Wired vs WIRELESS SECURITY

Outlines:

- Differences between Sired and Wireless
- Differences based on Security
- Wireless Security:
  - Shared key authentication
  - Key Authentication
  - Wi-Fi Protected Access (APA)

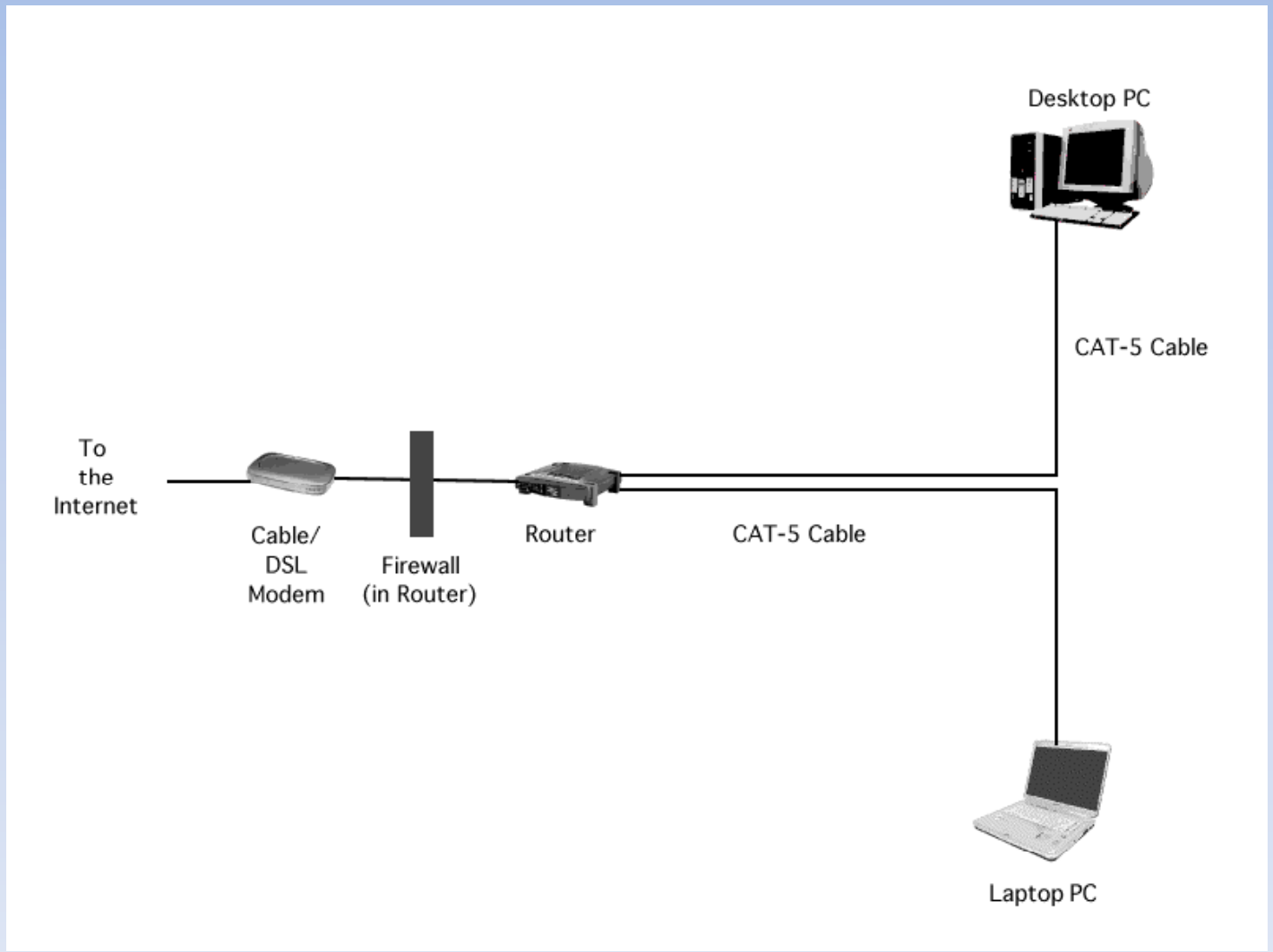
By: Arash Habibi Lashkari
July - 2010

what is the difference between a wired LAN (Local Area Network) and a wireless LAN?

Wired LAN

- Devices being networked
  - Include desktop computers, laptop computers, printers, servers, PDAs, video game systems, even TV and stereo systems
- Devices for connecting the above
  - Include network adapters, hubs, switches, routers, gateways and more
- Connecting medium
  - Networking cable; most common is Category 5 or CAT-5 for short

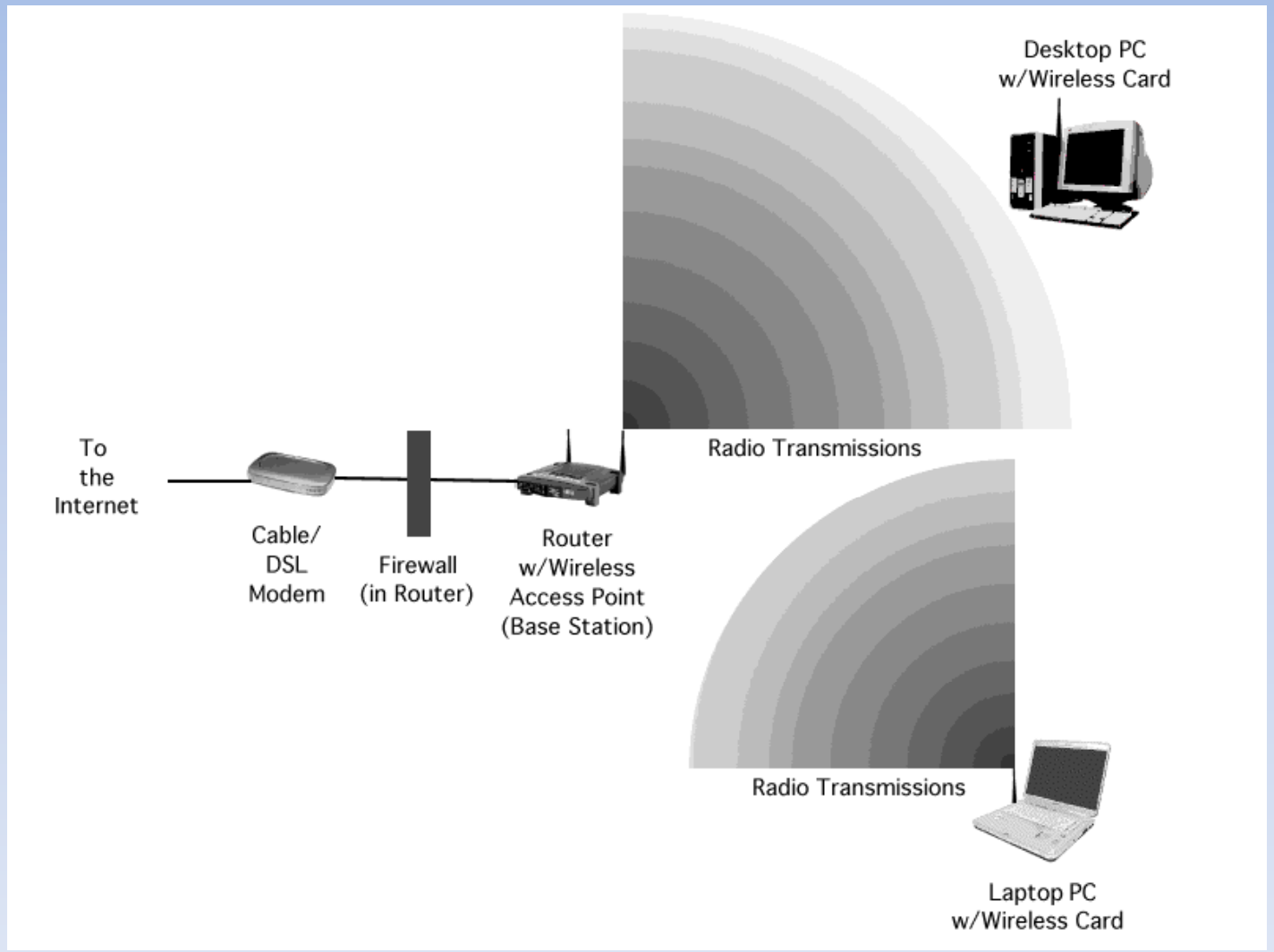
Simple home wired LAN



Wireless LAN

- Devices being networked (same as for wired)
  - Include desktop computers, laptop computers, printers, servers, PDAs, video game systems, even TV and stereo systems
- Devices for connecting the above
  - Include wireless adapters, access points, bridges, base stations and more
- Connecting medium
  - Radio waves; per Einstein, there is no CAT-5

Simple home wireless LAN



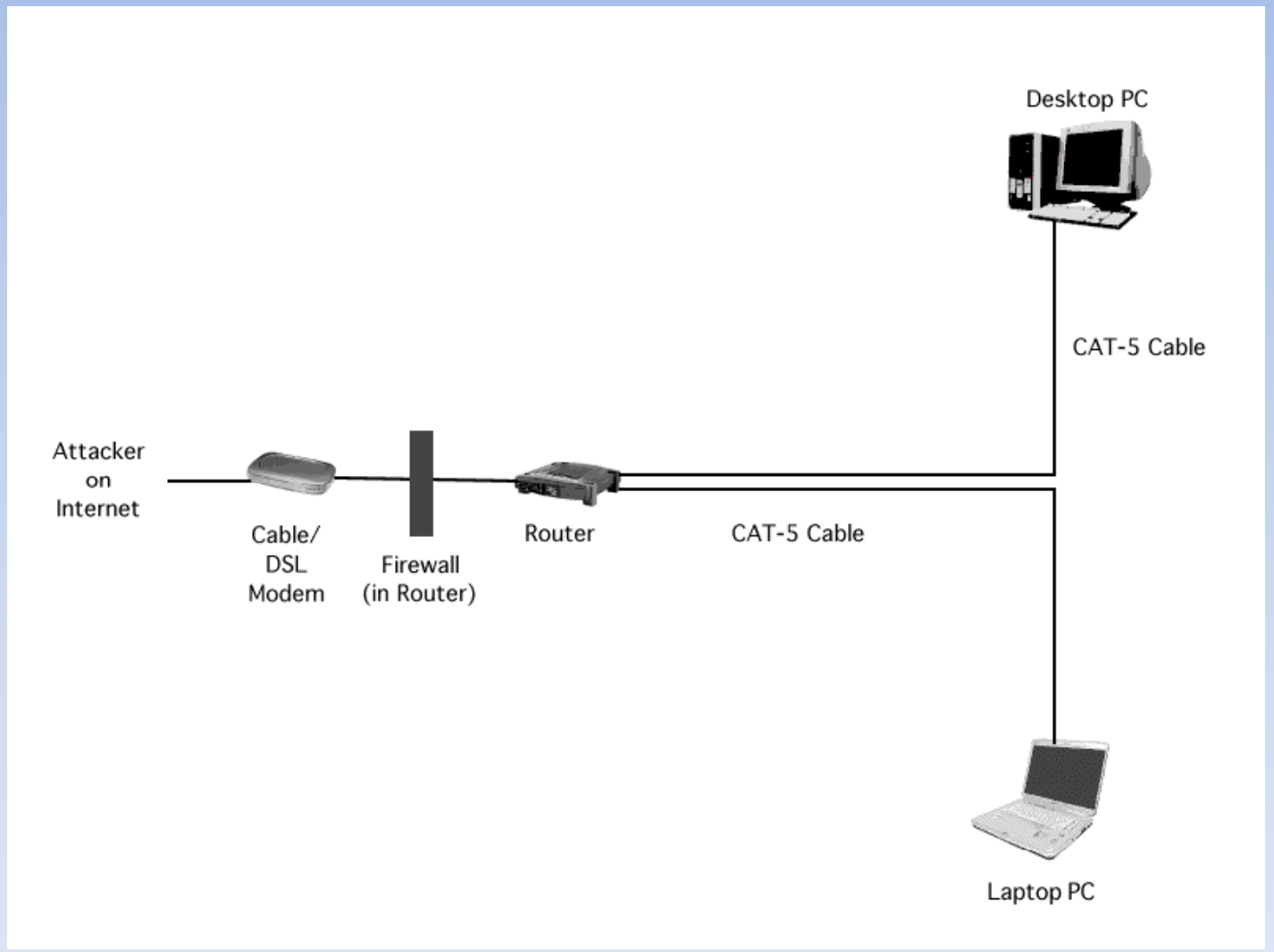
Securing your home LAN

Preventing (or limiting)
attacks against your network

Wired LAN outside attacks

- Must come in through Internet Gateway
- Attacks workstations and servers on the network
- Can be prevented by:
  - Installing a firewall (hardware and/or software)
    - This is often done on the Internet gateway
  - Turning off (or limiting) file-sharing and remote access

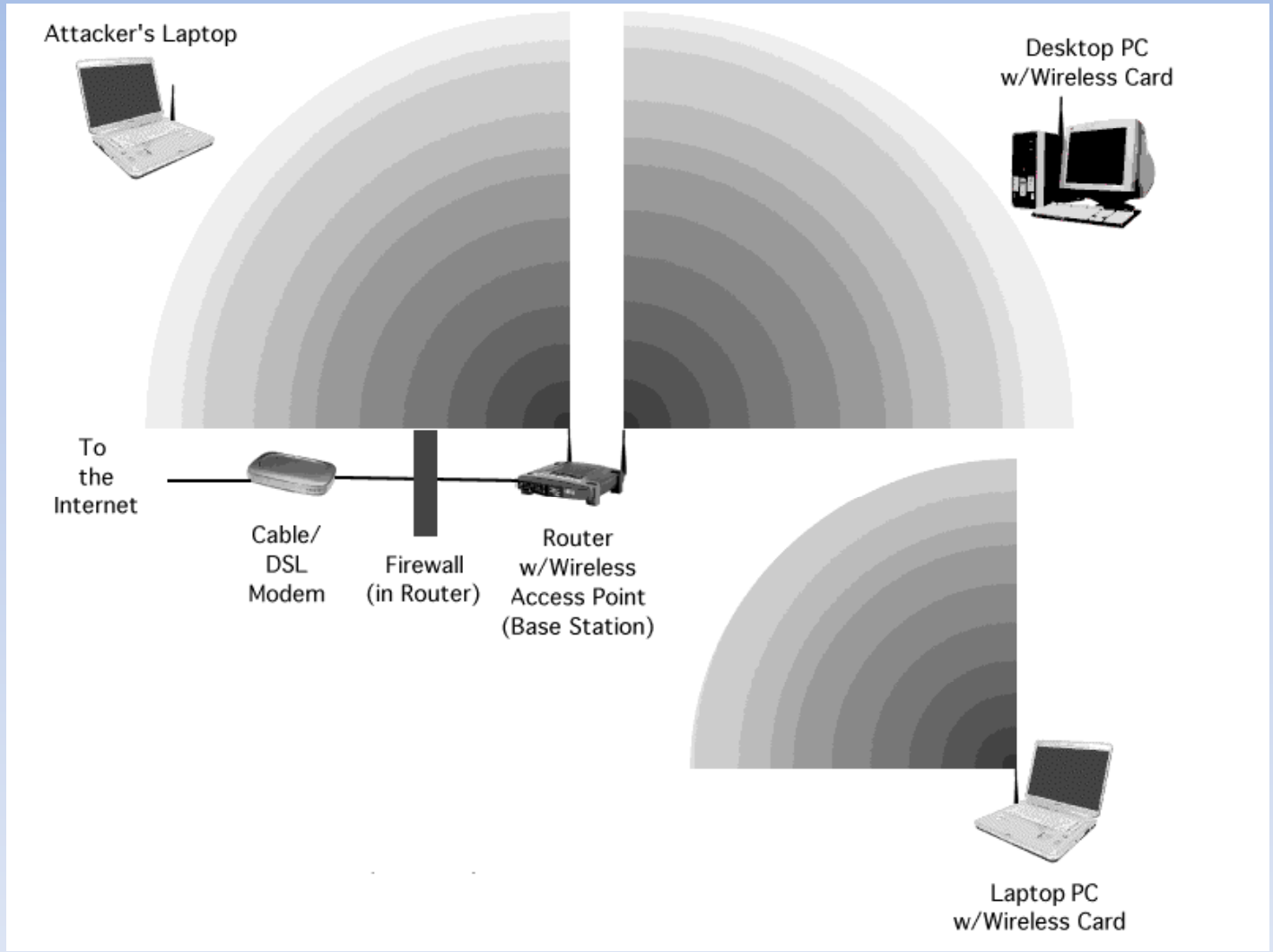
Wired LAN attack blocked by firewall



Wireless LAN outside attacks

- Even if you have a firewall installed on your Internet gateway, a wireless LAN attacker is, effectively, already inside your network
  - Wireless base station has to signal its existence so clients can connect
- Attackers of wireless LANs therefore need to be kept out by other means in addition to firewalls

Wireless attacker is inside firewall!



Wired vs Wireless

Wired networks

✓ Can't intercept signals down the wire; high-security
✓ Immensely high speeds (depending on cable and hardware)
✓ Incredibly long cables are still really cheap
✓ Plug and play; usually no faffing around with settings, instant-on
x Cable can be damaged

Wireless networks

✓ Convenient, allows freedom of working anywhere
✓ Less/no cables; more people connecting to one access point
x Limited signal range; speed decreases the further away you go
x Signals can be intercepted; low security
x Signals affected by other signals and radio waves
x Speed not as fast as wired networks

Wired vs Wireless Confidentiality

Wireless Confidentiality

Making an unauthorized copy of packets on the network allows an intruder to breach confidentiality. Wireless networks broadcast packets in radio waves that can be received by anyone. Wireless networks must encrypt packets to keep them secure. Wired Equivalent Privacy, or WEP, can easily be broken and should be avoided. Wi-Fi Protected Access, or WPA, is far superior to WEP and should be used whenever possible.

Wired Confidentiality

An intruder must have physical access to a wired network in order to copy information from the network. Access controls are usually good enough to prevent unauthorized snooping of packets on a wired network. Encryption is possible, but less frequently used on wired networks.

Wired vs Wireless Access Controls

Wireless Access Controls
Wireless networks require that a user know the name of the network, called the Service Set Identifier, or SSID, and the WPA passphrase. If the WPA passphrase is kept secret, unauthorized users cannot gain access to the network.

Wired Access Controls
Unauthorized access in wired networks can have additional controls by using IEEE 802.1x Port-Based Network Access Control. This requires a user enter a password when a computer is physically connected to the network. It is possible to use 802.1x on wireless networks, but it is not a common practice.

Wired vs Wireless

Wired networks

✓ Can't intercept signals down the wire; high-security
✓ Immensely high speeds (depending on cable and hardware)
✓ Incredibly long cables are still really cheap
✓ Plug and play; usually no faffing around with settings, instant-on
x Cable can be damaged

Wireless networks

✓ Convenient, allows freedom of working anywhere
✓ Less/no cables; more people connecting to one access point
x Limited signal range; speed decreases the further away you go
x Signals can be intercepted; low security
x Signals affected by other signals and radio waves
x Speed not as fast as wired networks

Introduction to Wireless

Wireless networks broadcast their packets using radio frequency or optical wavelengths. A modern laptop computer can listen in, but also an attacker can manufacture new packets on the fly and persuade wireless stations to accept his packets as legitimate.

This presentation covers the following subjects:

- WLAN Overview – Basic Concepts
- The IEEE 802.11 Standards
- IEEE 802.11 Security Measures
- WEP Encryption and Related Attacks
- WPA Encryption and Related Attacks
- WPA 2 Encryption
- Wireless Networks Best Practices

Before we start...

Who is a hacker?

(originally) Someone who makes furniture with an axe!

From the Jargon Dictionary

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.
3. A person capable of appreciating hack value.
4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it or on it.
6. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.

Before we start...

Who is a hacker?

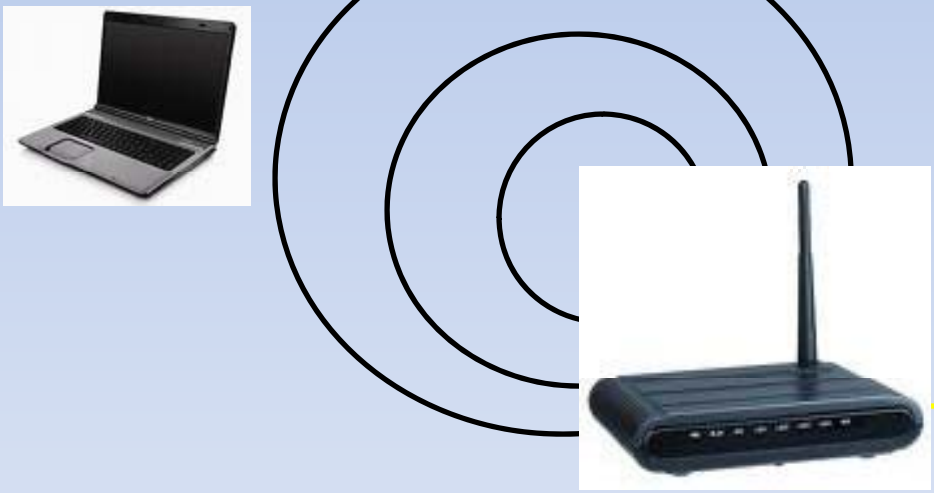
(originally) Someone who makes furniture with an axe!

From the Jargon Dictionary

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.
3. A person capable of appreciating hack value.
4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it or on it.
6. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.

WLAN Overview
Stations and Access Points

A wireless network interface card (adapter) is a device, called a **station**, providing the network physical layer over a radio link to another station.



An **access point (AP)** is a station that provides frame distribution service to stations associated with it.

The AP itself is typically connected by wire to a LAN.

WLAN Overview
MAC Address, SSID and Channels

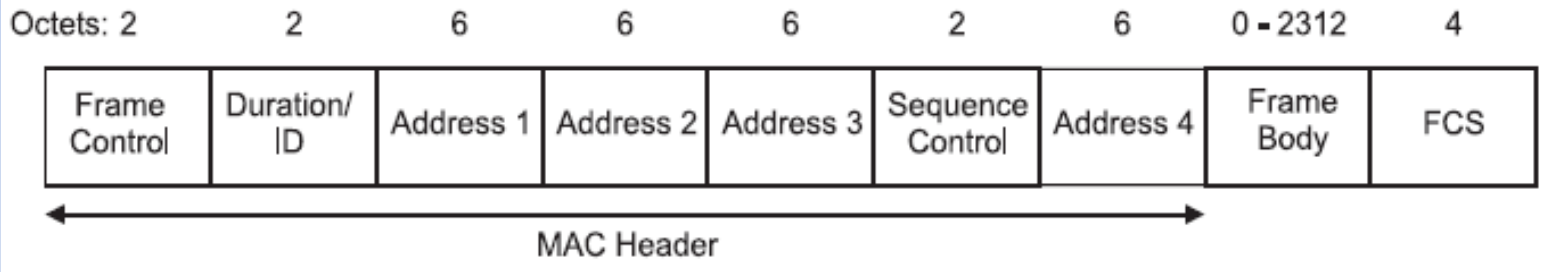
- Media Access Control (MAC) address:
  - The station and AP each contain a network interface that has a MAC address.
  - World-wide-unique 48-bit number.
  - Represented as a string of six octets separated by colons (00:02:2D:17:B9:E8).
  - Can be changed in software.

- Service Set Identifier (SSID):
  - Every AP has a SSID, which is used to segment the airwaves for usage.
  - If two wireless networks are physically close, the SSIDs label the respective networks and allow the components of one network to ignore those of the other.
  - It is possible that two unrelated networks use the same SSID.

- Channels
  - The stations communicate with each other using radio frequencies between 2.4 GHz and 2.5 GHz.
  - Neighboring channels are only 5 MHz apart.
  - Networks with neighboring channels may interfere with each other.

WLAN Overview
Frames

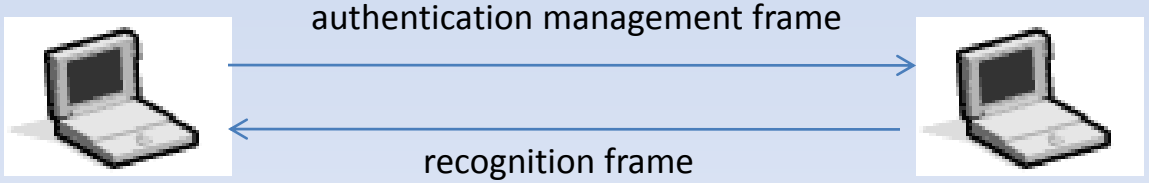
Both the station and AP radiate and gather 802.11 frames as needed.



WLAN Overview
Authentication

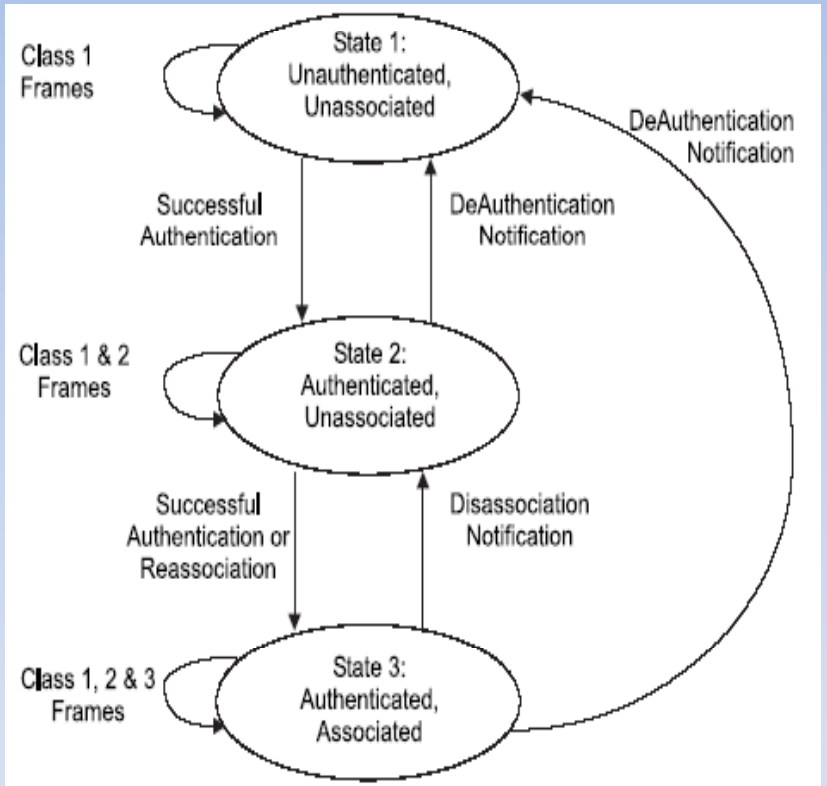
Authentication is the process of proving identity of a station to another station or AP.

- Open system authentication -> all stations are authenticated without any checking.
- Shared key authentication -> standard challenge and response along with a shared secret key.



WLAN Overview
Association

- Data can be exchanged between the station and AP only after a station is associated with:
  - an AP in the infrastructure mode
  - another station in the ad hoc mode.
- A station can be authenticated with several APs at the same time, but associated with at most one AP at any time.
- Association implies authentication.
  There is no state where a station is associated but not authenticated.



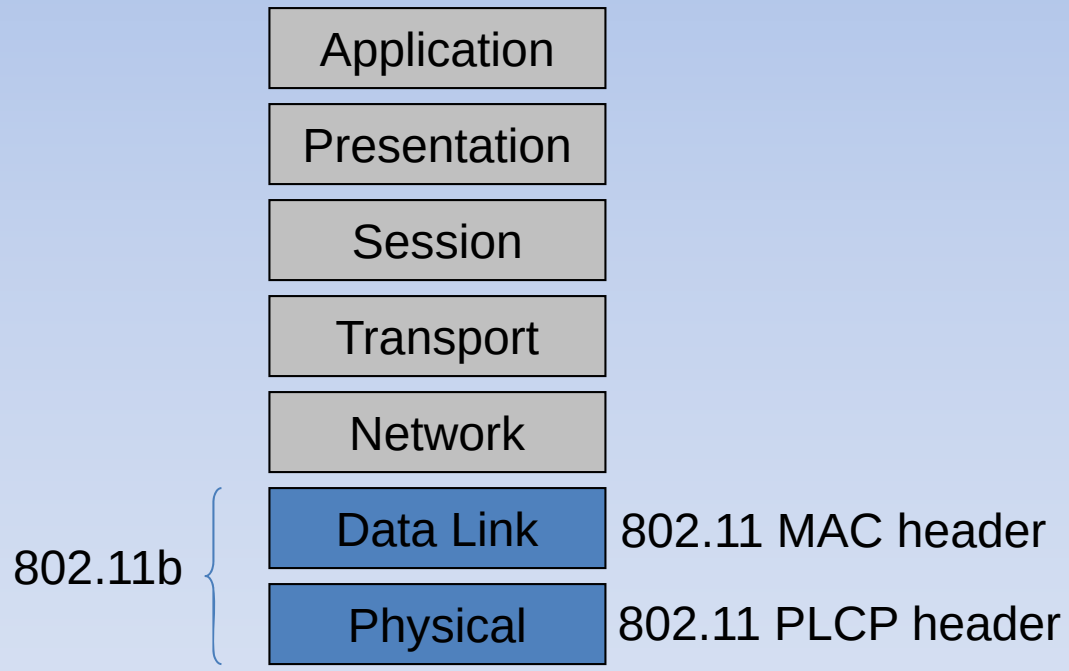
IEEE 802.11 Standards

IEEE 802 is a dominant collection of networking standards developed by IEEE.

IEEE 802.11 is a family of standards for wireless LANs.

- Baseline IEEE Std 802.11-1997 was approved in June 1997.
  - Offering 1 Mbps and 2Mbps rates.
  - Typical indoor range of 20m.
- 802.11b added 5.5 Mbps and 11 Mbps in 1999
  - range of 30-40m (indoor)
- 802.11g added 54 Mbps in 2002
  - range of 30-40m (indoor)
- 802.11n was published in October 2009.
  - Aiming for typical 75Mbps and maximum of 600Mbps
  - Range of 70m (indoor).
  - Products already available, based on draft standard.

IEEE 802.11 Standard in OSI Model



Security of IEEE 802.11 WLANs
Open System Authentication

- Relies on Service Set Identifier (SSID).
- Station must specify SSID to Access Point when requesting association.
- APs can broadcast their SSID as a beacon.
- Some clients allow * as SSID.
  - Associates with strongest AP regardless of SSID.

Security of IEEE 802.11 WLANs
SSID Hiding

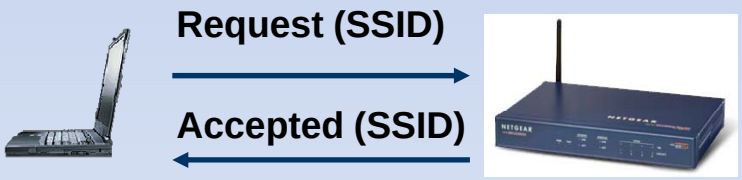
- AP can choose not to transmit SSID in its beacons.
- Can still attack APs that don't transmit SSID:
  - Send deauthenticate frames to client.
  - SSID then captured when client sends reauthenticate frames containing SSID.
- Open System Authentication only provides **trivial** level of security.
  - Even with SSID hiding.

Security of IEEE 802.11 WLANs
SSID Hiding

- 802.11b does not contain adequate authentication mechanisms. The two forms of authentication included with 802.11b are Open System Authentication (OSA) and Shared Key Authentication (SKA).

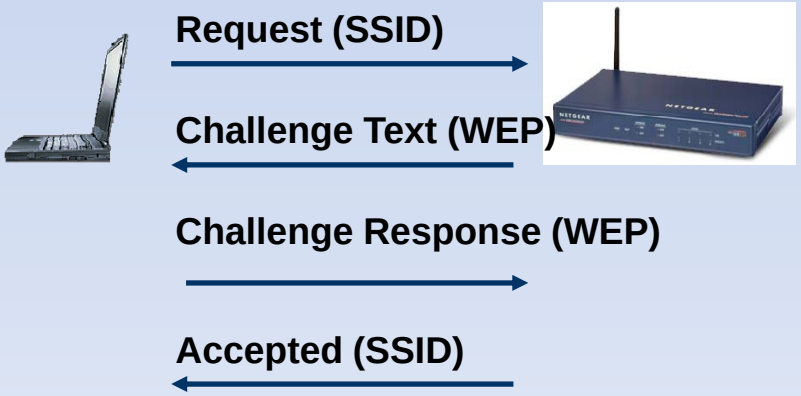
Open System Authentication

- **All you need is the SSID**
- **Negotiation is done in clear text**



Shared Key Authentication

- **SSID and WEP Encrypted key required**



Security of IEEE 802.11 WLANs
MAC Access Control Lists

- Access points may have Access Control Lists (ACLs).
- ACL is a list of allowed MAC addresses.
  - E.g. only allow access to:
    - 00:01:42:0E:12:1F
    - 00:01:42:F1:72:AE
    - 00:01:42:4F:E2:01
- But MAC addresses are sniffable and spoofable.
- Hence MAC ACLs are of limited value.
  - Will not prevent determined attacker.

Interception

- Wireless LAN uses radio signal.
- Not limited to physical building.
- Signal is weakened by:
  - Walls
  - Floors
  - Interference
- Directional antenna allows interception over longer distances.
  - Record is **124 miles** for an unamplified 802.11b signal (using a 4 metre dish).

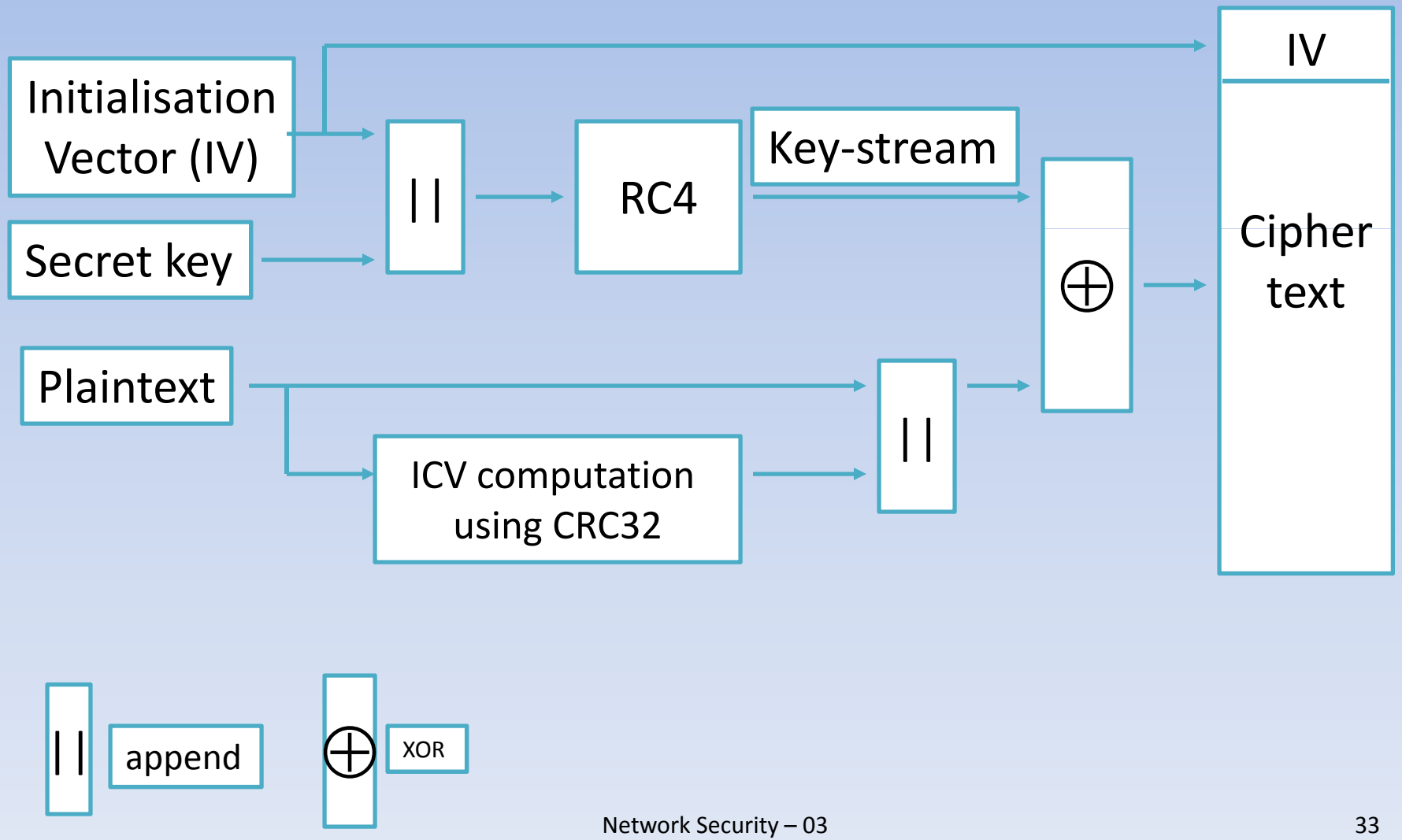
Directional Antennae

- Directional antenna provides focused reception.
- DIY plans available, using:
  - Aluminium cake tins
  - Chinese cooking sieves.

Wired Equivalence Privacy (WEP)

- Shared key between stations and an Access Point.
- Key used in stream cipher to encrypt WLAN traffic.
- Uses RC4 stream cipher
  - RC4 algorithm generates a stream of pseudo-random bits using key and Initialisation Vector (IV) as input.
  - RC4 is also used in the decryption of the ciphertext.
- Uses 32-bit Cyclic Redundancy Check (CRC32)
  - Basically a hash function
  - Used to compute Integrity Check Vector (ICV)

WEP Encryption



Shared Key Authentication (SKA)

- Station requests association with AP.
- AP sends challenge to station.
- Station encrypts challenge using WEP to produce response.
- Response received by AP, decrypted by AP and result compared to initial challenge. If they match AP sends a successful message and the station is authenticated.

WEP Safeguards

- Shared secret key required for:
  - Associating with an access point.
  - Sending data.
  - Receiving data.
- Messages are encrypted.
  - Confidentiality.
- Messages have checksum.
  - Intended to provide integrity.
- But has serious vulnerabilities…

Initialization Vector (IV)

- IV should be different for every message transmitted.
- But 802.11 standard doesn't specify how IV is calculated.
- Wireless cards use several methods:
  - Some use a simple ascending counter for each message.
  - Some switch between alternate ascending and descending counters.
  - Some use a pseudo-random IV generator.
- If 24-bit IV is an ascending counter, and if AP transmits at 11 Mbps, then all IVs are exhausted in roughly 5 hours!

Insecurity of SKA

- Rogue station records run of authentication protocol.
- Uses known plaintext (challenge) to compute portion of key-stream for the (known) IV.
  - C = P XOR key-stream.
- Rogue station can now respond to *any* future authentication challenge from AP encrypted with same key and same IV.
  - Rogue receives fresh challenge.
  - Wireless station gets to choose IV in protocol.
  - But same IV (and same secret key) means that RC4 produces the same key-stream bits.
  - Hence rogue who repeats IV can reuse old key-stream portion to encrypt, producing correct response

Wi-Fi Protected Access (WPA)

- The IEEE 802.11 community has responded to the many security problems identified in WEP.
- Intermediate solution: Wi-Fi Protected Access (WPA).
- Longer-term solution: WPA2.
- WPA and WPA2 are standardised in IEEE 802.11i
- Recently WPA has been cracked in just 60 seconds by Japanese researchers

Wi-Fi Protected Access (WPA)

- Wi-Fi Protected Access (WPA)
  - Works with 802.11b, a and g.
  - An intermediate solution to address WEP's problems.
  - Existing hardware can still be used; only firmware upgrade needed.
- WPA introduced new authentication protocol, improved integrity protection measure and per-packet keys.
  - To provide stronger authentication than in WEP.
  - To prevent spoofing attacks (i.e. bit flipping on WEP CRC).
  - To prevent FMS-style attacks.

Temporal Key Integrity Protocol (TKIP)

WPA introduced Temporal Key Integrity Protocol (TKIP).

- It is designed to be usable on already existing hardware by installing a new firmware.
- It is known to have several security weaknesses, but raises bar considerably compared to WEP.

TKIP Security Measures (I)

- A cryptographic message integrity code (MIC) is added to every packet before fragmentation.
  - Prevents attacks like fragmentation or chopchop, where fragments of a packet are rearranged or packets are modified
  - Protects the plaintext of the fragments to prevent an attacker from modifying the source or destination address of a packet.
- TKIP exchanges the per packet key completely after every single packet.
  - WEP changes only the first 3 bytes of the per packet key.

TKIP Security Measures (II)

- TKIP only allows a small number of messages where the CRC32 checksum is correct but the MIC is incorrect.
  - If more than two such messages are received by a station within a minute, TKIP is disabled for a minute and a renegotiation of the keys is suggested.
- A per packet sequence counter is used to prevent replay attacks.
  - If a packet is received out of order, it is dropped by the receiving station.
  - This prevents all kind of injection attacks where a packet is replayed.

WPA attacks

- Dictionary attack on pre-shared key mode
- Denial of service attack
  - If WPA equipment sees two packets with invalid MICs in 1 second, then:
    - All clients are disassociated.
    - All activity stopped for one minute.
    - So two malicious packets per minute is enough to stop a wireless network.

WPA2

Supersedes WPA's interim solution to WEP issues but does require new hardware.

- An enterprise level key management was added to IEEE 802.11, which allows a lot of modes of authentication:
  - No need for a single secret pre-shared key
  - Use of a username and a password, smartcards, certificates, hardware security tokens etc
- Every station uses individual keys to communicate with an AP
  - Eavesdropping by another station in the same network is not possible anymore.

Questions