SHARKFEST '12

Wireshark Developer and User Conference

Introduction to WiFi security and Aircrack-ng

Thomas d'Otreppe, Author of Aircrack-ng

~# whoami

- Author of Aircrack-ng and OpenWIPS-ng
- Work at NEK Advanced Securities Group

Agenda

- IEEE 802.11
- Wifi Networks
- Wireless Frames
- Network interaction
- Choose hardware
- Aircrack-ng suite

IEEE 802.11

- Institute of Electrical and Electronics Engineers
- Leading authority
- Split in committees and working groups
  - 802 committee: Network related norms
  - .11 working group: Wireless LAN
- Texts available for download

802.11 Protocols

- Lots of them
- Main protocols:
  - 802.11
  - 802.11a/b/g/n/ac
  - 802.11i

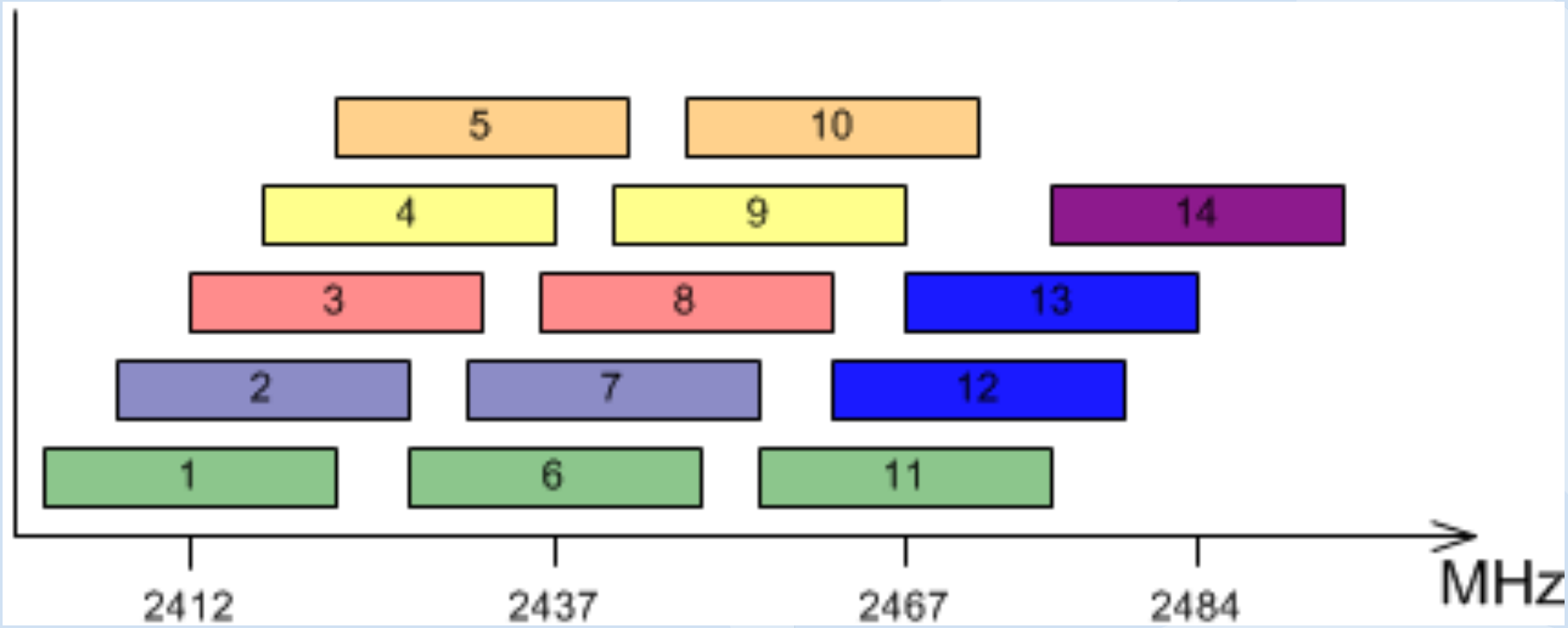
802.11

- Standard released in 1997
- Rates: 1-2Mbit
- Infrared/Radio (DSSS/FHSS)
- CSMA/CA

802.11b

- Amendment
- CCK coding
- New rates: 5.5 and 11Mbit
- 2.4GHz ISM band
- 14 overlapping channels
- 22MHz channels

802.11b (2)



802.11a

- 5GHz band
- More expensive => less crowded
- More than 14 channels (no overlap)
- OFDM
- Max rate: 54Mbit

802.11g

- ~= 802.11a on 2.4GHz
- Backward compatible with 802.11b

802.11n

- Work started in 2004 – Final: September 2009
- Single user MIMO
- 2.4GHz and 5GHz
- 40/80MHz channels
- MCS rates - http://mcsindex.com
- Greenfield mode

802.11n (2)

MCS Index	Number of spatial streams	Modulation (Stream 1/ 2/ 3/ 4)	Coding rate	$N_{BPSCS(iss)}$	N_{ES}		N_{SD}		N_{CBPS}		N_{DBPS}		Data Rate (in Mbps) (GI = 800ns)		Data Rate (in Mbps) (GI = 400ns)	
					20MHz	40MHz	20MHz	40MHz	20MHz	40MHz			20MHz	40MHz	20MHz	40MHz
0	1	BPSK	1/2	1	1	1	52	108	52	108			6.5	13.5	7.2	15.0
1	1	QPSK	1/2	2	1	1	52	108	104	216			13.0	27.0	14.4	30.0
2	1	QPSK	3/4	2	1	1	52	108	104	216			19.5	40.5	21.7	45.0
3	1	16-QAM	1/2	4	1	1	52	108	208	432			26.0	54.0	28.9	60.0
4	1	16-QAM	3/4	4	1	1	52	108	208	432			39.0	81.0	43.3	90.0
5	1	64-QAM	2/3	6	1	1	52	108	312	648			52.0	108.0	57.8	120.0
6	1	64-QAM	3/4	6	1	1	52	108	312	648			58.5	121.5	65.0	135.0
7	1	64-QAM	5/6	6	1	1	52	108	312	648			65.0	135.0	72.2	150.0
8	2	BPSK	1/2	1	1	1	52	108	104	216			13.0	27.0	14.4	30.0
9	2	QPSK	1/2	2	1	1	52	108	208	432			26.0	54.0	28.9	60.0
10	2	QPSK	3/4	2	1	1	52	108	208	432			39.0	81.0	43.3	90.0
11	2	16-QAM	1/2	4	1	1	52	108	416	864			52.0	108.0	57.8	120.0
12	2	16-QAM	3/4	4	1	1	52	108	416	864			78.0	162.0	86.7	180.0
13	2	64-QAM	2/3	6	1	1	52	108	624	1296			104.0	216.0	115.6	240.0
14	2	64-QAM	3/4	6	1	1	52	108	624	1296			117.0	243.0	130.3	270.0
15	2	64-QAM	5/6	6	1	1	52	108	624	1296			130.0	270.0	144.4	300.0
16	3	BPSK	1/2	1	1	1	52	108	156	324			19.5	40.5	21.7	45.0
17	3	QPSK	1/2	2	1	1	52	108	312	648			39.0	81.0	43.3	90.0
18	3	QPSK	3/4	2	1	1	52	108	312	648			58.5	121.5	65.0	135.0
19	3	16-QAM	1/2	4	1	1	52	108	624	1296			78.0	162.0	86.7	180.0
20	3	16-QAM	3/4	4	1	1	52	108	624	1296			117.0	243.0	130.0	270.0
21	3	64-QAM	2/3	6	1	2	52	108	936	1944			156.0	324.0	173.3	360.0

802.11ac

- Ran out of single letters, hence why 2 letters
- First draft: January 2011
- 5GHz only
- Multi user MIMO
- Different MCS rates – Up to 1Gbit/s+/user
- 80/160MHz channels

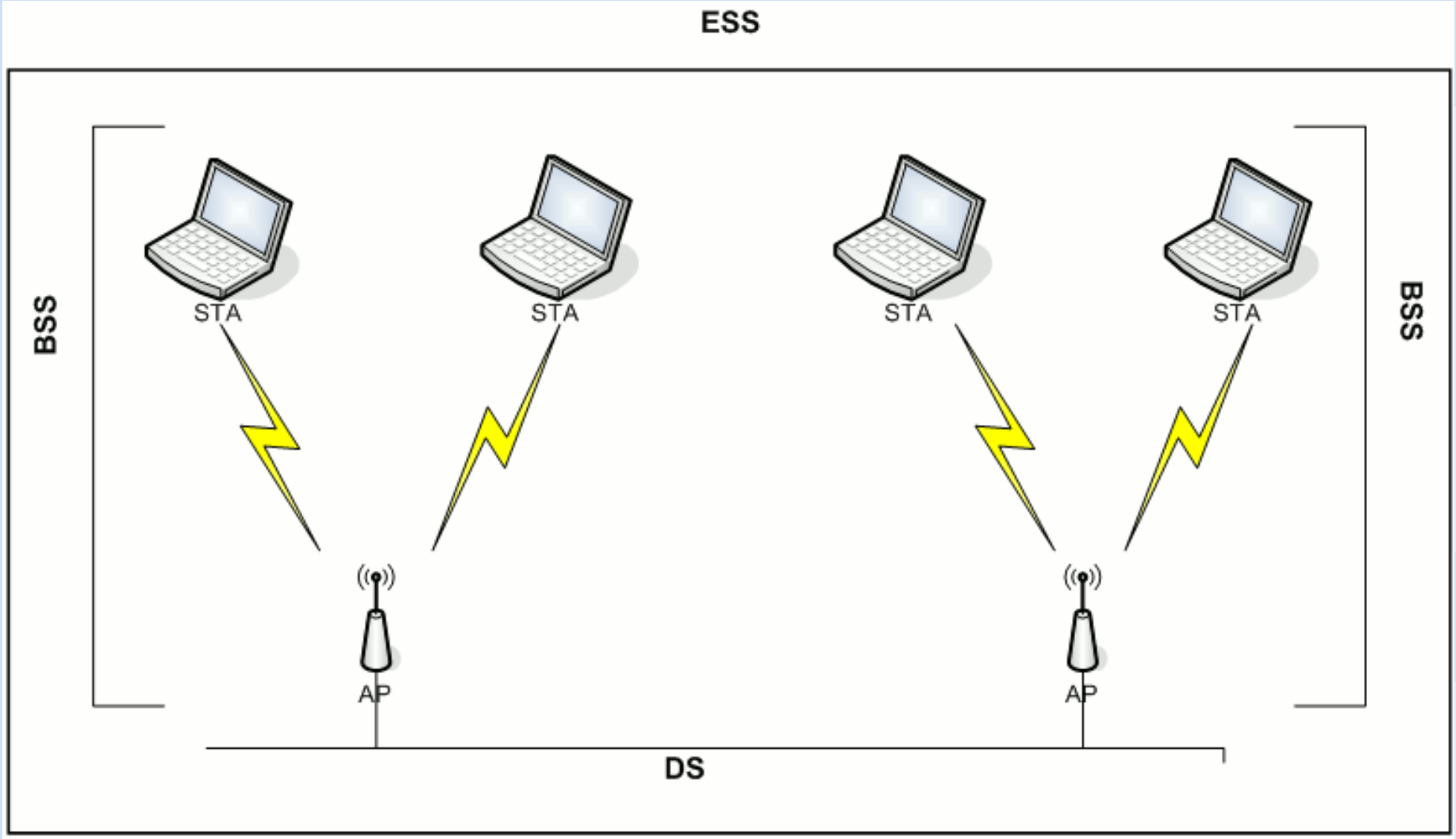
802.11ac – MCS rates 1x1

MCS index	Spatial streams	Modulation type	Coding rate	20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195
3	1	16-QAM	1/2	26	28.9	54	60	117	130	234	260
4	1	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390
5	1	64-QAM	2/3	52	57.8	108	120	234	260	468	520
6	1	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
7	1	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650
8	1	256-QAM	3/4	78	86.7	162	180	351	390	702	780
9	1	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7

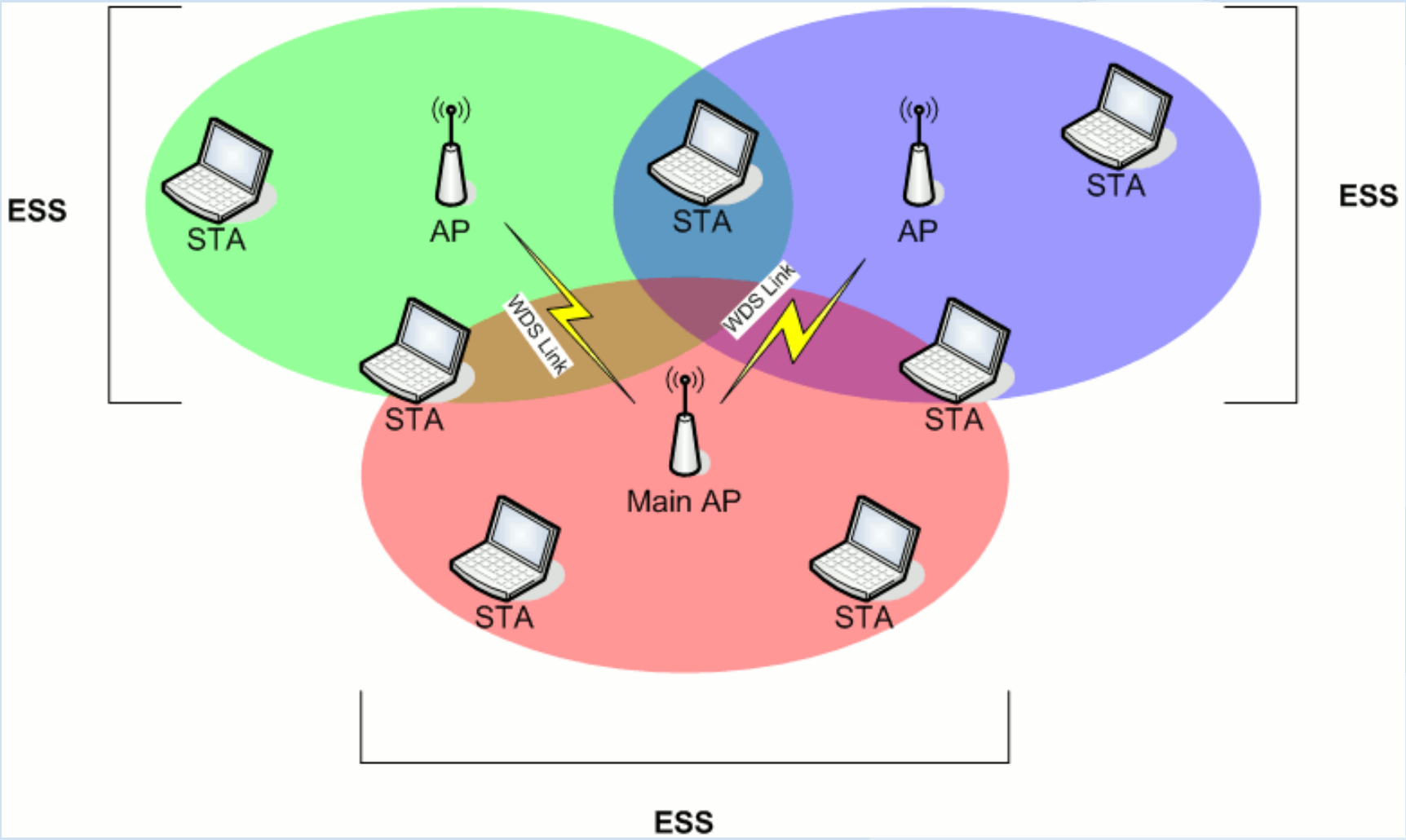
802.11 Networks

- 3 main modes of wireless operations
  - Infrastructure
    - WDS
  - Ad Hoc
  - Monitor Mode

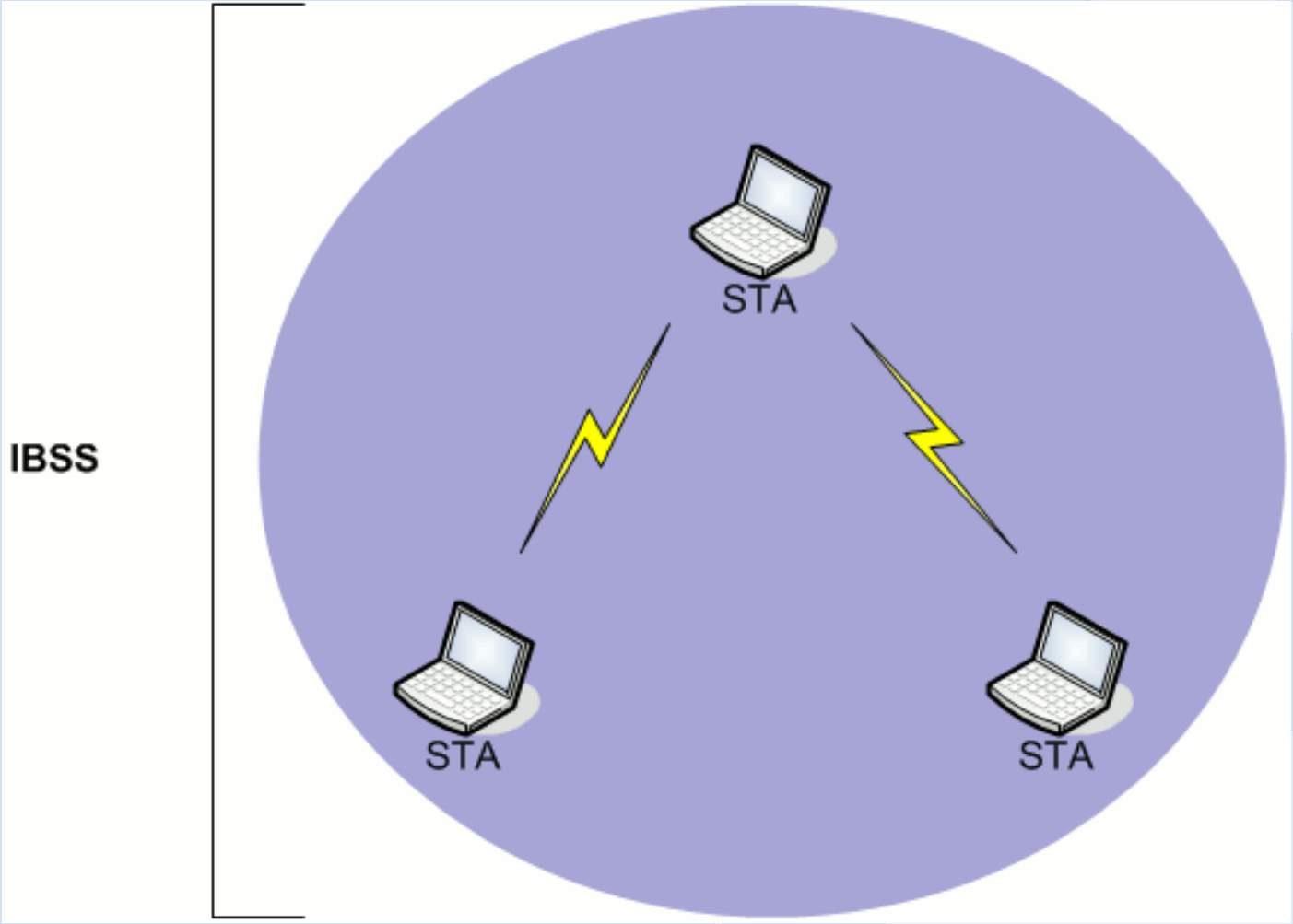
802.11 Networks - Infrastructure



802.11 Networks - WDS



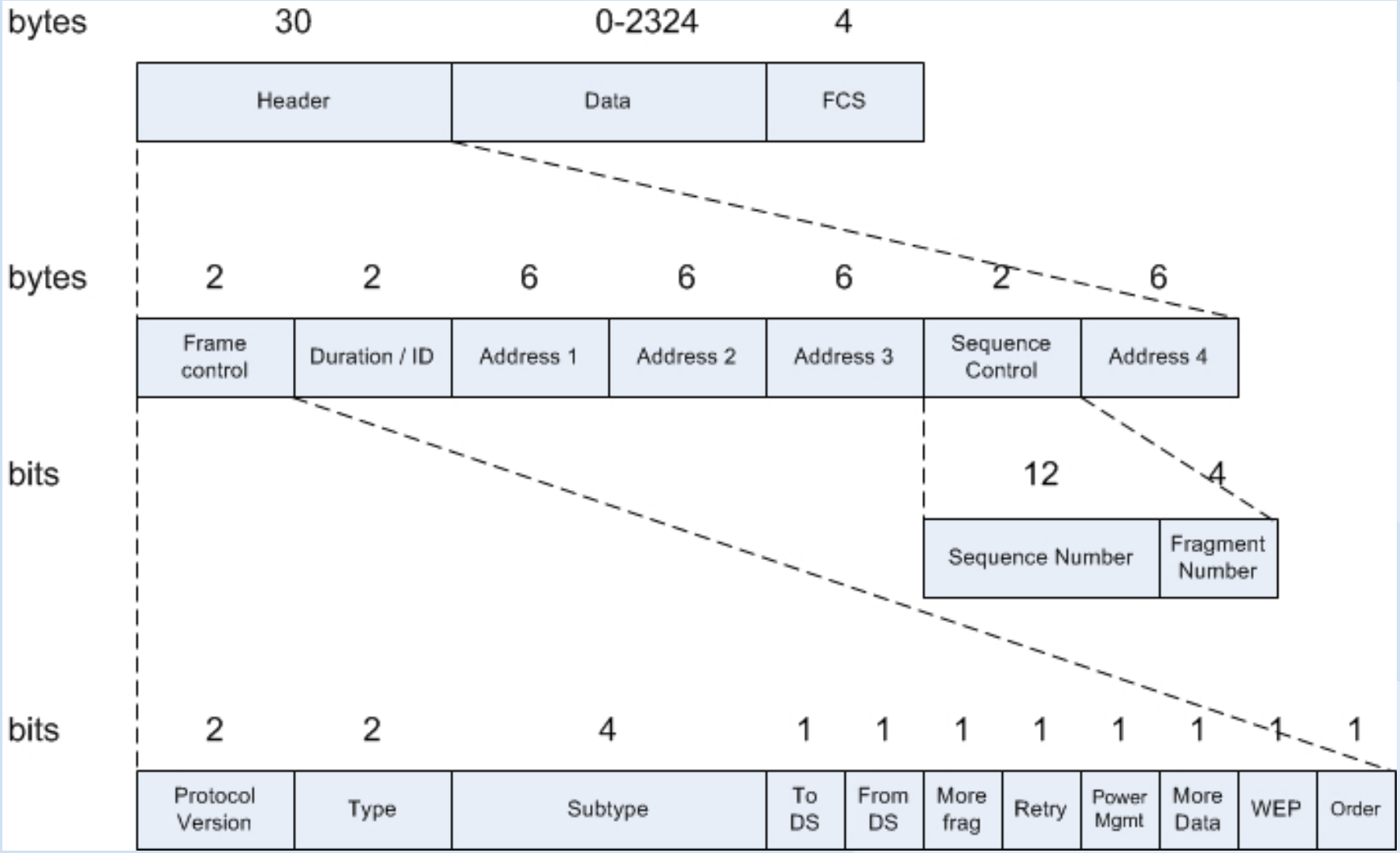
802.11 Networks – Ad Hoc



802.11 Frames

- Frame format
- 3 Types of frames
  - Management
  - Control
  - Data

802.11 Frame


bytes
30
0-2324
4
Header
Data
FCS
bytes
2
2
6
6
6
2
6
Frame control
Duration / ID
Address 1
Address 2
Address 3
Sequence Control
Address 4
bits
12
4
Sequence Number
Fragment Number
bits
2
2
4
1
1
1
1
1
1
1
1
Protocol Version
Type
Subtype
To DS
From DS
More frag
Retry
Power Mgmt
More Data
WEP
Order

802.11 Frame – ToDS/FromDS fields

ToDS	FromDS	Address 1	Address 2	Address 3	*Address 4*
0	0	DA	SA	BSSID	
0	1	DA	BSSID	SA	
1	0	BSSID	SA	DA	
1	1	RA	TA	DA	SA

- DA: Destination Address
- RA: Recipient Address
- SA: Source Address
- TA: Transmitter Address
- BSSID: Basic Service Set Identifier – MAC of the Access Point

802.11 Frames – Management Frames

Type	Subtype	Meaning
0	0	Association Request
0	1	Association Response
0	2	Reassociation Request
0	3	Reassocation Response
0	4	Probe Request
0	5	Probe Response
0	6	Measurement Pilot
0	7	**Reserved**

802.11 Frames – Management Frames (2)

Type	Subtype	Meaning
0	8	Beacon
0	9	ATIM
0	10	Disassociation
0	11	Authentication
0	12	Deauthentication
0	13	Action
0	14	Action No ACK
0	15	**Reserved**

802.11 Frames – Control Frames

Type	Subtype	Meaning
1	0-6	Reserved
1	7	Control Wrapper
1	8	Block ACK request
1	9	Block ACK
1	10	PS Poll
1	**11**	**RTS**
1	**12**	**CTS**
1	**13**	**ACK**
1	14	CF End
1	15	CF End + CF ACK

802.11 Frames – Data Frames

Type	Subtype	Meaning
2	**0**	**Data**
2	1	Data + CF ACK
2	2	Data + CF Poll
2	3	Data + CF ACK + CF Poll
2	4	Null Function (no data)
2	5	CF ACK (no data)
2	6	CF Poll (no data)
2	7	CF ACK + CF Poll (no data)

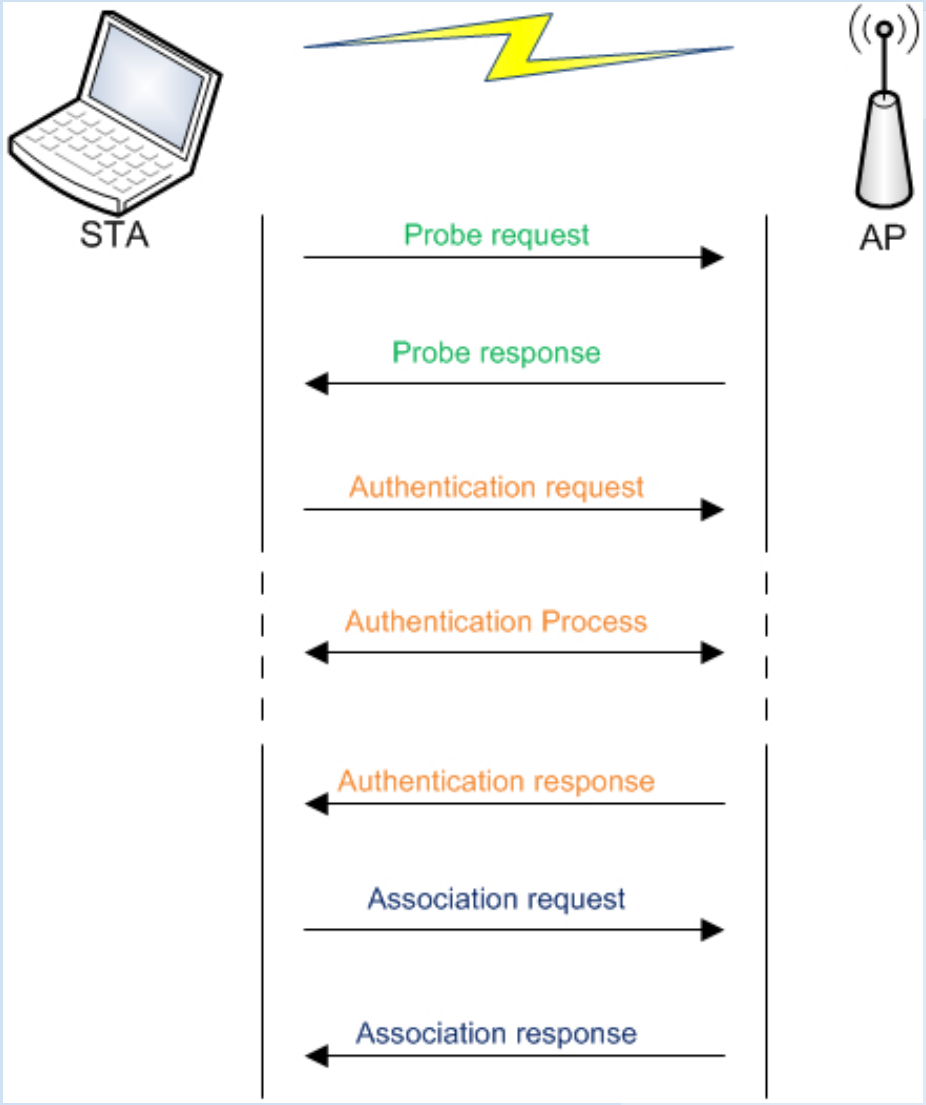
802.11 Frames – Data Frames (2)

Type	Subtype	Meaning
2	8	QoS data
2	9	QoS data + CF ACK
2	10	QoS data + CF Poll
2	11	QoS data + CF ACK + CF Poll
2	12	QoS Null (no data)
2	13	**Reserved**
2	14	QoS CF Poll (no data)
2	15	QoS CF ACK (no data)

Network interaction

- Connection to a network
- Open networks
- WEP networks
- WPA networks

Network interaction



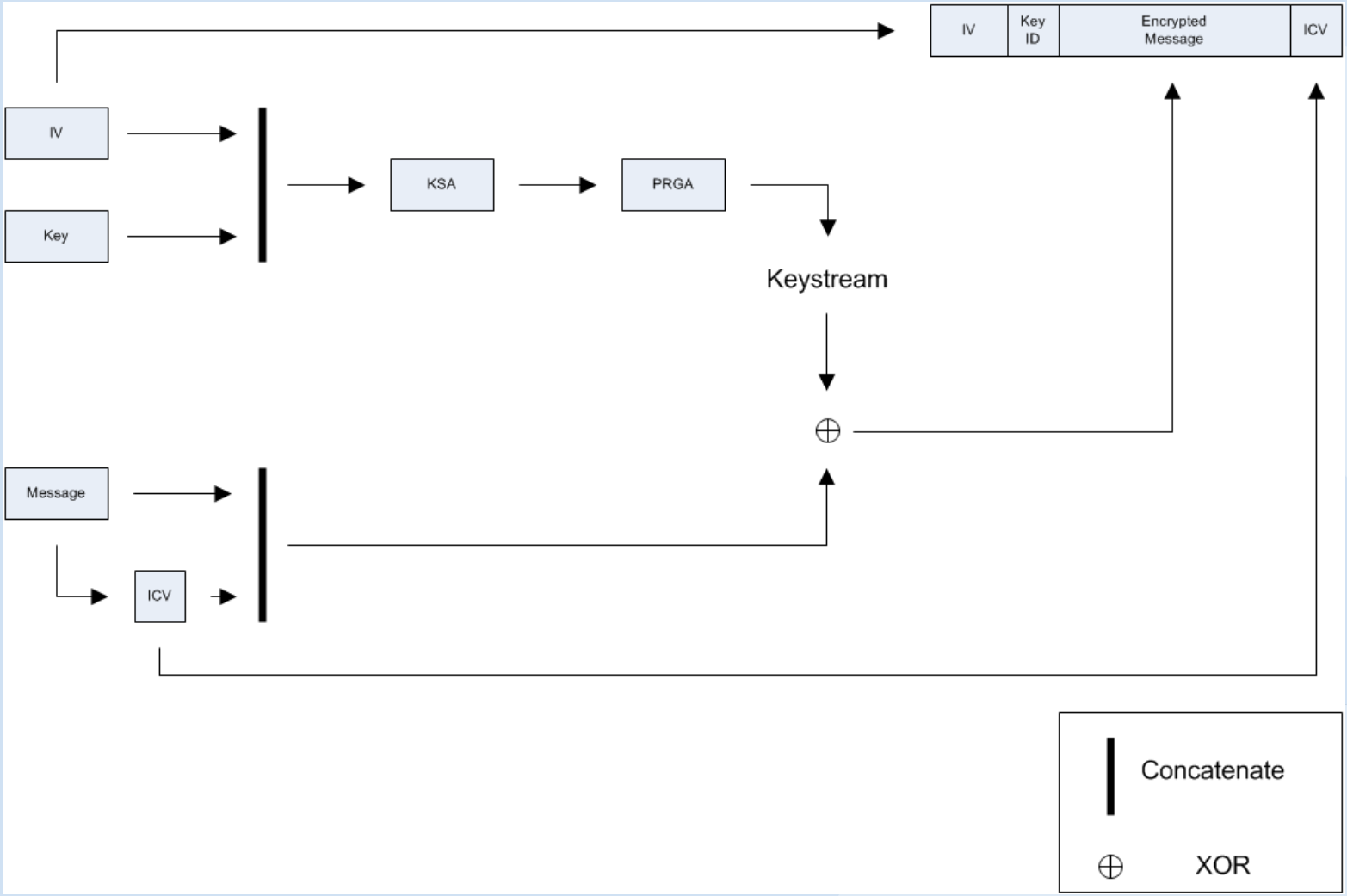
Network interaction – Open Networks

- Network_Interaction.pcap

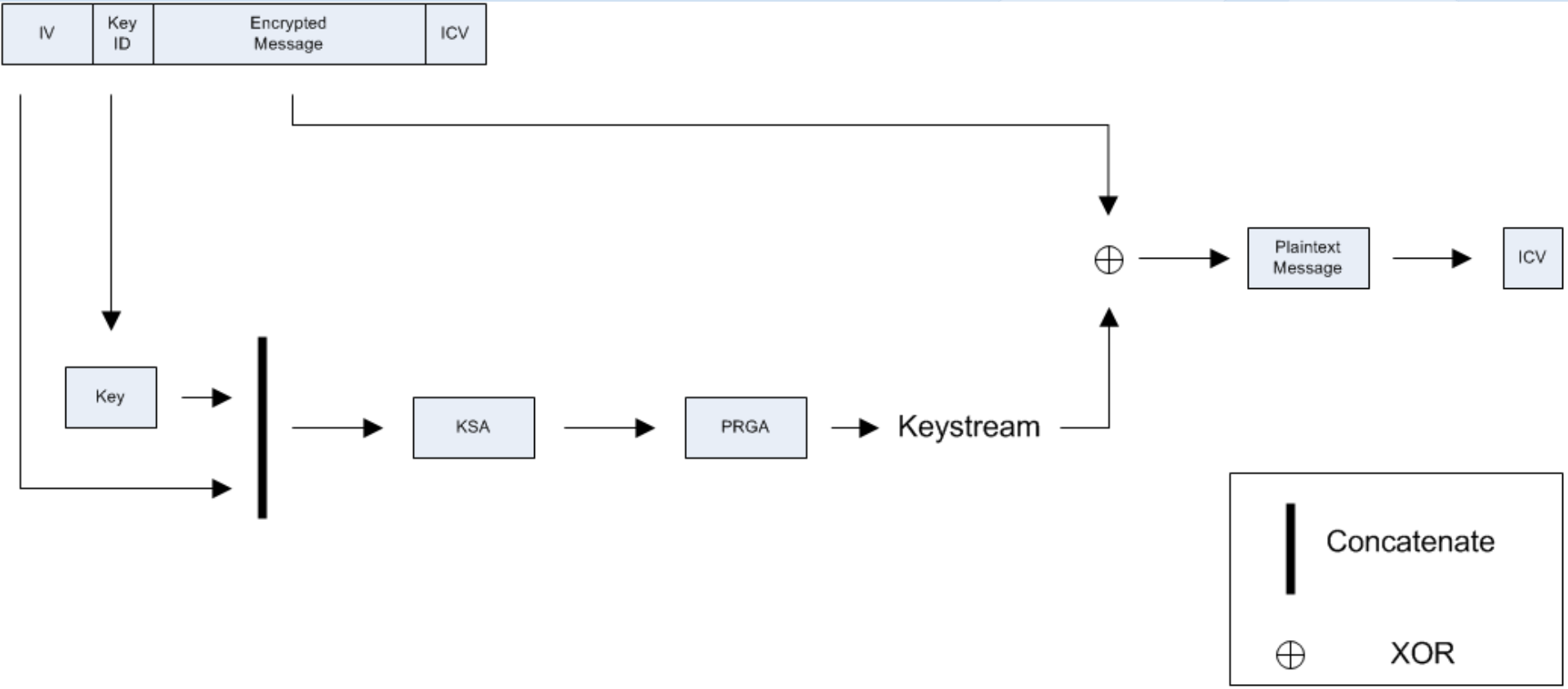
Network Interaction - WEP

- Wired Equivalent Privacy
- RC4
  - 24 bit Initialization Vector
  - Key Scheduling Algorithm
  - Pseudo Random Generation Algorithm
- CRC32

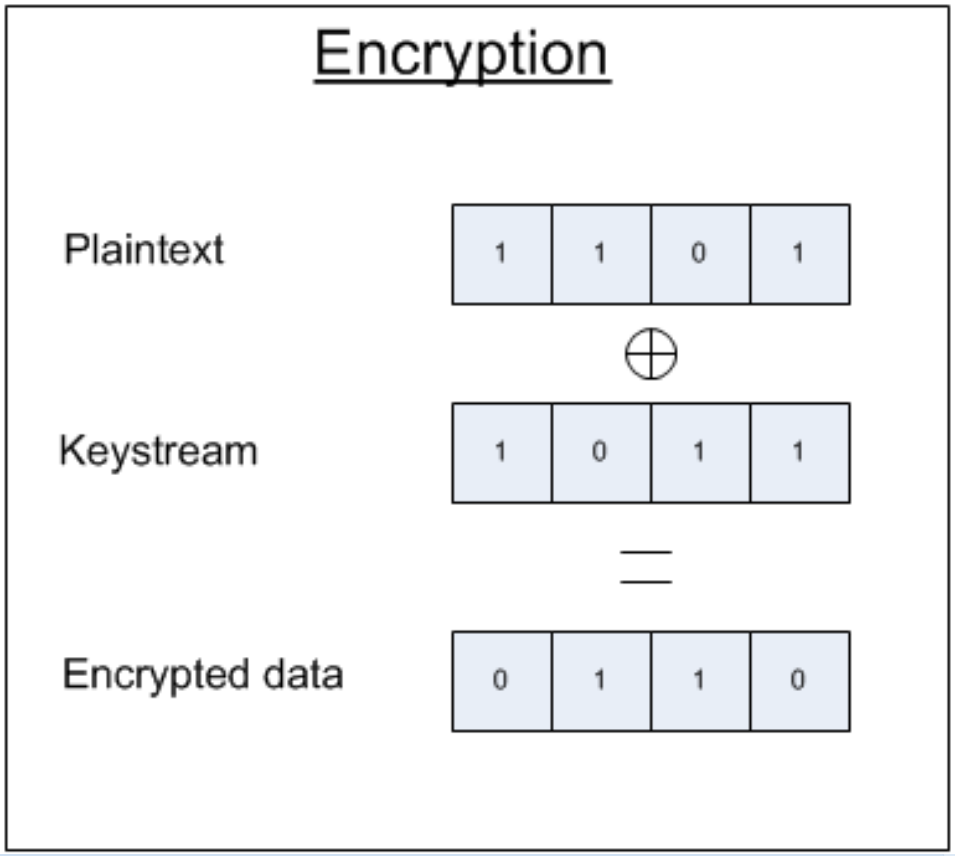
Network Interaction – WEP - Encrypt

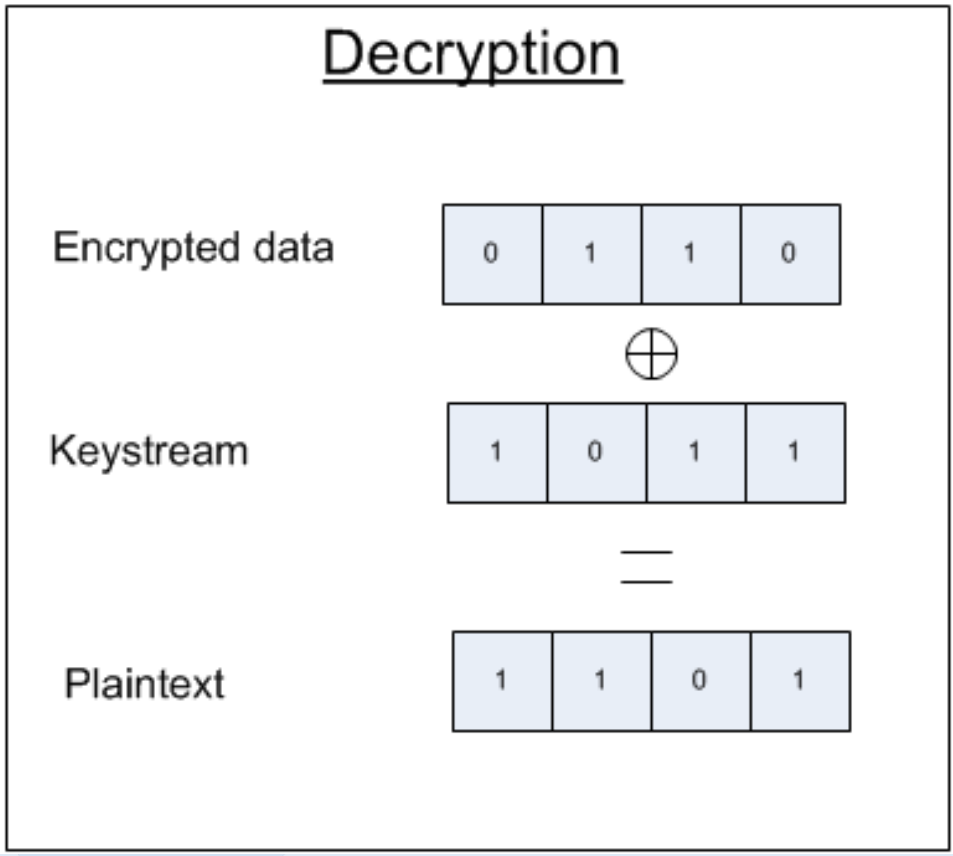


Network Interaction – WEP - Decrypt



Network Interaction – WEP





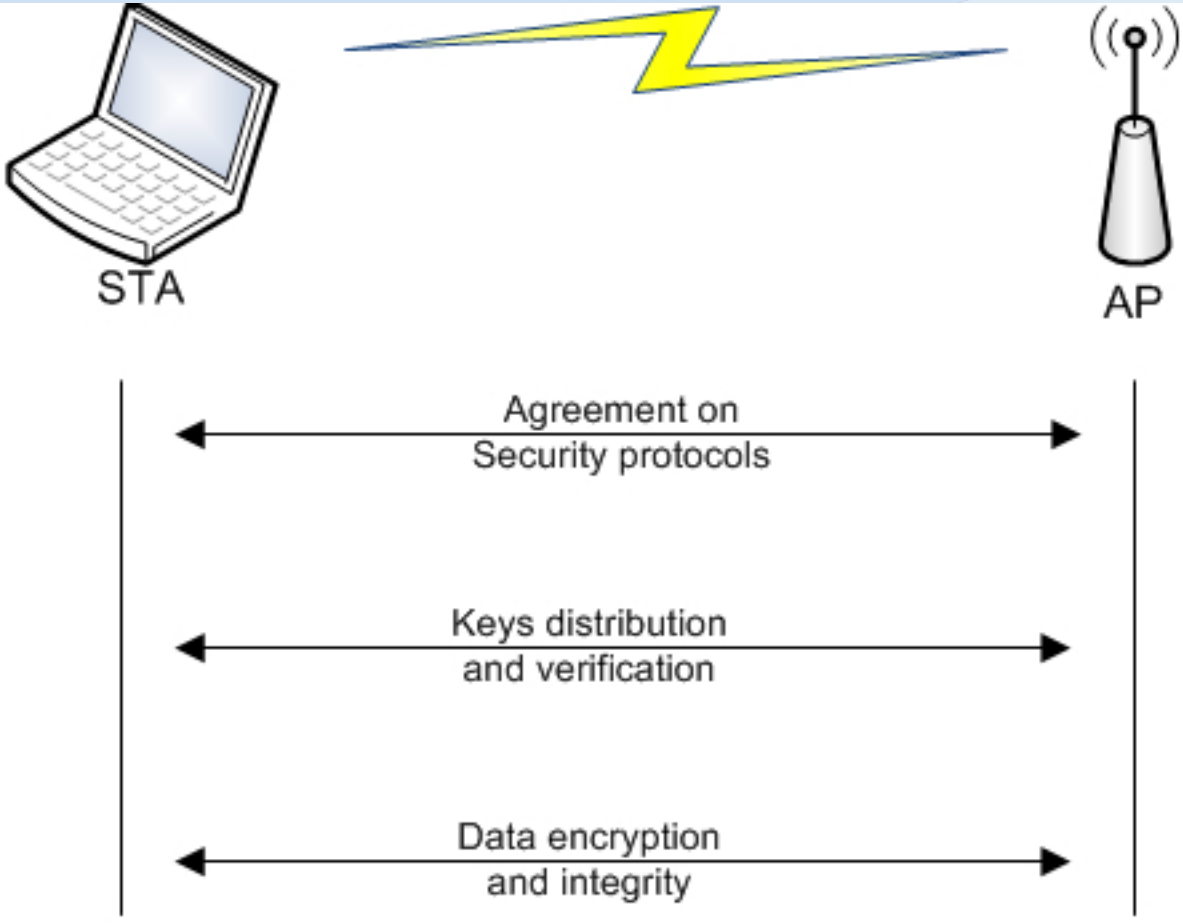
Network Interaction – WPA

- IEEE created 802.11i working group when WEP flaws discovered
- 2 Link layer protocols
  - TKIP -> WPA1
  - CCMP -> WPA2
- 2 flavors
  - Personal: PSK
  - Enterprise

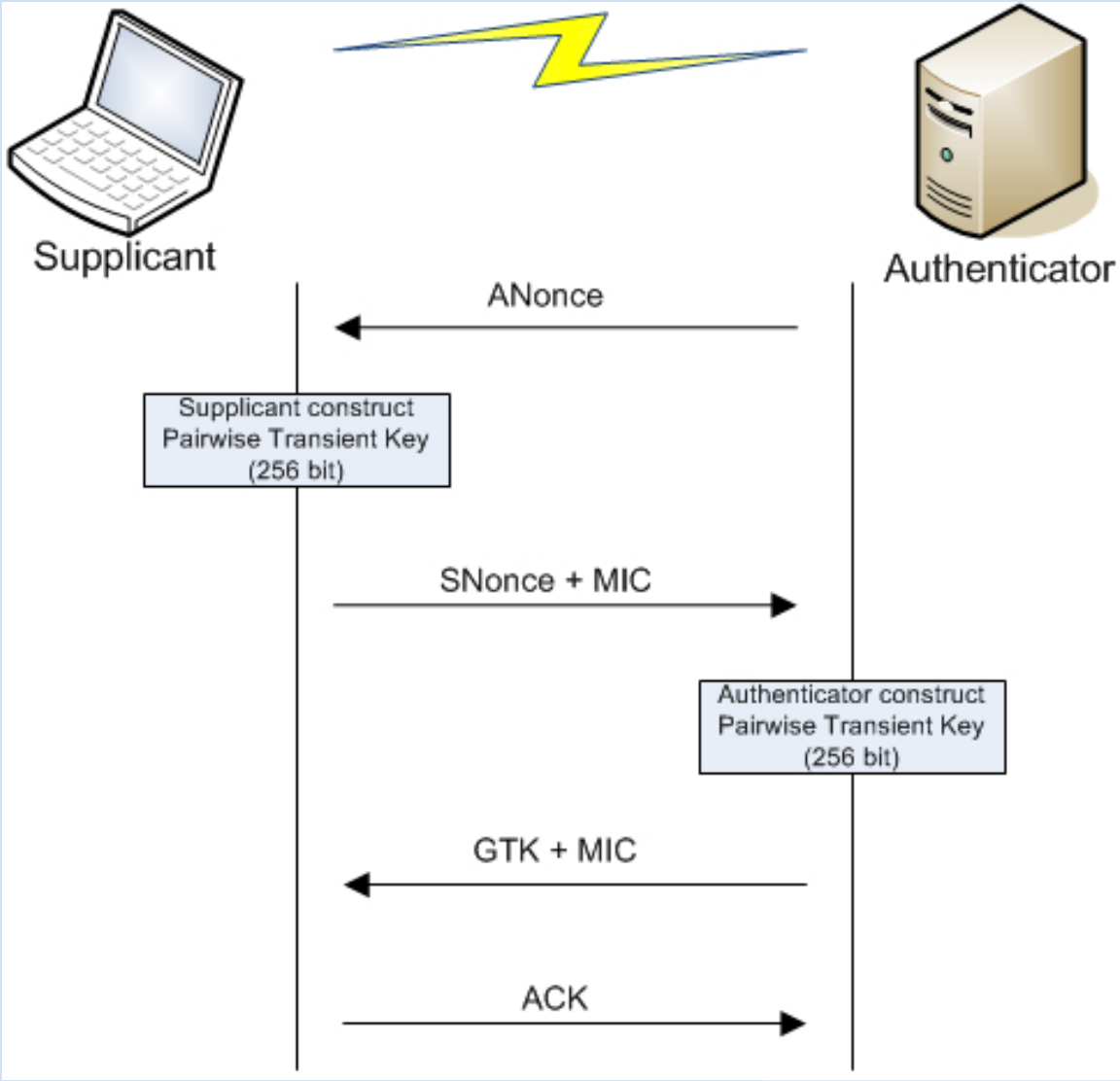
Network Interaction – WPA

- WPA 1
  - Based on 3rd draft of 802.11i
  - Uses TKIP
  - Backward compatible with old hardware
- WPA 2
  - 802.11i
  - Uses CCMP (AES)
  - Not compatible with old hardware

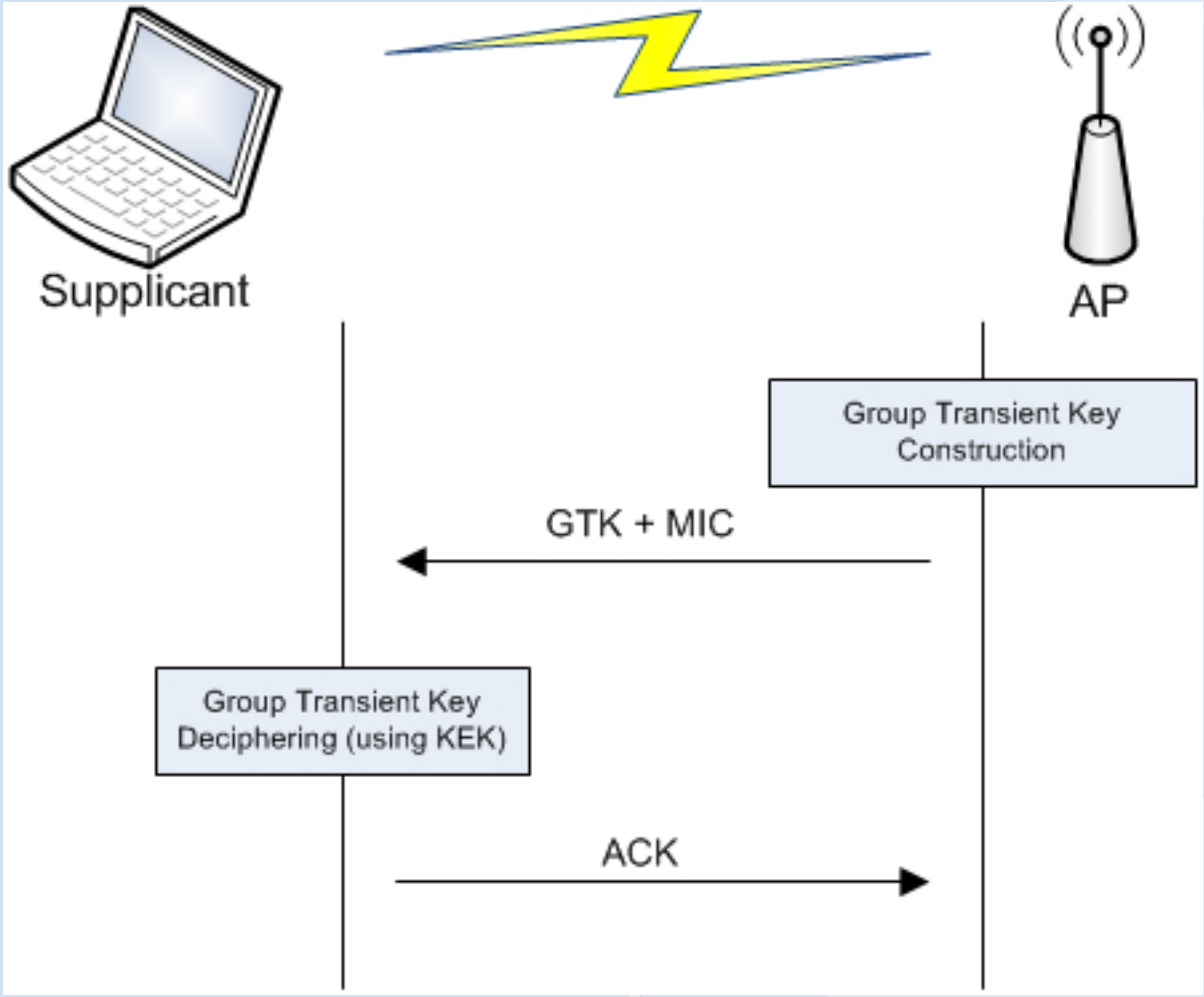
Network Interaction – WPA PSK



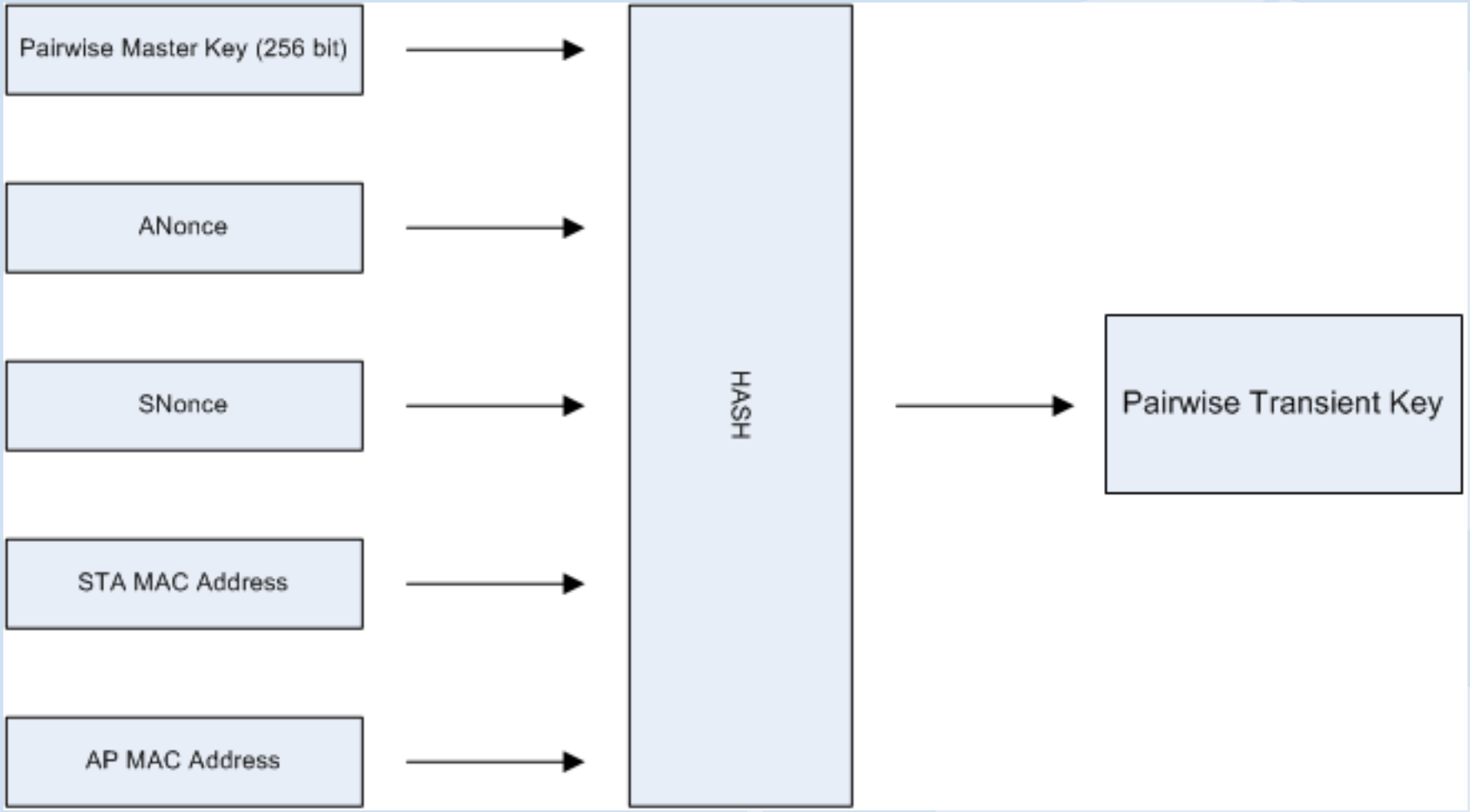
Network Interaction – WPA Authentication



Network Interaction – WPA – GTK



Network Interaction – WPA – PTK Construction



Network Interaction – WPA – Encryption and data integrity

- TKIP:
  - MIC + ICV
- CCMP
  - MIC

Choosing hardware

- Wireless adapter
- Antenna
  - Omni vs directional
  - Antenna pattern
  - Some math

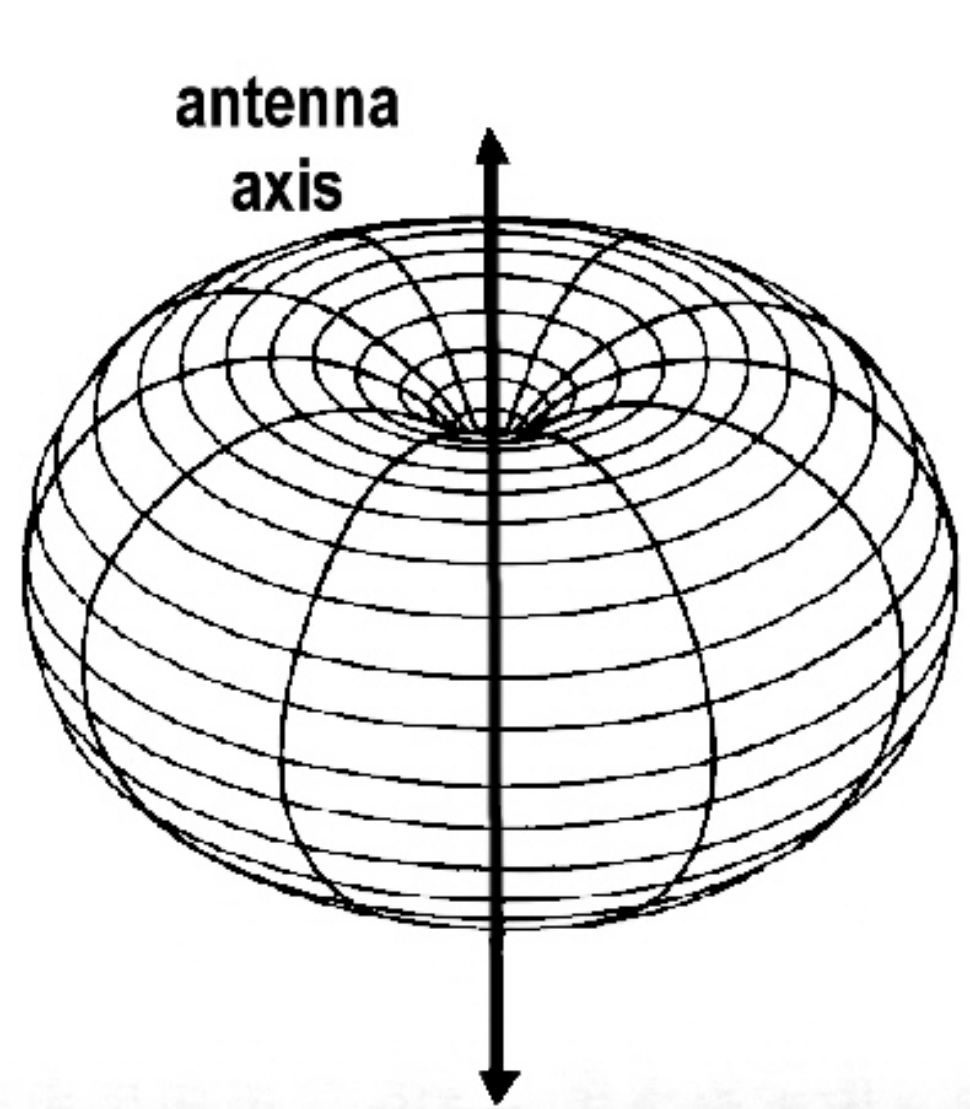
Choose a card

- Recommended chipsets
  - Atheros (Internal/PCI/Cardbus/Expresscard)
  - Realtek 8187
  - Ralink (802.11n)
- Better if with an antenna connector
- How to find the chipset?
  - Sometimes advertised
  - Run Linux and use airmon-ng/dmesg/lspci/lsusb
  - Through Windows driver

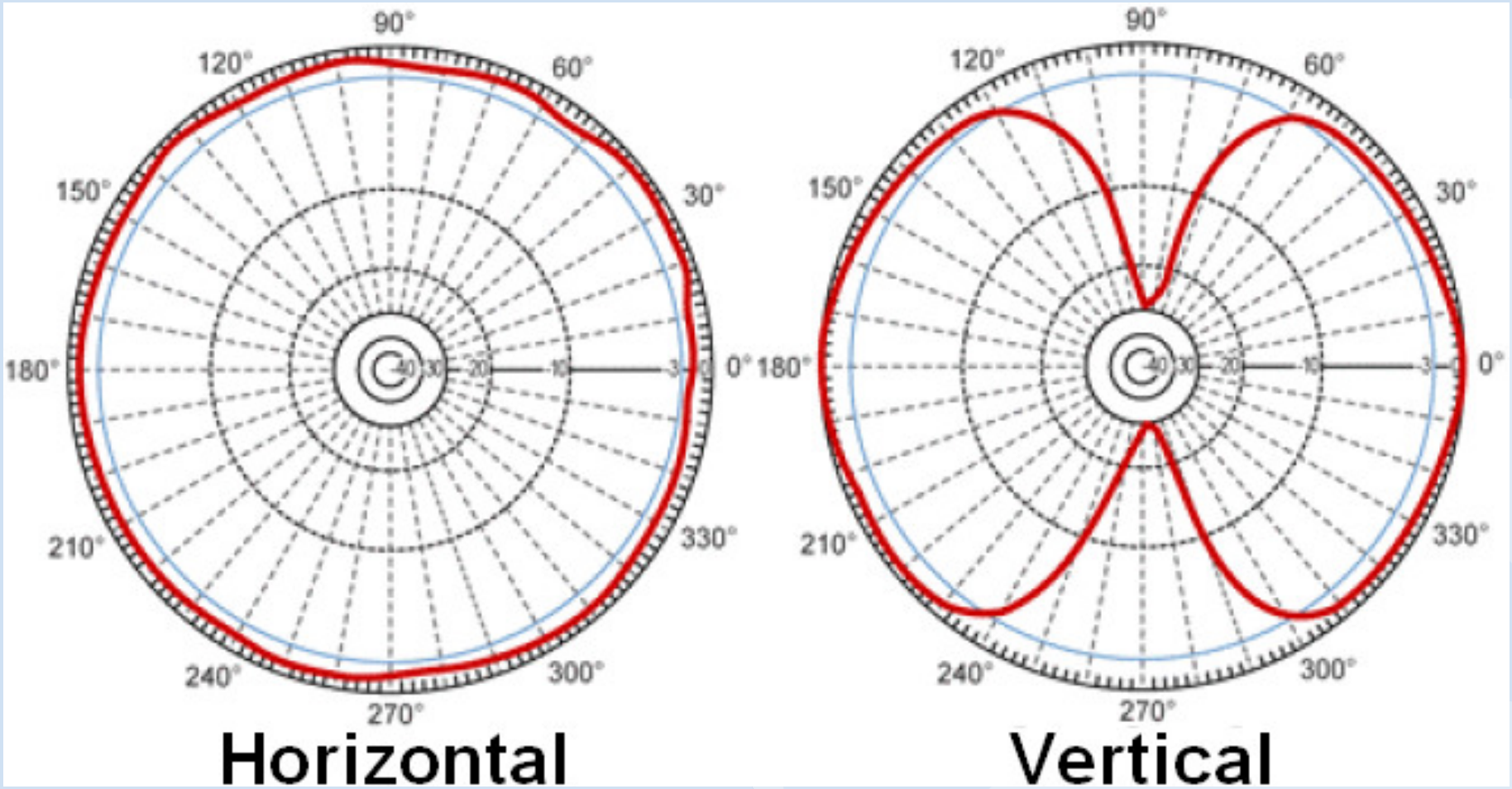
Choose an antenna – Omni/directional

- Bigger != Better
- Different gain = different RF propagation
- Omnidirectional:
  - Radiate in all directions, like a light bulb
- Directional:
  - Radiate in a single direction, like a camera zoom

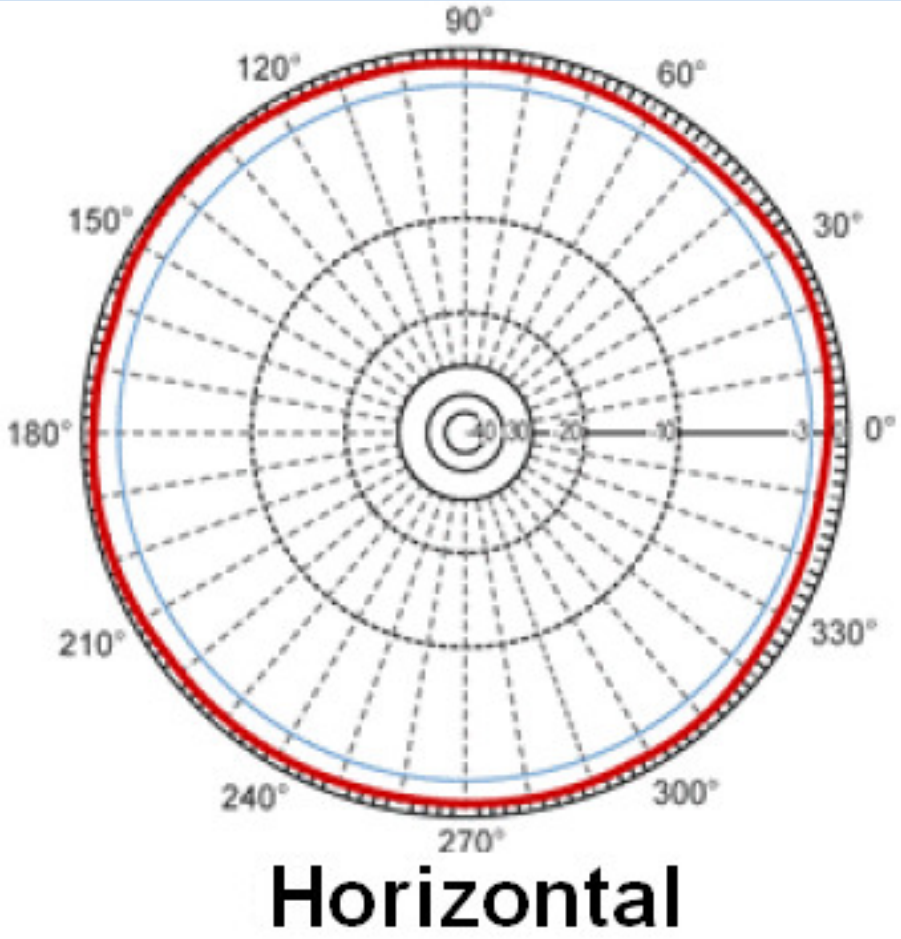
Choose an antenna – Omnidirectional



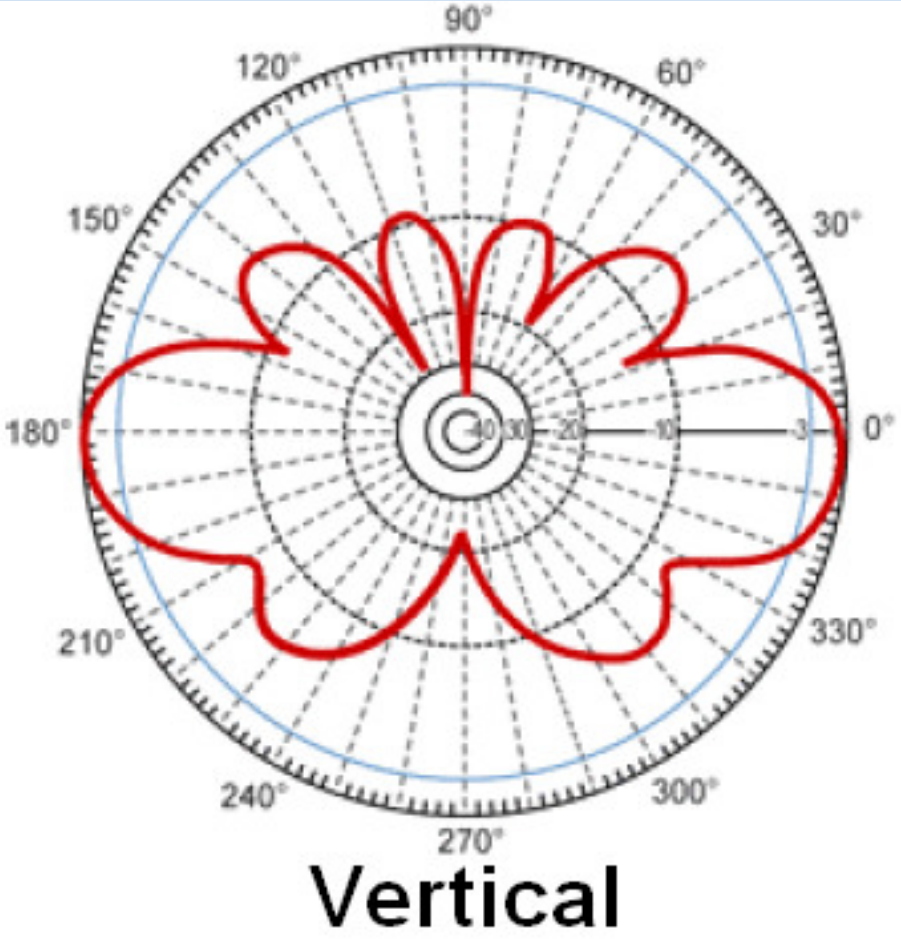
Choose an antenna – Omnidirectional (2)



Choose an antenna – Omnidirectional (3)

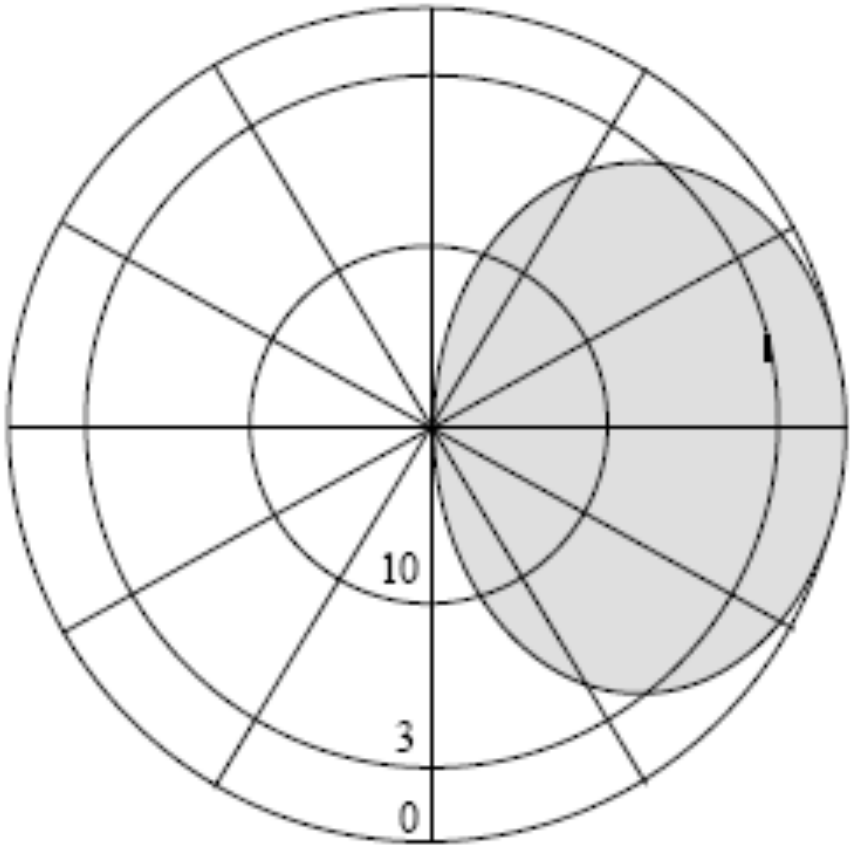


Horizontal

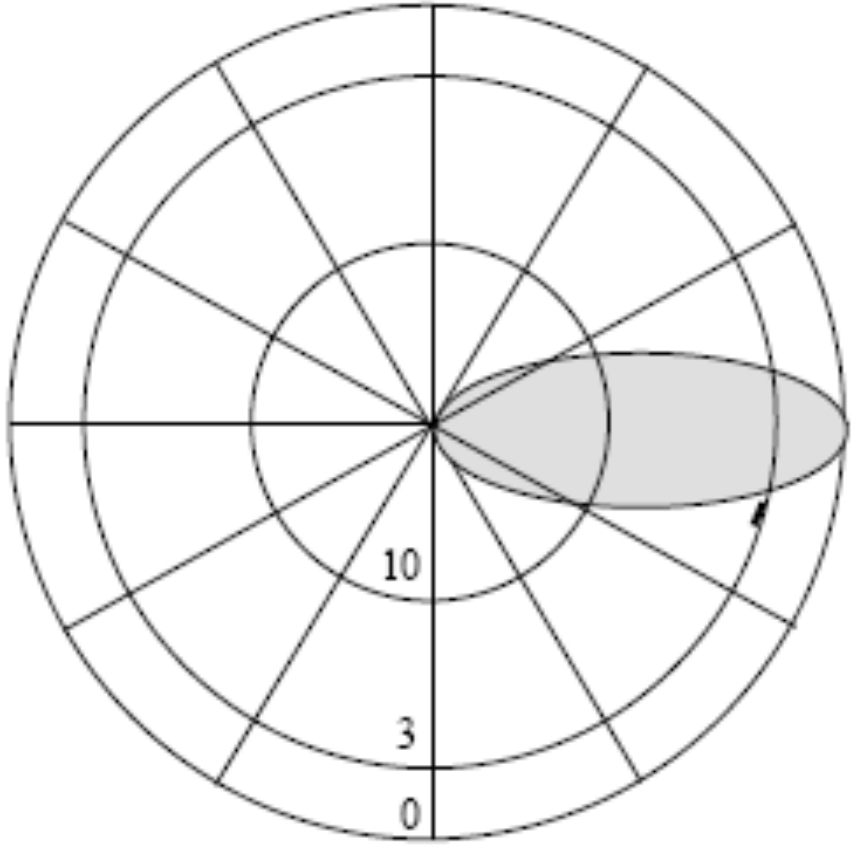


Vertical

Choose an antenna – Directional

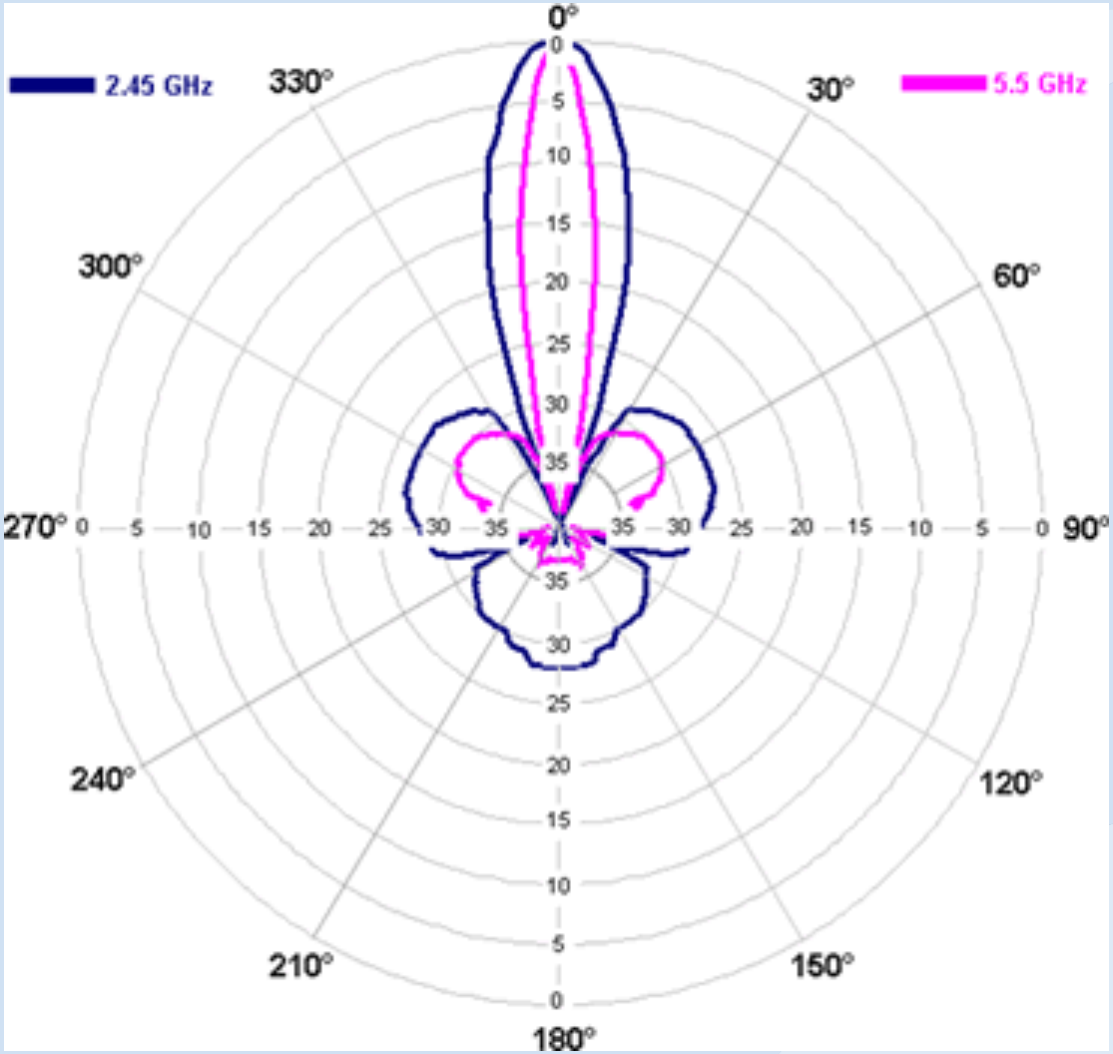


Horizontal Pattern



Vertical Pattern

Choose an antenna – Directional (2)



Choose an antenna - Math

- dB measures signal against normalized value: 1mW
  - dB power = 10 * log (signal / reference)
- How much dB is 100mW?
  - 10* log(100mW/1mW) = 20dBm

Choose an antenna – dBm - mW

- A 3dB increase = 2 times the power

dBm	mW
0	1
10	10
15	32
17	50
20	100
23	200
27	512
30	1000

Choose an antenna – Cables/connectors

- Cables & connectors add loss
- If broken, even more
- Adapters: ~0.5db
- Cables: depends on thickness

Choose an antenna - Exercise

- Example with an antenna and then add a cable (real values)

- Alfa AWUS036H: 500mW
- Antenna: 5dB
- Cable: RG58, 2 meters (~1dB/meter)

Aircrack-ng suite

- What is it?
- Different tools
- Installation
- Drivers installation

Aircrack-ng suite

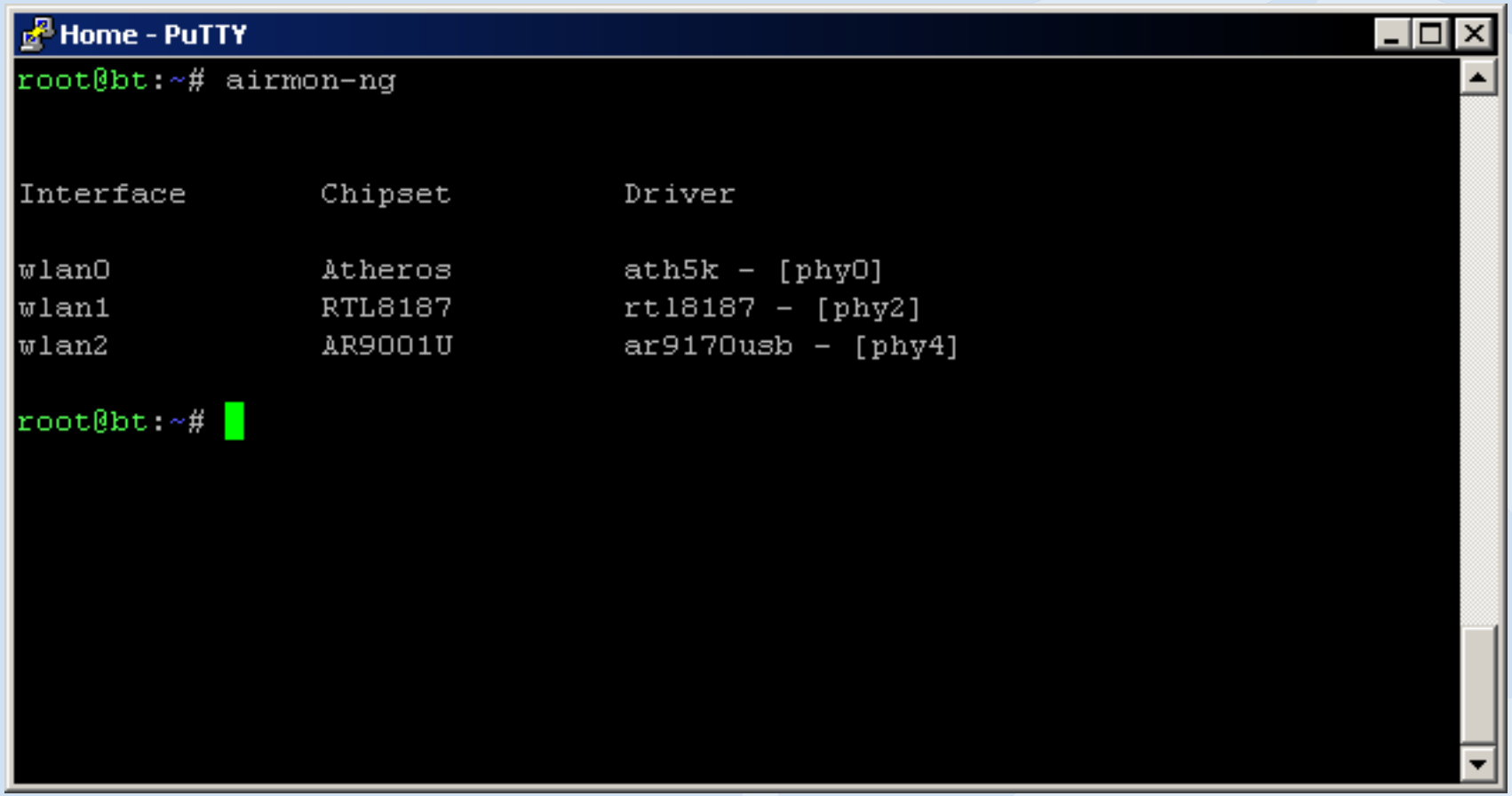
- What is it?

  "Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.

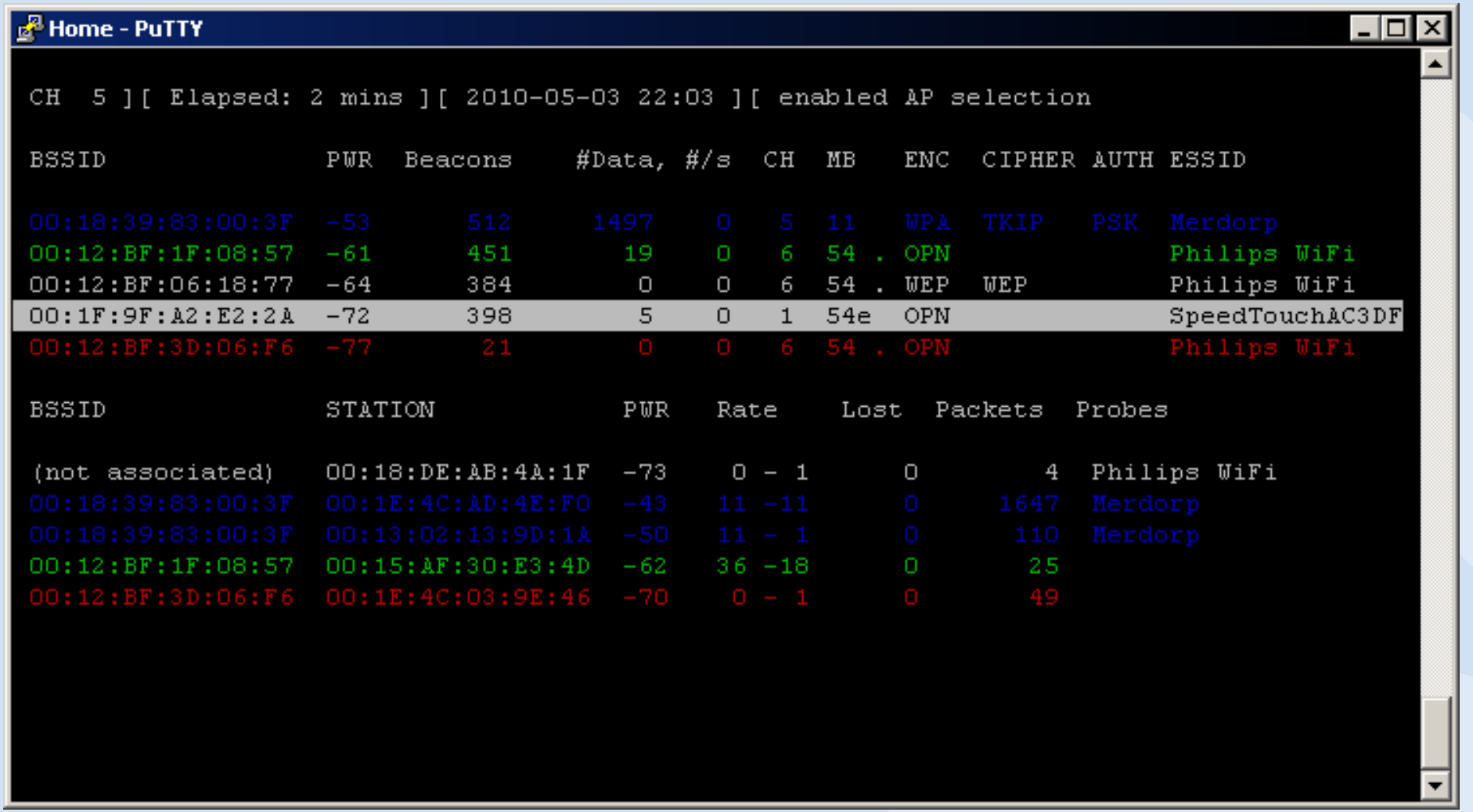
  In fact, Aircrack-ng is a set of tools for auditing wireless networks."

- Lots of scripts use it
- Important to know the tools to correctly use the scripts

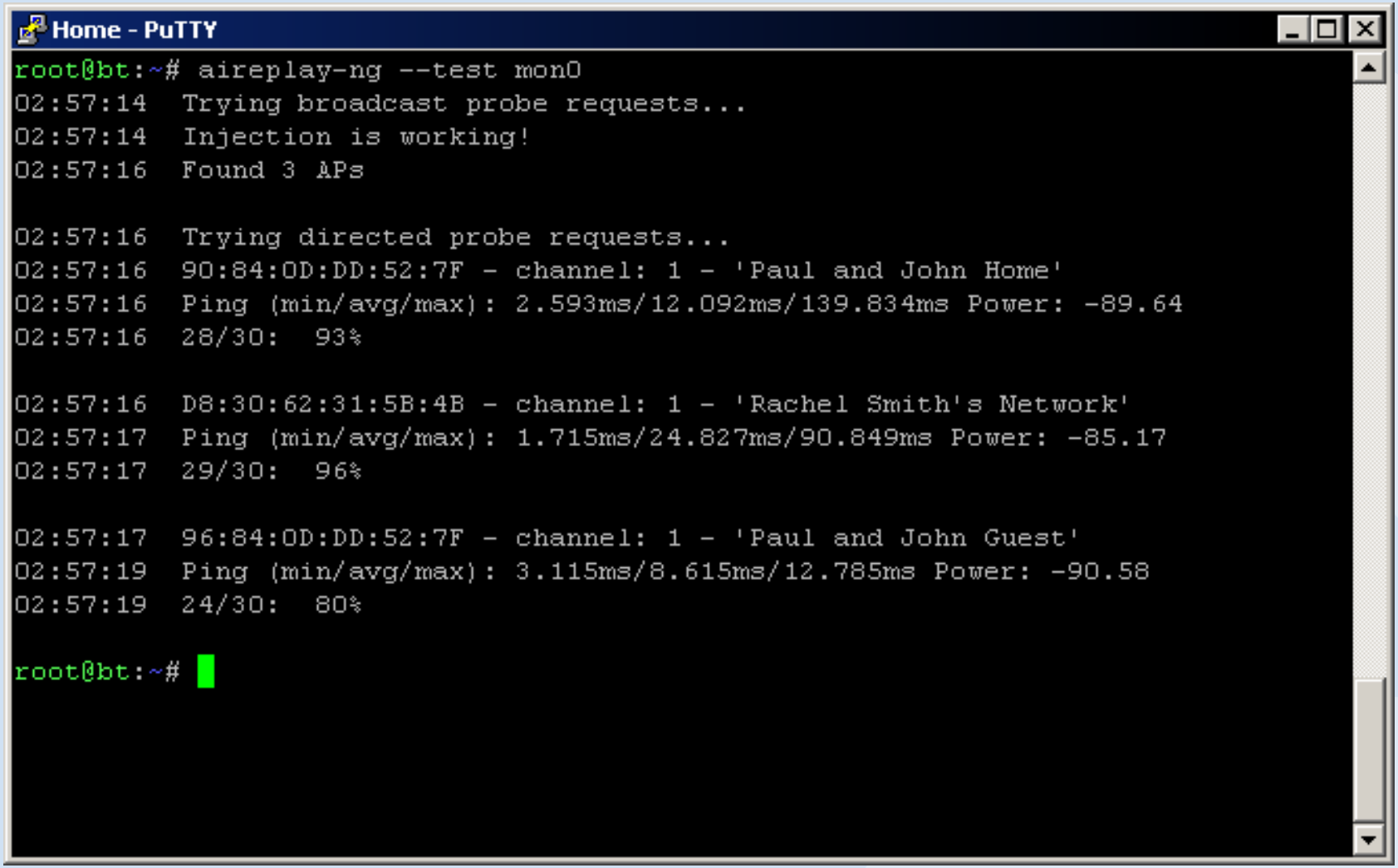
Airmon-ng


Home - PuTTY
root@bt:~# airmon-ng
Interface Chipset Driver
wlan0 Atheros ath5k - [phy0]
wlan1 RTL8187 rtl8187 - [phy2]
wlan2 AR9001U ar9170usb - [phy4]
root@bt:~#

Airodump-ng


Home - PuTTY
CH 5][Elapsed: 2 mins][2010-05-03 22:03][enabled AP selection
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:18:39:83:00:3F -53 512 1497 0 5 11 WPA TKIP PSK Merdorp
00:12:BF:1F:08:57 -61 451 19 0 6 54 . OPN Philips WiFi
00:12:BF:06:18:77 -64 384 0 0 6 54 . WEP WEP Philips WiFi
00:1F:9F:A2:E2:2A -72 398 5 0 1 54e OPN SpeedTouchAC3DF
00:12:BF:3D:06:F6 -77 21 0 0 6 54 . OPN Philips WiFi
BSSID STATION PWR Rate Lost Packets Probes
(not associated) 00:18:DE:AB:4A:1F -73 0 - 1 0 4 Philips WiFi
00:18:39:83:00:3F 00:1E:4C:AD:4E:F0 -43 11 -11 0 1647 Merdorp
00:18:39:83:00:3F 00:13:02:13:9D:1A -50 11 - 1 0 110 Merdorp
00:12:BF:1F:08:57 00:15:AF:30:E3:4D -62 36 -18 0 25
00:12:BF:3D:06:F6 00:1E:4C:03:9E:46 -70 0 - 1 0 49

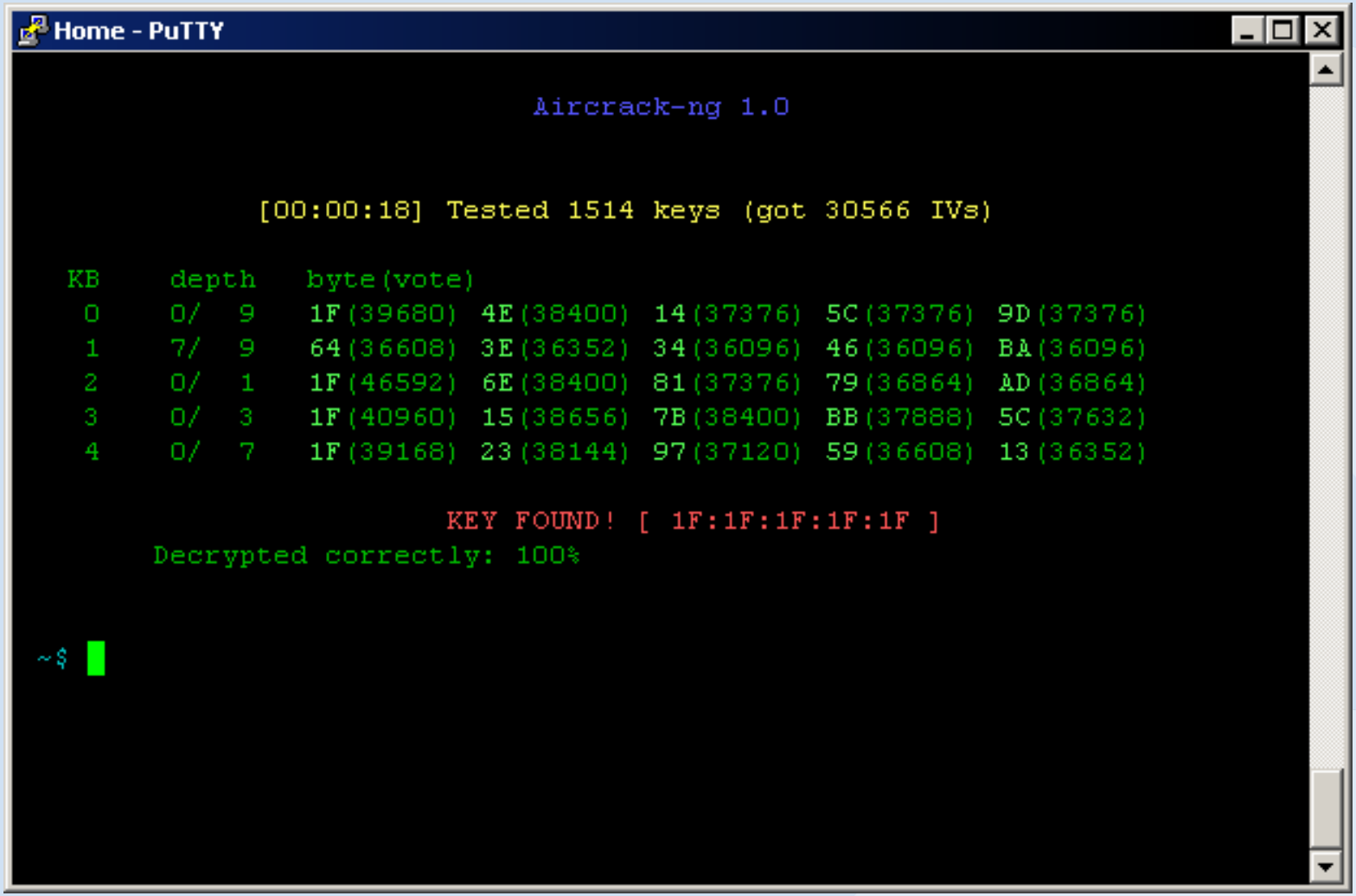
Aireplay-ng


Home - PuTTY
root@bt:~# aireplay-ng --test mon0
02:57:14 Trying broadcast probe requests...
02:57:14 Injection is working!
02:57:16 Found 3 APs
02:57:16 Trying directed probe requests...
02:57:16 90:84:0D:DD:52:7F - channel: 1 - 'Paul and John Home'
02:57:16 Ping (min/avg/max): 2.593ms/12.092ms/139.834ms Power: -89.64
02:57:16 28/30: 93%
02:57:16 D8:30:62:31:5B:4B - channel: 1 - 'Rachel Smith's Network'
02:57:17 Ping (min/avg/max): 1.715ms/24.827ms/90.849ms Power: -85.17
02:57:17 29/30: 96%
02:57:17 96:84:0D:DD:52:7F - channel: 1 - 'Paul and John Guest'
02:57:19 Ping (min/avg/max): 3.115ms/8.615ms/12.785ms Power: -90.58
02:57:19 24/30: 80%
root@bt:~#

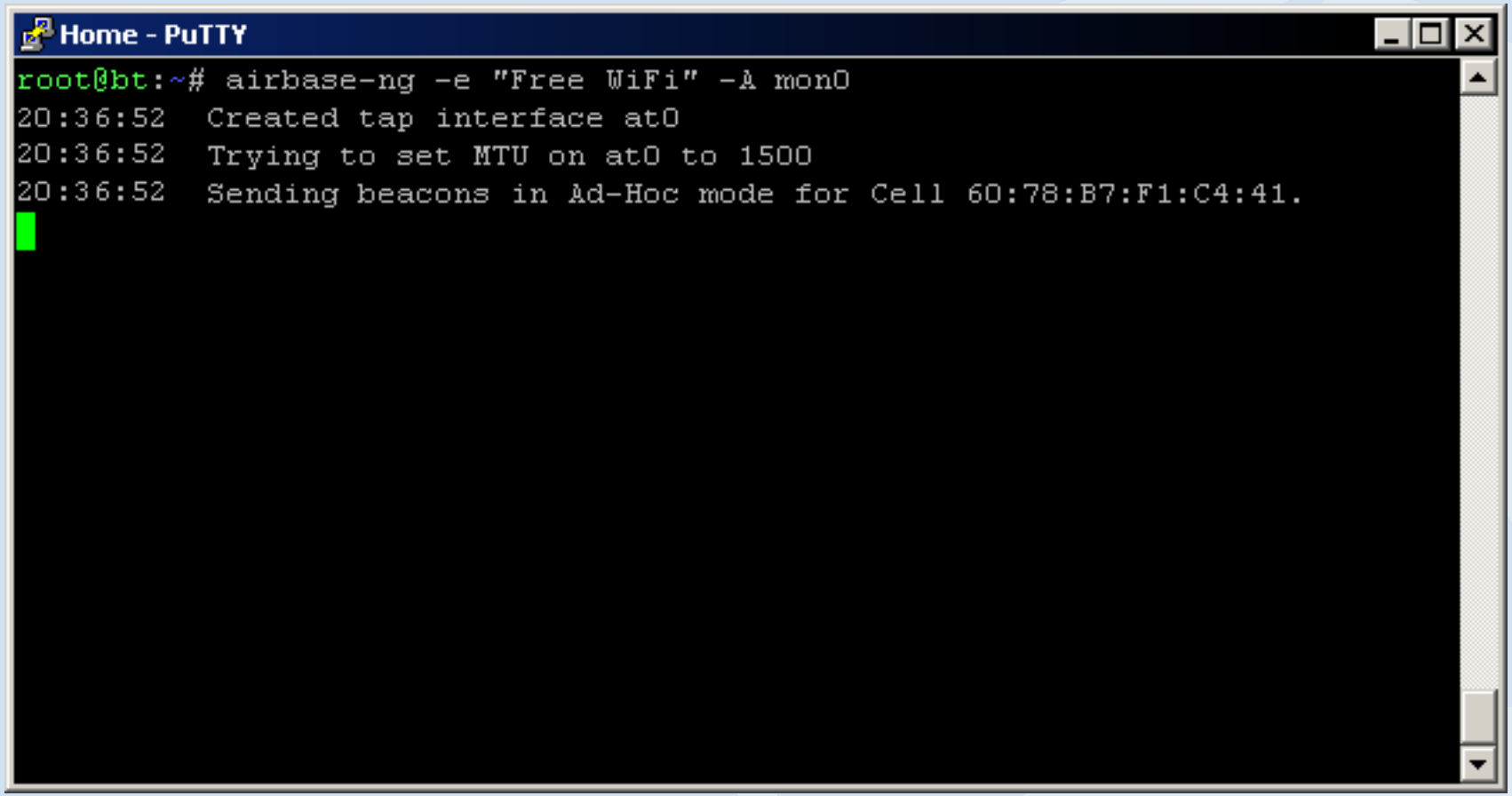
Packetforge-ng

- Generates WEP encrypted frame (ping/ARP/…)
- Requires keystream (XOR file)

Aircrack-ng


Home - PuTTY
Aircrack-ng 1.0
[00:00:18] Tested 1514 keys (got 30566 IVs)
KB depth byte(vote)
0 0/ 9 1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376)
1 7/ 9 64(36608) 3E(36352) 34(36096) 46(36096) BA(36096)
2 0/ 1 1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864)
3 0/ 3 1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632)
4 0/ 7 1F(39168) 23(38144) 97(37120) 59(36608) 13(36352)
KEY FOUND! [1F:1F:1F:1F:1F]
Decrypted correctly: 100%
~$

Airbase-ng


Home - PuTTY
root@bt:~# airbase-ng -e "Free WiFi" -A mon0
20:36:52 Created tap interface at0
20:36:52 Trying to set MTU on at0 to 1500
20:36:52 Sending beacons in Ad-Hoc mode for Cell 60:78:B7:F1:C4:41.

Airdecap-ng

- Decrypt captures (WEP/WPA)
- Confirm key/passphrase

Other tools

- Airolib-ng
- Airtun-ng
- Ivstools
- Etc…

- Scripts
  - Airgraph-ng
  - Airoscript-ng
  - Etc…

Aircrack-ng - Installation

- Compilation of stable or latest devel is the same
- Requirements:
  - Gcc/make: build-essential
  - OpenSSL development: libssl-dev or openssl-dev
  - Optional: SQLite development package

Aircrack-ng – Installation (2)

- `make && make install`

- Options:
  - `unstable`: easside-ng, tkiptun-ng, etc:
  - `sqlite`: Airolib-ng
  - Can be combined:
    - `make sqlite=true unstable=true`
    - `make sqlite=true unstable=true install`

Aircrack-ng – Compat-wireless

- Up to date wireless drivers for stable kernels
- No need to patch it anymore
- Most cases: Latest version

- I've heard funny names for it ;)
  - Compact wireless
  - Combat wireless

Aircrack-ng – Compat-wireless (2)

- Requires
  - Kernel headers/sources
  - Gcc/make
- Download latest stable
- Two step installation process
  1. `make`
  2. `make install`
- Sometimes install firmware

Break

- 15 minutes break

Exercises

- WEP
  - With client
  - Without client
- WPA
  - With client
  - Without AP

Exercises – Important notes

- Kill network managers/other software using the card to avoid issues

- Target:
  - ESSID: aircrackng

Exercise – WEP Cracking – With client

1. Put the card in monitor mode
2. Identify network
3. Record traffic on fixed channel
4. Deauth client
   - Will generate ARP
   - ARP will be replayed
5. Crack capture file

Exercise – WEP Cracking – Without client

1. Put the card in monitor mode
2. Identify network
3. Record traffic on fixed channel
4. Fake client
   - Fake authentication
   - Several options
     - ARP Replay
     - Interactive frame replay
     - Chopchop
     - Fragmentation
5. Crack capture file

Exercise – WPA Cracking

- Hard and easy to crack
  - Easy: just get the handshake
  - Hard:
    - Need to be close to target(s)
    - Passphrase length: 8-63 chars
- No real client => No handshake => No cracking

Exercise – WPA Cracking – With AP

1. Put the card in monitor mode
2. Identify network
3. Deauth client or wait for connection
4. Crack the capture

Exercise – WPA Cracking – Without AP

1. Put the card in monitor mode
2. Identify client through probes
3. Start `airbase-ng` in WPA mode
4. Crack capture file


That's all Folks!

Links - Contact

- Learn more:
  - http://aircrack-ng.org
  - http://www.nekasg.com
  - 2 day training @ DerbyCon: http://www.derbycon.com
  - 802.11 Wireless Networks, Matthew Gast

- Contact:
  - tdotreppe@aircrack-ng.org
  - thomas.dotreppe@nekasg.com

    Business cards are on the desk