Network

Networking Layers

Mercy College
CYBERSECURITY
Dr. John Yoon

IASP 505

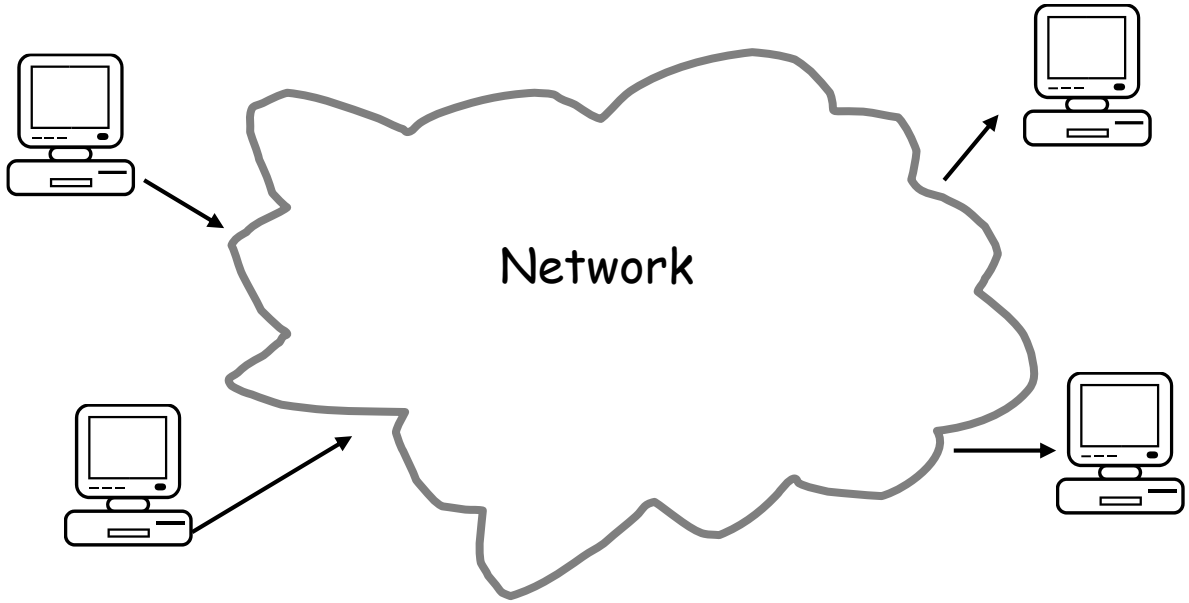
Network

What is a “Network”?

- A network is a way to get “stuff” between 2 or more “things”
- Examples: Mail, phone system, conversations, railroad system, highways and roads.

Networks

- Why they are interesting?
  - Overcome geographic limits
  - Access remote data
  - Separate clients and server
- Goal: Universal Communication (any to any)
- Design the cloud



Network Types

- Coverage
  - Locally oriented (LAN)
  - Globally oriented (WAN)
  - Personal Area Network (PAN)
  - Body Area Network (BAN)
- Carriage
  - Wired
    - Cables
  - Wireless
    - Waves/Particles

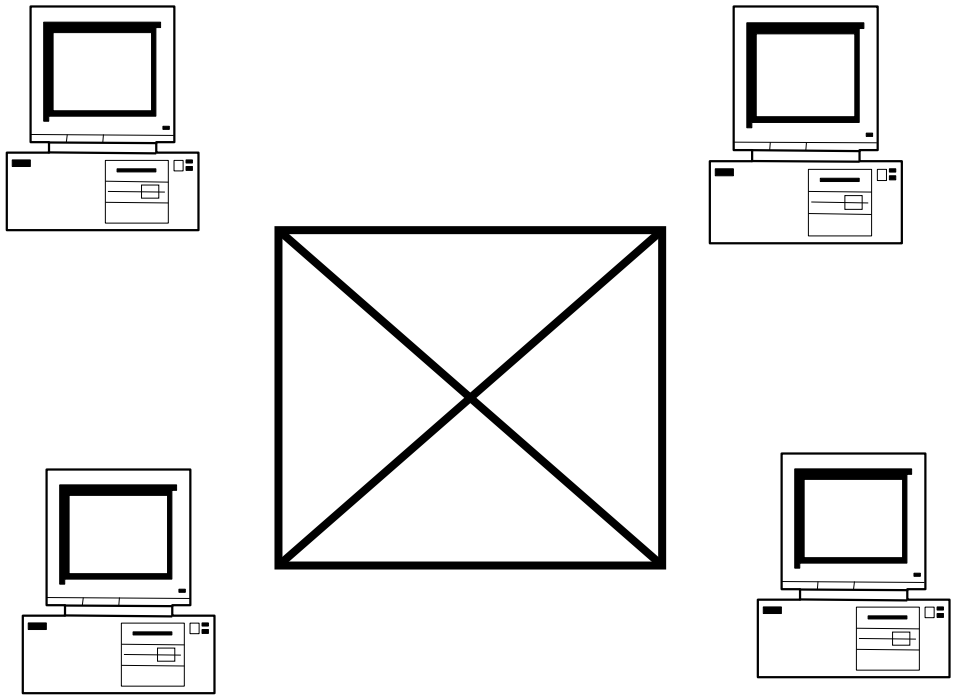
Connectivity

Link

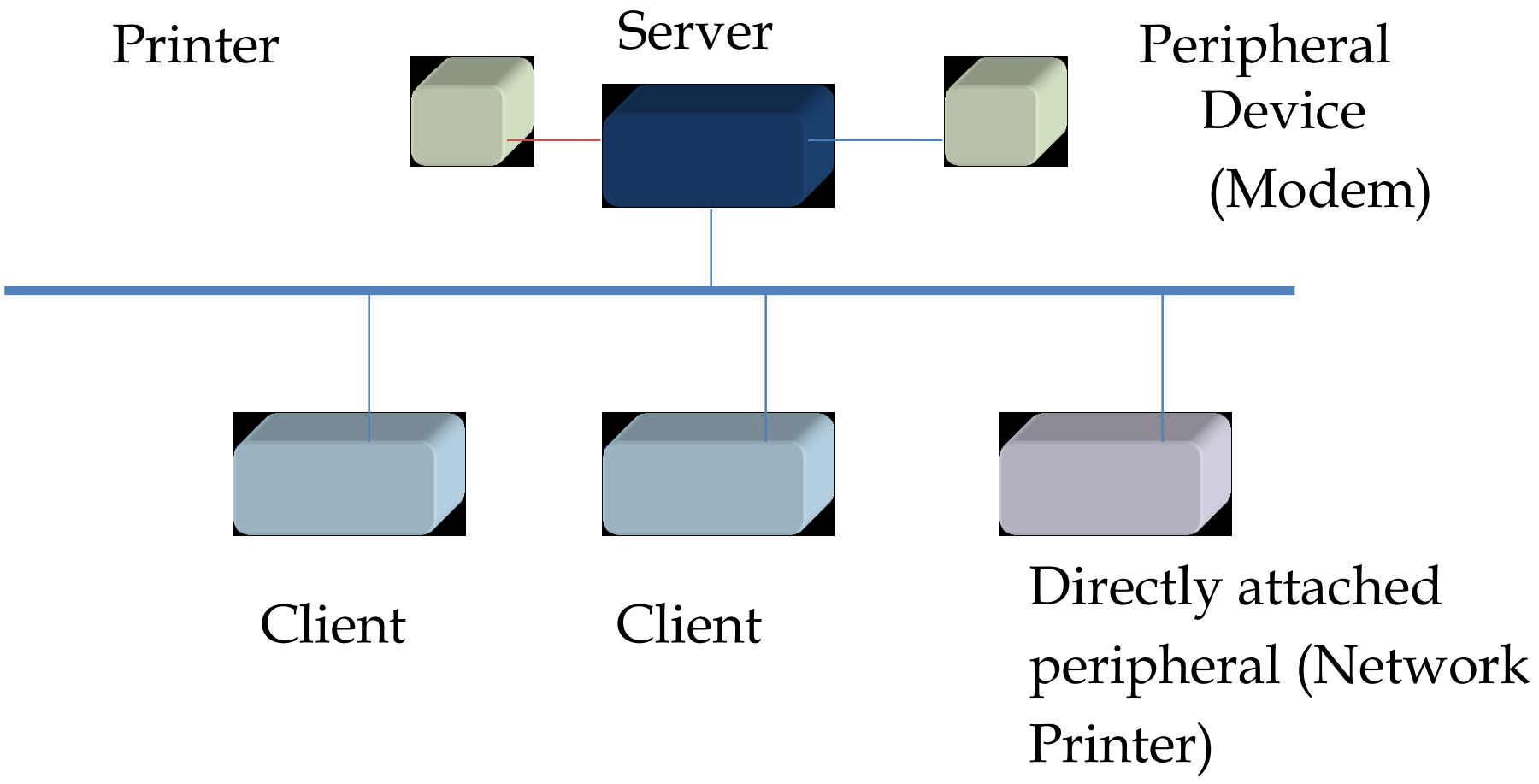
- DSL, T1, T3, ...
- Characterized by
  - Capacity or bit-rate (1.5 Mb/s, 100Mb/s, …)
  - Propagation delay (10us, 10ms, 100ms, ..)
  - Transfer time on a link = #bit/bit-rate + propagation delay

Connectivity

- A mesh requires N^2 links → too costly



A Simple Network

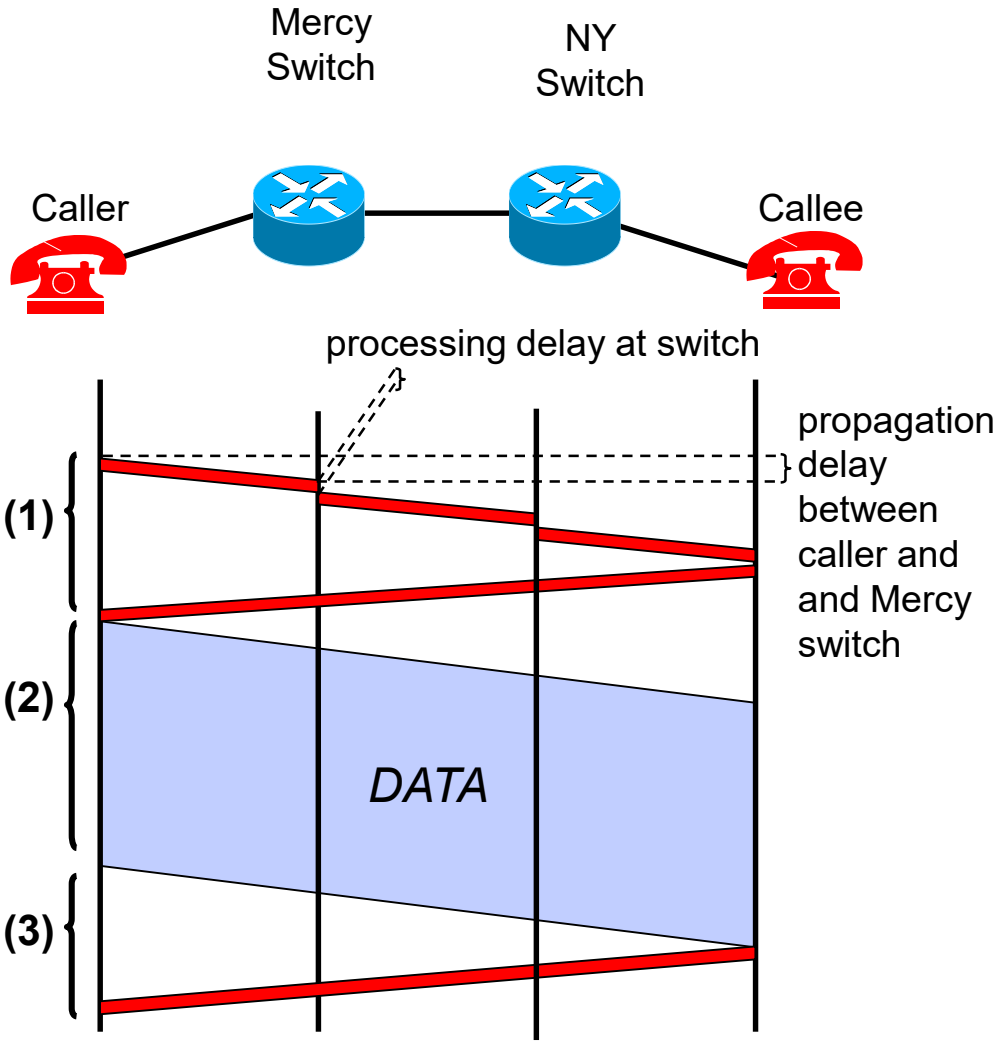


Two ways to share

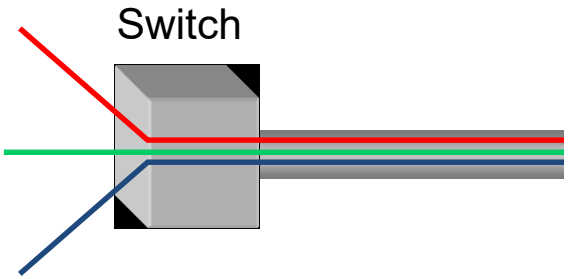
- Circuit switching (isochronous)
- Packet switching (asynchronous)

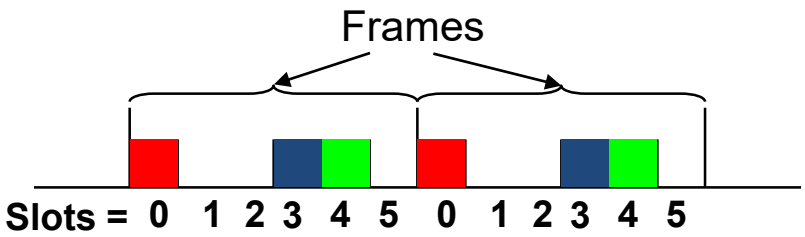
Circuit Switching

- It's the method used by the telephone network
- A call has three phases:
  1. Establish circuit from end-to-end ("dialing"),
  2. Communicate,
  3. Close circuit ("tear down").
- If circuit not available: "busy signal"



Circuit Switching: Multiplexing/Demultiplexing





One way for sharing a circuit is TDM:

- Time divided into frames and frames divided into slots
- Relative slot position inside a frame determines which conversation the data belongs to
  - E.g., slot 0 belongs to the red conversation
- Need synchronization between sender and receiver

Lecture notes use the word “frame” for slot

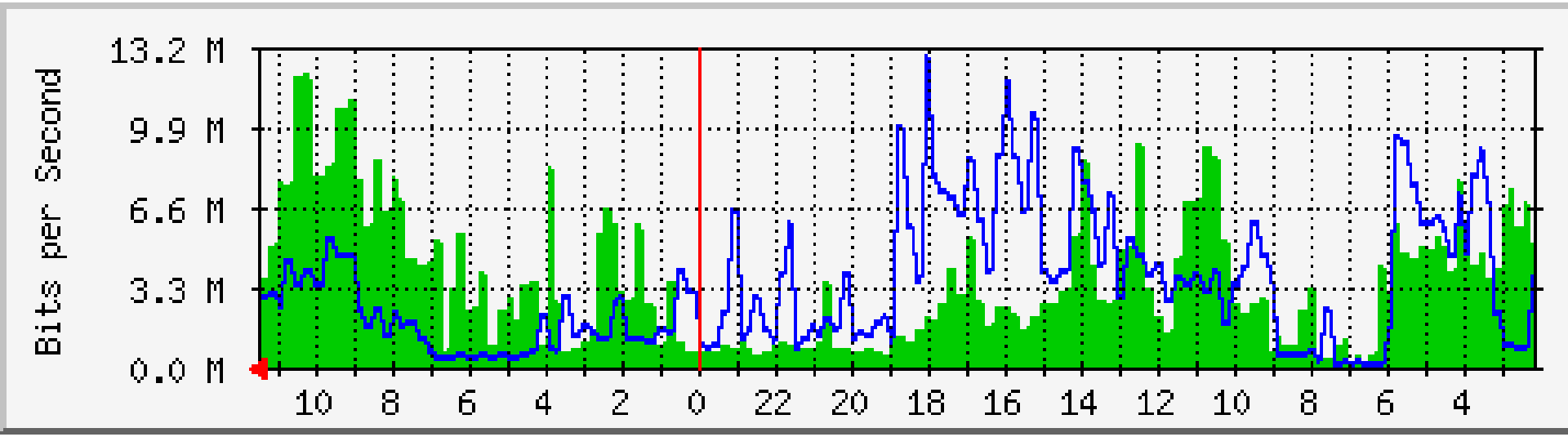
Circuit Switching

- Assume link capacity is C bits/sec
- Each communication requires R bits/sec
- #slots = C/R
- Maximum number of concurrent communications is C/R
- What happens if we have more than C/R communications?
- What happens if the a communication sends less/more than R bits/sec?

→ Design is unsuitable for computer networks where transfers have variable rate (bursty)

Internet Traffic Is Bursty

Daily traffic at an MIT-CSAIL router



Max In:12.2Mb/s

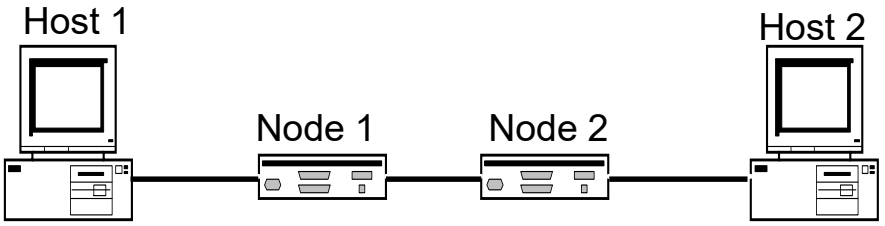
Avg. In: 2.5Mb/s

Max Out: 12.8Mb/s

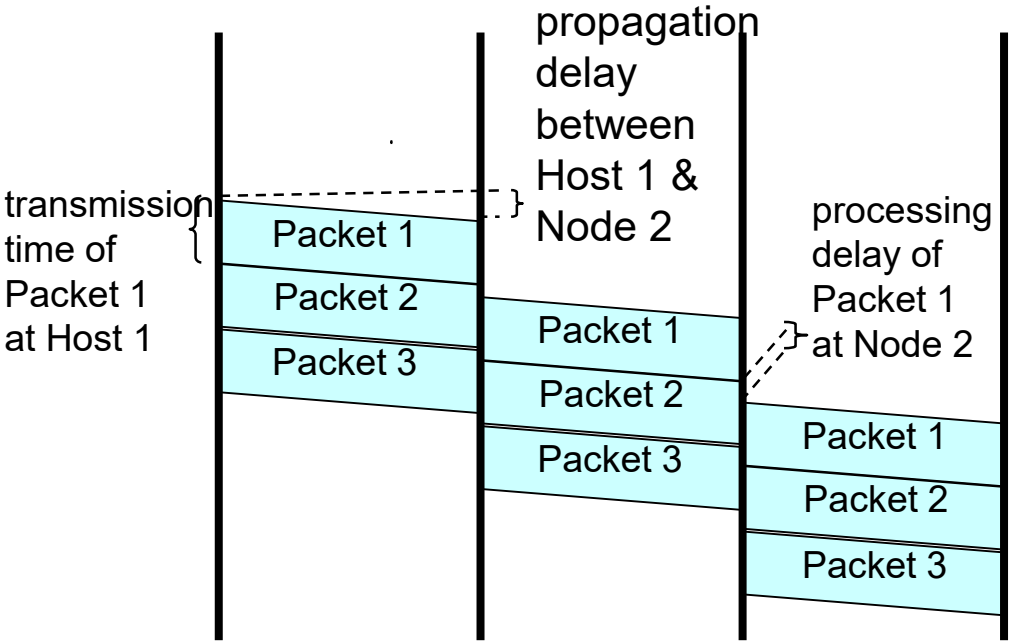
Avg. Out: 3.4 Mb/s

Packet Switching

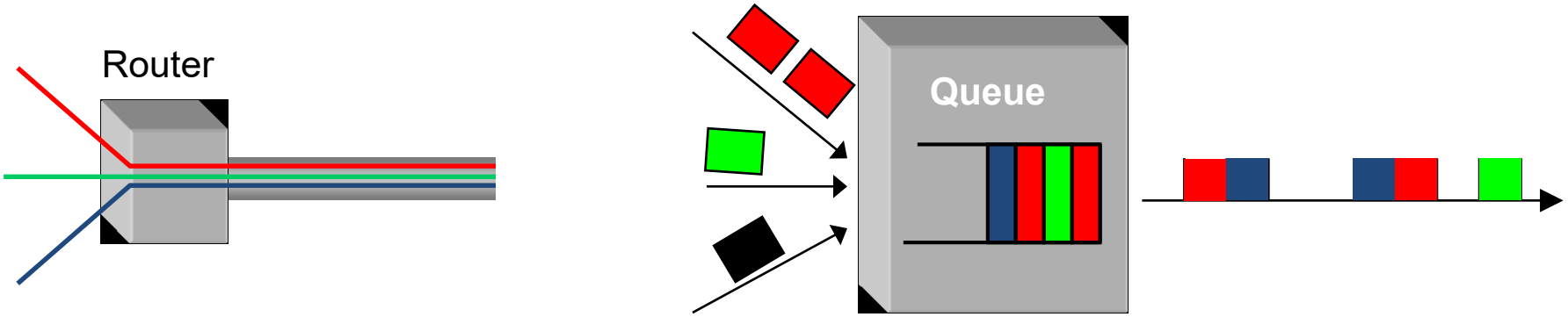
- Used in the Internet
- Data is sent in **Packets** (header contains control info, e.g., source and destination addresses)



- Per-packet routing
- At each node the entire packet is received, stored, and then forwarded (**store-and-forward networks**)
- No capacity is allocated



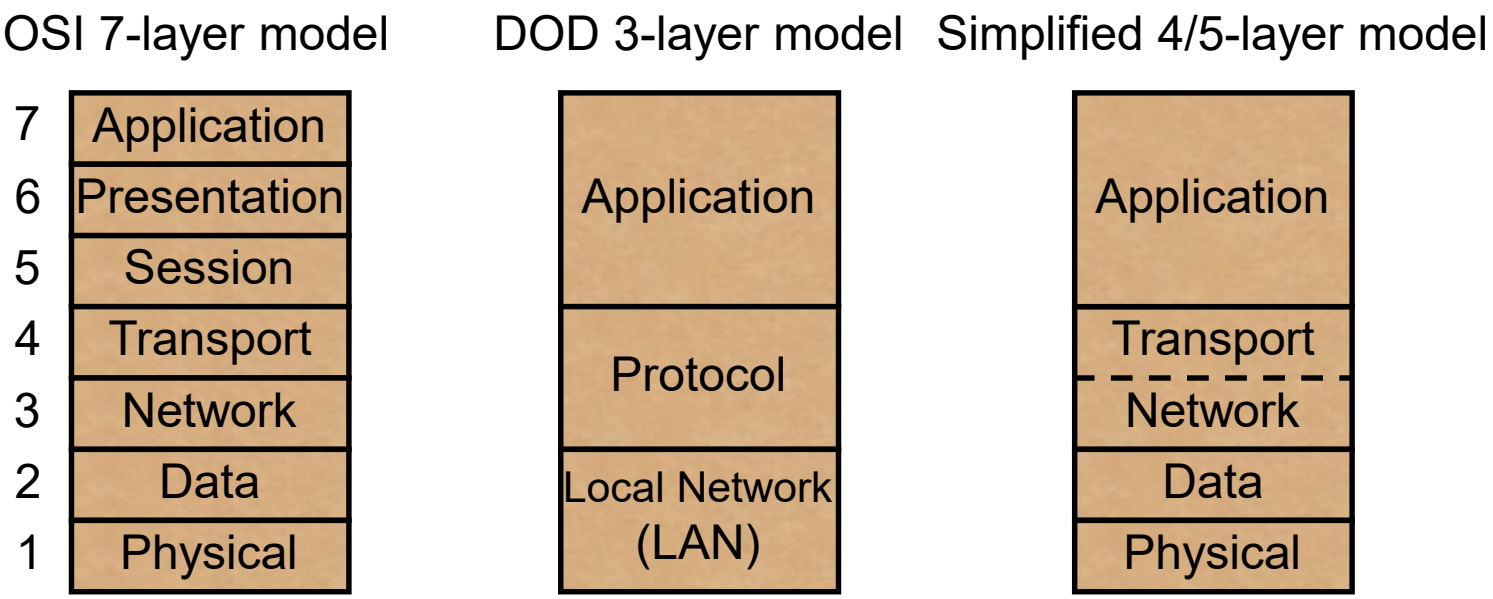
Packet Switching: Multiplexing/Demultiplexing



- Multiplex using a queue
  - Routers need memory/buffer
- Demultiplex using information in packet header
  - Header has destination
  - Router has a routing table that contains information about which link to use to reach a destination

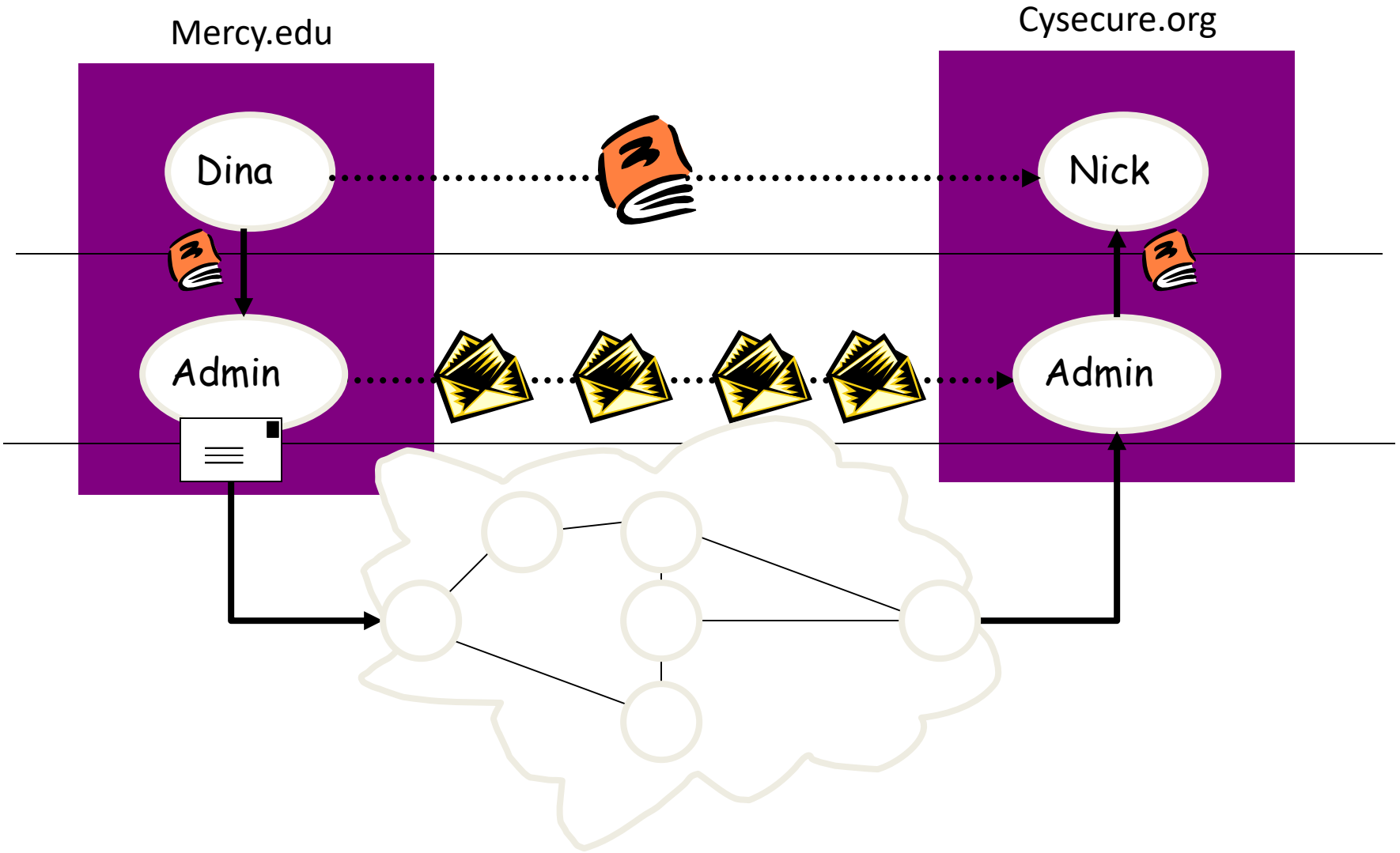
Computer Networking Models

- Models, also called protocol stacks, represented in layers, help to understand where things go right or wrong.



OSI (Open Systems Interconnection) mnemonic: All People Seem To Need Data Processing. If you ever take a test on networking, you'll have to now this, otherwise, use the simplified model.

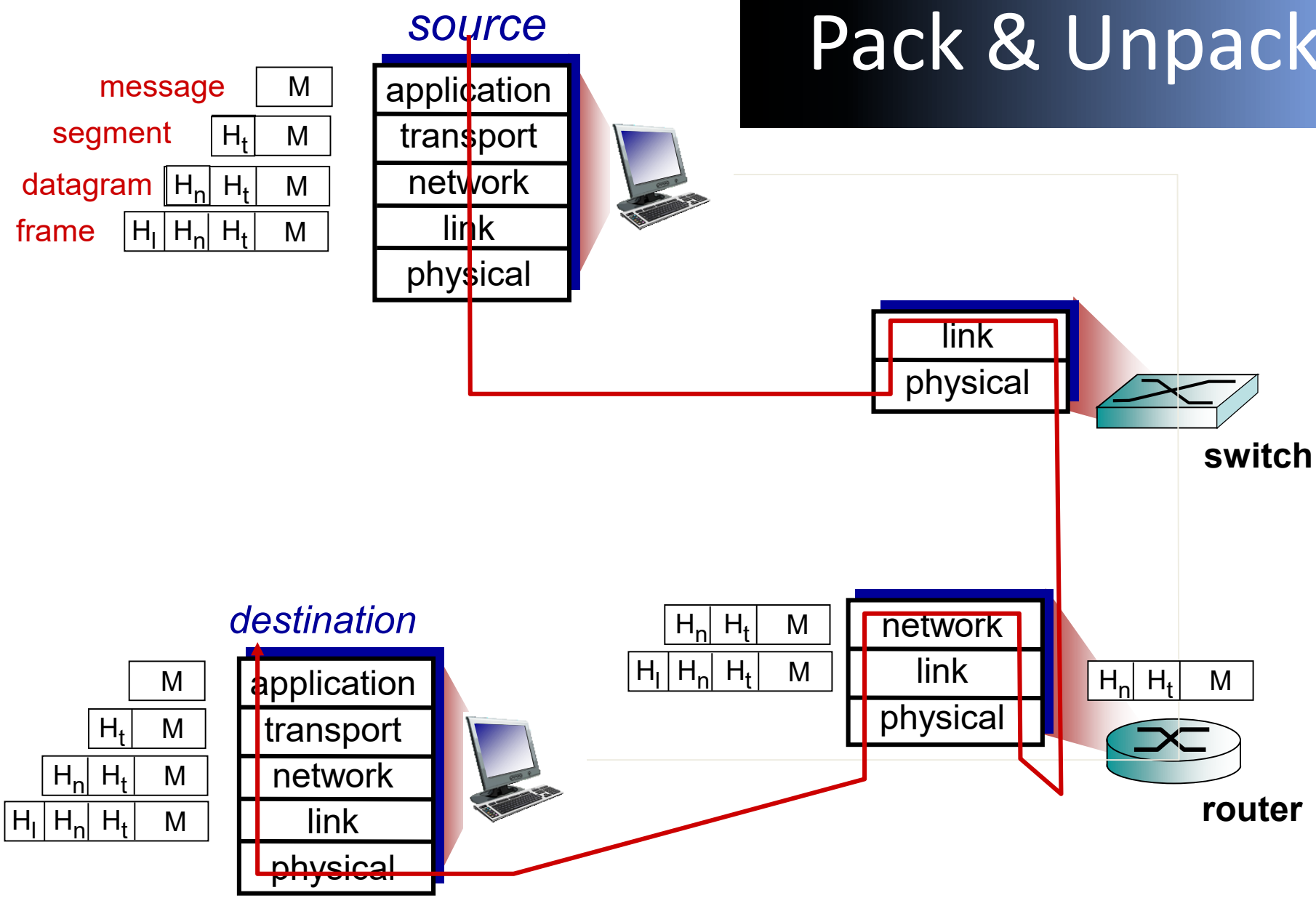
The mail system



Protocol Concepts

- Protocols are sets of rules.
- What do you want to do? (Application)
- Where are you going? (Addressing)
- How do you get there? (Media types)
- Did you get there? (Acknowledgments, Error checking)

Pack & Unpack



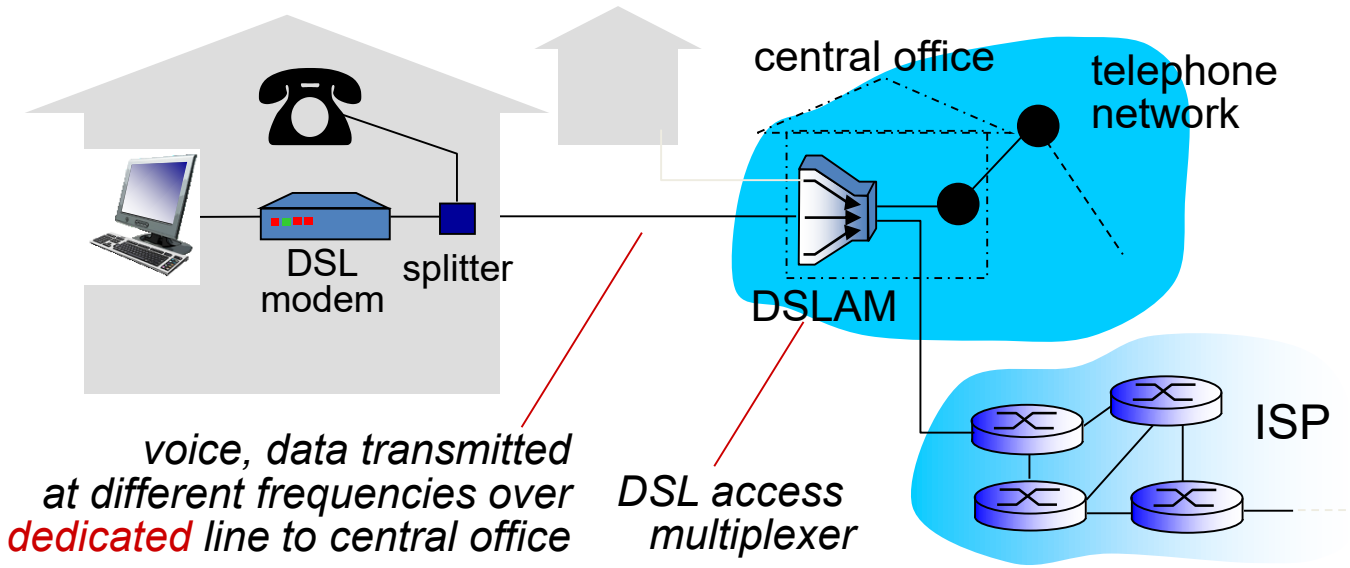
http://www.networksorcery.com/

Let's Work

- Visit
  - Network Sorcery: http://www.networksorcery.com/
- Download WireSHARK
  - From: https://www.wireshark.org/

To Our Home

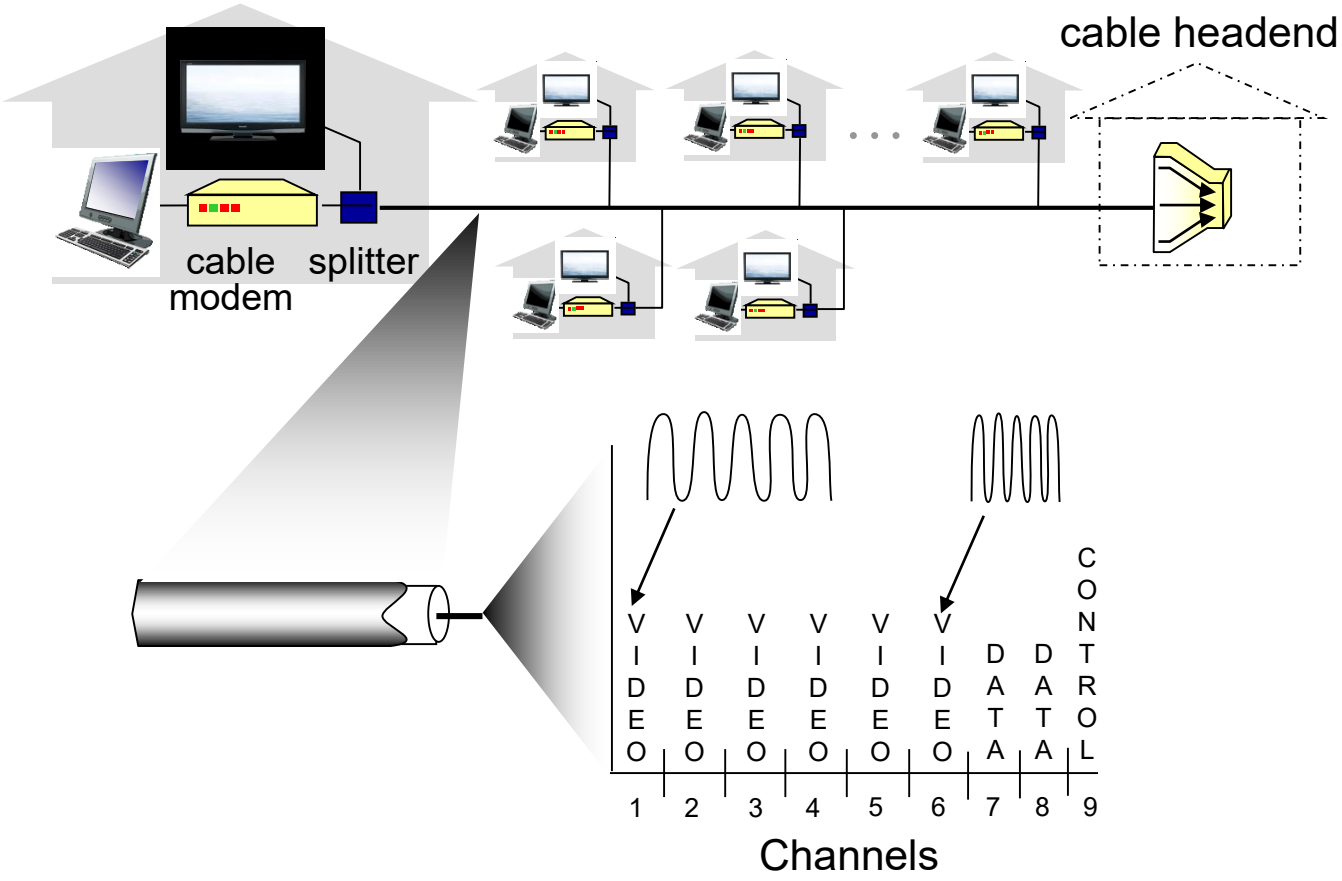
Access net: digital subscriber line (DSL)



DSL speed test
dsl-speed.org
dslreports.com

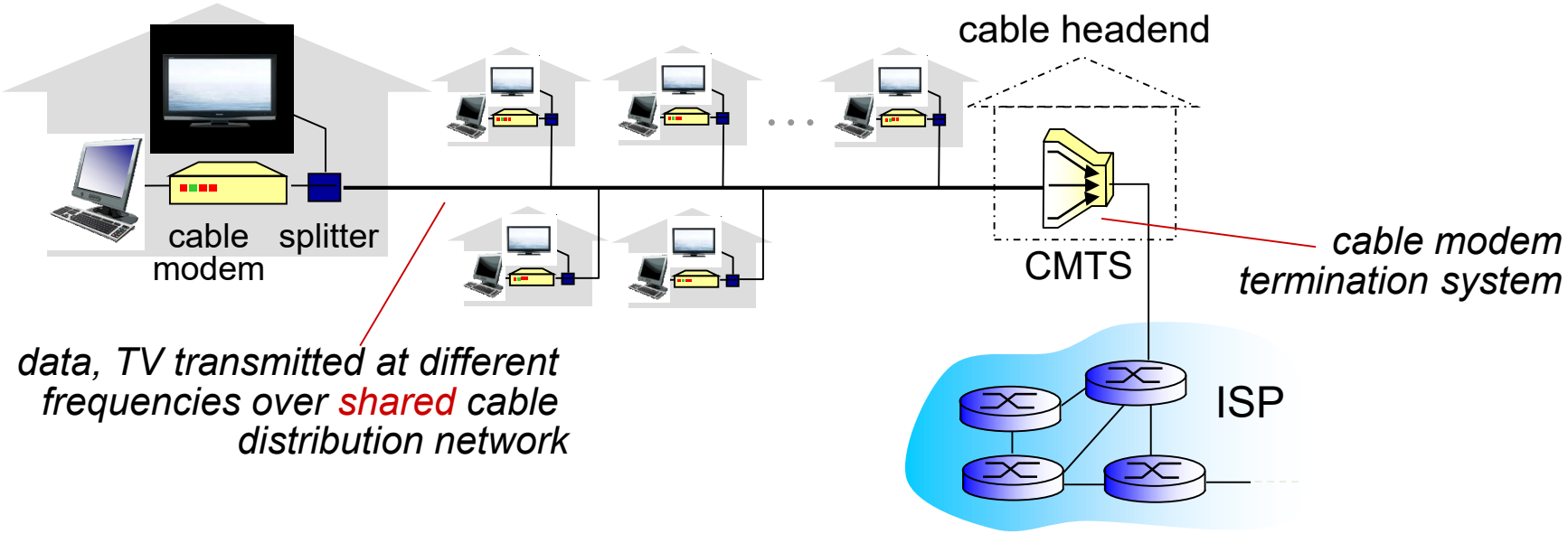
- use *existing* telephone line to central office DSLAM
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- < 2.5 Mbps upstream transmission rate (typically < 1 Mbps)
- < 24 Mbps downstream transmission rate (typically < 10 Mbps)

Access net: cable network



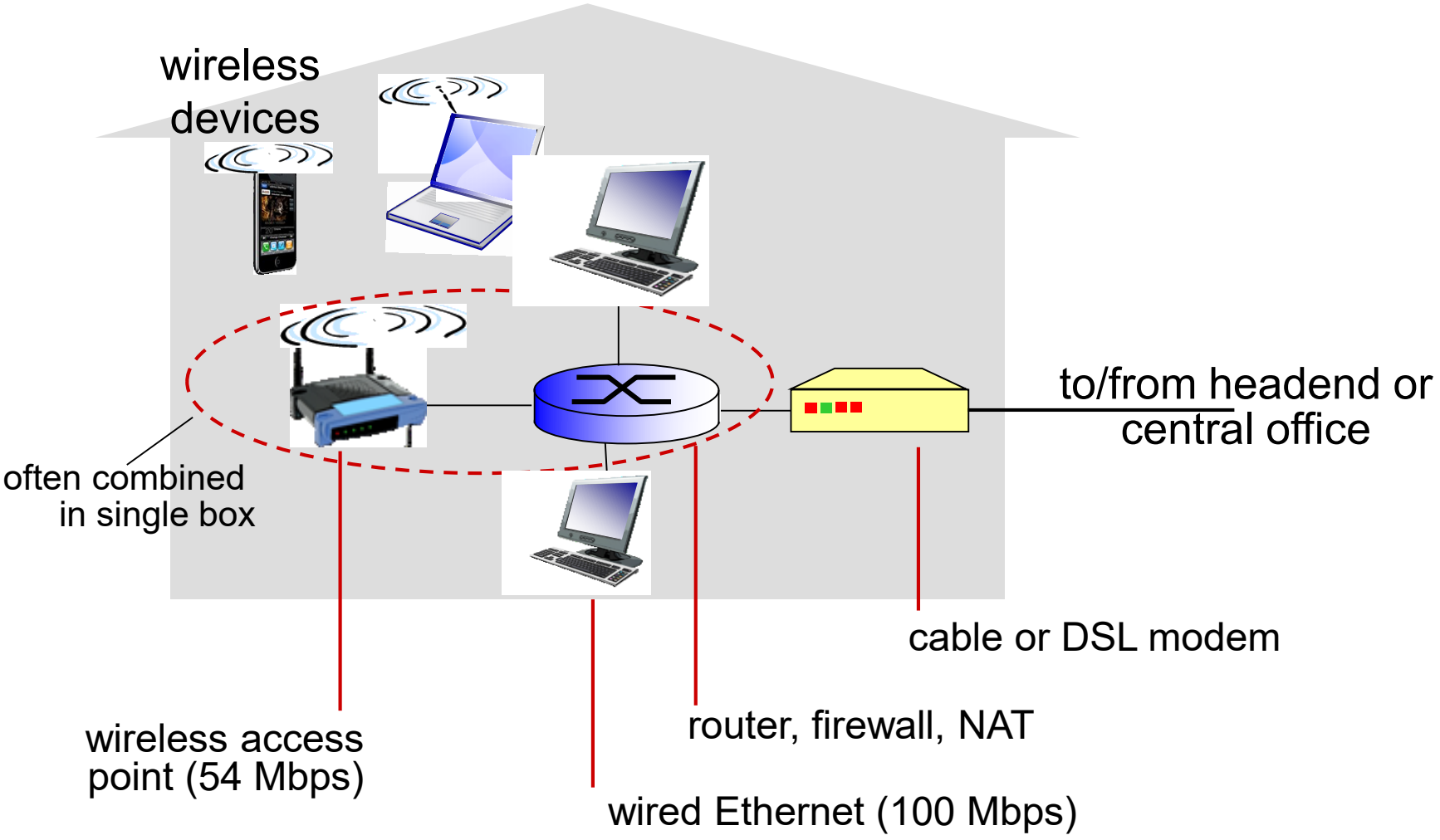
frequency division multiplexing: different channels transmitted in different frequency bands

Access net: cable network

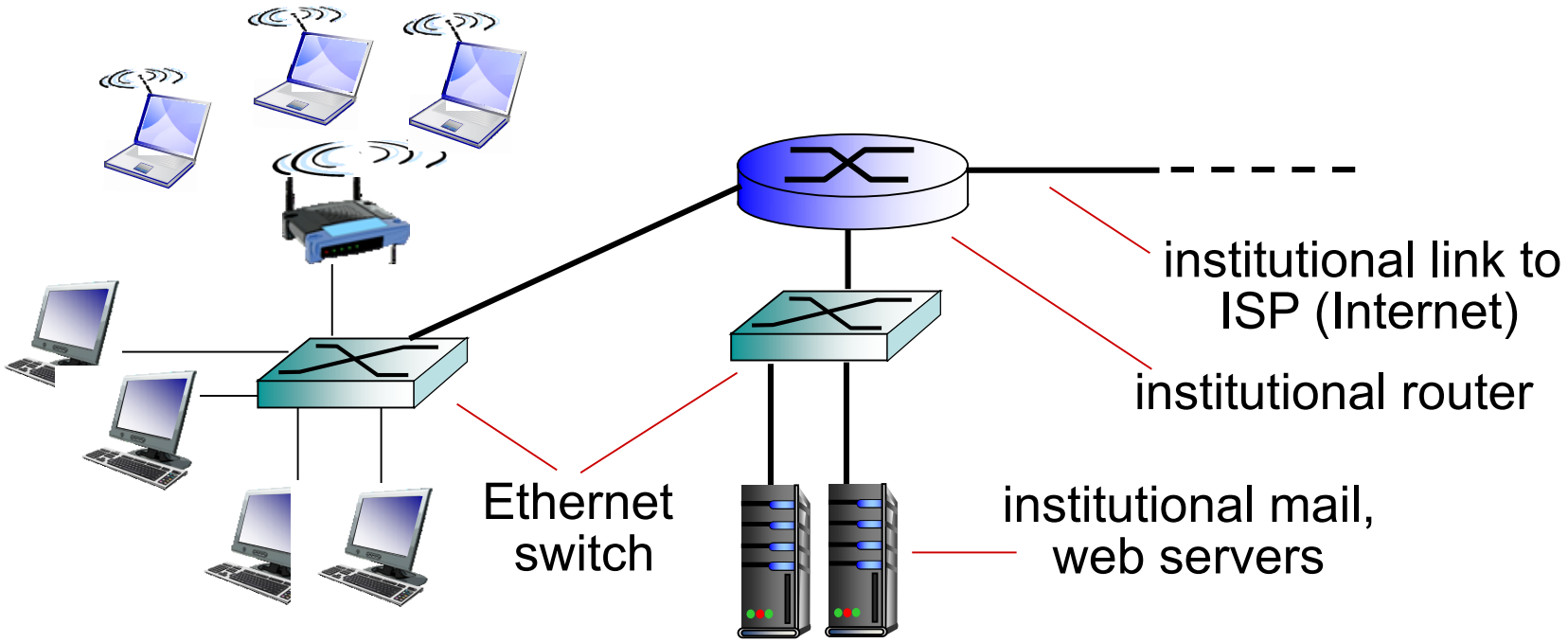


- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream transmission rate, 2 Mbps upstream transmission rate
- network of cable, fiber attaches homes to ISP router
  - homes *share access network* to cable headend
  - unlike DSL, which has dedicated access to central office

Access net: home network



Enterprise access networks (Ethernet)



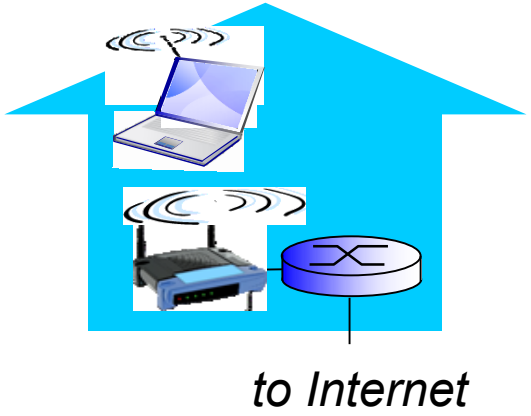
- typically used in companies, universities, etc
- 10 Mbps, 100Mbps, 1Gbps, 10Gbps transmission rates
- today, end systems typically connect into Ethernet switch

Wireless access networks

- shared *wireless* access network connects end system to router
  - via base station aka "access point"

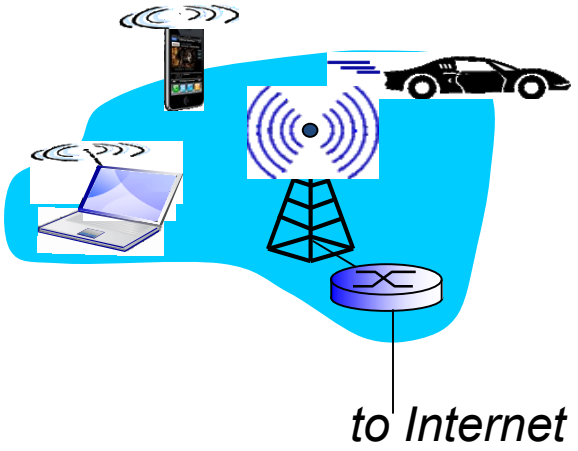
wireless LANs:

- within building (100 ft)
- 802.11b/g (WiFi): 11, 54 Mbps transmission rate



wide-area wireless access

- provided by telco (cellular) operator, 10's km
- between 1 and 10 Mbps
- 3G, 4G: LTE

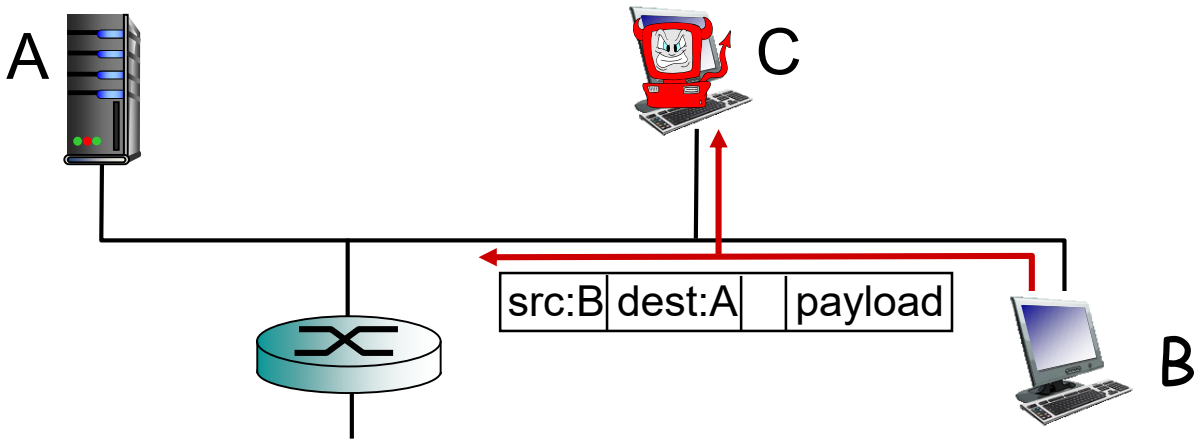


To Our Security

Bad guys can sniff packets

packet "sniffing":

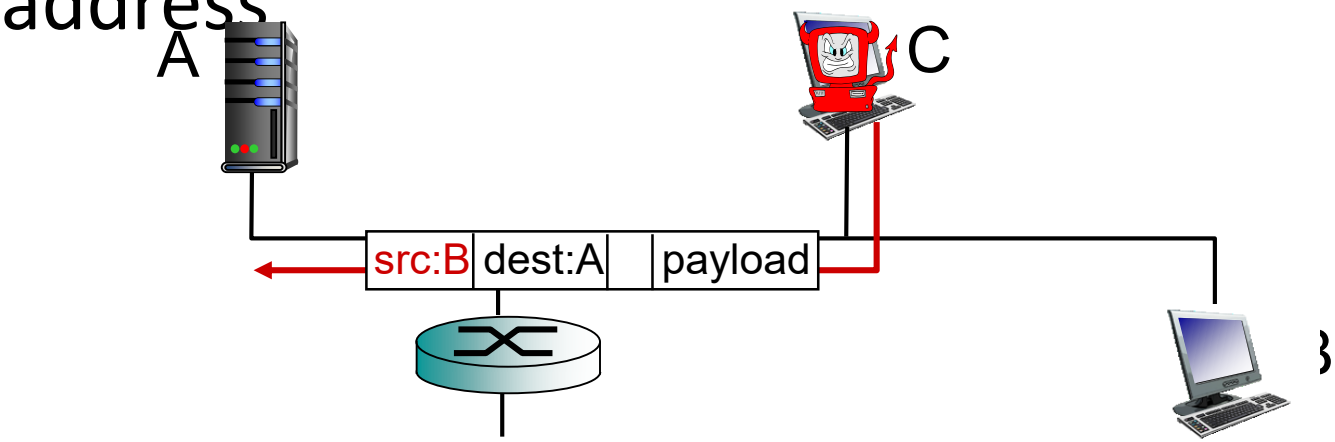
- broadcast media (shared ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- wireshark software used for end-of-chapter labs is a (free) packet-sniffer

Bad guys can use fake addresses

IP spoofing: send packet with false source address



Physical Layer (Layer 1)

- Nowadays: Pretty much just Cat 5 (or Cat 5e or Cat6) twisted pair copper wire and microwave (wireless).
- Other: Fiber (multi-mode or single-mode) coaxial copper (thick- and thin-net), Cable Modem, plain phone (DSL), microwaves (wireless ethernet), etc.

Hardware

- Servers
- Clients
- Peripheral devices
  - Network printers
  - NAS
- Media (Cabling)
  - Twisted pair, coaxial cable, optical fiber etc.
  - Wireless networks without cables
- Networking Devices
  - Hubs, switches, routers

Media

- CAT 5
  - 100 Mbps LANs
- CAT 5e
  - 1000 Mbps LANs
- CAT 6

Internetworking Devices

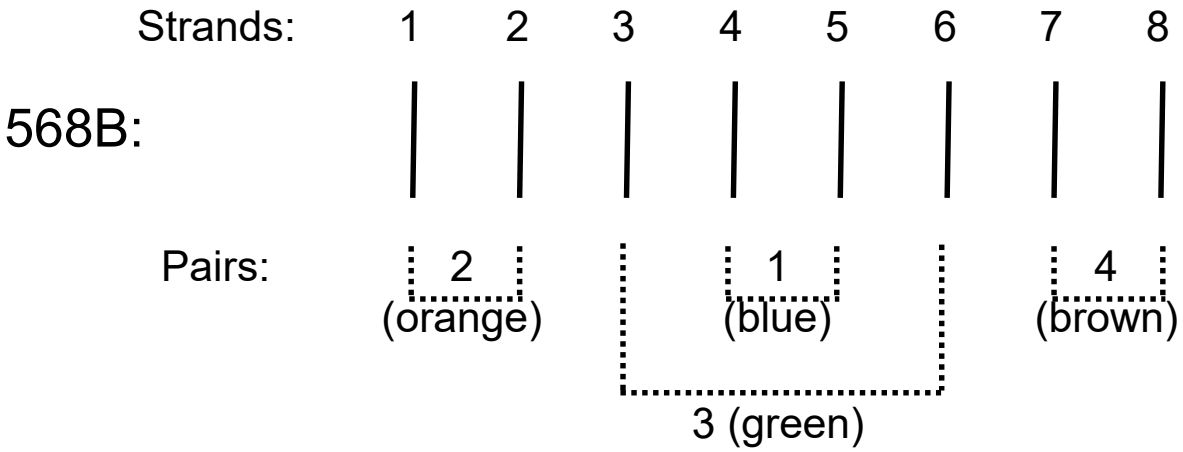
- Hub
  - Simply shares the electrical connection
- Switch
  - Switches the data packet based on MAC address
- Bridge
- Router
  - Routes the data packet based on the IP address

Twisted Pair (Cat 5/5e, Cat 6)

- Unshielded twisted pairs. Twists in wire keep down interference (from fluorescent lights, for example). Cat5e has more twists than Cat5, costs a bit more, works better for Gigabit, can exceed the 100m limitation for 100Mbit ethernet. Cat6 even more so.
- Cat3 and 4 are older, fewer twists, similar to phone, only good for 10Mbit. Phones work on Cat5/5e so current University standard is Cat5e (or Cat6 for special situations) everywhere. You can mix them, so don't worry about buying Cat6 jumpers if you want.
- Good for up to 100m, we don't like to go over 80m when wiring a building though.
- Standard connecter: RJ45.
- Star topology: each user gets their own path, easy to troubleshoot, costs more than a shared topology. Troubleshooting costs so much that bus and ring (shared) topologies are functionally dead.

Twisted Pair (continued)

- Common Terms: 10BaseT, 100BaseT, 1000BaseT. The “T” is for Twisted pair, the number is the speed, the base is “baseband” and ask someone with an EE degree what that means.
- 8 strands, 4 pairs. A couple of different standards, but 568A and 568B are the most common. Stanford uses 568B (for 568A, swap the labels for pairs 2 and 3, but no real functional difference):



10BaseT and 100BaseT only use pairs 2 and 3, so you may see some cables with only 4 strands, but since 1000T (gigabit) uses all pairs, don’t keep those cables.

Physical: Wireless

- Terms: 802.11b, 802.11a, 802.11g (coming soon: 802.16 a.k.a. “WiMax”)
- Uses microwave radio waves in the 2.4Ghz (802.11b and g) and 5.4Ghz (802.11a and n) bands to transmit data. These are unregulated frequencies, so other things (cordless phones, etc.) can use the same frequencies, but hopefully one or the other is smart enough to hop frequencies to stay clear of the other. 802.11b and g devices can use the same access points easily. 802.11a requires separate (or dual) antennae.
- For the most part, completely and utterly insecure. Very easy to capture someone else’s data. Make sure your application is secure (SSL, SSH, etc.)
- Although 802.11b at 11Mbps is the slowest (both 802.11a and g claim 54Mbps, 12-20Mbps in practice) it’s the cheapest and most ubiquitous, so you’ll still find some at Stanford. New ITS wireless is 802.11g.

Data Layer (Layer 2)

- The data layer takes the 1's and 0's handed it by the Network layer and turns them into some kind of signal that can go over the physical layer (electrical current, light pulses, microwaves, etc.) It also takes this signal and turns it back into 1's and 0's to pass up the stack on the receiving end.
- If there might be more than 2 devices on the connection, some form of addressing scheme is required to get the packet to the right destination.
- Some data layers: Token Ring, FDDI, LocalTalk, and the overwhelmingly most common data layer protocol: Ethernet.

Data Layer: Ethernet

- CSMA/CD: Carrier Sense, Multiple Access, Collision Detect. Simple!
- Since Ethernet was designed to be on shared media, with 2 or more users, and the “more” part can be very big (that’s the “Multiple Access” part) you have to listen to see if anyone else is talking before you talk (Carrier Sense) and if you and someone else start talking at the same time, notice it (Collision Detect), say “excuse me” stop and try again later. A polite free for all with rules.
- Ethernet is 10Mbit (10 million bits per second) only. Fast ethernet, which has nearly the same rules, is 100Mbit only. Gigabit ethernet is 1000Mbit only. Some Network Interface Cards (NIC’s) can speak at 10 or 100 (and sometimes 10 or 100 or 1000) but each end has to be using the same speed or there’s no connection. 10Mbit at one end and 100Mbit at the other end won’t work.

Ethernet: Addressing

- Since there can be many users on an ethernet network, everyone has to have their own unique address.
- This is called the Media Access Control (or MAC) address, or sometimes ethernet address, physical address, adaptor address, hardware addres, etc.
- It's a 12-digit (48 bit) hexadecimal address that is unique to that ethernet adaptor and no other in the world. It can be written as 00:30:65:83:fc:0a or 0030.6583.fc0a or 003065:83fc0a or 00-30-65-83-fc-0a but they all mean the same thing.
- The first 6 digits are the Vendor code, (003065 belongs to Apple), the last 6 are the individual inteface's own. Like a car's VIN. See http://coffer.com/mac_find/ to look up some vendor codes.

Ethernet: Finding your Address(es)

- On Windows 10, XP and Vista, open a command window and type “ipconfig /all” (Vista shows lots of extra junk).
- On MacOS 9, open the TCP/IP control panel and select “Get info”
- On MacOS X and most Unix or Unix-like systems, from a terminal, type ifconfig -a.

Ethernet addresses: now what?

- To send someone a message, start with a broadcast (FFFF.FFFF.FFFF) asking “where’s Bob?” Everyone’s supposed to look at broadcasts.
- “Bob” replies, in his reply, he includes his ethernet address. Since every ethernet packet has the destination and sender address listed, “Bob” knows your address (from your broadcast packet) so doesn’t have to start with a broadcast.
- For the rest of the conversation, you’ll put each other’s address as the destination (and yours as the sender), so the conversation can pass along the ethernet media between you.
- Who’s “Bob” and how did he get that name? That’s a layer 3 (Network) problem, layer 2 (Data) doesn’t care.

Hubs vs. Switches

- Hubs are shared media devices. Everyone sees everyone's packets, you're only supposed to pay attention to those specifically directed to you, or to broadcasts. Not too secure, but cheap. Most wireless still qualifies as a "hub," while actual wired ethernet hubs are becoming hard to find.
- Switches aren't shared, most of the time. The switch pays attention to the packets and makes a list of the "sender" ethernet addresses and makes a table (it removes old data after a while). When a packet comes along whose destination address is in the table (because that host has recently "talked" and identified itself) the packet only goes to that port. Unknown packets and broadcasts still go to all ports, but overall, there are nearly no collisions and is generally more secure. Switches are now much more common than hubs.

Network Layer (Layer 3)

- Network packets can be routed. This means they can be passed from one local network to another. Data layer packets can't be routed, they're local only. Your computer can only get data layer packets on its data layer interface, so network layer packets have to be stuffed inside the data layer packets. This is called "encapsulation" and is why a layered model is so handy.
- When you link computers up, via layers 1 (Physical) and 2 (Data) you get a network. When you link networks up, you get an internetwork. You need the Network layer (3) to get data between all the little networks (often called subnets) of your internetwork. There's one internetwork so well known, it drops the "work" and gets a capital "I." (There was a recent college Jeopardy final "answer" about the Internetwork!)
- Network Layer Protocols: Internet Protocol (IP) and some others that aren't used any more (AppleTalk, Netware, etc.)

Network Layer: IP

- The Internet Protocol (IP) is the Network layer protocol used on the Internet! It's so handy that most everyone uses it on all their networks big and small.
- Designed for huge, ever-expanding networks of networks. Works pretty well with unreliable links, routes can be re-built when links go down.
- ARP: Address Resolution Protocol. Turns an IP number into an ethernet number, very important. Instead of asking "Who's Bob?" you ask "Who's 172.19.4.15" and if you get a reply, associate the ethernet address with the IP address in your arp table, and now you can keep sending your data to the intended recipient via the correct ethernet address.
- Remember: the only packet you can actually send on ethernet is an ethernet packet, everything else has to be stuffed inside it.

IP Addressing

- IP addresses consists of 4 “octets” such as: 172.31.56.151
- Each “octet” consists of numbers between 0 and 255 (or OO and FF in hex!)
- It works sort of like the phone system, with “area codes” to the left, then “prefix” etc. but more flexible. On campus, your computer will know that “171.64.” means “Stanford” while it will figure out that “20” means “Pine Hall” and will learn that “23” means the computer called “networking.” It does this via subnet masking (in this case, 255.255.255.0), which isn’t covered in this class.

IP: Domain Name Resolution (DNS)

- Since most people find it easier to remember names instead of numbers, IP numbers can and almost always are associated with names.
- Your computer, however, needs a number, so the Domain Name System (DNS) exists to make everyone happy.
- A name, such as networking.stanford.edu tells you the first (or top) level domain (.edu, for educational institutions) the second level domain (stanford) and the actual host's name (networking). If you want the number for a host name within stanford.edu, you'll ask one of our DNS servers to give it to you. If you need to go outside stanford.edu, you'll still ask our servers, but they'll figure out which other server(s) should get your request, send it to them, and will send the reply back to you.

DNS Servers

- Since you need the DNS servers to turn names into numbers, you really need to know the numbers of the DNS servers.
- DHCP (Dynamic Host Configuration Protocol), not covered in this class, can hand this information to you automatically.

IP: Routing. “How do you get there from here?”

- As mentioned before, you can only send ethernet packets out of your ethernet interface, and ethernet packets stay on your local network.
- You can put an IP (Network layer) packet inside of an ethernet (data layer) packet, but somebody’s got to pass it along, and that somebody’s a router.
- Every IP number not on your local network will “belong” to your router in your ARP table.
- If you want to talk to someone outside your local network, you’ll send that ethernet packet to your router’s ethernet address and trust that it will work afterwards. It’s out of your hands now. You know what’s “local” or “not” by the subnet mask.

More routing.

- Routers keep tables of networks, often many and often large.
- Routers know: 1- Networks directly connected to them (sometimes one or two, sometimes a hundred or more), 2- Networks connected to their "friends and neighbors" and 3- The "default route" for everything else.
- When your ethernet packet arrives at the router, it takes the Network packet (and all its contents), looks at the destination IP number, checks its tables, and sends a new ethernet (or other layer 2) packet (where the "sender" is now the router, not you) out the (hopefully) correct interface. That may go to the final host if it's on one of the routers directly connected networks, or to another router, which does the same process, until your packet gets to the router responsible for that local network, who then sends your packet to to the intended host. Whether your final destination host is in the next building or on the other side of the world, it works the same way.

Who's my router?

- We serve most people on campus with only a handful of routers, each one serving many different networks.
- We also "cheat," in that we used to tell you on the main campus to use 171.64.1.1 (and perhaps 171.65.1.1, 171.66.1.1 and 171.67.1.1) which really isn't your router, but is much easier to remember. Plus we use a subnet mask of 255.255.0.0, which is another "cheat."
- When you try to talk to the "1.1" router, your actual router will intercept the packet and say: "That's me, I'll take care of that !" and you'll be none the wiser.
- This "cheat" is called Proxy ARP, and isn't really necessary any more. DHCP hands out the correct router and subnet mask, and the new departmental firewalls don't support Proxy ARP, so we're going to stop this cheat all over campus as soon as we can. Move to using DHCP, it makes your life easier!

It really can't be a networking class without ping and traceroute

- Ping and Traceroute are two somewhat useful tools for looking at and learning about your network.
- Ping sends a small packet to a host which may or may not choose to reply to it, and times how long the packet takes to get back. Lack of a reply doesn't indicate a problem with the host or network.
- Traceroute asks all routers along the path between you and the destination host if they'd like to respond to you, and times how long each of 3 requests take to get back to you. Some routers may not respond, but may still pass the traceroute packet along, and many hosts will not reply to the traceroute inquiry at all. Lack of a reply doesn't indicate a problem with the host or network.

Review.

- What's a network?
- What's a Protocol Stack?
  - What happened to layers 4 through 7?
- What's Cat 5? Cat 5e? What layer are they?
- What's Ethernet? Why do I care?
- What's IP?
- What kind of conversations can my computer have? Who can help it with more conversations?
- What's DNS?
- What's a router do? Why do I care? Does each building have one?

Resources

- Networking Web Page: http://www.stanford.edu/services/network/
  - Lots of links. Check out SUNet reports for lots of statistics on our network.
- LNA Guide: http://lnaguide.stanford.edu
  - Go to “training” for this presentation and others.
- Stanford’s wireless networks: http://wirelessnet.stanford.edu
  - Wireless Guest feature: http://wirelessguest.stanford.edu
- Essential Stanford Software: http://ess.stanford.edu
  - Instructions with pictures on how to get your computer onto the network.