

# WLAN Monitoring and Analysis

# Outline

- WLAN monitoring
- Tools
- Issues
- Solutions

# Introduction

- Wireless networking is a complex field.
- With countless standards, protocols, and implementations, it is not uncommon for administrators to encounter configuration issues that require sophisticated monitoring, troubleshooting and analysis mechanisms.
- See: Three Steps for Bullet-proof Wireless LAN Security & Management, NIST Guidelines for Securing Wireless Local Area Networks (WLANs), etc. for very interesting articles on the subject.

# Reasons to Monitor

- Troubleshooting
- Operation Analysis
- RF analysis
- Performance Testing
- Security Analysis
- Intrusion Analysis
- MAC and PHY

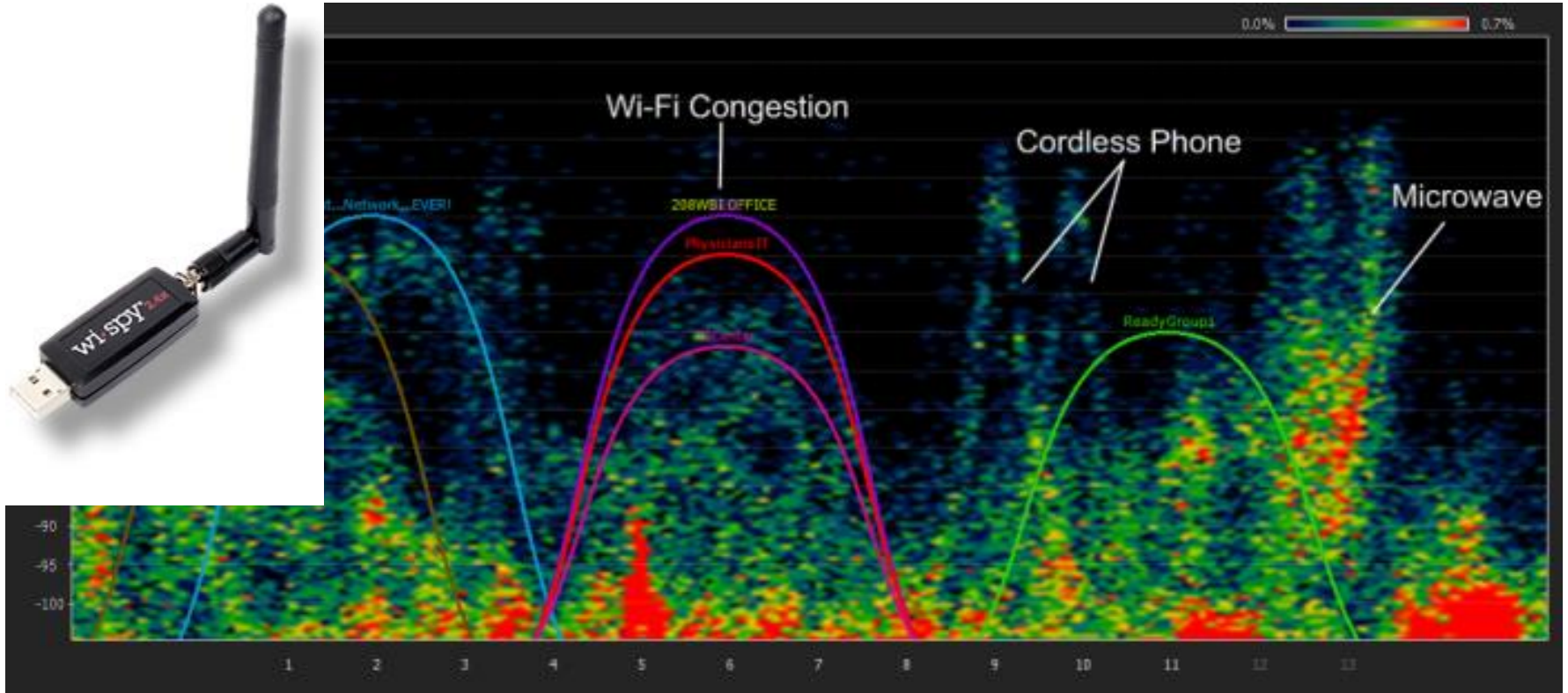
# Problems and Limitations

- RF Environment
- Multiple channels to monitor
- Range of monitor
- Wide area to cover
- Receiver Sensitivity
- Physical Environment
- Encrypted traffic

# RF Monitoring and Analysis

- A WiFi Spectrum Analysers will:
- Show RF activity on supported channels
- Detect Interference
- Help with site surveys
- Help decide which channels to use to get best performance

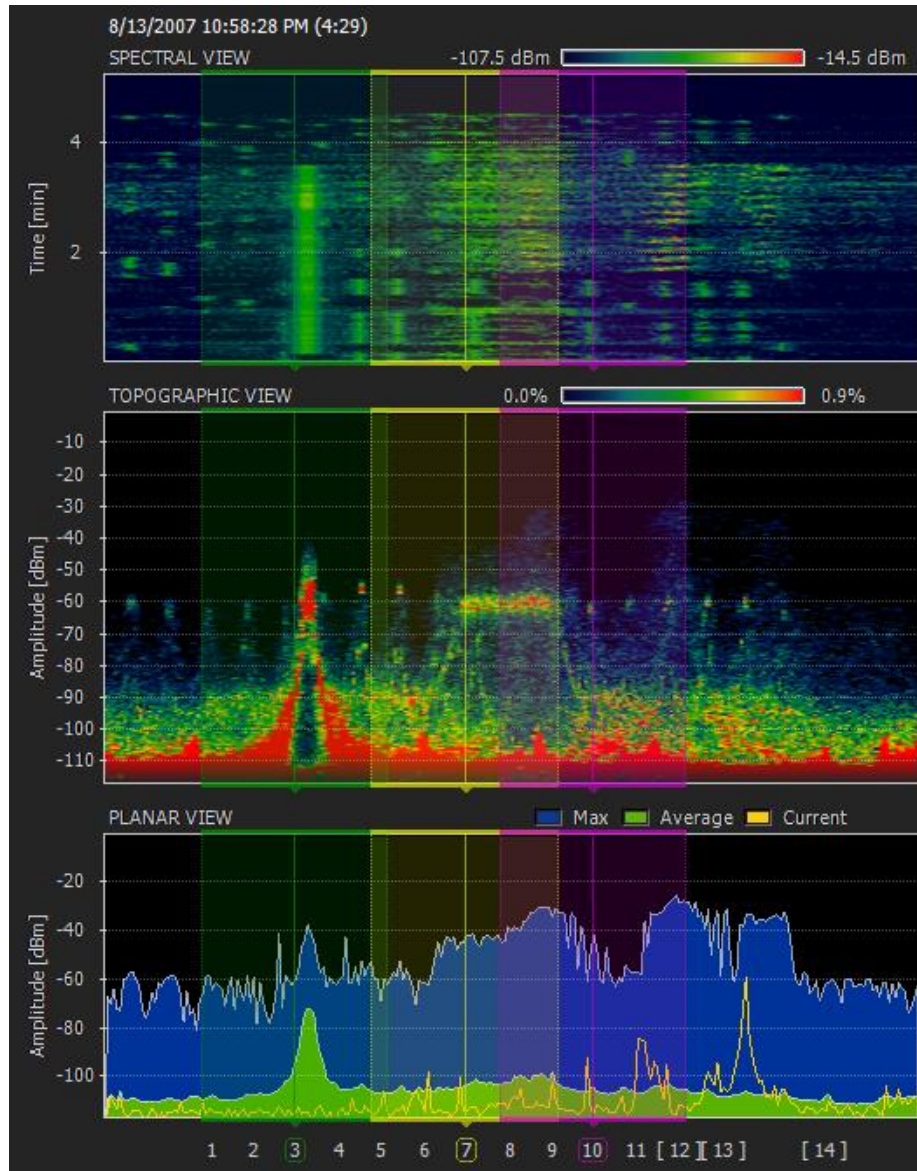
# WiSpy – Wi-Fi Spectrum Analyser



See you-tube video tour

<http://www.metageek.net/products/wi-spy-24x>

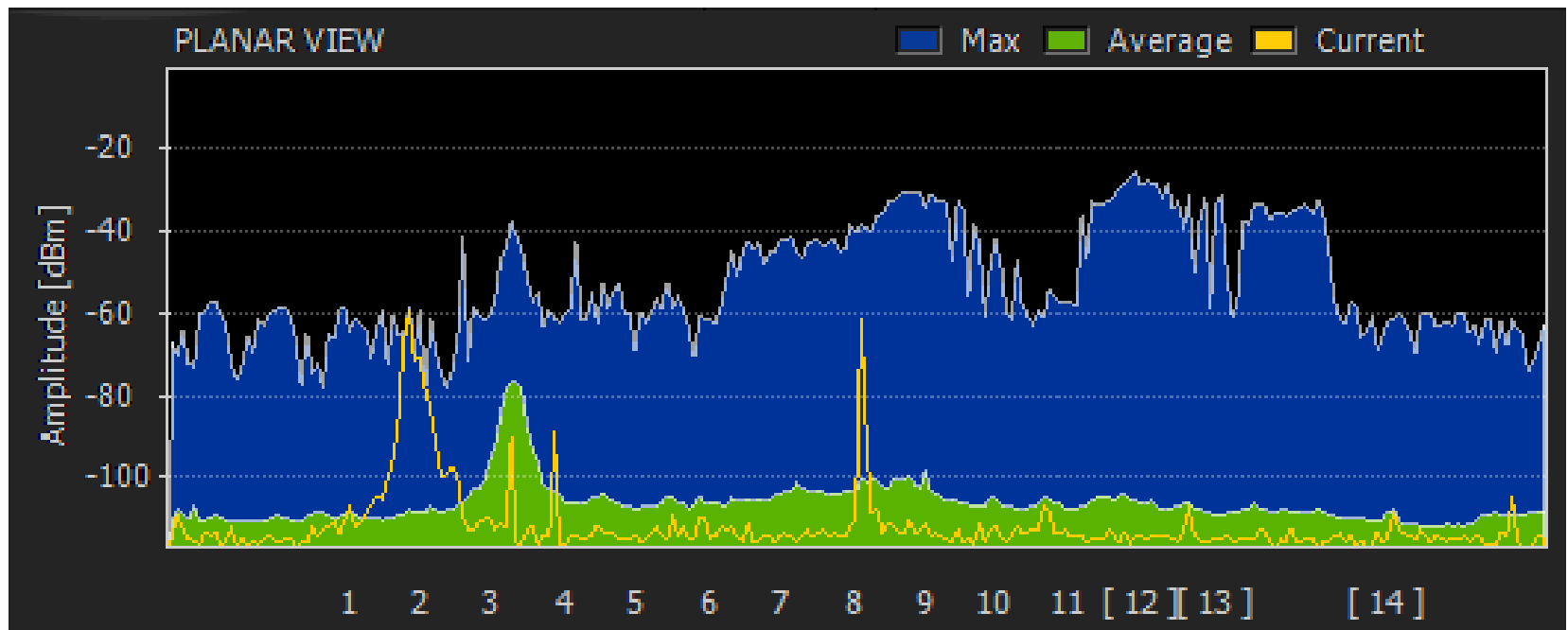
# WiSpy Chanalyser Package Views





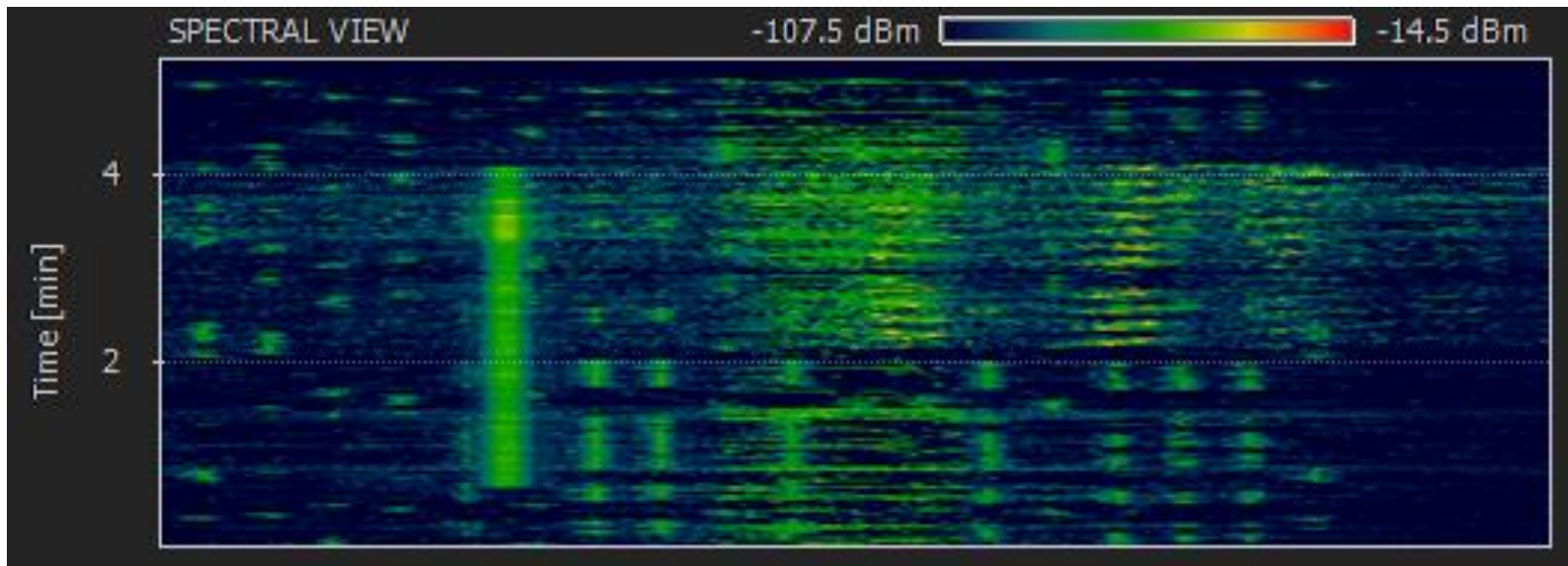
# Planar View

- Shows a **typical amplitude over frequency display**.
- The yellow line shows the current amplitude, the green shows the average amplitude, and the blue shows the maximum amplitude.



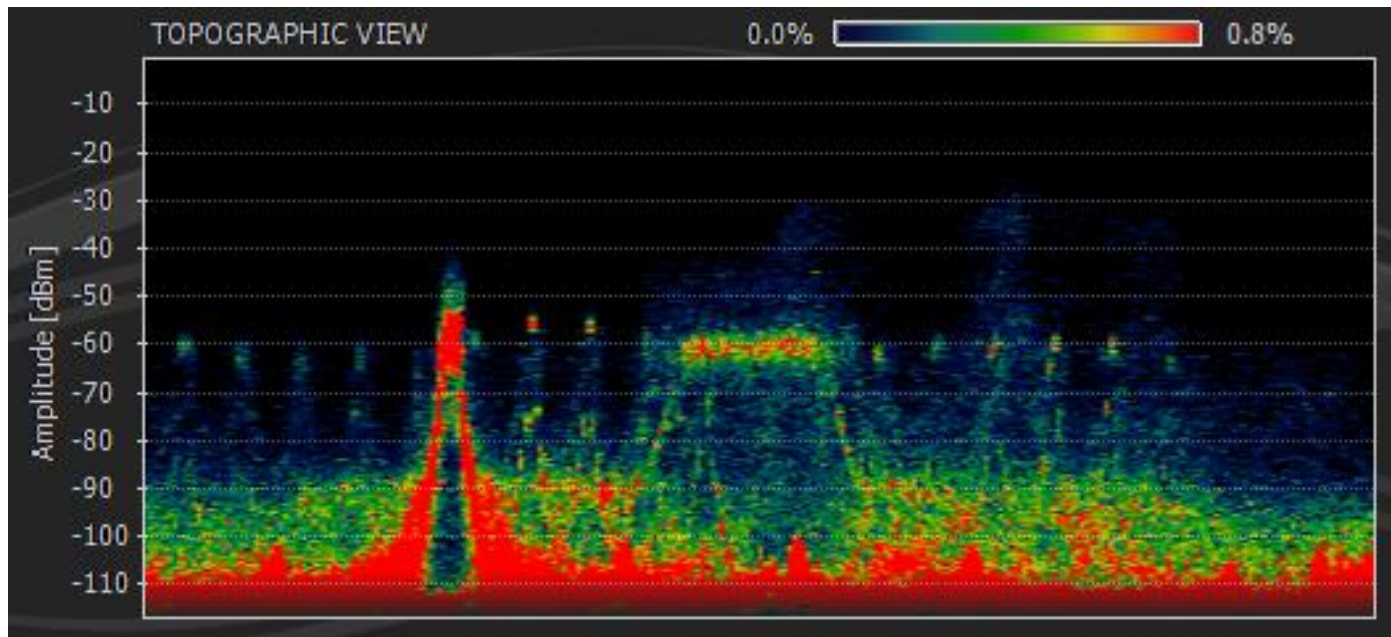
# Spectral View

- Contains a waterfall graph that shows amplitude over time for each frequency.
- The colour of each frequency/time coordinate represents the amplitude of that frequency, with dark blue representing low amplitudes and bright red representing high amplitudes as shown in the legend.

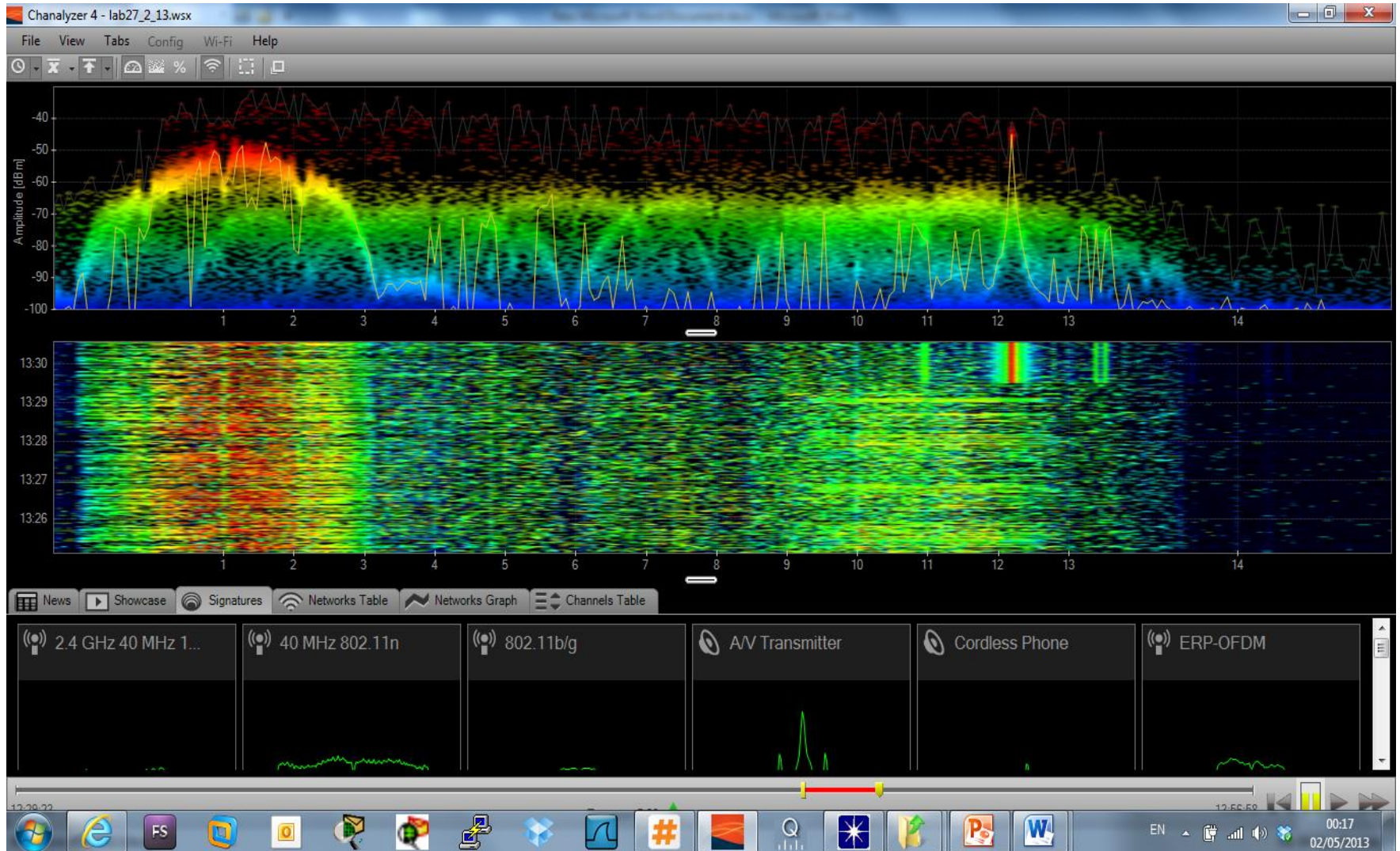


# Topographic View

- Contains an amplitude over frequency graph **showing the popularity of each frequency/amplitude coordinate during the time displayed.**
- The coloration of the similar to the Spectral View but represents popularity instead of the amplitude.



# Video Sender Interference



# Site Survey Tools

- Tools such as NetStumbler, inSSIDer and vendor supplied ones like Cisco Site Survey.
- Provide RF signal strength and many other useful performance, location and security indicators.
- InSSIDder can be integrated with Channelyzer site survey tool.



# NetStumbler

Network Stumbler - 20090203210300

File Edit View Device Window Help

20090203210300

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR
00184D63C4E8	SKY16753		6	54 Mbps	(Fake)	AP	WEP	7	-93	-100	7
001F9F47E7BD	ThomsonF82C7C		6	54 Mbps	(Fake)	AP	WEP	6	-94	-100	6
001E2AF05B16	SKY96438		1	54 Mbps	(Fake)	AP	WEP	16	-83	-100	17
001B2F6E4F8C	SKY58451		1	54 Mbps	(Fake)	AP	WEP	8	-90	-100	10
00184D62F374	SKY79278		1*	54 Mbps	(Fake)	AP	WEP	33	-67	-100	33

Ready

GPS: Disabled 5 / 5

Network Stumbler - 20100221141213

File Edit View Device Window Help

20100221141213

Channels

- 1
- 6
- 11

SSIDs

- 0016CE268BC1
- 00184D62F374**
- 0024B23D8B70

Filters

- Encryption Off
- Encryption On
- ESS (AP)
- IBSS (Peer)
- CF Pollable
- Short Preamble
- PBCC
- Short Slot Time (11g)

Signal/Noise, dBm

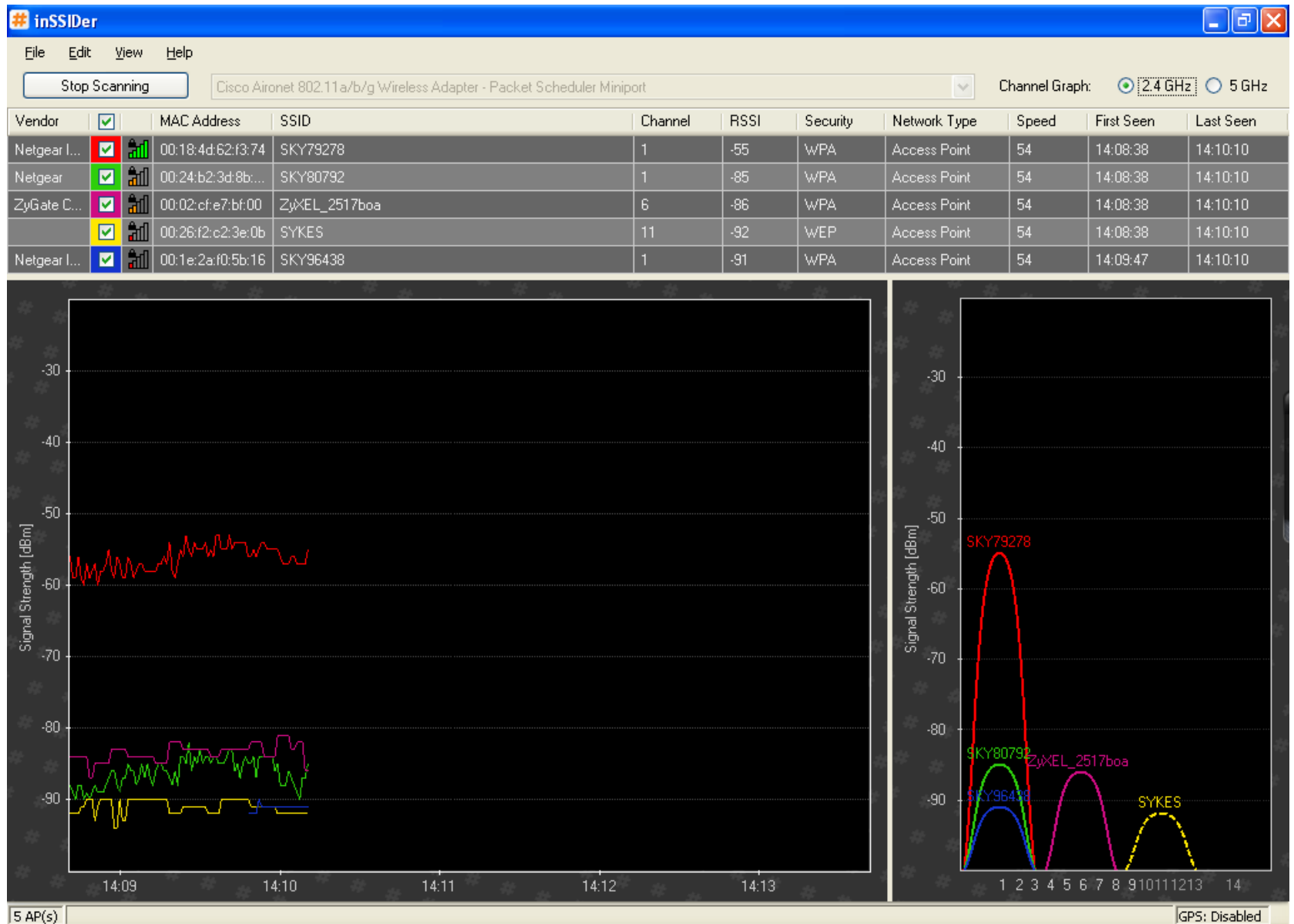
21/02/2010 14:12:15 21/02/2010 14:13:20 21/02/2010 14:14:20 21/02/2010 14:15:20 21/02/2010 14:16:20 21/02/2010 14:17:20 21/02/2010 14:18:20

Ready

5 APs active

GPS: Disabled

# InSSIDer



# Cisco Site Survey 1

**Cisco Aironet Site Survey Utility**

Action | Thresholds | AP Scanning | Help


Adapter Information

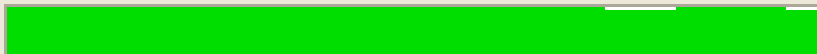
Device: Cisco Aironet 802.11 a/b/g Wireless Adapter  
Status: Associated


Associated AP Status | AP Scan List

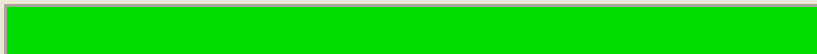
Access Point: MAC:00-18-4D-62-F3-74


Channel: 1 (2412 MHz)

Signal Strength: **-71dBm** 

Noise Level: **-93dBm** 

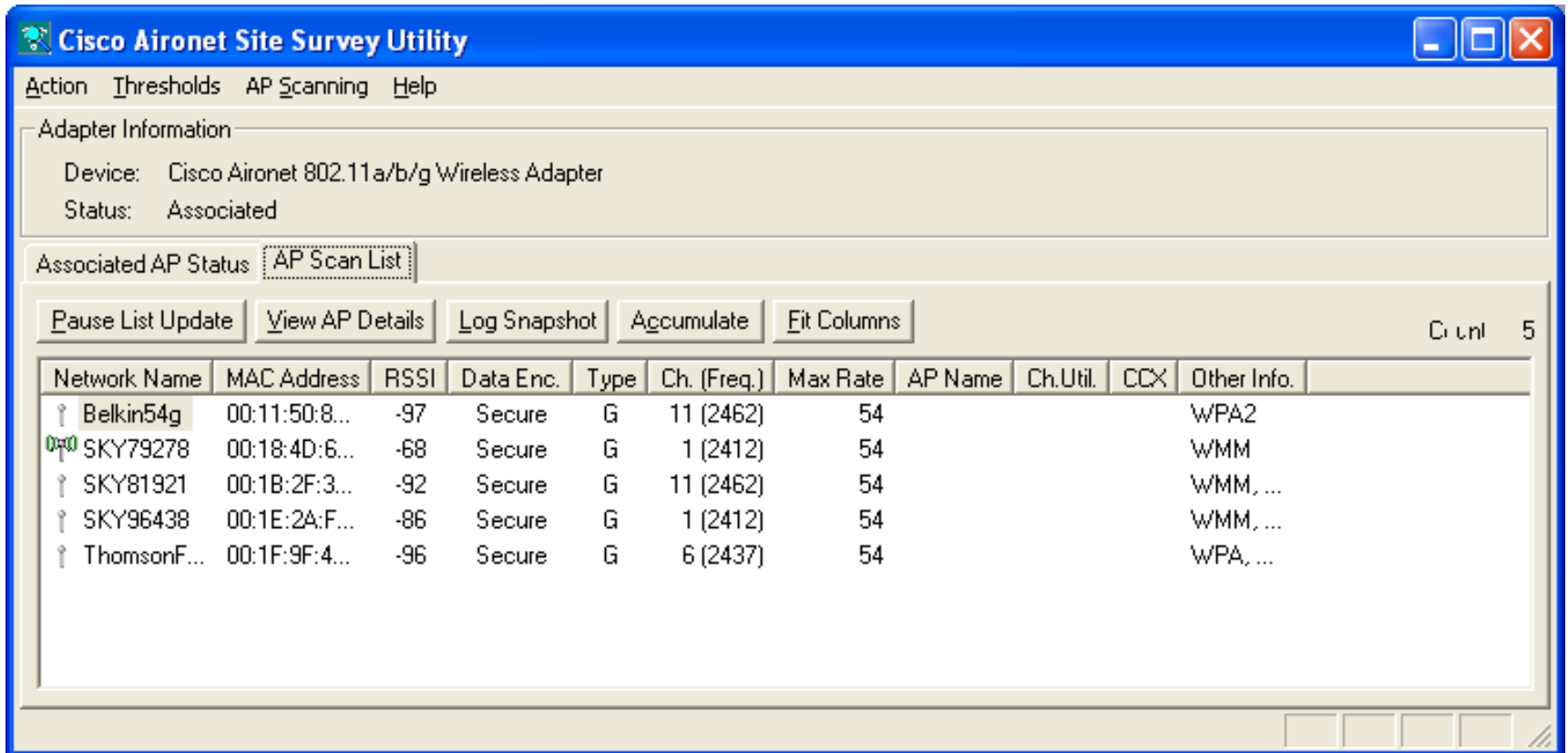
Signal-to-Noise Ratio: **Good (22dB)** 

Link Speed: **54Mbps** 

☐ Display in percent      - 10  Time in seconds 0



# Cisco Site Survey 2



The screenshot shows the Cisco Aironet Site Survey Utility window. The title bar reads "Cisco Aironet Site Survey Utility". The menu bar includes "Action", "Thresholds", "AP Scanning", and "Help". The "Adapter Information" section displays "Device: Cisco Aironet 802.11 a/b/g Wireless Adapter" and "Status: Associated". The "Associated AP Status" section has a tab labeled "AP Scan List". Below this are buttons for "Pause List Update", "View AP Details", "Log Snapshot", "Accumulate", and "Fit Columns". A status bar at the bottom right shows "Ctrl 5". The main area contains a table of associated APs.

Network Name	MAC Address	RSSI	Data Enc.	Type	Ch. (Freq.)	Max Rate	AP Name	Ch.Util.	CCX	Other Info.
Belkin54g	00:11:50:8...	-97	Secure	G	11 (2462)	54				WPA2
SKY79278	00:18:4D:6...	-68	Secure	G	1 (2412)	54				WMM
SKY81921	00:1B:2F:3...	-92	Secure	G	11 (2462)	54				WMM, ...
SKY96438	00:1E:2A:F...	-86	Secure	G	1 (2412)	54				WMM, ...
ThomsonF...	00:1F:9F:4...	-96	Secure	G	6 (2437)	54				WPA, ...

# Monitoring Issues

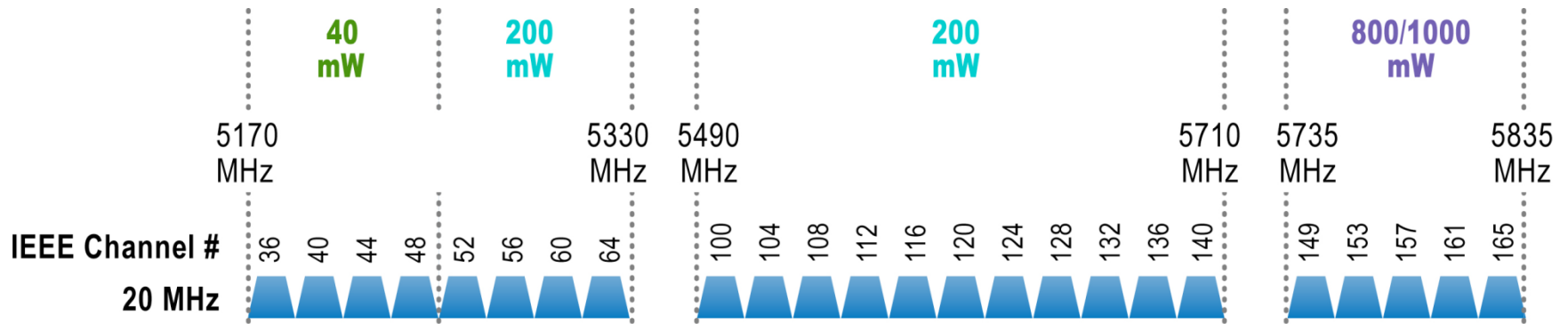
- Multiple channels to cover
- Wireless Modes
- Limited Range
- Receiver Sensitivity
- Wide area to coverage
- Environment
- Encrypted traffic

# IEEE 802.11 Channels

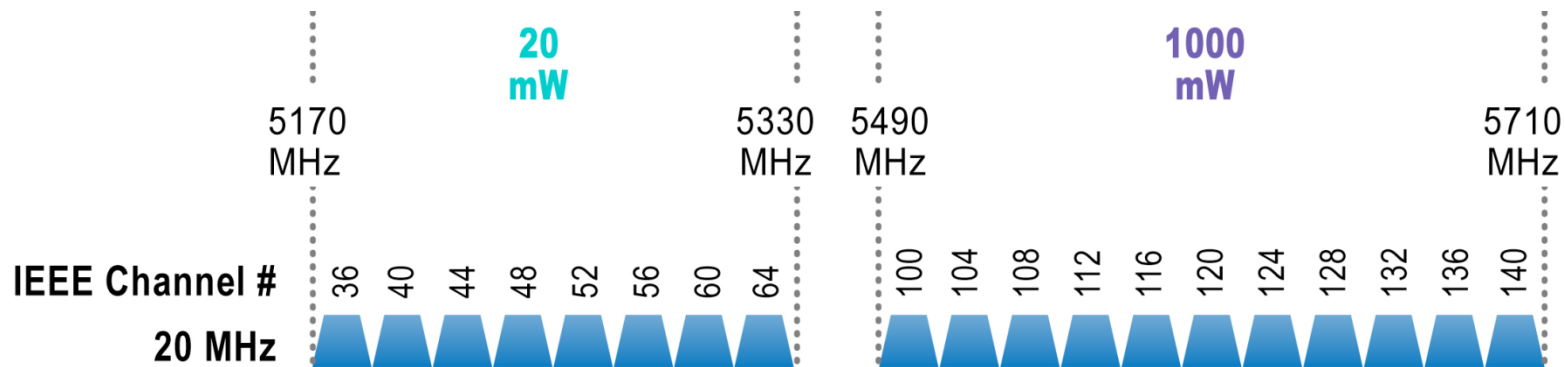
Frequency	Channel Number	Frequency	Channel Number
2.412 GHz	1	2.484 GHz	14
2.417 GHz	2	5.180 GHz	36
2.422 GHz	3	5.200 GHz	40
2.427 GHz	4	5.220 GHz	44
2.432 GHz	5	5.240 GHz	48
2.437 GHz	6	5.260 GHz	52
2.442 GHz	7	5.280 GHz	56
2.447 GHz	8	5.300 GHz	60
2.452 GHz	9	5.320 GHz	64
2.457 GHz	10	5.745 GHz	149
2.462 GHz	11	5.765 GHz	153
2.467 GHz	12	5.785 GHz	157
2.472 GHz	13	5.805 GHz	161

If you want to analyze the traffic for a specific wireless AP or station, you must identify the channel or frequency used by the target device, and configure your wireless card to use the same channel before initiating your packet capture. This is because wireless cards can only operate on a single frequency at any given time. If you wanted to capture traffic from multiple channels simultaneously, you would need an additional wireless card for every channel you wanted to monitor.

# New 5GHz Channels Allocation

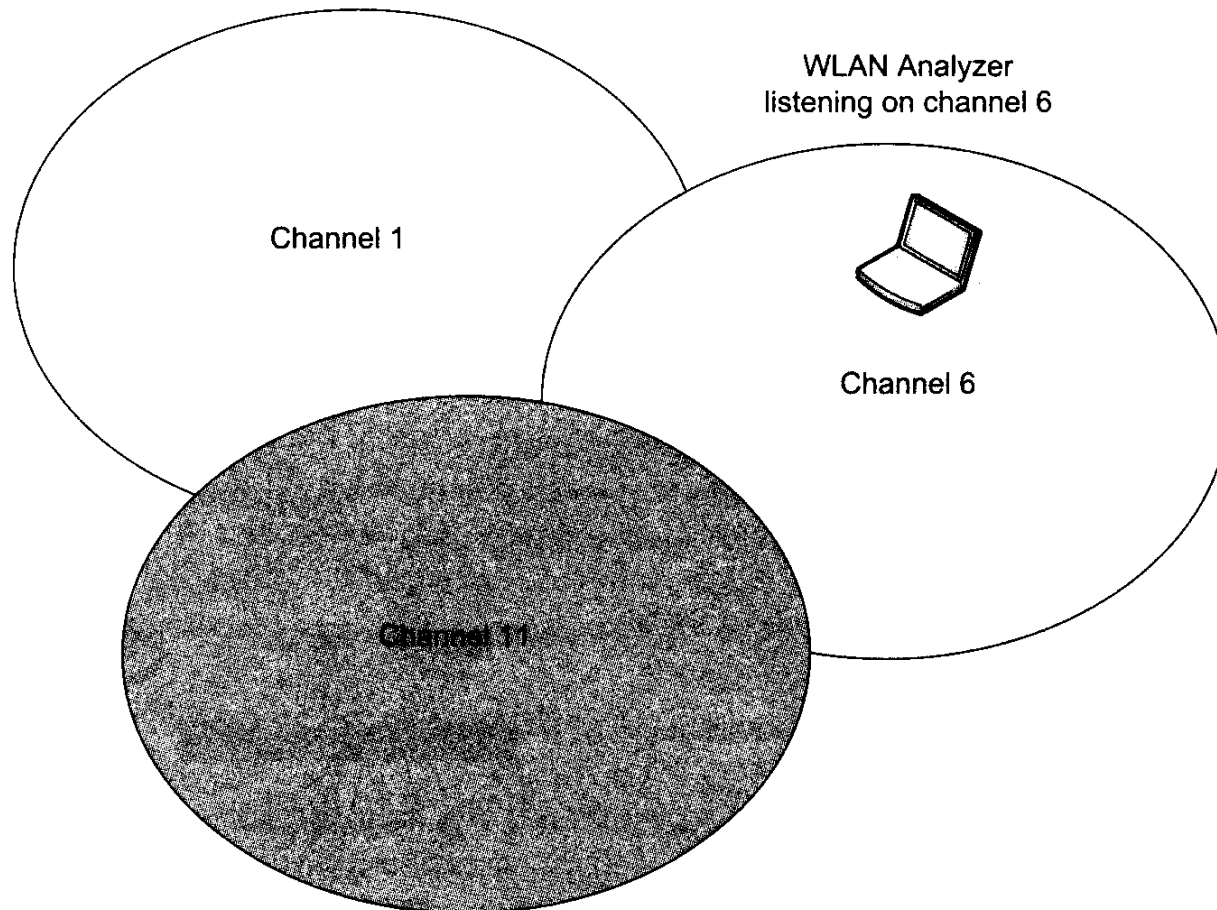


US Channel Allocations

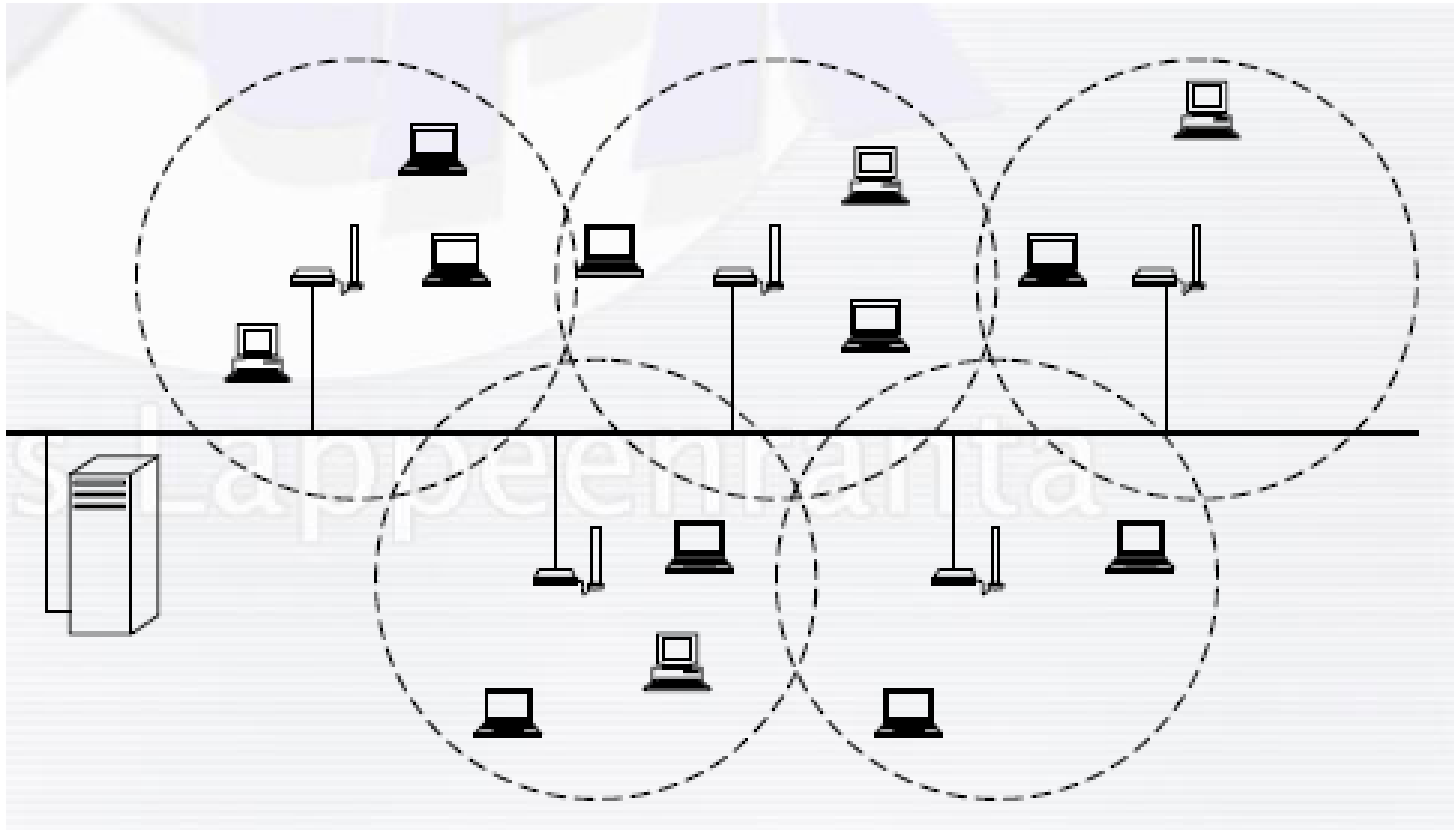


European Channel Allocations

# Multi-cell Monitoring Problem



# Extended Service Set

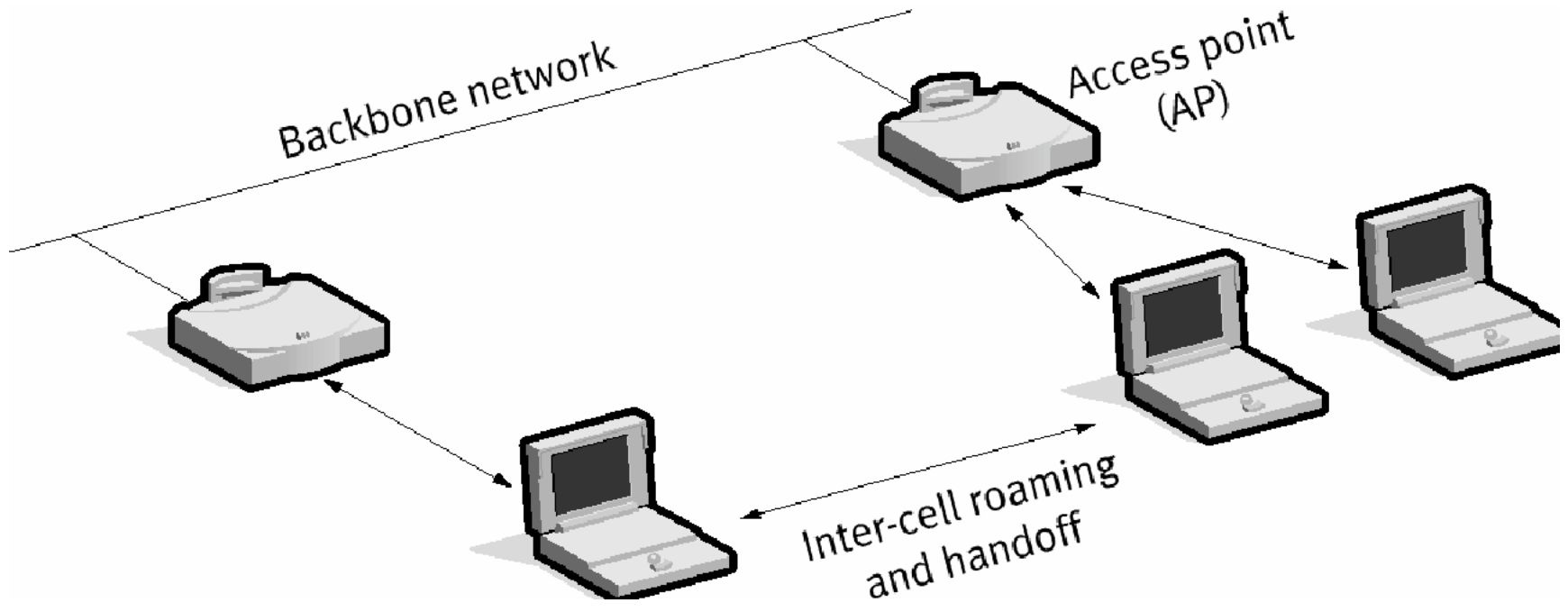


# Example1

## Multiple Channel Problem

- **Roaming between cells** and monitoring with a single analyser illustrates multiple channel area problems.
- Wireless station **changes channel** in order to associates with new Access Point making it difficult for a single wireless analyser to track.
- Most large WLANs use many access points and different channels.

# Roaming





# Roaming Issue

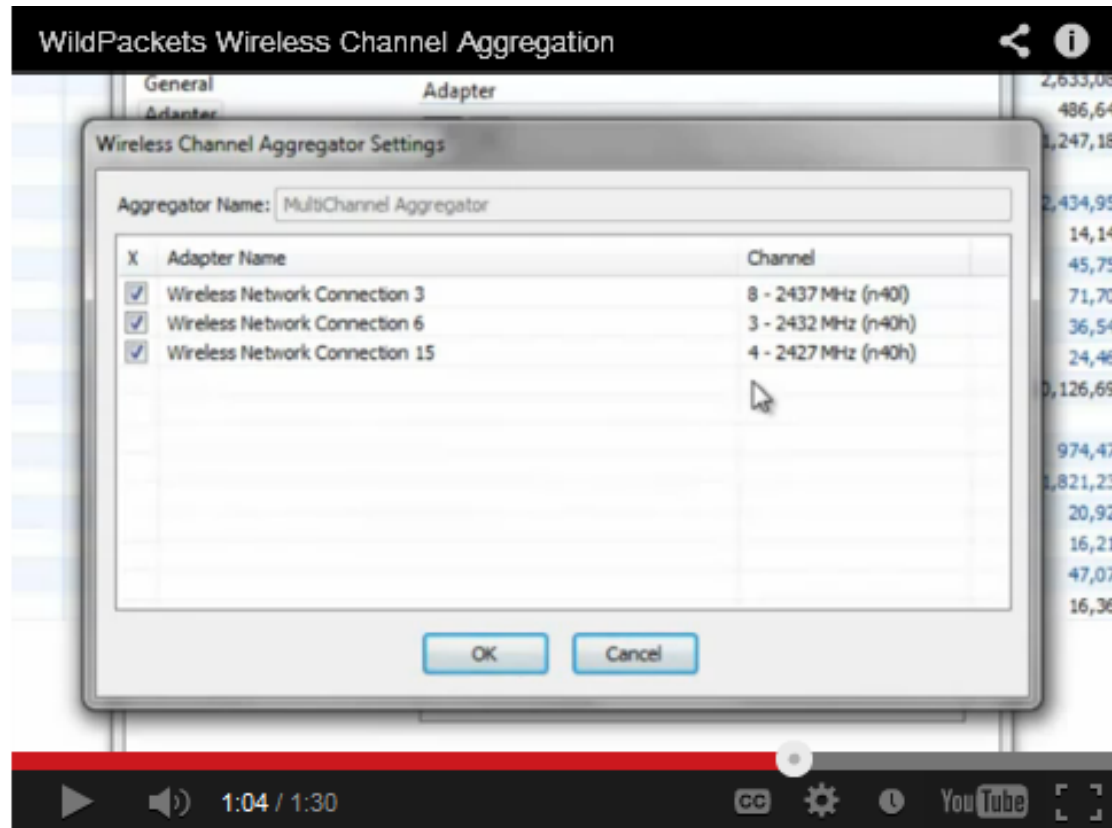
- To adequately monitor, analyse, and troubleshoot your WLAN you must collect data across multiple-channels **simultaneously** for visibility when users roam.
- With traditional wired network analysis, there's only one "channel" in use, so **channel aggregation** is a function that is **unique** to WLAN analysis.

# Solution 1 Channel Aggregation

- Employ an adapter for each channel of interest.
- e.g. Cover channel 1 , 6 and 11 in a typical 2.4 GHz band wireless LAN
- Some vendors such as WildPackets provide special drivers and aggregation software for the purpose of monitoring on multiple channels simultaneously.
- e.g. The Cisco EA1000 USB adapters can be used to do this

# WildPackets solution

## see video



[http://www.youtube.com/watch?feature=player\\_embedded&v=pVg-2SOeDBc](http://www.youtube.com/watch?feature=player_embedded&v=pVg-2SOeDBc)

# Solution2 Distributed Analyser

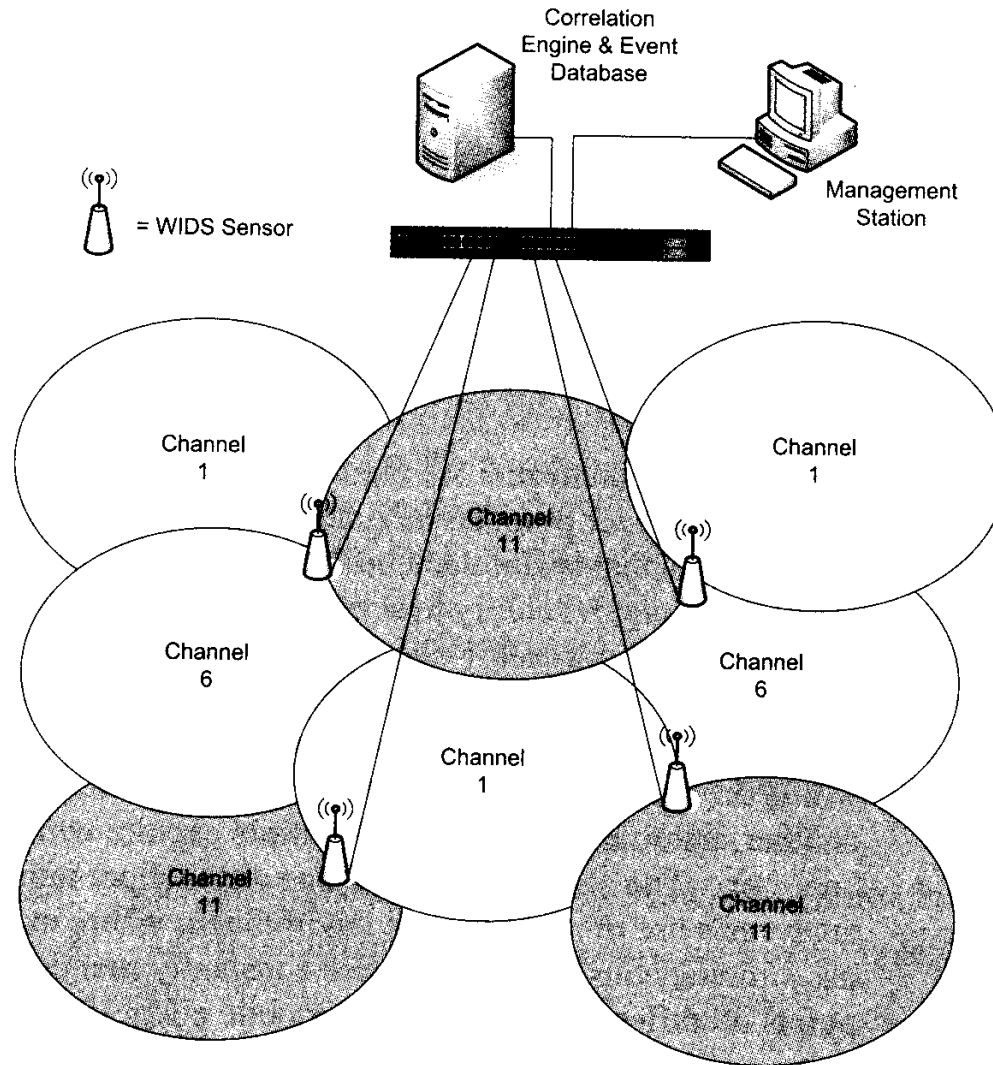
- **Wireless Intrusion Detection System (WIDS)** is a solution to wide area multiple channel problems.
- Special hardware sensors (or wireless stations running S/W) report back to a central correlation engine for analysis.

# WIDS Sensor

- Normally PoE Devices sited to give maximum coverage



# Distributed Analyzer Scenario



# Environmental Impact

- Wireless node proximity
- Output power and Antennas
- Multipath
- RF signal blockage
- RF interference sources
- Co-channel interference

# Encryption of Wireless Data

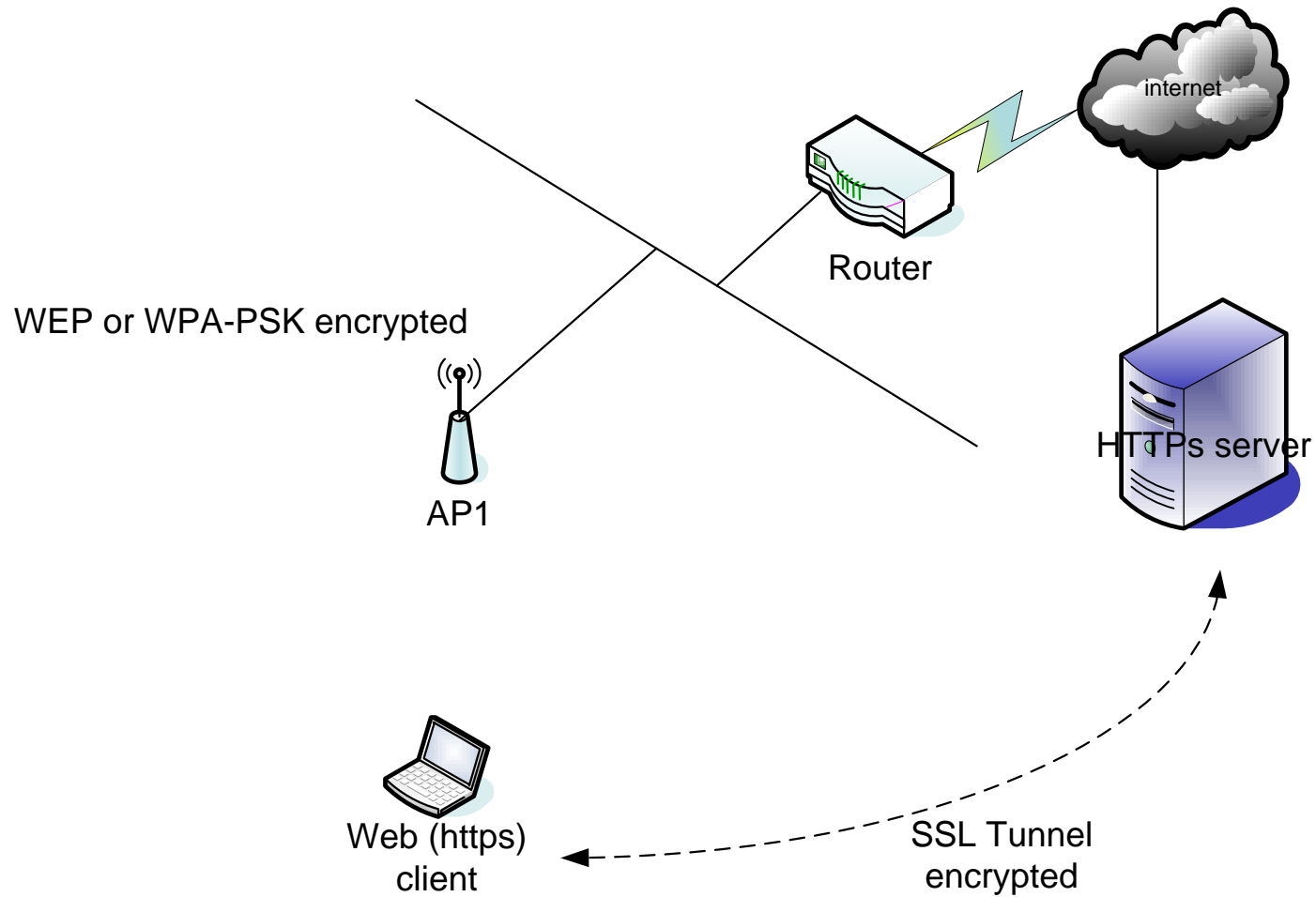
- Can have impact on ability to monitor and network performance.
- Encryption can occur at layer 2,3 or 7.
- Some enterprises encrypt at all 3 layers.
- E.g. L2 WEP or WPA
- L3 IPSec
- L7 SSL



# Example1      2-level Encryption

- Consider accessing a secure web site over a wireless LAN.
- In this case the analyser can only decrypt at layer 2 if WEP or WPA-PSK is used.
- So will only see SSL encrypted https packets.

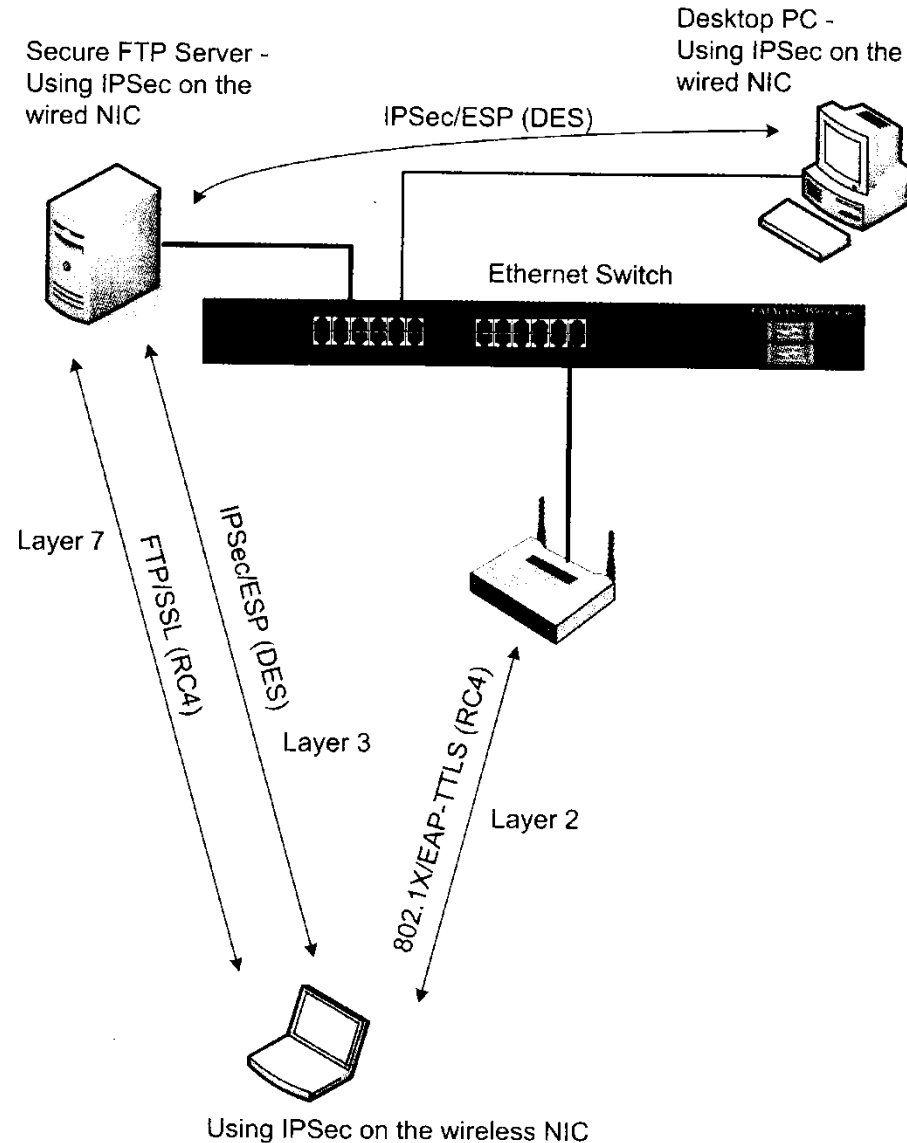
# Example 1 Diagram



## Example 2 of Multilevel Encryption

- In this case enterprise L2 security is in place and
- A L3 IPSec VPN is established and
- The file is being transferred with secure FTP
- The analyser will not see any of the data packets since it is not possible to use the enterprise class rotating keys for IEEE 802.1x EAP systems in the analyser.

# Example 2      3-level Encryption



# Encrypted ping Data Packets

pingtest2.cap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: data Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
74	3.656442	IntelCor_04:2a:c8	Broadcast	IEEE 802	QoS Data, SN=521, FN=0, Flags=.p....T
76	3.672326	IntelCor_04:2a:c8	Broadcast	IEEE 802	Data, SN=2976, FN=0, Flags=.p....F.
77	3.672317	Netgear_62:f3:74	IntelCor_04:2a:c8	IEEE 802	QoS Data, SN=2977, FN=0, Flags=.p....F.
79	3.672314	IntelCor_04:2a:c8	Broadcast	IEEE 802	QoS Data, SN=522, FN=0, Flags=.p....T
81	3.672326	IntelCor_04:2a:c8	Broadcast	IEEE 802	Data, SN=2978, FN=0, Flags=.p....F.
82	3.672317	Netgear_62:f3:74	IntelCor_04:2a:c8	IEEE 802	QoS Data, SN=2979, FN=0, Flags=.p....F.
85	3.703545	IntelCor_04:2a:c8	Broadcast	IEEE 802	QoS Data, SN=523, FN=0, Flags=.p....T
87	3.703559	IntelCor_04:2a:c8	Broadcast	IEEE 802	Data, SN=2981, FN=0, Flags=.p....F.
88	3.703551	Netgear_62:f3:74	IntelCor_04:2a:c8	IEEE 802	QoS Data, SN=2982, FN=0, Flags=.p....F.
89	3.703549	Netgear_62:f3:74	IntelCor_04:2a:c8	IEEE 802	QoS Data, SN=2982, FN=0, Flags=.p....R.F.
239	8.718911	IntelCor_04:2a:c8	Broadcast	IEEE 802	QoS Data, SN=524, FN=0, Flags=.p....T
241	8.718922	IntelCor_04:2a:c8	Broadcast	IEEE 802	Data, SN=3035, FN=0, Flags=.p....F.
242	8.718911	Netgear_62:f3:74	IntelCor_04:2a:c8	IEEE 802	QoS Data, SN=3036, FN=0, Flags=.p....F.
244	8.718911	IntelCor_04:2a:c8	Broadcast	IEEE 802	QoS Data, SN=525, FN=0, Flags=.p....T
246	8.718922	IntelCor_04:2a:c8	Broadcast	IEEE 802	Data, SN=3037, FN=0, Flags=.p....F.
247	8.718913	Netgear_62:f3:74	IntelCor_04:2a:c8	IEEE 802	QoS Data, SN=3038, FN=0, Flags=.p....F.
249	8.734783	IntelCor_04:2a:c8	Broadcast	IEEE 802	QoS Data, SN=526, FN=0, Flags=.p....T

Frame 74 (70 bytes on wire, 70 bytes captured)

IEEE 802.11 QoS Data, Flags: .p....T

Data (36 bytes)

Data: 765478B93A9119267357CA90F757CBA5A19F1E585D9BB6D6...

Offset	Hex	ASCII
0010	ff ff ff ff ff 90 20 00 00 69 02 13 00 76 54	.....i...VT
0020	78 b9 3a 91 19 26 73 57 ca 90 f7 57 cb a5 a1 9f	x...&sw ...w....
0030	1e 58 5d 9b b6 d6 1f 9d 20 5b ad f5 ae 75 7d 24	.X].....[...u]\$
0040	72 b5 e2 95 e8 3c	r....<

Data (data.data), 36 bytes

Packets: 5657 Displayed: 1438 Marked: 0

Profile: Default

# Decrypted ping Data Packet

The image shows a Wireshark capture window titled "pingtest2-dec.cap - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help), a toolbar with various icons, and a filter bar. The main packet list displays several packets, with packet 115 selected. Below the list, the packet details pane shows the structure of the selected packet: Internet Protocol (192.168.0.3 to 192.168.0.7), Internet Control Message Protocol (Type: 8, Code: 0, Checksum: 0x3f5c, Identifier: 0x0200, Sequence number: 3072), and Data (32 bytes). The data field is expanded, showing a hexadecimal dump and its corresponding ASCII representation.

No.	Time	Source	Destination	Protocol	Info
112	25.593989	IntelCor_04:2a:c8	Broadcast	ARP	who has 192.168.0.1? Tell 192.168
113	25.594000	IntelCor_04:2a:c8	Broadcast	ARP	who has 192.168.0.1? Tell 192.168
114	25.593990	Netgear_62:f3:74	IntelCor_04:2a:c8	ARP	192.168.0.1 is at 00:18:4d:62:f3:7
115	26.328215	192.168.0.3	192.168.0.7	ICMP	Echo (ping) request
116	26.328198	192.168.0.3	192.168.0.7	ICMP	Echo (ping) request
117	26.328207	192.168.0.7	192.168.0.3	ICMP	Echo (ping) reply
118	26.328199	192.168.0.7	192.168.0.3	ICMP	Echo (ping) reply
119	27.343572	192.168.0.3	192.168.0.7	ICMP	Echo (ping) request
120	27.343558	192.168.0.3	192.168.0.7	ICMP	Echo (ping) request
121	27.343565	192.168.0.7	192.168.0.3	ICMP	Echo (ping) reply
122	27.343559	192.168.0.7	192.168.0.3	ICMP	Echo (ping) reply
123	28.343569	192.168.0.3	192.168.0.7	ICMP	Echo (ping) request
124	28.343558	192.168.0.3	192.168.0.7	ICMP	Echo (ping) request

Internet Protocol, Src: 192.168.0.3 (192.168.0.3), Dst: 192.168.0.7 (192.168.0.7)

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0 ()
- Checksum: 0x3f5c [correct]
- Identifier: 0x0200
- Sequence number: 3072 (0x0c00)

Data (32 bytes)

Data: 61626364656666768696a6b6c6d6e6f707172737475767761...

Offset	Hex	ASCII
0010	00 3c a8 c7 00 00 40 01 50 9f c0 a8 00 03 c0 a8	...@. P.....
0020	00 07 08 00 3f 5c 02 00 0c 00 61 62 63 64 65 66	...?...\.. abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefgh hi

Data (data.data), 32 bytes      Packets: 1303 Displayed: 1303 Marked: 0      Profile: Default

# Wireless Monitoring and Measurement

- Wireshark and Observer can be used to capture and analyze IEEE 802.11 wireless network traffic when using a computer with suitable wireless LAN adapter that can operate in monitor mode.
- Several vendors also offer more specialist WLAN tools such as AiropEEK (now called OmniPeek) or the lower cost CommView for Wi-Fi.
- **Spectrum analysers** are invaluable for detecting and dealing RF interference problems e.g. WiSPY Airmagnet.

# WLAN Analysers

- Are based on LAN protocol analysers
- Most Analysers are used for both Wired and Wireless networks
- Operation is similar
- The WLAN analysers need wireless network adapters that function in **monitor mode** not just promiscuous mode.
- Must be capable of matching the network setup and performance: band, channel width, speed etc.



# WLAN Analyser Types

- Basically the same as LAN protocol analysers such as **Wireshark and Observer**.
- Many specialist features, however in most Enterprise level wireless analysers to deal with the particular monitoring and analysis problems posed by wireless networks.
- They can be Portable (stand alone) or distributed types.

# Common Features

- Easy to use interface
- Monitor mode WLAN card support
- Pre and post packet filters
- Extensive protocol support (all OSI layers)
- Import/Export of capture files
- Security analysis
- Expert analysis
- Site survey tools

# Enterprise Level Analysers

- Observer
- Airoppeek
- Commview for WiFi
- Airmagnet Laptop
- Wireshark is also very capable of capturing and analysing wireless traffic when paired with a monitor mode WLAN card under the Linux OS

# Analysis of Wireless Traffic

- Most analysers can provide information about nodes and channels on the network.
- Site survey tools with similar features to inSSIDder are often integrated into Enterprise level analysers.

# Node Stats

- MAC addresses
- Encryption
- Retries
- Signal Strength

# Channel Analysis

- Information for particular channels is obtained from inside the captured packets.
- Data rate, errors, noise level etc. can be reported.
- Problems arise when multiple channels need to be monitored at the same time.

# Conversation Analysis

- Protocol behaviour between communicating stations.
- Differentiating between user traffic and background traffic.
- Producing flow graphs to help with analysis of protocol operation.

# Expert Analysis

- Automated analysis feature in some analysers e.g. Observer Wireless events are useful for troubleshooting.
- They can be configured to detect rapid or intermittent events that would be otherwise difficult to diagnose.
- E.g. Interference problems or failing RF equipment produce recognisable performance problem signatures.

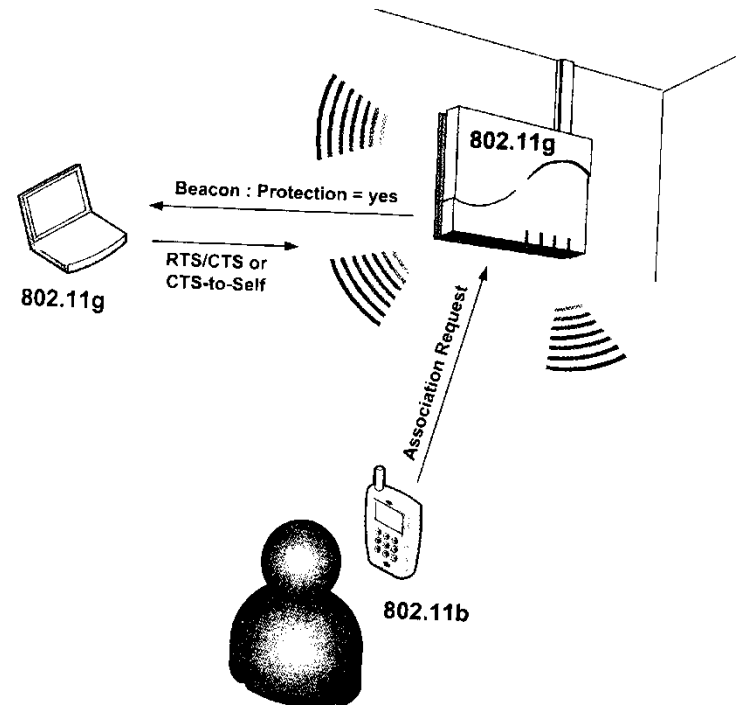


# Performance Measurements

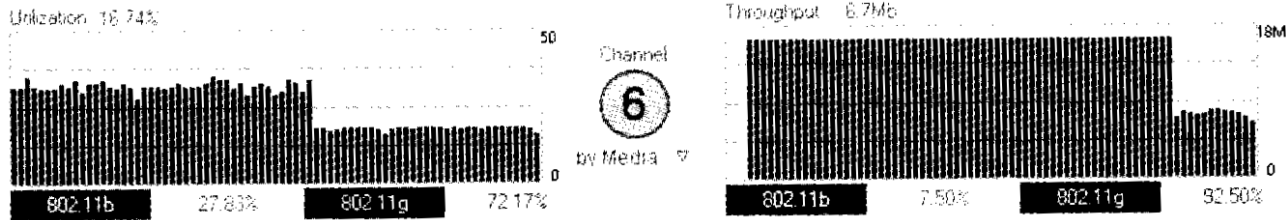
- Utilisation of the RF medium can be measured in real time by most analysers.
- In Pkts/sec or bits/sec to show how well the medium is being used or to detect abuse.
- Alarms can be set on pre-selected performance or security related signatures.
- E.g. heavy usage, unprotected access

# Mixed Mode Performance Problem

- Operating IEEE 802.11b and g in the same service set may reduce the throughput of the 802.11g stations by about 50%.
- Explain!
- Not as great a problem with 802.11n mixed mode



# 802.11b/g Problem Effects

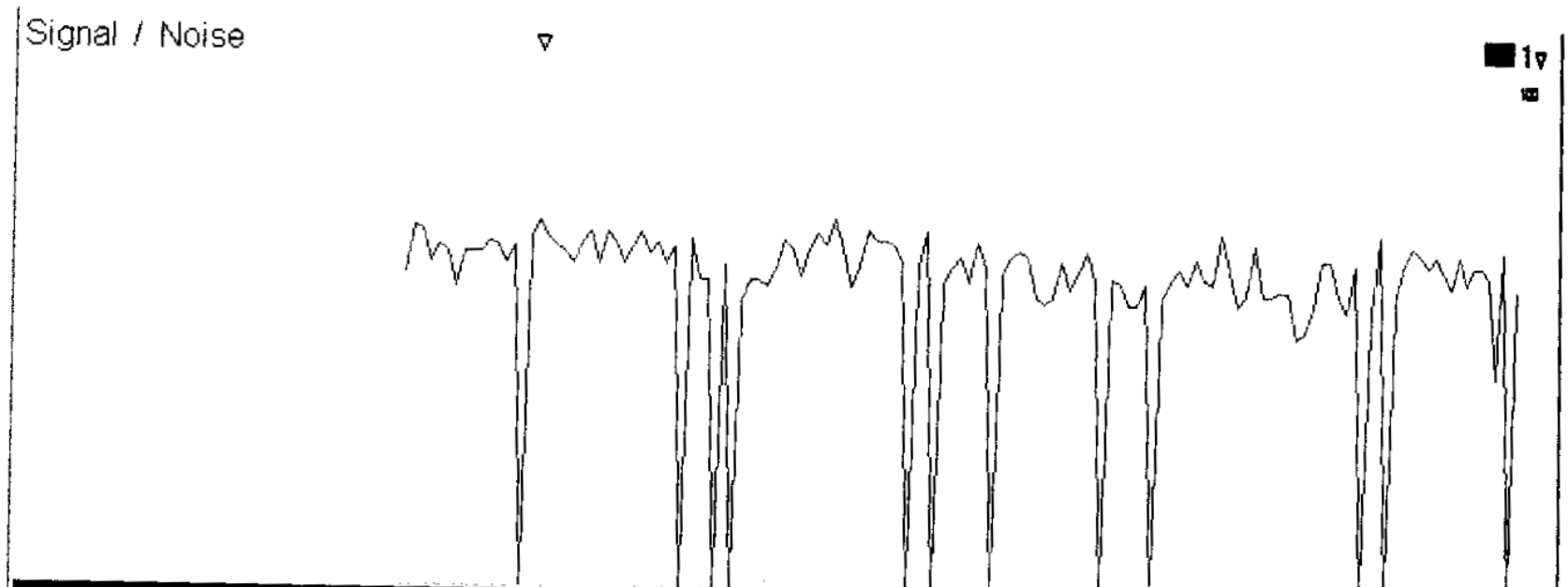


## 802.11b/g Mixed Mode Environment Throughput Scale

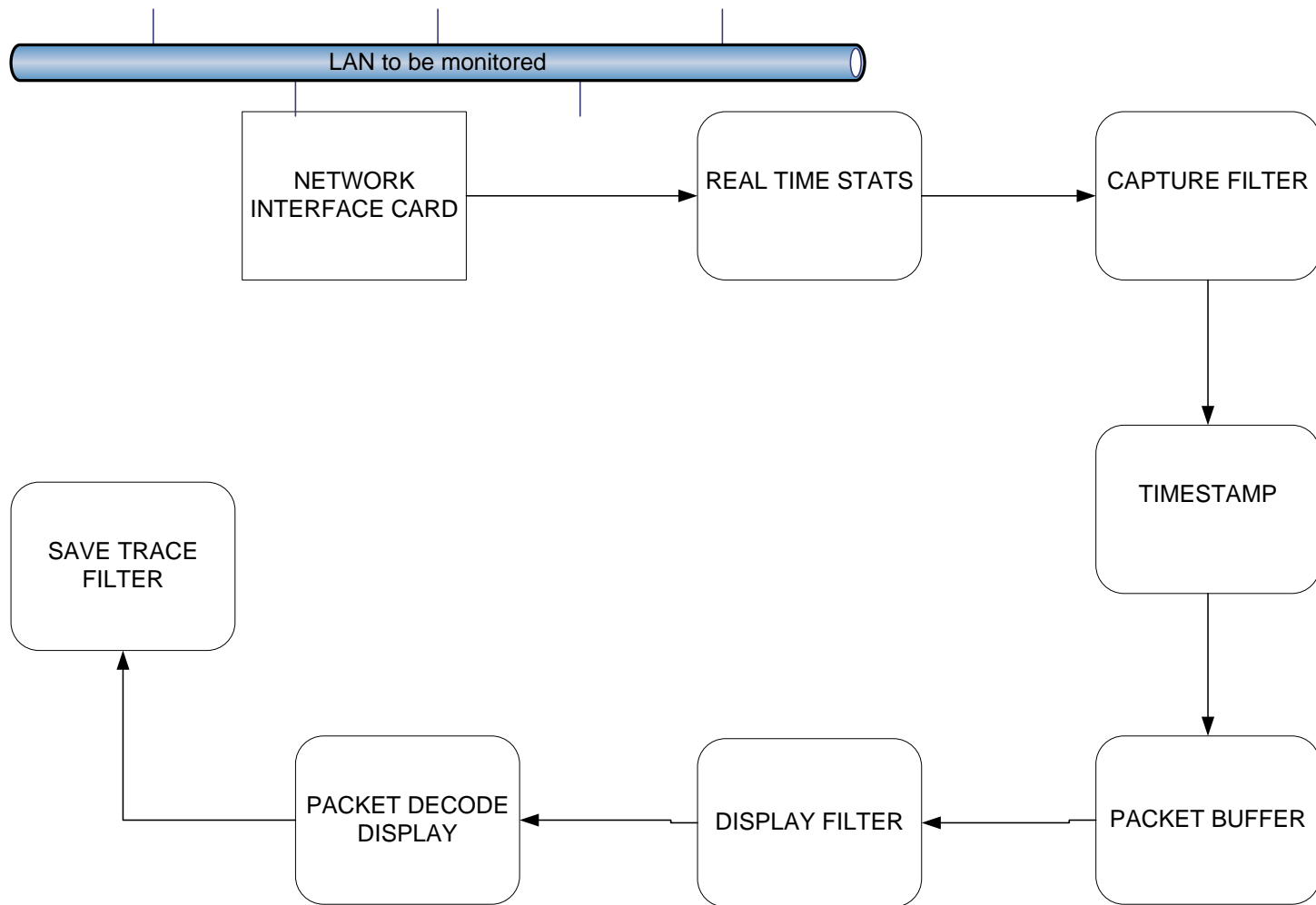
Number of 802.11b clients	10	5.9	6.2	6.5	6.8	7.0	7.2	7.4	7.6	7.8	8.0	8.2
	9	5.9	6.2	6.5	6.8	7.1	7.4	7.6	7.8	8.0	8.2	8.3
	8	5.9	6.3	6.6	6.9	7.2	7.5	7.7	8.0	8.2	8.4	8.5
	7	5.9	6.3	6.7	7.1	7.4	7.7	7.9	8.2	8.4	8.6	8.8
	6	5.9	6.4	6.8	7.2	7.6	7.9	8.2	8.4	8.7	8.9	9.1
	5	5.9	6.5	7.0	7.4	7.8	8.2	8.5	8.7	9.0	9.2	9.4
	4	5.9	6.6	7.2	7.7	8.2	8.5	8.9	9.2	9.4	9.6	9.8
	3	5.9	6.8	7.6	8.2	8.7	9.1	9.4	9.7	9.9	10.2	10.4
	2	5.9	7.2	8.2	8.9	9.4	9.8	10.2	10.4	10.7	10.9	11.1
	1	5.9	8.2	9.4	10.2	10.7	11.1	11.3	11.6	11.7	11.9	12.0
	0	0.0	22.1	22.1	22.1	22.1	22.1	22.1	22.1	22.1	22.1	22.1
	0	1	2	3	4	5	6	7	8	9	10	
Number of 802.11g clients												

# Radio Failing Problem

Intermittently Failing Radio



# Protocol Analyser Operation



# Wireshark Packet Decode

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.4	Broadcast	ARP	who has 192.168.0.100? Tell
2	0.002887	192.168.0.100	192.168.0.4	ARP	192.168.0.100 is at 00:09:5b:2c:e1:20
3	0.002909	192.168.0.4	192.168.0.100	ICMP	Echo (ping) request

Frame 3 (74 bytes on wire, 74 bytes captured)

Arrival Time: Feb 5, 2006 21:02:33.375159000  
[Time delta from previous packet: 0.000022000 seconds]  
[Time since reference or first frame: 0.002909000 seconds]  
Frame Number: 3  
Packet Length: 74 bytes  
Capture Length: 74 bytes  
[Protocols in frame: eth:ip:icmp:data]

Ethernet II, Src: 192.168.0.4 (00:09:5b:c8:df:91), Dst: 192.168.0.100 (00:09:5b:2c:e1:20)  
Destination: 192.168.0.100 (00:09:5b:2c:e1:20)  
Source: 192.168.0.4 (00:09:5b:c8:df:91)  
Type: IP (0x0800)

Internet Protocol, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.100 (192.168.0.100)  
Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP: 0x00, Default: ECN: 0x00)

0000 00 3c 91 39 00 00 80 01 27 c0 a8 00 04 c0 a8 ...<.9....  
0010 00 64 08 00 f5 5b 02 00 56 00 61 62 63 64 65 66 ...d...[...v.abcdef  
0020 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ...ghijklmn opqrstuv  
0030 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Header checksum (ip.checksum), 2 bytes | P: 10 D: 10 M: 0 Drops: 0

# Observer Packet Decode

http://www.networkinstruments.com - Screen Shot - Detail - Mi...

Decode and Analysis - Local Observer / Network 1

Start Stop Clear Settings View Tools

Packets: 510 First: 1 Last: 510 Selected: 120 Offset: 0

Pkt	Source	Destination	Size	Date	Day Time	Dst Time	Relative T
117	00:03:93:88:91:52	09:00:07:FF:FF:FF	64	Oct 31, 2003	15h:10m 23.326 104s	0.024 272	02.899 3...
118	00:40:10:11:6C:CE	broadcast	64	Oct 31, 2003	15h:10m 23.326 762s	0.000 658	02.899 9...
119	00:40:10:11:6C:CE	broadcast	64	Oct 31, 2003	15h:10m 23.376 905s	0.050 143	02.950 1...
120	netinst.netinst.com	BClark.mshome.net	81	Oct 31, 2003	15h:10m 23.401 861s	0.024 956	02.975 0...
121	BClark.mshome.net	netinst.netinst.com	64	Oct 31, 2003	15h:10m 23.402 110s	0.000 248	02.975 3...

< >

**p120: netinst.netinst.com -> BClark.mshome.net**

**IP: 207.218.140.1 -> 207.218.148.17**

**TCP PSH ACK, [110] POP3 -> [3129]**

- Ports
  - Source port [110] POP3, Destination port [3129]
- Source Port 110
- Destination Port 3129
- Sequence number 1745507605
- Acknowledgement 4257209219
- TCP flags PSH ACK Header length: [5]\*4 bytes = 20 bytes
- Window 64213
- Checksum 0xADEA (Good)
- Urgent Pointer 0 - not significant
- TCP data length 23 (calculated from Data Offset)
- Expected Acknowledgement 1745507628 (Calculated from Sequence Number and Data Length)

**POP3: -ERR = invalid password**

- Response -ERR
- Command Separator 0x20
- Message invalid password
- Response Terminator 0x000A

0000 00 08 02 68 78 40 00 40 10 11 6C CE 08 00 45 00 ...b(@.@..11..E.  
0010 00 3F AA 65 40 00 80 06 98 8B CF DA 8C 01 CF DA .?\*@.@.1.11IU.IU  
0020 8C 11 00 6E 0C 39 68 0A 55 15 FD BF DB 83 50 18 !..n.9h.U..U!P.  
0030 FA D5 AD EA 00 00 2D 45 52 52 20 69 6E 76 61 6C .0...-ERR inval  
0040 69 64 20 70 61 73 73 77 6F 72 64 0D 0A id password..

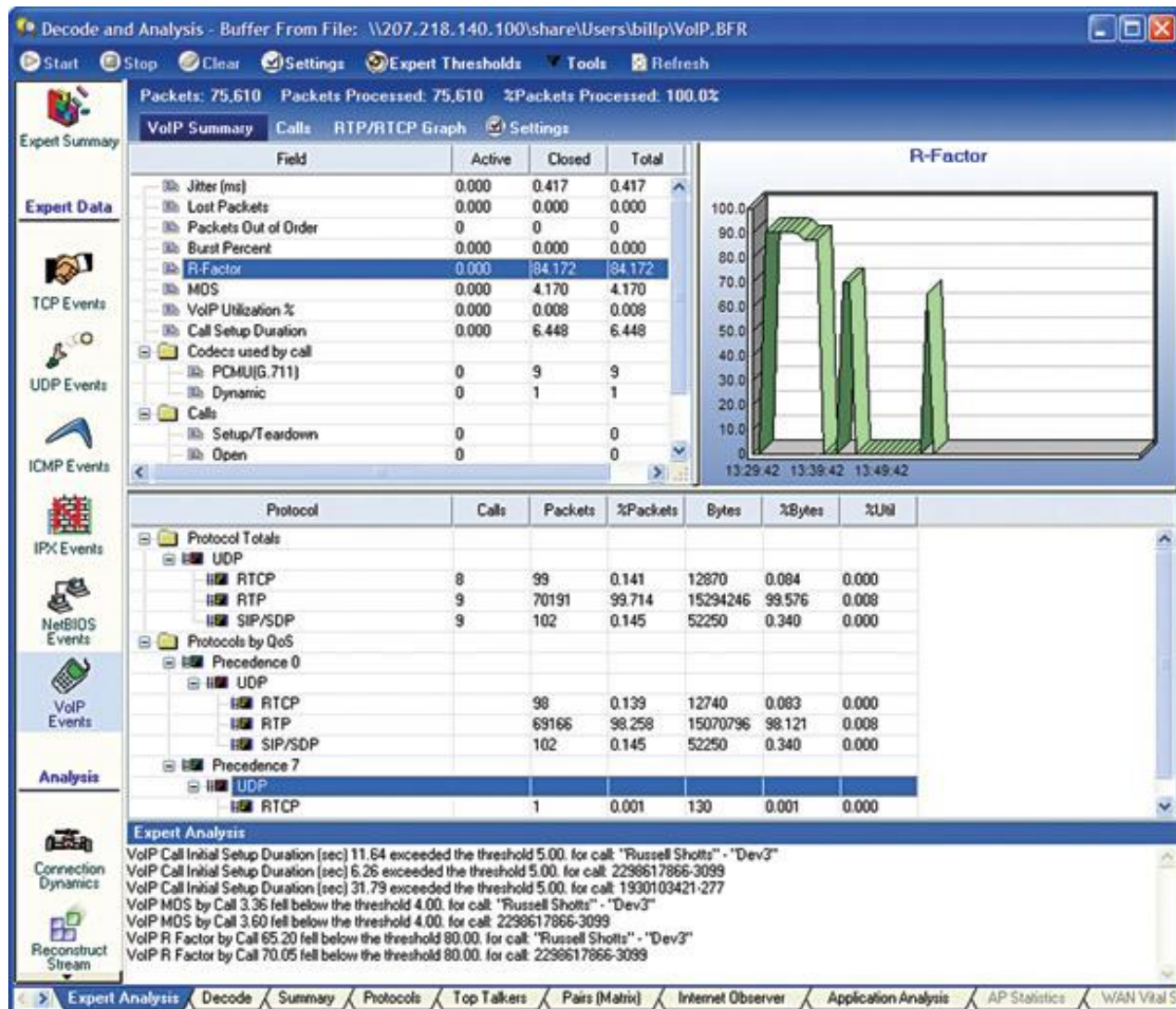
< >

Expert Analysis Decode Summary Protocols Top Talkers Pairs (Matrix) Internet Observer AP Statistics

**Packet Decode**  
Observer can decode over 500 primary protocols and countless subprotocols. Nano-second resolution provides precise analysis.

Done Internet

# Observer VoIP Expert





# OptiView

## OptiView™ Integrated Network Analyzer



# CommView for WiFi

The screenshot displays the CommView for WiFi application window. The title bar reads "CommView for WiFi - D-Link AirXp...". The menu bar includes "File", "Search", "View", "Tools", "Settings", and "Rule...". The toolbar contains icons for play, stop, refresh, folder, save, and a wireless antenna. Below the toolbar are three tabs: "Nodes" (selected), "Channels", and "Latest...".

The main window shows a list of network sessions with the following columns: "No", "Protocol", and "MAC Address".

No	Protocol	MAC Address
30824	IP/TCP	LinksysGro:60:
30825	IP/TCP	Intel:96:0C:EC
30826	IP/TCP	Intel:96:0C:EC
30827	MNGT/PROB...	AP_DLINK =>
30828	MNGT...	
30829	MNGT...	

A "TCP Session" window is open, showing a detailed view of the selected session. It has a menu bar with "File", "Edit", and "Settings". The session data is as follows:

Offset	Hex	ASCII
0x0000	00 50 54 41	GET /nwshp?gl=us&r
0x0010	00 2D 2D 2D	Accept: image/gif,
0x0020	00 2D 2D 2D	application/x-sho
0x0030	00 2D 2D 2D	

# OmniPeek

OmniPeek

File Edit View Capture Send Monitor Tools Window Help

WildPackets OmniPeek

Capture 1 History Statistics Node Statistics Protocol Statistics Summary Statistics Channel Statistics WLAN Statistics

Wireless Networks: 9 Ad Hoc Networks: 0 All Nodes  
Access Points: 8 Clients: 39

Node	Type	Channel	Frequency	Band	Encryption	Trust	Cur. Signal
0x00	ESSID	1					
00:15:63:D3:CC:E0	AP	1	2412 MHz	802.11bg	TKIP	Unknown	17
00:1D:E0:06:F8:F7	STA	1	2412 MHz	802.11bg	WEP	Unknown	15
0x0000000000	ESSID	6					
Aironet Wireless Comm:42:90:09	AP	6	2437 MHz	802.11bg	WEP	Unknown	17
00:19:30:2F:30:71	STA	6	2437 MHz	802.11bg		Unknown	10
0x000000000000	ESSID	2					
3com Europe:CF:C8:A8	AP	2	2417 MHz	802.11bg		Unknown	37
0x000000000000000000	ESSID	36					
D-link:E9:04:89	AP	36	5180 MHz	802.11a	TKIP	Unknown	31
ap2003a	ESSID	52					
Card Access:00:5F:DA	AP	52	5260 MHz	802.11a	WEP	Unknown	47
Nec Access Technica:38:03:87	STA	52	5260 MHz	802.11a		Unknown	45
CGP	ESSID	1					
00:15:63:D3:CC:E0	AP	1	2412 MHz	802.11bg	TKIP	Unknown	17
00:1D:E0:06:F8:F7	STA	1	2412 MHz	802.11bg	WEP	Unknown	15
ESSID Unknown		11					
Proxim:51:52:78	AP	11	2462 MHz	802.11bg	WEP	Unknown	15
BSSID Unknown							
Disconnected	ESSID						
@Home	ESSID						
Agere Sys:5C:B3:54	STA	1	2412 MHz	802.11bg		Unknown	25

# IEEE 802.11 Frames

- Management, Control frames and data frame headers require a frame capture card to operate in monitor mode.
- You can only analyse beacons, probes, association requests, etc. by capturing in **monitor mode**.
- Most PC based WLAN analysers have **special drivers** matched to particular network cards.

# Analysing Beacons

The image shows a Wireshark capture of a network file named 'pingtest2.cap'. The main display area shows a list of captured packets, primarily IEEE 802.11 Beacon frames. The packet list is as follows:

No.	Time	Source	Destination	Protocol	Info
61	2.906268	Netgear_f0:5b:16	Broadcast	IEEE 802	Beacon frame,
62	2.968764	Netgear_62:f3:74	Broadcast	IEEE 802	Beacon frame,
63	3.015835	Netgear_f0:5b:16	Broadcast	IEEE 802	Beacon frame,
64	3.062973	Netgear_62:f3:74	Broadcast	IEEE 802	Beacon frame,
65	3.172097	Netgear_62:f3:74	Broadcast	IEEE 802	Beacon frame,
66	3.265796	Netgear_62:f3:74	Broadcast	IEEE 802	Beacon frame,
67	3.312860	Netgear_f0:5b:16	Broadcast	IEEE 802	Beacon frame,
68	3.375361	Netgear_62:f3:74	Broadcast	IEEE 802	Beacon frame,
69	3.421916	Netgear_f0:5b:16	Broadcast	IEEE 802	Beacon frame,
70	3.469062	Netgear_62:f3:74	Broadcast	IEEE 802	Beacon frame,
71	3.531486	Netgear_f0:5b:16	Broadcast	IEEE 802	Beacon frame,
72	3.578116	Netgear_62:f3:74	Broadcast	IEEE 802	Beacon frame,
73	3.625182	Netgear_f0:5b:16	Broadcast	IEEE 802	Beacon frame,
74	3.656442	IntelCor_04:2a:c8	Broadcast	IEEE 802	QoS Data, SN=5
75	3.656444	IntelCor_04:2a:c8	IntelCor_04:2a:c8 (RA	IEEE 802	Acknowledgement
76	3.672326	IntelCor_04:2a:c8	Broadcast	IEEE 802	Data, SN=2976,
77	3.672317	Netgear_62:f3:74	IntelCor_04:2a:c8	IEEE 802	QoS Data, SN=2
78	3.672316	Netgear_62:f3:74	Netgear_62:f3:74 (RA	IEEE 802	Acknowledgement
79	3.672314	IntelCor_04:2a:c8	Broadcast	IEEE 802	QoS Data, SN=5

The packet details pane for the selected packet (Frame 1) shows the following structure:

- Frame 1 (111 bytes on wire, 111 bytes captured)
- IEEE 802.11 Beacon frame, Flags: .....
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters (12 bytes)
  - Tagged parameters (75 bytes)
    - SSID parameter set: "SKY79278"
    - Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 6.0 9.0 12.0 18.0

The packet bytes pane shows the raw data in hexadecimal and ASCII:

Offset	Hex	ASCII
0000	80 00 00 00 ff ff ff ff ff ff 00 18 4d 62 f3 74	.....Mb.t
0010	00 18 4d 62 f3 74 c0 b7 81 d5 40 7d 13 00 00 00	..Mb.t...@}...
0020	64 00 31 00 00 08 53 4b 59 37 39 32 37 38 01 08	d.1...SK Y79278..
0030	82 84 8b 96 0c 12 18 24 03 01 01 05 04 00 01 00	.....\$ .....
0040	00 2a 01 00 32 04 30 48 60 6c dd 18 00 50 f2 02	.*..2.0H \l...P..
0050	01 01 06 00 02 34 00 00 73 34 00 00 42 42 50 00	...PCA

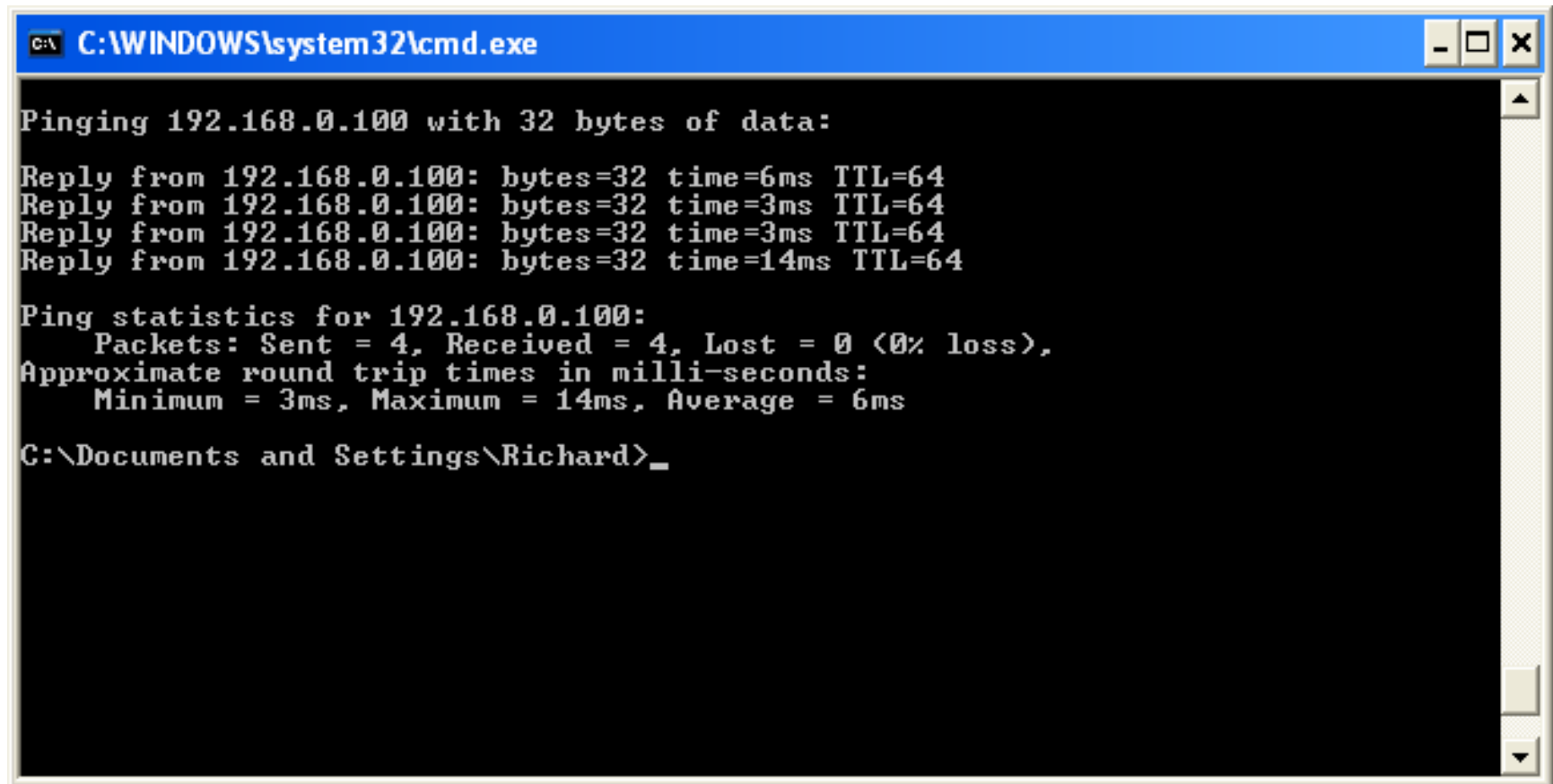
At the bottom, the status bar indicates: Frame (frame), 111 bytes | Packets: 5657 Displayed: 5657 Marked: 0 | Profile: Default

# Analysing PING with Wireshark

- Wireshark is a GUI network protocol analyser.
- It can examine data from a live network or from a capture file on disk.
- You can interactively browse the capture data, viewing summary and detail information for each packet.
- Can assemble all the packets in a TCP conversation and show you the ASCII (or EBCDIC, or hex) data in that conversation.
- Display filters are very powerful; more fields are filterable than in other protocol analysers.
- Demo capture of Ping packets on a wireless network to show pre and post filtering....also see lab sheet :

*IEEE 802.11 Wireless LAN Monitoring and Measurement*

# Command Prompt



A screenshot of a Windows Command Prompt window. The title bar is blue and contains the text "C:\WINDOWS\system32\cmd.exe" and standard window control buttons (minimize, maximize, close). The main area is black with white text. The text shows a ping command being executed against the IP address 192.168.0.100. The results show four successful replies with varying times and a TTL of 64. Below the replies, the ping statistics are displayed, showing 4 packets sent, 4 received, and 0% loss. The approximate round trip times are also shown: Minimum = 3ms, Maximum = 14ms, and Average = 6ms. The prompt ends with "C:\Documents and Settings\Richard>\_".

```
C:\WINDOWS\system32\cmd.exe

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=6ms TTL=64
Reply from 192.168.0.100: bytes=32 time=3ms TTL=64
Reply from 192.168.0.100: bytes=32 time=3ms TTL=64
Reply from 192.168.0.100: bytes=32 time=14ms TTL=64

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 14ms, Average = 6ms

C:\Documents and Settings\Richard>_
```

# Expand Details

The screenshot shows the Wireshark (Ethereal) interface with the following components:

- Filter:** Expression... Clear Apply
- Packet List:**

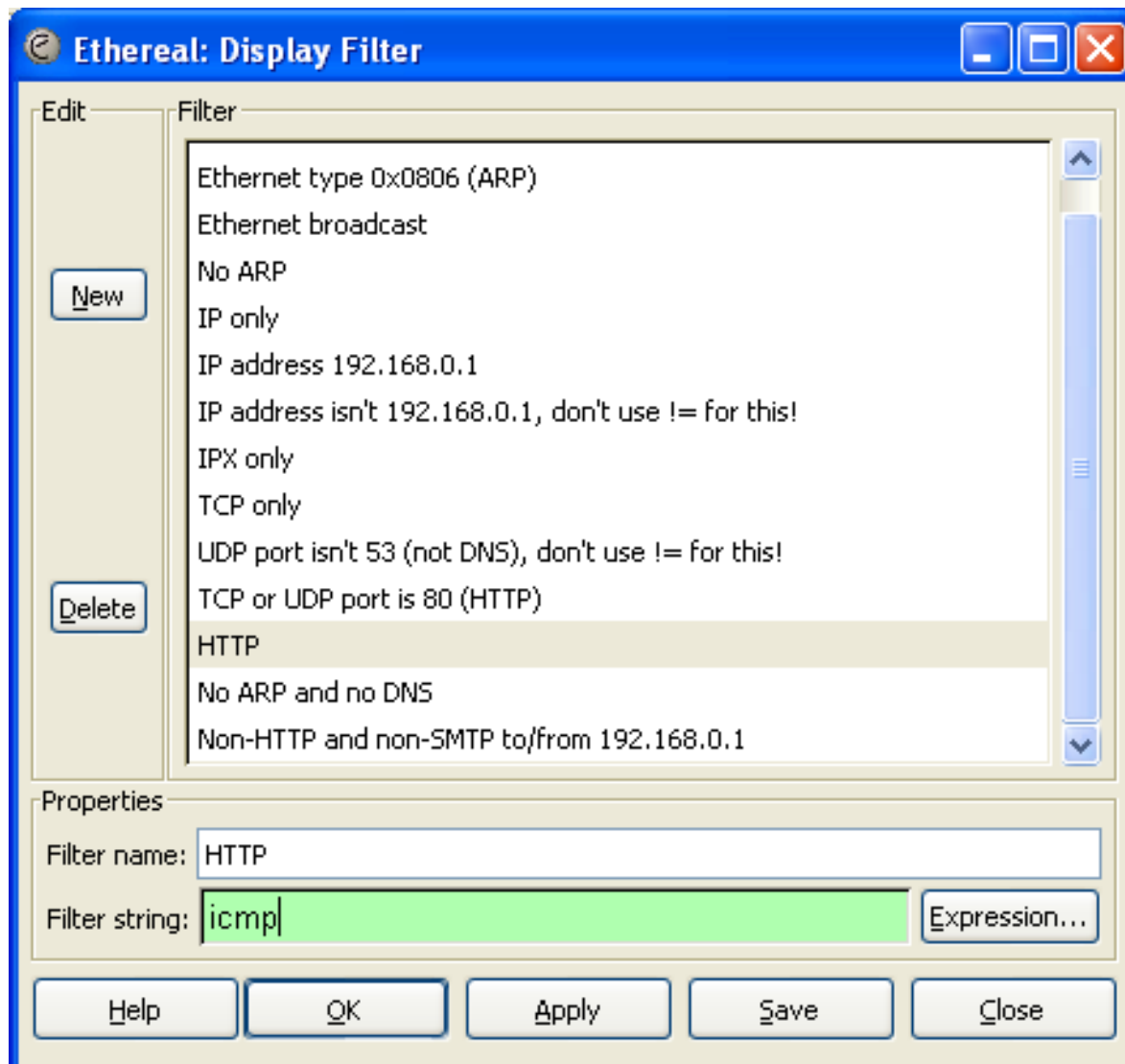
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.4	Broadcast	ARP	who has 192.168.0.100? Tell ...
2	0.002887	192.168.0.100	192.168.0.4	ARP	192.168.0.100 is at 00:09:5b:...
3	0.002909	192.168.0.4	192.168.0.100	ICMP	Echo (ping) request
- Packet Details:**
  - Frame 3 (74 bytes on wire, 74 bytes captured)
    - Arrival time: Feb 5, 2006 21:02:33.375159000
    - [Time delta from previous packet: 0.000022000 seconds]
    - [Time since reference or first frame: 0.002909000 seconds]
    - Frame Number: 3
    - Packet Length: 74 bytes
    - Capture Length: 74 bytes
    - [Protocols in frame: eth:ip:icmp:data]
  - Ethernet II, Src: 192.168.0.4 (00:09:5b:c8:df:91), Dst: 192.168.0.100 (00:09:5b:2c:e1:20)
    - Destination: 192.168.0.100 (00:09:5b:2c:e1:20)
    - Source: 192.168.0.4 (00:09:5b:c8:df:91)
    - Type: IP (0x0800)
  - Internet Protocol, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.100 (192.168.0.100)
    - Version: 4
    - Header length: 20 bytes
    - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
- Packet Bytes:**

Offset	Hex	ASCII
0010	00 3c 91 39 00 00 80 01 27 c1 c0 a8 00 04 c0 a8	...<.9... ..
0020	00 64 08 00 f5 5b 02 00 56 00 61 62 63 64 65 66	.d...[.. V.abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

Header checksum (ip.checksum), 2 bytes | P: 10 D: 10 M: 0 Drops: 0



# Apply Display Filters



# Display Filter Result

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: icmp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
3	0.002909	192.168.0.4	192.168.0.100	ICMP	Echo (ping) request
4	0.006625	192.168.0.100	192.168.0.4	ICMP	Echo (ping) reply
5	1.004295	192.168.0.4	192.168.0.100	ICMP	Echo (ping) request
6	1.007426	192.168.0.100	192.168.0.4	ICMP	Echo (ping) reply
7	2.005760	192.168.0.4	192.168.0.100	ICMP	Echo (ping) request
8	2.008928	192.168.0.100	192.168.0.4	ICMP	Echo (ping) reply
9	3.007197	192.168.0.4	192.168.0.100	ICMP	Echo (ping) request
10	3.021314	192.168.0.100	192.168.0.4	ICMP	Echo (ping) reply

Internet Protocol, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.100 (192.168.0.100)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0xf55b [correct]  
Identifier: 0x0200  
Sequence number: 0x5600  
Data (32 bytes)

0010 00 3c 91 39 00 00 80 01 27 cf c0 a8 00 04 c0 a8 .<.9....  
0020 00 64 08 00 f5 5b 02 00 56 00 61 62 63 64 65 66 .d...[. v.abcdef  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv  
0040 77 61 62 63 64 65 66 67 68 69 wabcdfgh i

Internet Control Message Protocol (icmp), 40 bytes P: 10 D: 8 M: 0 Drops: 0

# Packet Capture Filters

- Are **one of the most important features** of WLAN analysers because of the overwhelming amount of traffic.
- Most analysers have a comprehensive filter set covering protocols, frame types and addresses.
- A common wireless filter is 'no beacons' to get rid of the many beacon frames produced by APs.

# Types of Filtering

- Live capture or Pre filter –  
only frames accepted by filter will be captured.
- Display or Post capture –  
filter is applied to previously captured buffer or file and only frames accepted by the filter will be displayed.

# Types of Filter

- Can be inclusive or exclusive
- Reject Matching => frames matching the filter will be rejected
- Accept matching => frames matching will be accepted

# Observer and Wireshark Filters

- Can filter on layers 2 -7 of OSI and wireless filters are only one of many options in these analysers.
- Observer has a large set of pre-configured filters that can be customised using a flow chart analogy.
- Wireshark wireless display filters are constructed using character strings.

# Sample Observer Filters

- MAC address
- BSSID
- SSID
- MAC and exclude broadcast
- Invert filter to exclude beacons
- All data traffic
- Ping packets
- EAPoL packets
- Unencrypted data traffic

### Representing Wireless Frame Types

When assessing a wireless packet capture with Wireshark, it is common to apply display filters to look for or exclude certain frames based on the IEEE 802.11 frame type and frame subtype fields. If you are trying to exclude frames from a capture, it is easy to identify the Type and Subtype fields by navigating the Packet Details window and using the values for your filter. If you are looking for a specific frame type, however, you have to remember either the Frame Type and Subtype values, or the Combined Type/Subtype value assigned by Wireshark.

Instead of expecting you to memorize the 35+ values for different frame types, we've included them here for easy reference.

Frame Type/Subtype	Filter
Management Frames	<i>wlan.fc.type eq 0</i>
Control Frames	<i>wlan.fc.type eq 1</i>
Data Frames	<i>wlan.fc.type eq 2</i>
Association Request	<i>wlan.fc.type_subtype eq 0</i>
Association response	<i>wlan.fc.type_subtype eq 1</i>
Reassociation Request	<i>wlan.fc.type_subtype eq 2</i>
Reassociation Response	<i>wlan.fc.type_subtype eq 3</i>
Probe Request	<i>wlan.fc.type_subtype eq 4</i>
Probe Response	<i>wlan.fc.type_subtype eq 5</i>
Beacon	<i>wlan.fc.type_subtype eq 8</i>
Announcement Traffic Indication Map (ATIM)	<i>wlan.fc.type_subtype eq 9</i>
Disassociate	<i>wlan.fc.type_subtype eq 10</i>
Authentication	<i>wlan.fc.type_subtype eq 11</i>
Deauthentication	<i>wlan.fc.type_subtype eq 12</i>
Action Frames	<i>wlan.fc.type_subtype eq 13</i>
Block Acknowledgement (ACK) Request	<i>wlan.fc.type_subtype eq 24</i>
Block ACK	<i>wlan.fc.type_subtype eq 25</i>
Power-Save Poll	<i>wlan.fc.type_subtype eq 26</i>
Request to Send	<i>wlan.fc.type_subtype eq 27</i>



# More Wireshark Filters

Frame Type/Subtype	Filter
Clear to Send	<i>wlan.fc.type_subtype eq 28</i>
ACK	<i>wlan.fc.type_subtype eq 29</i>
Contention Free Period End	<i>wlan.fc.type_subtype eq 30</i>
Contention Free Period End ACK	<i>wlan.fc.type_subtype eq 31</i>
Data + Contention Free ACK	<i>wlan.fc.type_subtype eq 33</i>
Data + Contention Free Poll	<i>wlan.fc.type_subtype eq 34</i>
Data + Contention Free ACK + Contention Free Poll	<i>wlan.fc.type_subtype eq 35</i>
NULL Data	<i>wlan.fc.type_subtype eq 36</i>
NULL Data + Contention Free ACK	<i>wlan.fc.type_subtype eq 37</i>
NULL Data + Contention Free Poll	<i>wlan.fc.type_subtype eq 38</i>
NULL Data + Contention Free ACK + Contention Free Poll	<i>wlan.fc.type_subtype eq 39</i>
QoS Data	<i>wlan.fc.type_subtype eq 40</i>
QoS Data + Contention Free ACK	<i>wlan.fc.type_subtype eq 41</i>
QoS Data + Contention Free Poll	<i>wlan.fc.type_subtype eq 42</i>
QoS Data + Contention Free ACK + Contention Free Poll	<i>wlan.fc.type_subtype eq 43</i>
NULL QoS Data	<i>wlan.fc.type_subtype eq 44</i>
NULL QoS Data + Contention Free Poll	<i>wlan.fc.type_subtype eq 46</i>
NULL QoS Data + Contention Free ACK + Contention Free Poll	<i>wlan.fc.type_subtype eq 47</i>

# Sample Wireshark Filters

- MAC address
- BSSID
- SSID
- Mac and exclude broadcast
- Invert filter to exclude beacons
- All data traffic
- Ping packets
- EAPoL packets
- Unencrypted data traffic

# Display Filter Strings

- wlan.sa eq 00:09:5b:e8:c4:03
- wlan.bssid eq 00:11:92:6e:cf:00
- wlan\_mgt.tag.interpretation eq "netlab"
- wlan.sa eq 00:09:5b:e8:c4:03 and wlan.bssid ne ff:ff:ff:ff:ff:ff
- !(wlan.fc.type eq 0 and wlan.fc.subtype eq 8)
- icmp
- eapol
- wlan.fc.type eq 2
- wlan.fc.protected ne 1

# WLAN Management Problems

- Power to APs
- Default AP settings
- Rogue APs
- Unmanaged clients (anonymous access)
- Viruses, worms and trojans
- Personal devices: Laptops, tablets and smartphones
- Man in the Middle attacks
- DoS attacks

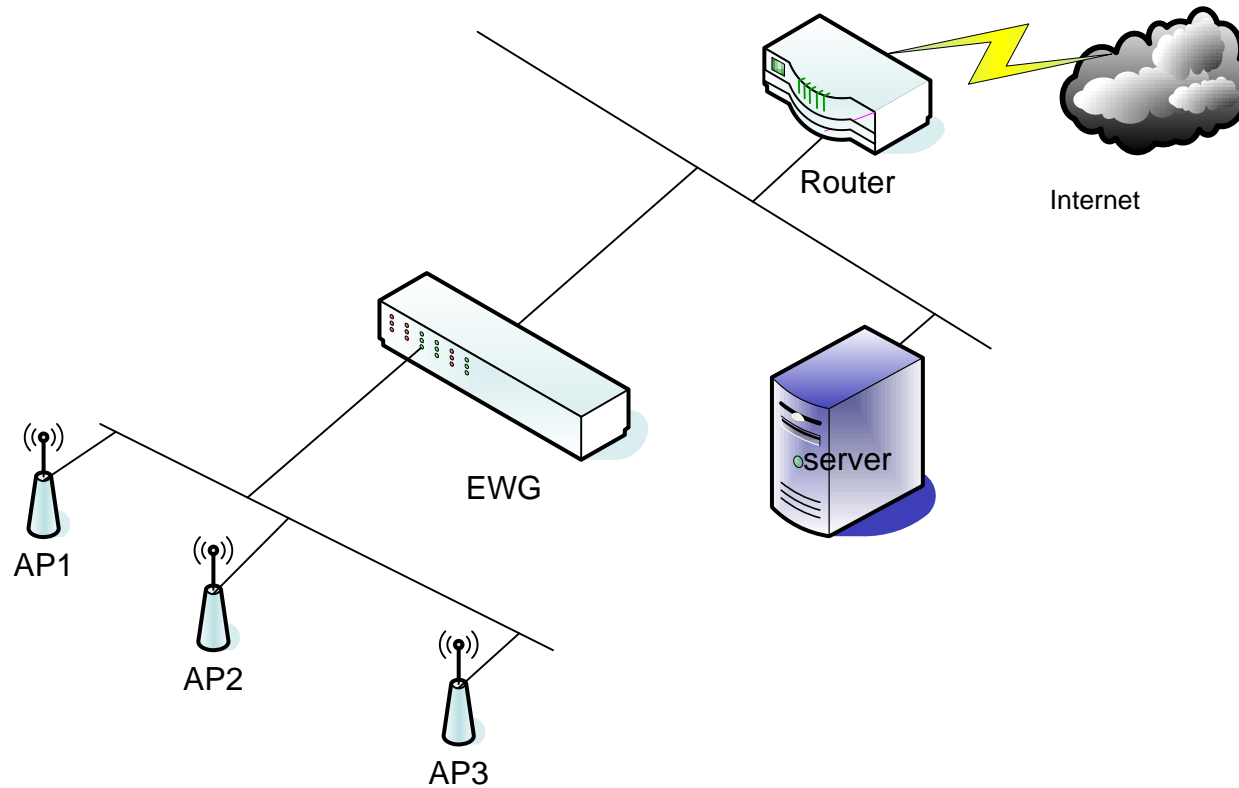
# Enterprise solutions

- VPN
- VLAN
- EWG
- EEG
- WLAN Switches

# Enterprise Wireless Gateway

- Device that can provide special authentication and connectivity for wireless and wired clients
- Combines switch, router, VPN and authentication server functionality
- Sits between the wireless and wired network infrastructures.

# EWG example

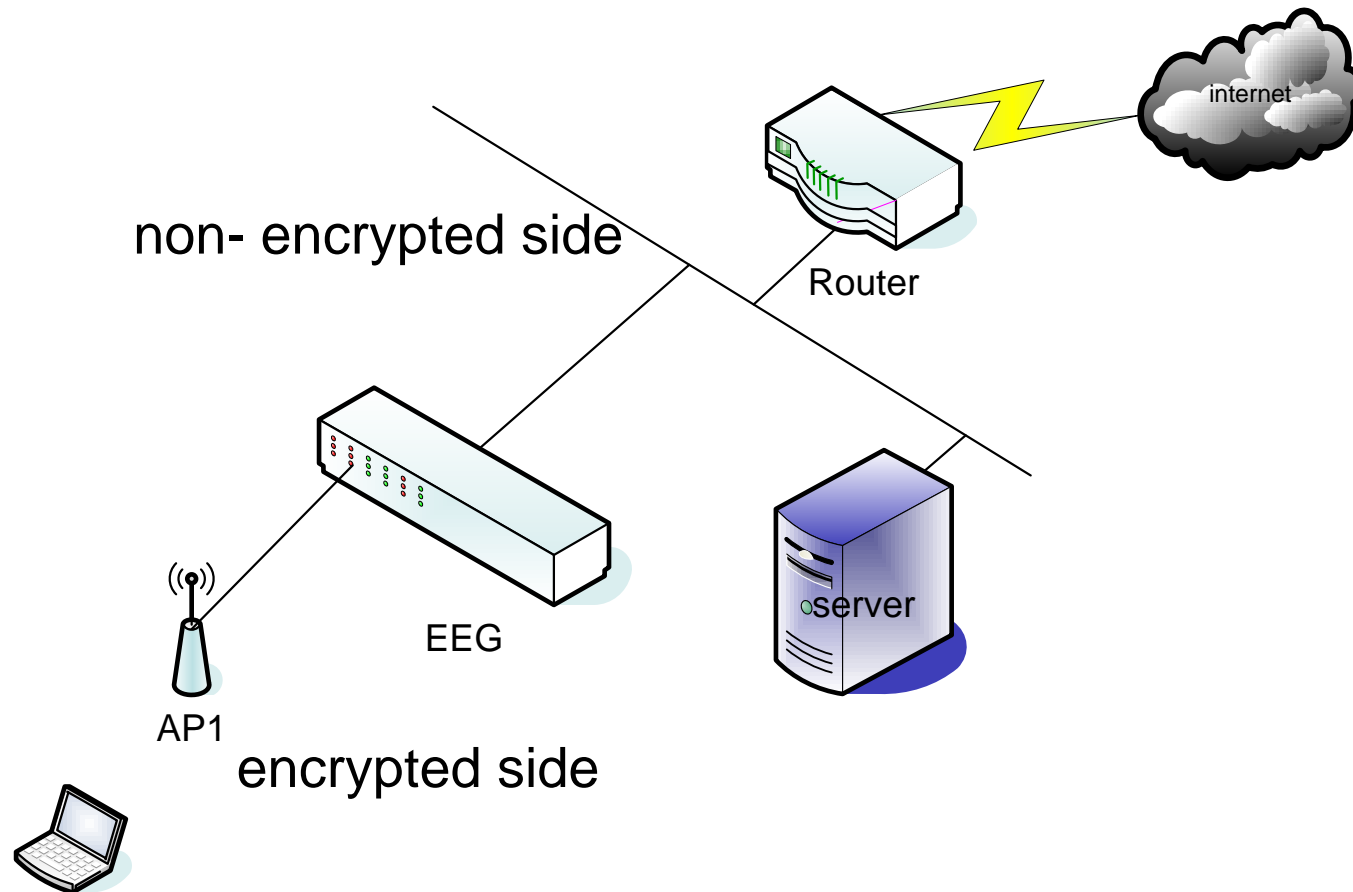


# Enterprise Encryption Gateways

- EEGs are L2 devices similar to VPNs
- Allow for strong authentication and encryption
- Clients have encryption software to use EEG as endpoint rather than AP
- This offloads the encryption duties from AP
- EEG devices have an encrypted and unencrypted side.



# EEG example

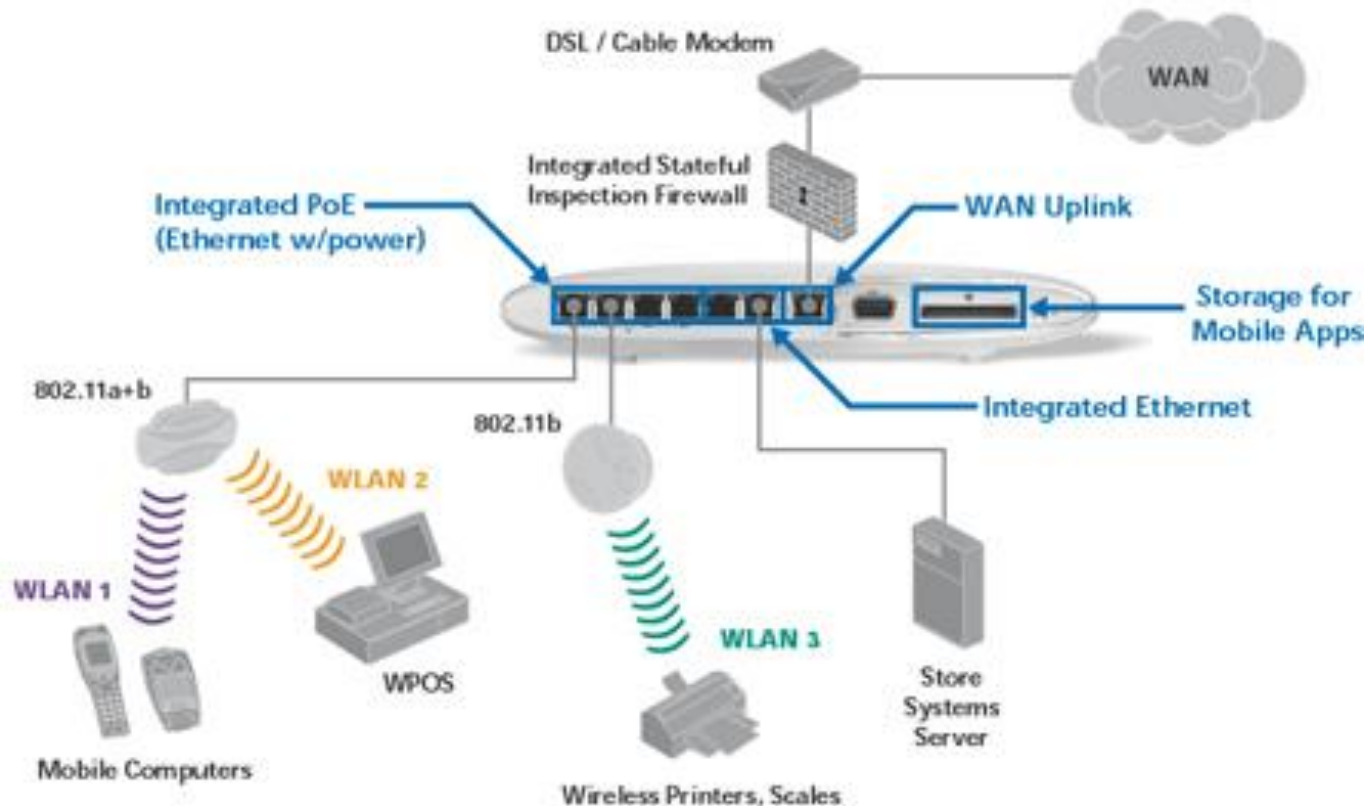


# WLAN Switch

- WLAN switches are like EWGs with additional features.
- For large enterprise installations it becomes difficult to manage/configure large numbers of APs and Roaming also becomes a problem.
- Some vendors (e.g. trapeze) have moved AP functionality into a management device known as a WLAN switch.

# WLAN Switch

Integrated Wired-Wireless Networking:  
WS 2000 in a Retail Wireless Store



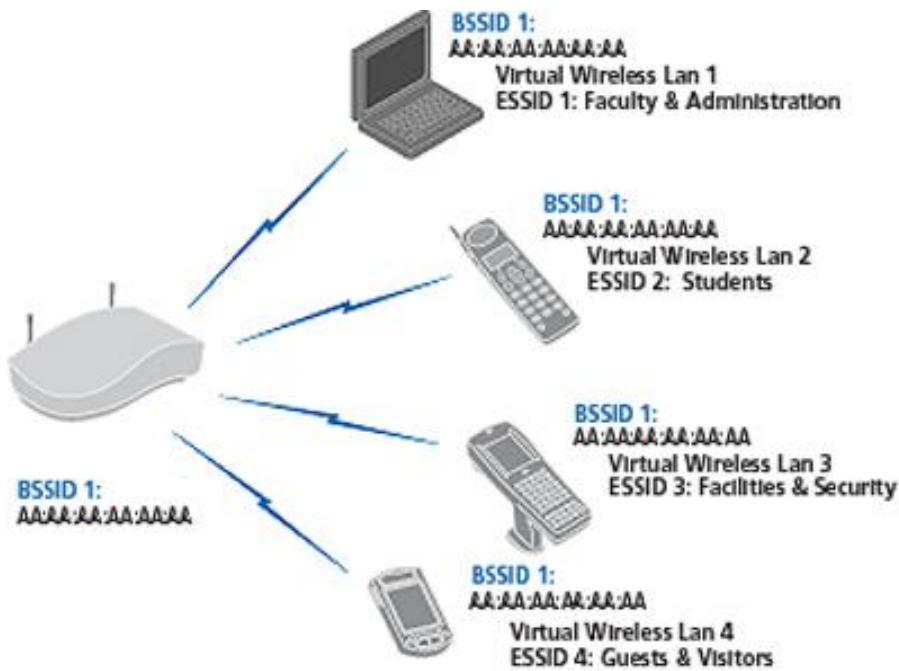
# WLAN Switch

- Used for management and security control of larger installations from a central point.
- Different policies can be assigned for each wired segment.
- WLAN switches have the functionality of several APs (logical devices).
- Most employ Thin APs (virtual APs).
- Also called access ports or mobility ports.

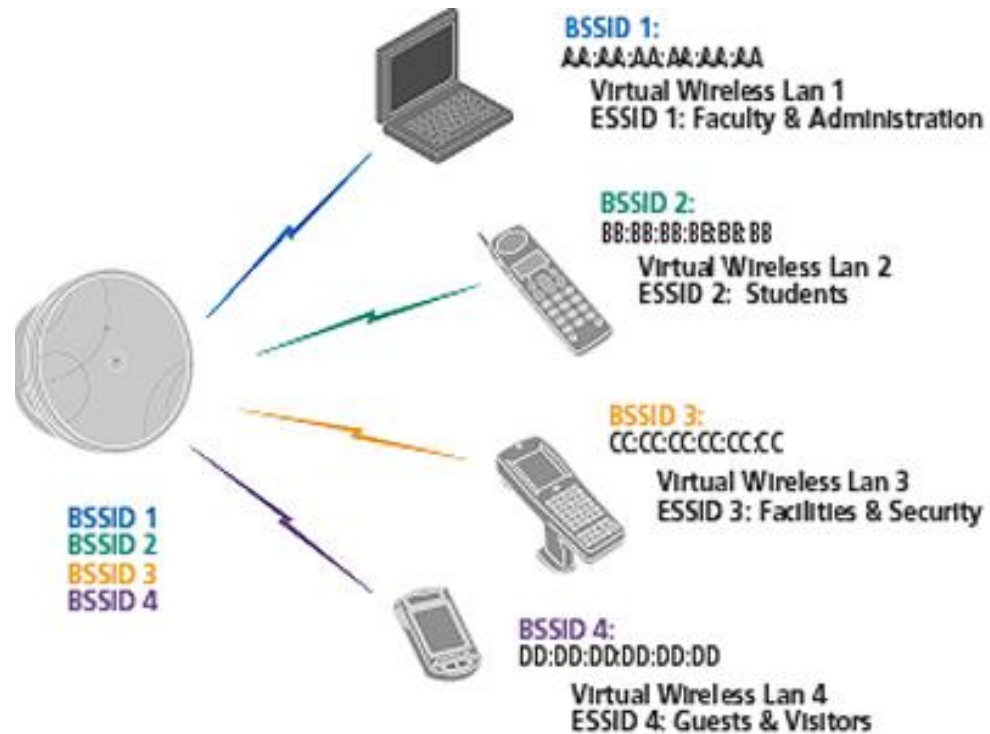
# Thin APs

- vary in implementation
- some are just antennas
- others have full function radios
- connect to WLAN switch via cat5 cable from POE switch ports
- communicate via Ethernet or 802.11 over wire or VPN tunnel

# WLAN Switch 2



Before



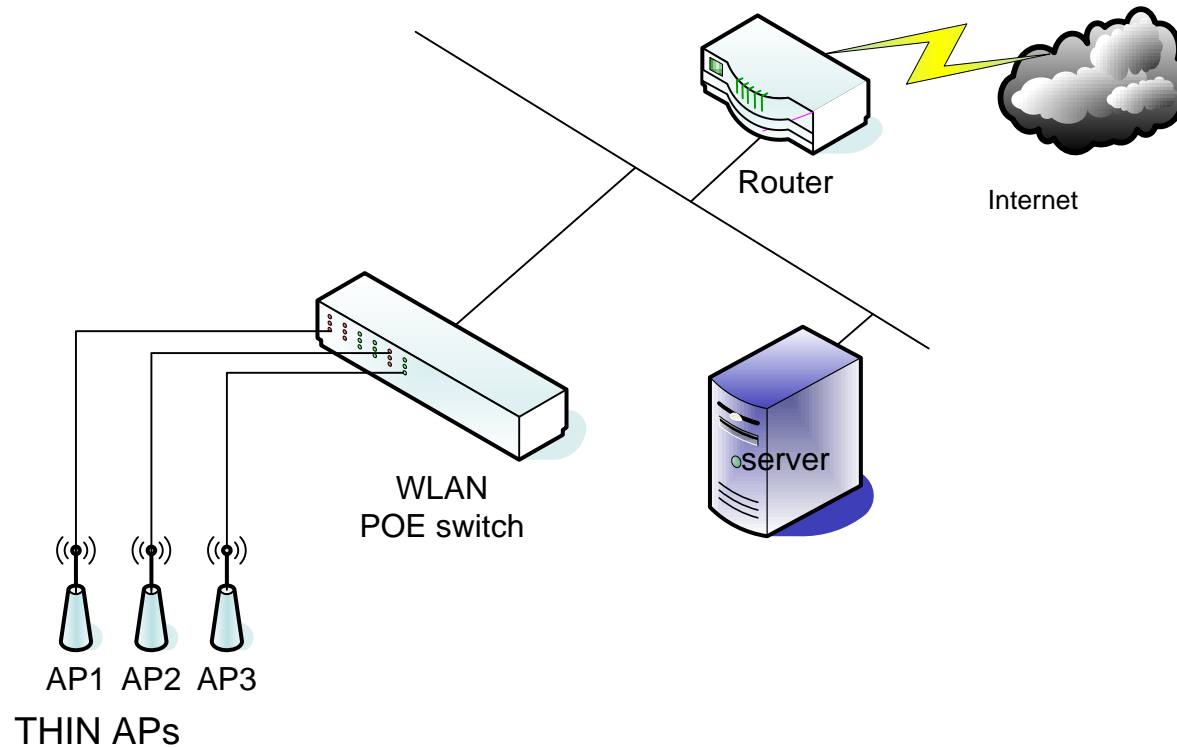
After

Can have *different* policies for each wired segment

# Edge or Core WLAN switch

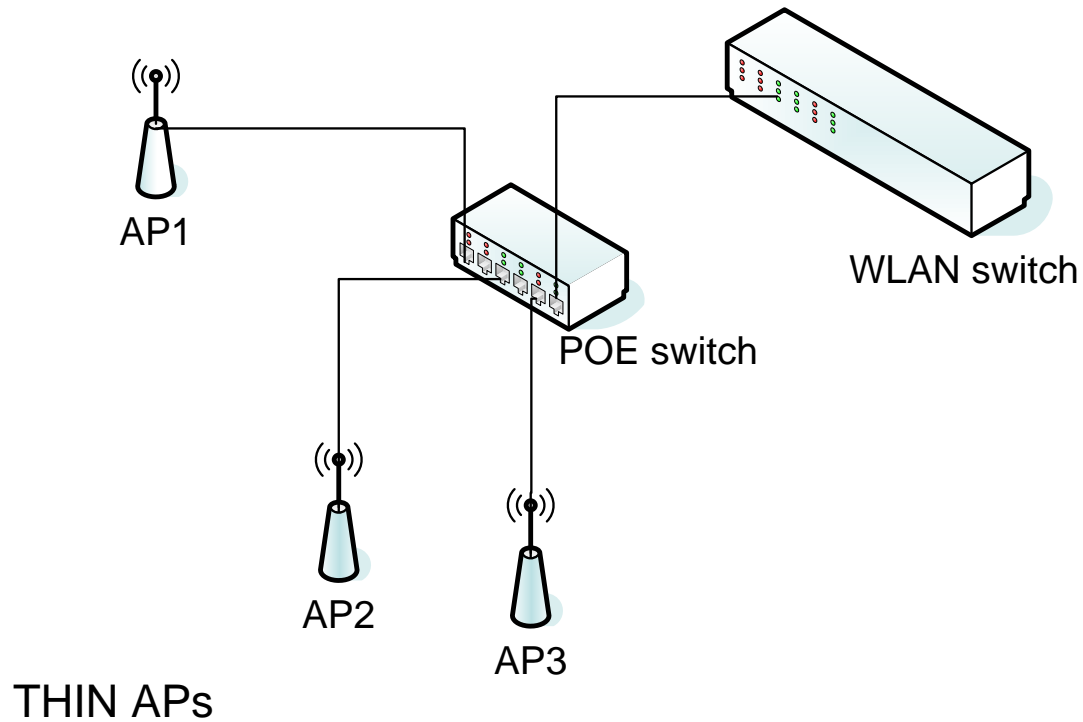
- Early WLAN switches were edge devices directly connected to the APs via POE.
- It is now more sensible to connect them to the core for easier management.
- Large WLAN networks have the WLAN switch at the centre and then connect to POE switches at the edge.

# Edge WLAN Switch





# Core WLAN switch



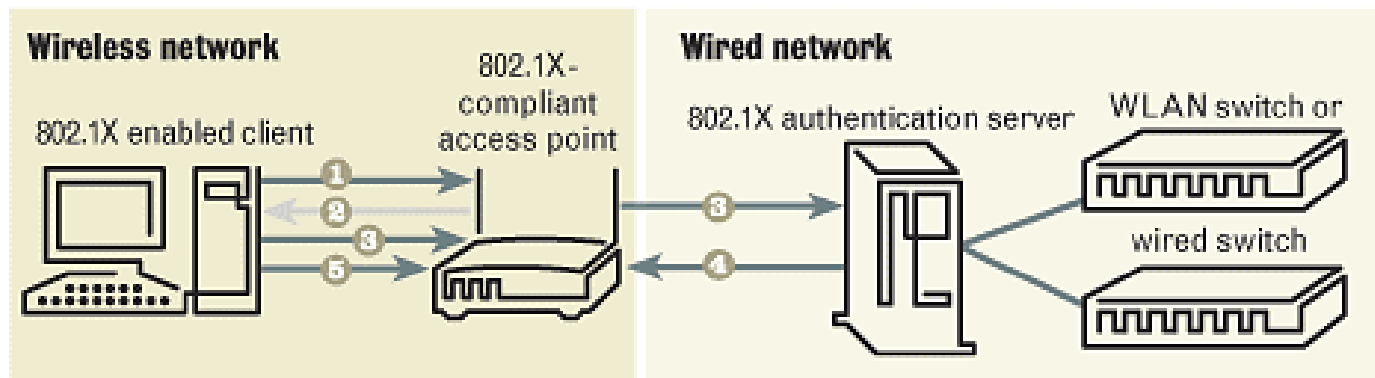
# Managed Access

- Corporate APs **do not allow anonymous** (unmanaged access).
- user or computer authentication or both are required for high security access via IEEE **802.1x EAP** methods.
- **RADIUS servers or EWG** devices control and monitor access.

# IEEE 802.1x Framework

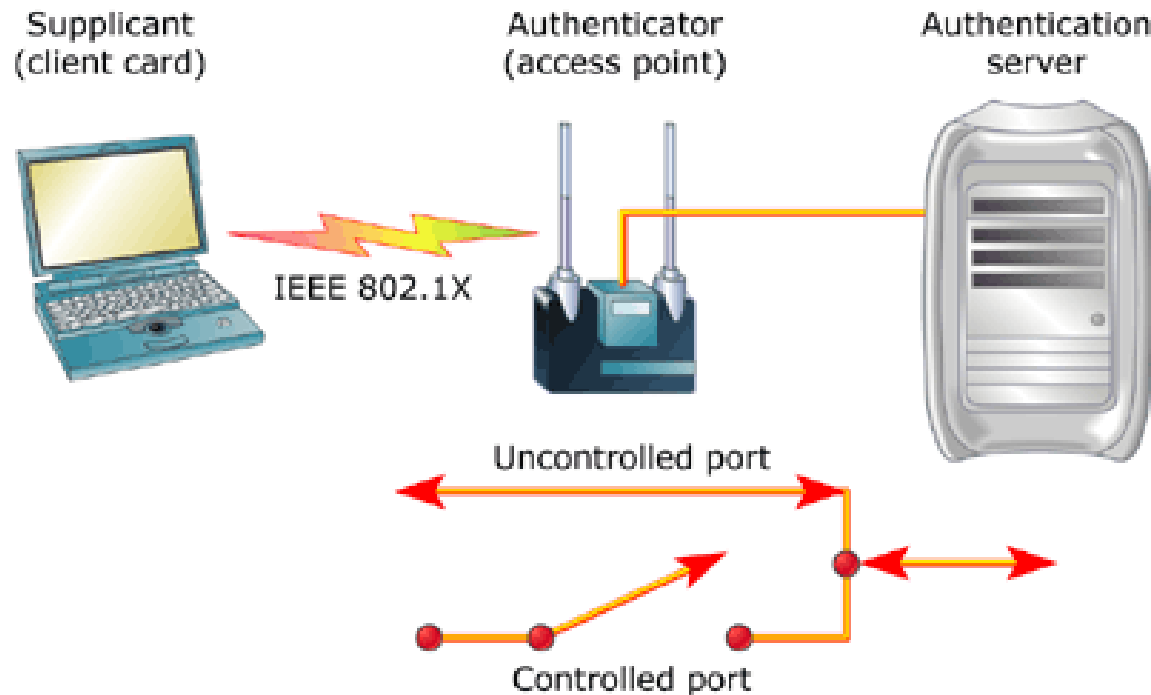
## The 802.1X framework

Under 802.1X, users can choose from a variety of authentication methods and encryption schemes.



- 1 Client asks access point for permission to send data over WLAN network.
- 2 Access point asks client to verify its identity.
- 3 Client sends identity information to authentication server. Identity information is encrypted using either WEP, WPA or 802.11i encryption methods.
- 4 Authentication server verifies client. Authentication mechanism under 802.1X framework can be EAP, LEAP, EAP-TTLS, Kerberos, pre-shared token, etc.
- 5 Client sends data to access point.

# IEEE 802.1x Use in IEEE 802.11i



- *IEEE 802.1X provides a framework to authenticate and authorize devices connecting to a network. It prohibits access to the network until such devices pass authentication.*
- *It also provides a framework to transmit key information between authenticator and supplicant.*

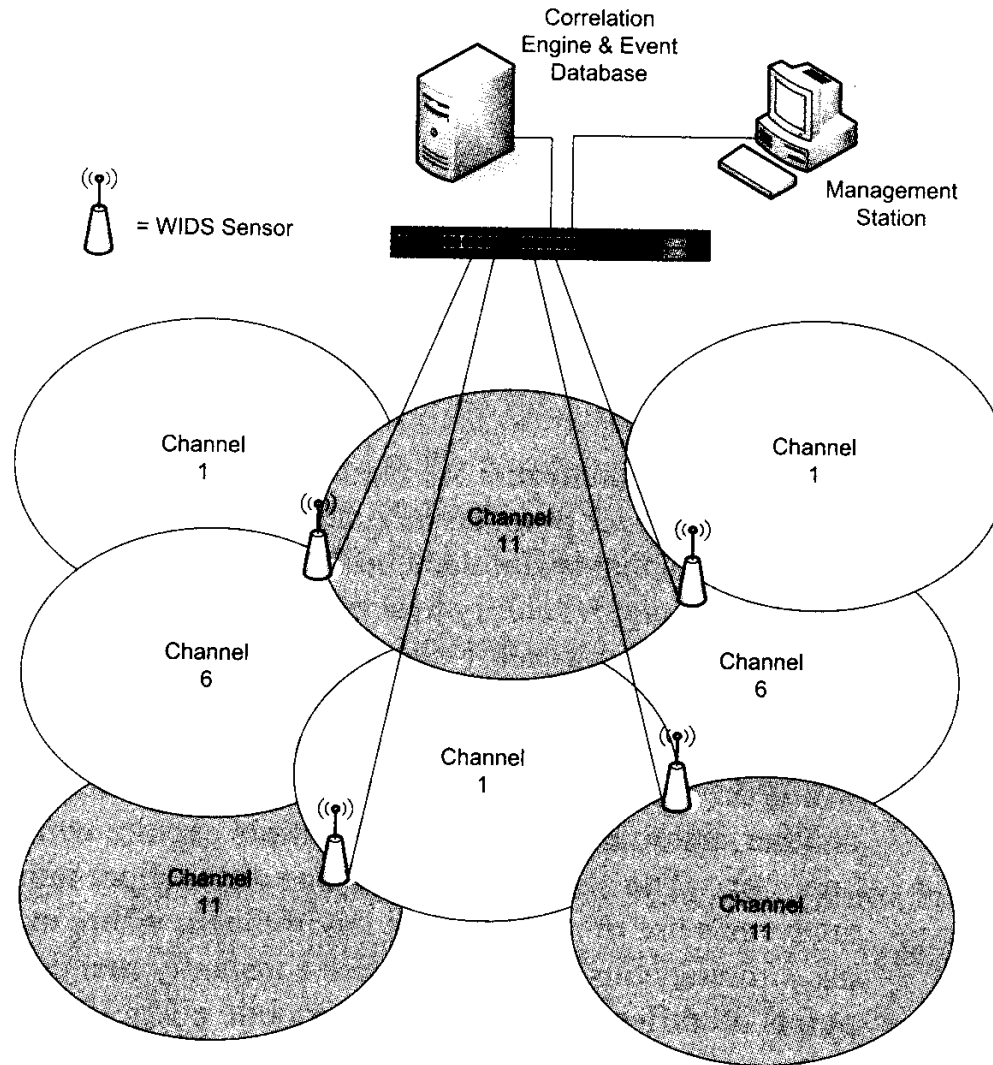
# Rogue APs

- Rogue (or unauthorized) access points are a **constant threat** to organisations.
- They allow **anonymous access**
- Employees are creating WLANs using rogue APs to connect personal devices to network.
- These rogue access points **create security breaches** that put the entire network at risk.
- The network is open to man-in-the-middle (MITM) attacks.

# Rogue AP Detection

- Some commercial grade APs include **rogue AP detection features** and try to shut them down.
- Wireless Intrusion Detection System (**WIDS**) appliances are now available to monitor the WLAN and detect rogue APs and unauthorised clients and well known exploits.
- Detectors dotted around a site can detect rogue APs and locate and quarantine them.

# WIDS



# Self-Study Resources

- How MIMO Cuts Data Transmission in Half  
<https://www.youtube.com/watch?v=gZbDS-qEmjo>
- Wireshark Packet Sniffing Usernames, Passwords, and Web Pages  
[https://www.youtube.com/watch?v=r0l\\_54thSYU](https://www.youtube.com/watch?v=r0l_54thSYU)
- Mobile Device Security Troubleshooting  
<https://www.youtube.com/watch?v=wp733UX-1ek>
- Troubleshooting Networks  
<https://www.youtube.com/watch?v=gPiid3NyN6U>
- Network Troubleshooting Tools  
<https://www.youtube.com/watch?v=5GbpYsoyUYg>
- Troubleshooting Wireless Configurations  
<https://www.youtube.com/watch?v=PLUQH0eseUw>
- EAP, LEAP, and PEAP  
<https://www.youtube.com/watch?v=1boAQhNJfso>