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

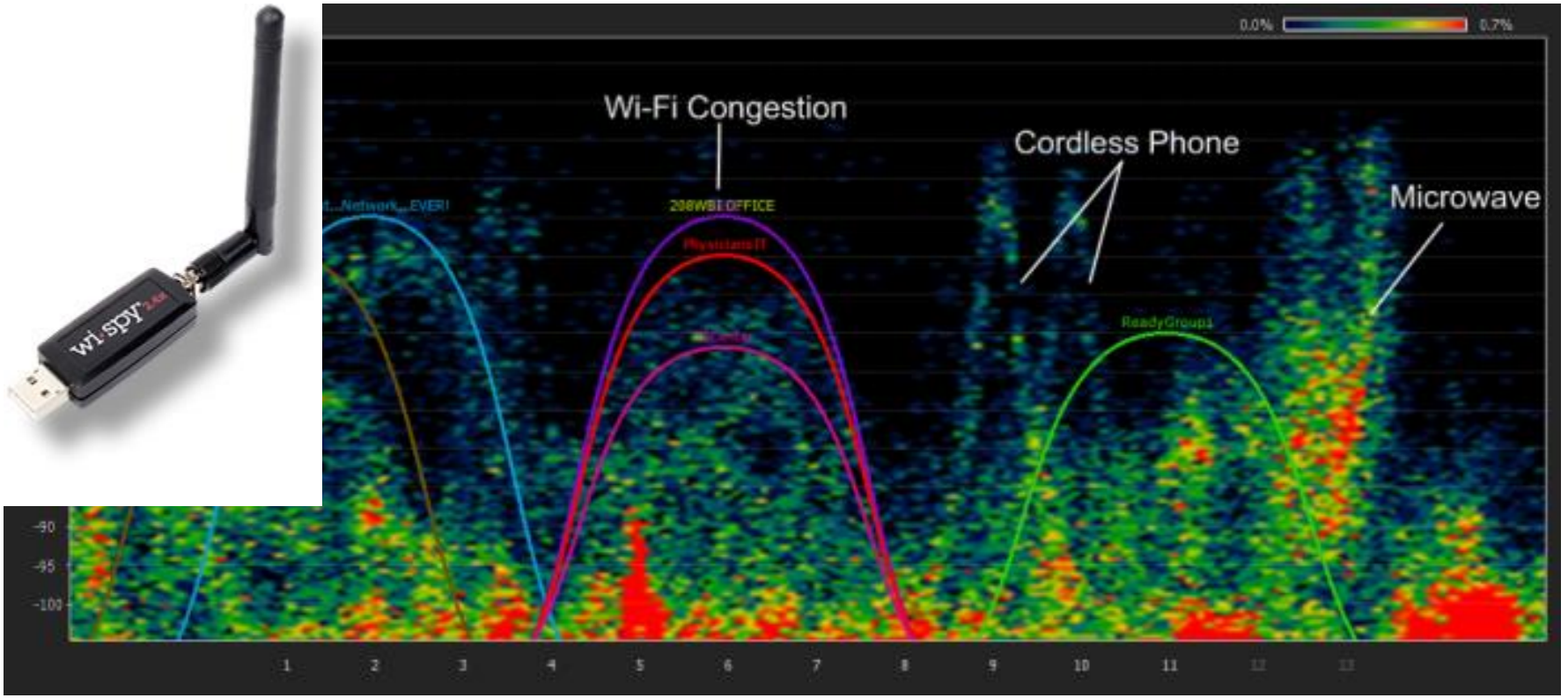
Problems and Limitations

- 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

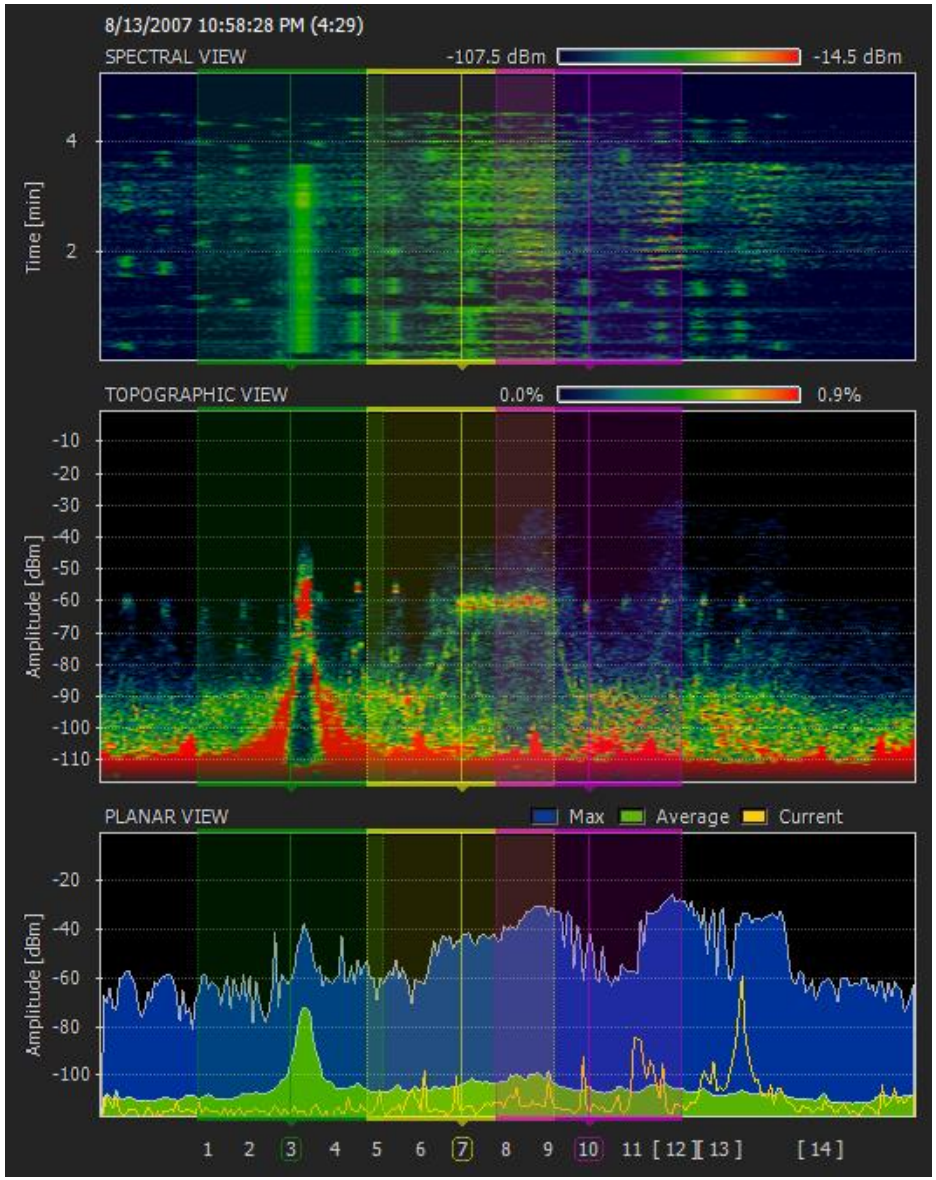
WiSpy – Wi-Fi Spectrum Analyser



See you-tube video tour

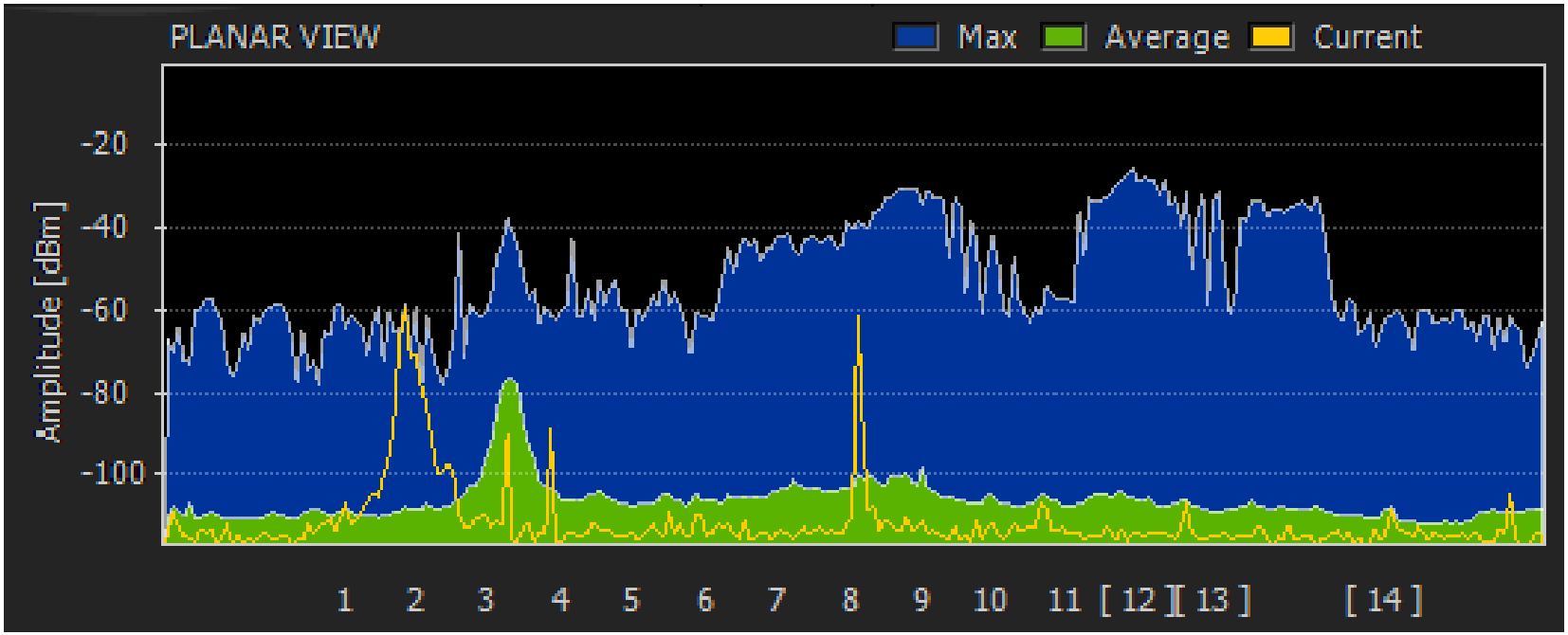
http://www.metageek.net/products/wi-spy-24x

WiSpy Chanalyser Package Views



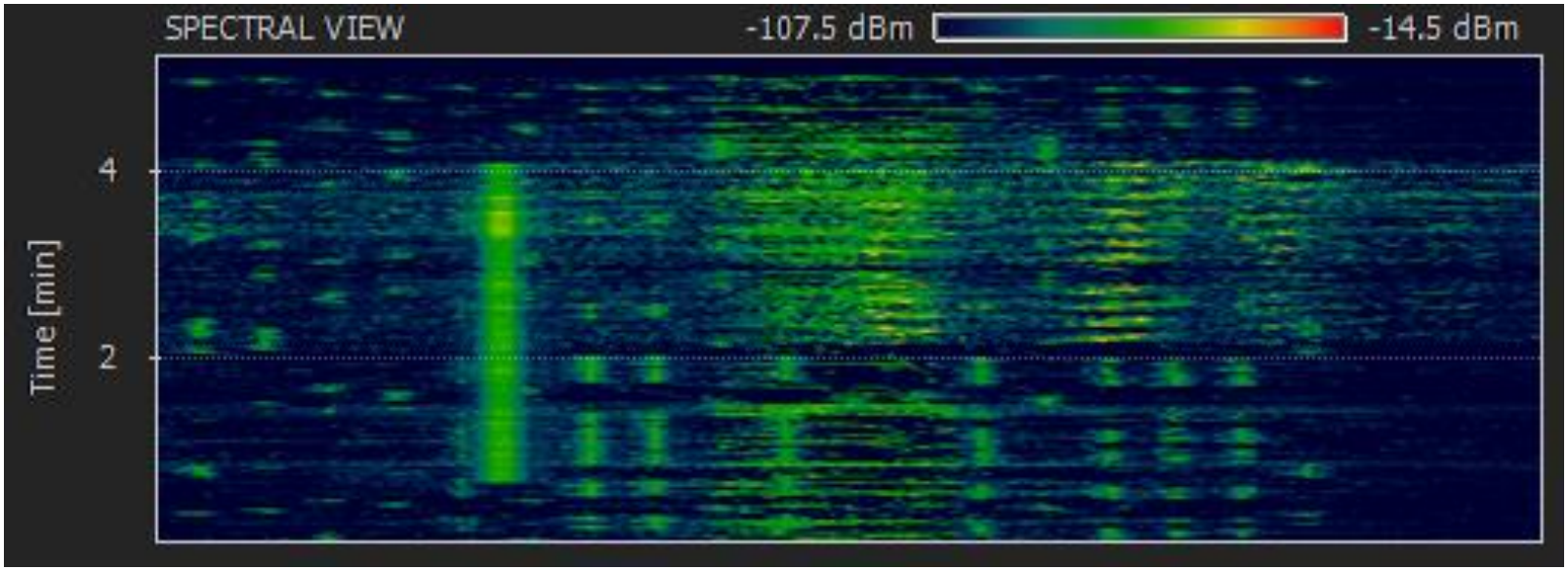
Planar View

- 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.



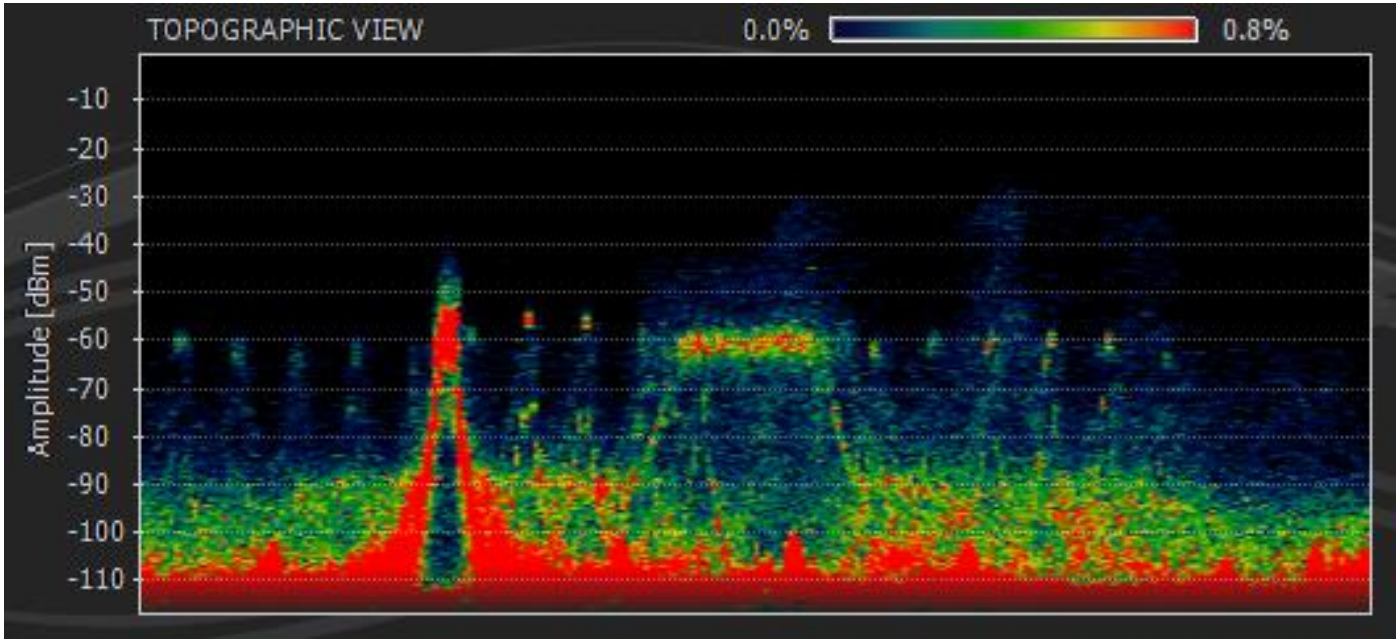
Spectral View

- 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.

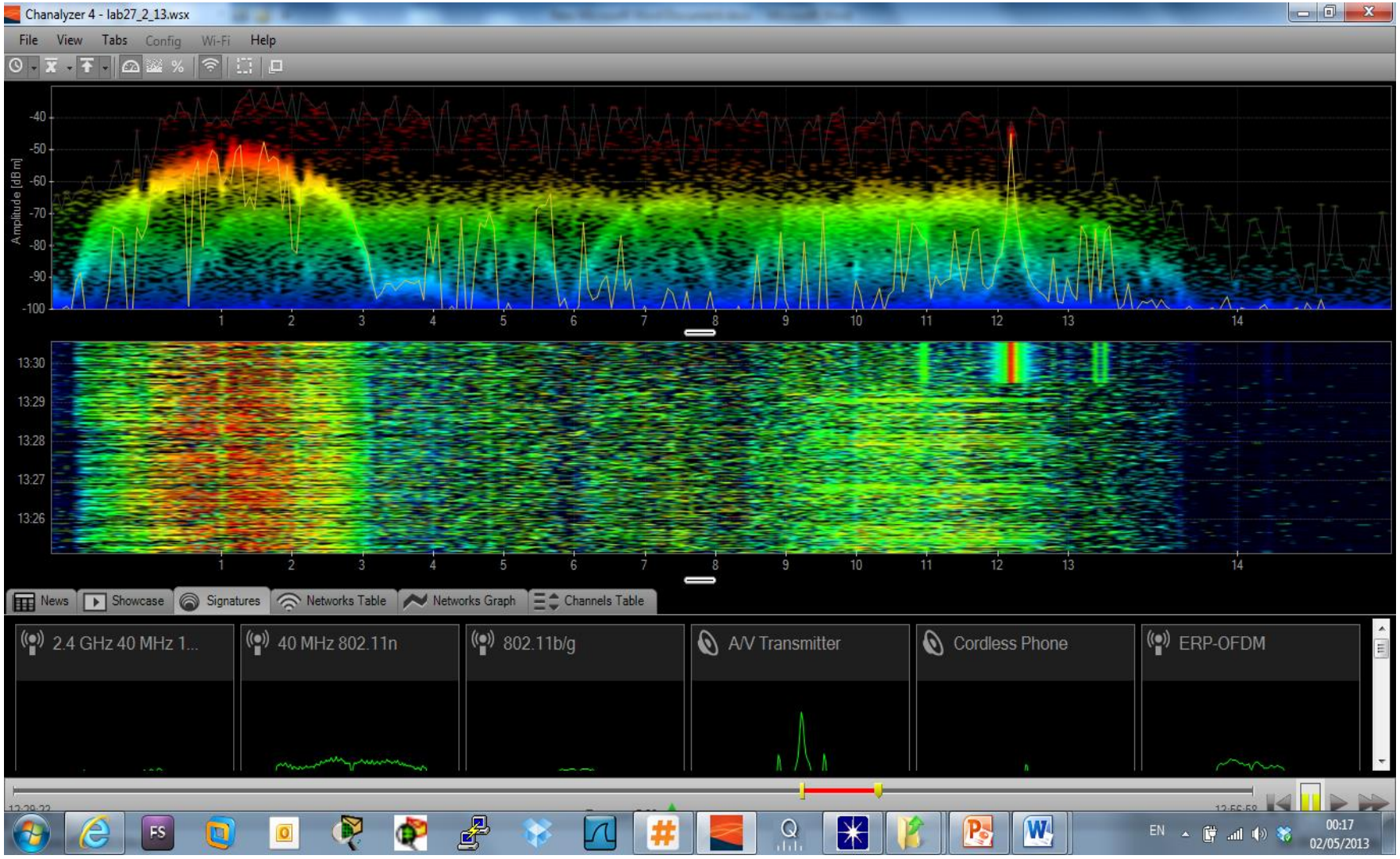


Topographic View

- 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.



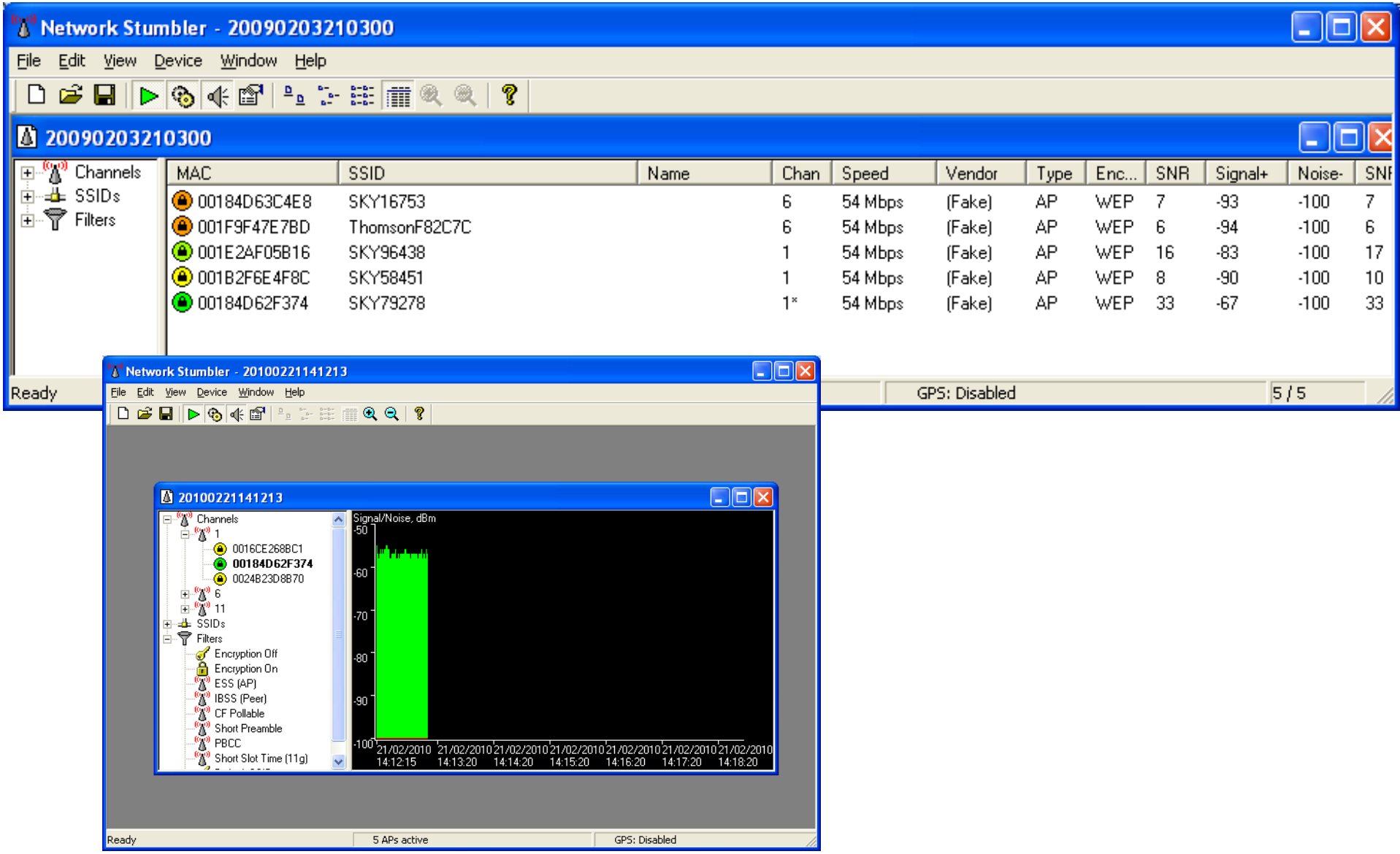
Video Sender Interference



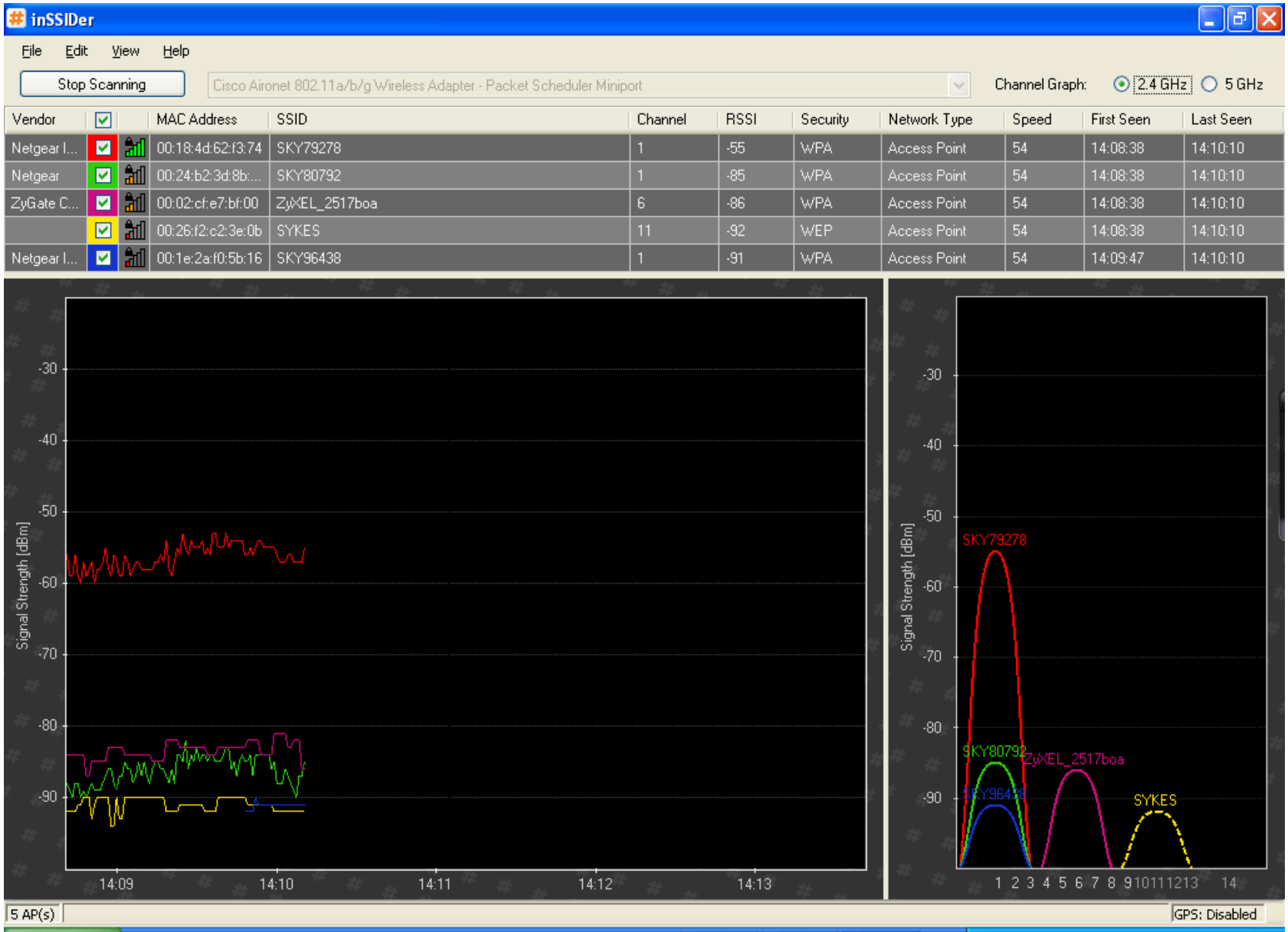
Site Survey Tools

- 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.

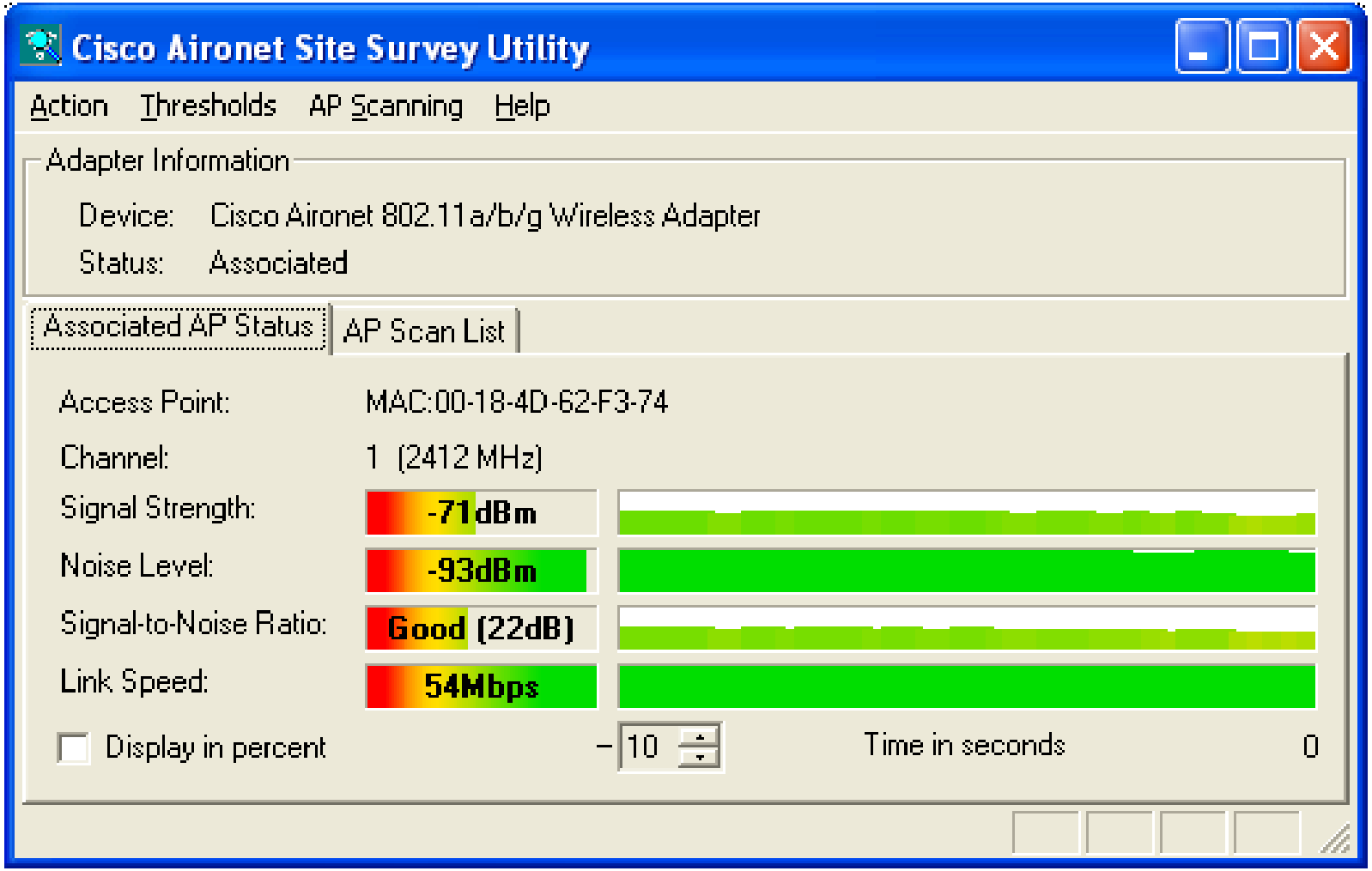
NetStumbler



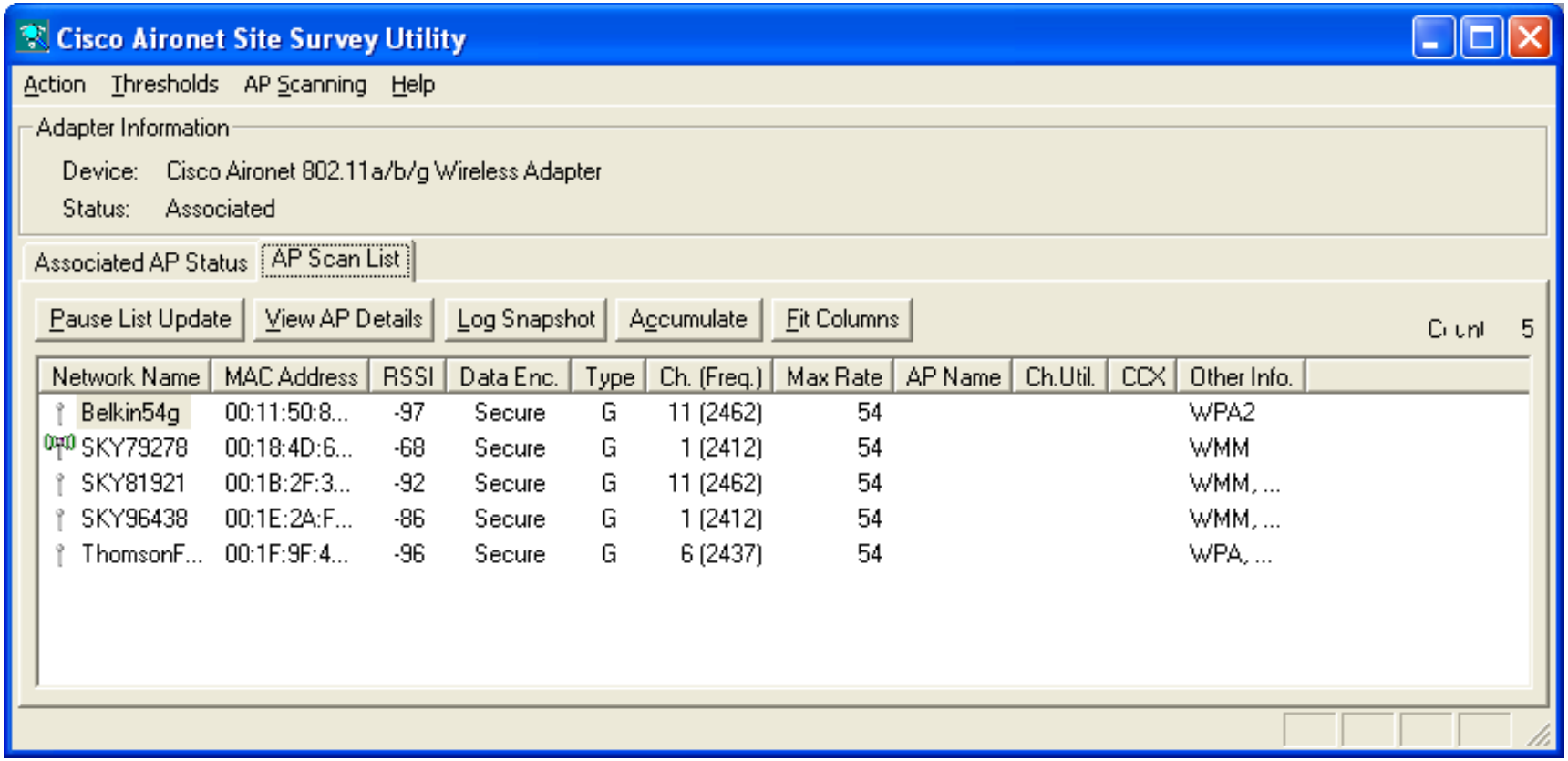
InSSIDer


inSSIDer
File Edit View Help
Stop Scanning
Cisco Aironet 802.11a/b/g Wireless Adapter - Packet Scheduler Miniport
Channel Graph: 2.4 GHz 5 GHz
Vendor | MAC Address | SSID | Channel | RSSI | Security | Network Type | Speed | First Seen | Last Seen
Netgear I... | 00:18:4d:62:f3:74 | SKY79278 | 1 | -55 | WPA | Access Point | 54 | 14:08:38 | 14:10:10
Netgear | 00:24:b2:3d:8b:... | SKY80792 | 1 | -85 | WPA | Access Point | 54 | 14:08:38 | 14:10:10
ZyGate C... | 00:02:cf:e7:bf:00 | ZyXEL_2517boa | 6 | -86 | WPA | Access Point | 54 | 14:08:38 | 14:10:10
00:26:f2:c2:3e:0b | SYKES | 11 | -92 | WEP | Access Point | 54 | 14:08:38 | 14:10:10
Netgear I... | 00:1e:2a:f0:5b:16 | SKY96438 | 1 | -91 | WPA | Access Point | 54 | 14:09:47 | 14:10:10
Signal Strength [dBm]
-30
-40
-50
-60
-70
-80
-90
14:09
14:10
14:11
14:12
14:13
SKY79278
SKY80792
ZyXEL_2517boa
SKY96438
SYKES
1 2 3 4 5 6 7 8 9 10 11 12 13 14
5 AP(s)
GPS: Disabled

Cisco Site Survey 1



Cisco Site Survey 2



Monitoring Issues

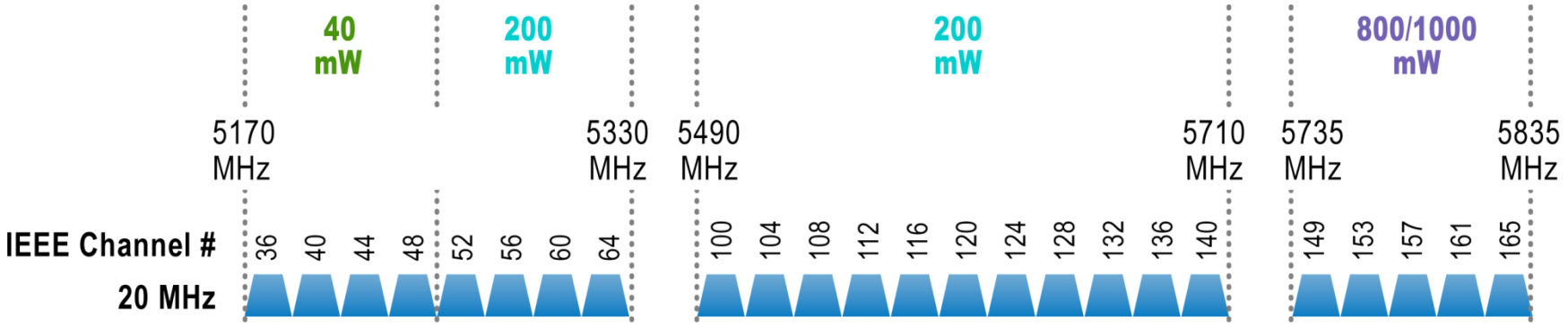
- Multiple channels to cover
- Wireless Modes
- Limited Range
- Receiver Sensitivity
- Wide area to coverage
- Environment
- Encrypted traffic

IEEE 802.11 Channels

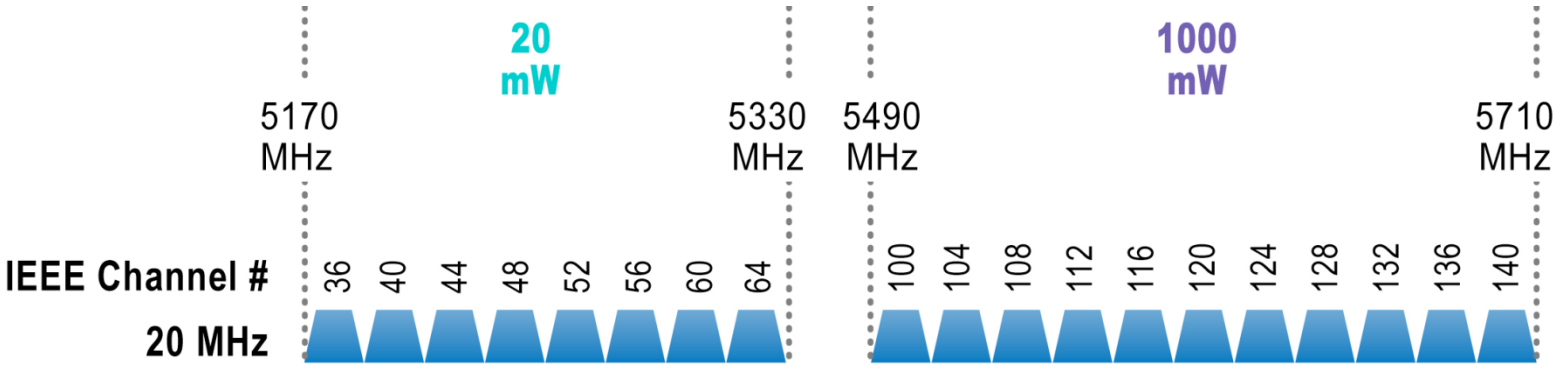
Frequency	Channel Number	Frequency	Channel Number
2.412 GHz	1	2.484 GHz	14
2.417 GHz	2	5.180 GHz	36
2.422 GHz	3	5.200 GHz	40
2.427 GHz	4	5.220 GHz	44
2.432 GHz	5	5.240 GHz	48
2.437 GHz	6	5.260 GHz	52
2.442 GHz	7	5.280 GHz	56
2.447 GHz	8	5.300 GHz	60
2.452 GHz	9	5.320 GHz	64
2.457 GHz	10	5.745 GHz	149
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

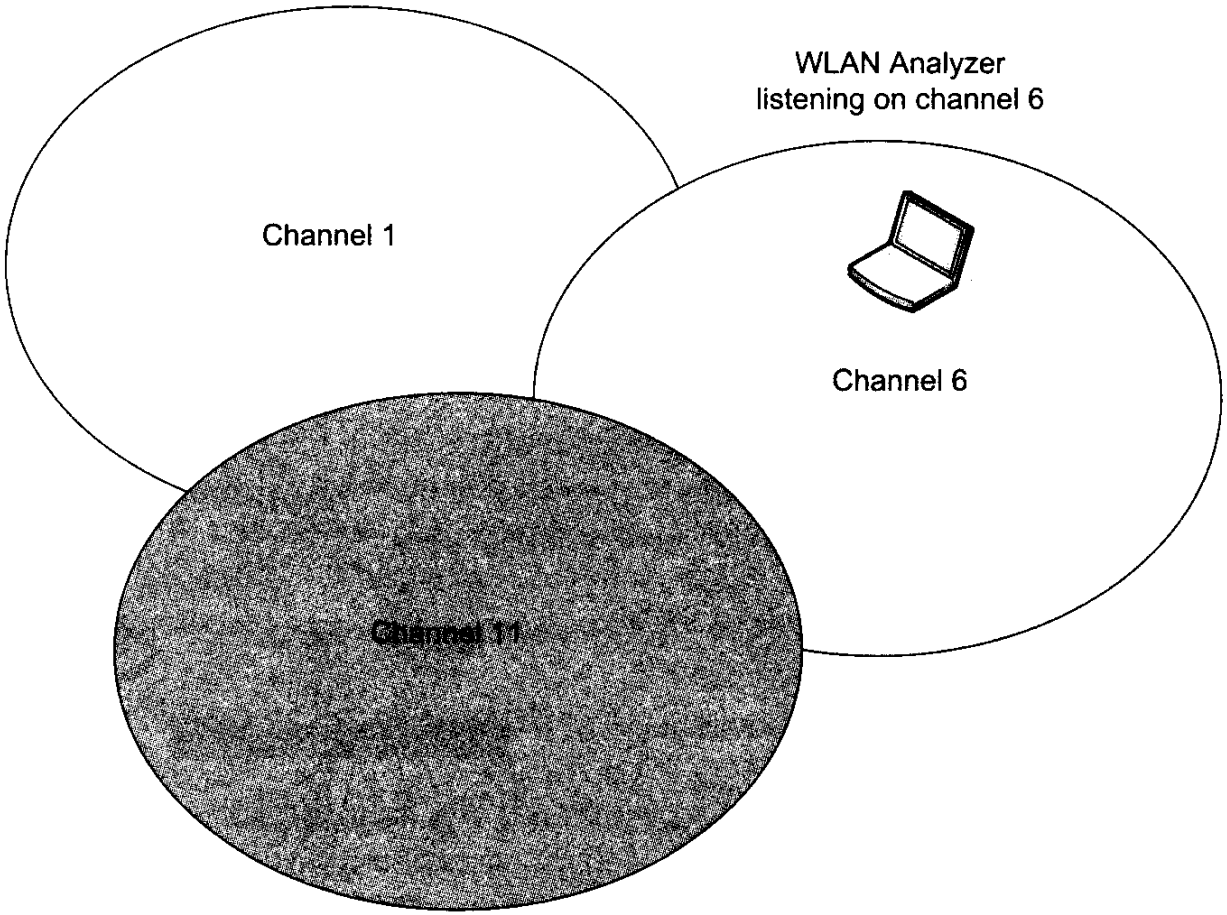


US Channel Allocations

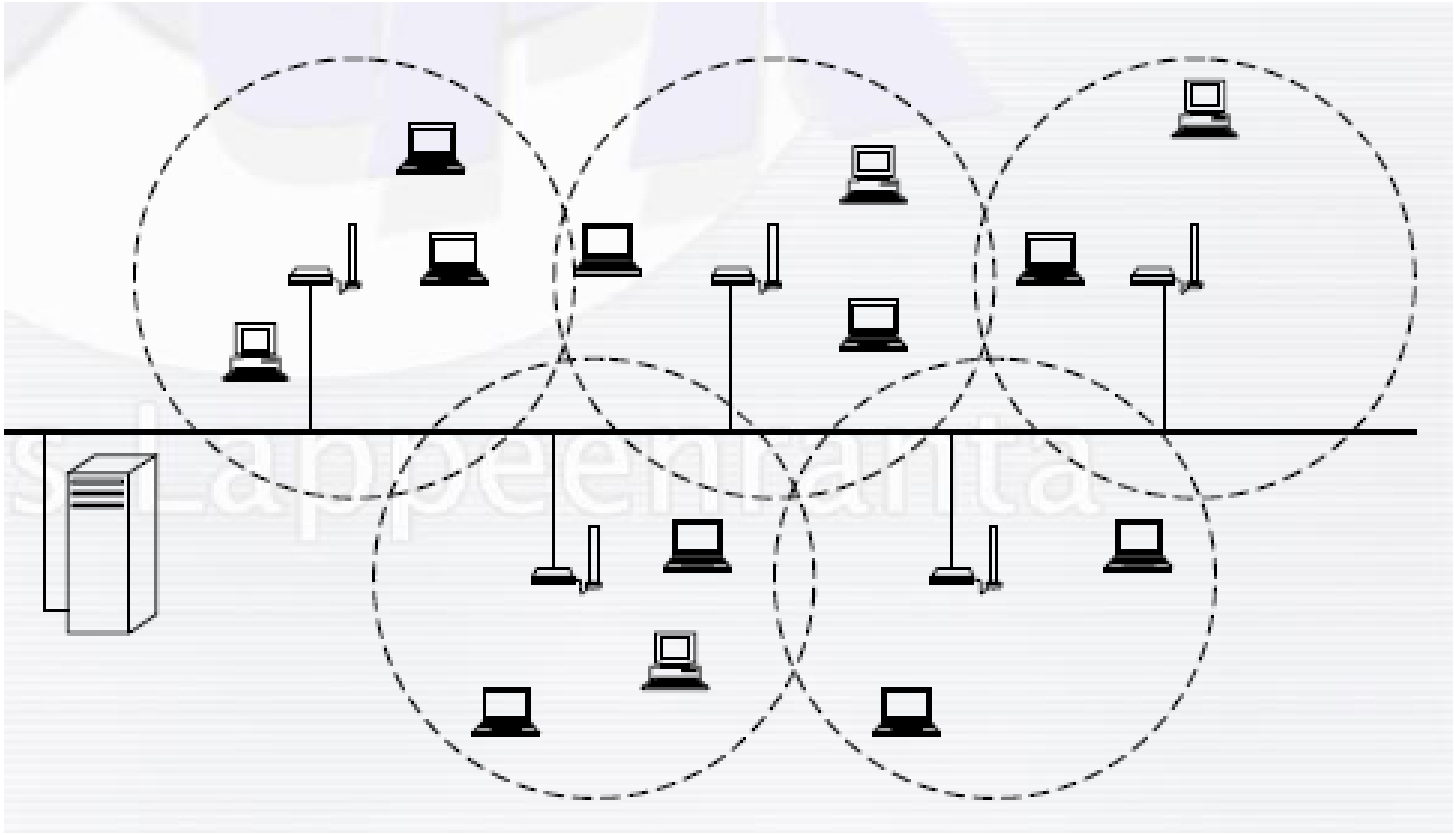


European Channel Allocations

Multi-cell Monitoring Problem



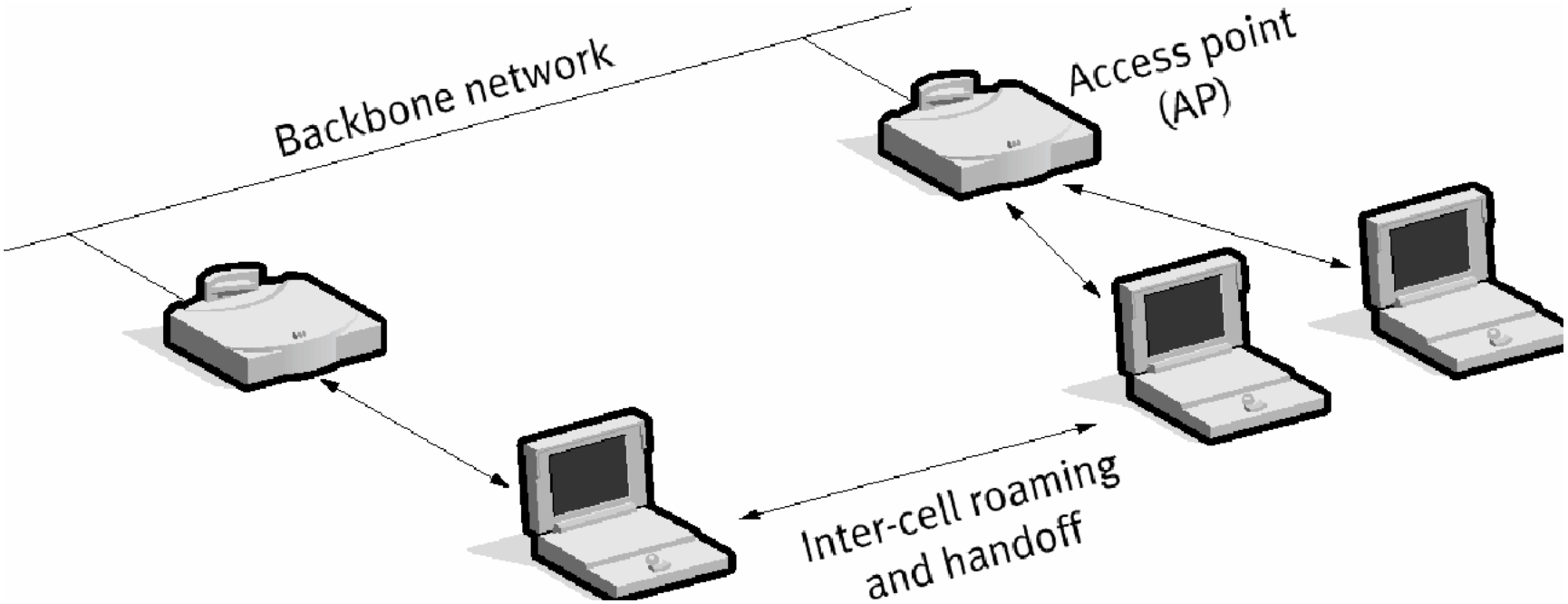
Extended Service Set



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


Backbone network
Access point
(AP)
Inter-cell roaming
and handoff

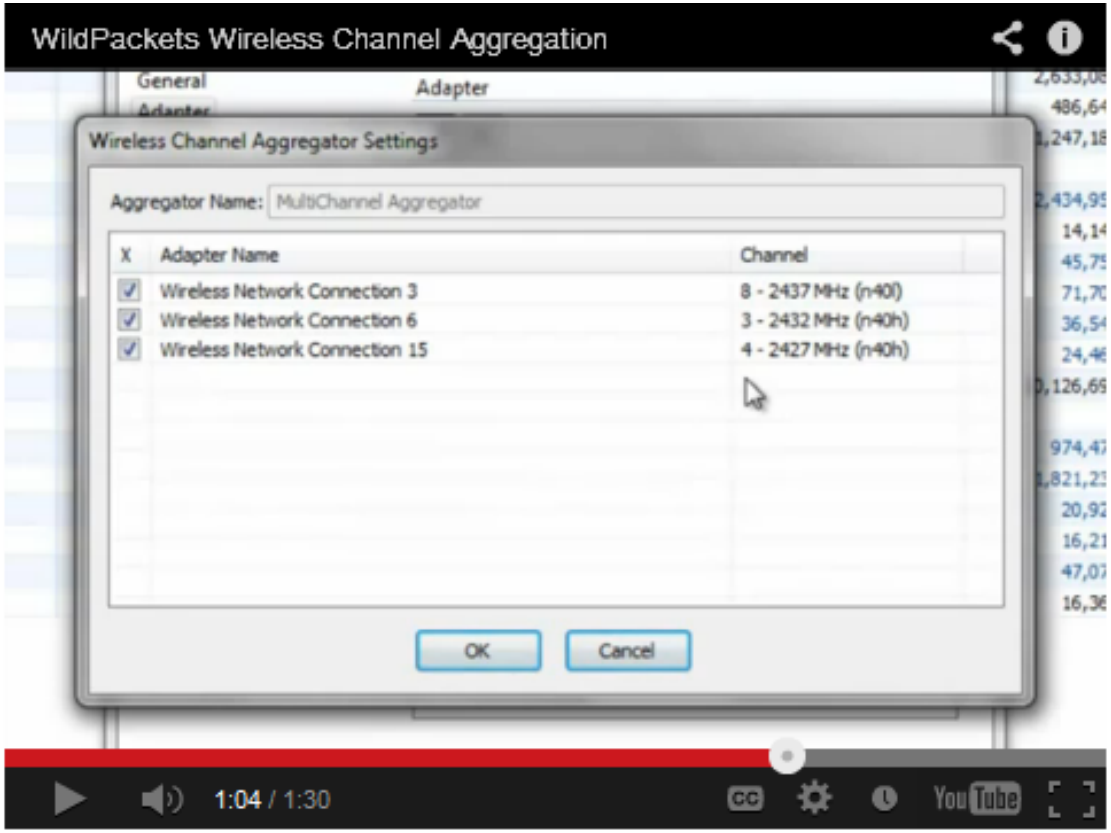
Roaming Issue

- 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

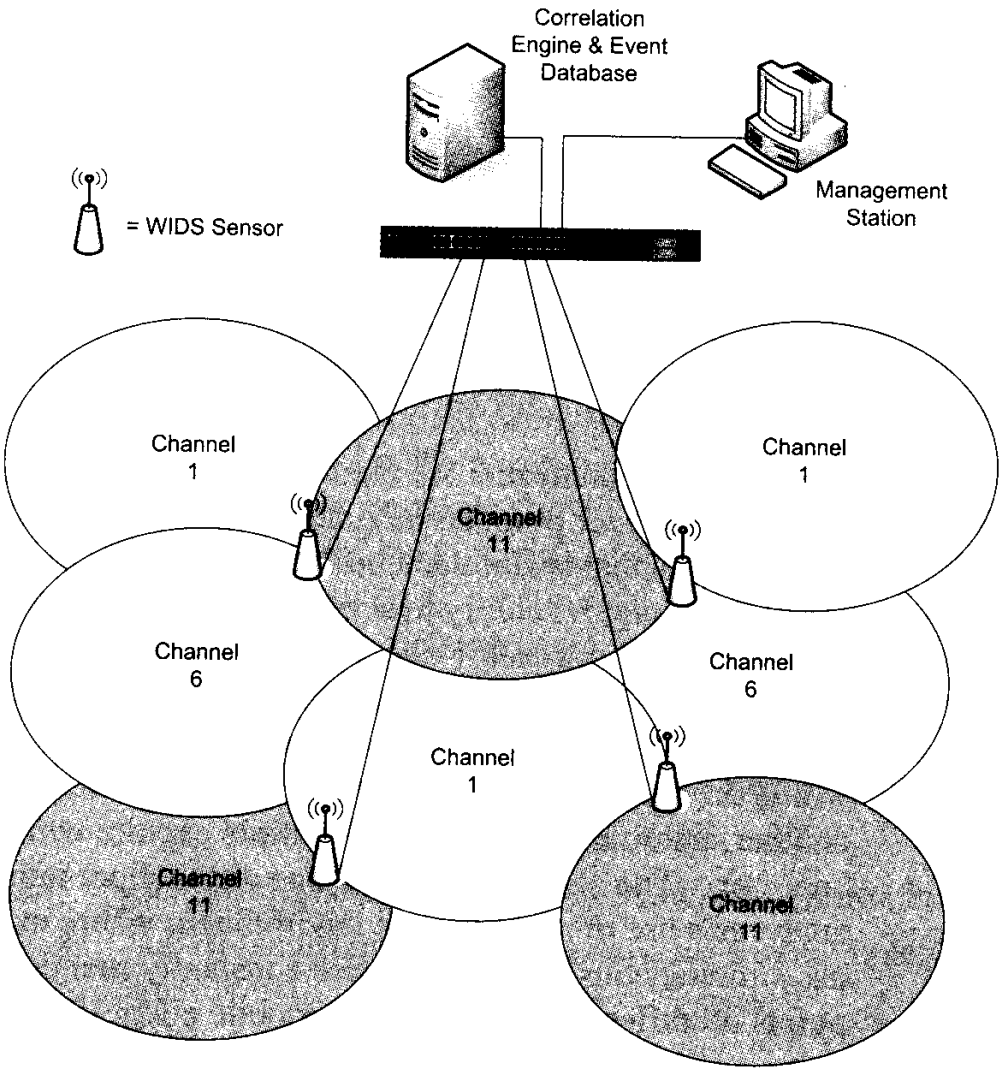
Solution2 Distributed Analyser

- 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

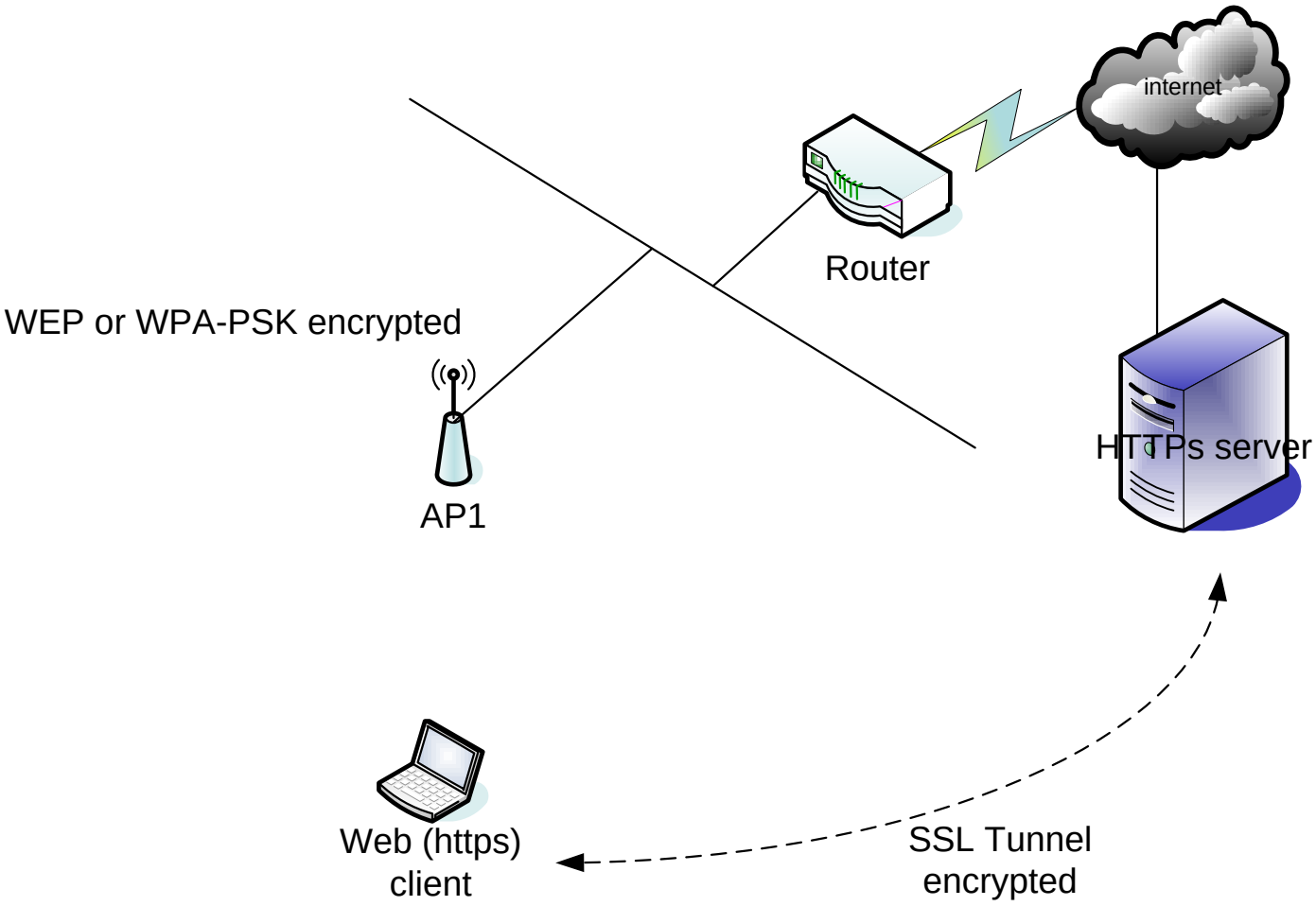
Encryption of Wireless Data

- 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.

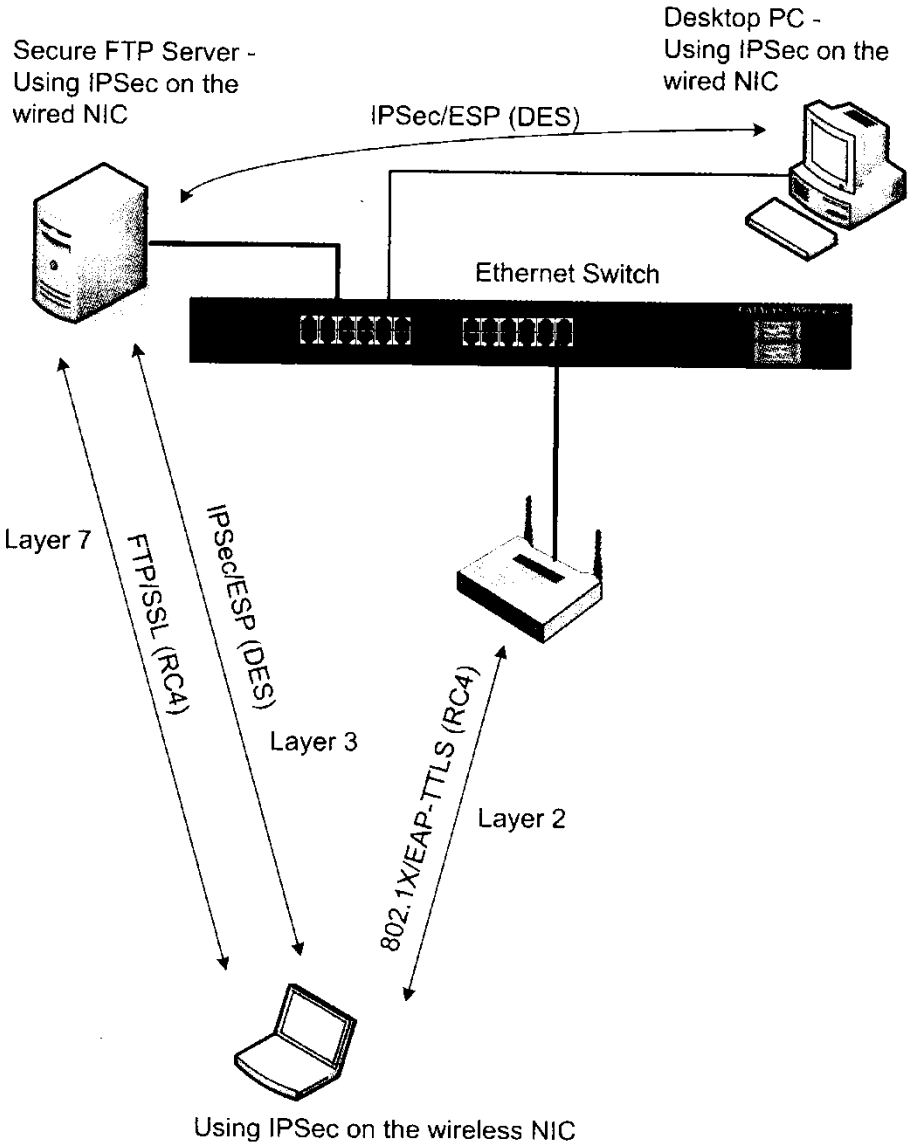
Example 1 Diagram



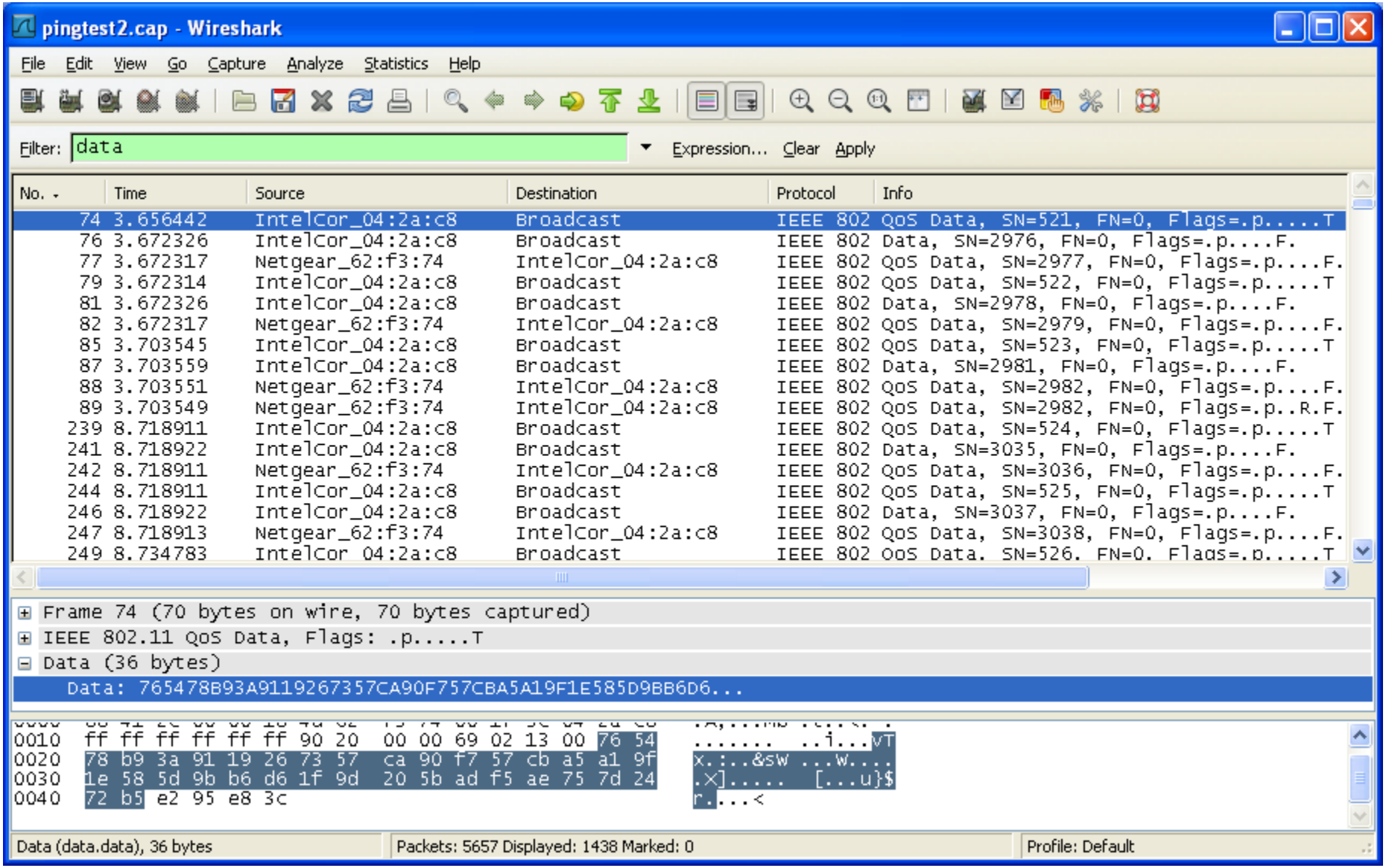
Example 2 of Multilevel Encryption

- 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.

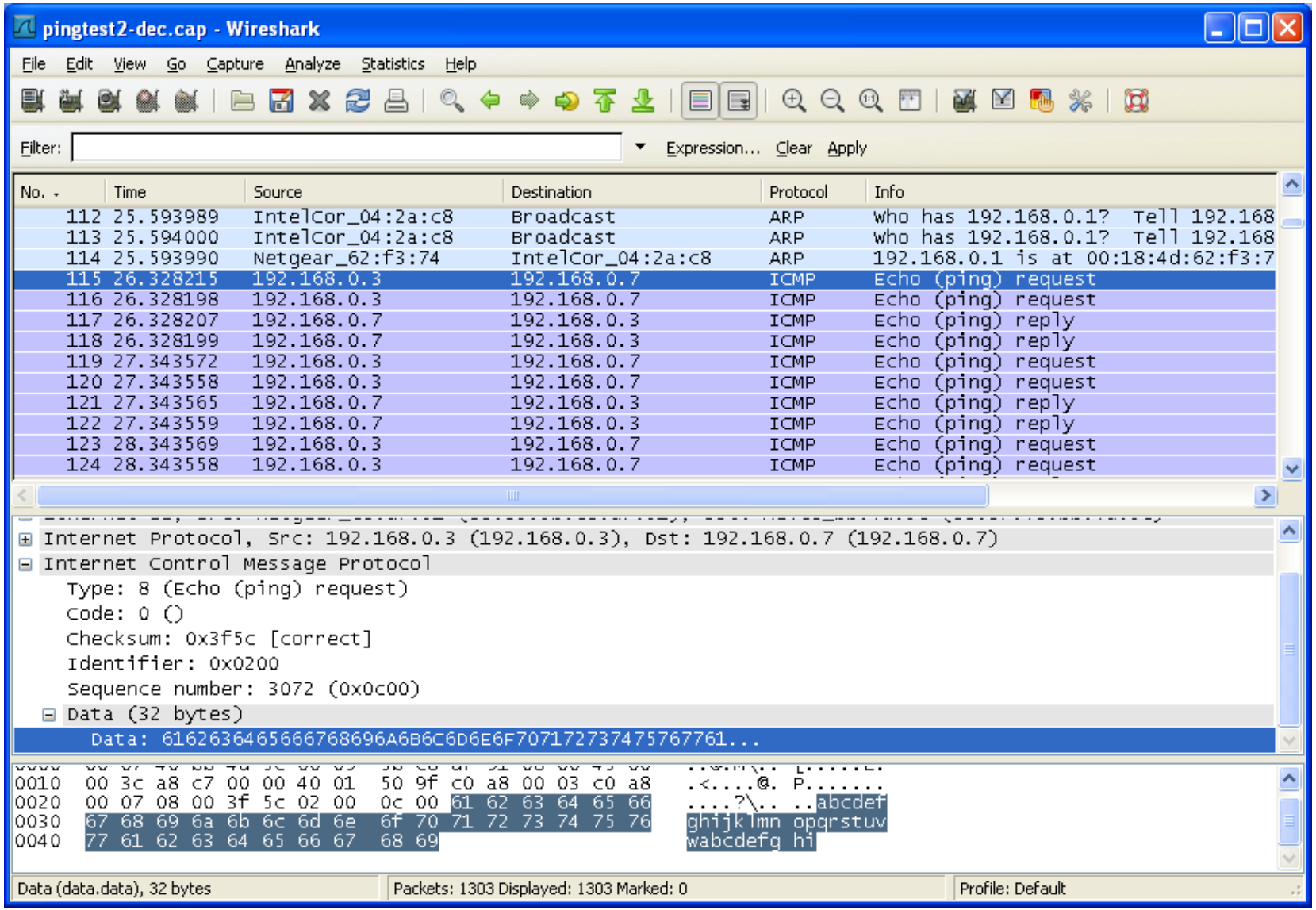
Example 2 3-level Encryption



Encrypted ping Data Packets



Decrypted ping Data Packet



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
- Airopeek
- 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.

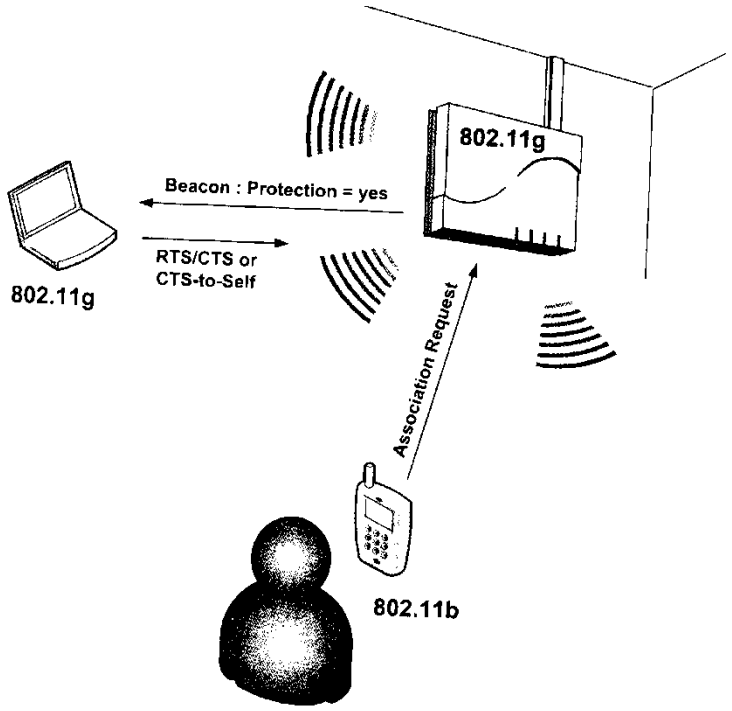
Performance Measurements

- 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

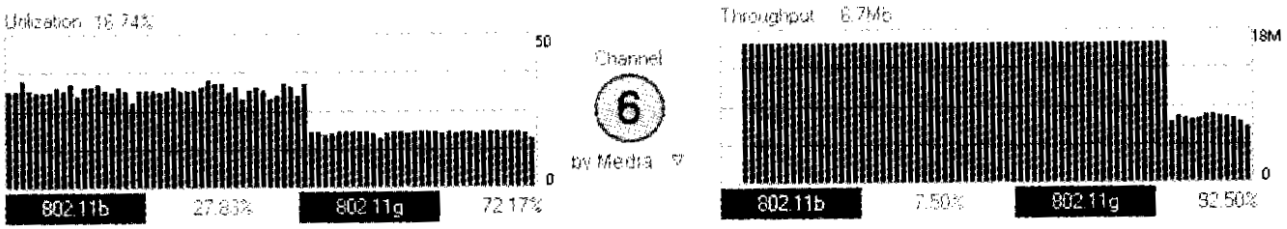
Mixed Mode Performance Problem

- 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



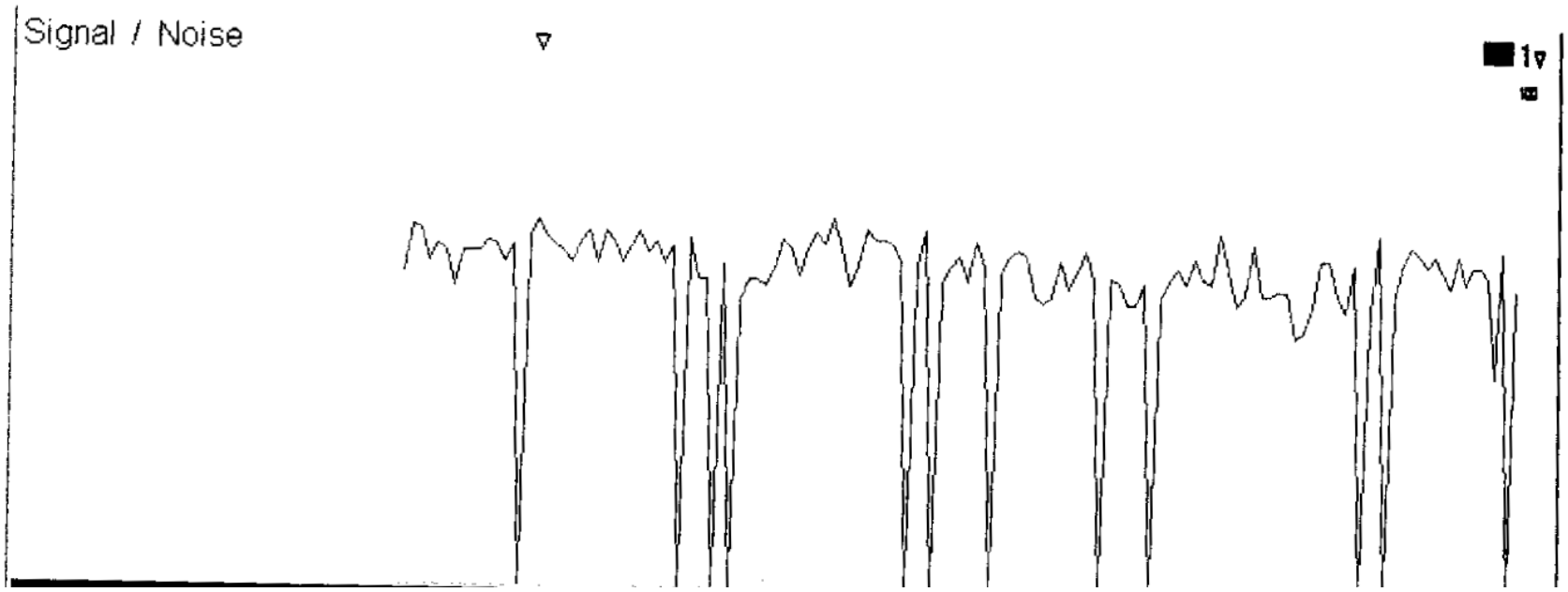
802.11b/g Mixed Mode Environment Throughput Scale

Number of 802.11b clients	0	1	2	3	4	5	6	7	8	9	10
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

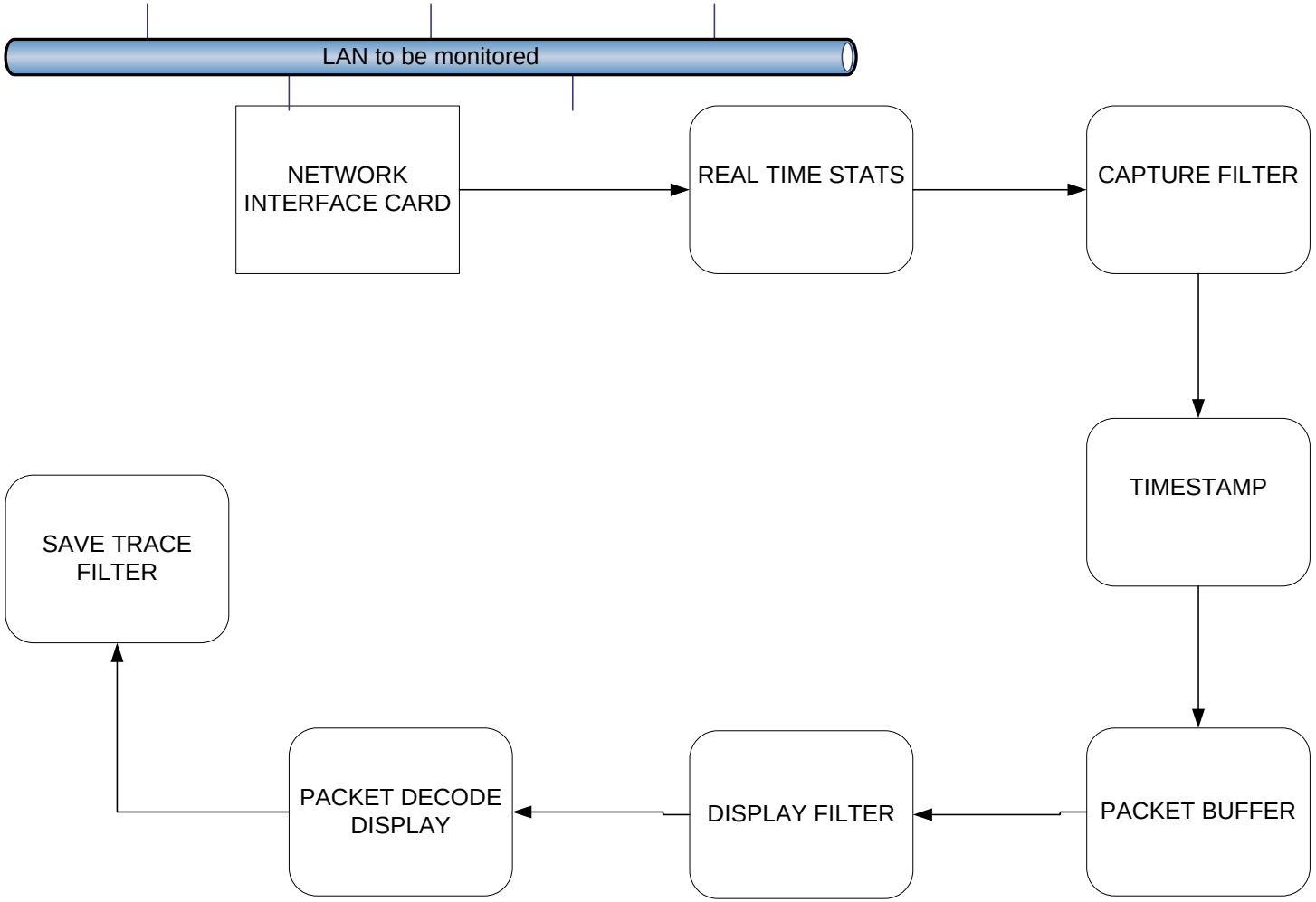
Number of 802.11g clients

Radio Failing Problem

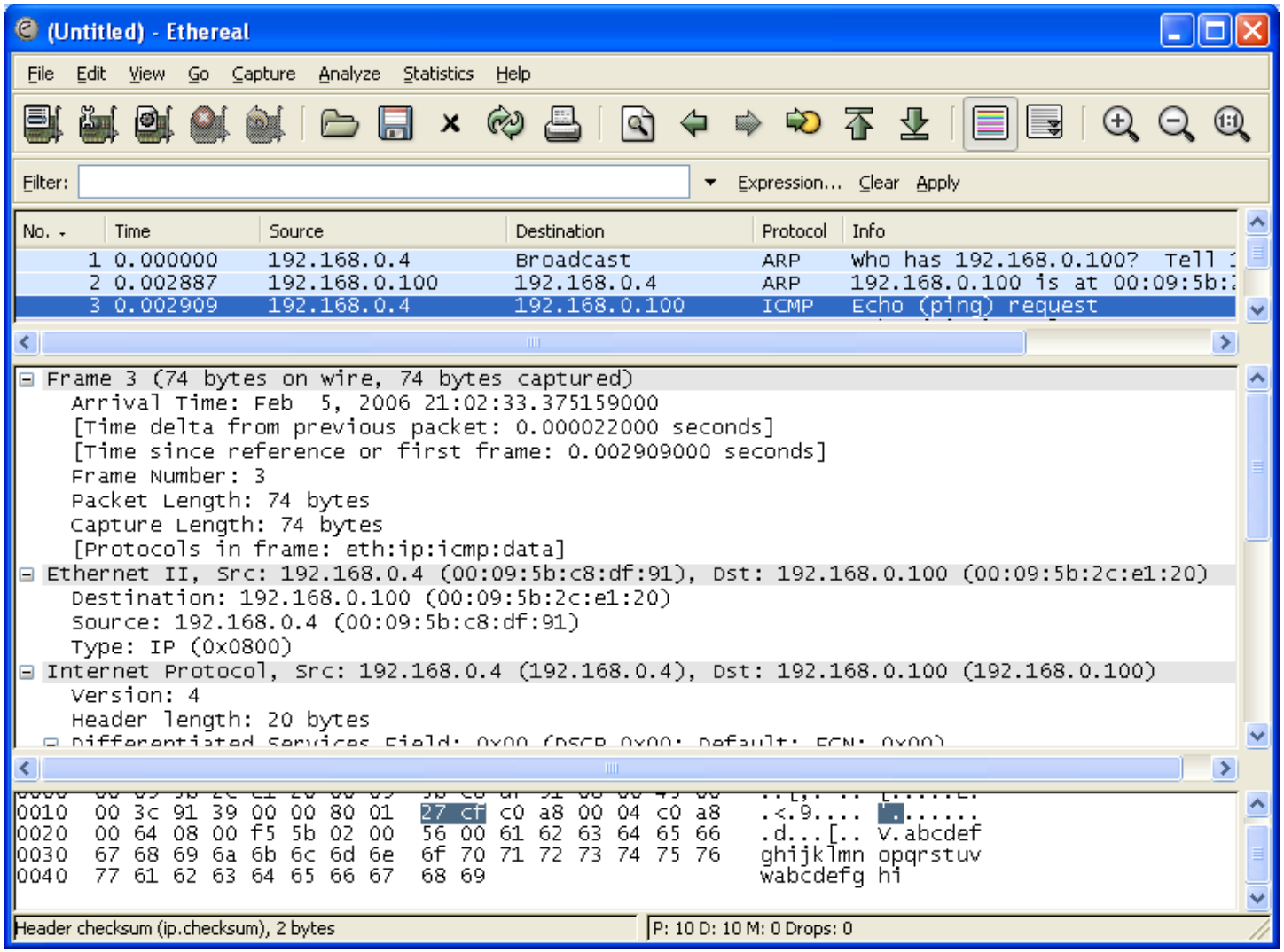
Intermittently Failing Radio



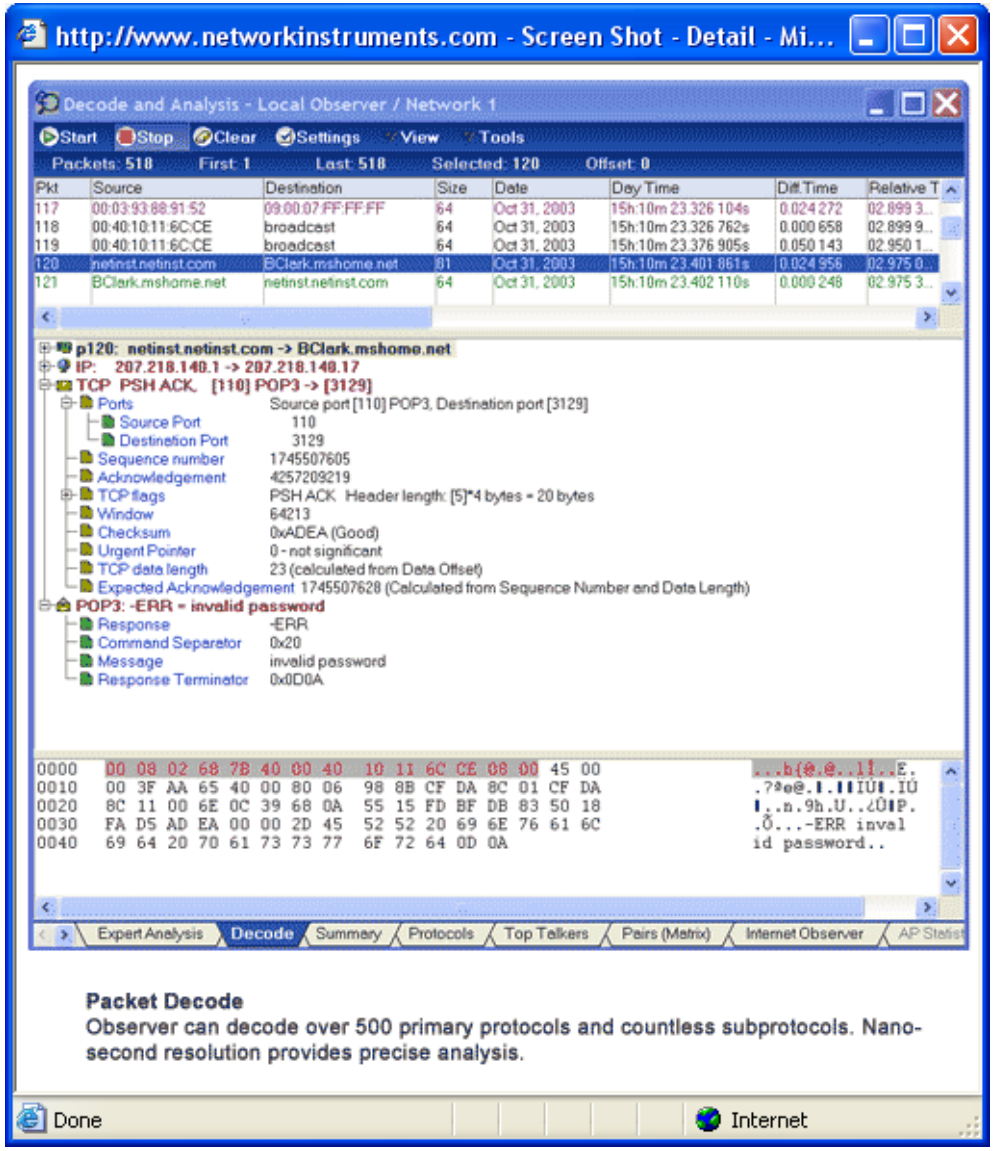
Protocol Analyser Operation



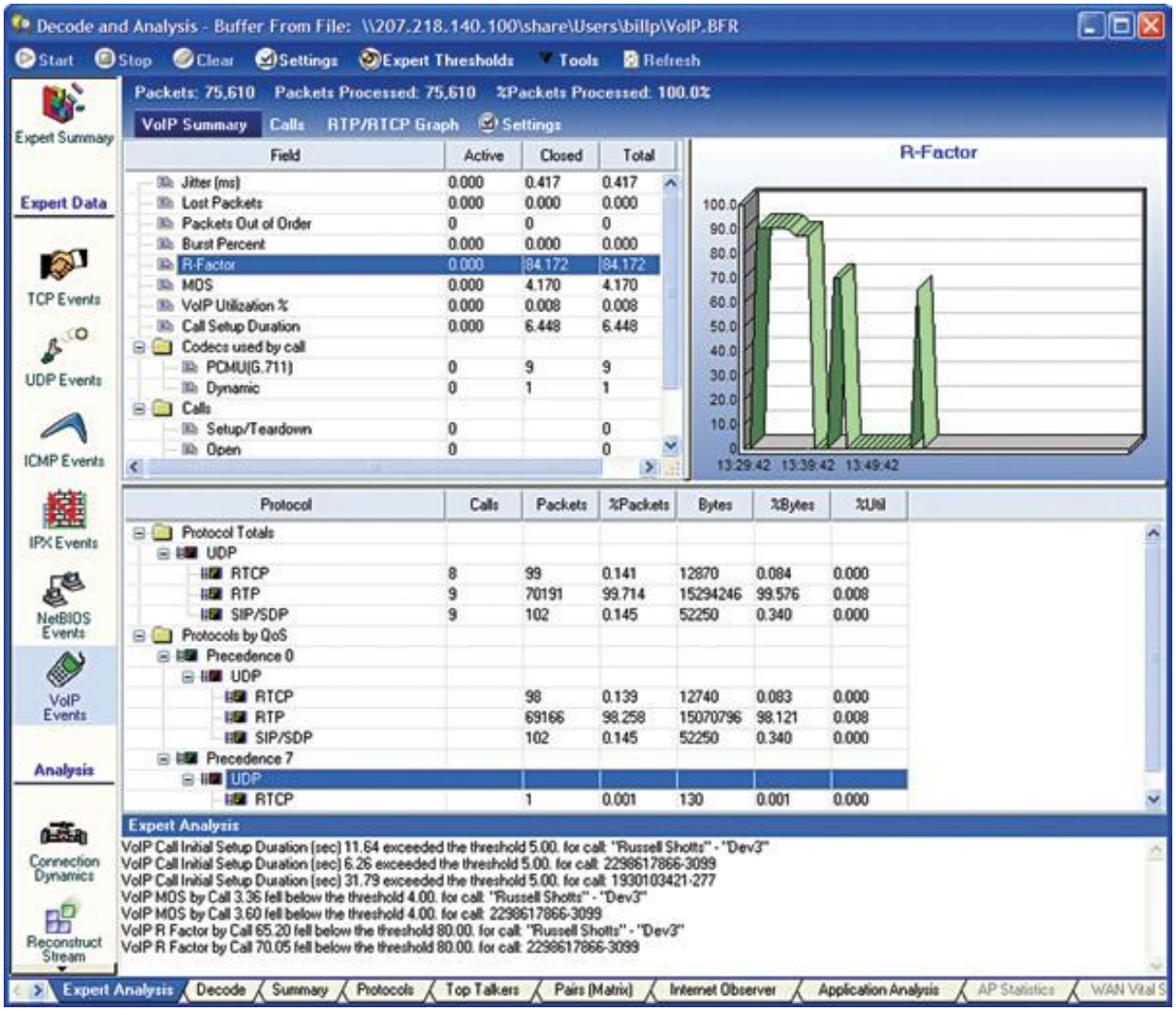
Wireshark Packet Decode



Observer Packet Decode

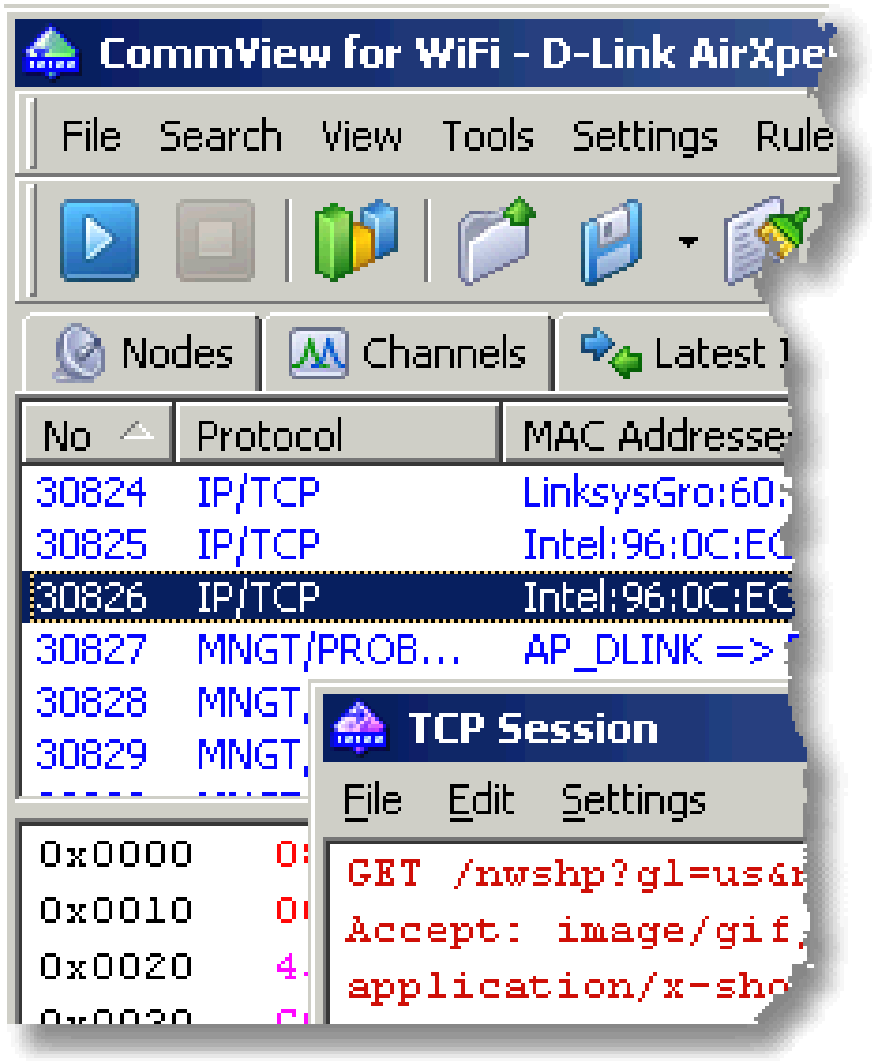


Observer VoIP Expert

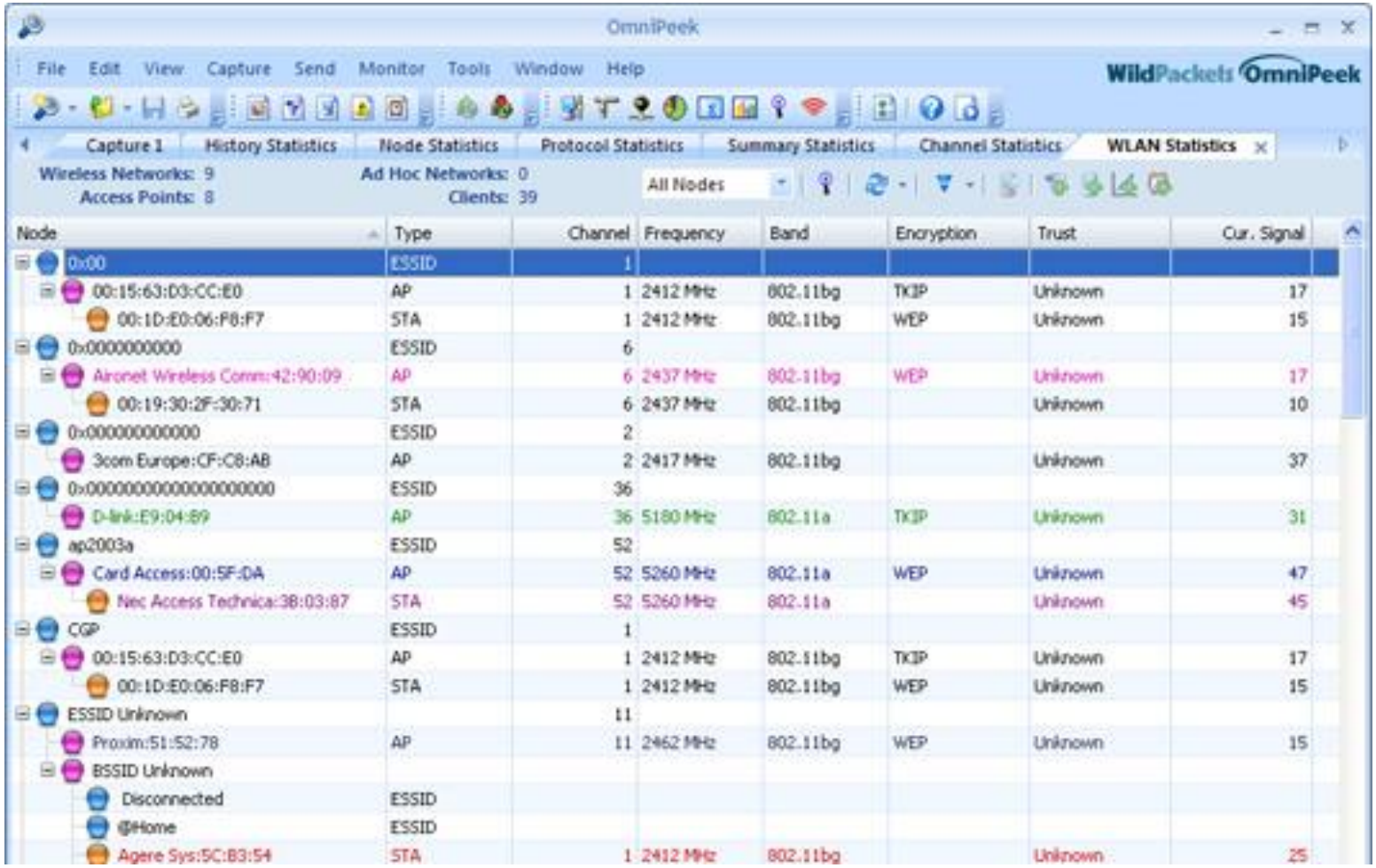


OptiView

CommView for WiFi



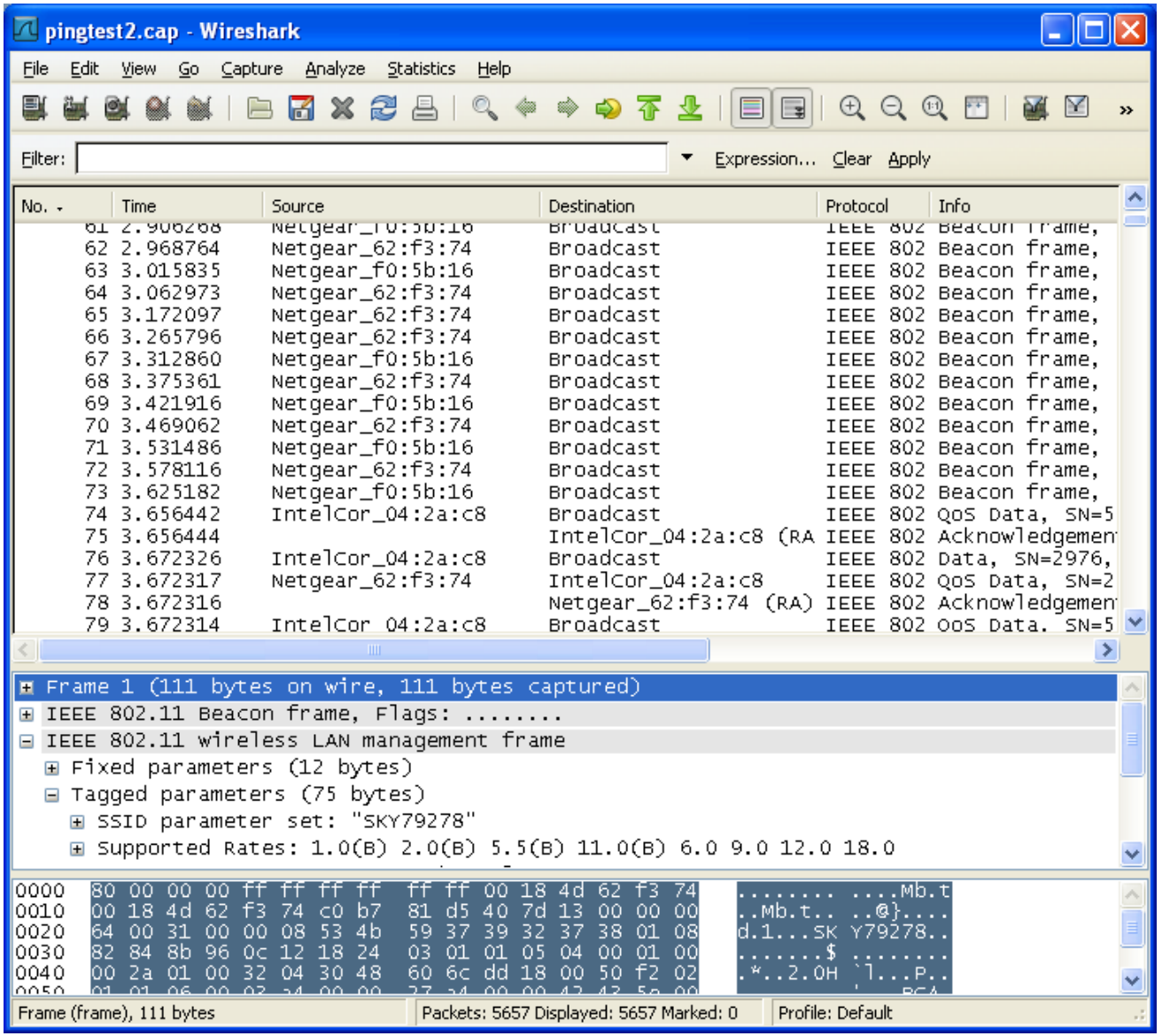
OmniPeek


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
Access Points: 8
Ad Hoc Networks: 0
Clients: 39
All Nodes
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:AB AP 2 2417 MHz 802.11bg Unknown 37
0x00000000000000000000 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:3B: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

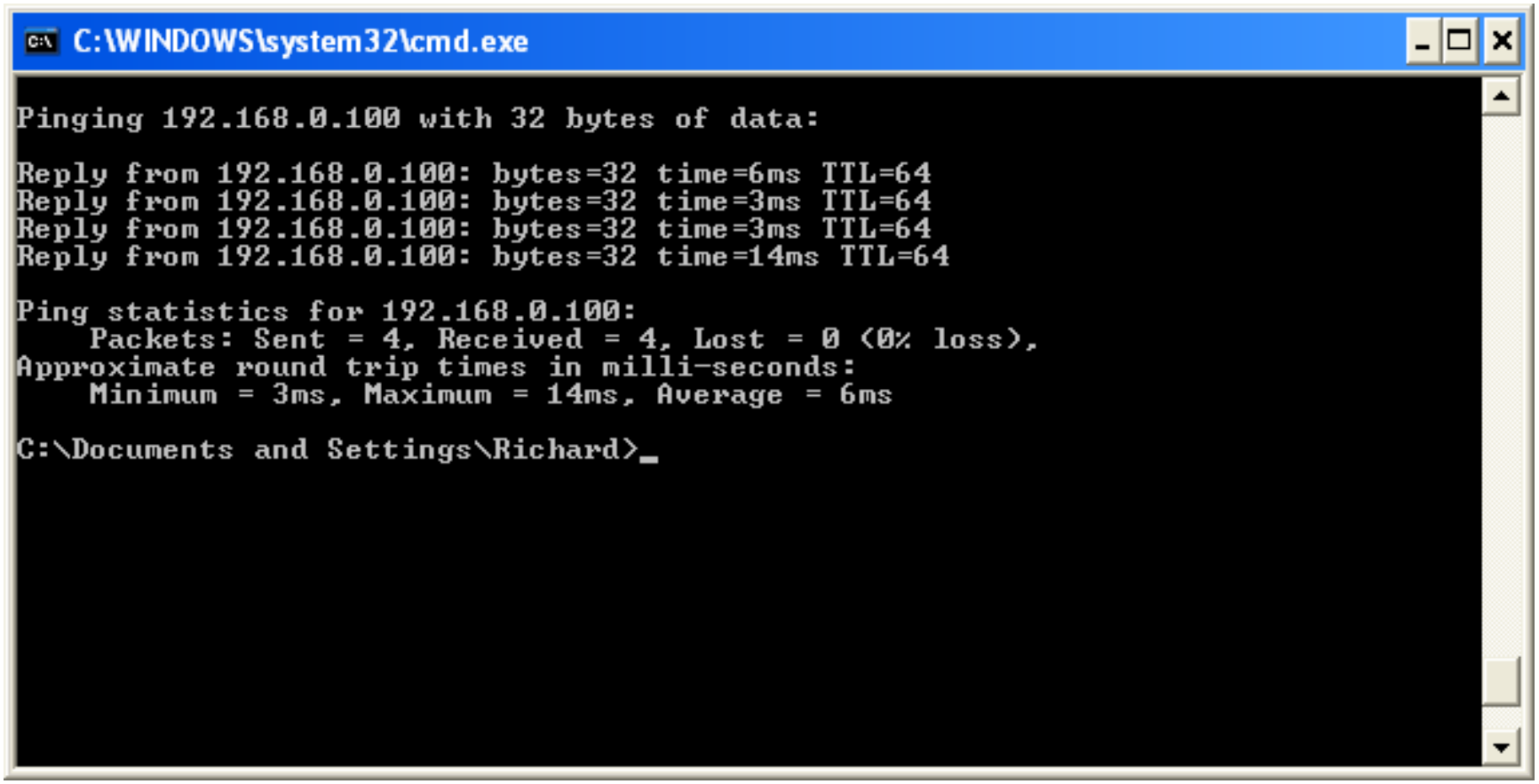


Analysing PING with Wireshark

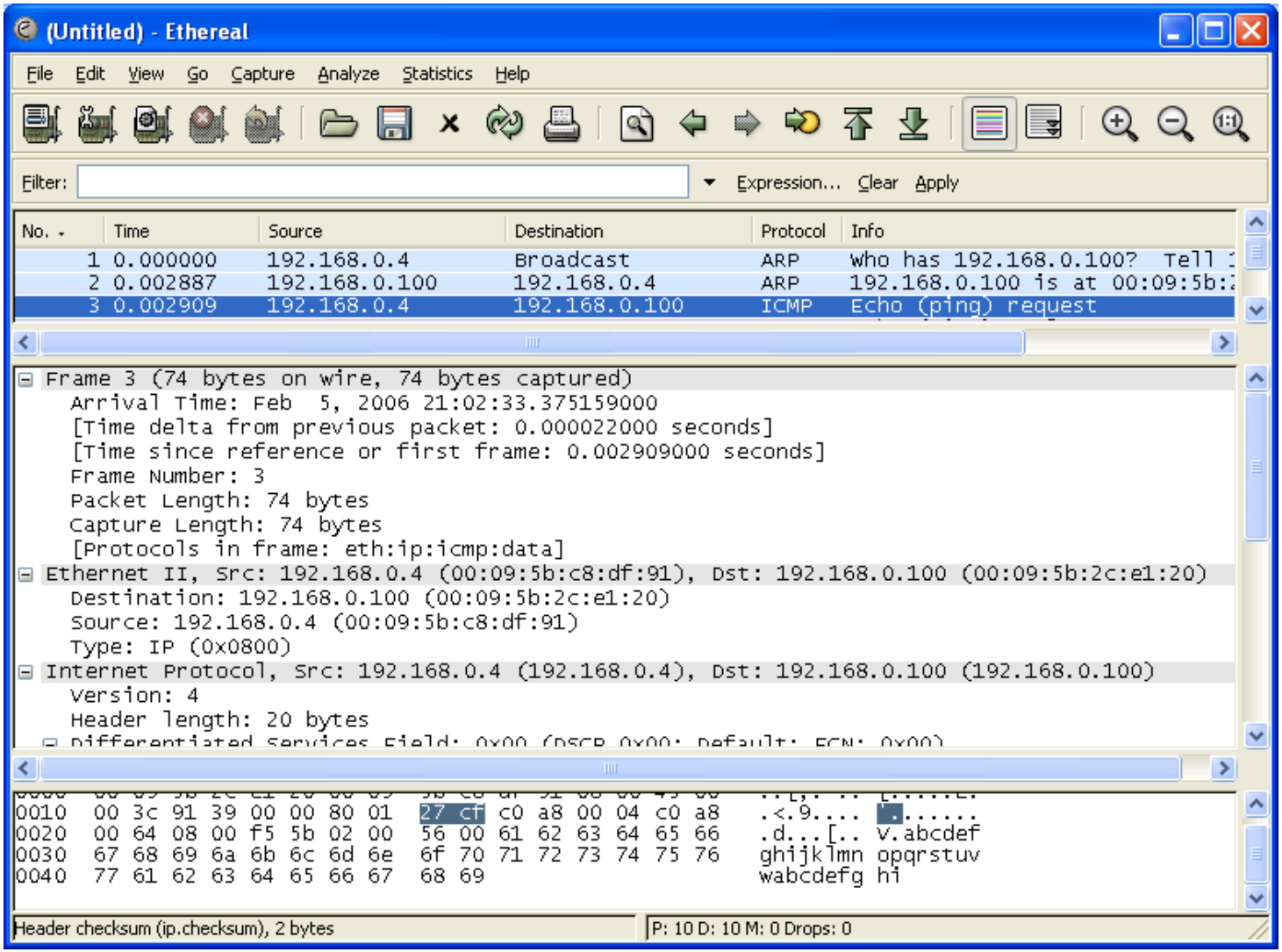
- Wireshark is a GUI network protocol analyser.
- It can examine data from a live network or from a capture file on disk.
- You can interactively browse the capture data, viewing summary and detail information for each packet.
- Can assemble all the packets in a TCP conversation and show you the ASCII (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

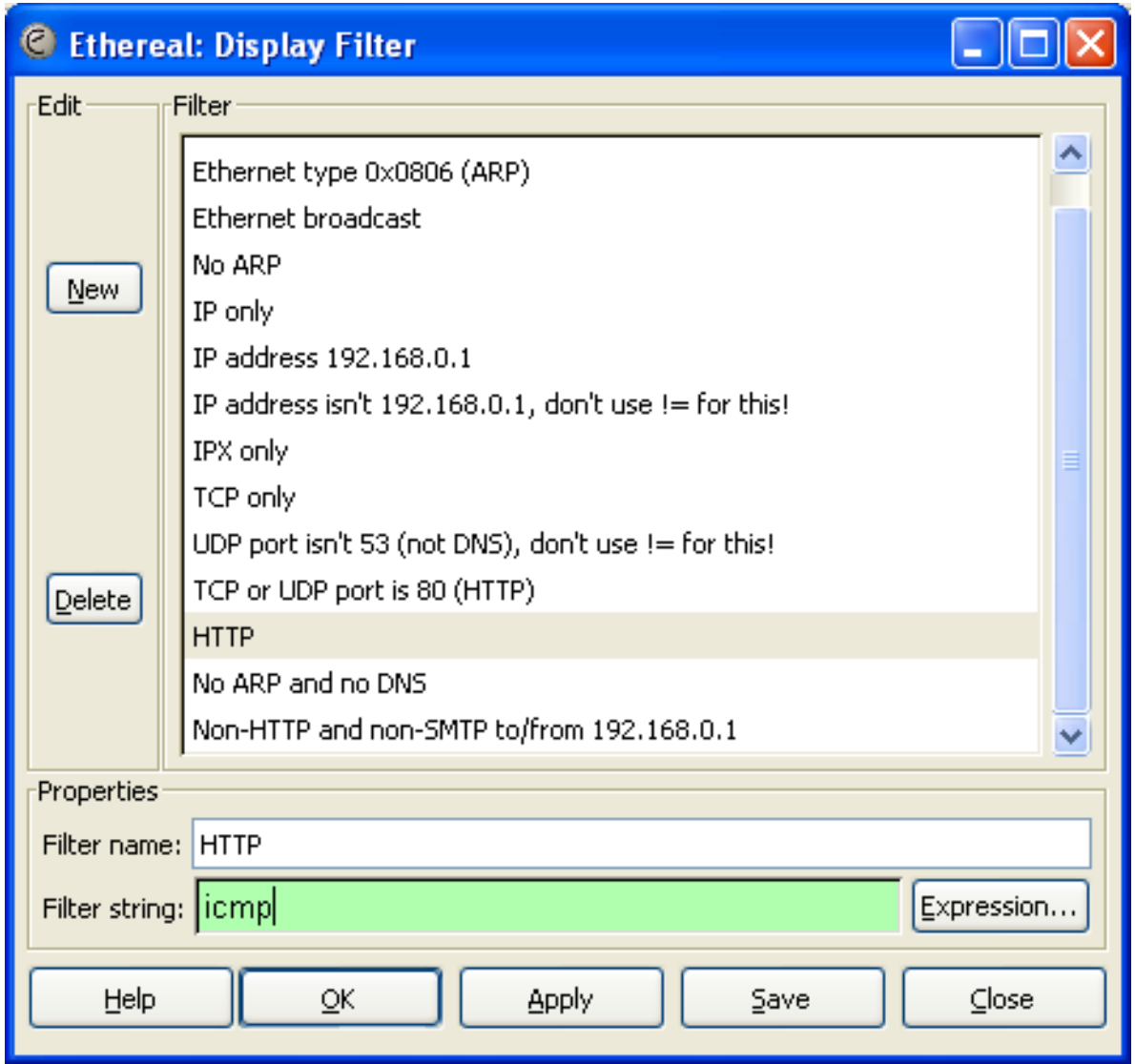
Command Prompt



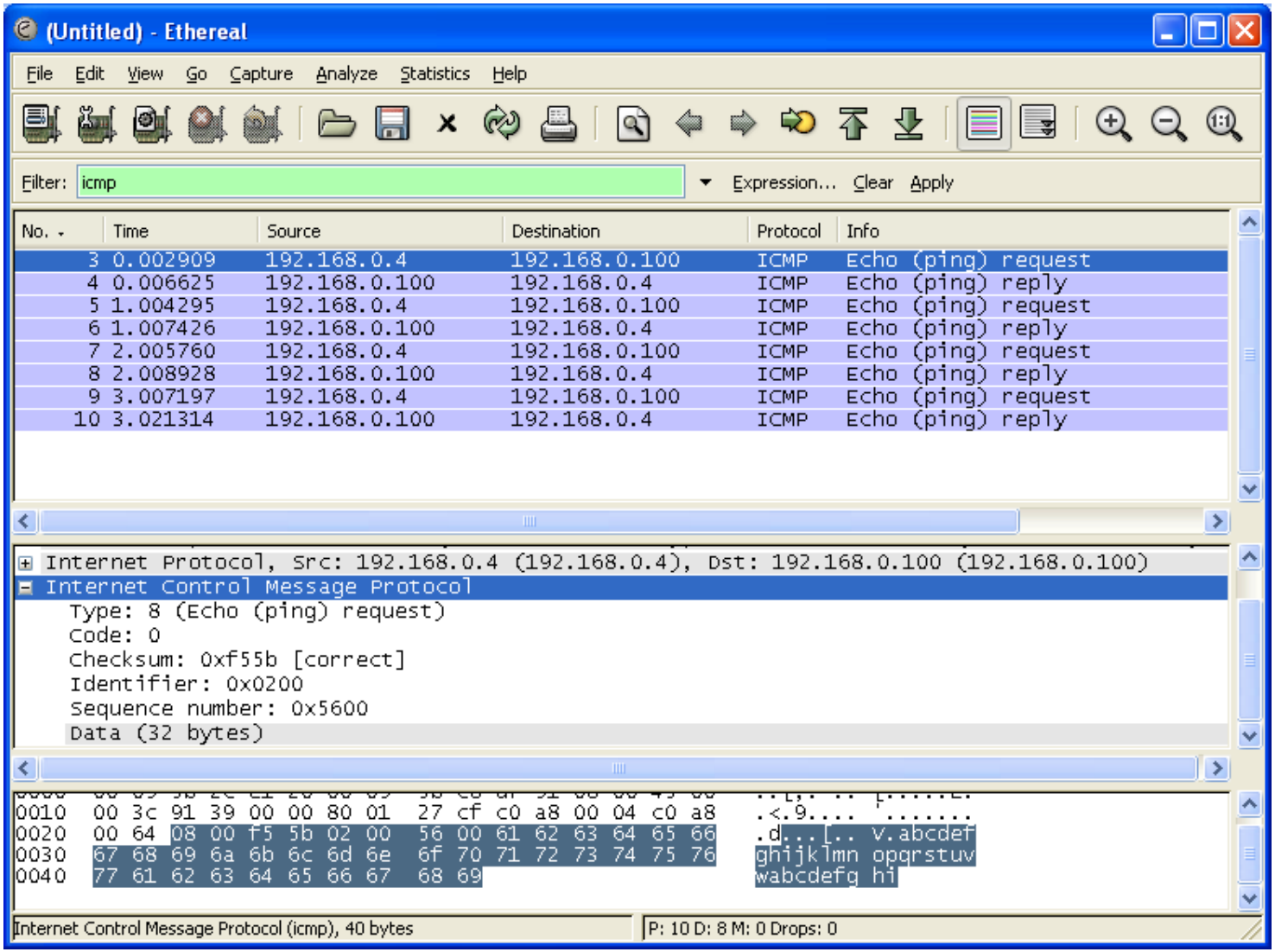
Expand Details



Apply Display Filters



Display Filter Result



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

Tools & Traps

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

More Wireshark Filters

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

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

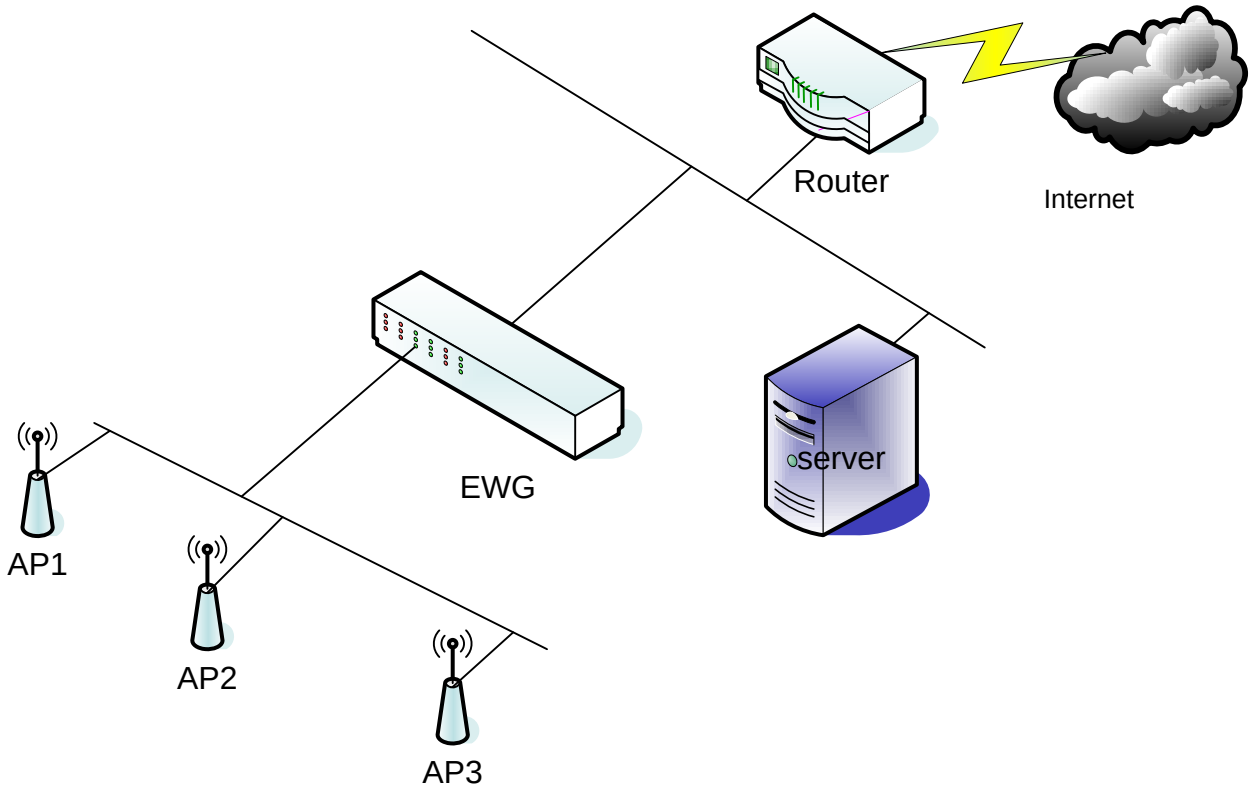
Enterprise solutions

- 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.

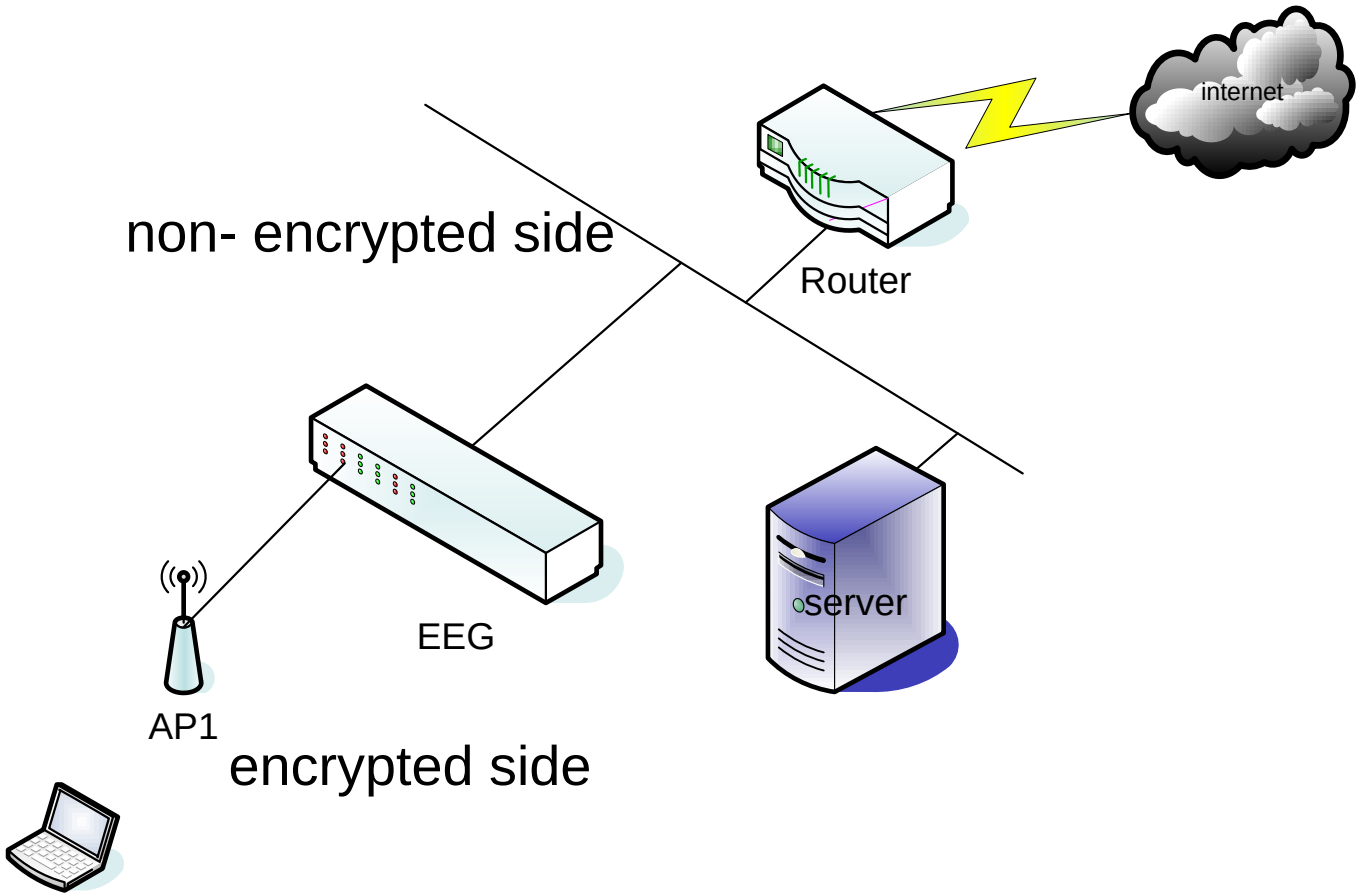
EWG example



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.

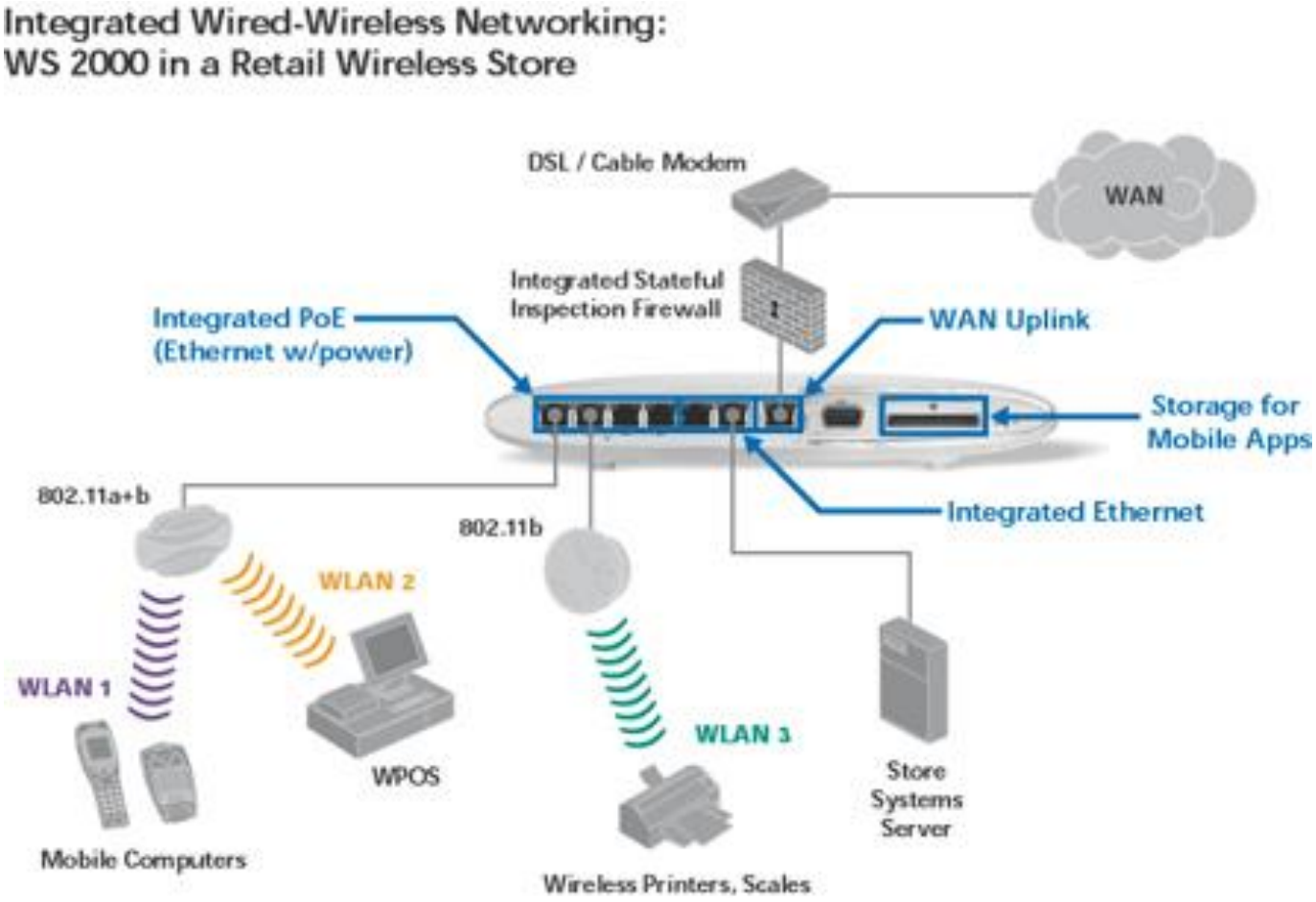
EEG example


internet
non- encrypted side
Router
EEG
server
AP1
encrypted side

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
DSL / Cable Modem
WAN
Integrated Stateful
Inspection Firewall
Integrated PoE
(Ethernet w/power)
WAN Uplink
Storage for
Mobile Apps
802.11a+b
802.11b
Integrated Ethernet
WLAN 2
WLAN 1
WLAN 3
WPOS
Store
Systems
Server
Mobile Computers
Wireless Printers, Scales

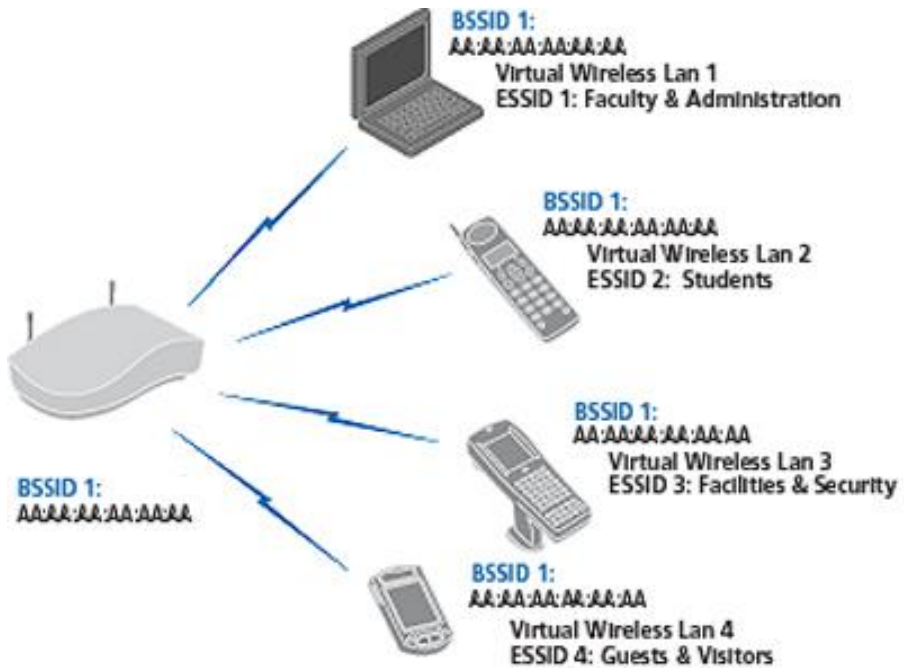
WLAN Switch

- 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.

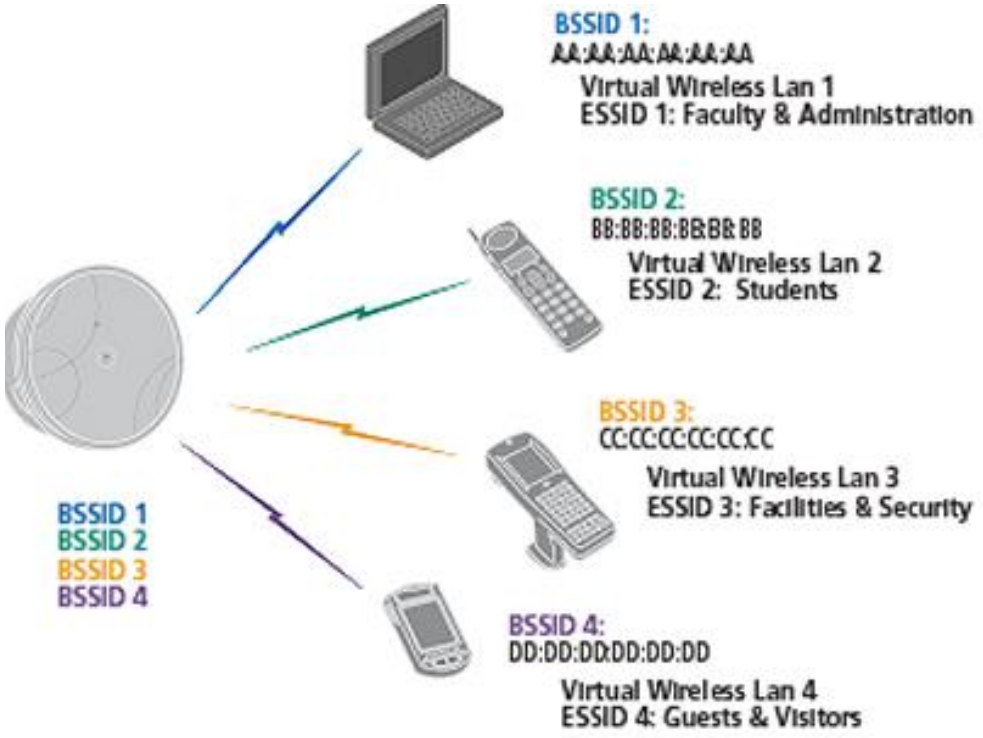
Thin APs

- 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



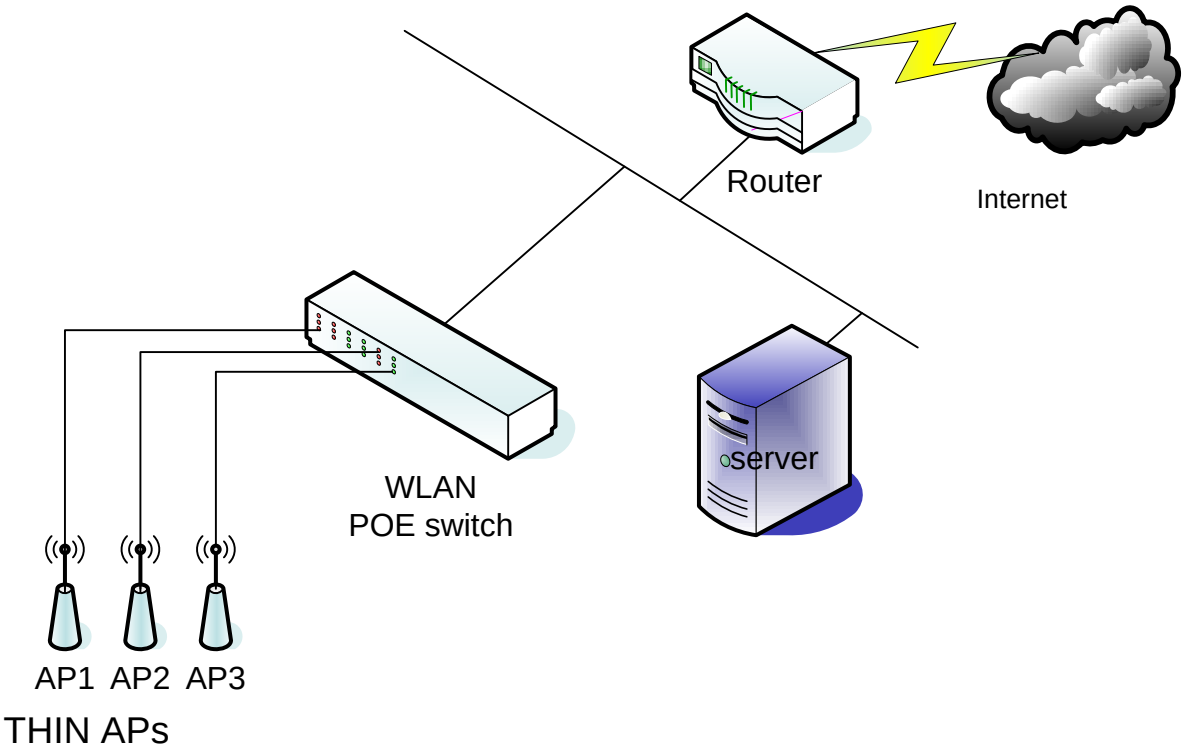
After

Can have *different* policies for each wired segment

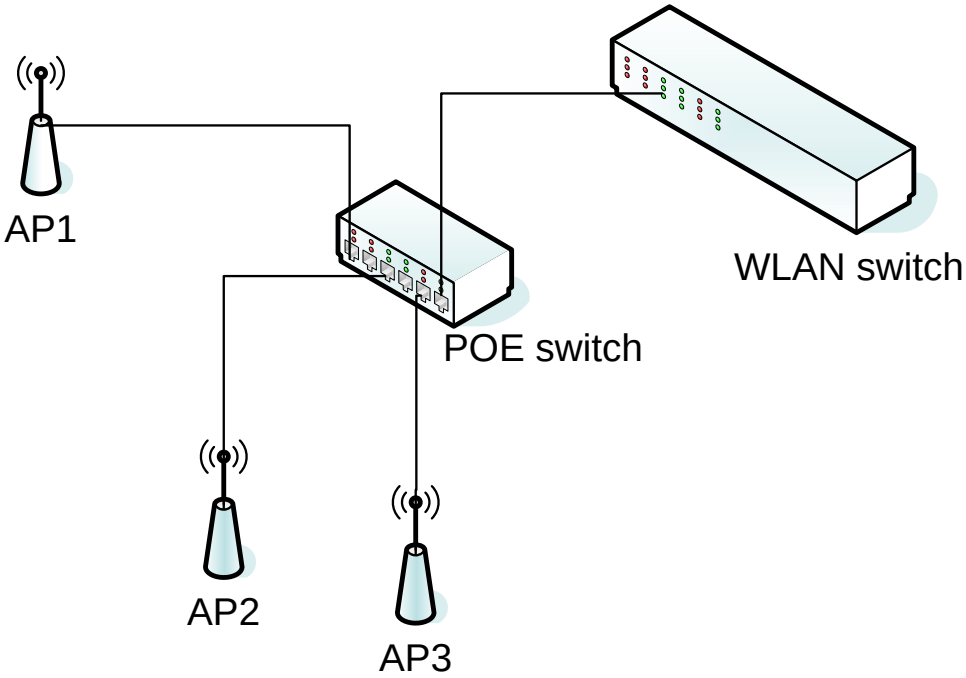
Edge or Core WLAN switch

- 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



THIN APs

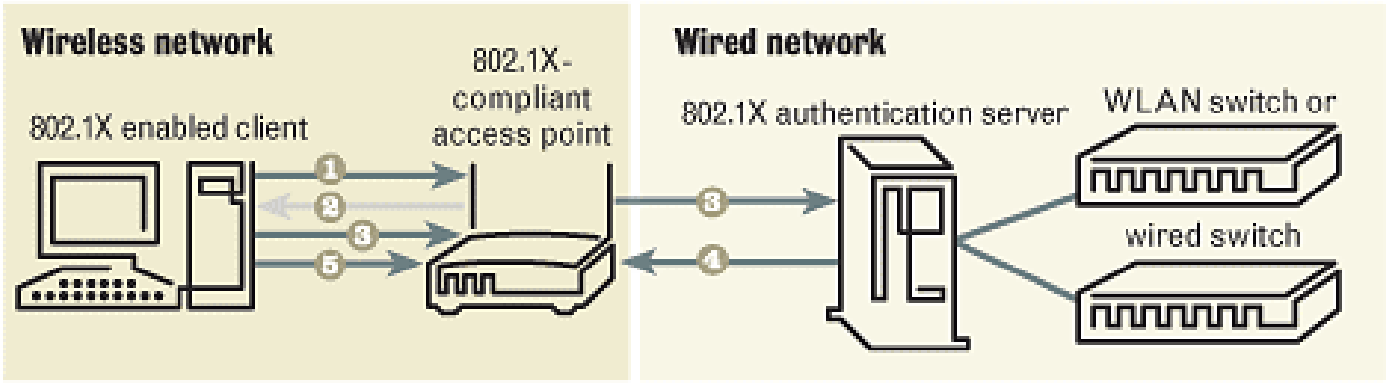
Managed Access

- 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

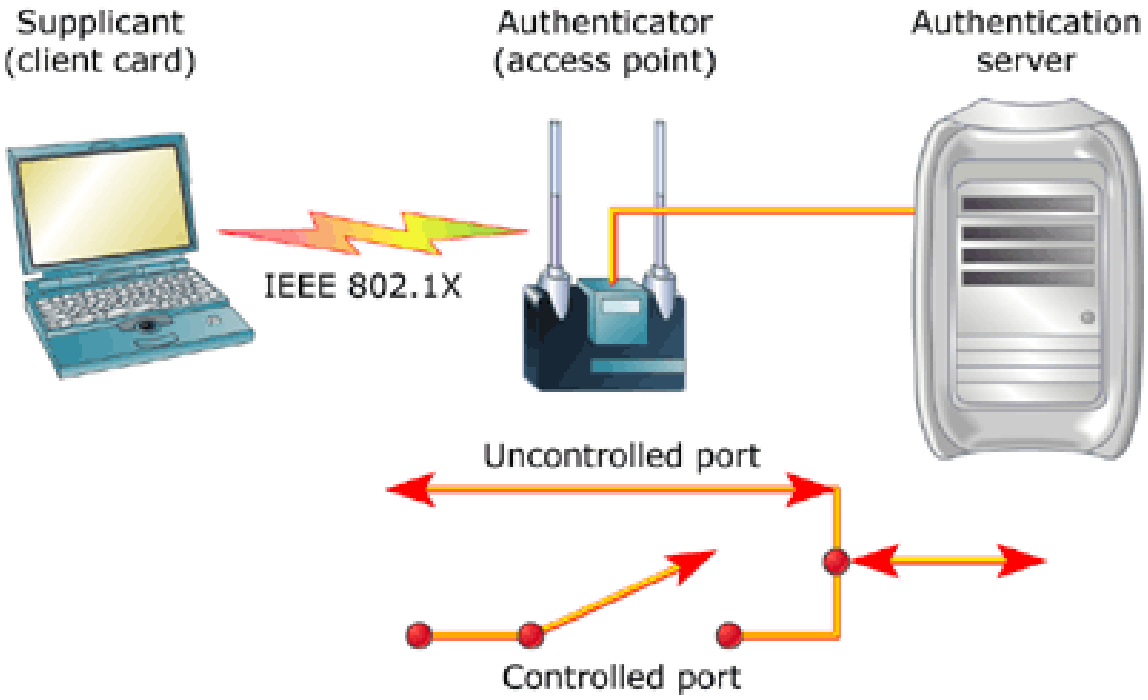
The 802.1X framework

Under 802.1X, users can chose 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.*

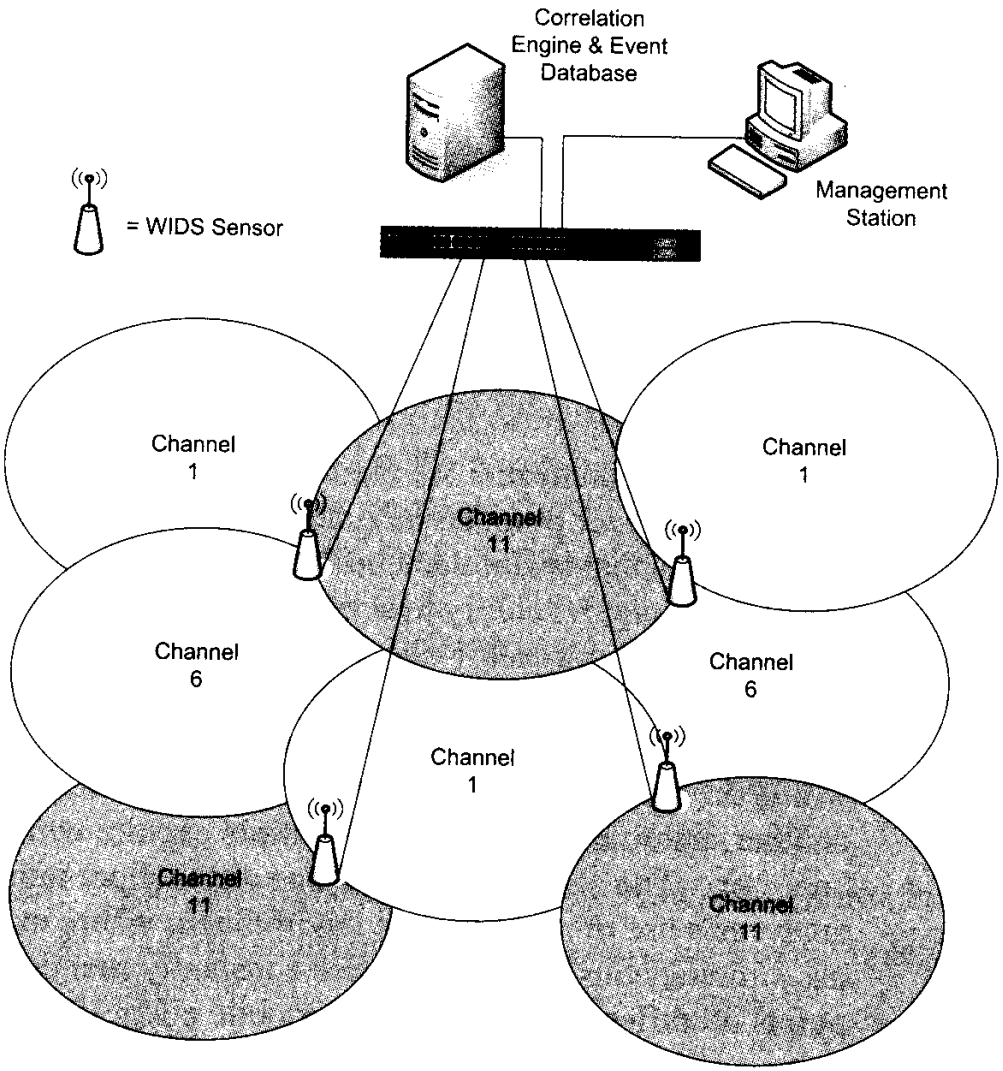
Rogue APs

- 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


Correlation
Engine & Event
Database
Management
Station
= WIDS Sensor
Channel
1
Channel
11
Channel
1
Channel
6
Channel
6
Channel
1
Channel
11
Channel
11

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
- 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