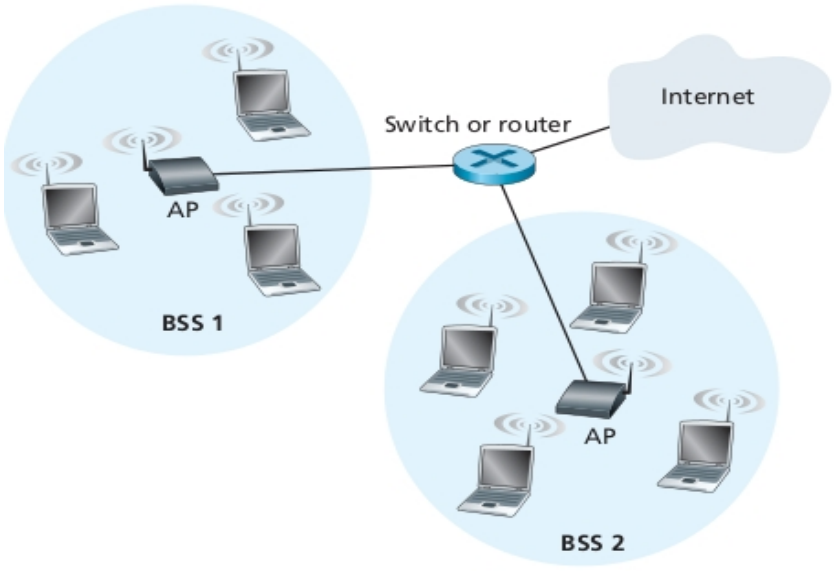
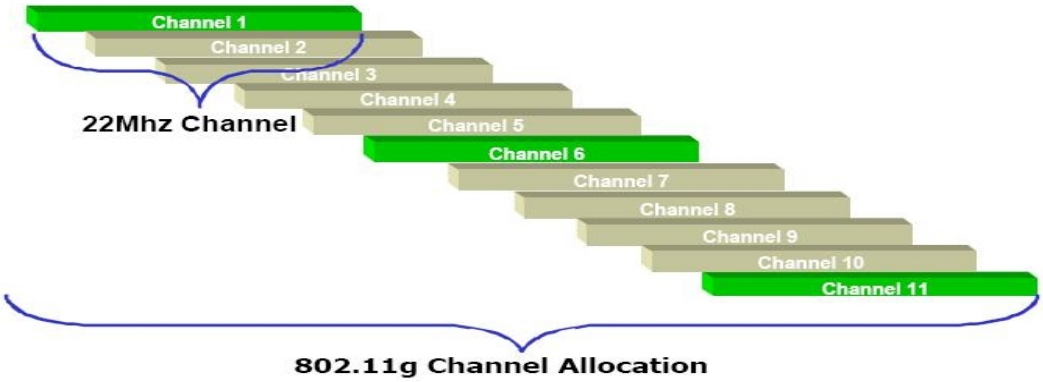
TD5: Wireless Local Area Networks (WLAN):Wifi or 803.11.



Part 1 – Wifi channels, protocol and frames

Wifi channels



In France the 802.11.g standard operates on 13 channels starting from 2.412 GHz. Each channel is 22 MHz wide with a 5MHz space between them (central frequency). For example channels 1, 6 and 11 are non-overlapping.

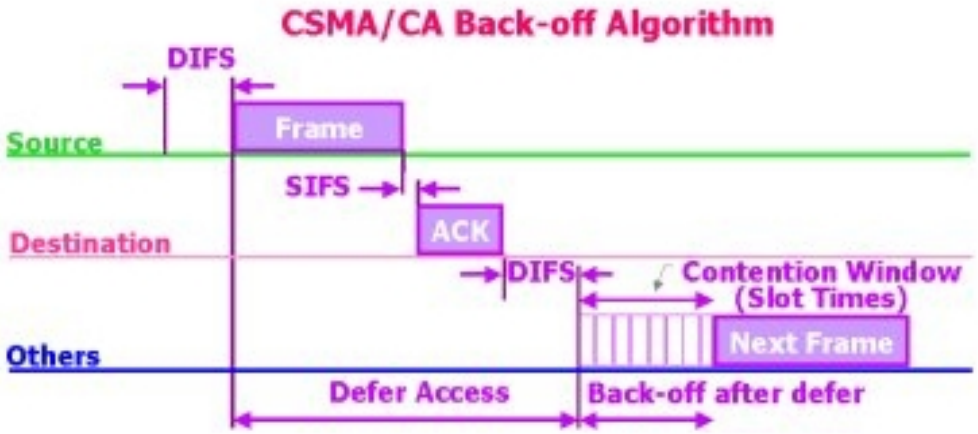
Exercise:

Calculate the frequency band of channel 6 and channel 11.

Wifi protocol and frames

The basic WiFi structure is connected to distribution network (Internet) by access points (AP), that is called BSS for basic service set. Note that WiFi protocol operates also with an ad-hoc configuration where the mobile hosts communicate directly between themselves.

WiFi (IEEE 803.11.x) uses CSMA/CA (**collision avoidance**) protocol on each radio channel. First it implies that the initial back-off value is not 0 slot, but something like 32 or 64 slots. After the "capture" of the channel the host sends the WiFi frames that carry **time reservation vector**, a value that indicates how long the transmission will take place. This value covers the time to send the data frame plus the time to receive the **acknowledgment** frame for this transaction. During this period all other stations must stay quiet. Note that WiFi protocol uses



the acknowledgment frame; on the radio channel this is the only way to know if the data frame has been received correctly.
On the figure above note Inter Frame slots: DIFS, SIFS and **back-off** sequence with short frame slots.

Explain why the CSMA/CA protocol starts with the back-off of 32 or 64 slots, (remind that Ethernet starts with 1 slot) ?

WiFi (MAC) frame header:

Frame (numbers indicate field length in bytes):

2	2	6	6	6	2	6	0-2312	4
Frame control	Duration	Address 1	Address 2	Address 3	Seq control	Address 4	Payload	CRC

Frame control field expanded (numbers indicate field length in bits):

2	2	4	1	1	1	1	1	1	1	1
Protocol version	Type	Subtype	To AP	From AP	More frag	Retry	Power mgt	More data	WEP	Rsvd

Explain the WiFi frame: why there are 4 MAC addresses ?, what is the meaning of control fields ?
Note that there are many types/subtypes of frames: Management, Control, and Data frames. Some of these frames are used to provide the accessibility and security: Assignment, Association, Encrypting, ..

Control fields:
type/subtype – type of frame: management, control, data
to AP/From AP – direction of the transmission
More frag – data transmission may be fragmented into several frames/fragments
Retry – retransmission
Power mgt – the mobile station may be in low power mode (sleep) – put to sleep/or awake
More data – more fragments indicator
WEP – open or WEP based authentication/encryption
Rsvd – strict processing order

Exercise: IEEE 802.11.g - useful data rate
Let us take a WiFi link with data rate **dr** and a standard WiFI frame with synchronization and control fields. The data field contains 1500 bytes.
A complete transaction implies 5 stages/periods:

- interframe period – **difs** (50 µs)
- average backoff period - **boffp** (from 0 to 31 slots) - each slot st (20 µs)
- frame transmission including:
  - **synchronization**: 192 bits at 1 Mb/s and
    this is the part of physical layer (coding, modulation) where the receiver and sender choose the modulation type/rate for the incoming transmission (it may depend on the distance from Access Point)
  - **overhead** with 34 bytes (MAC header and CRC) sent with 2,11,54 Mb/s
- short inter-frame spacing - **sifs** - 10 µs
- acknowledge frame **af** with 192 bits at 1 Mb/s and 14 bytes of data: 2,11,54 Mb/s

Evaluate the efficiency of the protocol for different link data rates (2,11, and 54 Mb/s):

efficiency = data_transmission_time/total_transmission_time

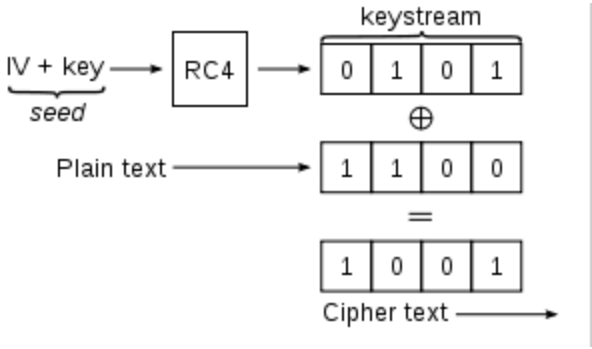
Take max data field size: 2312 bytes.

Part 2: WiFi and security (Wi-reless Fi-delity)

The radio transmission may be captured freely by any receiver close to the mobile station.
The first step is **association**.
The association is possible if the mobile station knows the MAC address of the Access Point. This may be done actively by the mobile station sending the request frame – probe (it contains the supporting data rates and so on) or passively by receiving the beacon frame send periodically by base station.
The following data transmission may be protected through the authentication and data encryption.
Study the basis of free kinds of security/authentication and encryption:

1. open authentication (how to protect the data ?, what can not be protected)
2. WEP (Wired Equivalent Privacy) based authentication and encrypting (symmetric key generated once for each session) – no cryptographic integrity protection (only CRC)
3. WAP1 based authentication and encrypting: WEP+TKIP (Temporal Key Integrity Protocol - key generated for each frame
4. WAP2 based on CCMP (Counter Cipher Mode) protocol (an AES-based encryption mechanism) – mandatory implementation since 2006

WEP: WEP uses the stream cipher RC4 for confidentiality.[5] and the CRC-32 checksum for integrity.[6] It was deprecated in 2004 and is documented in the current standard.
Standard 64-bit WEP uses a 40 bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key. At the time that the original WEP standard was drafted, the U.S. Government's export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, manufacturers of access points implemented an extended 128-bit WEP protocol using a 104-bit key size.



A 64-bit WEP key is usually entered as a string of 10 hexadecimal (base 16) characters (0-9 and A-F). Each character represents four bits, 10 digits of four bits each gives 40 bits; adding the 24-bit IV produces the complete 64-bit WEP key. Most devices also allow the user to enter the key as five ASCII characters, each of which is turned into eight bits using the character's byte value in ASCII; however, this restricts each byte to be a printable ASCII character, which is only a small fraction of possible byte values, greatly reducing the space of possible keys.

A 128-bit WEP key is usually entered as a string of 26 hexadecimal characters. Twenty-six digits of four bits each gives 104 bits; adding the 24-bit IV produces the complete 128-bit WEP key. Most devices also allow the user to enter it as 13 ASCII characters.

A 256-bit WEP system is available from some vendors. As with the other WEP-variants 24 bits of that is for the IV, leaving 232 bits for actual protection. These 232 bits are typically entered as 58 hexadecimal characters. ((58 × 4 bits =) 232 bits) + 24 IV bits = 256-bit WEP key.

Authentication

Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.

In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication. Any client can authenticate with the Access Point and then attempt to associate. In effect, no authentication occurs. Subsequently WEP keys can be used for encrypting data frames. At this point, the client must have the correct keys.

In Shared Key authentication, the WEP key is used for authentication in a four step challenge-response handshake:

1. The client sends an authentication request to the Access Point.
2. The Access Point replies with a clear-text challenge.
3. The client encrypts the challenge-text using the configured WEP key, and sends it back in another authentication request.
4. The Access Point decrypts the response. If this matches the challenge-text the Access Point sends back a positive reply.

After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4.

At first glance, it might seem as though Shared Key authentication is more secure than Open System authentication, since the latter offers no real authentication. However, it is quite the reverse. It is possible to derive the keystream used for the handshake by capturing the challenge frames in Shared Key authentication.[8] Hence, it is advisable to use Open System authentication for WEP authentication, rather than Shared Key authentication.

WPA: The WPA protocol implements the Temporal Key Integrity Protocol (TKIP). WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. **TKIP employs a per-packet key**, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.
WPA also includes a message **integrity check**. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard.

WPA2: WPA2 it introduces CCMP, a new AES-based encryption mode with strong security

PSK: Pre-shared key mode (PSK, also known as *Personal* mode) is designed for home and small office networks. Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. If ASCII characters are used, the 256 bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1.

CCMP: An AES-based encryption mechanism that is stronger than TKIP. Used by WPA2. Among informal names are "AES" and "AES-CCMP". According to the 802.11n specification, this encryption protocol **must be used** to achieve the fast 802.11n high bitrate schemes.

Case study:
WEP based protection: show how one can “crack” the WEP key
The result of ***airodump-ng mon1*** command (in monitor mode)

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:19:70:4C:C1:28  -35       41        0    0   6  54e. WPA2 CCMP   PSK  Livebox-cb5c
FA:2C:20:AA:12:89  -56       22        0    0   1  54e  OPN              FreeWifi
FA:2C:20:AA:12:8A  -52       21        0    0   1  54e  WPA  CCMP   MGT  FreeWifi_secure
4A:F9:DC:39:15:1D  -54       31        0    0  11  54e  OPN              FreeWifi
4A:F9:DC:39:15:1C  -54       28        0    0  11  54e  WEP  WEP         freefolies
4A:F9:DC:39:15:1E  -54       36        0    0  11  54e  WPA  CCMP   MGT  FreeWifi_secure
FA:2C:20:AA:12:88  -56       23        0    0   1  54e  WEP  WEP         freebox_MUWNQL
62:A1:D7:4F:E0:B7  -59       24        0    0   1  54e  WPA2 CCMP   MGT  SFR WiFi Mobile
62:A1:D7:4F:E0:B5  -60       22        0    0   1  54e  OPN              SFR WiFi Public
E0:A1:D7:4F:E0:B4  -59       24        2    0   1  54e  WPA  CCMP   PSK  SFR_E0B0
56:33:8E:EB:F2:20  -60       25        0    0   6  54e. OPN              orange
00:17:33:94:74:78  -61        8        0    0  11  54e  WPA  CCMP   PSK  NEUF_7474
5C:33:8E:EB:F2:20  -60       24        1    0   6  54e. WPA2 CCMP   PSK  Livebox-e3d0
00:19:70:5C:C7:A2  -62        6        0    0   6  54e. WPA2 CCMP   PSK  Livebox-3c16
62:17:33:94:74:7B  -62        6        0    0  11  54e  WPA2 CCMP   MGT  SFR WiFi Mobile
62:17:33:94:74:79  -62       11        0    0  11  54e  OPN              SFR WiFi Public
0A:19:70:5C:C7:A2  -63        8        0    0   6  54e. OPN              orange
62:25:15:BF:4F:F1  -63        2        0    0   7  54e  OPN              SFR WiFi Public
5C:33:8E:CF:15:AA  -64        3        0    0   6  54e. WPA2 CCMP   PSK  Livebox-e57d
52:33:8E:CF:15:AA  -64        3        0    0   6  54e. OPN              orange
96:FE:F4:AE:7E:71  -66        2        0    0   1  54e  OPN              Bouygues Telecom Wi-Fi
62:B8:04:B8:FD:E9  -66        7        0    0   1  54e  WPA2 CCMP   PSK  <length:  0>
62:B8:04:B8:FD:E8  -66       10        0    0   1  54   WPA  TKIP   PSK  freebox_DZHECV
96:FE:F4:AE:7E:70  -67        2        0    0   1  54e  WPA2 CCMP   PSK  Bbox-AE7E6D
```

OPN – no authentication required
WEP – only WEP key enabled (authorization and cypher)
WPA - cipher TKIP/CCMP + MGT/PSK authorization key

The ways/methods to decypher the installation/connection key:

- **Passive attacks to decrypt traffic:** These are based on **statistical analysis (WEP)**
- **Active attacks to inject new traffic from unauthorized mobile stations:** These are based on known plaintext (WEP)
- **Active attacks to decrypt traffic:** These are based on tricking the access point (WEP).
- **Dictionary-building attacks:** These are possible after analyzing enough traffic on a busy network (WPA).

The problems with the WEP algorithm. Check out these bugbears in the WEP initialization vector:

- **The IV is too small and in cleartext.** It's a 24-bit field sent in the cleartext portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes.

- **The IV is static.** Reuse of the same IV produces identical key streams for the protection of data, and because the IV is short, it guarantees that those streams will repeat after a relatively short time (between 5 and 7 hours) on a busy network.
- **The IV makes the key stream vulnerable.** The 802.11 standard does not specify how the IVs are set or changed, and individual wireless adapters from the same vendor may all generate the same IV sequences, or some wireless adapters may possibly use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use it to decrypt the ciphertext.
- **The IV is a part of the RC4 encryption key.** The fact that an eavesdropper knows 24-bits of every packet key, combined with a weakness in the RC4 key schedule, leads to a successful analytic attack that recovers the key after intercepting and analyzing only a relatively small amount of traffic. Such an attack is so nearly a no-brainer that it's publicly available as an attack script and as open-source code.
- **WEP provides no cryptographic integrity protection.** However, the 802.11 MAC protocol uses a non-cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledges packets that have the correct checksum. The combination of non-cryptographic checksums with stream ciphers is dangerous — and often introduces vulnerabilities. The classic case? You guessed it: WEP.

  There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet, and CRC sending it to the AP and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about ciphertext.

Only one of the problems listed above depends on a weakness in the cryptographic algorithm. Remember that IVs are the 24-bit values that are pre-pended to the secret key and used in the RC4 cipher. The IV is transmitted in **plaintext**. The reason we have IVs is to ensure that the value used as a seed for the RC4 PRNG is always different.

The key, whether it's 64 or 128 bits, is a combination of a shared secret and the IV. The IV is a 24-bit binary number. Do we choose IV values randomly? Do we start at 0 and increment by 1? Or do we start at 16,777,215 and decrement by 1? Most implementations of WEP initialize hardware using an **IV of 0**; **and increment by 1 for each packet sent**. Because every packet requires a unique seed for RC4, you can see that at higher volumes, the entire 24-bit space can be used up in a matter of hours. Statistical analysis shows that all possible IVs (2^{24}) are exhausted in about 5 hours. Then the IV re-initializes, starting at 0, every 5 hours.

The active steps to decrypt rapidely (few minutes) a WEP key are:

1. Switch your wifi into **monitor mode – you obtain monitor interface**
2. **Scan the network** and look for WEP enabled Access Points (we mean your own Access Points)
3. Look for hosts connected to the selected Access Point
4. Change your monitor MAC address to the selected/connected host MAC (spoofing)
5. Start sniffing ARP packets and reinject them into network
6. Start to register generated data traffic (dump)
7. Start WEP key cracking