Wi-Fi ® Security

Dr. Abbas Hatoum

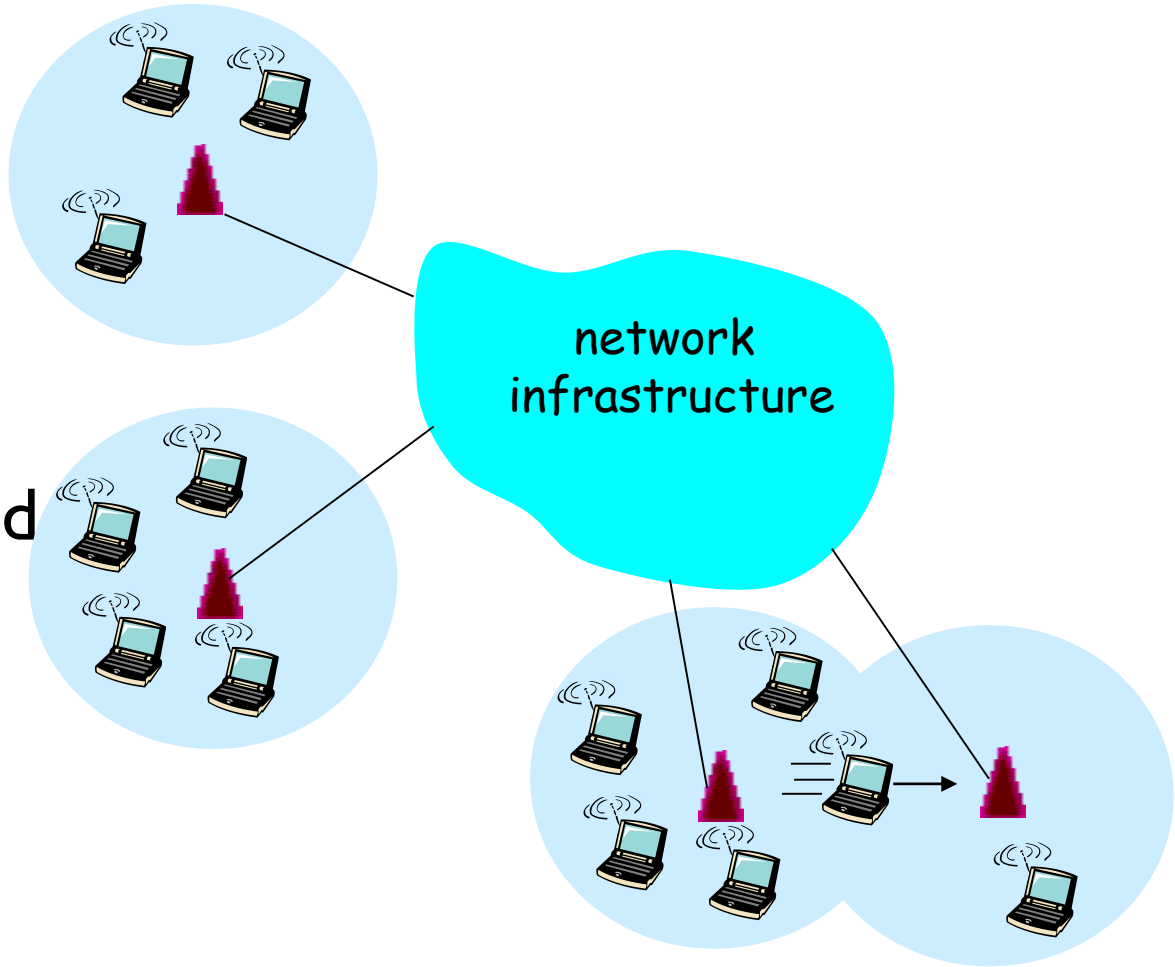
Jan 2019

Topics

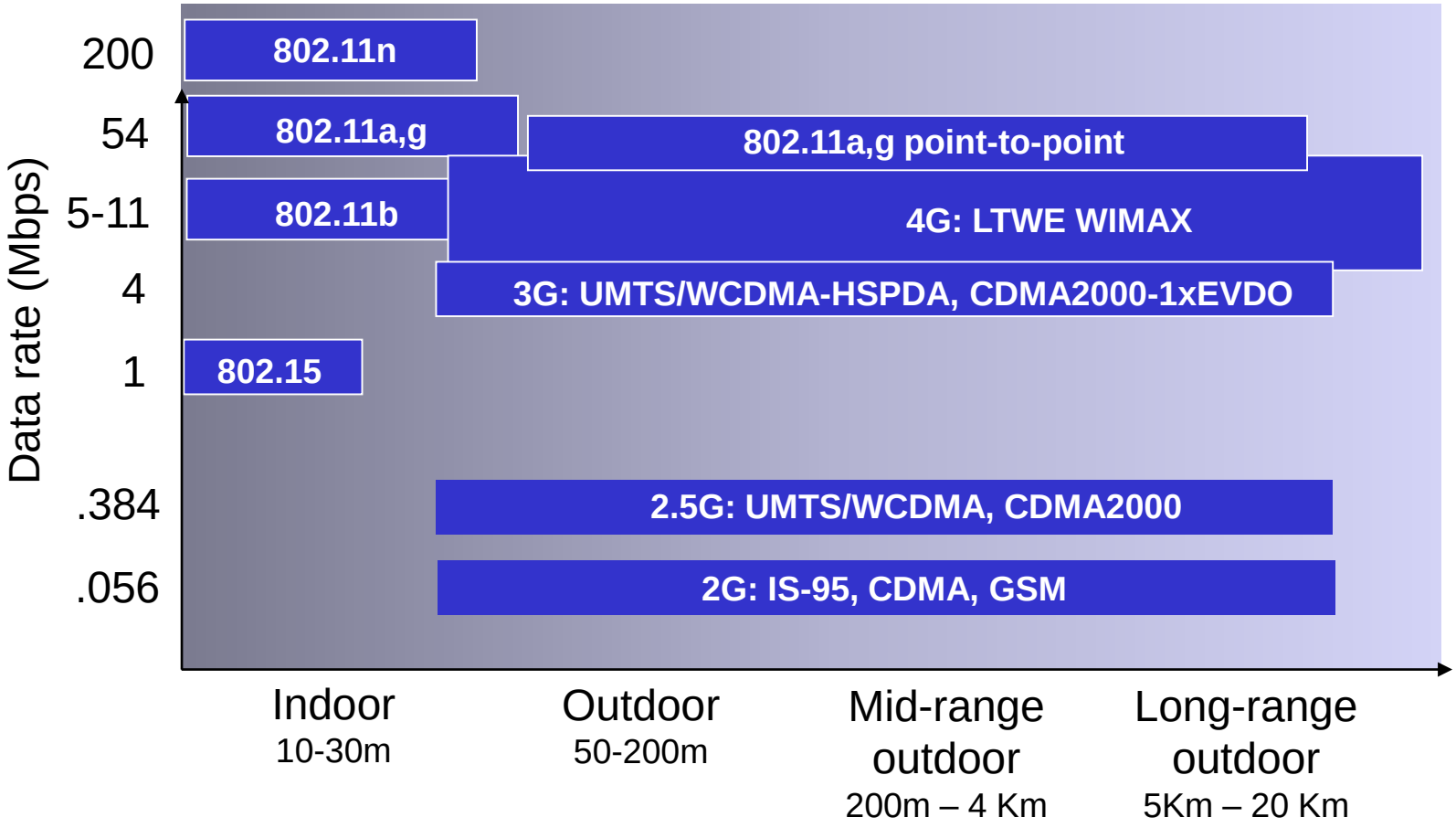
- Wireless Infrastructure
- Wi-Fi® Alliance
- Background
- Benefits
- 802.11 Architecture
- Wi-Fi Security
  - WEP
  - WPA/WPA2
  - EAP/ Radius
- Wi-Fi Future

Wireless: infrastructure

- Base stations relay traffic between wireless and wired networks
  - Cell towers
  - Access points
  - ...
- Infrastructure mod
- *vs.* ad-hoc
  - No base stations



Characteristics of selected wireless links



Wi-Fi Alliance

- An open, non-profit organizaton responsible of : Wi-Fi standards development, marketing, Wi-Fi certification etc.
- Wi-Fi Alliance developed standards: WPA, WPA2, WMM, Wi-Fi Direct etc.
- Formed originally to resolve the interoperability issues between different manufacturers' 802.11 devices.
- Similar organization to Bluetooth SIG

The IEEE 802.11 specification is an international standad describing the characteristics of a wireless Local Area Network

The term *Wi-Fi* suggests *Wireless Fidelity*, resembling the long-established audio-equipment classification term *high fidelity*

Background

Background

- **1990 : 802.11 development started by IEEE**

  The aim was to develop a standards for medium access control (MAC) and physical layer (PHY)

- **1997 : First version of 802.11 standard was ratified**

  First version delivered 1Mb/s and 2Mb/s data rates

- **1999 : 802.11a and 802.11b amendments were released**

  Data rates improved to 5.5Mb/s and 11Mb/s at 2.4GHz (802.11)

  Wired Equivalent Privace (WEP) introduced

  5GHz operation with OFDM modulation at 54Mb/s (802.11a)

- **2001 : FCC approved the use of OFDM at 2.4GHz**

- **2003 : OFDM modulation at 54Mb/s at 2.4GHz (802.11g)**

Background

- **2009 : 801.11n amendment were ratified**

  PHY relies heavily on multiple-input multiple-output (MIMO) technology

  Can use both 2.4Ghz and 5Ghz at the same time Throughput increased even up to 600Mbps

- **2009 : Bluetooth 3.0 + HS**

  802.11 selected as the Bluetooth high speed channel

- **2009 : Wi-Fi direct specification introduced 2011 : 802.11ac**

  More throughput with wider bandwith, more MIMO streams and
- wider 256-QAM modulation. Provides 500-1000Mbps throughput

2019: 802.11ax

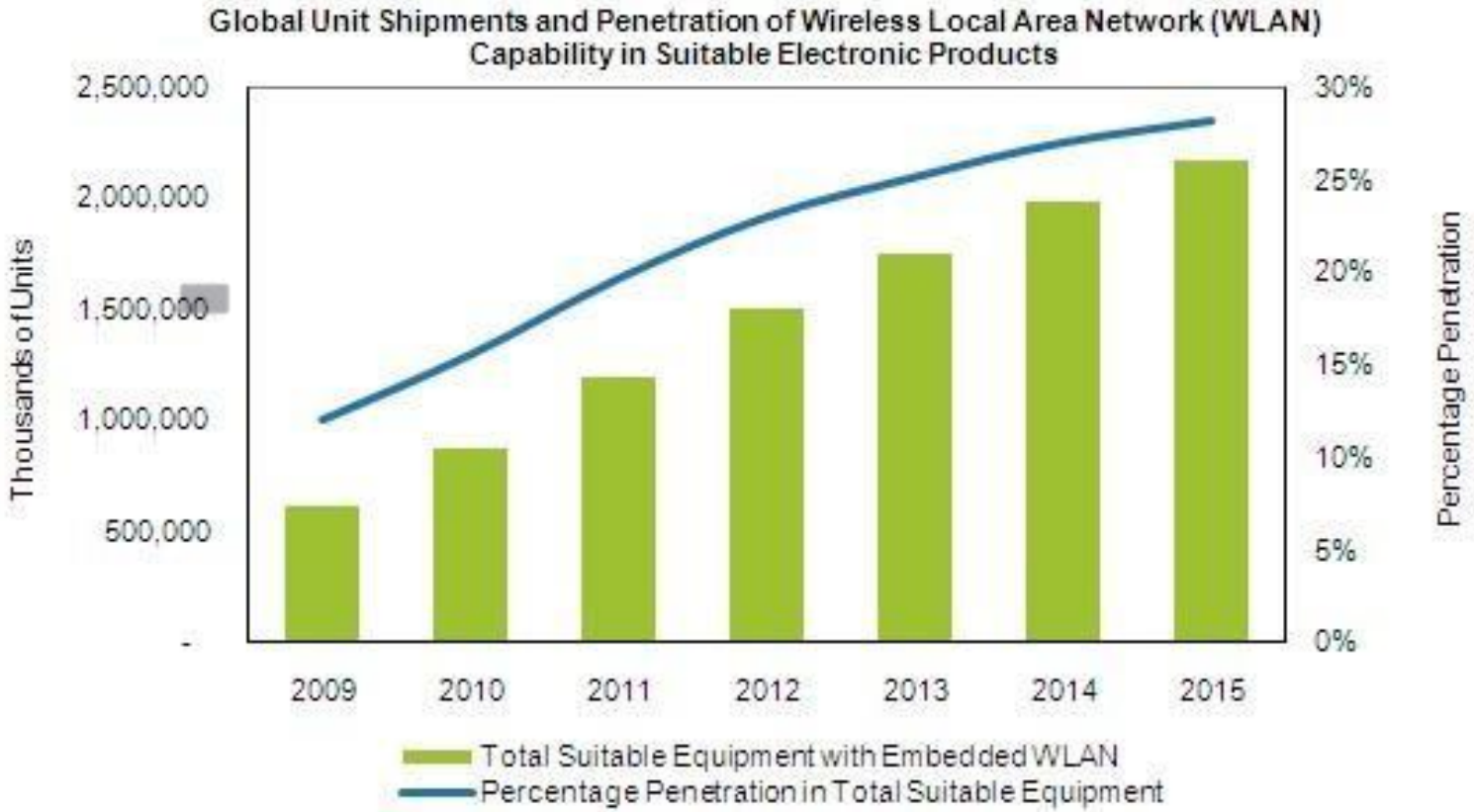
Benefits

Benefits of Wi-Fi

- **Mobility**
- **Compatibility with IP networks**
- **High speed data**
- **Unlicenced frequencies**
- **Security**
- **Easy and fast installation**
- **Scalability**
- **Installed infrastucture**
- **Low cost**

Eco-System Growth

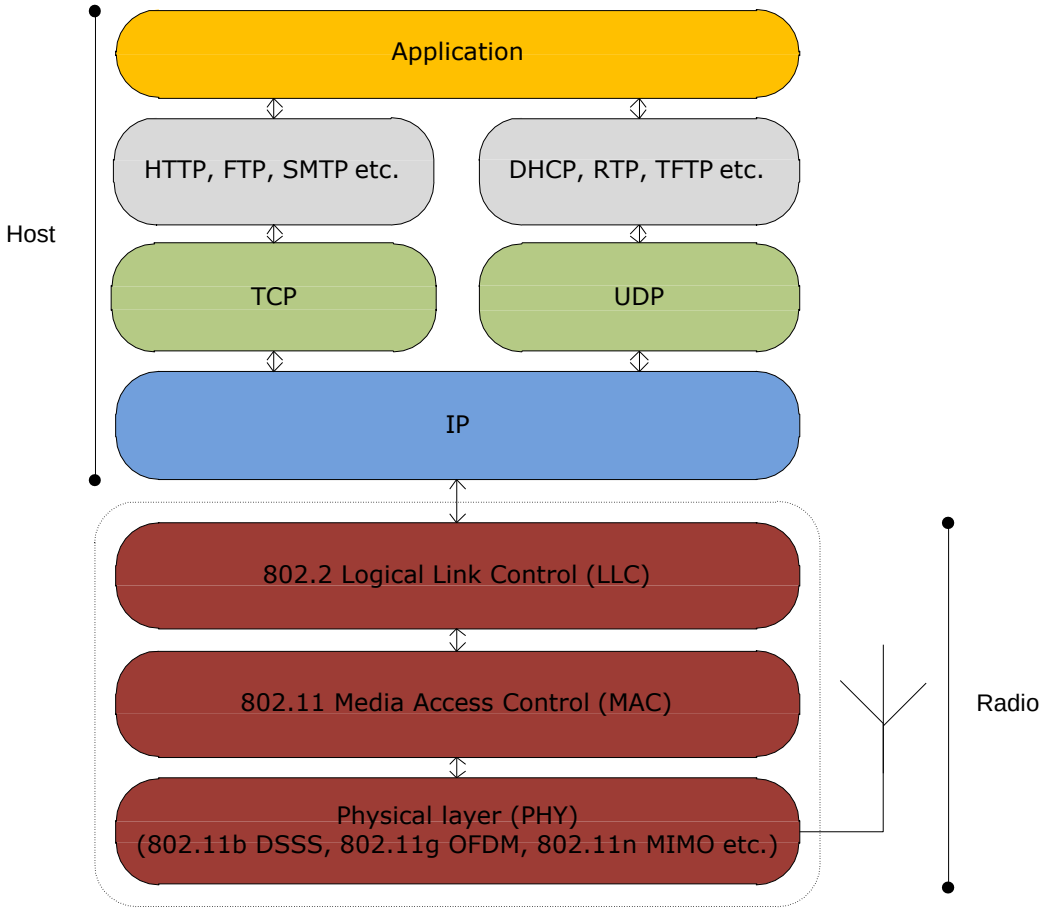
- **The number of Wi-Fi products is growing steadily.**



By iSuppli Market Research

802.11 Architecture

802.11 Architecture



Physical layer

2.4 GHz and/or 5GHz transciever Industrial Scientific Medical (ISM) band

- License free

Spread spectrum technology

FHSS, DSSS abnd OFDM modulations

FHSS (Frequency Hopping Spread Spectrum)

Bandwidth divided into 75 1MHz channels

- Data throughput limited to 2Mbps because of hopping overhead and FCC regulations (1 Mhz channel bandwidth)
- Obsolete

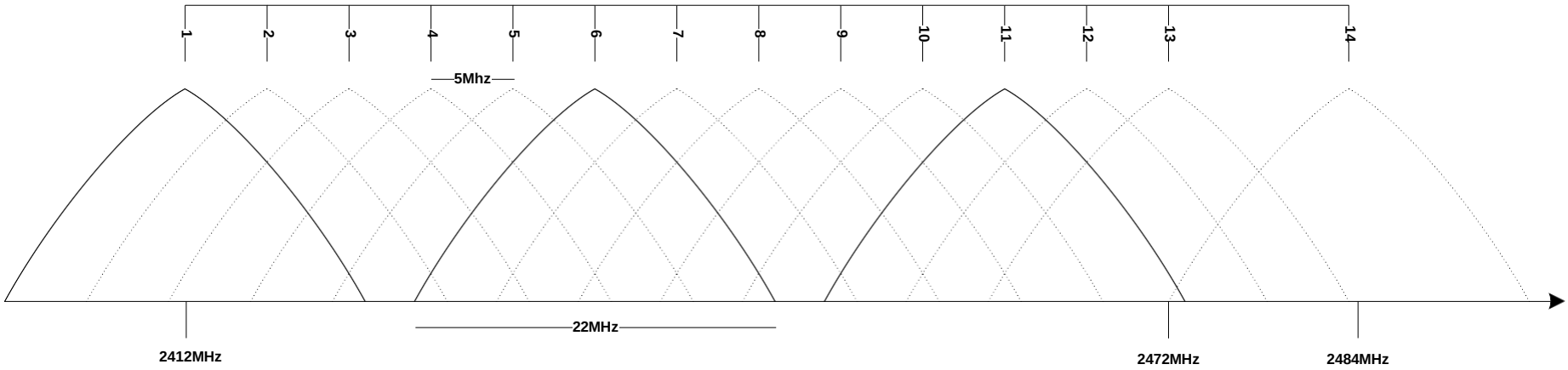
DSSS (Direct Sequency Spread Spectrum) Bandwidth divided into 14 22MHz channels Channels overlap partially

OFDM (Orthogonal Frequecy-Division Multiplexing)

20 or 40MHz bandwidth

Uses several non-overlapping channels Channels overlap partially

Physical layer



Europe : channels 1-13

USA : channels 1-11

Japan : channels 1-14

Physical layer

Standard	Frequency	Bandwidth	Symbol rate (Mb/s)	MIMO streams	Modulation
802.11	2.4GHz	20	1, 2	1	DSSS, FHSS
802.11a	5Ghz	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM
802.11b	2.4GHz	20	5.5,11	1	DSSS
802.11g	2.4GHz	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS
802.11n	2.4/5GHz	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM
		40	15, 30, 34, 60, 90, 120, 135, 150		

IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then

transmit entire frame (no CD)

2 if sense channel busy then

start random backoff time

timer counts down while channel idle

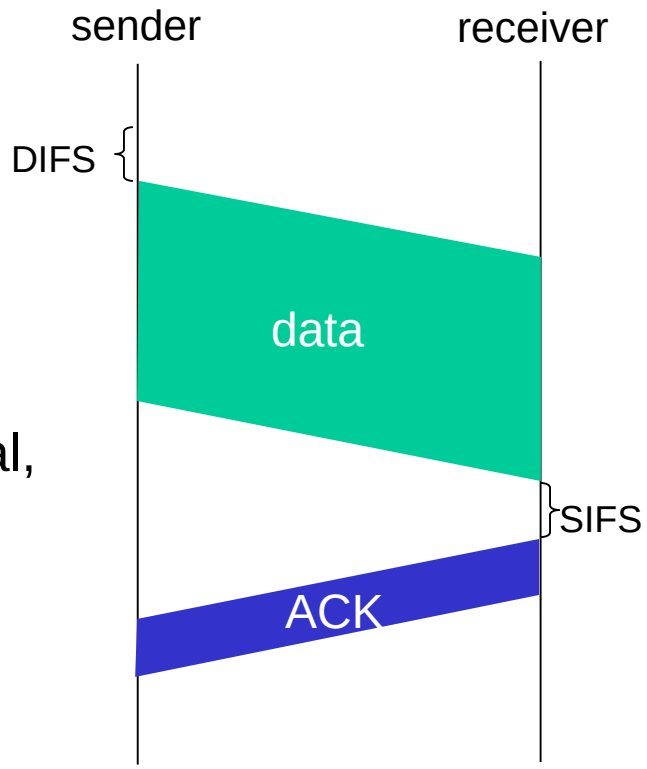
transmit when timer expires

if no ACK, increase random backoff interval, repeat 2

802.11 receiver

- if frame received OK

return ACK after **SIFS** (ACK needed due to hidden terminal problem)



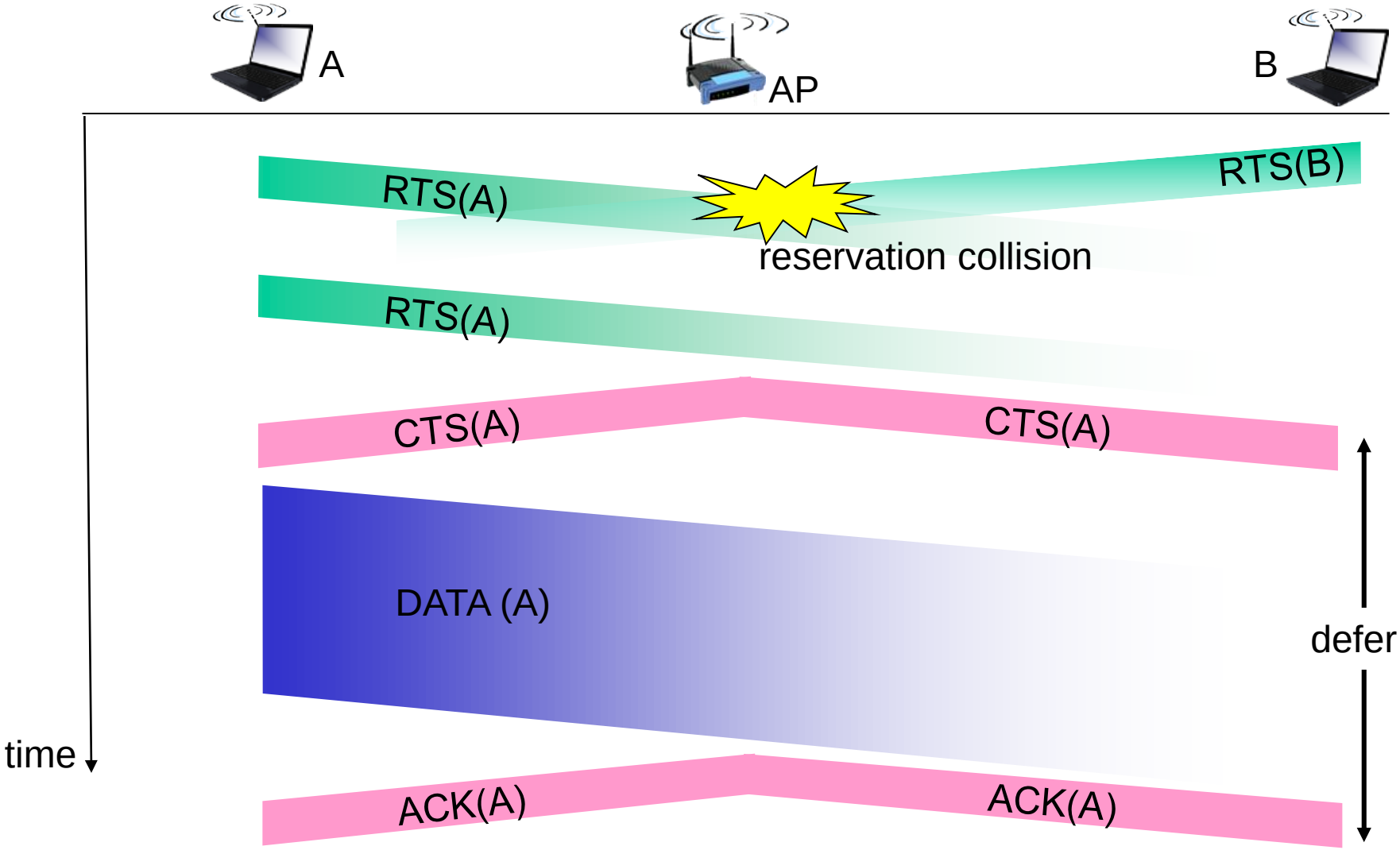
Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely using small reservation packets!

Collision Avoidance: RTS-CTS exchange



Wireless: 802.11 beacons / assocation

- Genesis of a wireless/WiFI network

JOIN ME Beacon!!!

I have powerful signal!

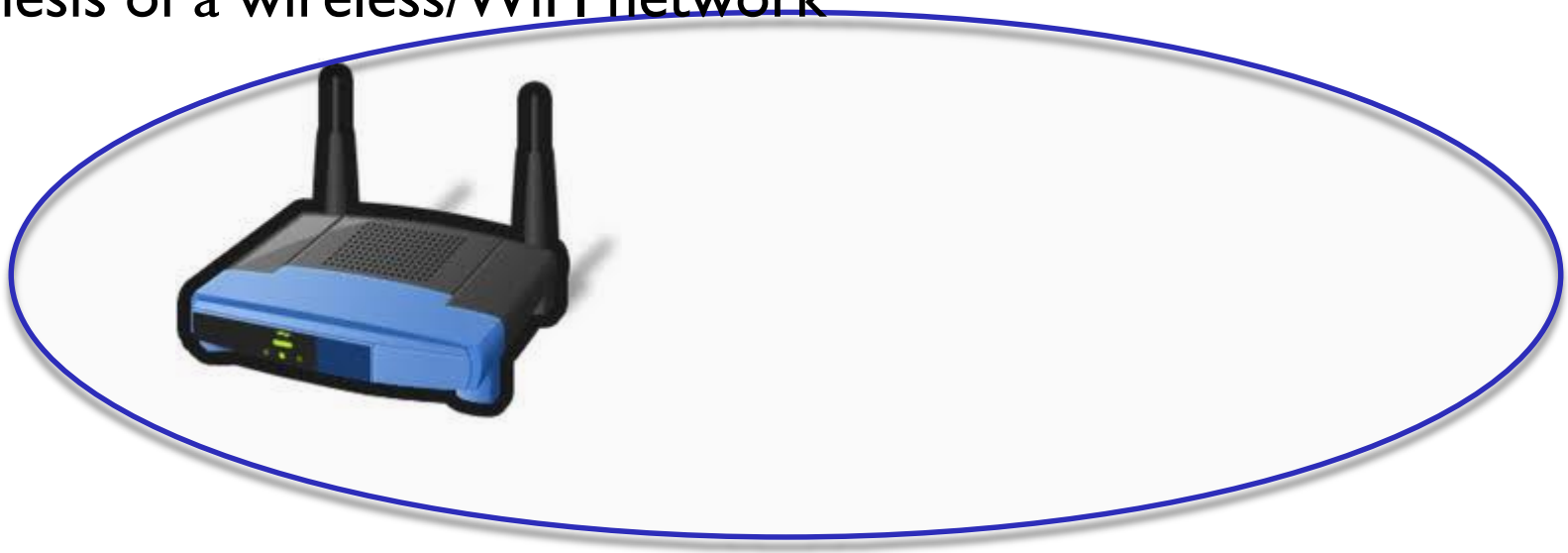
I am called Secure! (SSID)

My MAC address is 00:de:ad:be:ef:00 (BSSID)

I encrypt .. or not

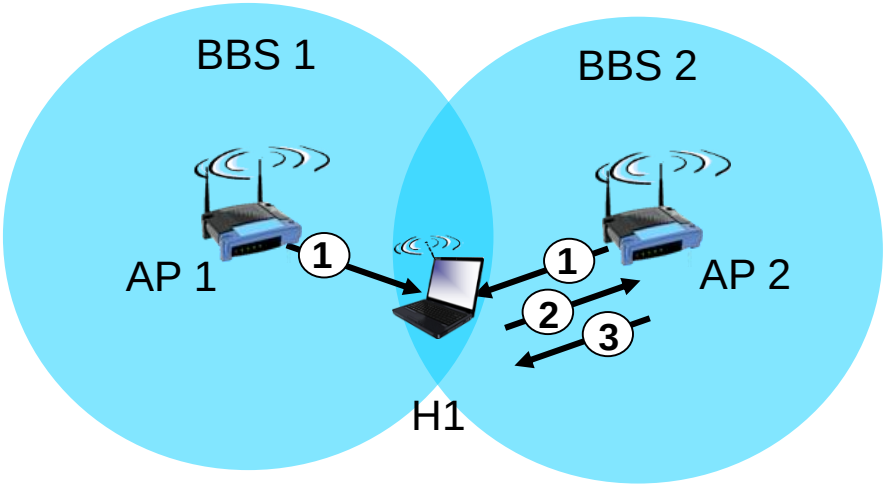
Wireless: 802.11 beacons / association

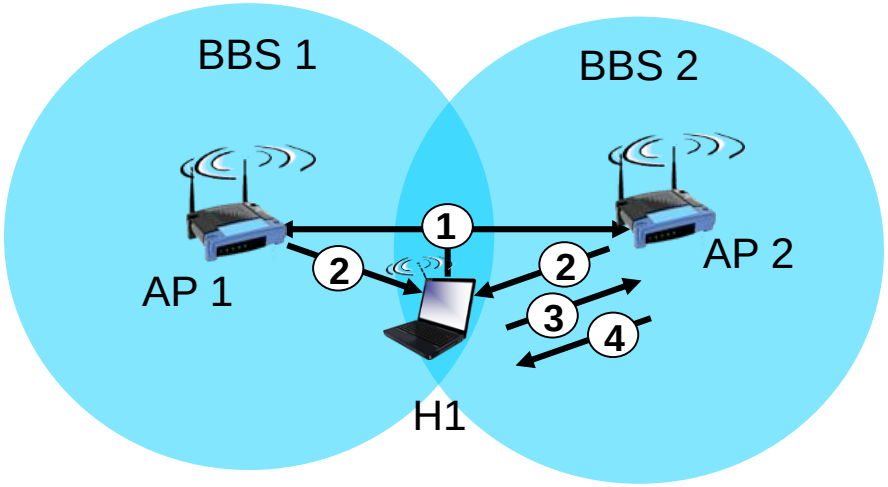
- Genesis of a wireless/WiFI network



- ... and a WLAN is born
- Afterward, may authenticate, run DHCP, etc.

802.11: passive/active scanning





passive scanning:

(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

active scanning:

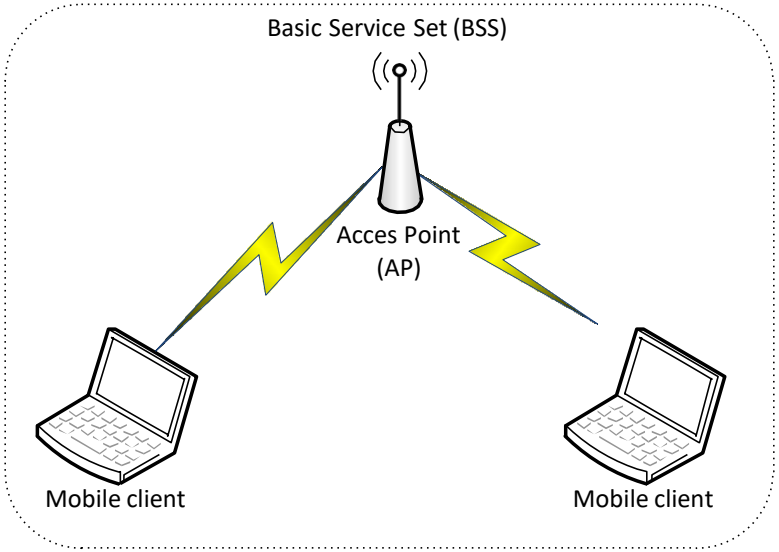
(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

Infrastructure

Basic Service Set (BBS)

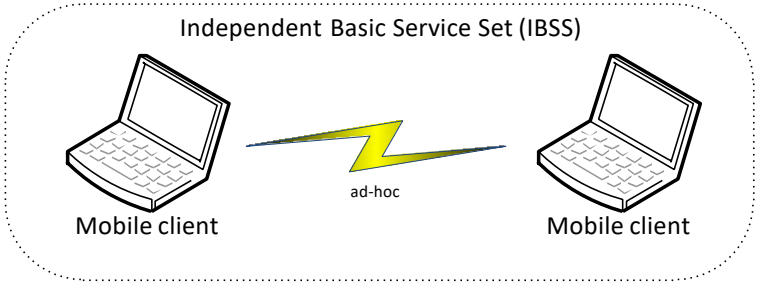
- A set of stations controlled by a single "Coordination Function"

- Typically uses an Access Point (AP)
- All mobile stations must be accessible by the access point of the infrastructure BSS
- In the infrastructure network, stations must associate with the access point in order to get access to network services



Independet Basic Service Set (IBBS)

- A BSS without an Access-Point ad-
- hoc networking



Infrastructure

Extended Service Set (ESS)

- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)

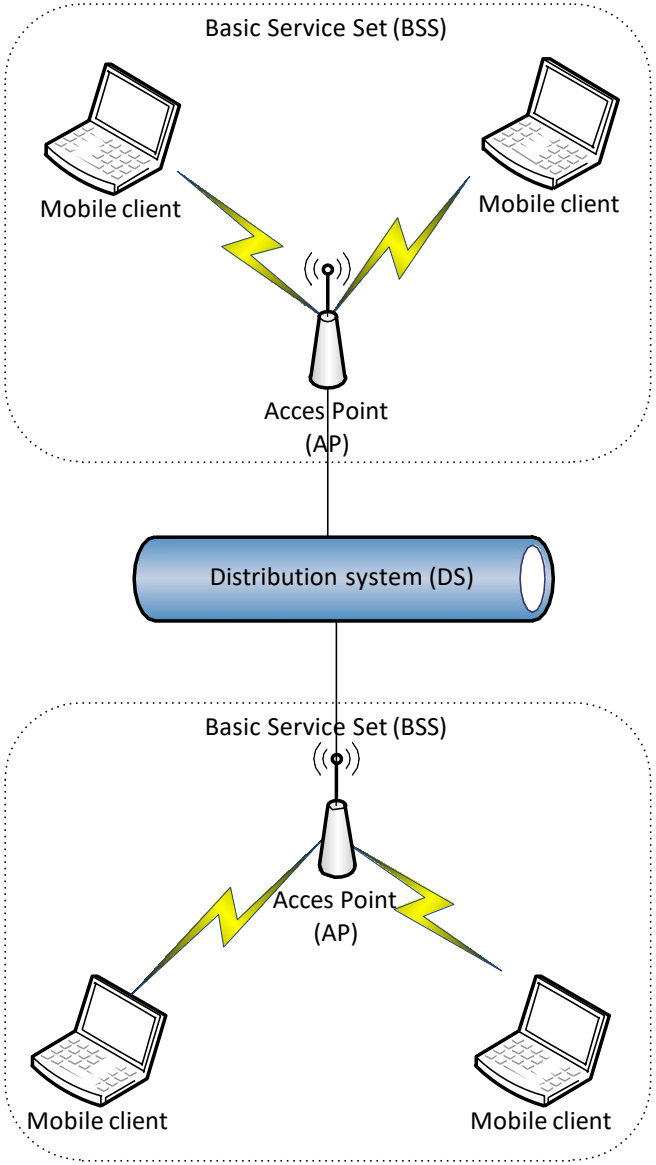
- Traffic always flows via Access-Point

Distribution System (DS):

- A system to interconnect two or more BSS

- Typically wired Ethernet

- Could be also wireless like 802.11, WiMax, 3G/4G etc.



Infrastructure

AP – client services:

- Authentication : open, shared key or WPS
- De-authentication
- Privacy : WEP, WPA or WPA2

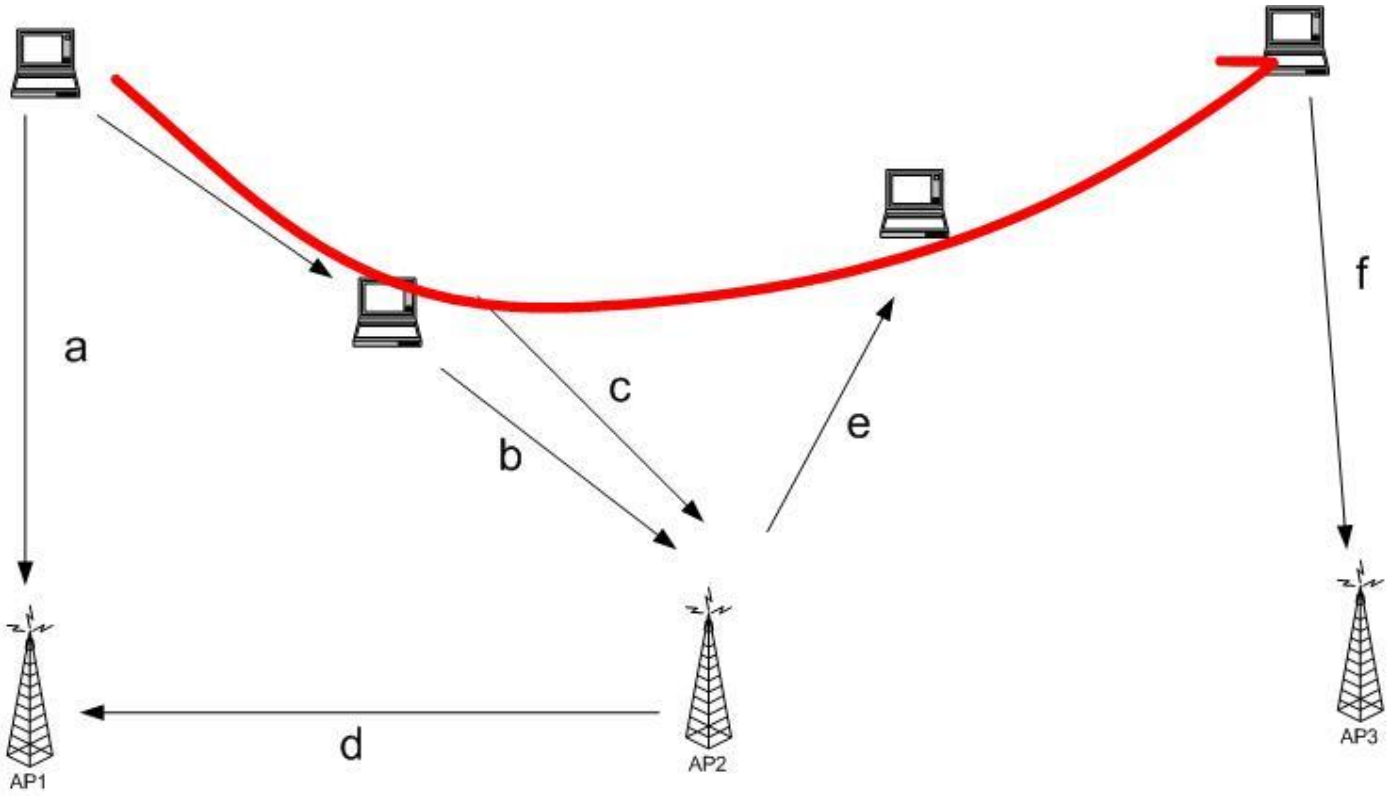
Distribution System services:

- Association
- Disassociation
- Distribution
- Integration
- Re-association

802.11 Media Access Control

Function	Explanation
Scanning	Scanning of access points. Both active (probe) and passive (beacon) scanning are provided by the standard.
Authentication	Authentication is the process of proving identity between the client and the access point.
Association	Once authenticated, the client must associate with the access point before sending data frames.
Encryption	Encryption of payload
RTS/CTS	The optional request-to send and clear-to-send (RTS/CTS) function allows the access point to control use of the medium for stations activating RTS/CTS.
Power Save Mode	The power save mode enables the user to turn on or off enables the radio.
Fragmentation	The fragmentation function enables an 802.11 station to divide data packets into smaller frames.

Ex



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

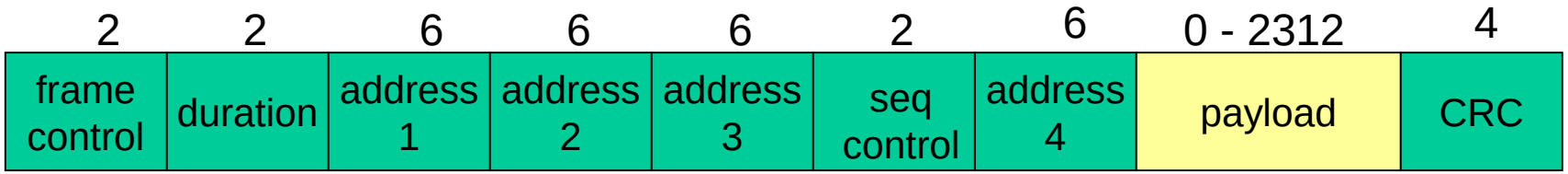
(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

802.11 frame: addressing



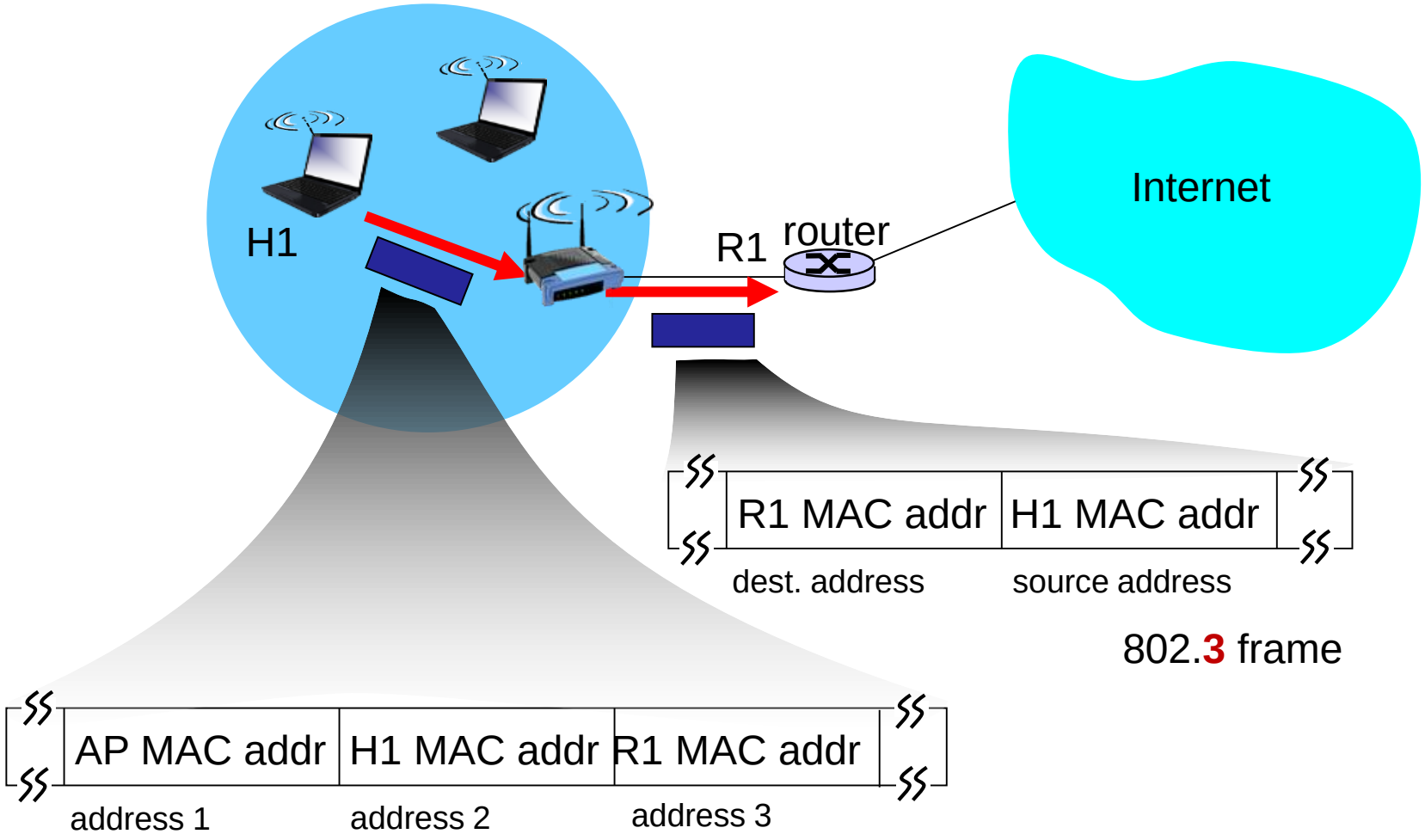
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing



Frame Subtypes

CONTROL	DATA	MANAGEMENT
❖ RTS ❖ CTS ❖ ACK ❖ PS-Poll ❖ CF-End & CF-End ACK	• Data • Data+CF-ACK • Data+CF-Poll • Data+CF-ACK+CF-Poll • Null Function • CF-ACK (nodata) • CF-Poll (nodata) • CF-ACK+CF+Poll	• Beacon • Probe Request & Response • Authentication • Deauthentication • Association Request & Response • Reassociation Request & Response • Disassociation • Announcement Traffic Indication Message (ATIM)

802.11: advanced capabilities

power management

- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

Security

Security

The 802.11 provides the following security features

- **Association**
  Client needs to associate with the Access Point

- **Authentication**
  Authentication is either open, shared key or WPS

- **Access control**
  Access Point can decide which clients are allowed to assiciate based on MAC address

Trivial to spoof MAC address

Security

- **Encryption**

Wired Equivalent Privacy (WEP)	(insecure)
Wireless Protected Access (WPA)	(insecure)
Wireless Protected Access 2 (WPA2)	(recommended)
WAPI	(for China)

- **Data integrity**
  Data can not be modified on-the-fly. Guaranteed by encryption.

- **Data confidentiality**
  No eavesdropping with decryption of data. Guaranteed by encryption.

Security

- **Wired Equivalent Privacy (WEP)**

  Wired Equivalent Privacy. This encryption standard was the original encryption standard for wireless.

  Security issues known since 2001, can be cracked in <1minute

- **Wirelsss Protected Access (WPA)**

  A software/firmware improvement over WEP. WPA is a trimmed-down version of the 802.11i security standard that was developed by the IEEE 802.11 to replace WEP.

  WPA uses TKIP for encryption, some routers also support AES.

  Security issues known since 2008 in TKIP, considered unsecure

- **WLAN Authentication and Privacy Infrastructure (WAPI)** A wireless security standard defined by the Chinese government. Must be supported by cell phones sold in China.

Security

Wireless Protected Access 2 (WPA2)

- WPA2 is a Wi-Fi Alliance branded version of the final 802.11i standard.
- The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature.
- The CCMP/AES algorithm is considered secure, given a good enough password
- WPA2 Personal (WPA2-PSK): Uses a password, common.
- WPA2 Enterprise (WPA2-RADIUS): Certificates on server

Note: Wi-Fi Alliance will mandate Wi-Fi CERTIFIED products only to support WPA2 CCMP/AES

Wired-Equivalent Privacy (WEP)

- First, let's optionally authenticate users
- Second, let's at least try to to encrypt every packet
  - How do we do that?
- Unless we want an open network, we're going to have to share a key
  - Later, we should have key management!
  - How would you implement this?
- At the time WEP was defined, export restrictions limited cryptography, so 64-bit RC4 was used
  - Extensions later for for 128-bit WEP

WEP Authentication

- What about authentication with shared key?

- First idea:
  - Client sends authentication request with key
  - Access point responds with ACCEPT if key cor

- Second idea:
  - Client sends num and hash(num | key)
  - Access point also computes hash, ACCEPTS if it likes the outcome

WEP Authentication

- Third idea:
  - Client sends intention to authenticate
  - Access point sends back a random number (nonce) x
  - Client computes hash(x | key), sends to access point
  - Access point sends ACCEPT if matches local hash(x | key)

- This is used in WEP

- Called 4-step challenge-response handshake
  - Avoids disclosing the (static) key
  - Prevents replay attack ("pass-the-hash")

WLAN security using WEP

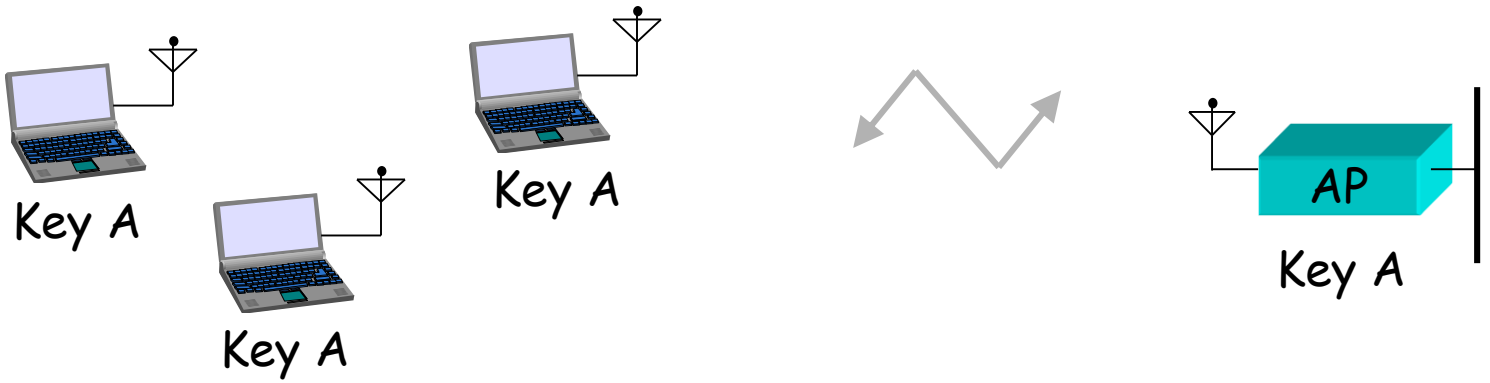
IEEE 802.11 specifies as an option usage of WEP which can take care of the following security mechanisms:

- Authentication ("shared key" user authentication)
- Confidentiality (RC4 stream cipher encryption)
- Integrity checking (CRC-32 integrity mechanism)

~~No key management~~

~~No protection against replay attacks~~

No key management in WEP



No key management in WEP ⇔ every wireless station and AP has the same "preshared" key that is used during authentication and encryption. This key is distributed manually (=> insufficient for enterprise applications).

Problems with preshared keys

Manual key management is not very flexible

Same key for everybody:

In a large network, users may wish to have independent secure connections. Just a single non-honest WLAN user can break the security.

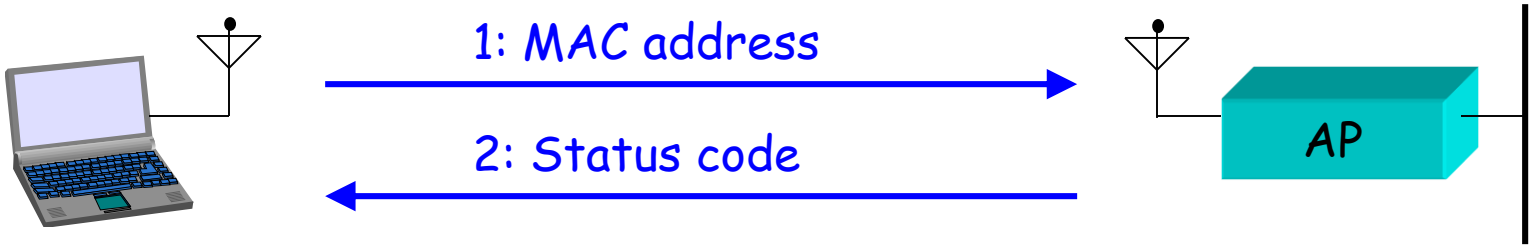
Static key:

Since it is relatively easy to crack WEP encryption in a reasonably short time, the keys should be changed often, but the preshared key concept does not support this.

WLAN authentication methods

1. Open system authentication (specified in WEP)
   - actually no authentication at all
2. Shared key authentication (specified in WEP)
   - weak due to non-existing key management
3. Authentication using SSID of AP
4. MAC address filtering
5. IEEE 802.1X authentication (specified in WPA)
6. SIM/AuC authentication (in operator-based network)

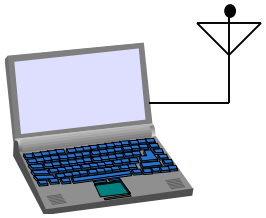
Open system authentication



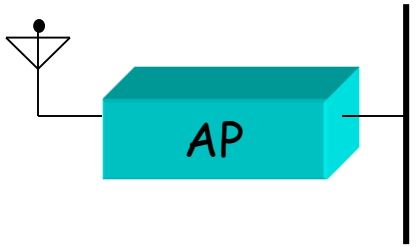
Status codes are defined in IEEE 802.11

Status code	Meaning
0	Successful
1	Unspecified failure
:	:
15	Authentication rejected (cause x)
:	:

Shared-key authentication



1: MAC address



2: Challenge text
(128 octets, clear)

WEP Encryption

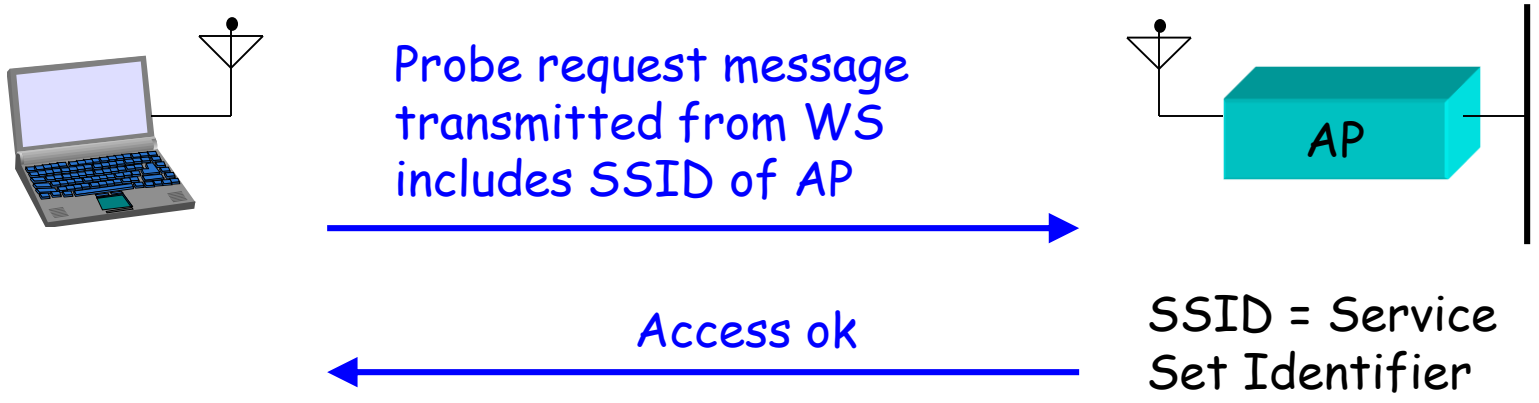
3: Response text
(WEP encrypted)

Authentication is successful, if WEP decryption gives original challenge text

4: Status code

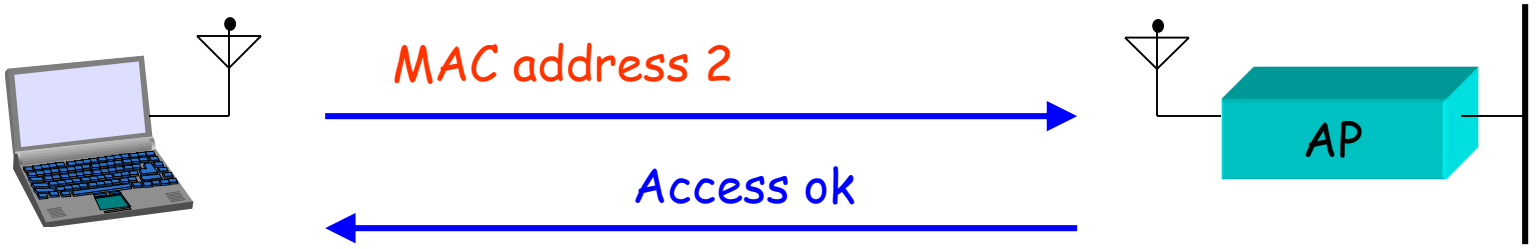
Authentication successful / failure

Authentication using SSID of AP



Not very secure: SSID is transmitted unencrypted over the wireless network and can be easily captured by an attacker.

MAC address filtering



Not very secure: Attacker can read MAC address of a wireless station attached to the WLAN and replace own MAC address with this stolen MAC address.

Accepted MAC addresses:

MAC address 1
MAC address 2
MAC address 3
MAC address 4
:

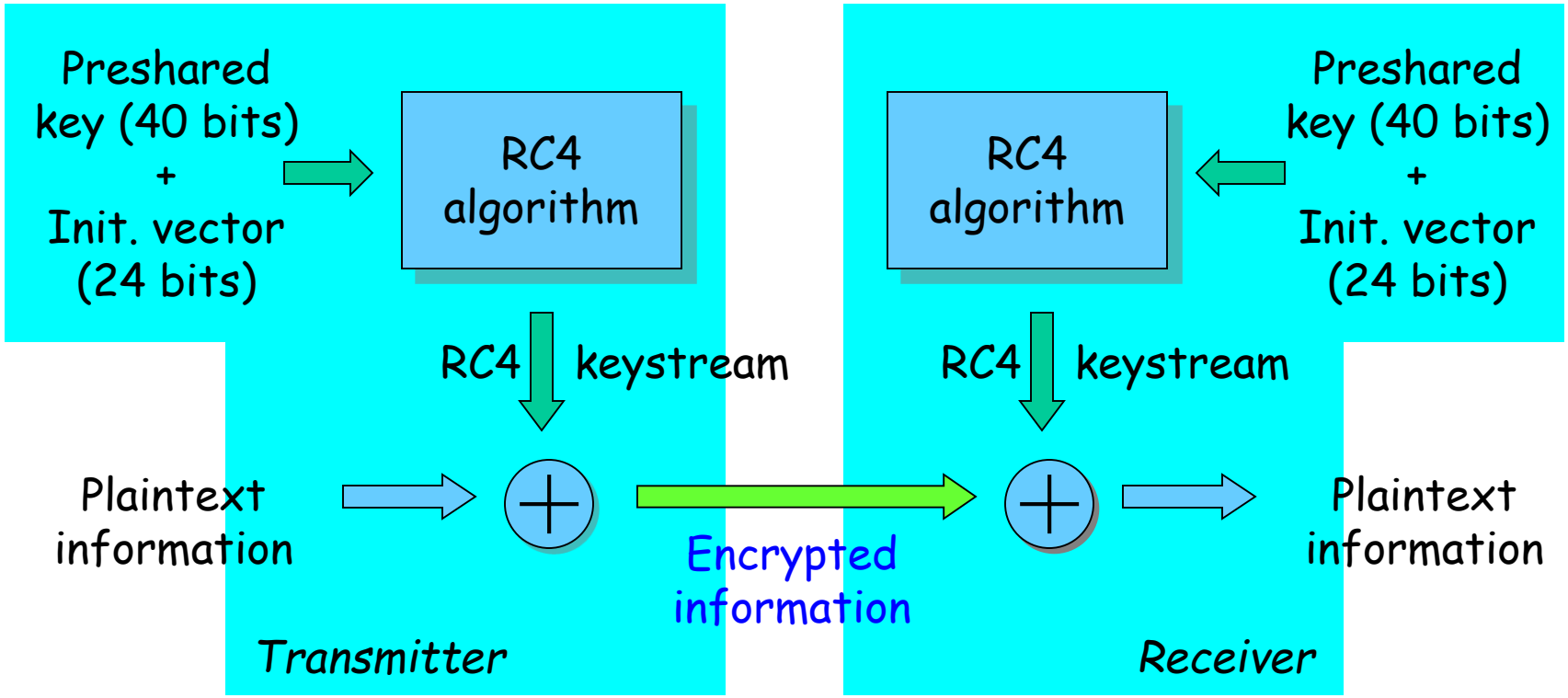
WEP encryption

WEP encryption is based on the RC4 stream cipher. First the preshared key (40 bits) is combined with a 24 bit initialization vector (IV) that should change from packet to packet (WEP does not specify how to select the IV).

The combined key (preshared key + IV) is fed to the RC4 algorithm that generates a continuous keystream.

The plaintext information (+ ICV, see future slide) is bit-wise combined with the keystream by employing the XOR operation, thus producing the encrypted information.

WEP encryption and decryption



WEP key lengths

Standard solution:

Enhanced solution:

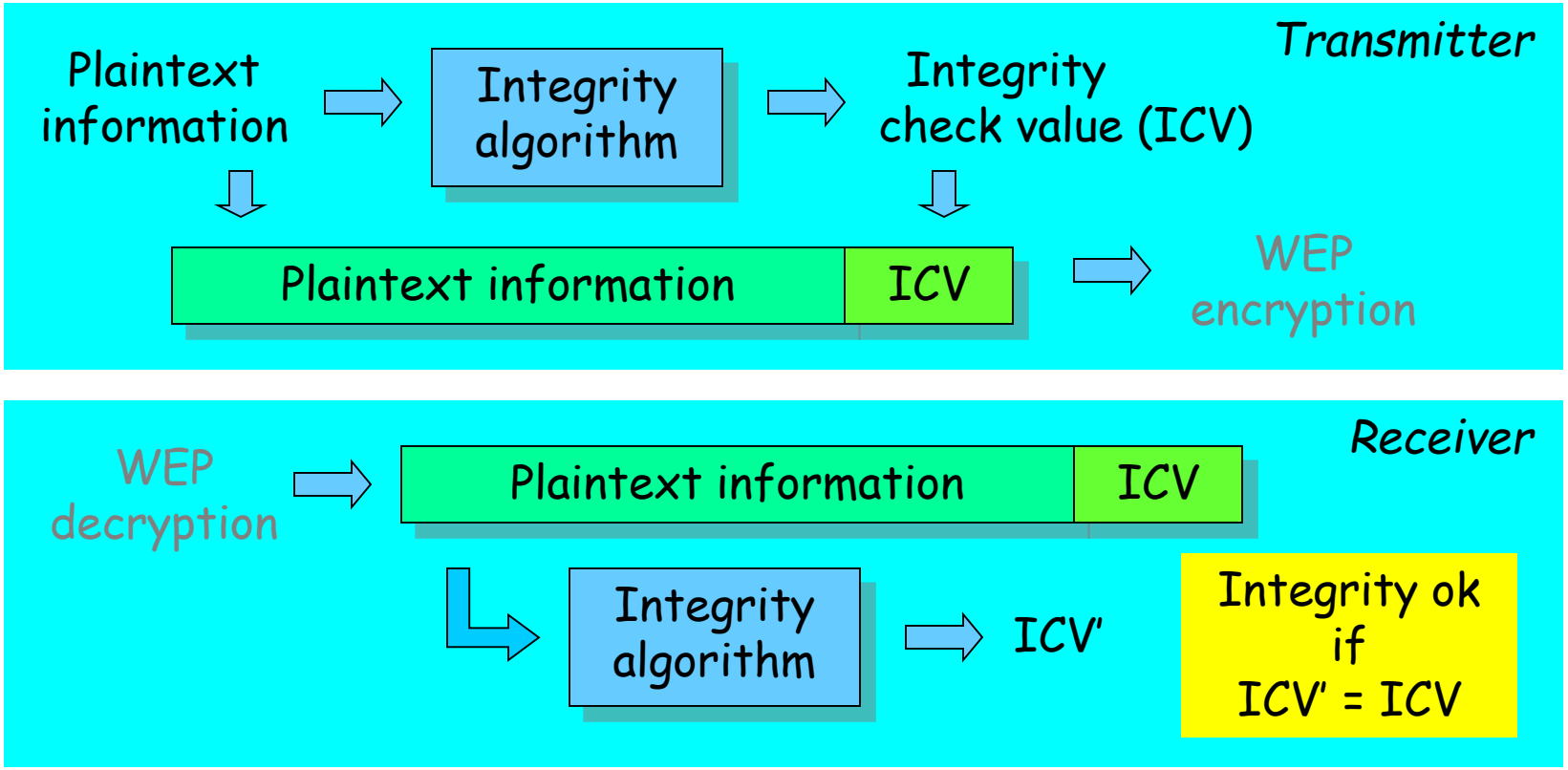
Initialisation vector (IV) is sent unencrypted over the wireless interface to the receiving end.

WEP integrity check

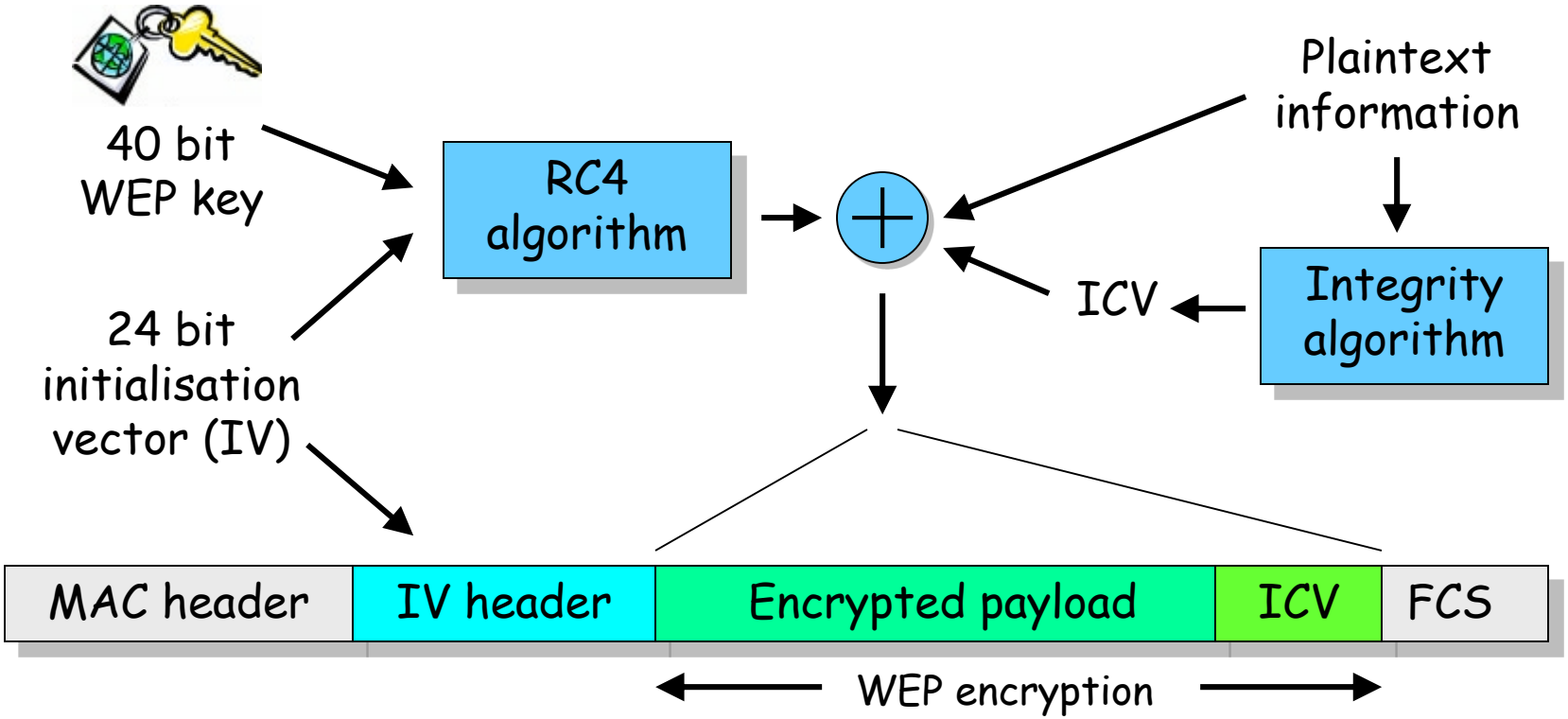
Integrity checking prevents man-in-the-middle attacks:

Integrity check is implemented in WEP by appending an integrity check value (ICV) bit sequence after the plaintext information before encryption at the transmitter.

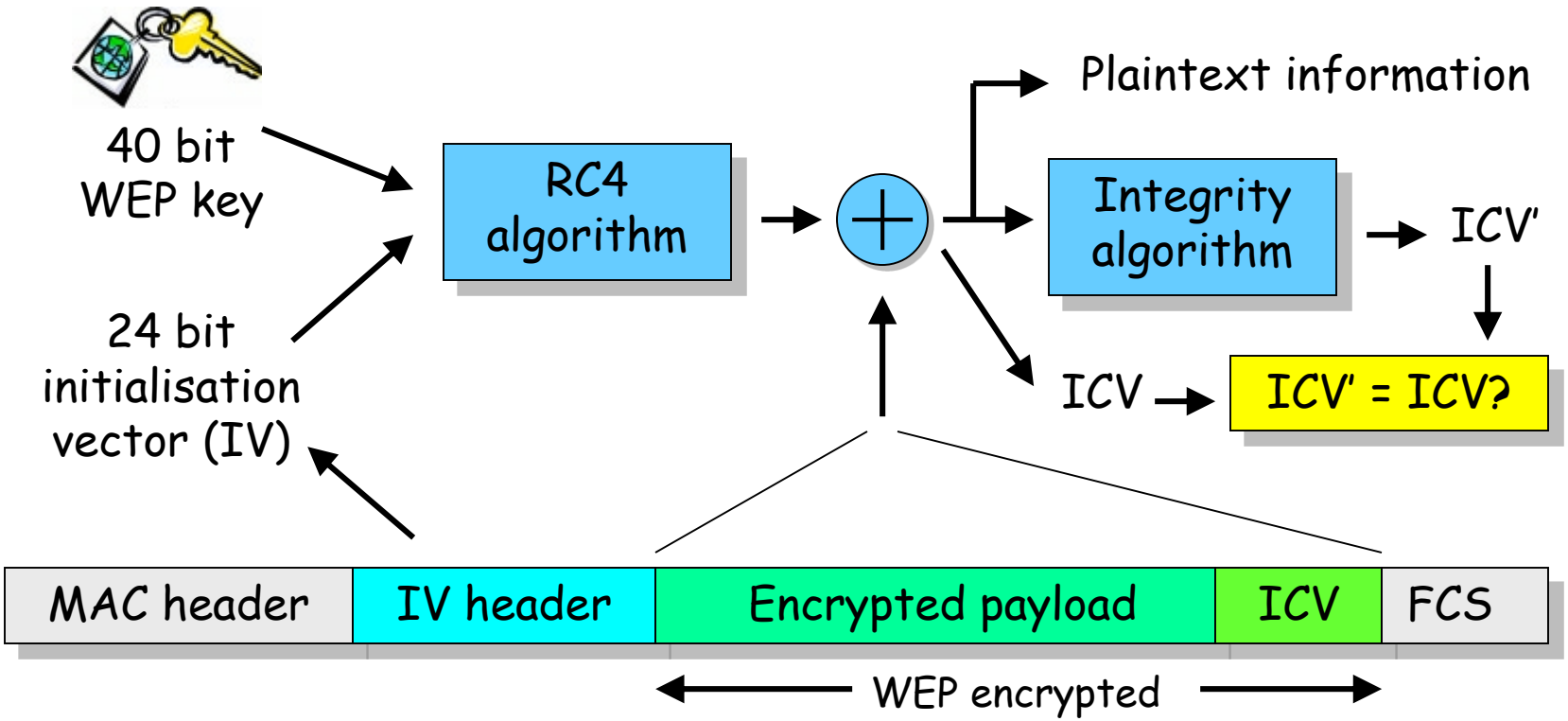
WEP integrity check



WEP operation: transmitter



WEP operation: receiver



WEP summary

Security measure	Features
Key management	WEP does not support key management
Authentication	Shared key authentication
Encryption	RC4 stream cipher, 40 bit key length is rather weak
Integrity protection	Rather weak in WEP
Replay attacks	No protection.

IV prevents key reuse: Any problems?

- IV (Initialization vector) is 24 bits long
  - Recall seeds for random number generators?
  - Only 16 million different RC4 cipher streams per key

- If an IV is ever reused, XOR between packets equivalent to XOR of plaintext messages
  - C = cipher text, P = plain text:
  - $C1 \oplus C2 = (P1 \oplus IV) \oplus (P2 \oplus IV) = P1 \oplus P2$
  - Guess one plain text message, have another

- How long until we expect a reused IV?

- IV is only 24 bits provide a 16,777,216 different RC4 cipher streams for a given WEP key

Chances of duplicate IVs are:

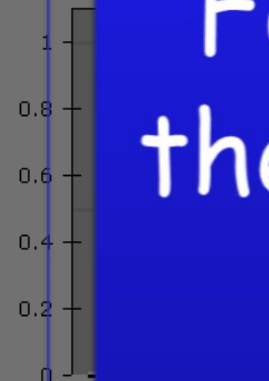
  - 1% after 582 encrypted frames
  - 10% after 1881 encrypted frames
  - 50% after 4,823 encrypted frames
  - 99% after 12,430 encrypted frames
- Increasing Key size will not make WEP any safer. Why?

  » refer to Jesse Walker paper "IEEE 802.11i wireless LAN: Unsafe at any key size", http://www.dis.org/wl/pdf/unsafe.pdf, Oct 2000

The Birthday Paradox

- 23 people in a room
- *Ho*
  sh

For m people and n days, the probability is about $1 - e^{-\frac{m^2}{2n}}$



$$\bar{p}(n) = 1$$

$$= \frac{365 \times 364 \cdots (365 - n + 1)}{365^n}$$

$$= \frac{365!}{365^n (365 - n)!}$$

$2\times365)$,

Answer: 50.7%!

Improving WEP: WPA

- It was quickly realized that WEP offered lax security.
  - WEP was decommissioned in 2004
- Teams from Wi-Fi Alliance set-up to think of two solutions for Protected Access (WPA)
- Backward compatible: WPA-TKIP
  - Stopgap solution for WEP that could be flashed as firmware on to existing infrastructure
  - (i) Uses a key mixing function between IV and key
  - (ii) Adds message integrity checks (MIC) instead of ICV of CRC32 (cryptographically insecure)
  - Attack (2008): Inject 7 packets to a wireless client

Improving WEP: WPA2

- Forward thinking: WPA2
  - Implemented more elaborate 4-way handshake and group key handshake
  - Supports TKIP, CCMP, etc.
  - WPA2 Personal: Pre-shared key between people
  - WPA2 Enterprise: Connect to a RADIUS server
    - Tedious to set up. Also means that if your WiFi credentials are compromised, your whole account will be too.
  - 2012: Flaw in WPS – the device configuration tool for routers that uses a PIN for fast access.
    - Even when disabled, obtains shared key in about 7 hours

WPA Security Enhancements

- WPA includes Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms.
- The combination of these two mechanisms provides dynamic key encryption and mutual authentication
- TKIP adds the following strengths to WEP:
  - Per-packet key construction and distribution:

  WPA automatically generates a new unique encryption key periodically for each client. This avoids the same key staying in use for weeks or months as they do with WEP.
  - Message integrity code: guard against forgery attacks.
  - 48-bit initialization vectors, use one-way hash function instead of XOR

WPA2

- In July 2004, the IEEE approved the full IEEE 802.11i specification, which was quickly followed by a new interoperability testing certification from the WiFi Alliance known as WPA2.
- Strong encryption and authentication for infrastructure and ad-hoc networks (WPA1 is limited to infrastructure networks)
  - Use AES instead of RC4 for encryption
- WPA2 certification has become mandatory for all new equipment certified by the Wi-Fi Alliance, ensuring that any reasonably modern hardware will support both WPA1 and WPA2.

WLAN security using WPA

WPA is basically a pre-standard version of IEEE 802.11i as accepted by the WiFi alliance. WPA offers:

- Key management (using the 802.1X framework, it is also possible to use preshared keys)
- Authentication (using the 802.1X framework)
- Confidentiality (TKIP encryption)
- Integrity checking ("Michael" protocol)
- Protection against replay attacks.

IEEE 802.11i Frameworks:

- RSN
  - **Authentication Enhancement:**
    - IEEE 802.11i utilizes IEEE 802.1X for its authentication and key management services.
  - **Key Management and Establishment:**
    - Manual key management
    - Automatic key management
  - **Encryption Enhancement:**
    - Temporal Key Integrity Protocol (TKIP)
    - Counter-Mode/CBC-MAC Protocol (CCMP)

Temporal Key Integrity Protocol (TKIP)

TKIP encryption is also based on the RC4 stream cipher, just like WEP encryption, with the following differences:

- The length of the initialization vector is 48 bit (instead of 24 bit in WEP)
- TKIP uses 104-bit per-packet keys, derived from a master secret and different for each packet (instead of a 40-bit or 104-bit static preshared key in WEP).

Note that AES (Advanced Encryption Standard) encryption used in IEEE 802.16i is significantly different.

IEEE 802.1X authentication framework

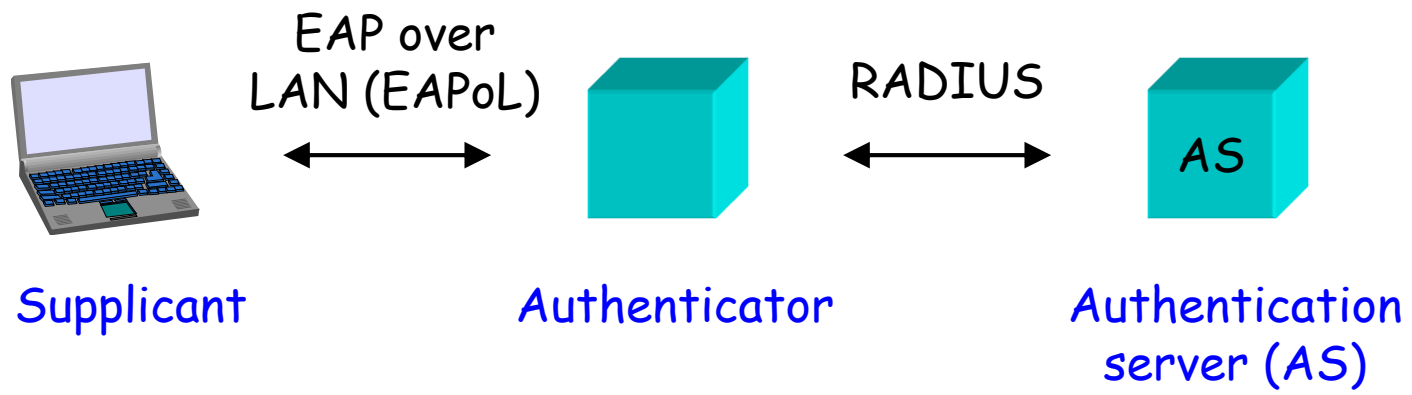
The 802.1X authentication framework protects wired and wireless networks from unauthorised use in open environments (such as university campus).

802.1X uses EAP (Extensible Authentication Protocol) to handle authentication requests. As the name implies, EAP is extensible and therefore should be future proof.

802.1X also uses RADIUS (Remote Authentication Dial-in User Service) for handling secure signalling between AP and authentication server.

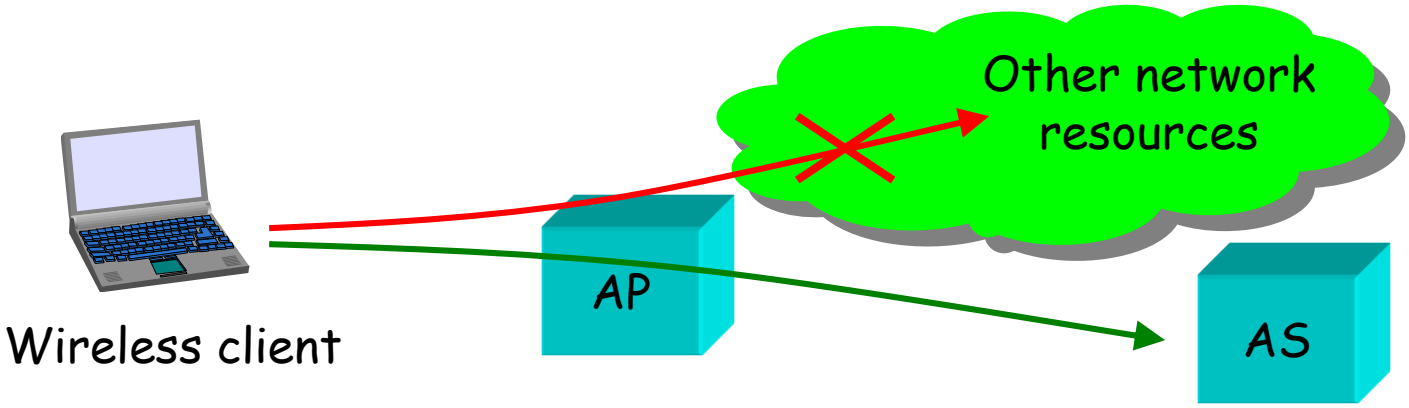
802.1X architecture

802.1X defines three network entities: Supplicant (the wireless client in the wireless station), authenticator (in a WLAN usually the AP) and authentication server (containing user-related authentication information).



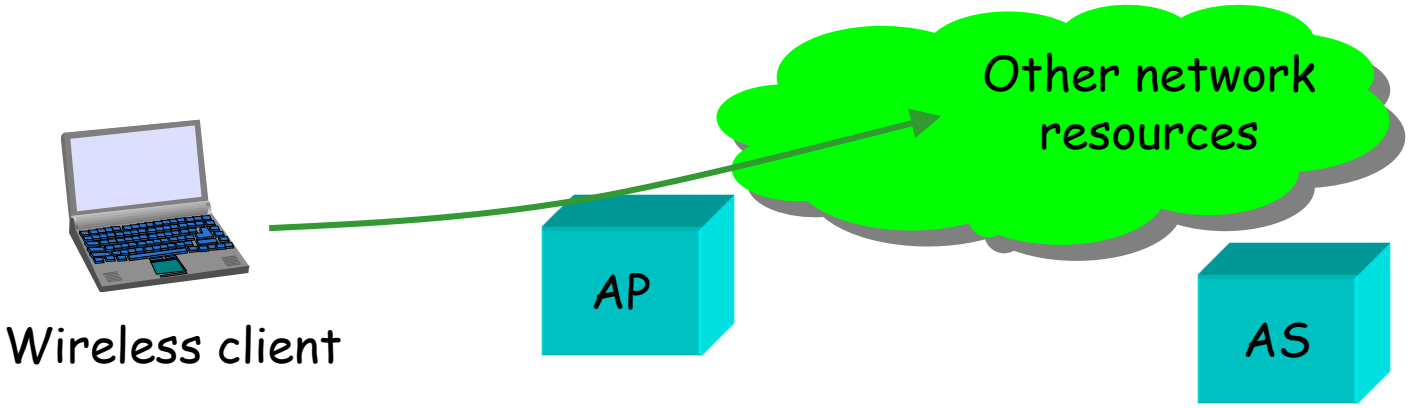
802.1X authentication procedure (1)

With 802.1X, authentication occurs after association. However, prior to successful authentication, a wireless client is only allowed access to the AS. All other traffic is blocked at the AP.

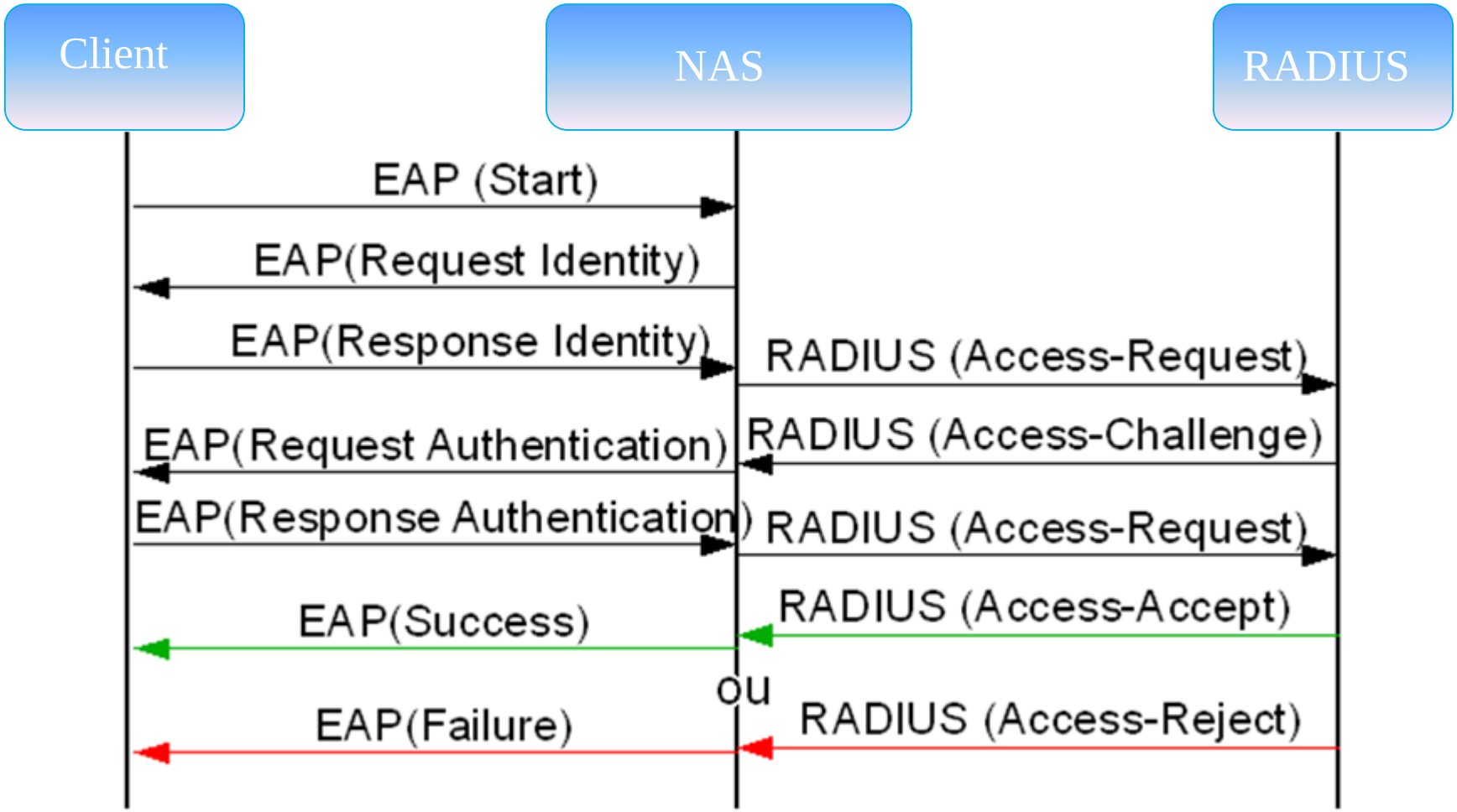


802.1X authentication procedure (2)

After successful authentication, the wireless client is granted access to other network resources by the AP.



EAP Protocol



WiFi Defenses

Basic security features of most wireless networks

- Open
- Hidden SSID
- MAC address filtering
- Encryption and user authentication
  - WEP
  - WPA2-PSK
  - WPA2-Enterprise with radius server for authentication
- All can be broken or bypassed
  - Absolutely not in every instance obviously but often true