



How To Plan, Install, and Secure Wireless Networks

David Black

President/CEO

Insource Technology Corporation

(281) 774-4150

david.black@insource.com

www.insource.com

INSOURCE
TECHNOLOGY

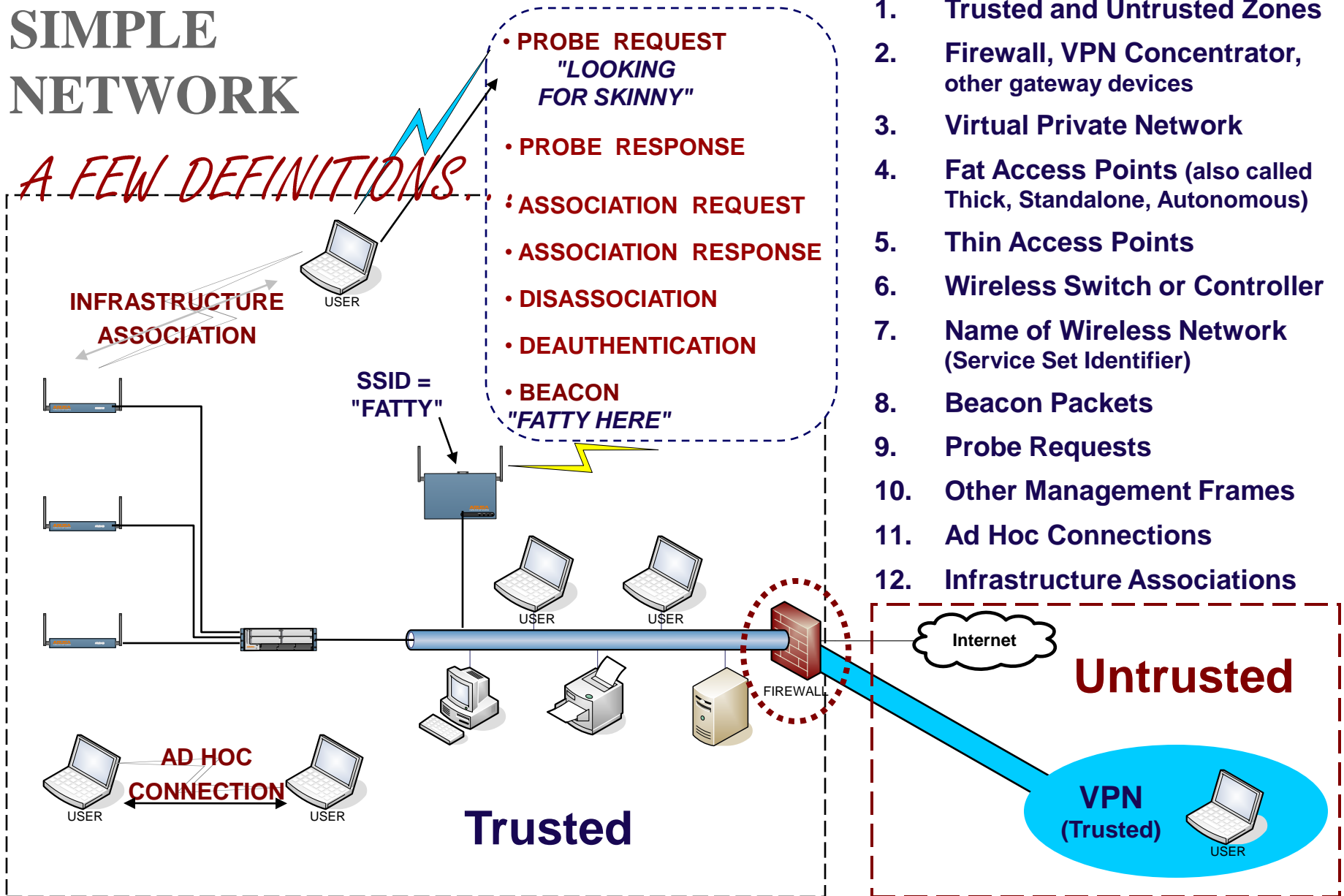


INTERESTED IN WIRELESS LANs?

- There's no shortage of advice
- A lot of it is incomplete, biased, and sometimes just flat-out wrong
 - Manufacturers
 - Trade press
 - Self-proclaimed experts

SIMPLE NETWORK

A FEW DEFINITIONS





PLANNING YOUR WIRELESS NETWORK

- ✓ 1. Make sure your business needs it
 - Doing wireless right takes more work than most people expect
- ✓ 2. Understand security
 - The cost of what you mitigate
 - And the residual risk

- ✓ 3. Familiarize yourself with upcoming standards
 - Decide: proceed or wait

Plan the rest of the system after you've done these three things



CAN WLANs BE JUST AS SECURE AS WIRED?

- YES, but...
 - "Safe" means "safe today"
- All networks are vulnerable to interception, jamming, and spoofing
 - In wired-networks, access to cables/equipment is restricted
 - Many vulnerabilities remain purely theoretical
- With wireless, you do not have control of physical access



2. WIRELESS SECURITY

1. Privacy and Message Integrity
2. Authentication
3. Intrusion Detection and Prevention
4. Endpoint Protection
5. Policies and Enforcement
6. User Education and Awareness

STREET JOURNAL.

MAY 4, 2007 - VOL. CCXLIX NO. 104 ***** \$1.00

FOXX 56 3888.84 ▲ 0.4% 10-YR TREAS ▼ 7/32, yields 4.674% OIL \$53.19 ▼ \$0.49 GOLD \$681.80 ▲ \$9.50 EURO \$1.3558 YEN 120.41

As Market Cools,
Home Buyers
Seek a Way Out
Builders Face Lawsuits

BREAKING THE CODE

**How Credit-Card Data
Went Out Wireless Door**

*In Biggest Losses Theft
Retailer's Weak Security
Lost Millions of Numbers*

By JOSEPH PEREIRA

Big Hacks
Some major breaches of credit- and debit-card
data in the past three years:
■ B2: Wholesale Club Inc., March 2004
40,000 cards compromised
■ DSW Retail Ventures Inc., March 2005

60 MINUTES Nov. 25, 2007

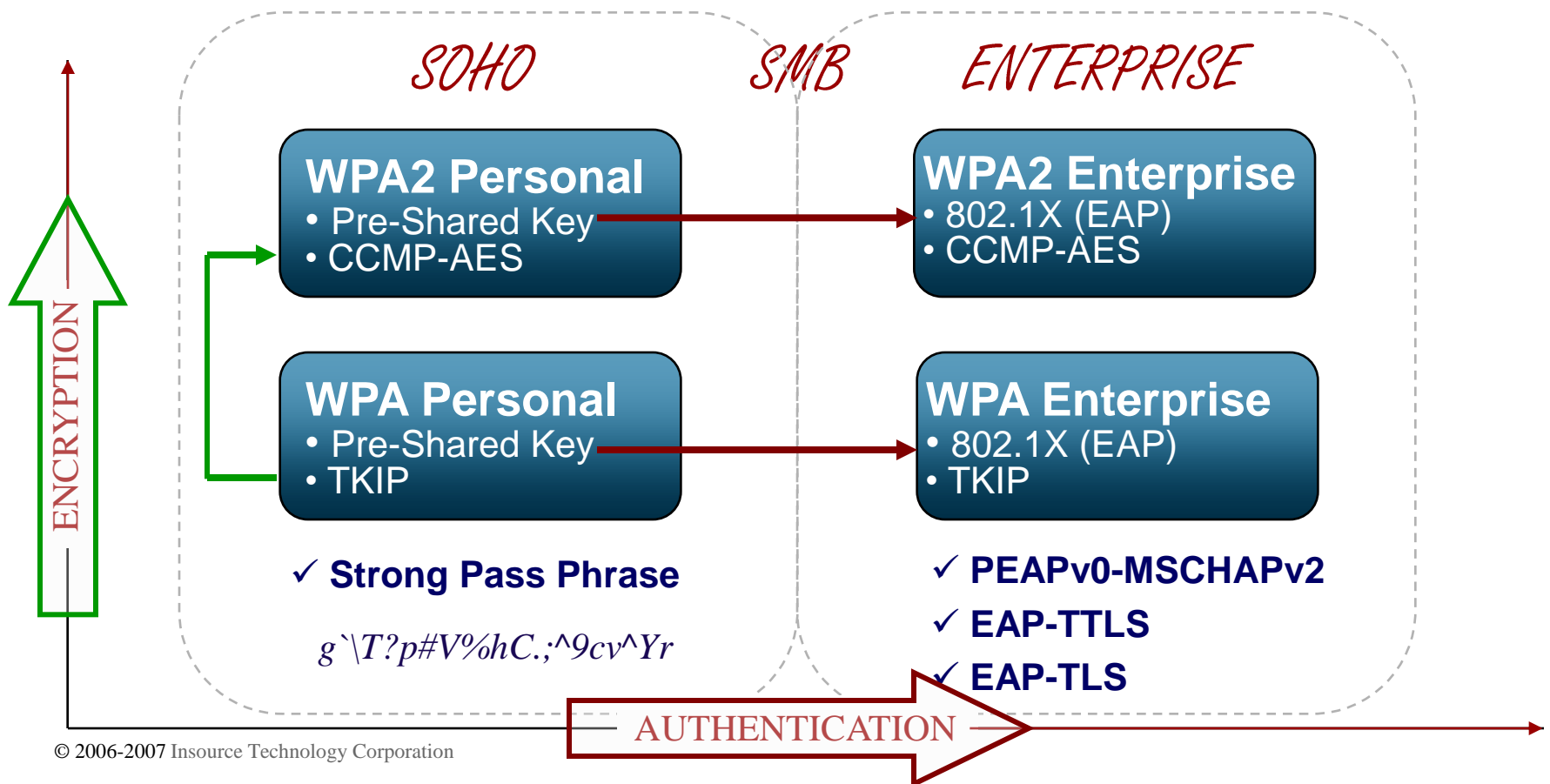


T.J-maxx **Marshalls**

- Initially penetrated a wireless network used by handhelds
- Next, gained access to main corporate systems
- Undetected for 18 months
- At least 46M credit/debit cards and 451,000 identities stolen
- Numerous mistakes
- Several lawsuits expected
- Projected to cost upwards of \$1B



WIRELESS SECURITY





WIRELESS SECURITY


INEFFECTIVE

- × WEP
- × MAC Filtering
- × Dynamic WEP

WASTEFUL

- × Hiding SSID
- × Static IP
(or restricting DHCP)
- × Containing RF
(AP location,
special antennas, etc)

DANGEROUS

- × LEAP 
- × EAP-FAST
(anon DH mode)



WIRELESS SECURITY

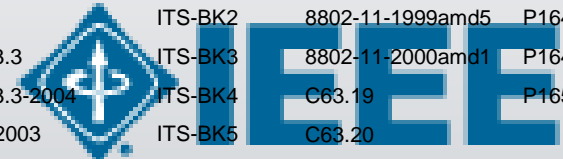
- The future track record should be better
 - WPA and WPA2 were extensively vetted by cryptologists
 - But the game of cat-and-mouse will be never-ending
 - New vulnerabilities will be discovered
 - Exploits will be developed for some
 - Hacking tools will continue to improve
- "Safe" means "safe today"



3. UPCOMING STANDARDS

- Standards help the wireless industry and the market
 - Lower costs, interoperability, transportable skills
 - Eliminate proprietary solutions and vendor lock-in
 - Provide a roadmap of where the industry is headed
- Most are developed by the Institute of Electronics and Electrical Engineers

802.11	802.11k	802.15.4	802.16a
802.11.2	802.11-ma	802.15.4-2003	802.16a-2003
802.11-1997	802.11n	802.15.4a	802.16b
802.11-1999	802.11p	802.15.4b	802.16c-2002
802.11a	802.11r	802.16	802.16-Con2
802.11b-1999	802.11s	802.16.1	802.16-Con3
802.11b-Cor1	802.11u	802.16.1b	802.16d
802.11d	802.11v	802.16.2	802.16e
802.11d-2001	802.15.1-2005	802.16.2-2001	802.16f
802.11e	802.15.1-2005	802.16.2-2004	802.16g
802.11f-2003	802.15.2	802.16.2a	802.16h
802.11g-2003	802.15.2-2003	802.16.3	802.20
802.11h-2003	802.15.3-2003	802.16-2001	802.21
802.11i-2004	802.15.3a	802.16-2004	802.22
802.11j-2004	802.15.3b	802.16-2004-Cor1	1528
1529	ITS-BK2	8802-11-1999amd5	P1640.2
1073.3.3	ITS-BK3	8802-11-2000amd1	P1640.5
1073.3.3-2004	ITS-BK4	C63.19	P1654
1528-2003	ITS-BK5	C63.20	
1528a	ITS-BK6	C95.1b-2004	
1802.16.2	P1073.0.1.1	C95.1b-2004	
8802-11-1999	P1451.5	ITS-BK1	
8802-11-1999amd4	P1612		



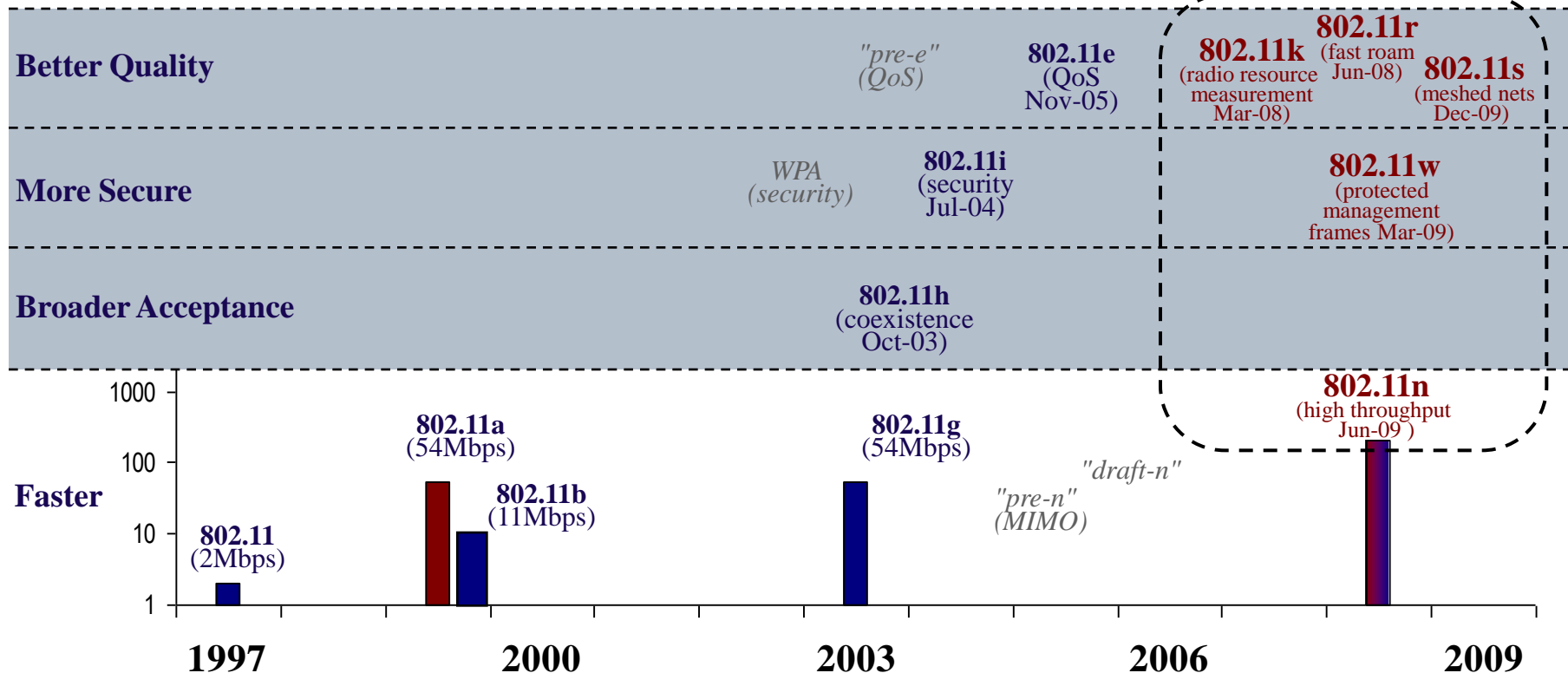


REASONS FOR ALL THESE STANDARDS

- FASTER
- BETTER QUALITY
- MORE SECURE
- BROADER ACCEPTANCE
- Enhancements to achieve higher data rates
- Enhancements to improve Quality of Service (required by time-sensitive applications)
- Enhancements for improved authentication, data privacy, message integrity
- Enhancements to comply with regulatory requirements of various countries (coexistence, frequency, power)



TIMELINE FOR 802.11 EXTENSIONS





802.11n (HIGH THROUGHPUT)

- Higher data rates and improved performance in pure 11n environments
 - 100+ Mbps throughput from advanced modulation, protocol improvements, and frame aggregation
 - Even higher throughput from channel bonding (if allowed)
 - Extended range and reduced interference by utilizing MIMO
 - Multiple independent radios & antennas
- Support for legacy hardware (802.11a, b, g)
- Approval expected mid-2009



802.11s (MESHED WLANs)

- "Meshing" (cell-to-cell transport) functionality added to access points
- "Multi-hop" (client-to-client transport) allows clients to reach out-of-range AP
- Enables traffic to route around failed nodes
- Parameterized QoS, load balancing, improved reliability and range of wireless networks
- Simplified deployments (AP placement not as critical)
- Approval expected late-2009



4. COVERAGE AND CAPACITY

- Define the desired coverage areas
 - Start small, limit to common areas
- Determine the basic needs in those areas
 - Quantity and types of users
 - Desired bandwidth per user
- Rules-of-thumb are ok for rough estimates (eg: one AP per 5,000 sq.ft. or 20 users)
 - But it's better to construct your own model





COVERAGE AND CAPACITY

TYPE	EXAMPLE	BANDWIDTH / USER (Mb/s)
Store / Warehouse Personnel	Bar code scanning of inventory	0.1
Guests	Internet access, POP3	0.5
General Office Workers	Email, light file and print sharing	1.0
Power Users	Heavy file and print, CAD, video, imaging	3.0+

Examples



COVERAGE AND CAPACITY

TYPE	TOTAL BANDWIDTH (Mbps)	AVAILABLE BANDWIDTH (Mbps)
802.11b	11	5
802.11a	54	23
802.11g	54	23
802.11b/g mixed	54 (g)	8 or 12 (g)



USERS PER ACCESS POINT

Use these

TYPE	802.11b/g @ 8 or 12 Mbps	802.11g @ 23 Mbps	802.11a @ 23 Mbps
------	-----------------------------	----------------------	----------------------

Store Personnel
@ 0.1Mbps

Guests
@ 0.5Mbps

General Office
@ 1Mbps

Power Users
@ 3Mbps

Use your own



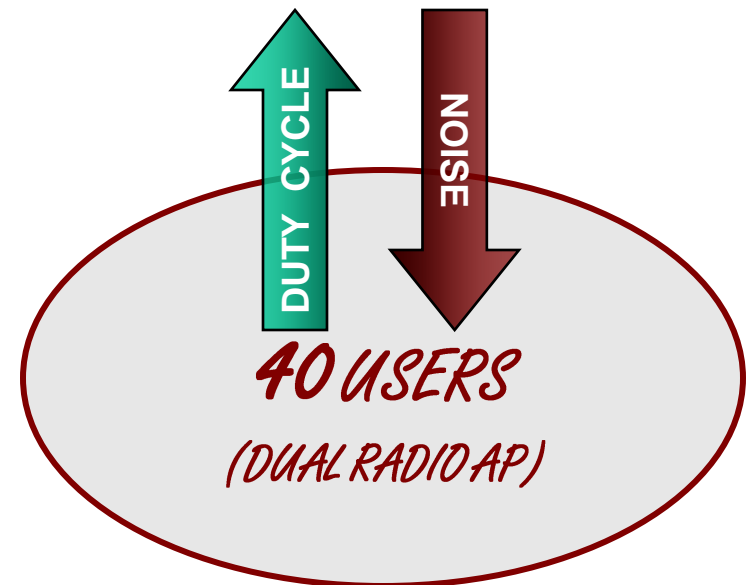
USERS PER ACCESS POINT

TYPE	802.11b/g @ 8-12Mbps	802.11g @ 23Mbps	802.11a @ 23Mbps
Store Personnel @ 0.1Mbps	80 or 120	230	230
Guests @ 0.5Mbps	16 or 24 10-15 (70%Emp / 30%Gst)	~ 40 USERS <i>PER DUAL-RADIO AP</i>	46 30 (70%Emp / 30%Gst)
General Office @ 1Mbps	8 or 12		23
Power Users @ 3Mbps	3 or 4	8	8



DUTY CYCLE AND NOISE

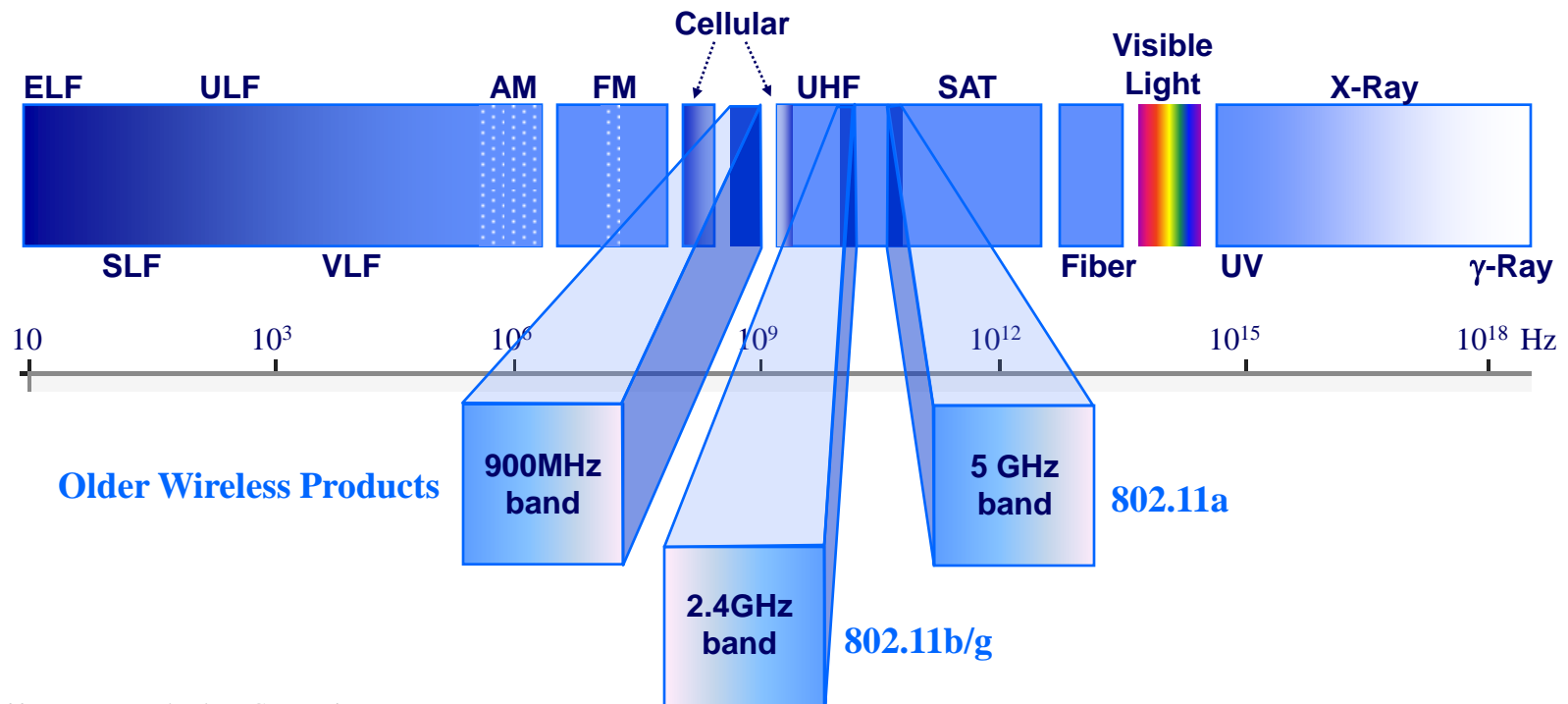
- "Not everyone will be using the network at the same time. Can I increase the number?"
- Maybe, but for now assume that any gain arising from duty cycle
- Will be offset by losses to interference





INTERFERENCE

- Unlike radio, TV, or cellular, 802.11 uses unlicensed public spectrum





INTERFERENCE

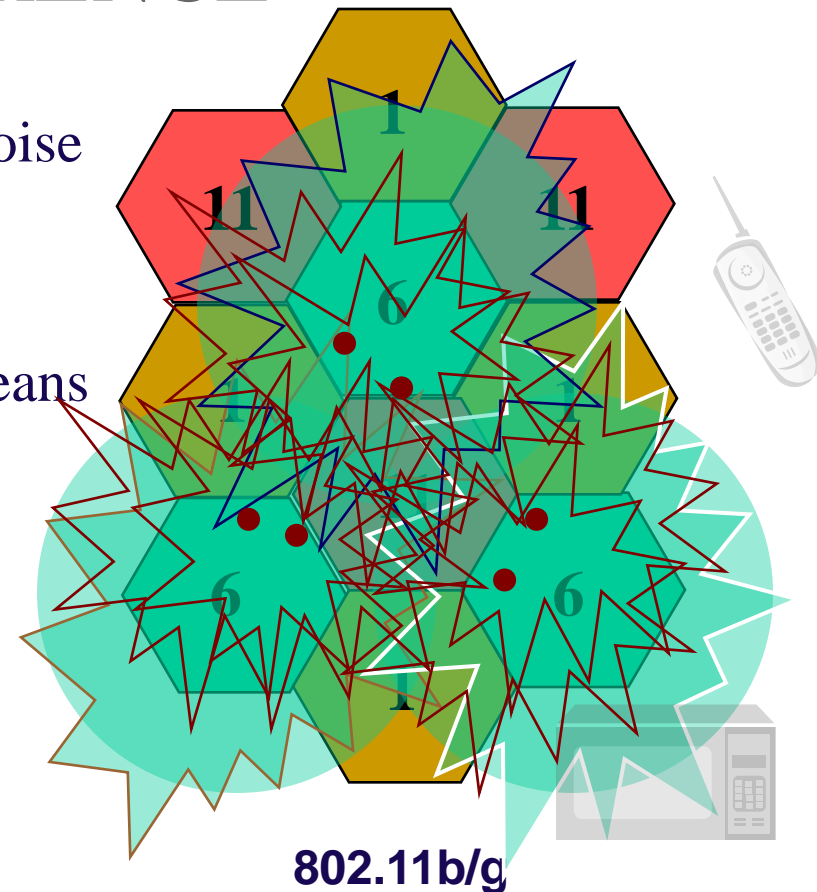
- Unlike radio, TV, or cellular, 802.11 uses unlicensed public spectrum
- Other non-802.11 devices use the same spectrum
- And this presents a problem – particularly in the heavily congested 2.4GHz band
 - Cordless phones, Microwave Ovens, other 2.4GHz devices





CO-CHANNEL INTERFERENCE

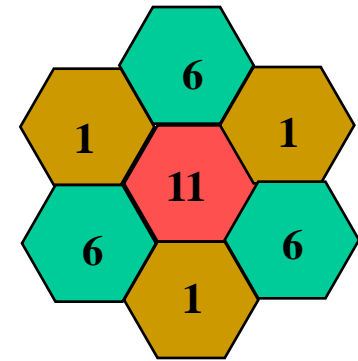
- The single most significant source of noise
 - Other AP's on the same channel
- Adequate signal at a cell's perimeter means signal well beyond that cell's perimeter
- AP's can hear at greater distances than they transmit
- Wireless clients also contribute





CO-CHANNEL INTERFERENCE

- Random bursts of static, not continuous jamming
- Has the same affect as collisions
- Becomes a much bigger problem over time
 - As the number of users increases
 - As bandwidth needs increase
 - As cells are divided into smaller cells that are packed even closer together

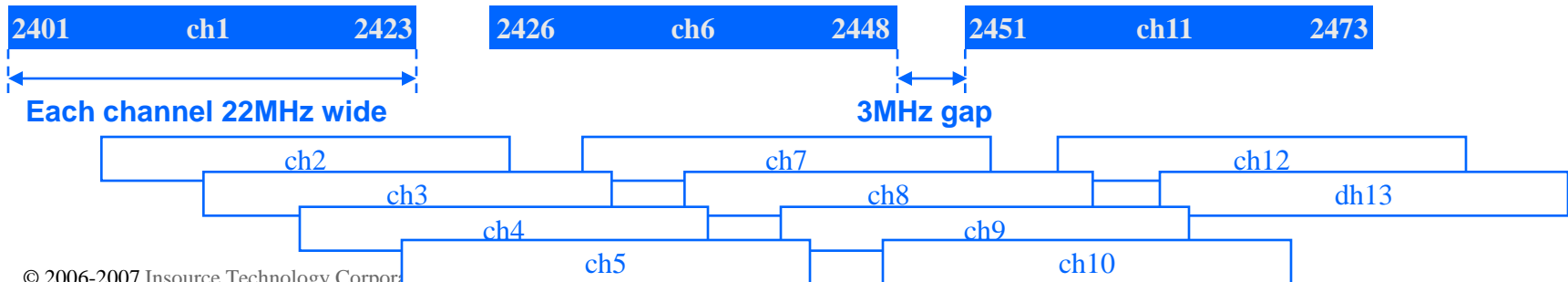


802.11b/g



802.11b CHANNELS AND POWER

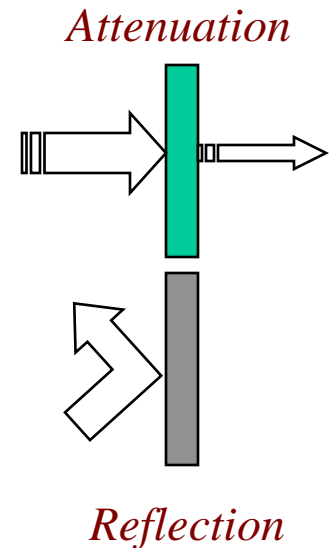
Channel	1	2	3	4	5	6	7	8	9	10	11	12	13	14	Max Power (mW)
Frequency (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484	2.2 / 6 / 12dB
Americas & ANZ	•	•	•	•	•	•	•	•	•	•	•	-	-	-	100 / 100 / 100
Europe	•	•	•	•	•	•	•	•	•	•	•	•	•	-	50 / 30 / 5
France	-	-	-	-	-	-	-	-	•	•	•	•	•	-	50 / 30 / 5
Israel	-	-	•	•	•	•	•	•	•	-	-	-	-	-	50 / 30 / 5
China	•	•	•	•	•	•	•	•	•	•	•	-	-	-	5 / 0 / 0
Japan	•	•	•	•	•	•	•	•	•	•	•	•	•	•	30 / 30 / 0
ROW	•	•	•	•	•	•	•	•	•	•	•	•	•	-	50 / 30 / 5





CAPACITY AND COVERAGE

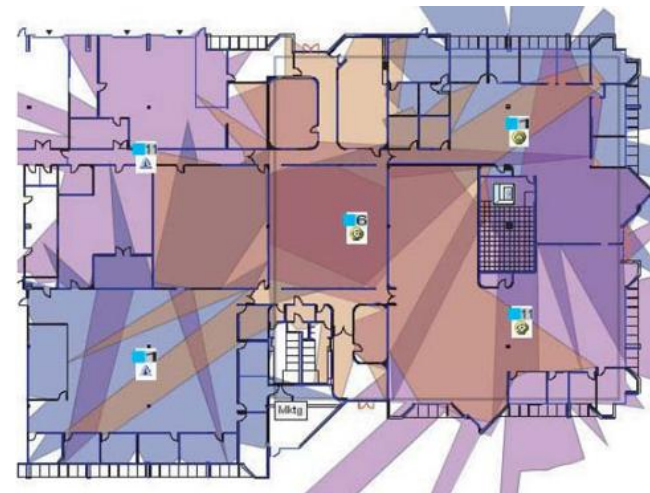
- Several factors complicate coverage planning
 - Quantity, height, composition of walls
 - Metal structures such as studs, beams, elevator cores, air handlers, blinds
 - Other external/internal sources of interference in the 2.4GHz band
- RF Modeling Software can help
- Physical site-survey is generally recommended, particularly to assess noise





SITE SURVEY

- Physical Site Survey
 - Deploy test APs, collect data, analyze
 - Fingerprint the site's RF propagation
- RF Modeling Software
 - Requires very detailed site knowledge
 - Or physical survey results to calibrate
 - Once calibrated, a fairly good "what-if" tool





5. EQUIPMENT SELECTION

- Access Points:

SOHO
Consumer

ENTERPRISE
Commercial

- Radios:

SMB
bg single radio

a + bg dual radio

- Architecture:

Fat AP

Thin AP +
Controller(s)

*NO PRE-N, DRAFT-N, ETC.
NO SUPER-THIS, TURBO-THAT...
PLAIN OLD B/G IS FINE*

*AVOID 802.11N FOR NOW
(WAIT FOR THE STANDARD AND
DEPLOY IN 5GHz BAND ONLY)*



✓ *RECOMMENDED*

COMMERCIAL GRADE AP's

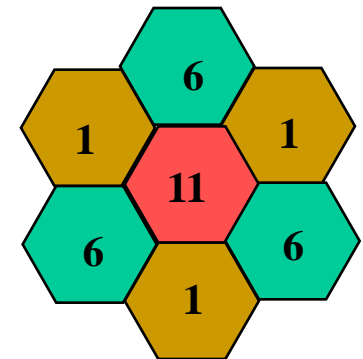
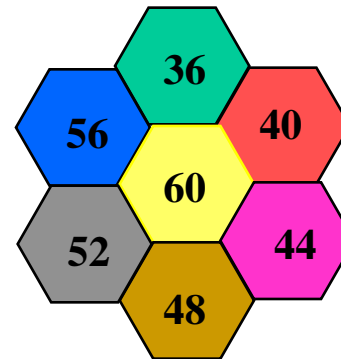
- Designed to work as a system (eg: reliable roaming)
- Better radios, multiple radios, more control over the radios
- Multiple SSID's, encryption, and authentication methods; VLAN tags
- More powerful hardware
 - Handle more users and more demanding encryption methods
- Plenum rated (more secure, more esthetically pleasing)
- Broader selection of antennas
- Power Over Ethernet
- Intrusion Detection functionality (impacts WLAN performance)
- Auto-power and auto-channel selection



✓ *RECOMMENDED*

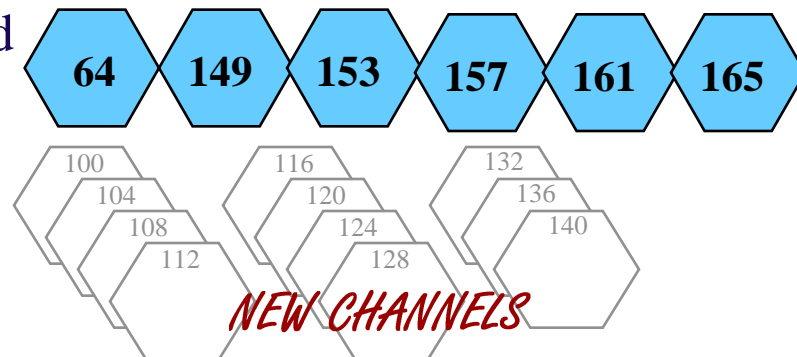
EQUIPMENT SELECTION

- 802.11a
 - Significantly less interference
 - Plenty of channels
 - Performance equal to pure 11g in a noise-free environment
 - But "a" smokes "g" in real-world environments
 - Ignore critics who cite higher cost and decreased range



802.11a

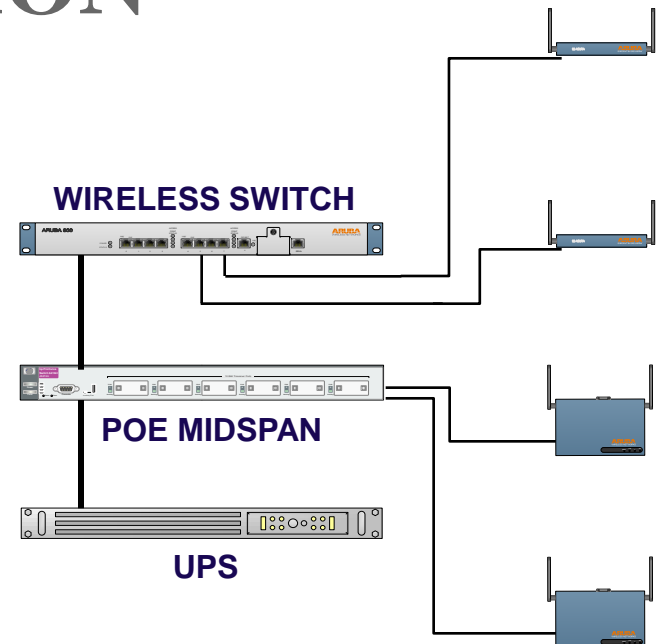
802.11b/g





EQUIPMENT SELECTION

- Power over Ethernet
 - Simplifies AP installation, adds, moves, changes
 - Easier to reset or shut down individual AP's
 - Allows for UPS Backup
 - Managed POE worth the extra cost

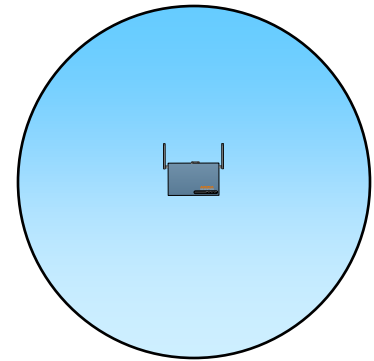




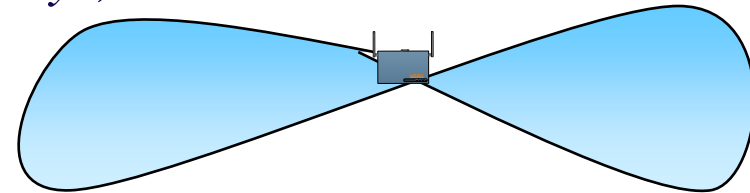
ANTENNA SELECTION

- Omni (general purpose 360°)
 - Gain determines ceiling/floor penetration
- Di-Pole
 - Optimized for max front/back and min side/side
- Patch, Panel, Sector
 - Various gains and beamwidths from 60 to 180°

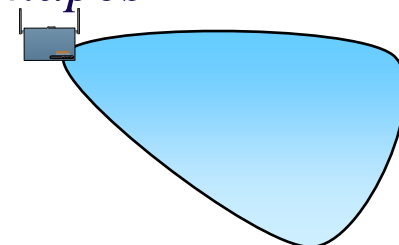
- *General office*



- *Hallways, etc*



- *Corners, ends, odd shapes*

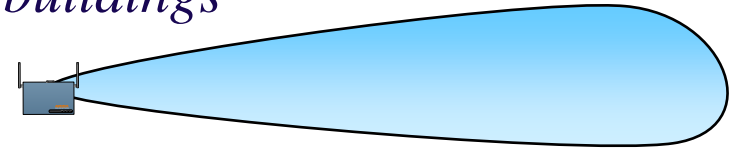




ANTENNA SELECTION

- Yagi, Backfire
 - Long range, 20-30° beam width
 - Thousands of feet
- Parabolic
 - Very long range, 5-10° beam
 - Miles
 - Requires very solid mounting

- *Point-to-point bridging between buildings*

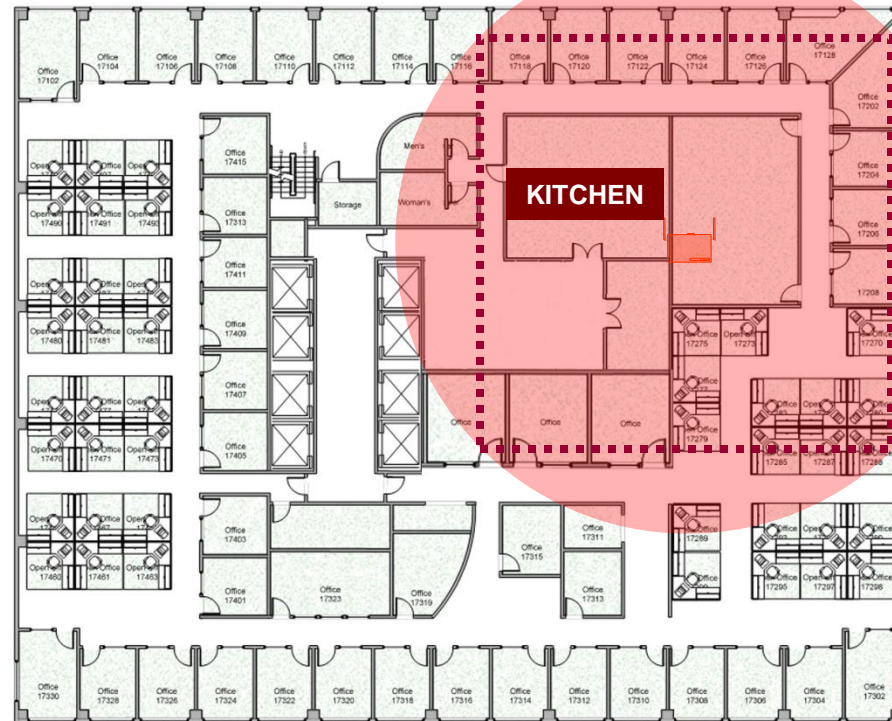


- *Point to point backhaul between towers*





COMMON AREA 802.11abg



AP#1
7,500 sqft
20+ users
CH 1
CH 52
OMNI



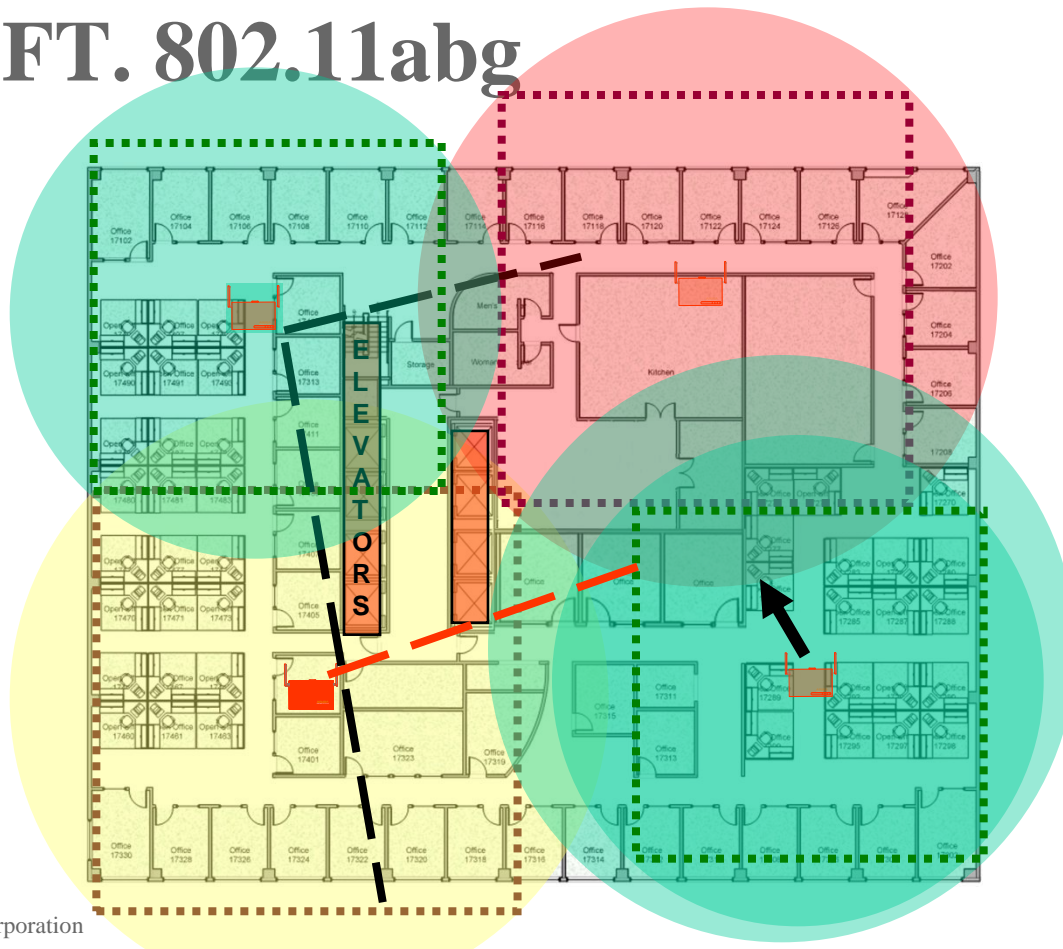
20,000 SQ.FT. 802.11abg

AP#4
5,500 sqft
21 users
CH 6
CH 157
OMNI

AP#3
7,500 sqft
25 users
CH 11
CH 149
OMNI

AP#1
7,500 sqft
20+ users
CH 1
CH 52
OMNI

AP#2
5,500 sqft
22 users
CH 6
CH 60
OMNI





20,000 SQ.FT. 802.11abg

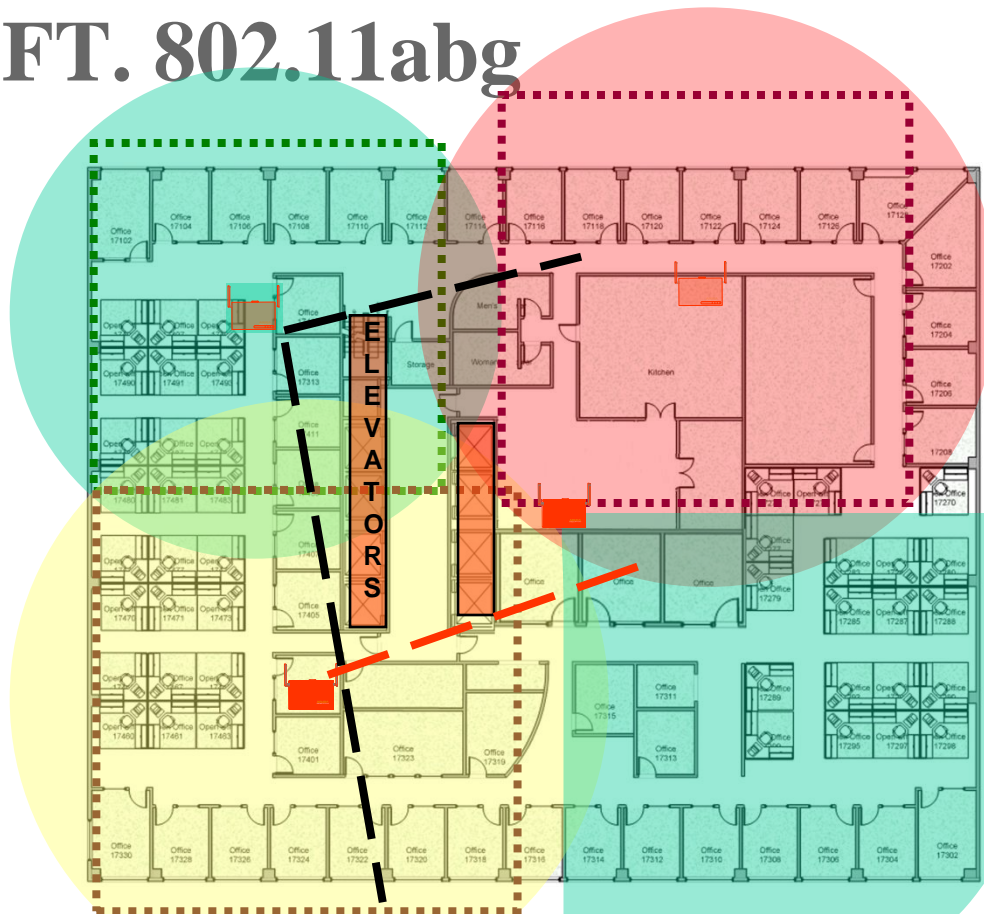
AP#4
5,500 sqft
21 users
CH 6
CH157
OMNI

AP#3
7,500 sqft
25 users
CH 11
CH 149
OMNI

AP#1
7,500 sqft
20+ users
CH 1
CH 52
OMNI

AP#2
5,500 sqft
22 users
CH 6
CH 60

PATCH 90



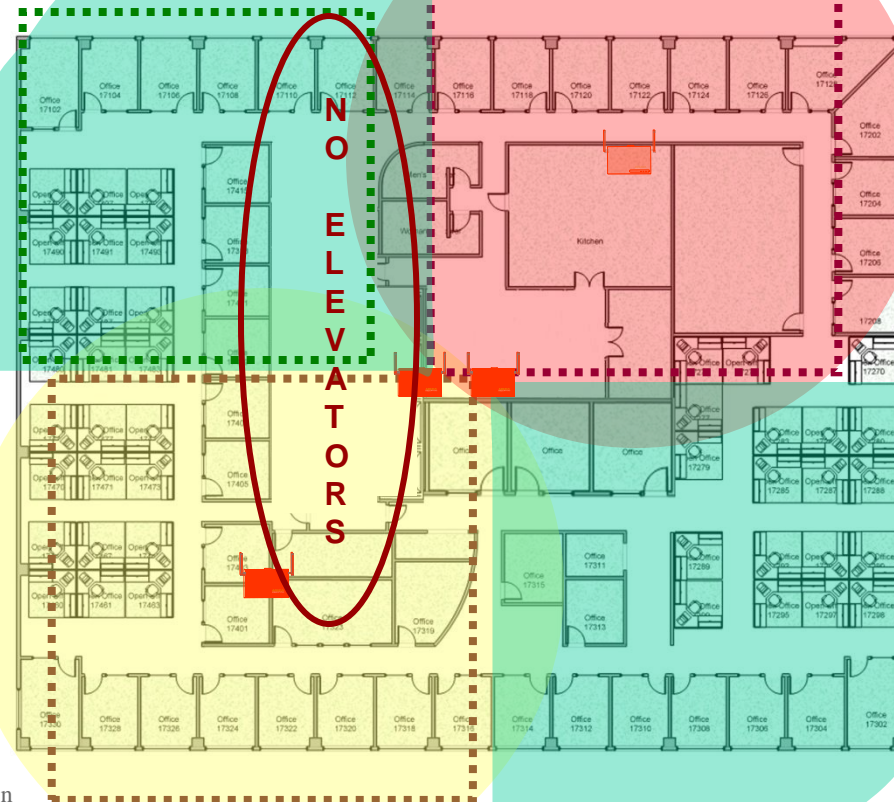


20,000 SQ.FT. 802.11abg

AP#4
5,500 sqft
21 users
CH 6
CH 157

PATCH 90

AP#3
7,500 sqft
25 users
CH 11
CH 149
OMNI



AP#1
7,500 sqft
20+ users
CH 1
CH 52
OMNI

AP#2
5,500 sqft
22 users
CH 6
CH 60

PATCH 90



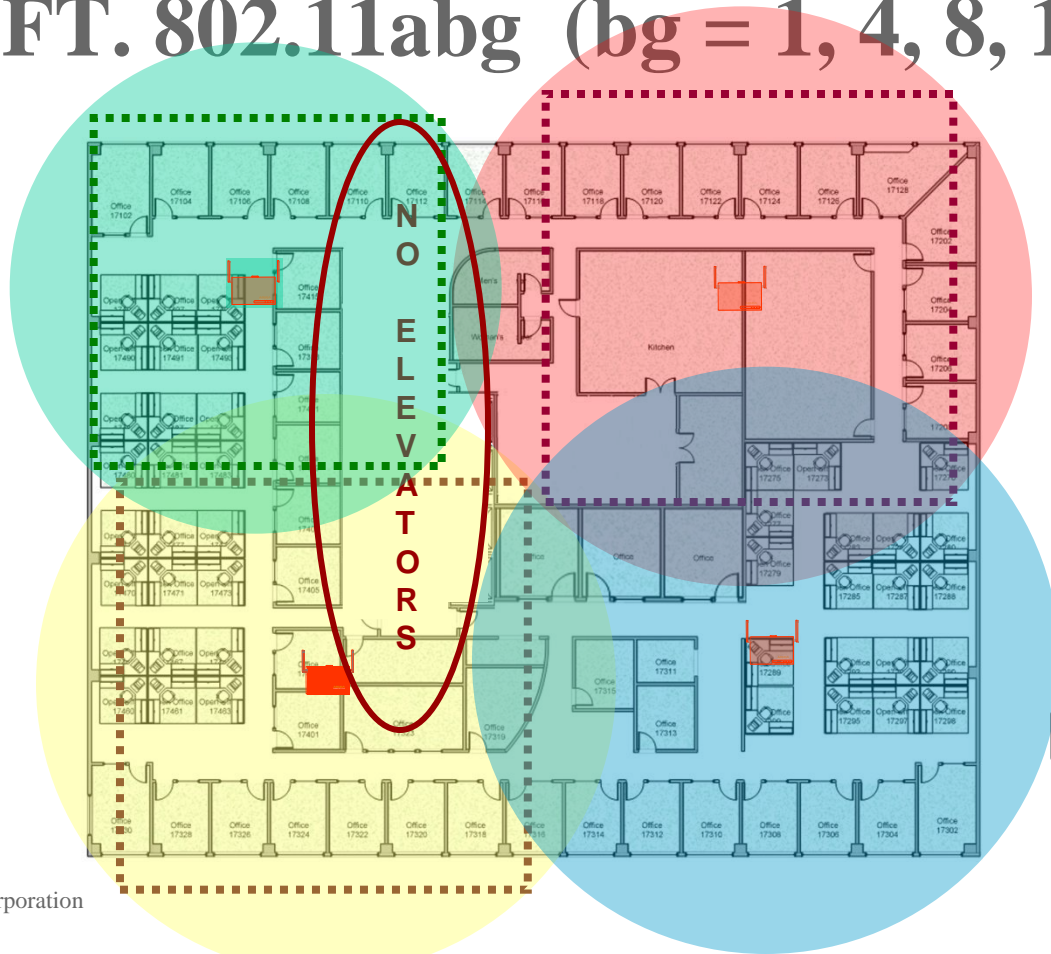
20,000 SQ.FT. 802.11abg (bg = 1, 4, 8, 11)

AP#4
5,500 sqft
21 users
CH 11
CH 157
OMNI

AP#3
7,500 sqft
25 users
CH 4
CH 149
OMNI

AP#1
7,500 sqft
20+ users
CH 1
CH 52
OMNI

AP#2
5,500 sqft
22 users
CH 8
CH 60
OMNI





WIRELESS SECURITY SUMMARY

	SOHO	SMB	Enterprise
WPA or WPA2-Personal	✓	✓	
Strong Pass Phrase	✓	✓	
WPA or WPA2-Enterprise		✓	✓
PEAP		✓	✓
EAP-TTLS			optional
EAP-TLS			optional
Wireless Intrusion Detection		consider	✓
Endpoint Protection		consider	✓



ADDITIONAL RECOMMENDATIONS

- Wireless Client Update for XP (KB 917021)
- Disable Ad Hoc connections
- VLAN and/or firewall different classes of wireless traffic
- Strong password on all access point interfaces (web, telnet, SNMP)
- No LEAP or EAP-FAST
- Avoid 802.11n for now



FIVE POINTS TO REMEMBER

- Start small and select manageable hardware
- Your vendor is your friend ...maybe
- Resist immature or problematic technologies
- Stay informed on security, and perform periodic wireless security assessments periodically
- Educate management and end-users about wireless risks



How To Plan, Install, and Secure Wireless Networks

David Black

President/CEO

Insource Technology Corporation

(281) 774-4150

david.black@insource.com

www.insource.com



INSOURCE
TECHNOLOGY

Backup Slides

© 2006-2007 Insource Technology Corporation



INSOURCE WIRELESS TUTORIALS

Wireless Networks

- Security Choices
- Upcoming Standards
- Capacity Modeling
- Duty Cycle and Noise
- Co-Channel Interference
- Factors affecting Coverage
- Site Surveys
- RF Modeling Software
- Equipment Selection
- Antenna Types and Usage
- Sample Designs

Wireless Security

- Security Choices
- What NOT to do
- Hacker Tools
- Attack Vectors
- Live CDs
- Botnets & Organized Crime
- Preventing Infections
- Wireless Intrusion Detection
- Endpoint Protection
- Recommendations

Anatomy of a Wireless Hack

- Hacker Tools
- Attack Vectors
- Downloading and configuring the necessary tools
- Executing a Man-In-The-Middle attack
- Protecting your users

Demonstration of how readily available, powerful, and effective today's hacking tools are

For those trying to understand if today's threats are real or exaggerated



SOURCES FOR SECURITY INFORMATION

- AVIEN (Anti Virus Information Exchange Network) -- www.avien.org
- Bleeding Edge Threats -- www.bleedingthreats.net
- The Shadowserver Foundation -- www.shadowserver.org
- Anti-Virus vendors (Sophos, Kaspersky, McAfee, Trend Micro)
- Security software vendors (Authentium, SecureWorks, Secunia)
- Security resources (Honeypots.net, EthicalHacker.net)
- U.S. Computer Emergency Readiness Team -- www.us-cert.gov



Wireless Client Update for XP (KB 917021)

- WPA2 support in wireless Group Policy settings
 - Manual configuration by users no longer necessary
- Changes for nonbroadcast networks
 - Users can specify networks as broadcast or nonbroadcast
 - Probe requests sent for nonbroadcast networks only
- Changes in parking behavior
 - Now encrypted with a random PSK to go along with the random SSID
- Changes for ad hoc networks
 - Probe requests no longer sent



VoWLAN

- Causes as many problems for network designers as it offers advantages for users
- Common problems with no real solutions -- jamming, coverage, latency
- Vulnerable to other 802.11 protocol attacks -- NAV, deauthentication, ...
- 802.11w adds protection for management frames (late 2008)
- Vendors claim to handle dozens of calls per AP, QoS, fast roaming, ...
- But none point out that the spectrum is license-free and cannot be controlled



802.11e (QUALITY OF SERVICE)

- Adds basic (prioritized) QoS support for audio and video transmissions
- A forward looking standard designed to expand uses of Wi-Fi
- Most network admins will not be concerned with 11e yet (unless they are considering VoWiFi)
- Parameterized QoS (guaranteed bandwidth) will be addressed by a future standard
- Approved September 2005



802.11i (SECURITY)

- WPA2-Enterprise: user-authentication and data privacy for enterprise wireless networks
 - Enhanced encryption (AES) that improves upon WPA
 - Strong user-authentication as a core feature (802.1x)
- WPA2-Personal: scaled-down version for smaller networks
 - Pre-shared key configured identically on clients and access points (group authentication only)
 - Higher maintenance
- Approved June 2004



802.11r (FAST ROAMING)

- Persistent connections enabling user to move from one access point to another
- Important in applications that need low latency and high QoS
- Quick hand-off of clients from one access point to another with their authentication and QoS intact
- Also provides traffic balancing when an access point becomes saturated
- Approval expected mid-2008



ENTERPRISE WIRELESS NETWORKING SERVICES

- Requirements planning
- Security Assessments
- Wireless network design
 - New installs or expansion of existing networks
 - General coverage (indoor/outdoor)
 - Bridging and Meshing (point-to-point and point-to-multipoint)
 - Site surveys (predictive and active)
 - Capacity and coverage modeling
 - Wireless intrusion detection and prevention (integrated or overlay)
 - Locationing
 - Simple and Secure Guest Access
- Transparent 802.1X Single-Sign-On for highly secure employee access
- Design and implementation of complex, latency sensitive wireless networks for voice or video
- Troubleshooting of reliability or performance problems
- Spectrum analysis services
- Diagnostic and performance monitoring toolkits
- Endpoint protection solutions
- Turnkey implementation, or assistance to your team
- Solutions for Small and Medium Businesses and Large Enterprises
- Simple, low-cost "Jumpstarts"



SIMPLE, LOW-COST JUMPSTARTS

- Secure Wireless Guest Access
 - Reception area + 2 conference rooms
 - Bulk Manager software for IT
 - Guest Manager software
 - Controller, access points, cabling and POE injectors
 - Professional installation
 - 1 year warranty

\$ 3,995

The image displays two overlapping screenshots of the Insource Technology software interface. The primary screenshot is a web browser window titled 'Wireless - GuestManager' showing a 'Create User' form with fields for 'Guest Name', 'Guest Company', and 'Guest Email' (all marked as 'Optional'). Below this is a 'Guest Account Set' section with fields for 'Guest Username' (containing 'phillip') and 'Guest Password' (containing 'texon'). A 'Create User' button and a 'Print Receipt' icon are at the bottom. The inset screenshot is a 'Microsoft Internet Explorer' window titled 'Insource Technology Wireless Network Login'. It features a login form with 'User Name' and 'Password' fields, a 'Log In' button, and links for 'Change Password', 'Install CA Certificate', and 'Help'. A 'Select Language' dropdown and a 'Change Language' button are also visible. The browser's address bar shows 'https://10.16.4.5/login.pl?custom_login_id=2'. The footer of the browser window indicates 'Version 4.0 - Press F1 for help.' and 'Tuesday October 2, 2007'.

INSOURCE

T E C H N O L O G Y

Intelligent IT By Design™