniquely identifies* the host on the global internet
- IP addresses are usually assigned by a server on the local network
  - A device's IP address typically changes when it connects to a new network

Data sent over the internet layer is called a **packet**, which is enclosed in a link layer frame



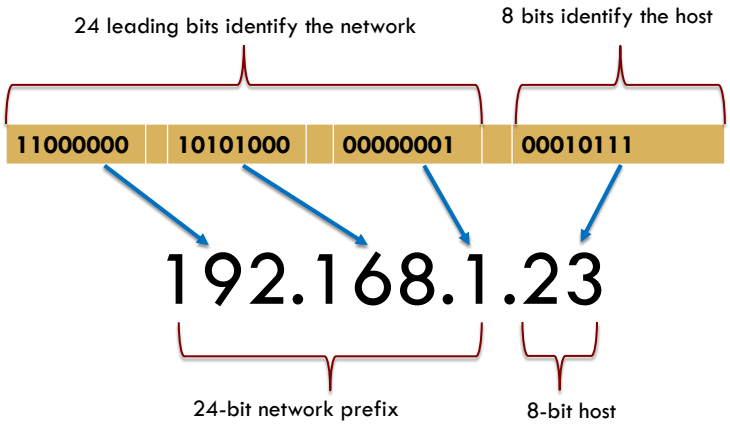
Addresses and subnets [1/3]

- Computers connected to the same local network
  - Have IP addresses that begin with the same leading bits
  - Said to be on the same **subnet**
- Computers on the same subnet can communicate directly
  - Where?
    - At the link layer
    - Because they are operating on the same physical network

Addresses and subnets [2/3]

- Computers that are on *different subnets* must send their traffic through a **router**
  - A device that connects subnets and operates at the internet layer
- Subnetting divides the IP address into two parts:
  - the **network prefix**, which all devices on the same subnet share
    - The number of bits included in the network prefix varies based on the network configuration
  - the **host identifier**, which is unique to a host on that subnet

Addresses and subnets [3/3]



Two versions of Internet Protocol are in use on the internet today

- Internet Protocol Version 4 (**IPv4**) is the dominant version in use
  - The other active version is Internet Protocol Version 6 (**IPv6**)
- What happened to IPv5?
  - No such protocol ever existed
  - But an experimental protocol called Internet Stream Protocol identified its IP version as 5
  - So IPv5 was skipped when the successor to IPv4 was developed

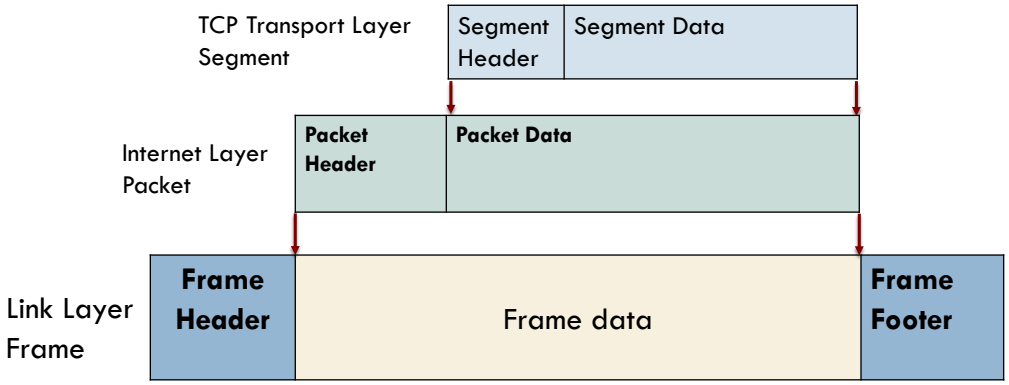
Transport Layer

- The transport layer provides a communications channel that applications may use to send and receive data
- There are two commonly used transport layer protocols:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)

Transport Layer: TCP and UDP

- TCP provides a **reliable connection** between two hosts
  - Ensures that errors are minimized, data arrives in order, lost data is resent, and so forth
  - Data sent with TCP is known as a **segment**
- UDP is a "*best effort*" protocol, meaning its delivery is **unreliable**
  - UDP is preferred when speed is valued over reliability
  - Data sent with UDP is known as a **datagram**

Depicting data segments sent using TCP



Addresses …

- The **link layer includes a destination MAC address** in the frame header
  - Identify a local network interface
- The **internet layer includes a destination IP address** in the packet header to identify the host on the internet
  - That's enough information to get a packet to a specific device on the internet

Once a packet has reached its destination host

- The transport layer header includes a **destination network port number**
  - Identifies the specific service or process that will receive the data
- A host with a single IP address can have **multiple active ports**
  - Each used for performing a different type of activity on the network

An analogy [1/2]

- An **IP address** is like the *street address* of an office building,
  - A network **port number** is like the *office number* of a worker in that office building
- The IP address uniquely identifies a host computer, just as a street address uniquely identifies an office building
  - Using the internet protocol, a packet can be delivered to a host in the same way that a package can be delivered to an office building

An analogy [2/2]

- However, once a packet arrives at the computer, the operating system must decide what to do with it
  - The **packet isn't intended for the OS itself**, but for some process running on the computer
  - In the same way, a package arriving at an office building likely isn't intended for the mailroom worker but for someone else in the building
- The OS examines the port number and delivers the inbound data to the process listening on the specified **port**
  - Just as a mailroom worker examines the name or office number on the package to deliver the package to the right person

NETWORK PORTS

Network Ports

- Network ports in the range of 0 to 1,023
  - Called **well-known ports**
- Ports in the range of 1,024 to 49,151 can be registered with the Internet Assigned Numbers Authority (IANA)
  - Known as **registered ports**
- Ports with a value greater than 49,151 are **dynamic ports**

Some port numbers

20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH) Secure Login
25	Simple Mail Transfer Protocol (SMTP) email delivery
53	Domain Name System (DNS) service
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
123	Network Time Protocol (NTP)
161	Simple Network Management Protocol (SNMP)

Ports for servers and clients

- Servers use well-known ports to make it easy for clients to connect
- However, most network communication is a two-way street
  - So, the **client needs to have an open port as well** so that it can receive data from the server
- A client only needs to temporarily open such a port, just long enough for it to complete its communication with a server
  - Such ports are called **ephemeral ports**
  - Assigned by the networking components in the operating system

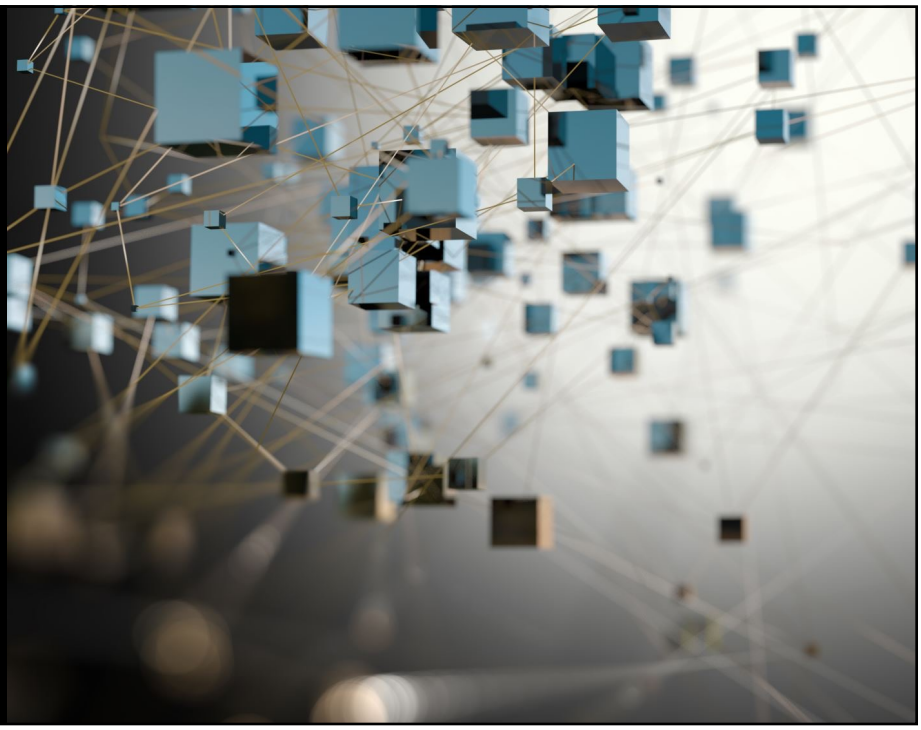
For example

- When a client web browser connects to a web server on port 80?
  - An **ephemeral port** on the client is also opened
    - Let's say port number 61,348
- The client sends its web request to port 80 on the server, and the server sends its response to port 61,348 on the client
- An IP address plus a port number form an **endpoint**
  - An instance of an endpoint is the **socket**

Network hosts (such as a client or server) make use of protocols from all four layers

- Networking hardware (such as switches and routers) only use protocols associated with lower layers
  - Link layer (for the specific hardware e.g., WiFi, Ethernet, FDDI, Token ring)
  - IP
- Switches and routers can perform their jobs without bothering to examine the higher layer protocol data

APPLICATION LAYER



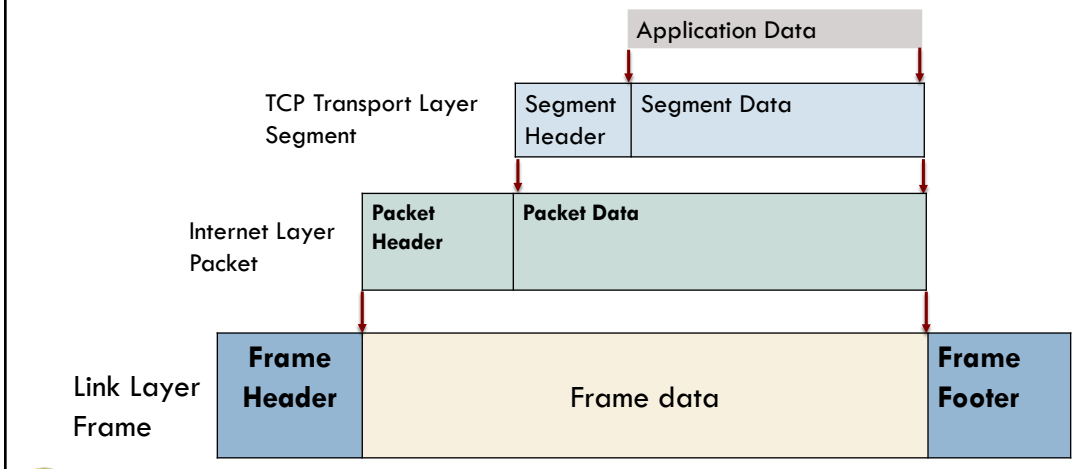
Application Layer [1/2]

- The application layer is the **final, topmost layer** of the internet protocol suite
  - The lower three layers provide a generalized foundation for communication over the internet
- Protocols at the application layer focus on **accomplishing a specific task**
  - HyperText Transfer Protocol (HTTP) for retrieving and updating web content
  - Email servers use Simple Mail Transfer Protocol (SMTP) for sending and receiving email messages
  - File transfer servers use File Transfer Protocol (FTP) to transfer files

Application Layer [2/2]

- The application layer is where we get to the protocols that **describe the behavior** of applications
- The lower layers of the stack are the "**plumbing**" that enables applications to do the things they want to do over the internet

Depicting data sent from the application layer



39

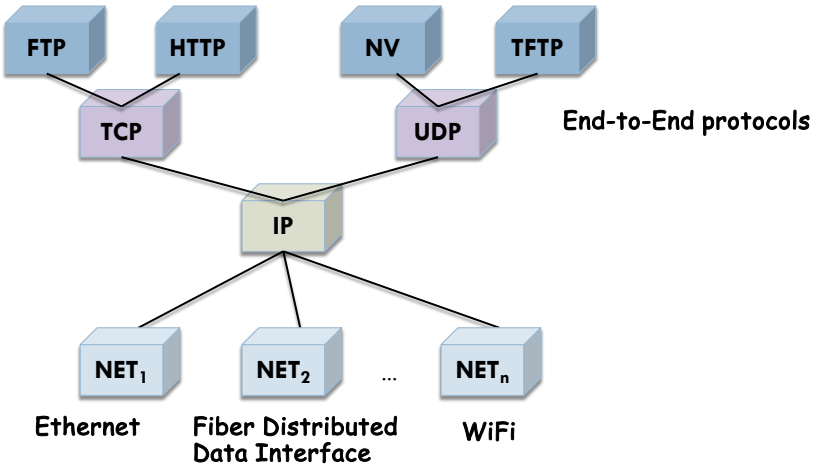
INTERNET ARCHITECTURE

40

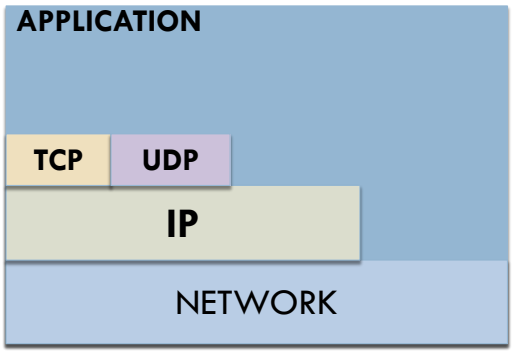
Internet architecture

- Evolved out of experiences with ARPANET
  - Funded by ARPA of the US DoD
- A **4-level** model

Internet protocol graph



Alternative view of the Internet Architecture



Internet architecture

- DOES NOT imply strict layering
  - Bypassing immediate lower layers is possible
- Layer has an **hour-glass** shape
  - Wide at top and bottom
  - Narrow in the middle
  - **IP** is the **focal point** of the architecture

INTERNETWORKING

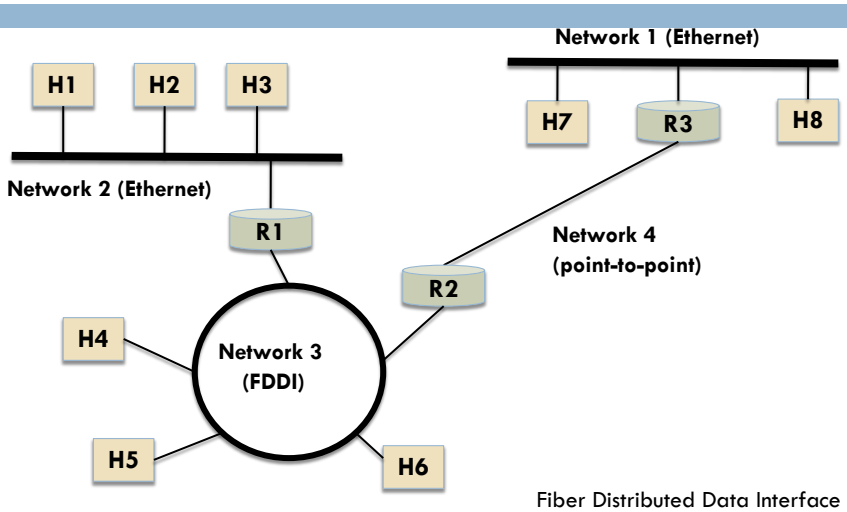
45

Internetwork

- Arbitrary collection of **interconnected** networks
  - To provide some sort of host-host packet delivery service
- Network of networks
  - Made up of lots of smaller networks

46

A simple internetwork

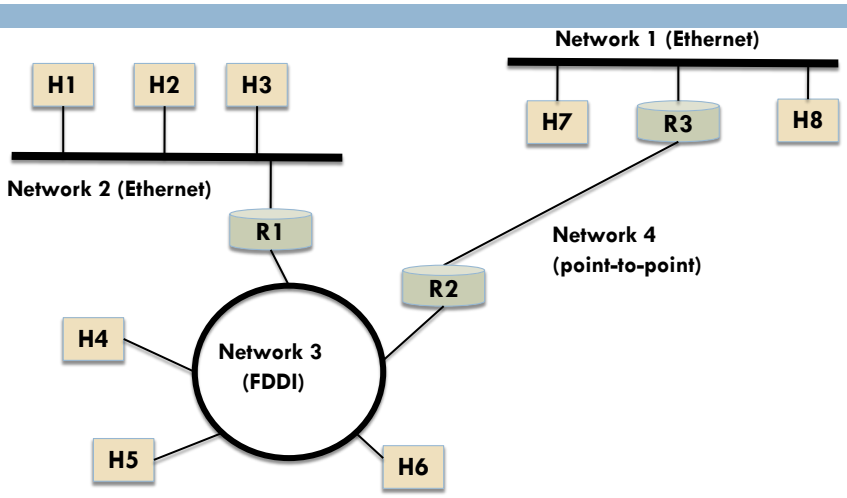


Fiber Distributed Data Interface (FDDI)

Internet Protocol (IP)

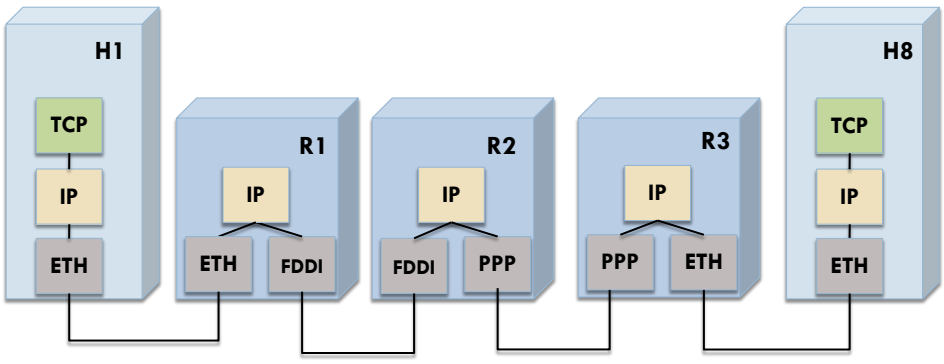
- Key tool to build scalable, **heterogeneous** networks
- Runs on all nodes (hosts and routers)
- Allows nodes and networks to *function as a single logical network*
- It is possible to build an internetwork without IP
  - But IP is the only one that has faced scale issues

A simple internetwork: Communication between H1-H8



49

Example depicting how hosts (H1-H8) are logically connected



50

The IP service model

- Datagram model of **delivery**
  - Connectionless
  - Best effort
- **Addressing** scheme
  - Identifies all hosts in the internetwork

Datagram delivery

- Datagram is a type of packet
  - Sent in a **connectionless** fashion
- No need for any *advance* setup mechanisms
  - That tell network what do when packet arrives
- Every datagram contains enough information
  - To forward packet to correct destination

The network makes a best effort to send datagrams across

- Things that could go **wrong** with the packets
  - Lost
  - Corrupted
  - Misdelivered
  - Out of order and duplicates
- When things go wrong, the network does **nothing**
  - No attempt to recover from the failure

Keeping routers simple was one of the original design goals of IP

- Important to **run over anything**
- Putting extra functionality into routers to make up for network deficiencies?
  - Not a good idea
- Higher-level protocols/apps that run above IP need to be aware of failure modes

The contents of this slide-set are based on the following references

- *Computer Networks: A Systems Approach. Larry Peterson and Bruce Davie. 4th edition. Morgan Kaufmann. ISBN: 978-0-12-370548-8. [Chapter 1, 2]*
- Matthew Justice. *How Computers Really Work: A Hands-On Guide to the Inner Workings of the Machine.* ISBN-10/ISBN-13 : 1718500661/ 978-1718500662. No Starch Press. [Chapter 11]