



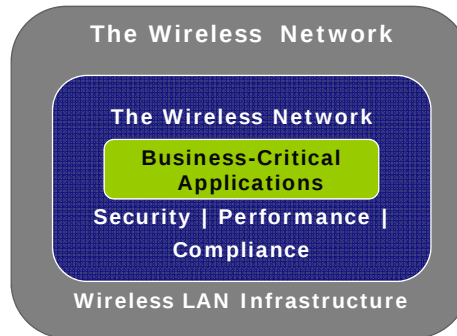
Designing, Securing and Monitoring 802.11a/b/g/n Wireless Networks

The importance of Wireless today

- Increasingly in the Corporate Environment, Wireless is becoming an enabling technology to facilitate workforce mobility.
 - *There are dangers!*
 - Design of the network needs to be correct.
 - Security needs to be considered
 - Monitoring is a must
 - Troubleshooting can be difficult.

Before we start designing!

- Understand what applications and their requirements
 - *Min coverage signal strength*
 - *coverage redundancy*
 - *max noise floor*
 - *interference tolerance*
 - *min data rate*
 - *User capacity*
 - *802.11n*
 - Channel bandwidth (20MHz/40MHz)
 - Operation mode (Legacy, mixed, green field)
 - MIMO streams and MCS`



3

The Design

- This is where the problems start, too frequently!
 - *Suck it and see approach!*
 - If we stick an AP here we should have coverage!
 - If not, we can add another AP
 - Run another GPO in to power it
 - Select any channel for the AP, mainly in 802.11 b/g band
 - » Only 3 non overlapping channels in b/g, Channels 1, 6 and 11
 - Leave the power turned right up
 - » Brute force approach
 - What “a” band?

4

The WiFi design Dork!



- Sticks Access Points to parts of an office layout with Velcro and Cable ties.
- Walks around with a PC looking at signal strength bars and connectivity drop outs.
- Tends to use freebie tools.

WRONG! Where is the science here?

5

The Design

- A structured, scientific approach is required.
 - *Use professional tools!*
 - Survey the environment first
 - Don't go in blind!
 - Plan for the deployment
 - Simulate your coverage
 - Estimate the throughput rates from various locations
 - Generate a professional set of documents covering the deployment.



6

The Survey

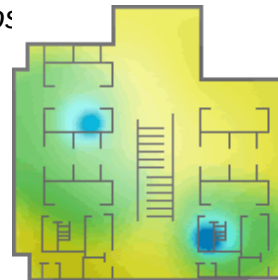
- Key Reasons to do a WLAN Survey
 - Efficient use of WLAN Infrastructure
 - Understand the properties of location
 - Wireless environments change
 - Performance driven applications in the network
 - Their requirements need to be considered.



7

The Survey

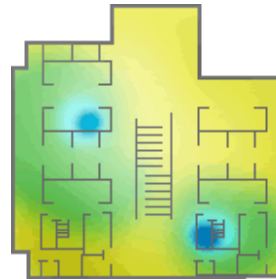
- We need to achieve a complete accurate picture of WiFi Visibility.
 - *Confirm coverage area, see black spots and potential interference areas*
 - *Measure real-world client performance in terms of connection speed, packet loss and end-user capacity*
- Output the result to the client in a clear intelligent manner.



8

The Survey

- Multiple Surveying Methods
 - **Passive Surveys**
 - Overview of the entire wireless environment
 - Includes sources of noise and any wireless signals from neighboring networks
 - **Active Surveys**
 - Measure and map actual end-user network performance
 - Associates to a specific AP
 - See how users will perform in the “real-world”
 - **Iperf Surveys**
 - Measure uplink/downlink end-user WLAN performance
 - Mandatory for 802.11n deployments
 - **Voice Surveys**
 - Validate phone call quality and other voice statistics on the floor map



9

The Survey

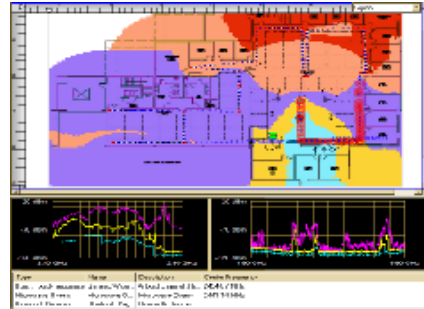
- **Try to achieve a Multi-View of the site**
 - Helps re-use services of a single access point for multiple floors
 - Lower equipment and deployment cost
 - See the effects of APs across multiple floors
 - Compare active surveys to passive designs to improve modeling accuracy.
 - More on modeling shortly.



10

The Survey

- Don't forget a Spectral Analysis
 - *There are things out there in the WiFi frequency range that are not part of the network, but they will affect the networks performance:*
 - Microwave Ovens
 - Hand portable phones
 - Bluetooth Devices
 - Wireless Modems



11

The Survey

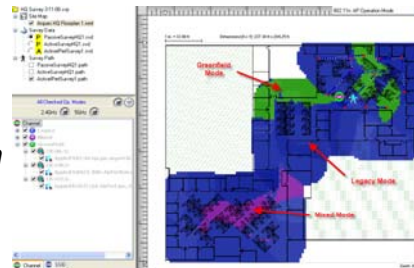
- Deploying an outside network?
 - *Make sure your survey tool accepts GPS data*
 - *Accept Maps in common formats*
 - *Potential export to Google Earth.*



12

The Survey

- **802.11n site survey challenges**
 - 11n Fundamentally Changes WLAN Survey
 - MIMO and many other options that impact performance are location-specific, making signal strength not an accurate indicator of performance
 - 11n Requires Active Surveying
 - Use iPerf functionality to actively test both uplink and downlink performance



13

Planning the Network

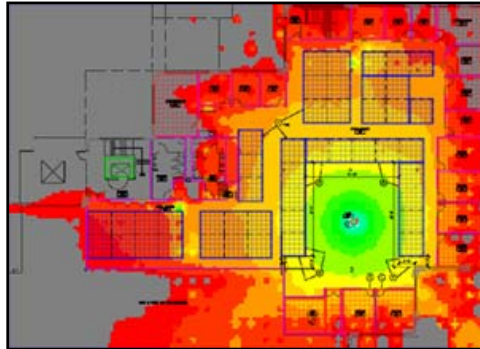
- A complete survey is only half the battle.
 - We now know what is there.
 - What we do not know is how our deployment will work.
 - Using a planning/modeling tool offers many advantages
 - Uses building floor plans
 - Allows simulated placement of APs
 - Allows experimentation with Antenna designs and AP output power settings
 - Allows experimentation on the effects of furniture and office lay outs
 - Generates a 'Heat Map' of Network coverage



14

Planning the Network

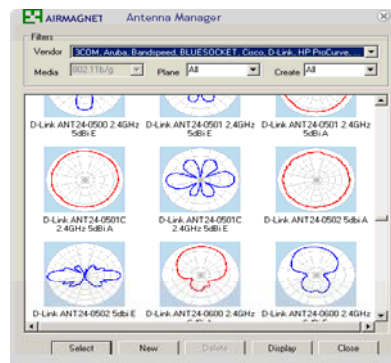
- Using a modeling tool gives many benefits to the designer
 - Optimised AP count
 - Optimised layout and configuration for maximised coverage and performance.



15

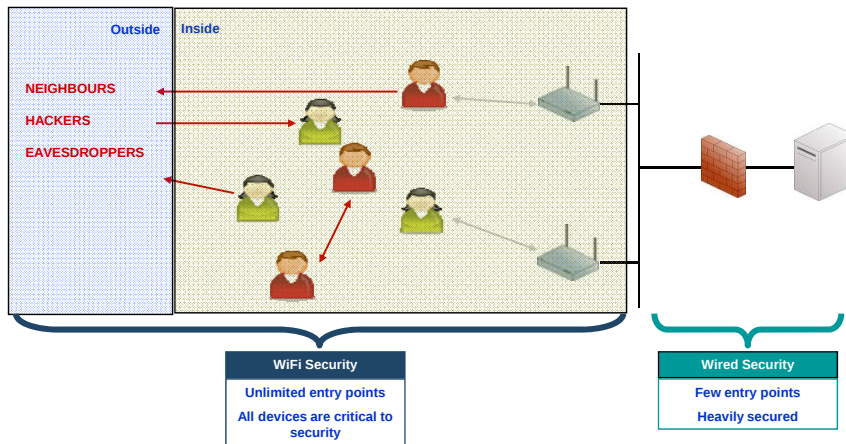
Planning the Network

- Knowing the Antenna Radiation pattern is important.
 - By modifying the antenna we can alter the WiFi coverage of the AP*
 - Most APs come with Omni Directional antennas
 - Black spots can be covered with directional antennas
 - Radiation outside you building can be regulated by changing antenna designs



16

Securing the Network



17

Securing the Network

- Some of the common threats we have to defend the network from:
 - *Rogue AP or Station*
 - *Penetration Attack*
 - Honeypot AP. Man-in-the-Middle, Aircrack, ASLEAP
 - Dictionary Attacks, Hotspotter, etc.
 - *Denial-of-Service Attacks*
 - 802.11/802.1x Protocol Attacks against AP/Station
 - RF jamming against WiFi infrastructure

18

Securing the Network

- Configuration Vulnerability and Policy Violation
 - Enterprise authentication and encryption scheme
 - AP - SSID bcast, Config Changes, Default Config
 - Client – Ad-hoc mode, Exposed WiFi, Unauthorised Association
- WiFi Anomalies
 - After-hour traffic
 - Excessive 802.11 packet fragmentation
 - Netstumber, Wellenwreiter probing
 - Protocol fussing

19

Securing the Network

Requirements for a secure WiFi Network

- Choose security measures appropriate for the network.
- Establish and document Wi-Fi security policies.
- Monitor and enforce 100 % policy compliance.
- Monitor for evolving security vulnerabilities and configuration problems.
- Monitor for wireless intrusions and attack techniques.
- Build in threat response and suppression mechanisms.

20

Are you vulnerable?

?	Intel:BC:05:51	00:19:02:8C:05:51	g	0	?	?	N	2ndAgeNurmonor, desai, ErrData01, desai family
?	Intel:AA:05:D1	00:1F:38:AA:05:D1	g	0	?	?	N	APICA, wlanhop
10	Intel:19:03:ED	00:21:5C:19:03:ED	g	0	?	?	N	Arithony
?	Senao:4E:30:98	00:02:6F:4E:30:98	g	0	Open	?	N	Azure
?	10:30:0:14	00:02:6F:40:27:00	g	0	Open	?	N	Azure
?	Intel:70:A6:F7	00:0E:35:70:A6:F7	g	0	?	?	N	DALMOAK
?	Intel:60:0F:C1	00:1F:3C:60:0F:C1	g	0	Encrypted	?	N	DLINK
?	PS:1E:0F:87:80:8E	PS:1E:0F:87:80:8E	g	0	?	?	N	Hugo2
?	00:23:76:D3:FD:25	00:23:76:D3:FD:25	g	0	?	?	N	Instant Internet, linksys
?	Intel:0A:C7:2E	00:12:F0:0A:C7:2E	g	0	?	?	N	3GEB, Didji-WiFi High Speed Internet 2, Wifzone, linksys
?	PS:0E:30:08	00:13:02:0E:30:08	g	0	?	?	N	3onby
?	00:23:7A:89:A1:8A	00:23:7A:89:A1:8A	g	0	?	?	N	Magicians
?	00:26:FF:08:08:40	00:26:FF:08:08:40	g	0	?	?	N	RSS
4	Intel:56:F7:36	00:19:02:56:F7:36	g	0	WPA-P	?	N	Telstra6014
?	Intel:FC:0F:60	00:0C:35:FC:0F:60	g	0	?	?	N	Unipark
?	00:24:9F:5A:00:A5	00:24:9F:5A:00:A5	g	0	?	?	N	aldgate lawyers, Datac SurfZone.pg
?	Fluke:22:00:00	00:00:17:00:00:00	g	0	?	?	N	default
?	00:04:3E:84	00:18:77:04:3E:84	g	0	?	?	N	linksys

21

Securing the Network

- Choose best practices when looking at Security protocols and Encryption.
 - Two Way Authentication
 - Strong Encryption Algorithms
- Considered best practice at the moment?
 - WPA2/802.11i
 - Uses 802.1X Radius for two way Authentication
 - Strong Encryption



22

Securing the Network

- Comparison between commonly used WiFi Security mechanisms

Standard Name	WEP	WPA	802.11i/WPA2
Encryption Type	WEP	TKIP	CCMP
Cipher	RC4 40 or 128 bits 24 Bit IV	RC4 128 Bits 48 Bit IV	AES 128 Bits 48 Bits IV

More reading:

<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

23

Monitoring the Network

- The network is now installed and in production, we now need to consider monitoring that network.
 - *Who is on my network?*
 - What are they doing?
 - *Are there any new WiFi networks coming up?*
 - Source of interference and performance drop
 - *Am I under Attack?*
 - Who is doing it and where are they?
 - *Do I have a rogue AP?*
 - Where is it and who did it?

24

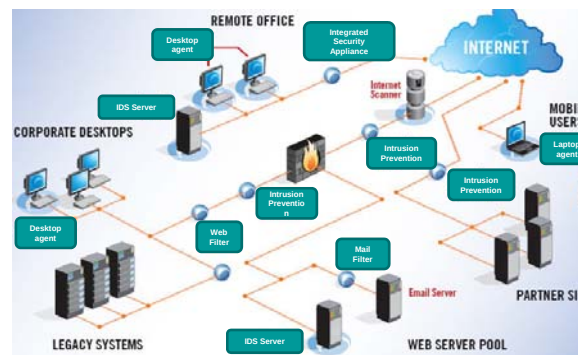
Monitoring the Network

- Remember, the infrastructure **can not** monitor itself. Self protection is NOT effective, you need to be pro-active.
 - Network infrastructure is designed to effectively move and control protocol traffic and application data.
 - Network monitoring equipment is purpose built to analyse traffic behaviour.
 - Points of presence – effective network monitoring requires inspection where problems occur.

25

Monitoring the Network

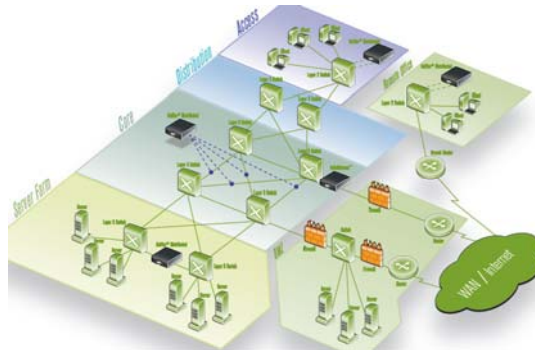
Network IDS – Effective, Universally Accepted Overlay Architecture
For WiFi – WIDS – Wireless Intrusion Detection System.



26

Monitoring the Network

Distributed Traffic capture – Effective, Proven Overlay Architecture
Great compliment to Network IDS and Wireless IDS.



27

Monitoring the Network

- We also need to consider the WiFi Networks operating mode.
 - **Casual** – WLAN used for complimentary connectivity to enable employee mobility, guest internet access, hotspot service.
 - **Business Critical** – WLAN used to support critical real-time business applications.
 - **Intense Applications** – WLAN used for applications / devices with strong QoS requirements.
 - **Heterogeneous System** – WLAN devices from several vendors blended into multi-function application platform.

28

Monitoring the Network

- With each operating mode, there are issues to be addressed
 - Casual – Comprehensive WIDS
 - Business Critical – PLUS uptime monitoring, remote troubleshooting.
 - Intense Applications – PLUS performance optimisation monitoring.
 - Heterogeneous System – PLUS detailed protocol state analysis.

29

Monitoring the Network

Critical Features				
	WIDS / WIPS	Uptime Monitoring	Performance Optimisation Monitoring	Protocol state analysis
Casual	NEED	NICE	NICE	NICE
Business Critical	NEED	NEED	NICE	NICE
Intense Applications	NEED	NEED	NEED	NICE
Heterogeneous System	NEED	NEED	NEED	NEED

30

Monitoring the Network

- Important Monitoring recommendations
 - *24/7 dedicated overlay system*
 - You don't miss a thing, part time AP based... you may miss something critical
 - *Look for Historical data collection*
 - Gives forensic post analysis capability, you didn't have to be watching the screen when the event happened.

31

Monitoring the Network

- Important Monitoring recommendations
 - *Very Deep WIDS Event Detection capability*
 - Find every WiFi attack and hack currently known
 - *Look for comprehensive reporting*
 - The "Boss" report, regulatory compliance – PCI, SoX
 - *Ability to integrate with existing solutions*
 - Enterprise NWM system

32

Monitoring the Network

- Important Monitoring recommendations
 - *Be able to detect, locate and remotely remediate rogue APs and client devices.*
 - Wireless Blocking, wired tracing and port killing
 - *For an Enterprise system, to be remotely accessible*
 - Troubleshoot and investigate from Head Office
 - *Spectrum Analysis Capability*
 - It may not be a WiFi problem

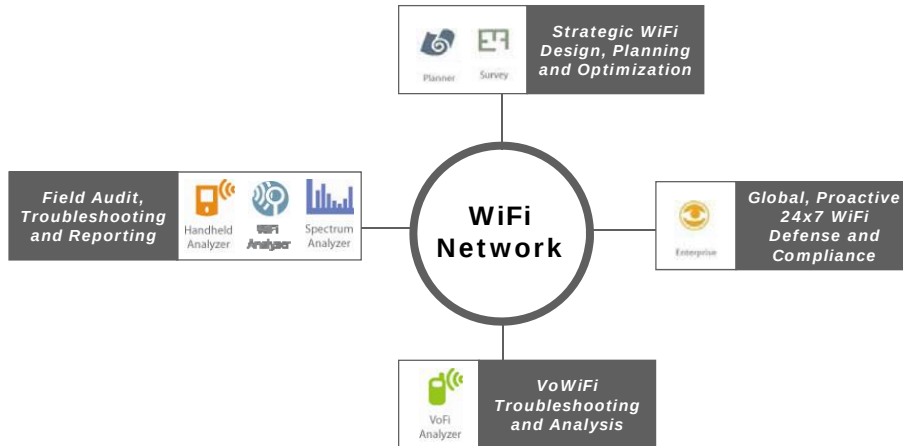
33

In conclusion

- Wireless is becoming an important part of today's Enterprise Network fabric.
 - *You need to check the environment before deploying your solution.*
 - *Your solution should be designed scientifically for not only today's requirement but also for the future.*
 - *Monitor your wireless network just as you would your wired network.*

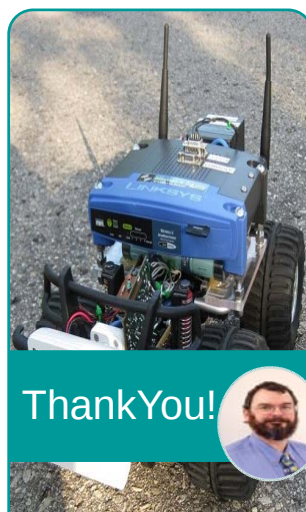
34

Life Cycle of WLAN



35

Questions?



Is your WiFi Network safe from this?

36