

WLAN Security and Analysis

April 1, 2008

Thomas d'Otreppe de Bouvette

Aircrack-ng

SHARKFEST '08

Foothill College

March 31 - April 2, 2008

Agenda

- Who Am I?
- Wireless networks
 - Timeline
 - Overview of 802.11 networks
 - Wireless packets
 - Encryption
 - Interactions with networks
 - Capture files analysis
- OSdep
- Demo

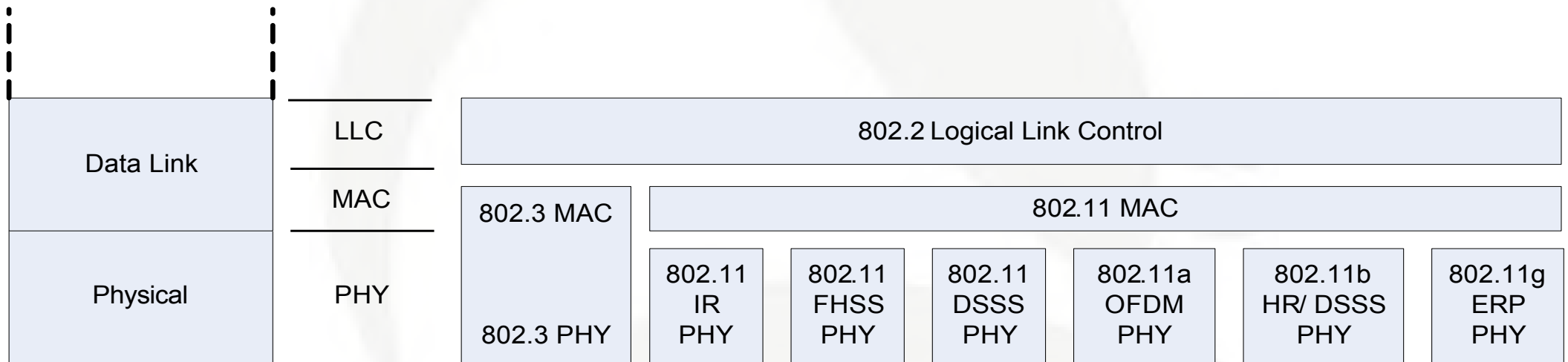
Who Am I?

- Started Aircrack-ng ~2 years ago.
- Graduated from Brussels High School in June 2006
- Currently work as IT consultant
- Created Offensive-Security WiFu course

Overview of 802.11 networks - Timeline

- 802.11: '97
- 802.11a: '99
- 802.11b: '99
- 802.11g: 2003
- 802.11n: Group started in January 2004
 - D1.0 (1.06): November 2006
 - D1.1: January 19, 2007
 - D2.0: March 2007
 - D3 (3.02): January 2008

Overview of 802.11 networks - OSI

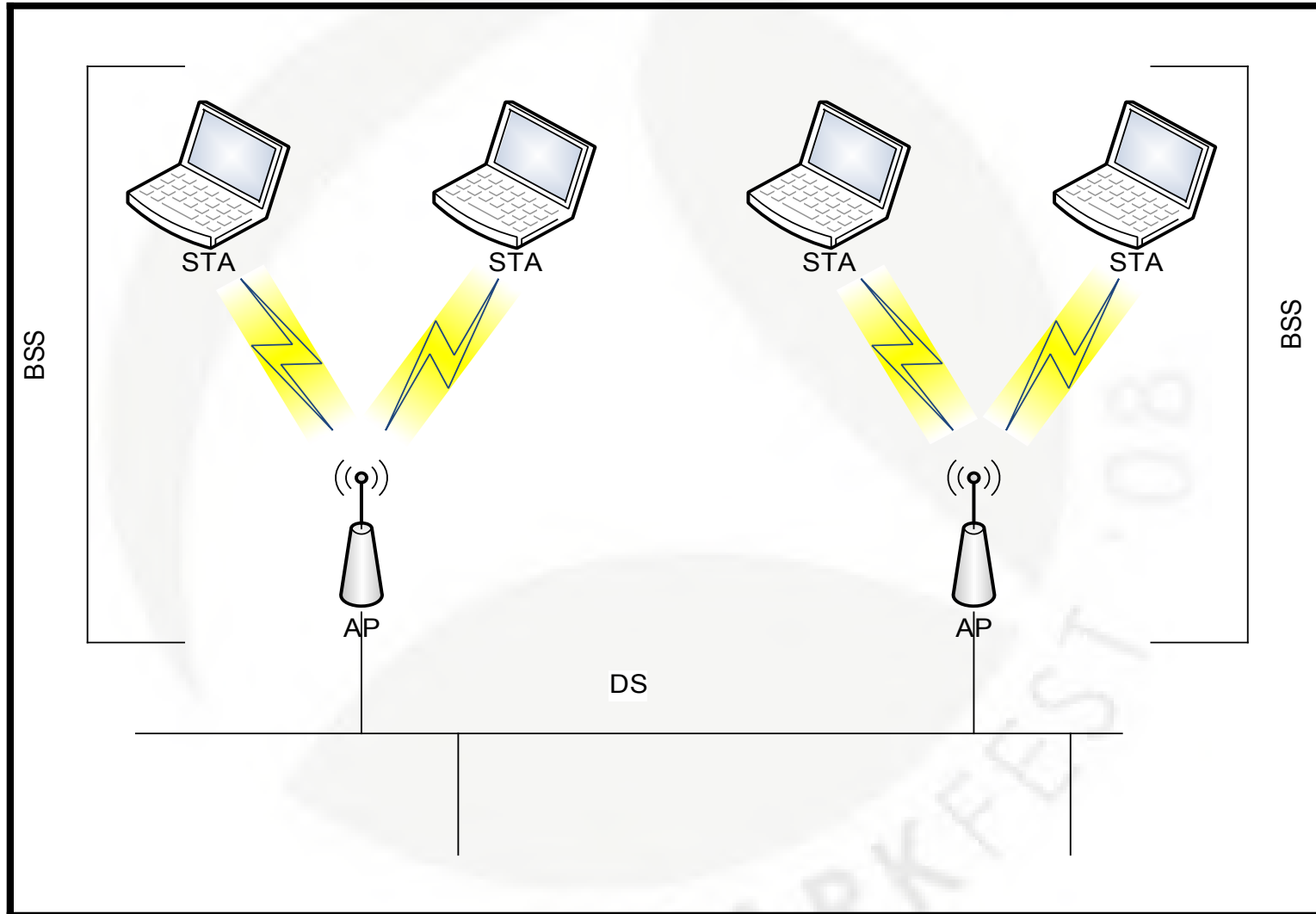


Overview of 802.11 networks – Operating Modes

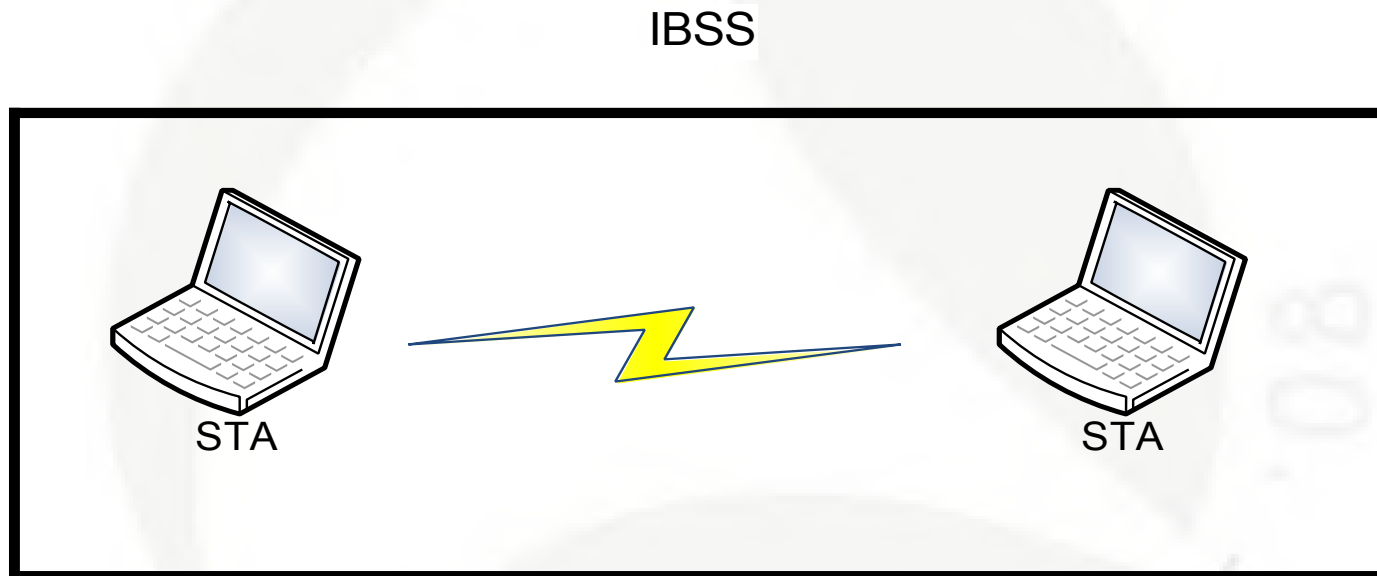
- Infrastructure
- Ad hoc

Overview of 802.11 networks - Infrastructure

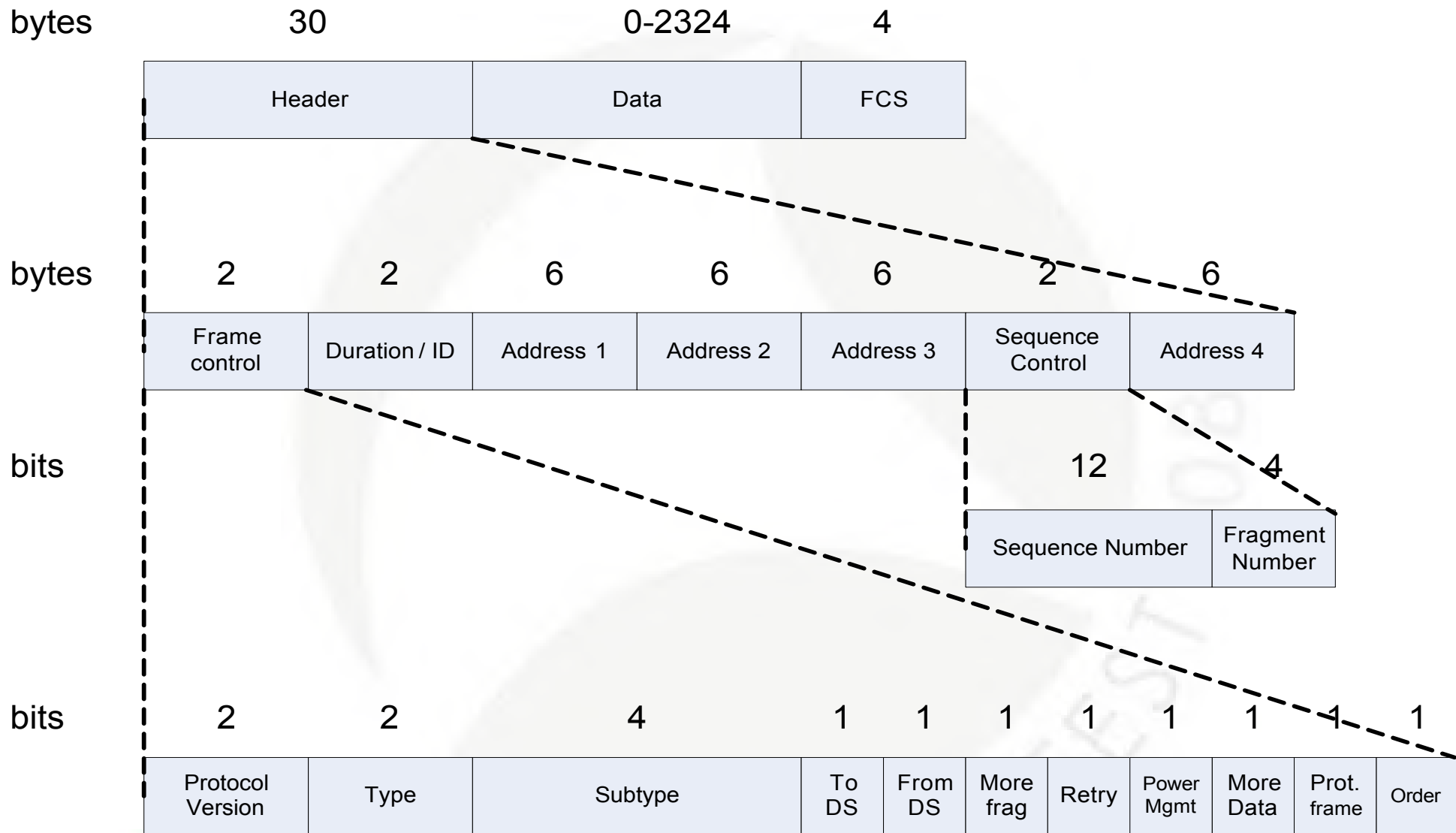
ESS



Overview of 802.11 networks – Ad hoc



Wireless packets – Frame structure



Wireless packets – Frame structure

Addresses

FromDS bit	ToDS bit	Address 1	Address 2	Address 3	Address 4	Mode
0	0	DA	SA	BSSID		IBSS
0	1	BSSID	SA	DA		AP
1	0	DA	BSSID	SA		AP
1	1	RA	TA	DA	SA	WDS

Wireless packets – Frames types

- Management frames
- Control frames
- Data frames

Windows taskbar: m200@m200: -

```
CH 1 ][ BAT: 2 hours 2 mins ][ Elapsed: 1 min ][ 2008-03-30 14:19
```

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
0A:ED:9D:E5:17:D4	-1	0	10027	406	0	1	11	OPN			hpsetup

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
0A:ED:9D:E5:17:D4	00:16:CF:28:03:33	0	0-0	30	5063	
0A:ED:9D:E5:17:D4	00:1D:4F:09:6F:E2	0	0-0	25	5488	
(not associated)	00:1B:77:05:93:71	0	0-0	0	146	

TELENETHOTSPOT,CK-AP-Y-1,co_presidents_club,tmobile,concourse,pcswifi,attwifi,hhonors,CLTNET,r4

System tray: m200, Sun 30 Mar, CPU 1200MHz, 116 procs, 3 mem, PWR 55.00, hda 38.00


```
root@mx6110:~# nmap -sS 169.254.21.35
```

```
Starting Nmap 4.50 ( http://insecure.org ) at 2008-02-14 13:01 CET
Interesting ports on 169.254.21.35:
Not shown: 1709 filtered ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:1F:3A:1E:9D:58 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 30.868 seconds
root@mx6110:~# nmap -sO 169.254.21.35
```

```
Starting Nmap 4.50 ( http://insecure.org ) at 2008-02-14 13:03 CET
Interesting protocols on 169.254.21.35:
Not shown: 255 open/filtered protocols
PROTOCOL STATE SERVICE
1         open  icmp
MAC Address: 00:1F:3A:1E:9D:58 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 22.005 seconds
```

```
root@mx6110:~# nmap -sO -O 169.254.21.35
```

```
WARNING: Disabling OS Scan (-O) as it is incompatible with the IPProto Scan (-sO)
```

```
Starting Nmap 4.50 ( http://insecure.org ) at 2008-02-14 13:04 CET
```

```
root@mx6110:~# nmap -sS -O 169.254.21.35
```

```
Starting Nmap 4.50 ( http://insecure.org ) at 2008-02-14 13:04 CET
Interesting ports on 169.254.21.35:
Not shown: 1709 filtered ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:1F:3A:1E:9D:58 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2000
OS details: Microsoft Windows 2000 Server SP3 or SP4
Network Distance: 1 hop
```

```
OS detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 56.240 seconds
```

```
root@mx6110:~# █
```

Wireless packets – Management frames

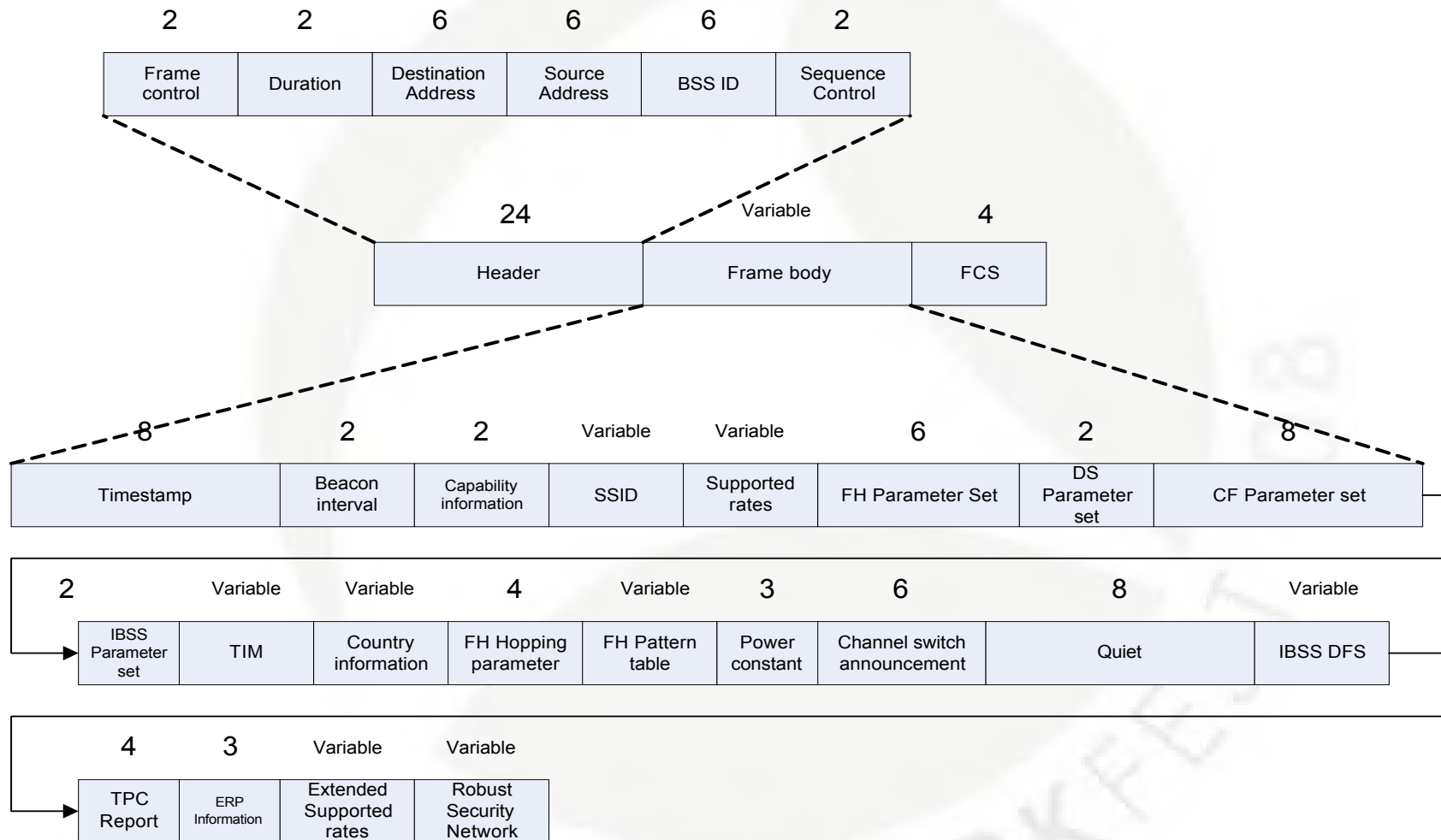
- **Definition:** used to negotiate and control the relationship between the AP and the station.
- Type field value: 0

Subtype field value	Description
0	Assoc. request
1	Assoc. response
2	Reassoc. req.
3	Reassoc. resp.
4	Probe request
5	Probe response
6	Meas. Pilot

Subtype field value	Description
7	Reserved
8	Beacon
9	ATIM
10	Disassociation
11	Authentication
12	Deauthentication
13	Action
14	Action No ACK
15	Reserved

Wireless packets – Management frames (1)

Beacon



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco-Li_83:00:3f	Broadcast	IEEE 802	Beacon frame, SN=1, FN=0, Flags=.....
2	61.438336	Cisco-Li_83:00:3f	Broadcast	IEEE 802	Beacon frame, SN=50, FN=0, Flags=.....

- ⊕ Frame 1 (84 bytes on wire, 84 bytes captured)
 - ⊕ IEEE 802.11 Beacon frame, Flags:
 - ⊖ IEEE 802.11 wireless LAN management frame
 - ⊖ Fixed parameters (12 bytes)
 - Timestamp: 0x0000000003A9818B
 - Beacon Interval: 61,440000 [seconds]
 - ⊕ Capability Information: 0x0411
 - ⊖ Tagged parameters (48 bytes)
 - ⊕ SSID parameter set: "linksys"
 - ⊕ Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 18,0 24,0(B) 36,0 54,0
 - ⊕ DS Parameter set: Current Channel: 11
 - ⊕ Traffic Indication Map (TIM): DTIM 0 of 1 bitmap mcast
 - ⊕ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
 - ⊕ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
 - ⊕ Extended Supported Rates: 6,0(B) 9,0 12,0(B) 48,0
 - ⊕ Vendor specific: Broadcom

0000	80 00 00 00 ff ff ff ff ff ff 00 18 39 83 00 3f 9..?
0010	00 18 39 83 00 3f 10 00 8b 81 a9 03 00 00 00 00	..9..?..
0020	60 ea 11 04 00 07 6c 69 6e 6b 73 79 73 01 08 82	...li nksys...
0030	84 8b 96 24 b0 48 6c 03 01 0b 05 04 00 01 01 00	...\$.H1.
0040	2a 01 00 2f 01 00 32 04 8c 12 98 60 dd 06 00 10	*../.2.
0050	18 02 00 00

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Aironet_a0:1c:74	Broadcast	IEEE 802	Beacon frame, SN=2531, F
2	0.326013	Arcadyan_12:32:29	Broadcast	IEEE 802	Beacon frame, SN=3781, F
3	5.088080	AethraTe_07:04:da	Broadcast	IEEE 802	Beacon frame, SN=1012, F
4	371.126314	D-Link_77:0c:9b	Broadcast	IEEE 802	Beacon frame, SN=1, FN=0

- ⊕ Frame 1 (177 bytes on wire, 177 bytes captured)
 - ⊕ IEEE 802.11 Beacon frame, Flags:
 - ⊖ IEEE 802.11 wireless LAN management frame
 - ⊕ Fixed parameters (12 bytes)
 - ⊖ Tagged parameters (141 bytes)
 - ⊕ SSID parameter set: "\000"
 - ⊕ Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)
 - ⊕ DS Parameter set: Current Channel: 6
 - ⊕ Traffic Indication Map (TIM): DTIM 1 of 2 bitmap empty
 - ⊕ Cisco Unknown 1 + Device Name
 - ⊕ Vendor specific: WPA
 - ⊕ Vendor specific: Aironet Unknown
 - ⊕ Vendor specific: Aironet CCX version = 3
 - ⊕ Vendor specific: Aironet Qos
 - ⊕ Vendor specific: WME

```

0020 64 00 31 00 00 01 00 01 04 82 84 8b 96 03 01 06  d.1....
0030 05 04 01 02 00 00 85 1e 00 00 81 00 1f 00 ff 03  .....
0040 19 00 61 70 70 61 72 74 00 00 00 00 00 00 00 00  ..appart
0050 00 00 00 00 00 22 dd 18 00 50 f2 01 01 00 00 50  .....P...P
0060 f2 02 01 00 00 50 f2 02 01 00 00 50 f2 02 28 00  .....P...P(
0070 dd 06 00 40 96 01 01 00 dd 05 00 40 96 03 03 dd  ...@....@....
    
```



Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Aironet_a0:1c:74	Broadcast	IEEE 802	Beacon frame, SN=2531, F
2	0.326013	Arcadyan_12:32:29	Broadcast	IEEE 802	Beacon frame, SN=3781, F
3	5.088080	AethraTe_07:04:da	Broadcast	IEEE 802	Beacon frame, SN=1012, F
4	371.126314	D-Link_77:0c:9b	Broadcast	IEEE 802	Beacon frame, SN=1, FN=0

- ⊕ Frame 2 (73 bytes on wire, 73 bytes captured)
 - ⊕ IEEE 802.11 Beacon frame, Flags:
 - ⊖ IEEE 802.11 wireless LAN management frame
 - ⊕ Fixed parameters (12 bytes)
 - ⊖ Tagged parameters (37 bytes)
 - ⊕ SSID parameter set: "Appart"
 - ⊕ Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 22,0
 - ⊕ DS Parameter set: Current Channel: 3
 - ⊕ Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
 - ⊕ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
 - ⊕ Extended Supported Rates: 6,0 9,0 12,0 18,0 24,0 36,0 48,0 54,0

```

0000  80 00 00 00 ff ff ff ff ff ff 00 12 bf 12 32 29  .....2)
0010  00 12 bf 12 32 29 50 ec 22 21 79 16 00 00 00 00  .....2)P. "!y....
0020  64 00 71 04 00 06 41 70 70 61 72 74 01 05 82 84  d.q...Ap part....
0030  8b 96 2c 03 01 03 05 04 00 01 00 00 2a 01 00 32  ...,....*...2
0040  08 0c 12 18 24 30 48 60 6c                                ....$0H` 1
    
```



Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Aironet_a0:1c:74	Broadcast	IEEE 802	Beacon frame, SN=2531, F
2	0.326013	Arcadyan_12:32:29	Broadcast	IEEE 802	Beacon frame, SN=3781, F
3	5.088080	AethraTe_07:04:da	Broadcast	IEEE 802	Beacon frame, SN=1012, F
4	371.126314	D-Link_77:0c:9b	Broadcast	IEEE 802	Beacon frame, SN=1, FN=0

- ⊕ Frame 3 (79 bytes on wire, 79 bytes captured)
 - ⊕ IEEE 802.11 Beacon frame, Flags:
 - ⊖ IEEE 802.11 wireless LAN management frame
 - ⊕ Fixed parameters (12 bytes)
 - ⊖ Tagged parameters (43 bytes)
 - ⊕ SSID parameter set: "LAN1-AP013842"
 - ⊕ Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)
 - ⊕ DS Parameter set: Current Channel: 11
 - ⊕ Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
 - ⊕ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
 - ⊕ Extended Supported Rates: 6,0 9,0 12,0 18,0 24,0 36,0 48,0 54,0

```

0000  80 00 00 00 ff ff ff ff ff ff 00 d0 d6 07 04 da  .....@? d.....
0010  00 d0 d6 07 04 da 40 3f 64 01 e0 af bf 00 00 00  .....@? d.....
0020  64 00 31 04 00 0d 4c 41 4e 31 2d 41 50 30 31 33  d.1...LA N1-AP013
0030  38 34 32 01 04 82 84 8b 96 03 01 0b 05 04 00 01  842.....
0040  00 00 2a 01 00 32 08 0c 12 18 24 30 48 60 6c  ..*..2.. ..$OH`|
    
```


Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
2	0.326013	Arcadyan_12:32:29	Broadcast	IEEE 802	Beacon frame, SN=3781, F
3	5.088080	AethraTe_07:04:da	Broadcast	IEEE 802	Beacon frame, SN=1012, F
4	371.126314	D-Link_77:0c:9b	Broadcast	IEEE 802	Beacon frame, SN=1, FN=0

```

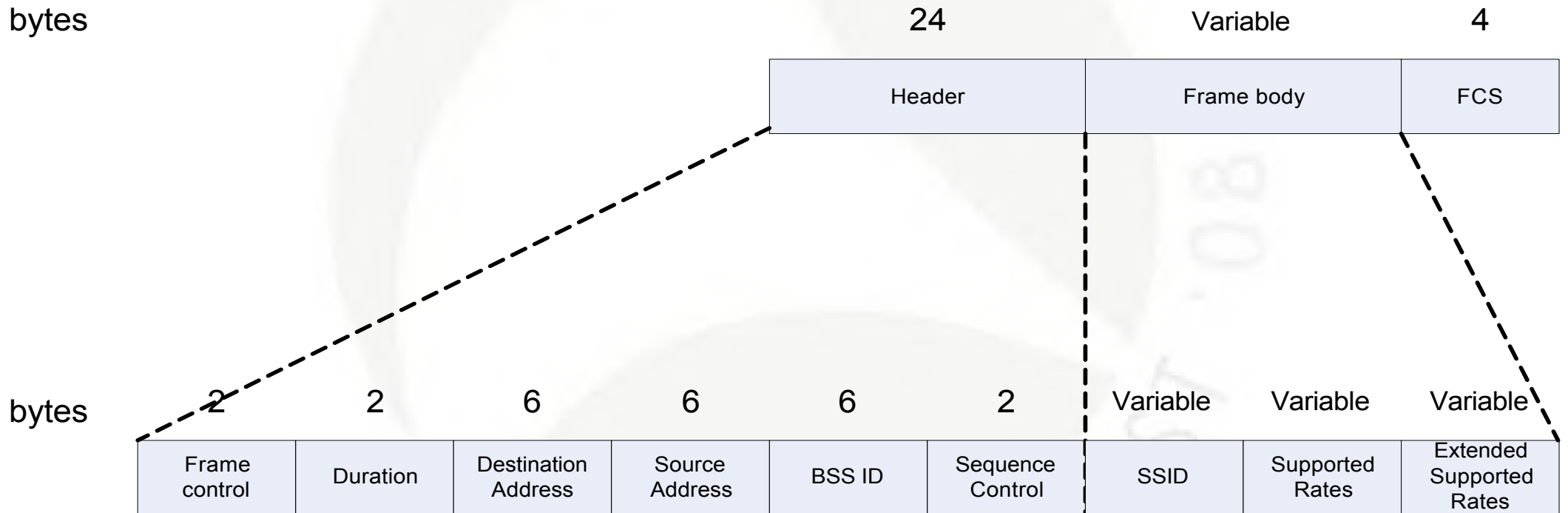
+ Frame 4 (197 bytes on wire, 197 bytes captured)
+ IEEE 802.11 Beacon frame, Flags: .....
- IEEE 802.11 wireless LAN management frame
  + Fixed parameters (12 bytes)
  - Tagged parameters (161 bytes)
    + SSID parameter set: "DLINK"
    + Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 18,0 24,0 36,0 54,0
    + DS Parameter set: Current Channel: 6
    + Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
    + ERP Information: no Non-ERP STAs, use protection, short or long preambles
    + ERP Information: no Non-ERP STAs, use protection, short or long preambles
    + Extended Supported Rates: 6,0 9,0 12,0 48,0
    + Vendor specific: Broadcom
    + HT Capabilities (802.11n D1.10)
    + Vendor specific: HT Capabilities (802.11n D1.10)
    + HT Information (802.11n D1.10)
    + Vendor specific: HT Additional capabilities (802.11n D1.00)
    
```

```

0040 02 2f 01 02 32 04 0c 12 18 60 dd 09 00 10 18 02  ./...2... ..
0050 01 f4 01 00 00 2d 1a 1e 18 1a ff ff 00 00 00 00  .....-.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0070 00 dd 1e 00 90 4c 33 1e 18 1a ff ff 00 00 00 00  .....L3.....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0090 00 2d 1e 06 0d 03 00 00 00 00 00 00 00 00 00  .....
    
```

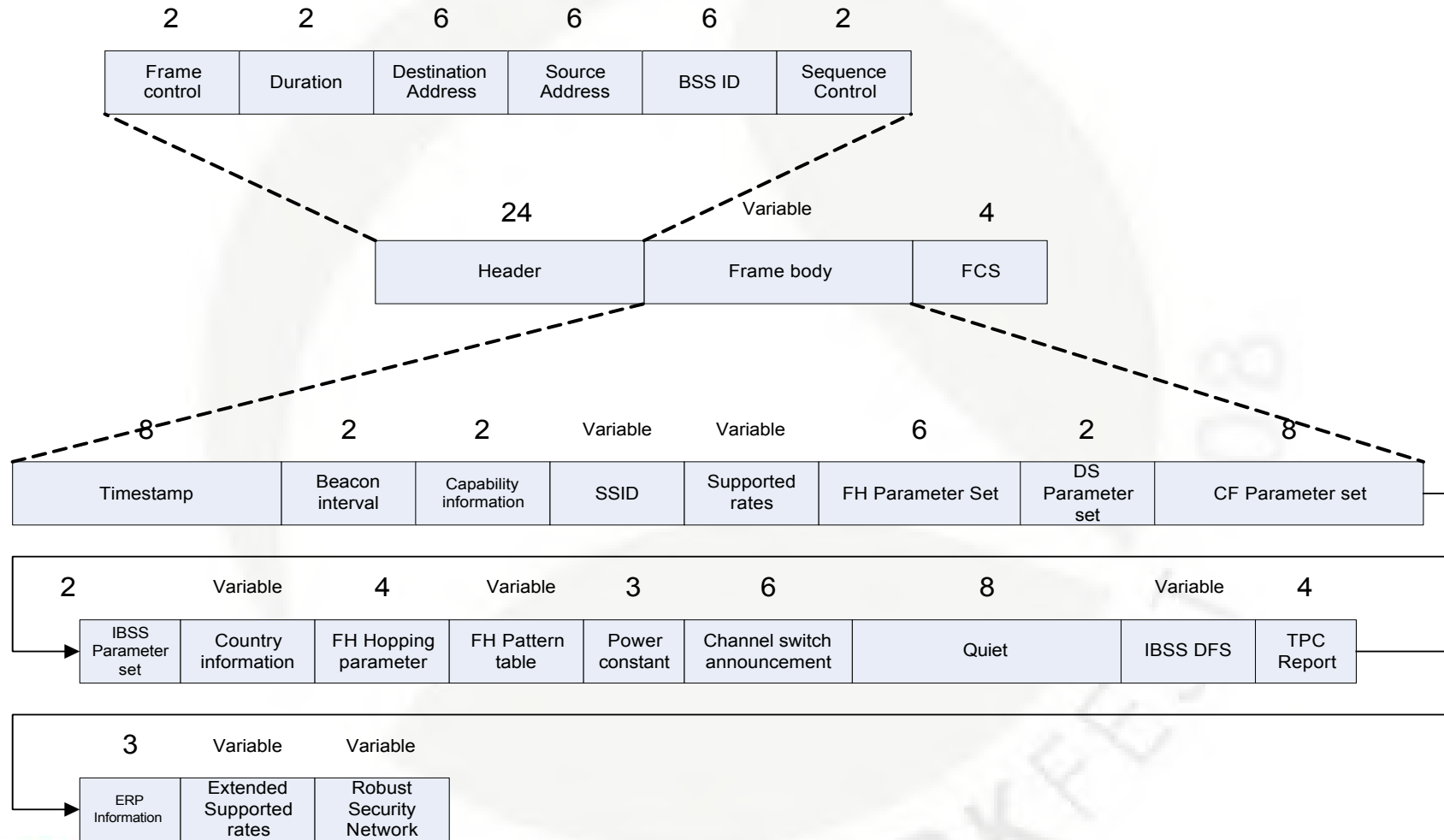
Wireless packets – Management frames (2)

Probe Request



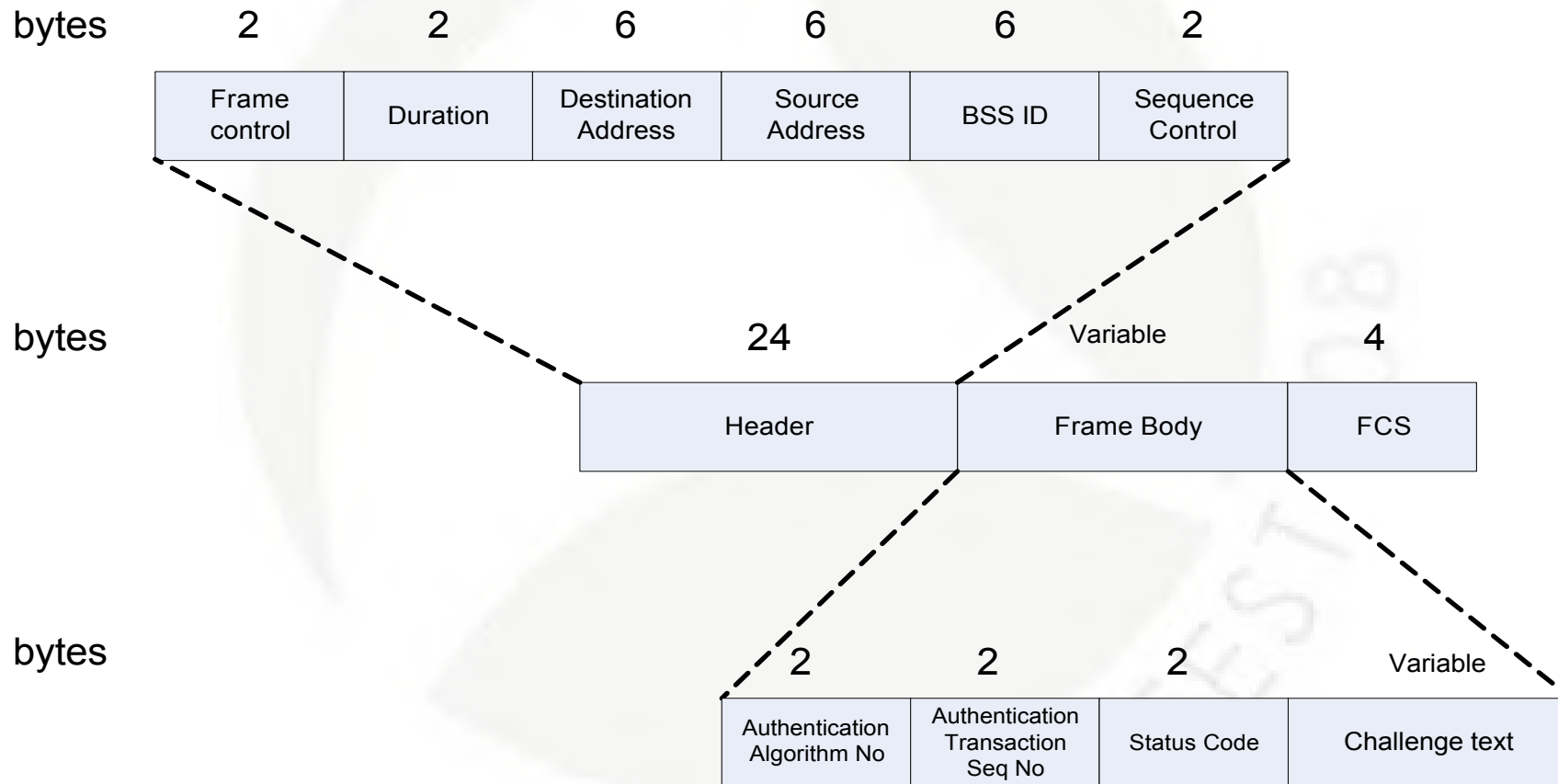
Wireless packets – Management frames (3)

Probe response



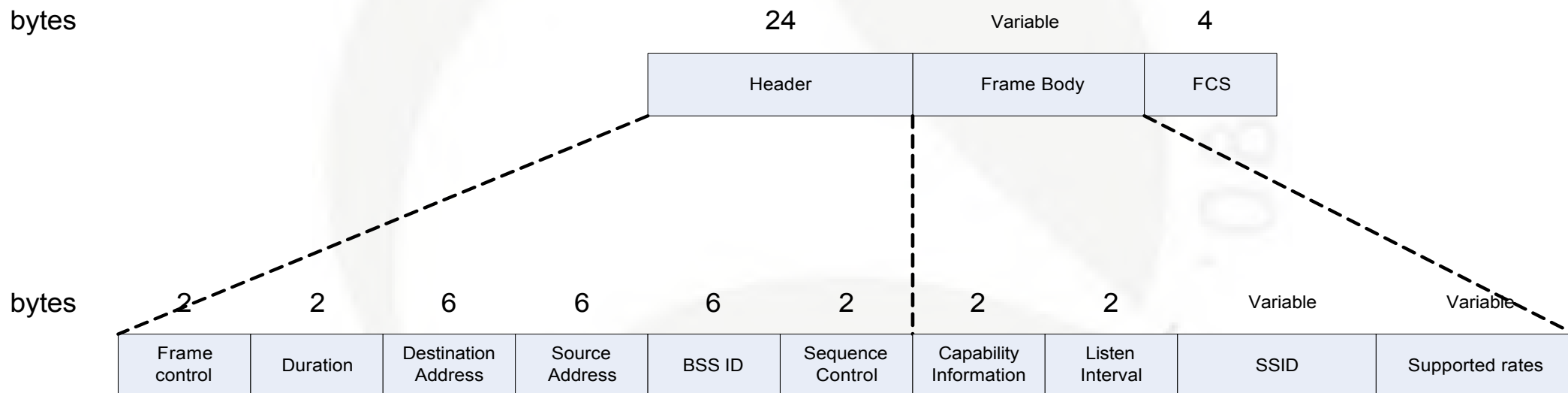
Wireless packets – Management frames (4)

Authentication



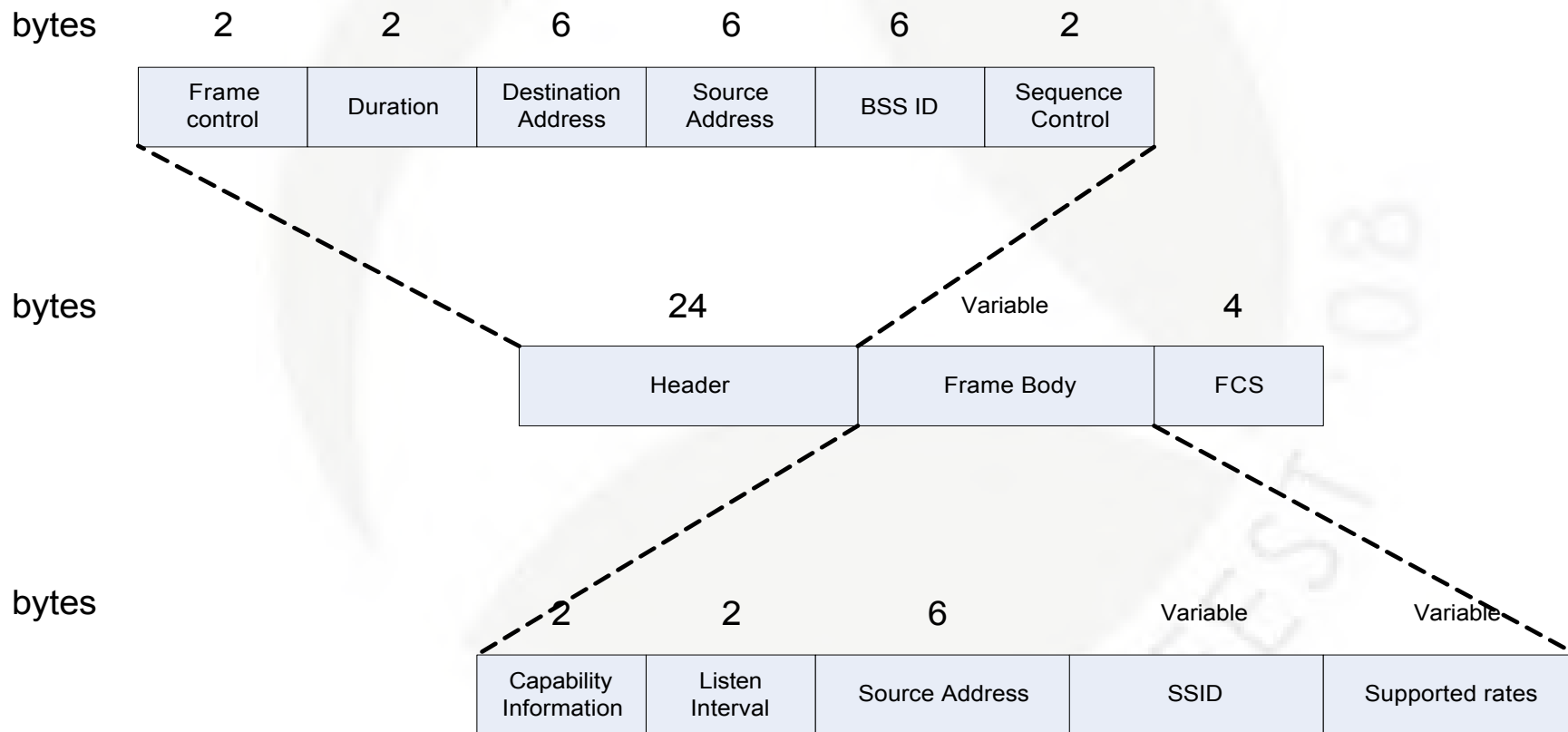
Wireless packets – Management frames (5)

Association request



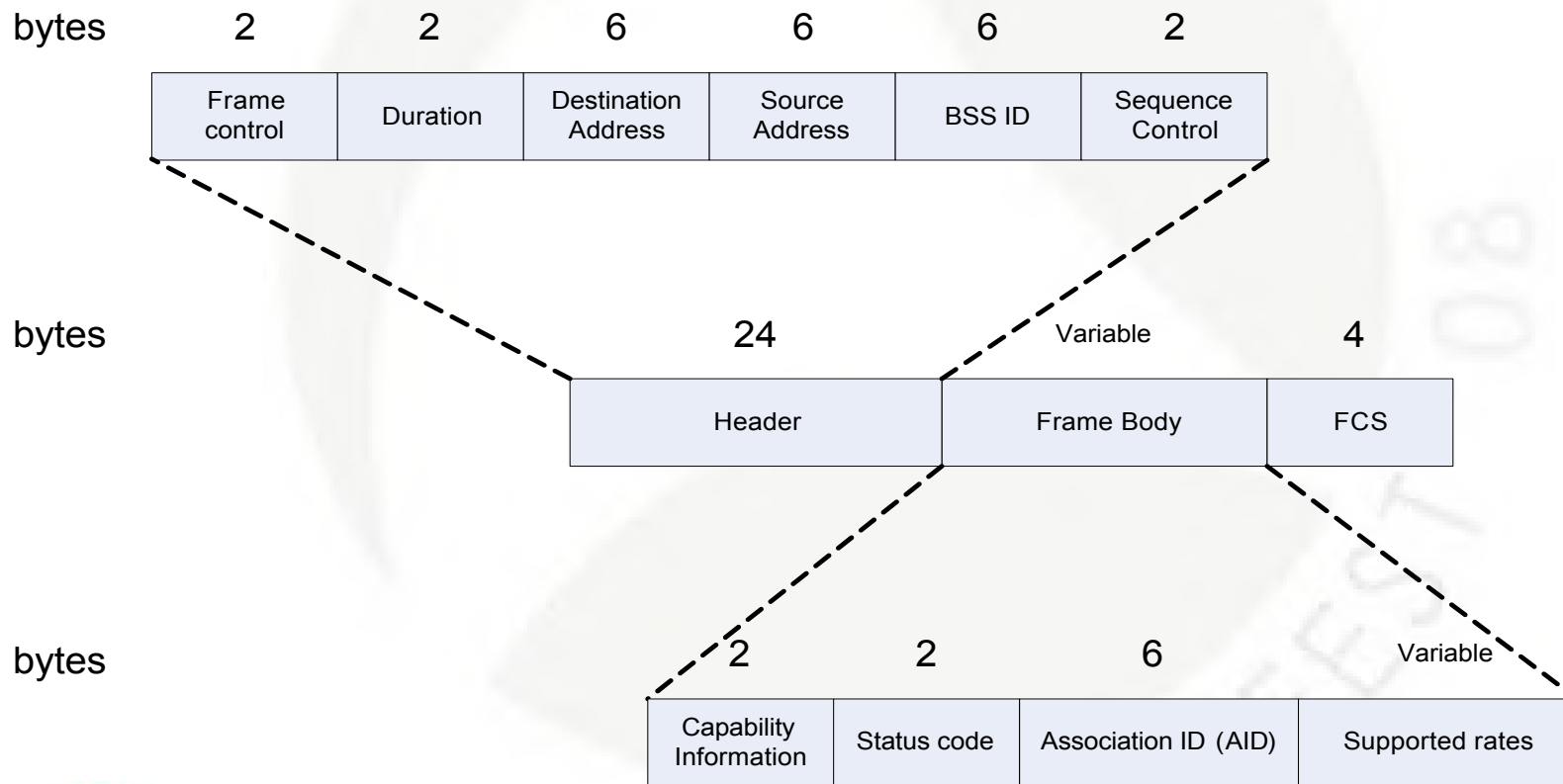
Wireless packets – Management frames (6)

Reassociation request



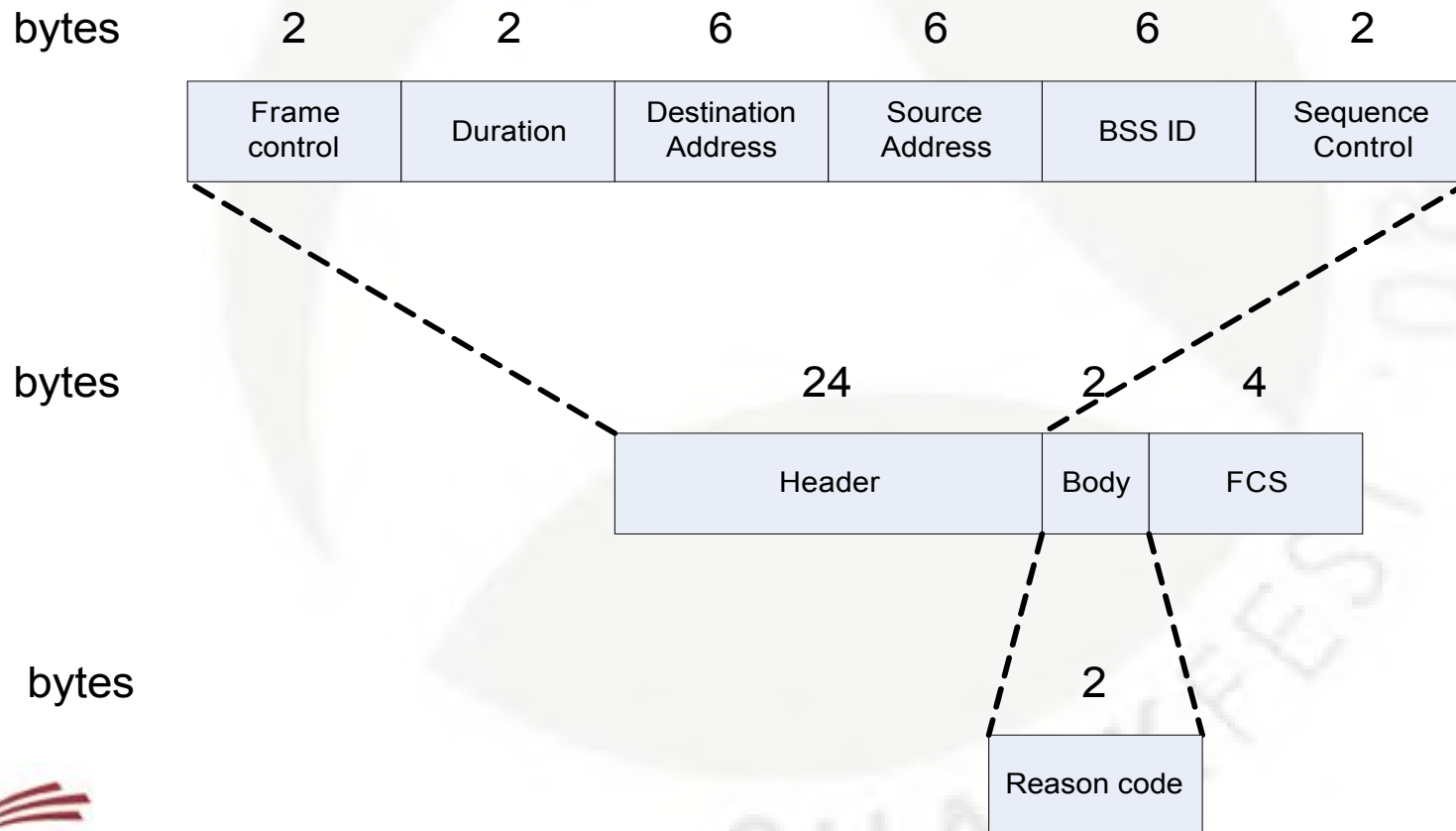
Wireless packets – Management frames (7)

Association/Reassociation response



Wireless packets – Management frames (8)

Disassociation / Deauthentication frame



Wireless packets – Control frames

- **Definition:** Assist in the delivery of management and data frames.
- Type field value: 1

Subtype field value	Description
0-6	Reserved
7	Control Wrapper
8	Block ACK request
9	Block ACK
10	PS-Poll

Subtype field value	Description
11	RTS
12	CTS
13	ACK
14	CF End
15	CF-End + CF-ACK

Wireless packets – Control frames

(2)

RTS

bytes	2	2	6	6	4
	Frame control	Duration	Receiver Address	Transmitter Address	FCS

CTS

bytes	2	2	6	4
	Frame control	Duration	Receiver Address	FCS

ACK

bytes	2	2	6	4
	Frame control	Duration	Receiver Address	FCS

Wireless packets – Data frames

- **Definition:** Carry higher level protocol data in the frame body
- Type field value: 2

Subtype field value	Description
0	Data
1	Data + CF ACK
2	Data + CF Poll
3	Data + CF ACK + CF Poll
4	Null function
5	CF ACK
6	CF Poll

Subtype field value	Description
7	CF ACK + CF Poll
8	QoS data
9	QoS data + CF-ACK
10	QoS data + CF-Poll
11	QoS data + CF-ACK + CF-Poll
12	QoS Null (no data)
13	Reserved
14	QoS CF-Poll (no data)
15	QoS CF-ACK + CF-Poll (no data)

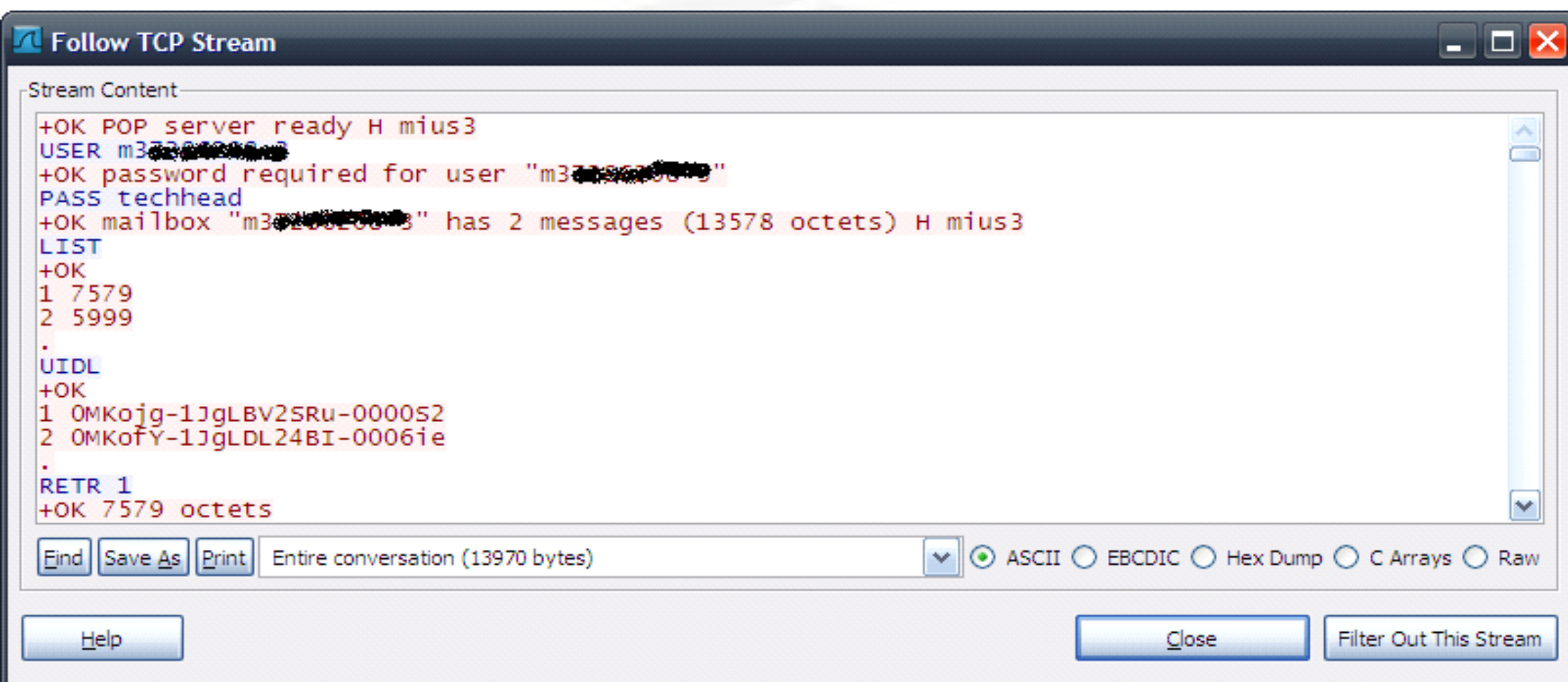
Interactions with networks – Encryption

- Open network
- WEP
- WPA

Interactions with networks – Encryption - Open networks

- No encryption
- Hotspot, mesh networks

Thanks for your passwords ;)



```
+OK POP server ready H mius3
USER m377962883
+OK password required for user "m377962883"
PASS techhead
+OK mailbox "m377962883" has 2 messages (13578 octets) H mius3
LIST
+OK
1 7579
2 5999
.
UIDL
+OK
1 0MKojg-1JgLBV2SRu-0000S2
2 0MKofY-1JgLDL24BI-0006ie
.
RETR 1
+OK 7579 octets
```

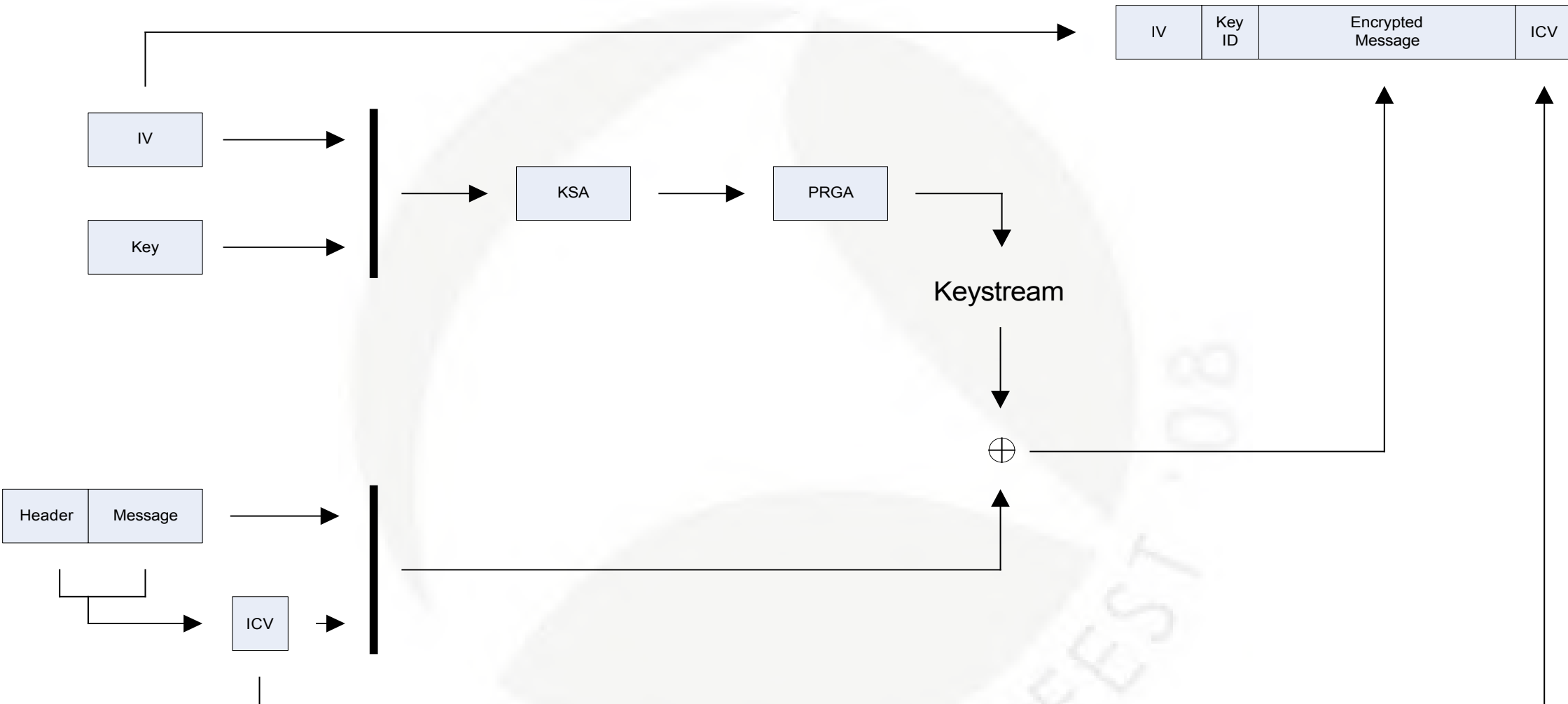
Find Save As Print Entire conversation (13970 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help Close Filter Out This Stream

Interactions with networks – Encryption - WEP

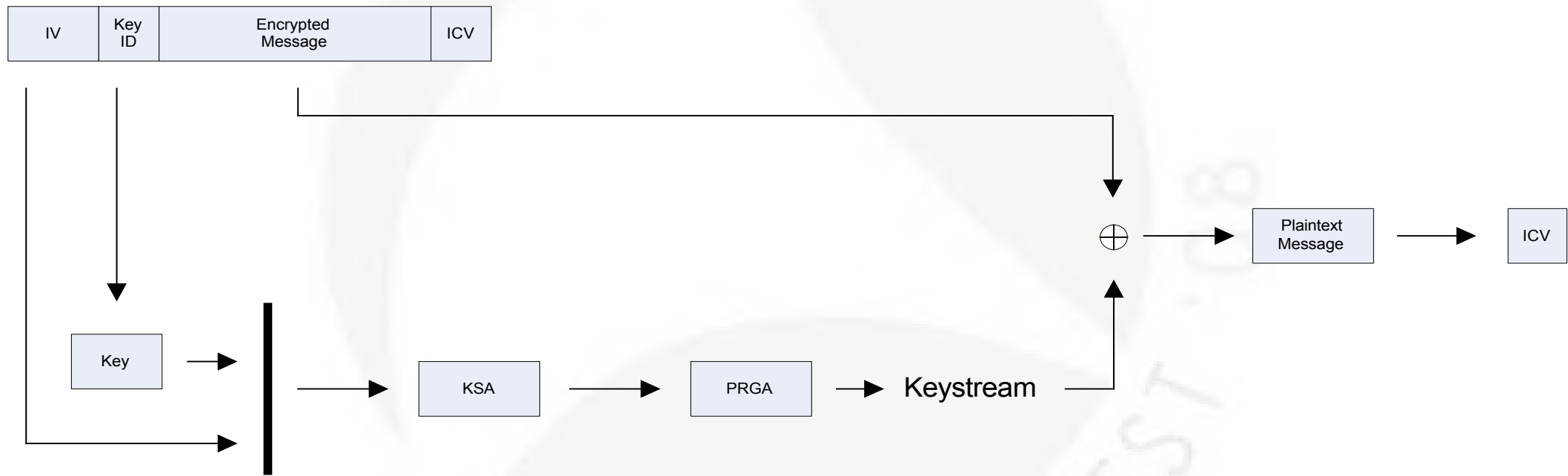
- Wired Equivalent Privacy
- Part of 802.11
- RC4
- 24 bit IV
- CRC32 (ICV) for message integrity

Interactions with networks – Encryption - WEP (2)



Interactions with networks – Encryption - WEP (3)

Decryption



Interactions with networks – Encryption - WEP (4)

```
function KSA ()  
  for i from 0 to 255  
    S[i] := i  
  endfor  
  j := 0  
  for i from 0 to 255  
    j := (j + S[i] + key[i % keylength]) % 256  
    swap(S[i], S[j])  
  endfor  
endfunction
```

Interactions with networks – Encryption - WEP (5)

```
function PRGA ()  
    i := 0  
    j := 0  
    while GeneratingOutput:  
        i := (i + 1) % 256  
        j := (j + S[i]) % 256  
        swap(S[i], S[j])  
        output S[(S[i] + S[j]) mod 256]  
    endwhile  
endfunction
```

Interactions with networks – Encryption - WEP (6)

Encryption

Plaintext

1	1	0	1
---	---	---	---

\oplus

Keystream

1	0	1	1
---	---	---	---

=

Encrypted data

0	1	1	0
---	---	---	---

Decryption

Encrypted data

0	1	1	0
---	---	---	---

\oplus

Keystream

1	0	1	1
---	---	---	---

=

Plaintext

1	1	0	1
---	---	---	---

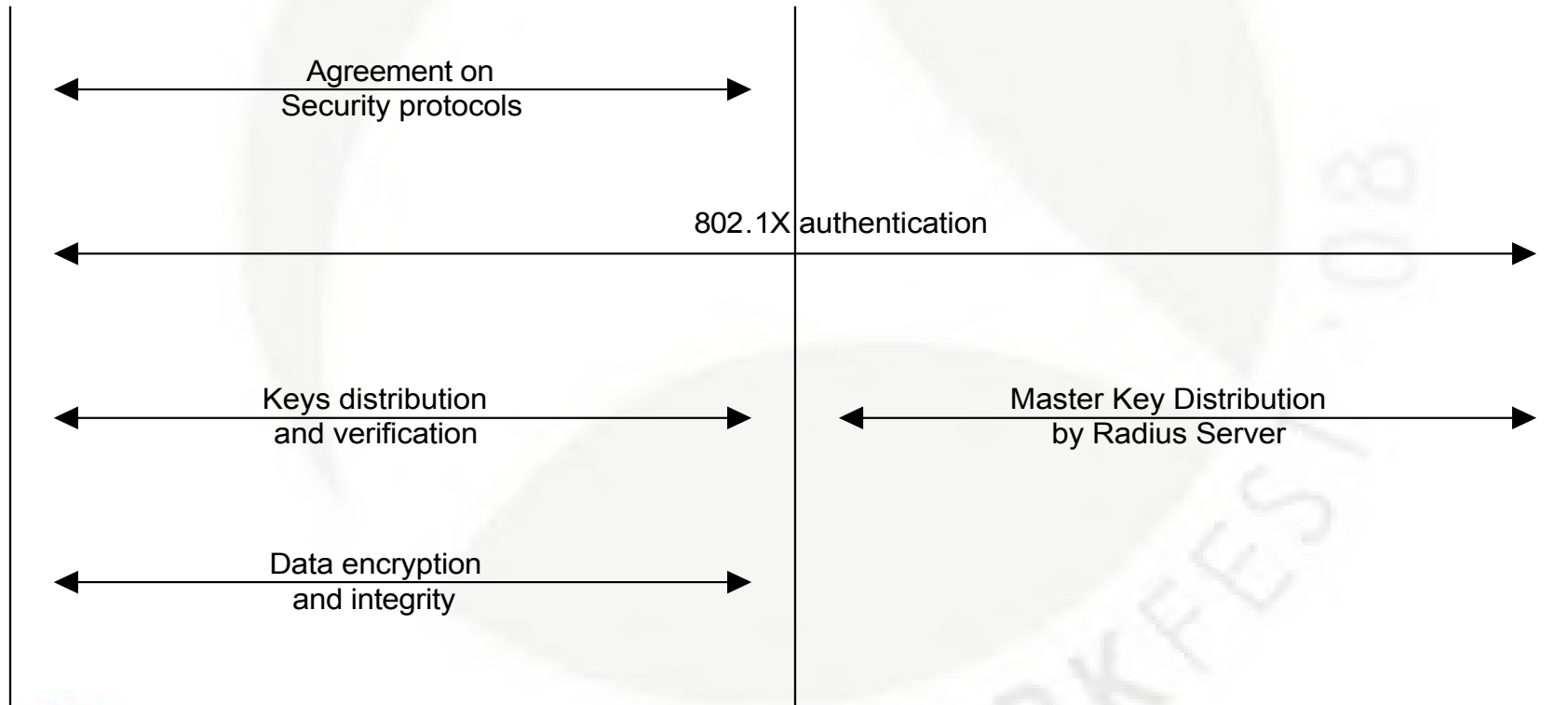
Interactions with networks – Encryption - WPA

- 802.11i group
- Developed two link-layer protocols:
 - TKIP – WPA1: Draft 3 of 802.11i group (backward compatible with legacy hardware).
 - CCMP – WPA2: final 802.11i standard
- Two flavors:
 - Personal: PSK
 - Enterprise: MGT

Interactions with networks – Encryption - WPA (2)



Authenticator



Interactions with networks – Encryption - WPA (3)

Agreement on security protocols

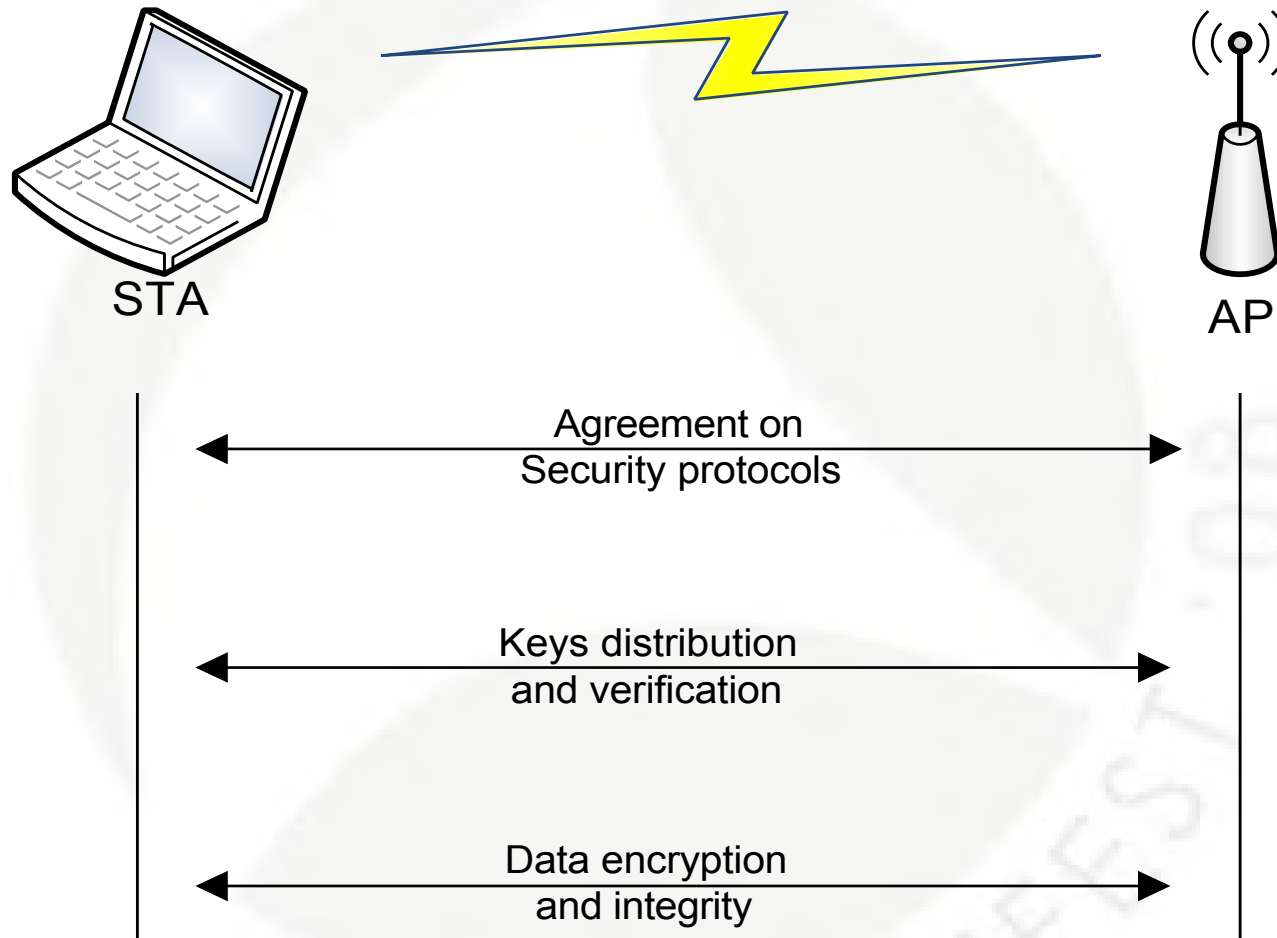
- Beacons and probe
- Authentication: PSK or Radius server
- Encryption suite for unicast and multicast/broadcast:
TKIP, ...

Interactions with networks – Encryption - WPA (4)

802.1X Authentication

- Not done with PSK
- Use EAP
- When successfully authenticated:
 - ACK sent to the client
 - Generated Master Key sent to the AP

Interactions with networks – Encryption - WPA (5)



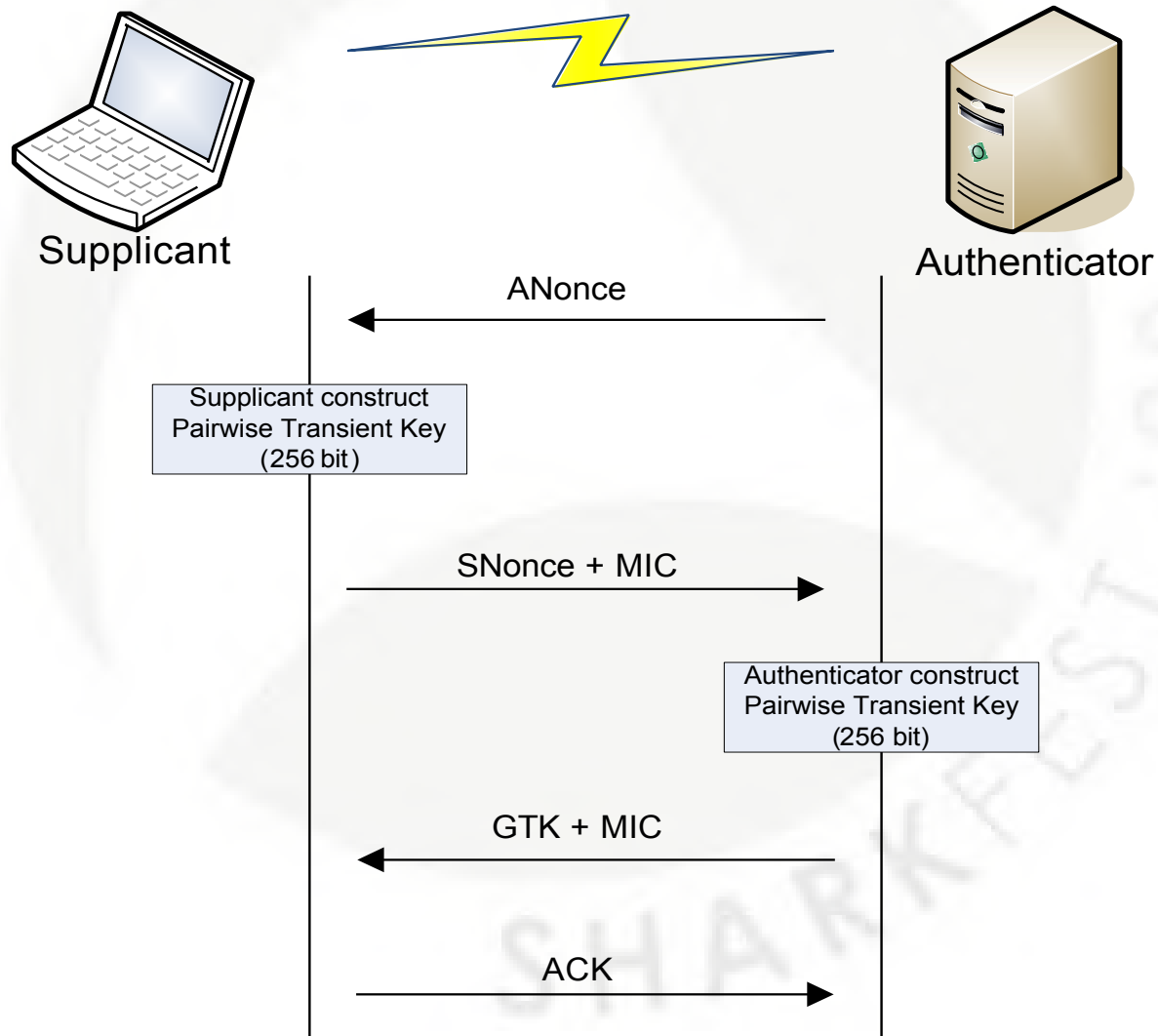
Interactions with networks – Encryption - WPA (6)

Key distribution and verification

- Confirmation of the cipher suite used
- Confirmation of the PMK knowledge
- Installation of the integrity and encryption keys
- Send GTK securely

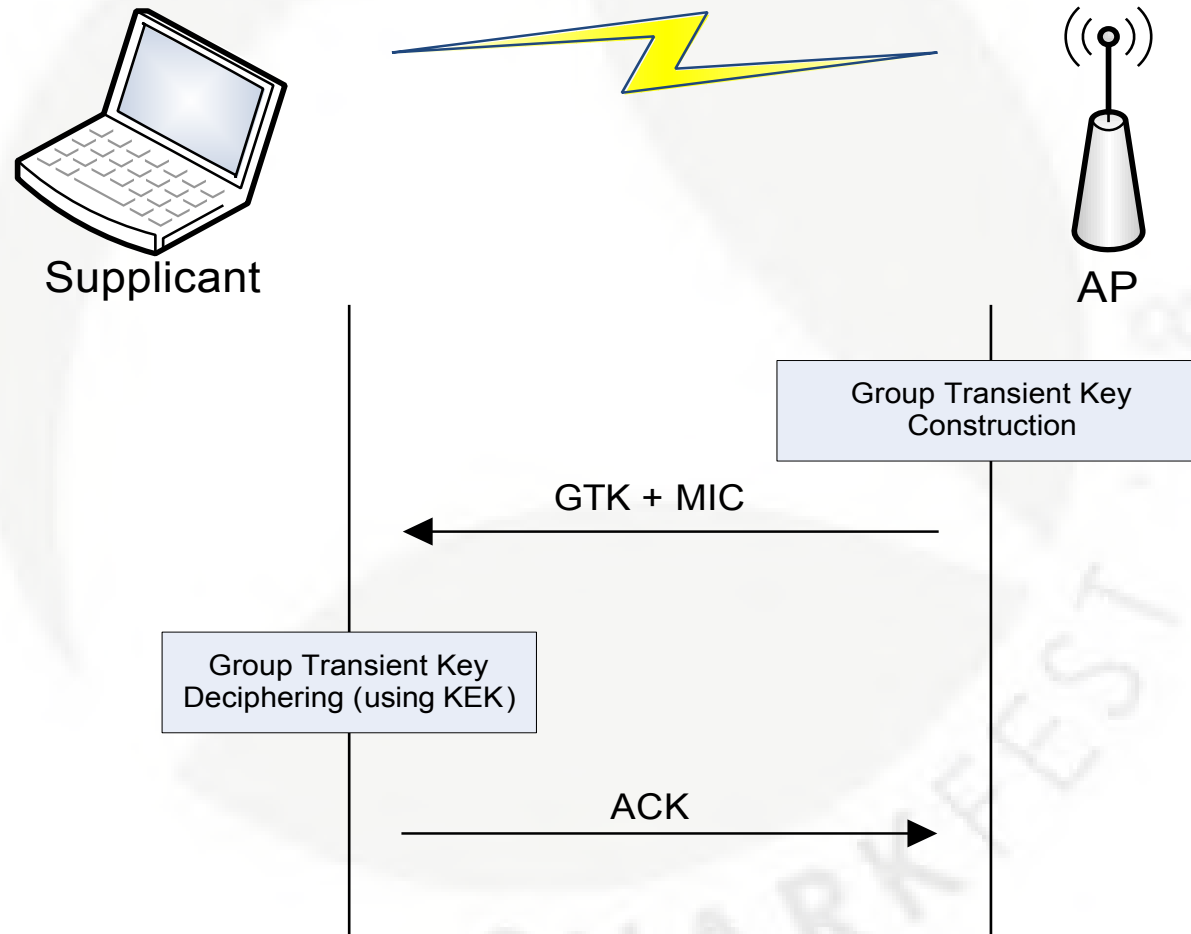
Interactions with networks – Encryption - WPA (7)

WPA Key distribution and verification 4-way handshake



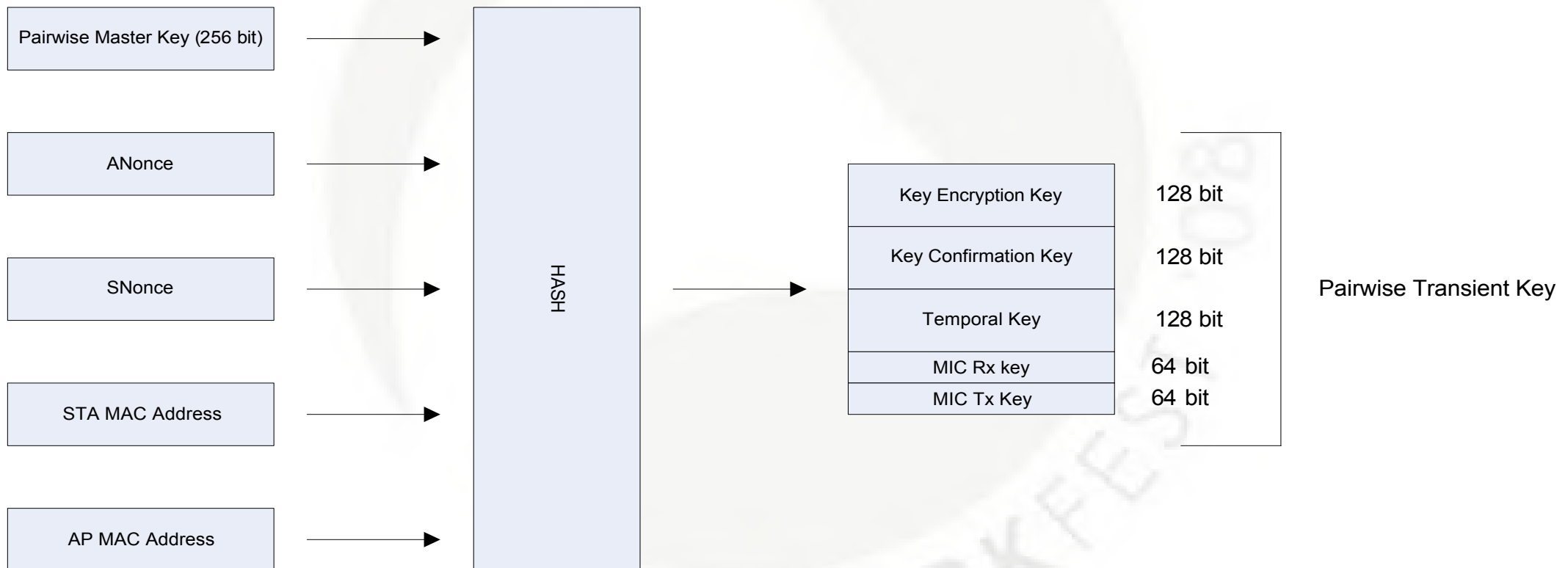
Interactions with networks – Encryption - WPA (8)

Group key handshake



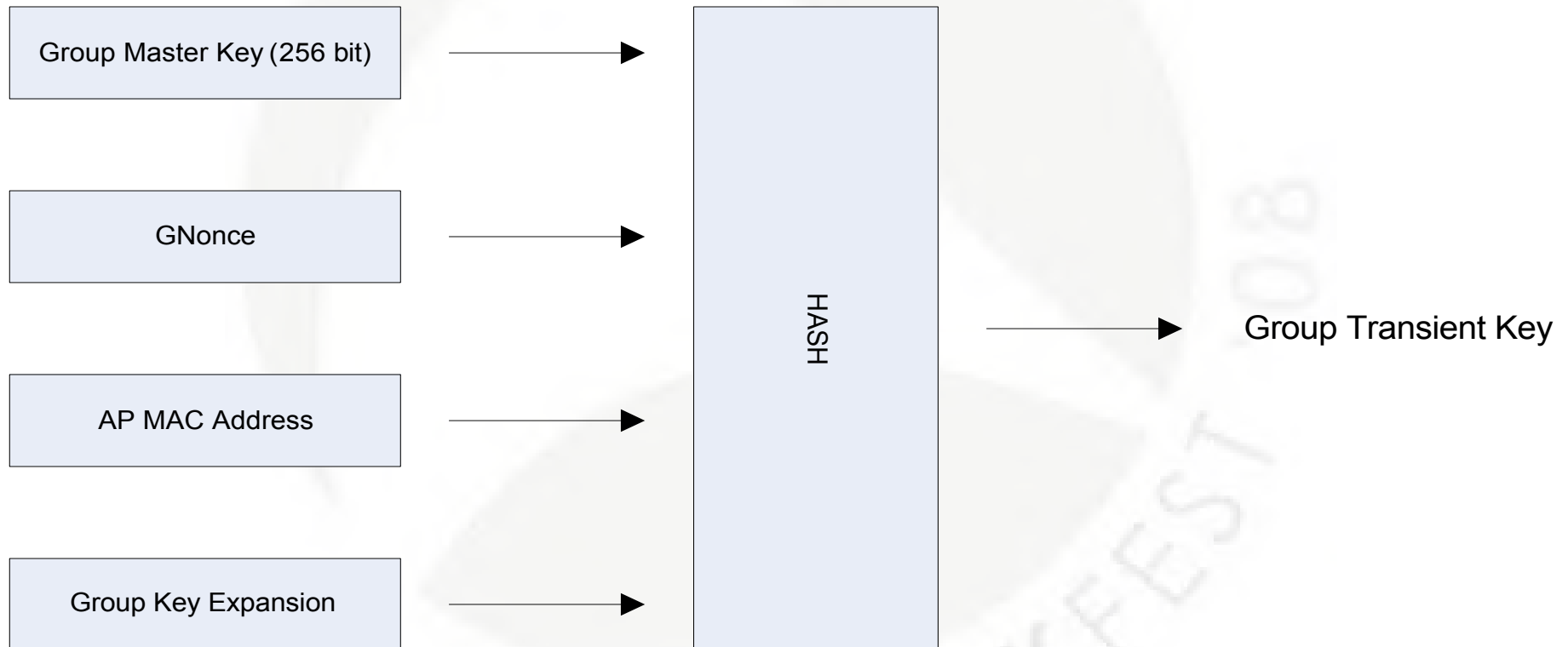
Interactions with networks – Encryption - WPA (9)

WPA Key exchange and verification PTK Generation



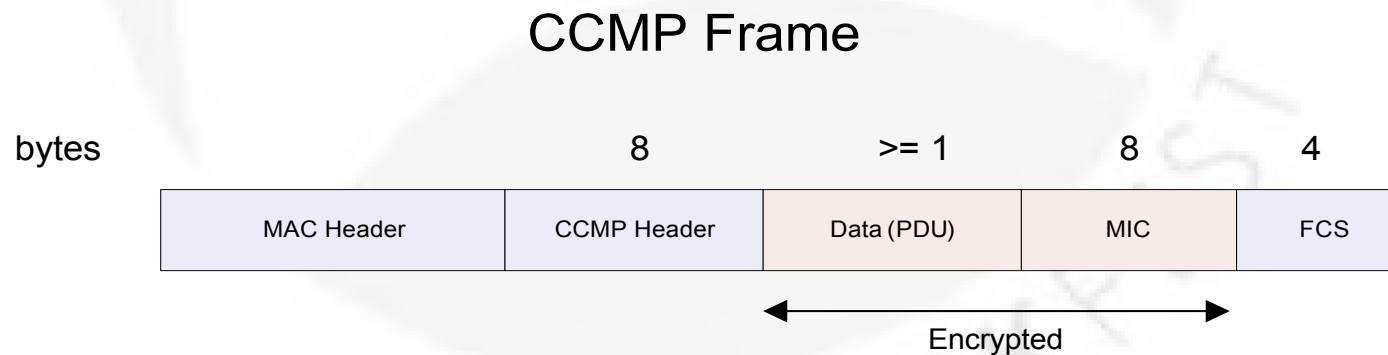
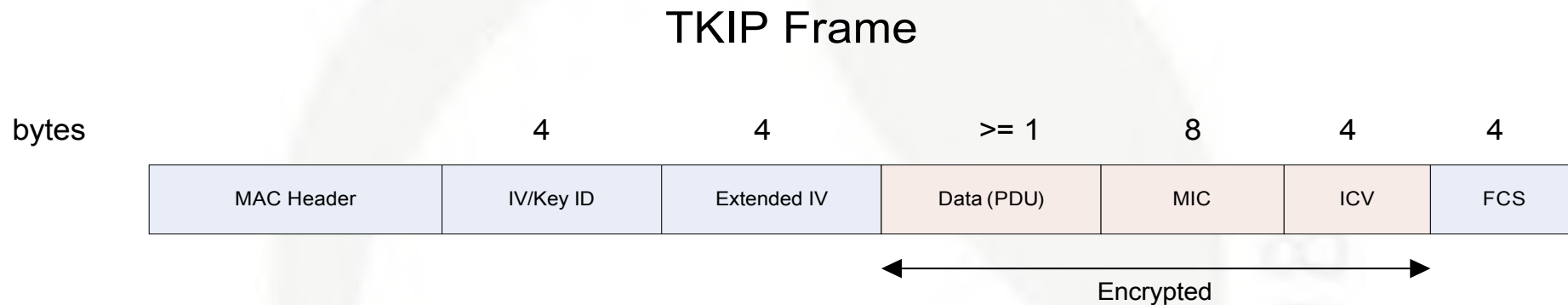
Interactions with networks – Encryption - WPA (10)

WPA Key exchange and verification GTK Construction

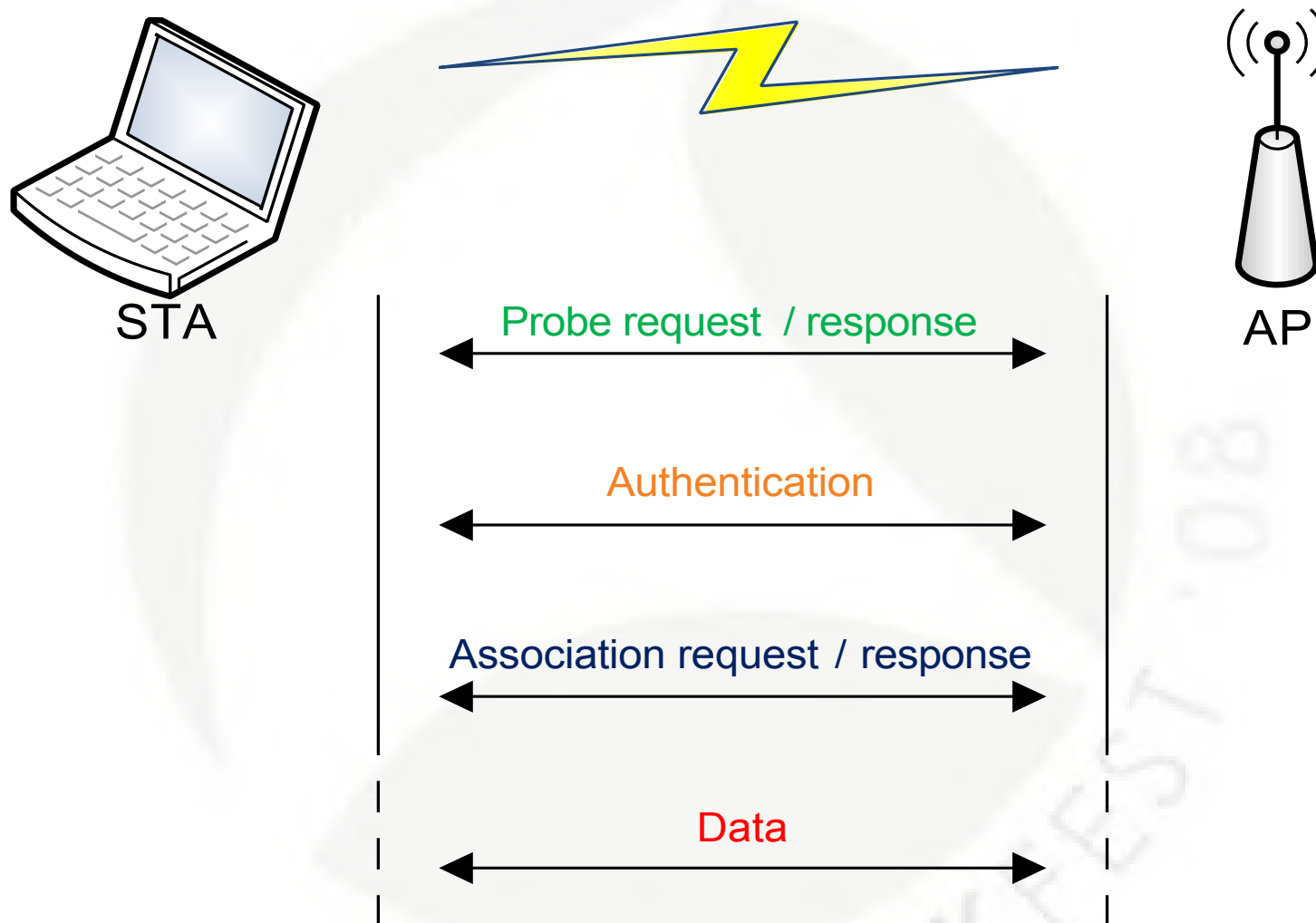


Interactions with networks – Encryption - WPA (11)

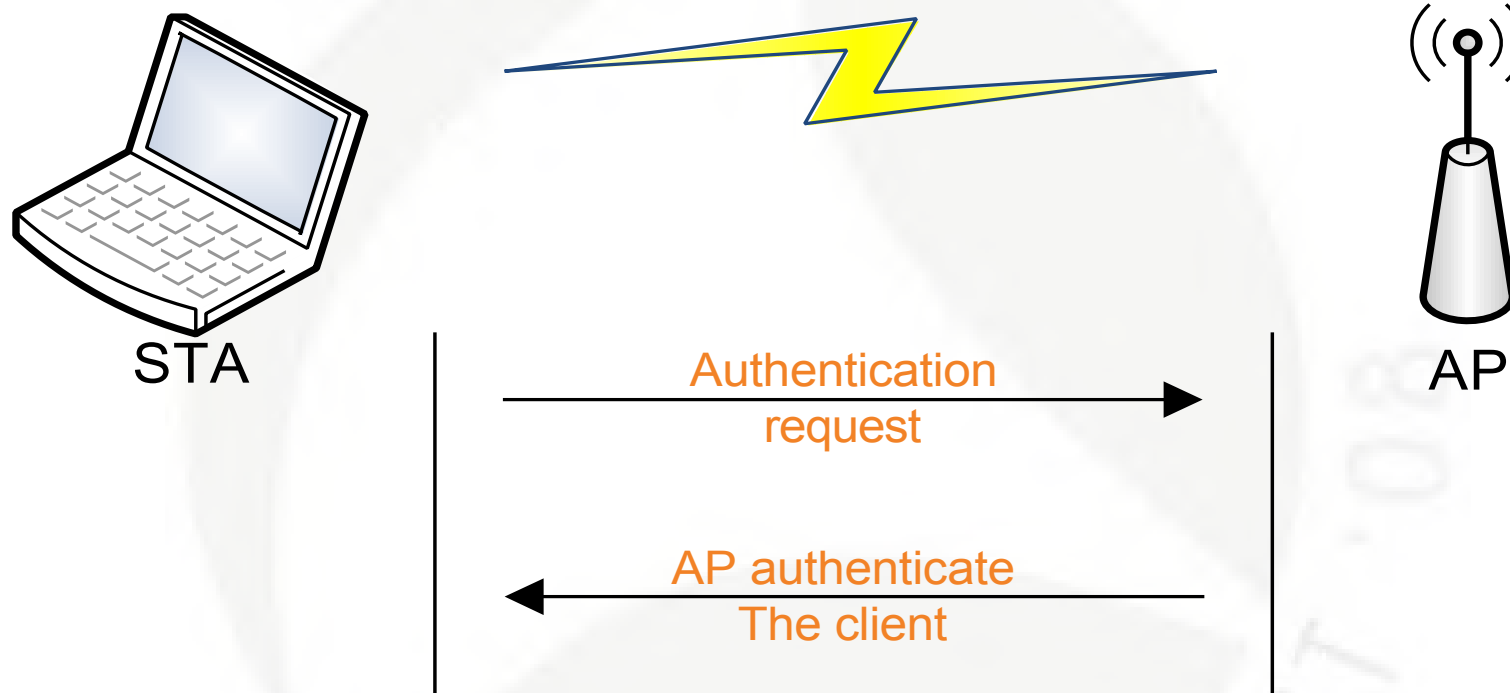
Data Encryption and Integrity



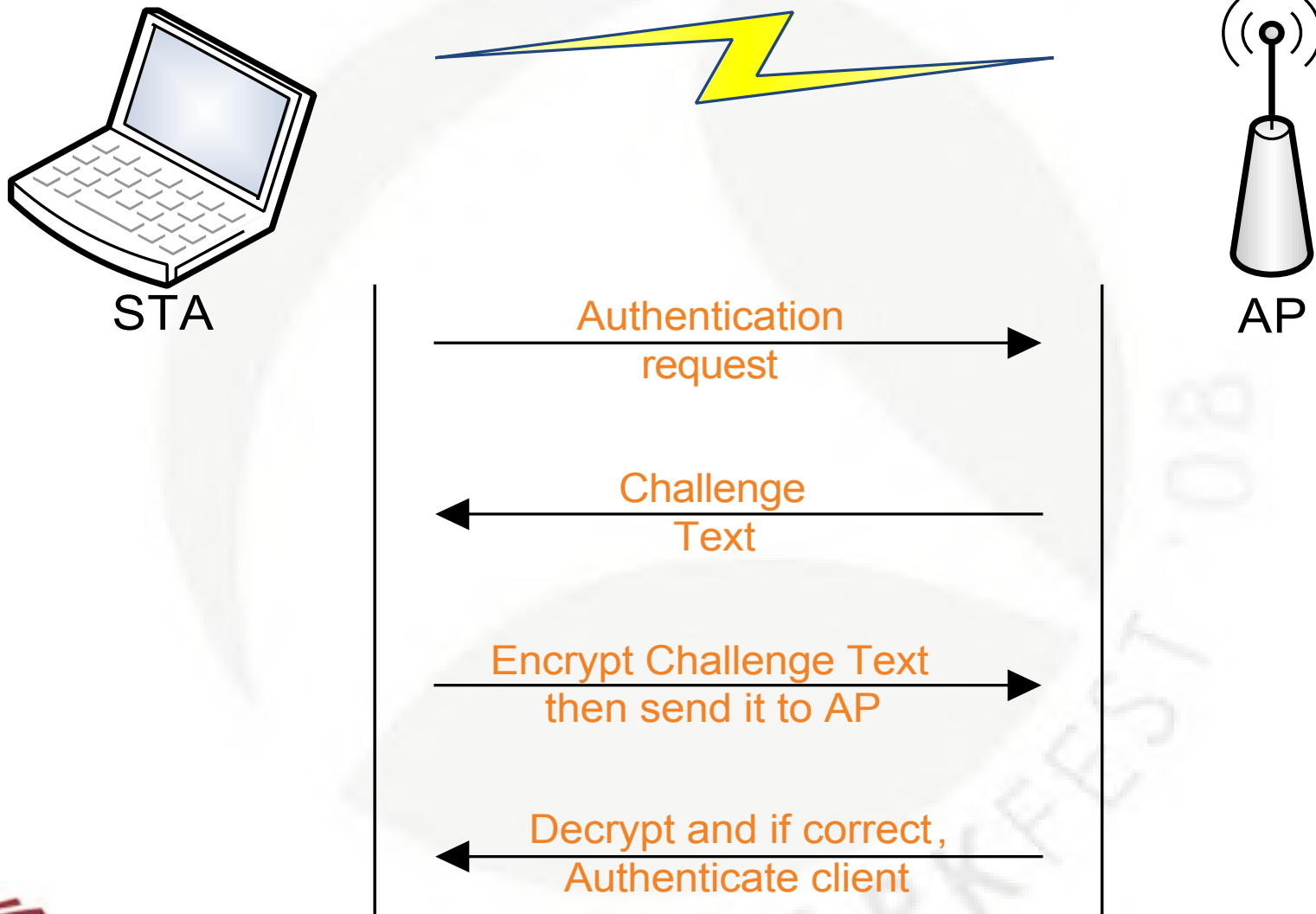
Interactions with networks



Interactions with networks – Authentication - Open



Interactions with networks – Authentication - Shared



Capture file analysis

- Hotspot / Open network
- WEP network (Shared authentication)
- WPA network

OSdep

- Similar to LORCON
- OS supported: Linux, *BSD, Windows
- Automatic recognition of the interface / driver
- Sniffing capabilities

OSdep (2)

- Control interfaces
 - Get and set MAC address
 - Get and set Channel
 - Get and set rate
- Networking
- Create your own DLL to interact with special drivers on windows

OSdep - Applications

- Existing tools:
 - Aircrack-ng 1.0
 - MDK3

- Sample application:

www.aircrack-ng.org/wifiping.tar.gz

Questions?