

Unit 3: Networks

Network types

acronym	definition
PAN	Personal area network: The devices around your person communicating with each other. Commonly utilizing Bluetooth. Devices include phone, watch, fitness device, possibly a laptop or hotspot.
LAN	Local area network: The devices within your property communicating with each other, eg within the home, on the school campus, the office building. Commonly using wireless or hard wired Ethernet cabling.
VLAN	Virtual local area network: For security and organisational reasons, typically larger organisations will split their LAN into several VLANs. For instance, the school might have a Students VLAN and a Staff VLAN, each of which grant access to different files/resources on the network
WLAN	Wireless local area network. Same as a local area network but just utilizing wireless technologies. Eg: what you, the students, get to enjoy here at school ;-)
MAN	Metropolitan area network. Yeah... a bit ambiguous... when is it a MAN and when is it a WAN? You tell me then we'll both know :-p MAN is limited to a metropolitan geographical region.
WAN	Wide area network. Multiple properties connected together over a long distance connection, most commonly fibre optic cable. Could be a MAN, could also be interstate, intercontinental etc.
SAN	Storage area network: Network based storage
VPN	Virtual private network: Establishing a connection to a remote network but granted access as if you are physically present. Discussed further later
Internet	Ummm... the internet!
Extranet	Extranet: Authenticated & authorised access via the public internet to secure services hosted by a network, eg: logging on to your banks website

Network topologies

Topologies may be used to describe the physical or logical layout/structure of a network. The names are fairly loose definitions, most networks these days are a blend of these traditional topologies.

- Point to point
- Bus
- Star
- Ring
- Mesh
- Tree
- Fully connected
- Hybrid

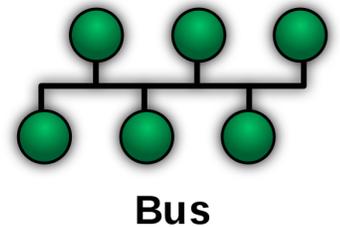
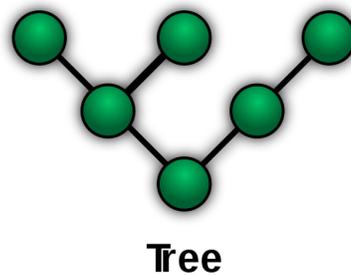
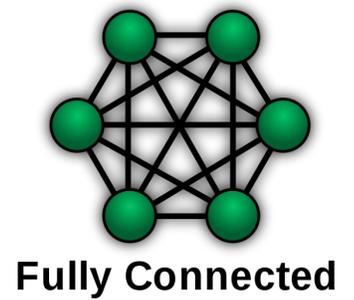
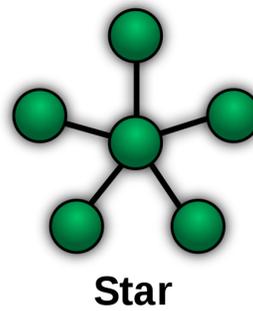
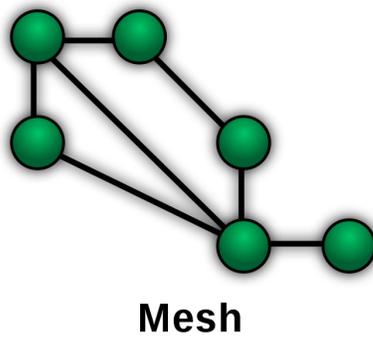
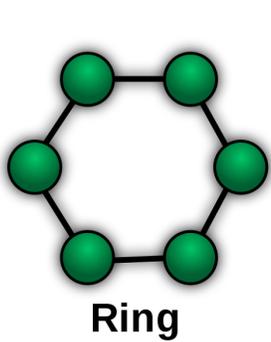


Image: NetworkTopologies.png: Maksimderivative work: Malyszcz [Public domain], via Wikimedia Commons

The need for standards

Standards ensure compatibility

Define protocol

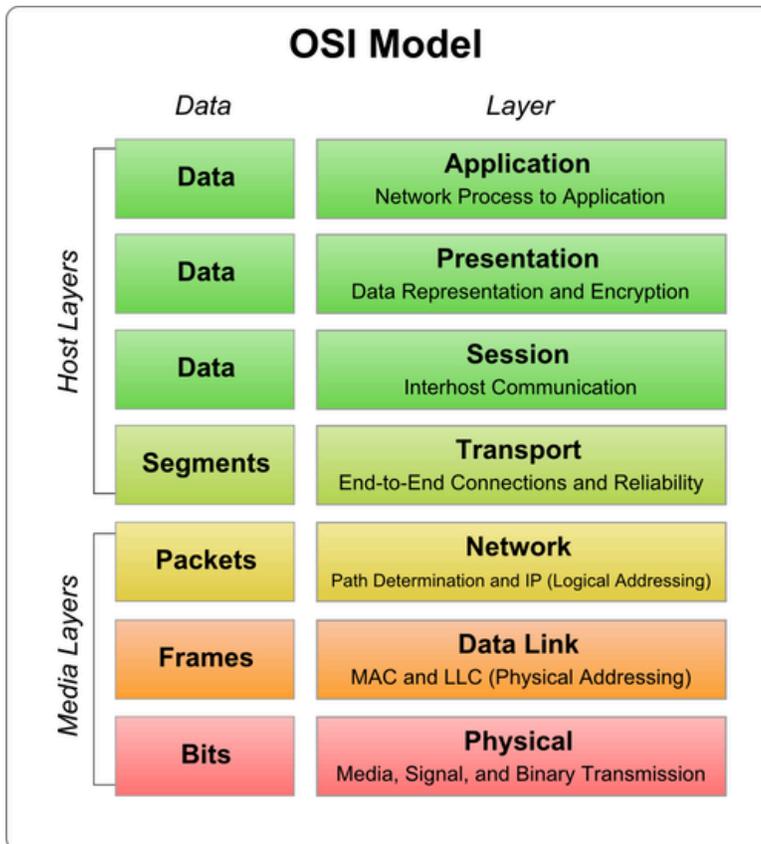
Roles: data integrity, flow control, deadlock resolution, congestion, error checking

Standards in networking are recorded in documents known as RFCs (request for comment).

- RFC 761 Transmission Control Protocol - <ftp://ftp.rfc-editor.org/in-notes/rfc761.txt>
- RFC 791 Internet Protocol - <ftp://ftp.rfc-editor.org/in-notes/rfc791.txt>
- RFC 2616 Hypertext Transfer Protocol 1.1 - <ftp://ftp.rfc-editor.org/in-notes/rfc2616.txt>
- [Partial list of RFCs on Wikipedia](#)

Layers of network communication

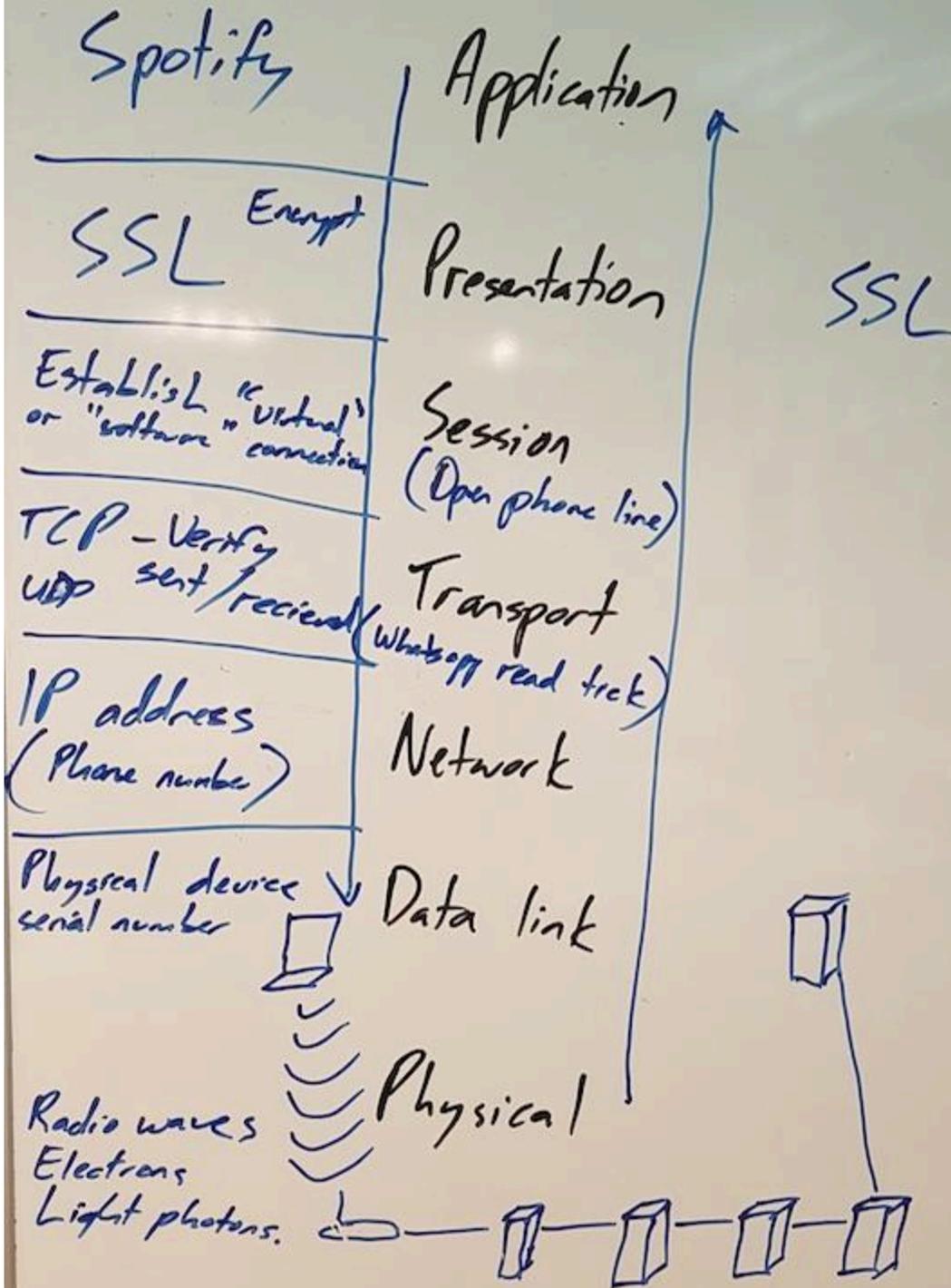
The layers of network communication is known as the OSI (open systems interconnect) model. Each layer has a range of protocols that are commonly used.



An example of the different layers in action between the Spotify App on your device, and Spotify HQ.

You

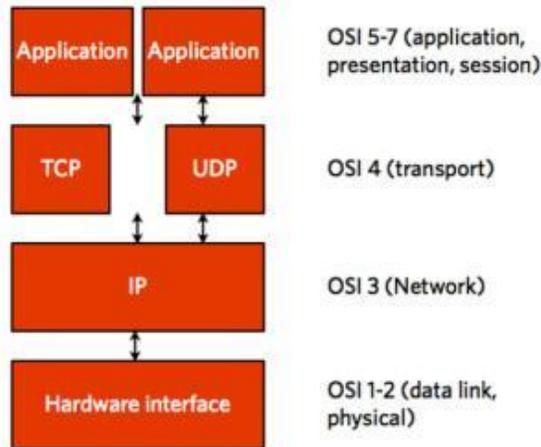
Spotify HQ



The TCP/IP stack

TCP/IP is an amalgamation of two protocols: TCP (transport control protocol) and IP (internet protocol).

TCP/IP stack



- Linus' Techquickie, 2016, What is TCPIP? https://www.youtube.com/watch?v=PpsEaqjV_A0

Protocols: TCP & UDP

Layer: Transport

TCP and UDP are transport layer protocols, responsible for **packet switching and delivery**.

Both TCP and UDP are protocols used for sending bits of data – known as packets – over the Internet. They both build on top of the Internet protocol. In other words, whether you are sending a packet via TCP or UDP, that packet is sent to an IP address. These packets are treated similarly, as they are forwarded from your computer to intermediary routers and on to the destination

TCP (Transport Control Protocol) guarantees the recipient will receive the packets in order by numbering them. The recipient sends messages back to the sender saying it received the messages. If the sender does not get a correct response, it will resend the packets to ensure the recipient received them. Packets are also checked for errors. TCP is all about this reliability

UDP (User Datagram Protocol) just sends packets to the recipient. The sender will not wait to make sure the recipient received the packet – it will just continue sending the next packets. If you are the recipient and you miss some UDP packets, too bad – you can not ask for those packets again. There is no guarantee you are getting all the packets and there is no way to ask for a packet again if you miss it, but losing all this overhead means the computers can communicate more quickly. UDP is used when speed is desirable and error correction is not necessary. For example, UDP is frequently used for live broadcasts and online games.

A TCP joke:

Hello, would you like to hear a TCP joke?
Yes, I'd like to hear a TCP joke.
OK, I'll tell you a TCP joke.
OK, I'll hear a TCP joke.
Are you ready to hear a TCP joke?
Yes, I am ready to hear a TCP joke.
OK, I'm about to send the TCP joke. It will last 10 seconds, it has two characters, it does not have a setting, it ends with a punchline.
OK, I'm ready to hear the TCP joke that will last 10 seconds, has two characters, does not have a setting and will end with a punchline.
I'm sorry, your connection has timed out... ...Hello, would you like to hear a TCP joke?
A UDP joke:

I know a UDP joke, but you might not get it.
Credits:

- <https://www.howtogeek.com/190014/htg-explains-what-is-the-difference-between-tcp-and-udp/>
- Image: Oddbodz [CC BY-SA 3.0], from Wikimedia Commons

Protocol: IP

Layer: Network

The Internet Protocol (IP) is the method or protocol by which a packet of data is sent from one computer to another on the Internet. A packet is a small amount of data sent over a network. Similar to a real-life package, each packet includes a source and destination as well as the content (or data) being transferred. When the packets reach their destination, they are reassembled into a single file or other contiguous block of data.

So while the Internet Protocol is most well known for being the basis of the "IP address", the Internet Protocol is more than just addresses. It governs the structure of the actual data payload (the actual information being sent) and all the associated information that packet needs to get from one computer to another (the IP addresses being part of that).

There are currently three different ways the Internet Protocol is being used on the internet

- IP version 4
- IP version 4 with NAT (network address translation)
- IP version 6

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,920,938,463,463,374,607,431,768,211,456$

While the exact structure of a packet varies between protocols, a typical packet includes two sections – a header and payload. Information about the packet is stored in the header.

For example, an IPv6 header includes the following fields:

- Source address (128 bits) – IPv6 address of the packet origin
- Destination address (128 bits) – IPv6 address of the packet destination
- Version (4 bits) – "6" for IPv6
- Traffic class (8 bits) – priority setting for the packet
- Flow label (20 bits) – optional ID that labels the packet as part of a specific flow; used to distinguish between multiple transmissions from a single origin
- Payload length (16 bits) – size of the data, defined in octets
- Next header (8 bits) – ID of the header following the current packet; may be TCP, UDP, or another protocol
- Hop limit (8 bits) – maximum number of network hops (between routers, switches, etc) before the packet is dropped; also known as "TTL" in IPv4

The payload section of a packet contains the actual data being transferred. This is often just a small part of a file, webpage, or other transmission, since individual packets are relatively small. For example, the maximum size of an IP packet payload is 65,535 bytes, or 64 kilobytes. The maximum size of an Ethernet packet or "frame" is only 1,500 bytes or 1.5 kilobytes.

Explainer:

- Linus' Techquickie, 2014, Internet Protocol – IPv4 vs IPv6 as Fast As Possible <https://www.youtube.com/watch?v=aor29pGhIFE>

Credits:

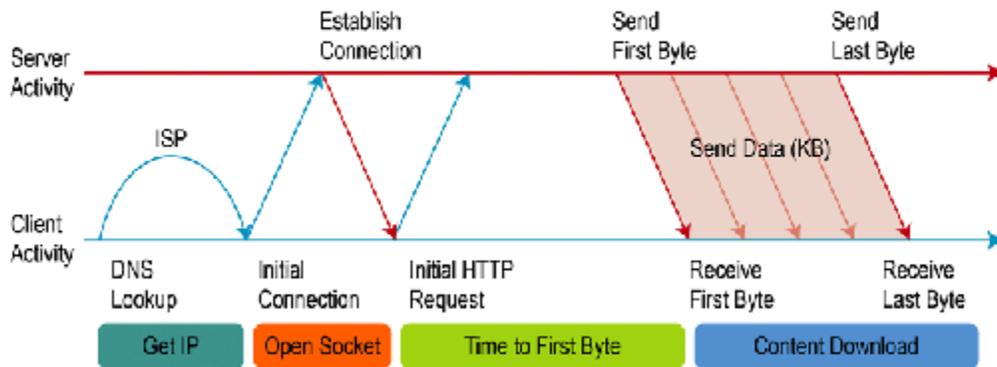
- Image: <https://phoenixts.com/blog/ipv6-vs-ipv4/>
- <http://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol>
- <https://techterms.com/definition/packet>

Protocol: HTTP

Layer: Application

Let's take a closer look at one common protocol, HTTP

The HTTP Request

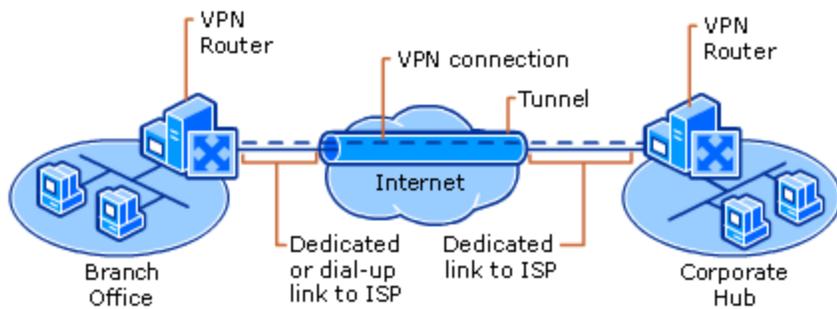


Other Protocols

Some other protocols that are useful to have an understanding of are:

- SSL v TLS
 - HTTP
 - HTTPS
 - IPv4, IPv6
 - DNS
 - DHCP
-

VPNs (Virtual Private Networks)



A VPN (virtual private network), is a software tool that provides an encrypted "tunnel" over the open internet for you to connect and interact with a remote network as if you were physically and presently connected to it.

An extranet is a range of services a network makes available for clients to access externally. They are not treated (granted the privileges) as if they were physically present on the LAN.

What is a VPN? We'll let Linux explain,

- Linus' Techquickie, 2015, VPNs or Virtual Private Networks as Fast As Possible <https://www.youtube.com/watch?v=DhYeqqufYss>
- Text: p145-148

VPN properties

- VPN authenticates the sender before (establishing the tunnel)
- VPN access is always encrypted, whereas an extranet may have limited encryption
- VPN transmission is always encrypted
- VPN users have access to everything whereas extranet users only have access to (enabled) specific services

VPN security features:

- Authentication
- Encryption
- Tunneling
- Multiple exit nodes

Evaluate VPNs

Why network speeds can vary

- Factors affecting transmission rates (bandwidth, transfer rates of storage devices, interference, number of devices, malware, packet loss, security processes, transmission media)

- Denial of service attacks
-

Compression

- The need for compression
- Compression: Lossy (jpg, mp3, mp4), lossless
- Tom Scott (Why Snow and Confetti Ruin YouTube Video Quality) 4m <https://www.youtube.com/watch?v=r6Rp-uo6Hml>

Class exercise: How does loss-less compression work?

Demonstration:

how much wood could a woodpecker peck, if a woodpecker could peck wood!

Your turn:

she sells sea shells by the sea shore. the shells she sells are surely seashells. so if she sells shells on the seashore, i'm sure she sells seashore shells.

By the way, my current record holder is Chetan from my 2018 class who compressed the 157 characters to 70 including the dictionary. That's 44.5% of original size. Can you beat his record?

Huffman coding and huffman trees

- [Tom Scott Basics: Huffman coding and huffman trees](#) (6:30)
-

Characteristics of transmission media

- Media: Wires (copper, coaxial, utp), wifi (microwave, infrared, sat, bluetooth), fibre
- The Internet: Wires, Cables & Wifi (code.org) <https://www.youtube.com/watch?v=ZhEf7e4kopM>
- Compare Coax, Twisted pair & Fibre (4:30m) <https://www.youtube.com/watch?v=EOCme3sNqws>
- Coaxial cabling – Speeds of up to 10Mbps over 300m
- Twisted pair cabling – Speeds of up to 1000Mbps over 100m though is typically running at speeds of 100Mbps in most installations.
- Optical cabling – Speeds of up to 40,000Mbps over many kilo metres (speeds of up to 1Tbps are under development!)
- Wireless – Currently offering speeds of up to 50Mbps over 90m (Also known as 802.11)
- HSDPA – The 3G mobile phone broadband network offering speeds of 3Mbps over about a kilometre (ie: to the phone tower)
- Satellite – Speeds ranging from 1 to 40Mbps shared over all users in the region. Weather (especially rain) will slow the signal significantly. Latency becomes a significant issue – 500 to

900 milliseconds. Geostationary satellites are 35,000Kms high in orbit! That's a lot of distance for the signal to travel. What uses would be affected by this kind of latency?

The Internet: Wires, Cables & Wifi

(code.org) <https://www.youtube.com/watch?v=ZhEf7e4kopM> Compare Coax, Twisted pair & Fibre (4:30m) <https://www.youtube.com/watch?v=EOCme3sNqws>

Wireless networking

Advantages & disadvantages of wireless networks

Discuss in relation to:

- Changes in work patterns
- Social activities
- Health issues, concerns

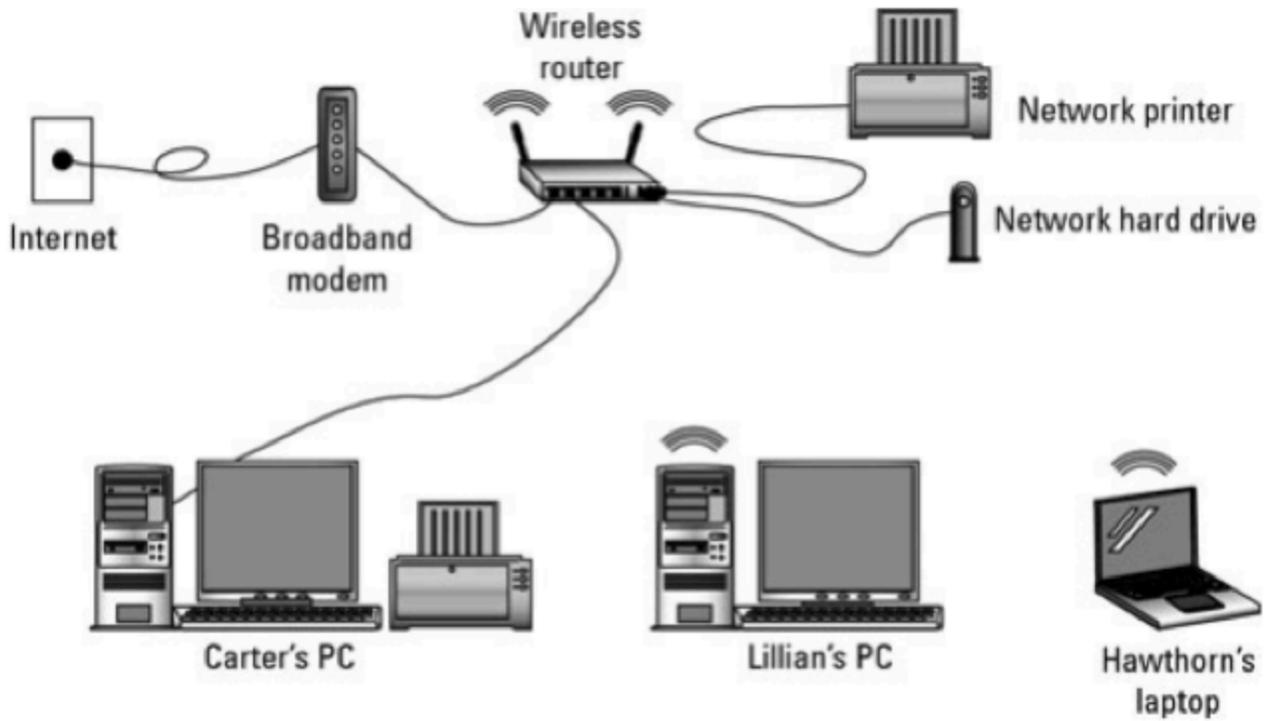
Some positives

- Freedom of movement
- Less infrastructure (no expensive cable runs)
- (Usually) easier to setup
- More devices per uplink

Some negatives

- Slower (shared bandwidth)
 - Range
 - Susceptible to interference and jamming
 - Vulnerable to eavesdropping
 - An increasing number of devices are wireless only
-

Components of wireless networks



- Modem
 - Router, wireless router
 - Wireless NIC for each device
 - Wireless antennas
 - Wireless repeater
-

Characteristics of wireless networks

802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Mobile Wireless Networks - Evolution



GRANDMETRIC
NETWORK & WIRELESS... STAY CONNECTED.

- 802.11 B, G, N, A
- Mobile wireless internet: 2G, 3G, 4G
- LTE
- WiMax

History nerd time: Where does the name 802.11 come from?

Credits:

- 802.11 image: <http://www.l-com.com/content/Article.aspx?Type=N&ID=10638>
 - Mobile networks
image: <https://www.quora.com/What-are-the-differences-between-1G-2G-3G-4G-and-5G>
-

Security

- The Internet: Cybersecurity & Crime (Code.org) https://www.youtube.com/watch?v=AuYNXgO_f3Y
- Wireless security (Google.com) <https://www.youtube.com/watch?v=j9rKM5ShvV8>

Key issues to discuss:

- symmetric key encryption vs public-key encryption
- passwords
- firewalls
- passwords on wifi access points, routers
- enable/disable ssid broadcast
- enable/disable access by mac address
- WEP, WPA, WPA2, WPA3 wireless encryption protocols - *is WPA2 "broken"?*
- WPS (wireless protected setup)
- controlling physical access

Advantages and disadvantages of network security methods

- Computer Science Core (p161-170)
-

Review questions

- Computer Science Illuminated by Nell Dale & John Lewis (page numbers based on 6th edition):
- End of chapter 15 (page 526), exercises 16-64