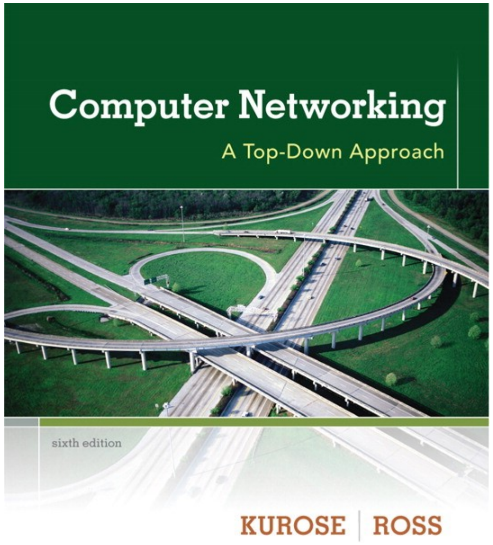
Computer Networking

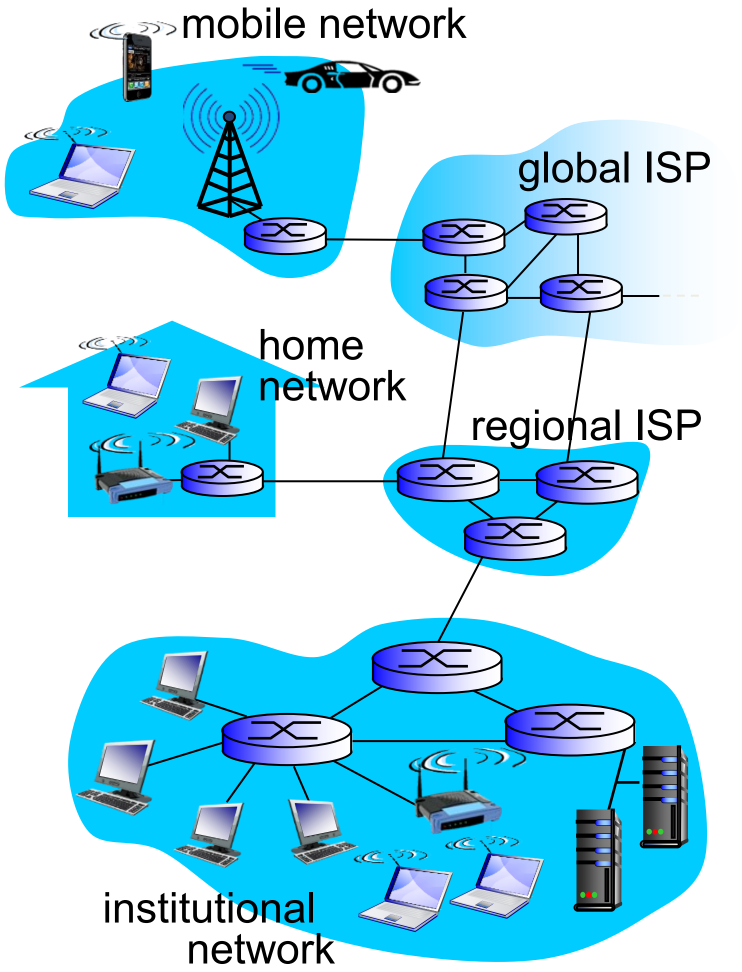
Access Networks



Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

A closer look at network structure

- *network edge:*
  - hosts: clients and servers
  - servers often in data centers
- *access networks, physical media:* wired, wireless communication links
- *network core:*
  - interconnected routers
  - network of networks



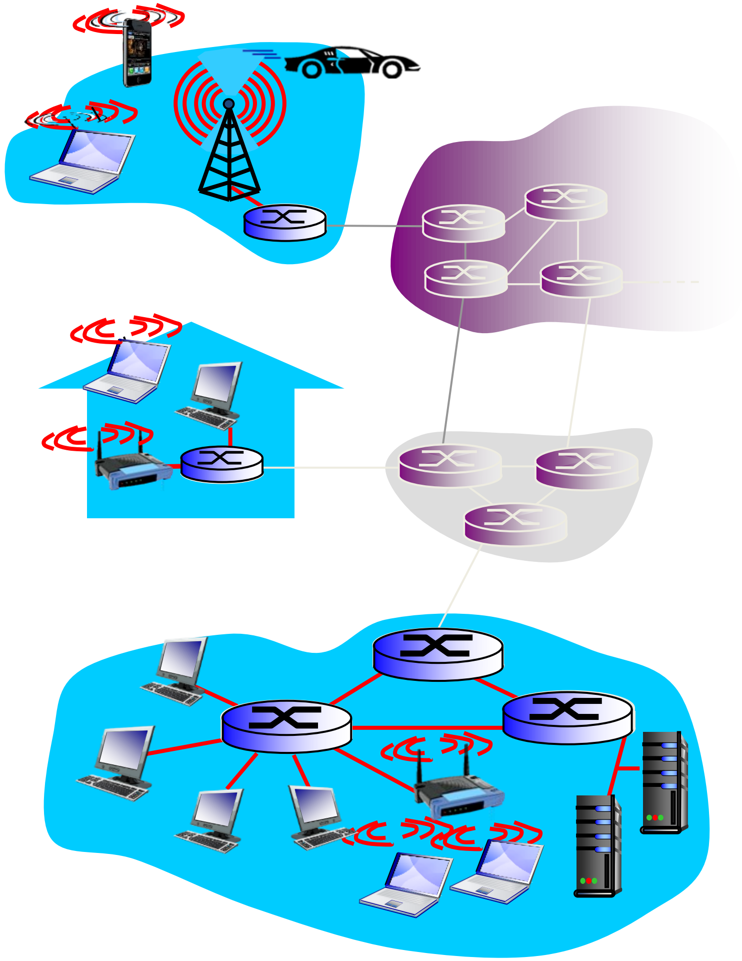
Access networks and physical media

Q: How to connect end systems to edge router?

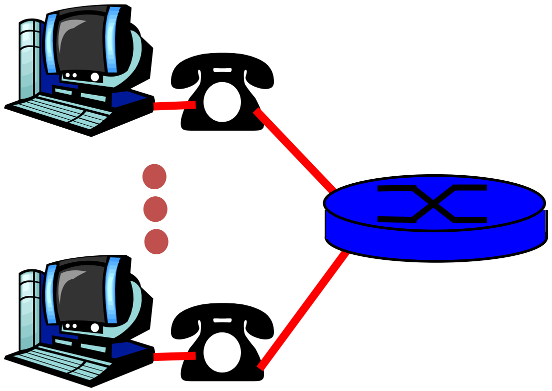
- residential access nets
- institutional access networks (school, company)
- mobile access networks

keep in mind:

- bandwidth (bits per second) of access network?
- shared or dedicated?

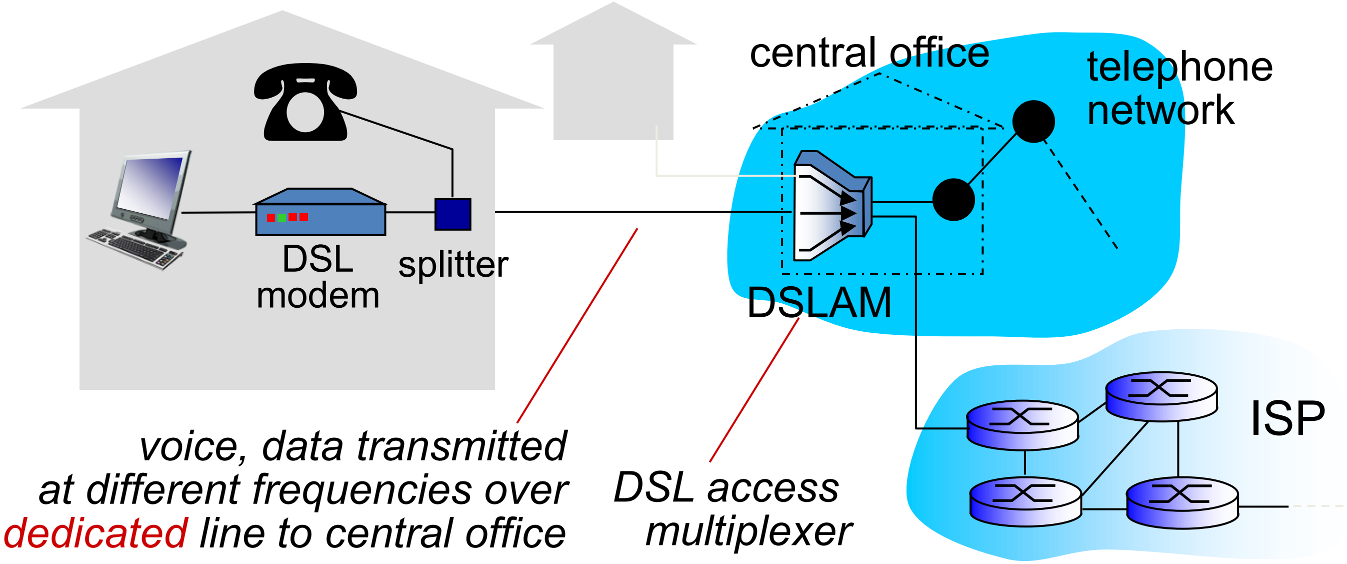


Access net: dial up via modem



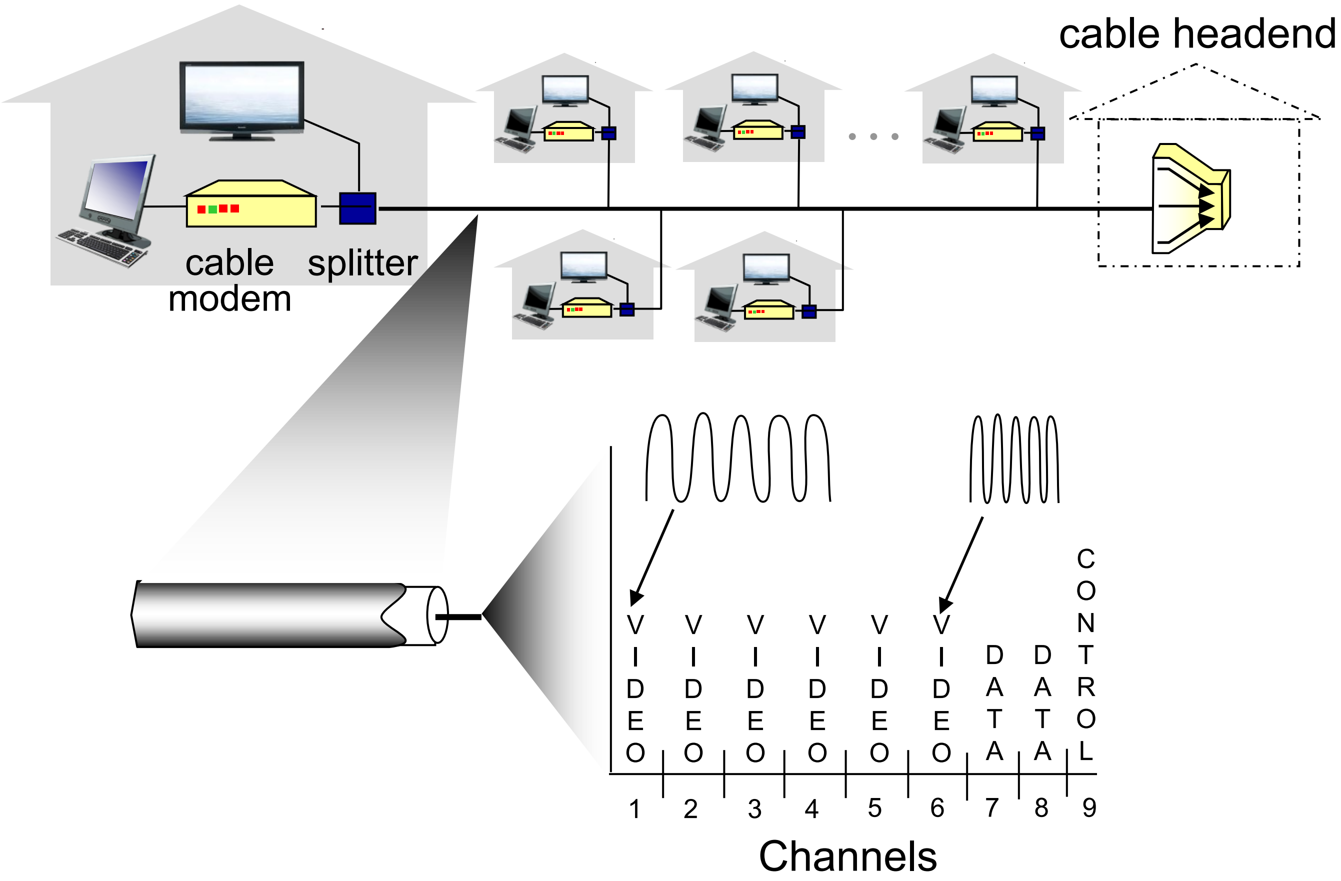
- up to 56Kbps direct access to router (often less)
- Can’t surf and phone at same time: can’t be “always on”

Access net: Digital Subscriber Line (DSL)


central office
telephone network
DSL modem
splitter
DSLAM
ISP
voice, data transmitted at different frequencies over *dedicated* line to central office
DSL access multiplexer

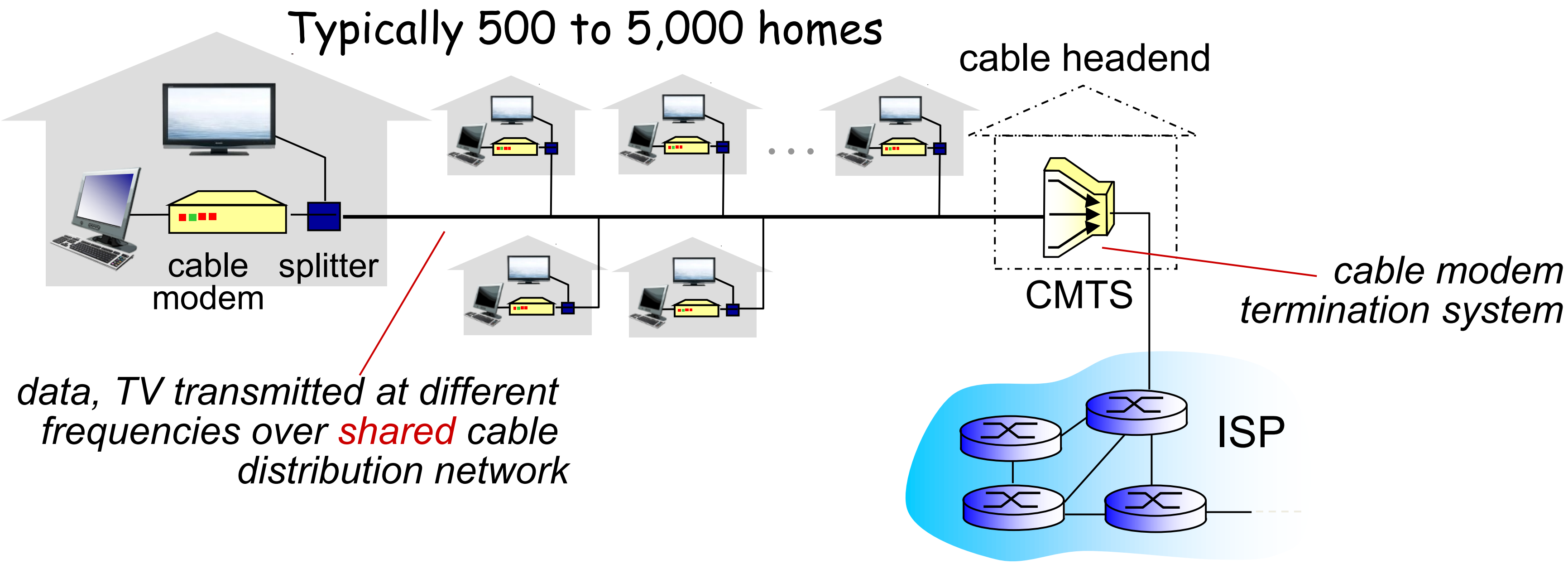
- use *existing* telephone line to central office DSLAM
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- < 2.5 Mbps upstream transmission rate (typically < 1 Mbps)
- < 24 Mbps downstream transmission rate (typically < 10 Mbps)

Access net: cable network



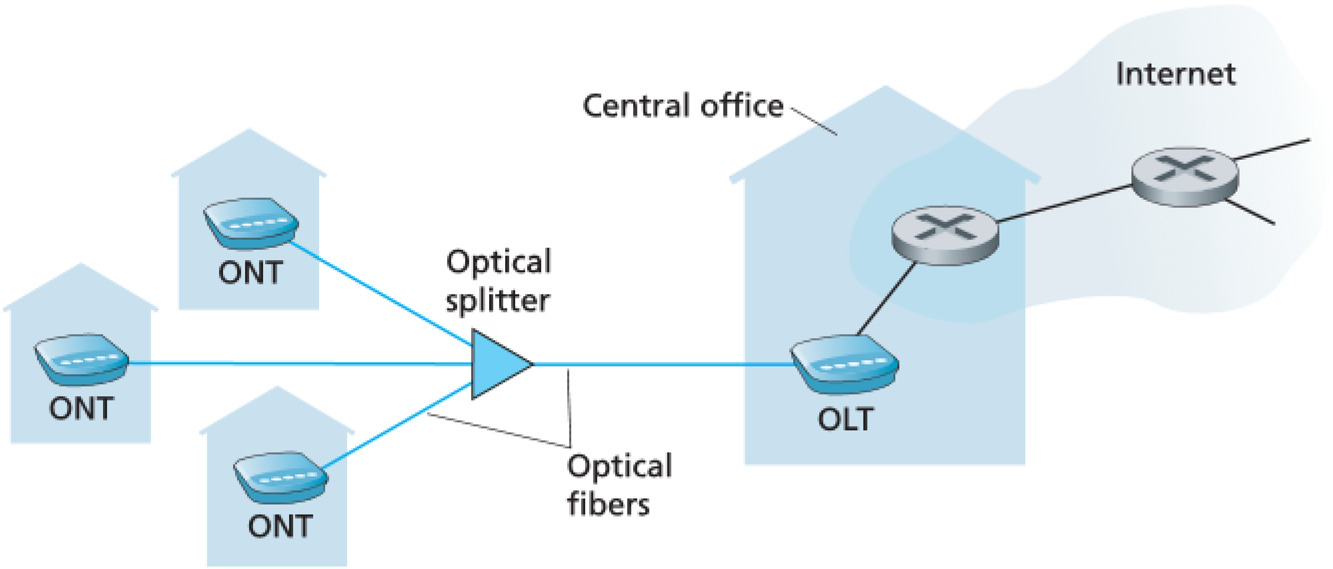
frequency division multiplexing: different channels transmitted in different frequency bands

Access net: cable network


Typically 500 to 5,000 homes
cable headend
cable modem
splitter
CMTS
cable modem termination system
data, TV transmitted at different frequencies over shared cable distribution network
ISP

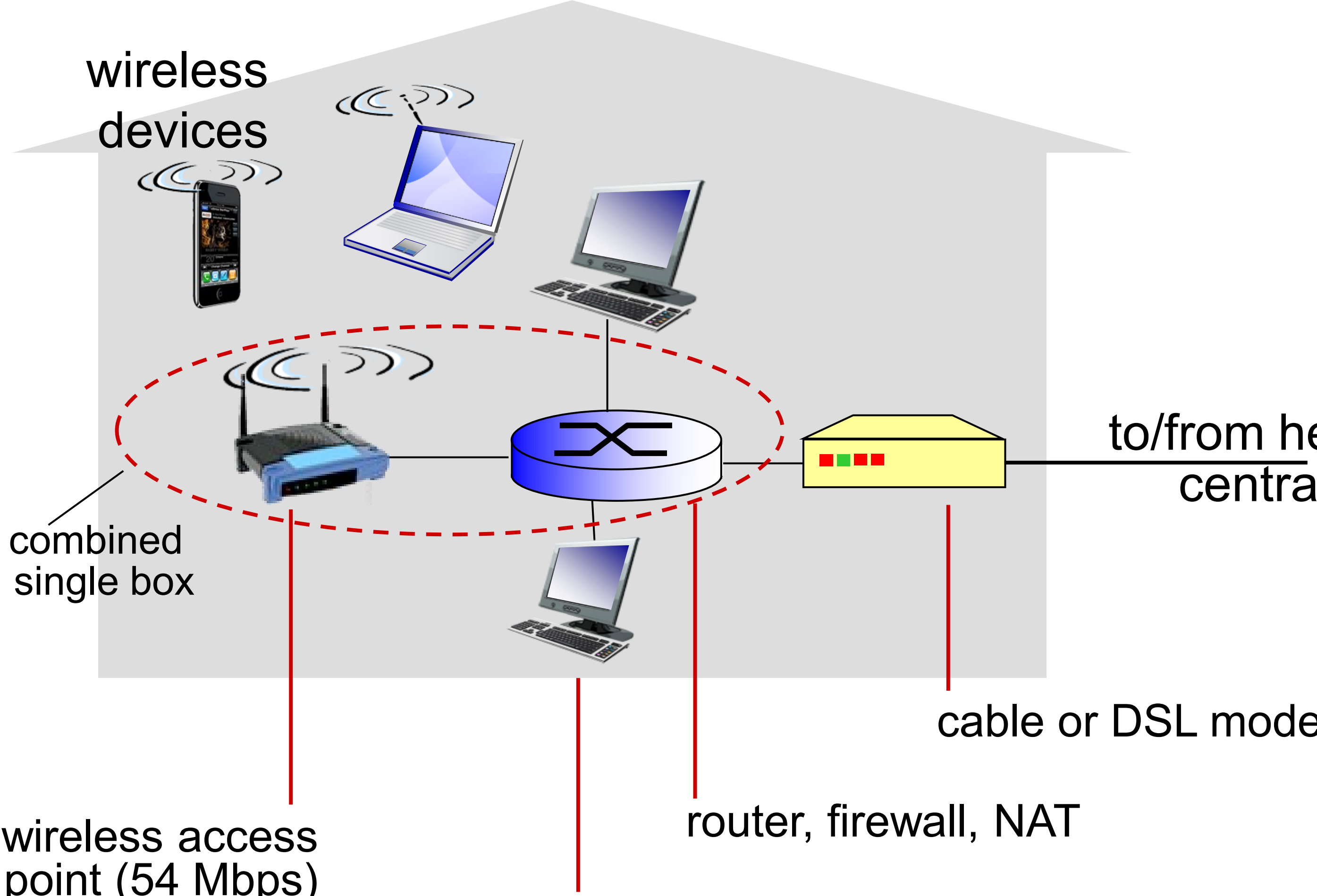
- Uses cable TV infrastructure, rather than telephone infrastructure
- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream transmission rate, 2 Mbps upstream transmission rate
- network of cable, fiber attaches homes to ISP router
  - homes *share access network* to cable headend
  - unlike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

Access net: Fiber To The Home (FTTH)



- Provides an optical fiber path from the CO directly to the home.
- Higher speed

Access net: home network



wireless devices

often combined in single box

to/from headend or central office

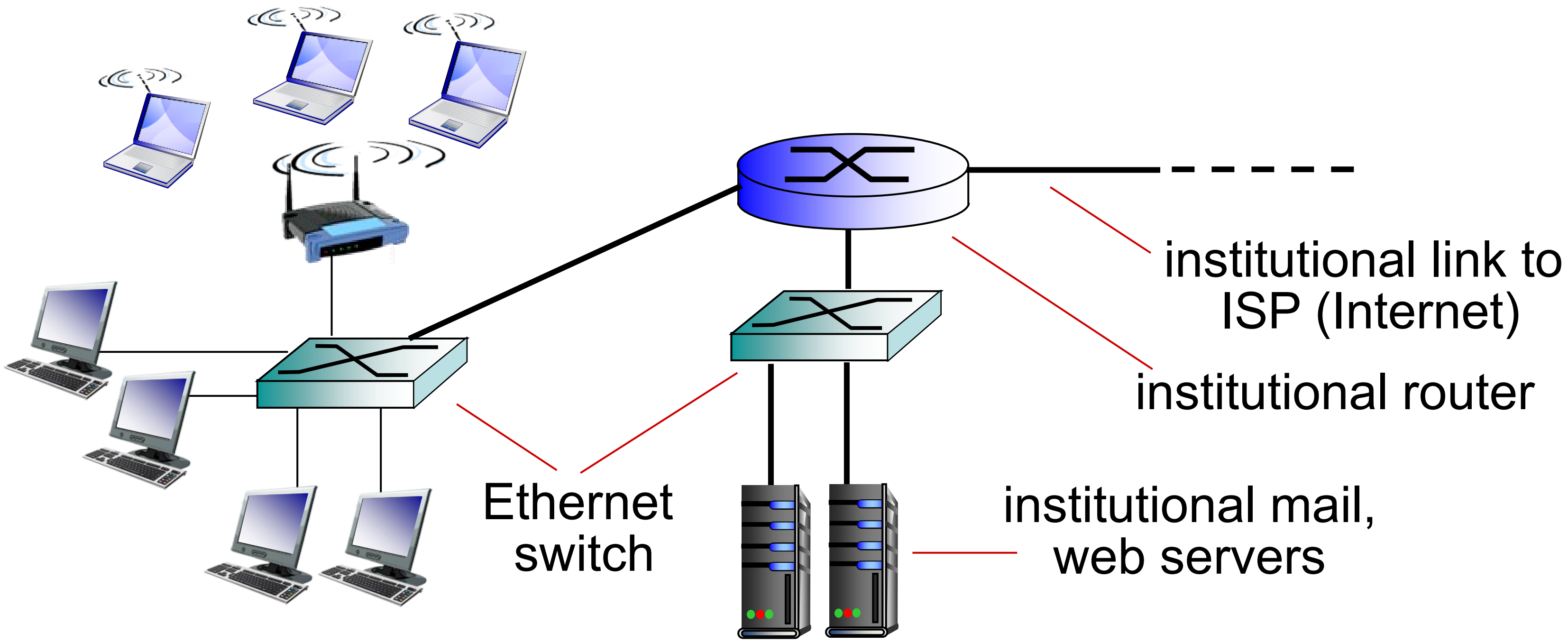
cable or DSL modem

router, firewall, NAT

wireless access point (54 Mbps)

wired Ethernet (100 Mbps)

Enterprise access networks (Ethernet)


institutional link to ISP (Internet)
institutional router
Ethernet switch
institutional mail, web servers

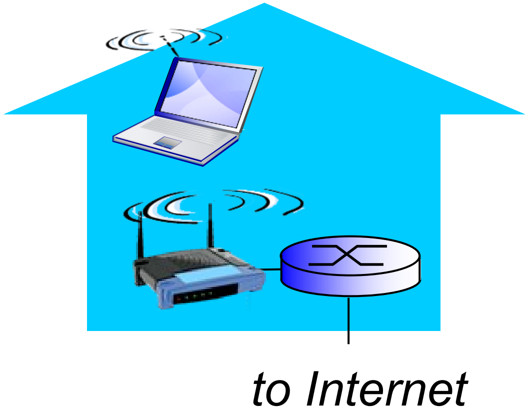
- Typically used in companies, universities etc.
- 10 Mbps, 100Mbps, 1Gbps, 10Gbps transmission rates
- today, end systems typically connect into Ethernet switch

Wireless access networks

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

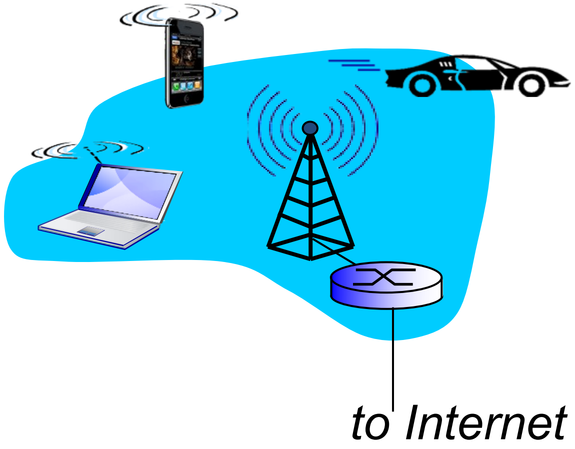
wireless LANs:

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



wide-area wireless access

- provided by telco (cellular) operator, 10's km
- between 1 and 10 Mbps
- 3G, 4G, 5G



Wireless access networks

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	late 2019 (expected)	60 GHz	100 Gbps	300-500 m.
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

Physical media

- bit: propagates between transmitter/receiver pairs
- physical link: what lies between transmitter & receiver
- guided media:
  - signals propagate in solid media: copper, fiber, coax
- unguided media:
  - signals propagate freely, e.g., radio

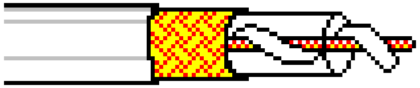
Twisted Pair (TP) Copper Wire

- two insulated copper wires
  - Category 5: 100 Mbps, 1 Gpbs Ethernet
  - Category 6: 10Gbps

Physical media: coax, fiber

Coaxial Cable:

- two concentric copper conductors
- bidirectional
- broadband:
  - multiple channels on cable
  - HFC



Fiber Optic Cable:

- glass fiber carrying light pulses, each pulse a bit
- high-speed operation:
  - high-speed point-to-point transmission (e.g., 10’ s-100’ s Gpbs transmission rate)
- low error rate:
  - repeaters spaced far apart
  - immune to electromagnetic noise

Physical media: Radio

- Signal carried in electromagnetic spectrum
- No physical “wire”
- Bidirectional
- Propagation environment effects:
  - reflection
  - obstruction by objects
  - interference

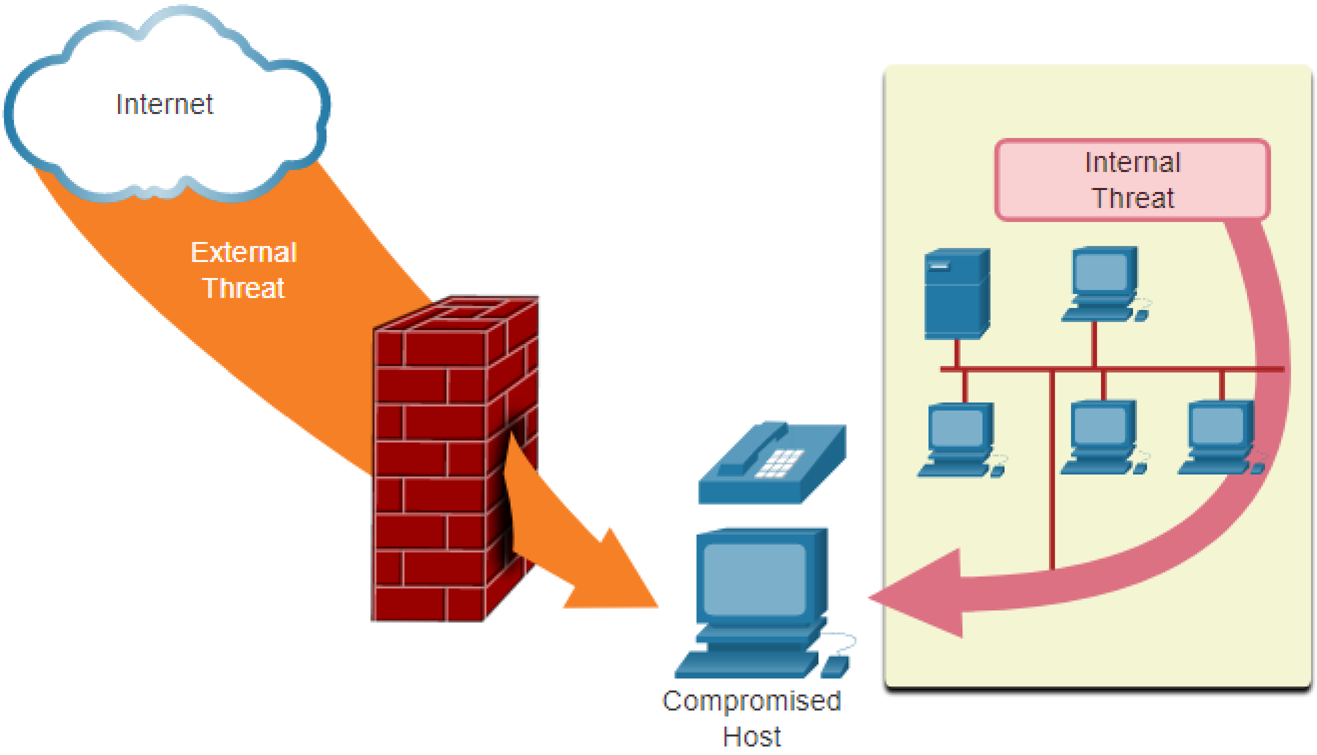
Radio link types:

- terrestrial microwave
  - e.g. up to 45 Mbps channels
- LAN (e.g., WiFi)
  - 11Mbps, 54 Mbps
- wide-area (e.g., cellular)
  - 3G cellular: ~ few Mbps
- satellite
  - Kbps to 45Mbps channel (or multiple smaller channels)
  - 270 msec end-end delay
  - geosynchronous versus low altitude

Network Security

- Field of Network Security:
  - How bad guys can attack computer networks
  - How we can defend networks against attacks
  - How to design architectures that are immune to attacks
- Internet not originally designed with (much) security in mind
  - *Original vision:* "a group of mutually trusting users attached to a transparent network" ☺
  - Internet protocol designers playing "catch-up"
  - Security considerations in all layers!

Security Threats



CCNAv7.0, Section 1.8

Bad guys: put Malware into Hosts via Internet

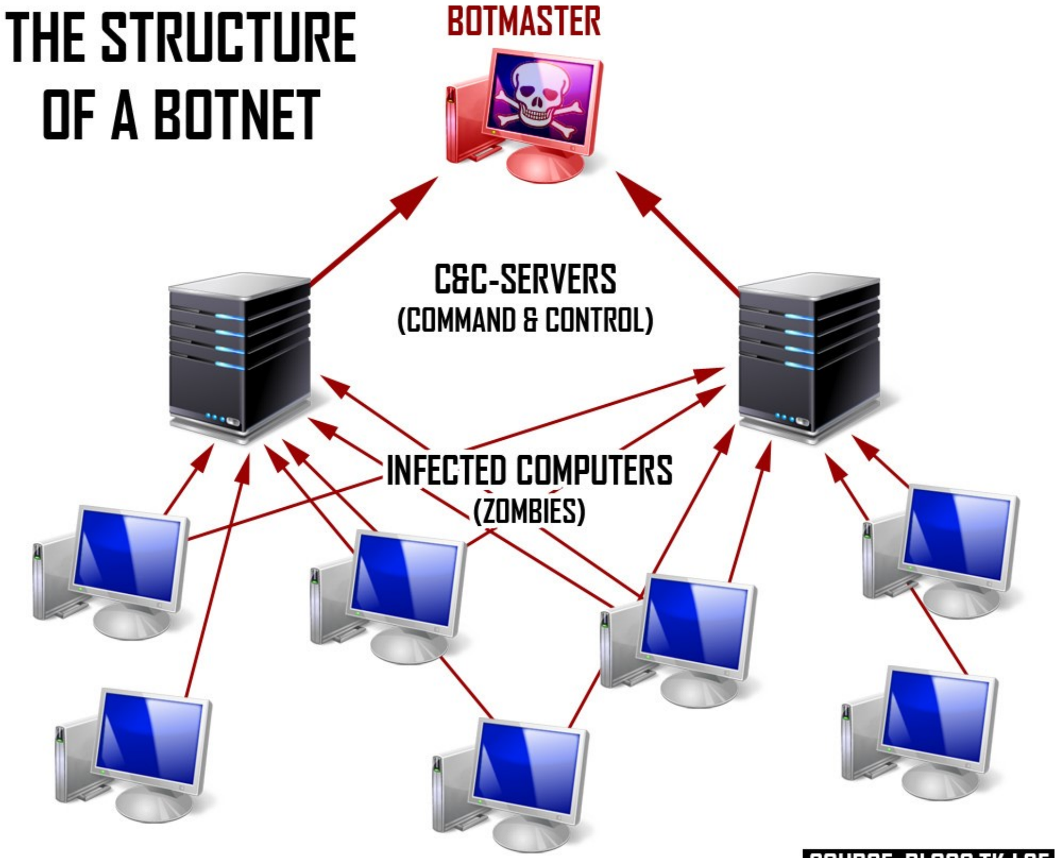
- Malicious stuff—collectively known as *Malware*—that can also enter and infect our devices.
- Malware can get in host from:
  - *Virus:* self-replicating infection by receiving/ executing object
    - Viruses attach themselves to clean files and infect other clean files.
    - They can spread uncontrollably, damaging a system's core functionality and deleting or corrupting files.
    - They usually appear as an executable file (e.g. e-mail attachment).

Bad guys: put Malware into Hosts via Internet

- *Worm:* self-replicating infection by passively receiving object that gets itself executed
  - Worms are malware that can enter a device without any explicit user interaction.
  - Example: Michelangelo
- Spyware: designed to spy on you.
  - It hides in the background and takes notes on what you do online, including your passwords, credit card numbers, surfing habits and more.
  - Can record keystrokes, web sites visited, upload info to collection site
  - Example: CoolWebSearch, Gator

Bad guys: put Malware into Hosts via Internet

- Adware: advertising malware
  - Though not always malicious in nature, particularly aggressive advertising software can undermine your security just to serve you ads — which can give a lot of other malware a way in.
  - Pop-ups are really annoying (admit!).
- Botnets: Botnets are networks of infected devices that are made to work together under the control of an attacker.
  - Users are often unaware of a botnet infecting their system.
  - Example: 'Star Wars' Twitter Botnet



SOURCE: BLOGG.TKJ.SE

Bad guys: put Malware into Hosts via Internet

- Trojans: This kind of malware disguises itself as legitimate software, or is included in legitimate software that has been tampered with.
  - It tends to act discretely and create backdoors in your security to let other malware in.
  - Types: Backdoor, Exploit, rootkit ...
- Ransomware: Also called *scareware*.
  - Can lock down your computer and threaten to erase everything — unless a ransom is paid to its owner.
  - Cryptolocker, Bad rabbit

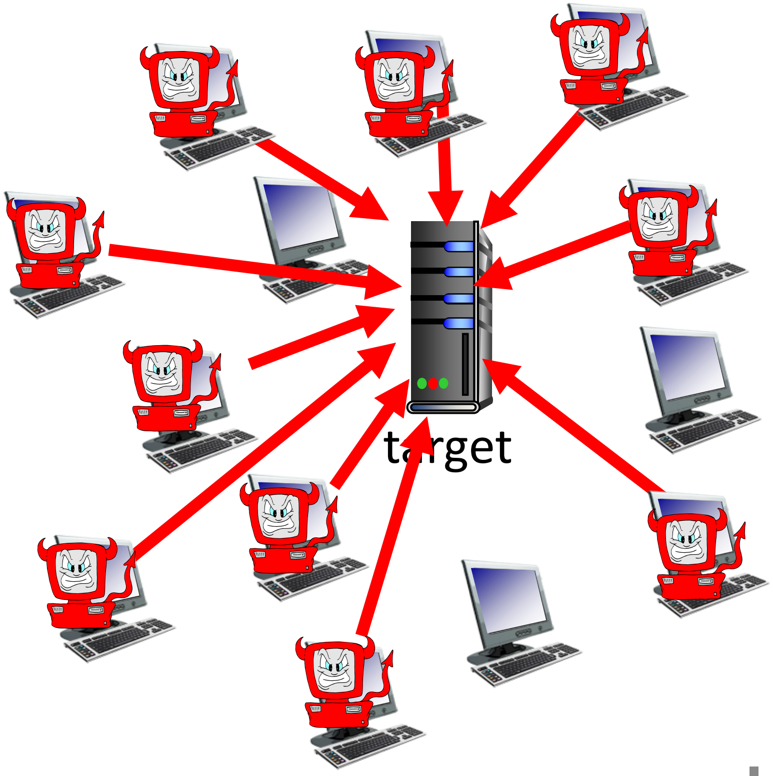
Bad guys: attack server, network infrastructure

Denial of Service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target
2. break into hosts around the network (see botnet)
3. send packets to target from compromised hosts

Distributed Denial of Service (DDoS):

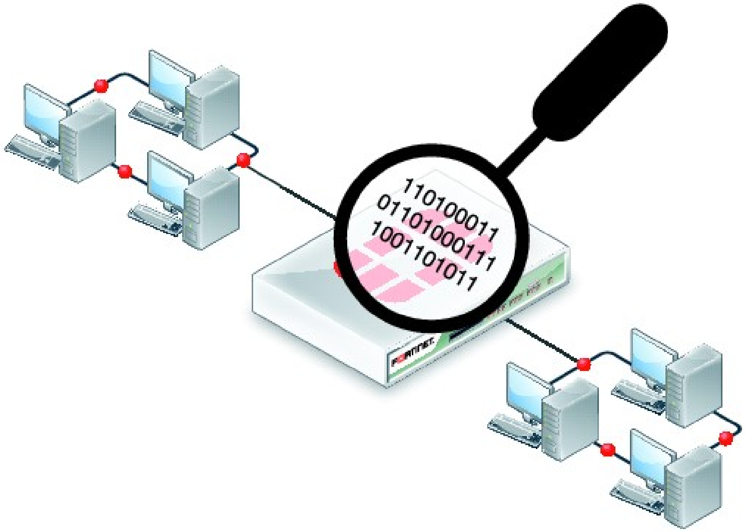
A Distributed Denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers



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
- a packet sniffer is a program that can see all traffic flowing over the network back and forth.



Bad guys can masquerade as someone you trust

- *IP spoofing:* send packet with fake addresses
  - The ability to inject packets into the Internet with a false source address is known as IP spoofing, and is but one of many ways in which one user can masquerade as another user.

Security Solutions

- No single solution can protect the network.
- Should implemented in multiple layers.
- A home network security implementation - Basic.
- Implement it on the end devices, router and put trust on ISP.
- Basic security components for a home or small office network:
  - **Antivirus and antispyware** - These applications help to protect end devices from becoming infected with malicious software.
  - **Firewall filtering** - Firewall filtering blocks unauthorized access into and out of the network. This may include a host-based firewall system that prevents unauthorized access to the end device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

Security Solutions

Network security implementation for a corporate network or larger networks

- Consists of many components built into the network to monitor and filter traffic.
- Use antivirus, antispyware, and firewall filtering, but they also have other security requirements:
  - **Dedicated firewall systems -** filter large amounts of traffic with more granularity.
  - **Access control lists (ACL) -** filter access and traffic forwarding based on IP addresses and applications.
  - **Intrusion prevention systems (IPS) -** These identify fast-spreading threats, such as zero-day or zero-hour attacks.
  - **Virtual private networks (VPN) -** These provide secure access into an organization for remote workers.