Wi-Fi Challenges in the Small Enterprise Market

Jason D. Hintersteiner, CWNA, CWDP, CWAP
President and Chief Technology Officer
Imperial Network Solutions LLC

Twitter: @EmperorWiFi
Blog: http://www.emperorwifi.com

About the Presenter
Jason D. Hintersteiner

- Founder, President & CTO: Imperial Network Solutions
  - Extensive experience in Wi-Fi design & deployment
  - Principal network architect and troubleshooter for several hundred SMB networks across numerous venues
  - Well versed with numerous enterprise access point, switch, router, firewall, and controller technologies
  - Private consultant for 1.5 years. Over 6 years as a WISP's Vice President of Technology
- Education
  - Bachelor of Science (BS) from the Massachusetts Institute of Technology
  - Master of Science (MS) from the Massachusetts Institute of Technology
  - Master of Business Administration (MBA) from the University of Connecticut
  - CWNP and CompTIA certifications

Agenda

- Market Definition
- Market Players
- Requirements and Constraints
- Challenges in Network Security
- Other Challenges
- Sample Projects

Challenges of the Small Enterprise

Who is the Small Enterprise Market?

Residential

- Large private homes
- Apartment complexes
- Condominiums
- RV parks
- Student housing
- Military housing
- Assisted living
- Hotels
  (budget / mid-range / B&B / Resorts)

Commercial / Industrial

- Cafés
- Restaurants
- Professional offices (doctor, dentist, lawyer)
- Small companies
- Retail
- Houses of Worship
  (churches / synagogues / mosques)
- Small private schools
- Parks
- Warehouses / Factories

Challenges of the Small Enterprise
What is the Size of this Market?

- 5.82 Million SMBs with 1-99 employees (as of 2008)*
  - About 4 million SMBs of 5-25 employees*
  - Worldwide SMB IT systems market: $33 billion**
  - 2012 SMB LAN switch market: $4 billion***

* US Census Bureau Statistics about Business Size, 2008
** Global SMB IT Spending Market 2014-2018
*** Cisco 2012 10Q

http://cdn.caycon.com/blog/wp-content/uploads/2013/10/Market-Share.jpg

Large and growing market segment.
Probably the largest growth sector in Wi-Fi

Challenges of the Small Enterprise
Who Services this Market?

- Service is local / regional
  - Low voltage electricians
  - IT technicians
  - Self-installed
  - ISPs / WISPs
  - Telcos and cable companies
- Challenges with local network installers
  - Know virtually nothing about Wi-Fi
  - Know virtually nothing about network security

http://cdn.alleywatch.com/wp-content/uploads/2013/03/service-people.jpg

Challenges of the Small Enterprise
How is the Market Serviced?

- Service model 1: On Call
  - SMB or IT consultant advises on equipment
  - Charges standard rate to install
  - Disengages until “crisis”, charges hourly rate to fix
  - Motivation: Many repair calls
- Service Model 2: Managed Services
  - IT consultant resells specific vendor(s)
  - Recurring fee for online monitoring
  - Motivation: 0 repair calls

http://1.bp.blogspot.com/-RmeUF3k7ypY/VREcuIFlMuI/AAAAAAAAAkE/Lyhaf2KLMhA/s1600/computer_repair_icon-770372.gif

Challenges of the Small Enterprise

Lack of Large Enterprise Vendor Suitability: Cost

https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcTqNLYu3ajll3rDoj5wO4lrEw8_oDDXoE3ZnImISwdRa6bZFc4E5g

- Cost
  - Why buy a $1000 AP when a $200 AP is adequate?
  - Why buy a $2000 switch when a $350 switch is adequate?
- Small Enterprise: Small Budgets
  - Customers ALWAYS have a limited budget, and ALWAYS want more than they can afford
  - Little understanding as to why more expensive options are “better”
  - Value discussions establish realistic expectations regarding the options and tradeoffs in equipment and technologies

Challenges of the Small Enterprise

Lack of Large Enterprise Vendor Suitability: Complexity

- Complexity
  - Too many features
  - Too many options
  - Too little guidance and documentation
- Practical Obstacles
  - Why buy equipment that only a CWNE knows how to configure?
  - Many vendors require VARs to be educated (certified) to be eligible for good equipment discounts: shuts out the smaller players

http://www.eurasianet.org/sites/default/files/imagecache/galleria_thumb/060711_16_0.jpg

Challenges of the Small Enterprise

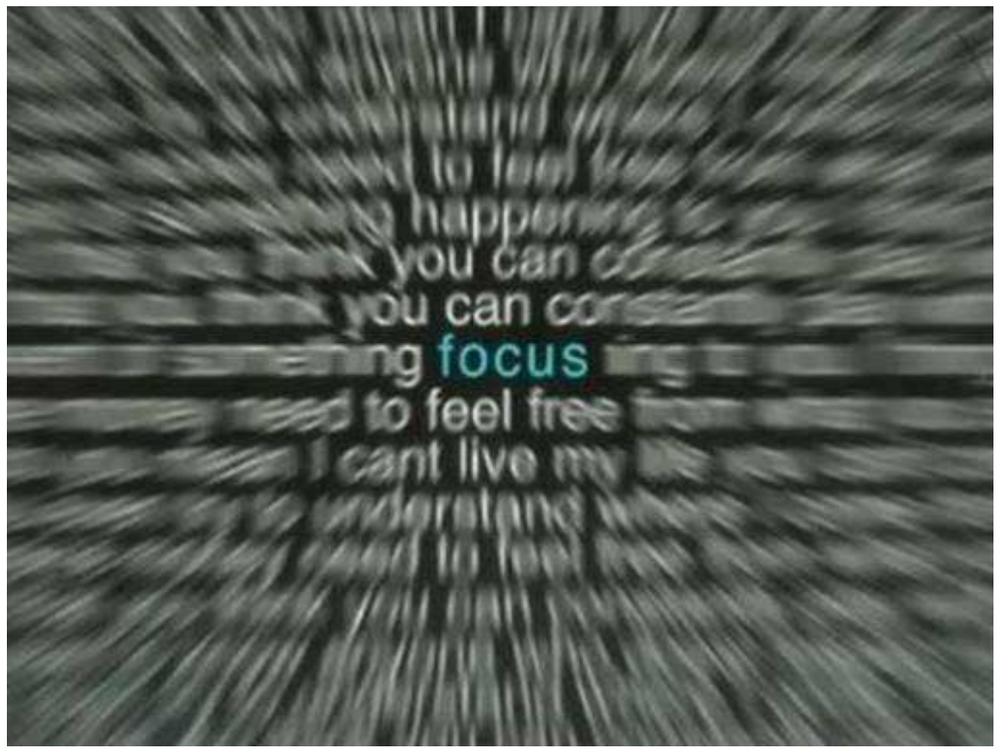
Lack of Large Enterprise Vendor Suitability: Life Cycle

- Planned Obsolescence
  - Shrinking Wi-Fi product life cycle (clients and APs)
  - Customer expectations increase while install-base remains static
- SMB Network Life Cycle
  - Average network life is 5-7 years
  - Design for tomorrow, not today!
  - Today's latest and greatest APs → 2-3 generations old in 5 years
- Infrastructure is key
  - APs can be upgraded
  - Switches can be upgraded
  - Cabling is forever!

http://sr.photos3.fotosearch.com/bthumb/CSP/CSP161/k1619289.jpg

Challenges of the Small Enterprise

Lack of Large Enterprise Vendor Suitability: Focus



http://yourservantinchristministries.org/wp-content/uploads/2012/07/focus-22.jpg

Challenges of the Small Enterprise

Lack of Large Enterprise Vendor Suitability: Focus

- Consumer Market
  - Be first
  - Be cheap
- Large Enterprise Market
  - Leading edge features
  - Niche: best in class at particular applications
  - Large projects: large revenue opportunities (stadiums, malls, campuses, schools)

- Small Enterprise Market
  - Functional: not necessarily the most feature-rich
  - Cost-effective: not necessarily the cheapest
  - Small projects: efficient so can do many deployments
  - Trust: build relationships so success → future business

Different Markets Require Different Strategies

Challenges of the Small Enterprise
Lack of Large Enterprise Vendor Suitability: Focus

- Consumer and SMB product segments in larger companies are never given appropriate level of technology, marketing, or sales resources
- No AP vendor has ever successfully competed in multiple markets simultaneously, even via acquisition
  - HP and Colubris
  - Juniper and Trapeze
  - Cisco and Linksys
  - …

Challenges of the Small Enterprise

Who are the players in Wi-Fi for SMB?

SMB AP Vendors

- EnGenius
- Ubiquiti
- Meraki (Cisco)
- SonicWALL (Dell)
- Open Mesh
- MicroTik
- Luxul

Consumer AP Vendors

- Belkin
- Linksys
- D-Link
- Asus
- TP-Link
- Netgear
- Amped Wireless
- Edimax

…and the numerous managed service providers (MSPs) who utilize and deploy these products.

But do any of them get it right?

Requirements and Constraints

https://akinjidepetersdotcom.files.wordpress.com/2015/01/requirement.gif

Requirements and Constraints
The Angst of the Small Enterprise Owner

- I must supply Wi-Fi to keep my customers happy
- My customers complain about the Wi-Fi (too slow, hard to use, frequent drops)
- I would love to leverage my Wi-Fi investment to enhance business operations
- All these new network gadgets are cool. Can I put them on the network?
- I don't really understand Wi-Fi
- What do you mean, I can't just plug it in and Wi-Fi works?
- I've been burned before using consumer gear
- I won't spend a lot of money on Wi-Fi

https://psyknyheter.files.wordpress.com/2010/11/angst.jpg

Requirements and Constraints
Definition of Requirements

- Requirements – What must the network do?
  - *Standard Requirements:* True for virtually all deployments in any SMB vertical market
  - *Vertical Requirements:* Dependent upon the specific, vertical market (e.g. hospitality, retail, residential, assisted living, etc.)
  - *Customer-Specific Requirements:* Dependent upon the specific needs of the individual customer

Requirements are independent of each other. Bad design solution choices hamper your ability to satisfy all requirements simultaneously.

Requirements and Constraints
Solicitation and Documentation

- Get the information up front
  - Who is using the network?
  - What types of devices need access?
  - What areas need to be covered?
  - Building structure / layout / materials?
  - Aesthetics?
  - Budget?
- Documentation
  - Validates everyone has the same understanding
  - Enables quick identification of scope creep
  - When managing multiple sites, a centralized documentation database is essential

Requirements and Constraints
Guest Networks

- Public / Semi-Public Access Network (resident, guest, patron, consumer, etc.)
- Controlled Access
  - Free (or paid / hybrid)
  - Client device isolation (within and between APs)
  - Content filtering
  - Bandwidth control and restrictions (SLA)
  - CALEA compliance

https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcQZ-dhaUCjc3E-zbvzk4VCbBVoW4kZiZi9tKjAVGHb_Sb_s0E9S5g

Requirements and Constraints
Guest Networks: Captive Portals

- Multiple login methods
  - Username & Password
  - Terms and Conditions
  - Email / Social Media
- Necessary evil
  - Display legalese to absolve provider of any liability
  - Nobody reads it
  - Often is technical mechanism used to identify individual users and control bandwidth

http://dave.harris.uno/wp-content/files/2010%2F6%2Fdoredisclaimer.jpg

- Usually implemented poorly
  - Not mobile-device friendly
  - Too many screens to click-through
  - Too many forms to fill out
  - Too long a process to actually get online

Requirements and Constraints
Guest Networks: Free or Paid?

- Why should the Wi-Fi be offered for free?
  TANSTAFL
  "There ain't no such thing as a free (wireless) LAN"
- Ugly reality: Monetization doesn't work
  - Too many competitors offer free service
  - Too difficult to build enough revenue to be profitable
  - FCC gets annoyed when you overcharge & block Mi-Fi devices
- With a hybrid approach, free service must be usable
  - Won't pay extra if the free service is good enough
  - Too slow → customers complain
- Paid portion of hybrid service: marketing tool
  - Attract groups (e.g. conferences)
  - Placate angry customers
  - Incentivize rewards memberships

http://wheelingout.com/wp-content/uploads/2012/12/free-wifi-cafe.jpg

Requirements and Constraints
Staff Networks: Operations Infrastructure

- Day-to-day business operations
- Order taking / credit card transactions (PCI-DSS)
- Customer records (PCI-DSS, HIPAA, FINRA)
- Full access to facility resources
  (e.g. printers, shared drives, on-site servers)
- Integration with VPNs
- WPA2-AES Encryption
  (Personal is commonplace, Enterprise is rare)

http://www.ceebusinessportal.eu/documents/10180/470540/infrastructure.jpg/dff5560f-b789-4e00-b27b-4ec626b135e1?t=1412584233082

Requirements and Constraints
Appliance Networks: The IoT (R)evolution

- High Bandwidth
  - Video Surveillance
  - Multimedia (i.e. SONOS, AppleTV)

http://www.engeniustech.com/products/networked-surveillance-cameras/mini/eds1130.html

http://toucharcade.com/2015/07/31/its-a-day-that-ends-in-y-so-of-course-apple-tv-app-store-rumors-are-flying/

- Low Bandwidth: Internet of Things (mostly 2.4 GHz only, often 802.11b only)
  - Security & Access Control
  - Temperature & HVAC control
  - Lighting
  - Kitchen Appliances
  - Toys

https://nest.com/thermostat/meet-nest-thermostat/

Fundamental disconnect between the Wi-Fi appliances emerging on the market and the latest Wi-Fi specs and capabilities.

Requirements and Constraints
Client Devices: All About the BYOD

- New client devices emerging constantly
  - Client devices are “uncontrolled”
  - Consume more data
  - More devices
    (design for capacity vs. coverage)
  - More likely to have malware
- “New” ≠ “better” from Wi-Fi Perspective
  - Cheap wireless chipsets
  - Weak client transceivers
  - Inadequate wireless antennas
  - Roaming aggressiveness / stickiness
  - Only or preferential on 2.4 GHz
  - Dual-band: Support DFS?

http://www.apple.com/iphone/

Have to actually design the Wi-Fi:
AP / Antenna Type, Location, Channel, and Power!

Requirements and Constraints
Unique Customer Requirements

- Some are to your advantage
  - Assisted living property operates their own emergency power backup plant – can keep network online during power outage without UPS
- Some are challenges
  - Demarc is unheated basement room, temperatures below -20^{o}F
  - Equipment cabinet on west side of building with sun exposure, temperatures above 140^{o}F
  - Support 22 HDTVs in one $25M mansion (2 outdoor, 2 in master bathroom)
- Some are downright “unique”
  - Explosion-proof APs for hazardous waste treatment plant (IP68 not enough)
  - Mount cameras and PTP links on poles and not buildings – low-income property expecting residents to shoot out cameras, don’t want guns aimed at residential apartment units

Requirements and Constraints
Definition of Constraints

- Constraints – What do you have to work around?
  - *Physical Constraints:* Driven by the physical characteristics of the facility
  - *Logical Constraints:* Driven by the customer / organization owning the facility

http://image.sportsmansguide.com/adimgs/l/1/112010_ts.jpg

Requirements and Constraints

Physical Constraints: Every Wi-Fi Network is Tailored

Property Layout

- Areas of indoor coverage
- Areas of outdoor coverage
- Multiple buildings
- Cable paths / conduit?

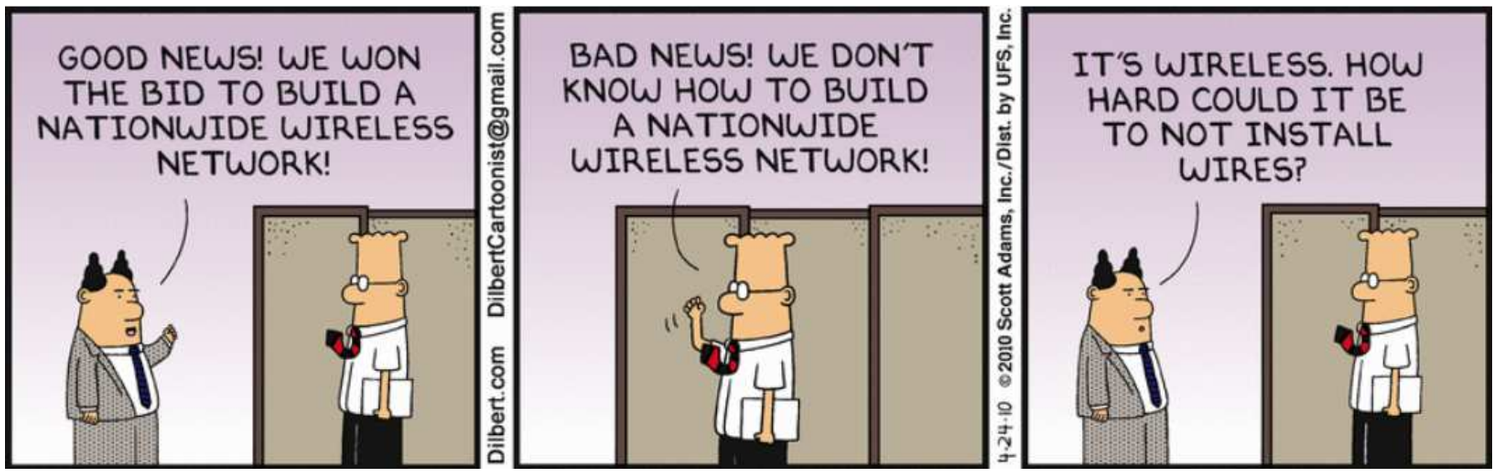
Building Materials

- Drywall
- Concrete
- Brick
- Wire mesh stucco
- Plaster

Drives the need for mass customization – a consistent underlying architecture with a unique implementation

Requirements and Constraints

Physical Constraints: Low Voltage Cabling



http://dilbert.com/strip/2010-4-24

- Is there existing low-voltage cabling infrastructure?
- Is it possible to run cabling where it is needed?
- Do we need to run point-to-(multi)point? Mesh?
- Do you use CAT5e or future proof with CAT6a?
- Running cables is expensive…
  - "I love the design, but we can only cable the hallways."
  - "Why can't we do security cameras wirelessly?"

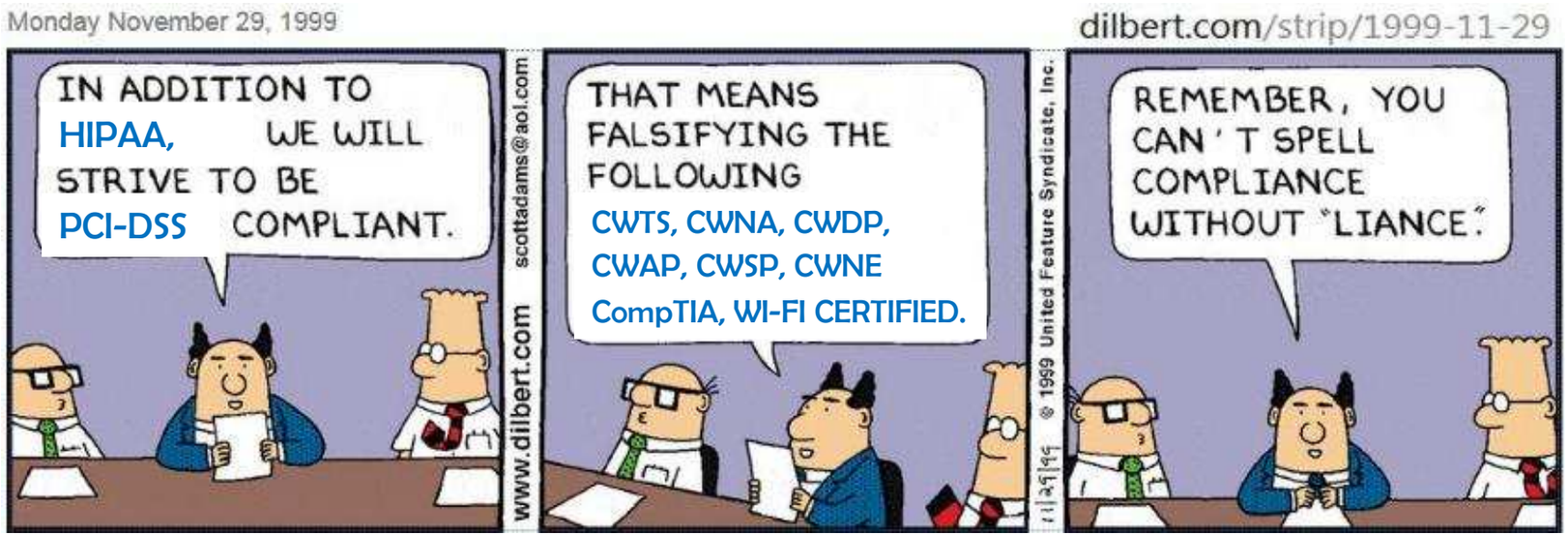
Requirements and Constraints
Logical Constraints

- Budget
- Aesthetics
- Integration with an existing wired and/or wireless network
  - Generally old AP locations won't meet new network requirements
  - Legacy clients may need upgrades as well
- Accessibility to AP locations / telco closets for maintenance

Drives the types of APs, placement, limitations in coverage, and overall network capabilities

Requirements and Constraints

Regulatory and Legal Compliance



Requirements and Constraints
Regulatory and Legal Compliance: PCI-DSS

https://digitalguardian.com/sites/default/files/credibility_pci-logo.png

- Payment Card Industry – Data Security Standard
- Detailed specification for computers and computer networks handling, transporting, and storing credit card data
- Spec is periodically reviewed and amended with new technology development
- Latest version: PCI-DSS 3.1 https://www.pcisecuritystandards.org/security_standards/pcidss_agreement.php?association=pcidss

- Key requirements
  - Install firewall
  - Do not use default passwords / SNMP
  - Protect stored cardholder data
  - Encrypt transmission across networks (wired and wirelessly – requires 802.11i)
  - Use anti-virus software
  - Develop and maintain secure systems
  - Restrict access to data (virtual & physical)
  - Assign unique user IDs and monitor / track
  - Test security regularly (periodic assessment)
  - Maintain security policies

Requirements and Constraints
Regulatory and Legal Compliance: PCI-DSS

https://digitalguardian.com/sites/default/files/credibility_pci-logo.png

- Not strictly required in many SMB environments
  - 3rd party payment vendors (e.g. Square, Harbortouch)
  - Isolated systems that work over phone line or dedicated Internet connection
  - Many SMBs do not want to wrestle with PCI-DSS requirements
- Where needed
  - Tablet-based order-taking / payment processing
  - Multi-station (e.g. multiple cash registers)

Requirements and Constraints
Regulatory and Legal Compliance: HIPAA

http://bhmpc.com/wp-content/uploads/2015/03/hipaa.png

- Health Insurance Portability and Accountability Act - Title II
  - Privacy Rule: Regulates use and disclosure of protected health information (PHI)
  - Security Rule: Administrative, Physical, and Technical
- HITECH Act
  - Reporting rules in case of data breach
- More info: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

- Key requirements
  - Administrative safeguards
  - Physical safeguards (control physical access to data)
  - Technical safeguards (control access to computer systems and networks)
- For Wi-Fi, functionally similar to PCI-DSS (PCI-DSS has more detailed requirements)
  - Isolated VLANs
  - WPA2-AES encryption (personal ok)
  - Firewalls

Requirements and Constraints
Regulatory and Legal Compliance: FINRA

https://d0.awsstatic.com/Developer%20Marketing/Big%20Data/finra-logo.jpg

- Financial Industry Regulatory Authority
  - Oversight of financial firms / securities industry
  - Regulation of brokers / dealers and financial markets in conjunction with SEC
  - Non-profit organization authorized by US Congress
  - Enforcement of investor protections
- More info: http://www.finra.org/

- Key IT requirements
  - Generate reports and audit trails for compliance
  - Configuration / User Privileges Enforcement
  - Network Security
  - Device Security / Applications
- For Wi-Fi, functionally similar to PCI-DSS (PCI-DSS has more detailed requirements)
  - Isolated VLANs
  - WPA2-AES encryption (personal ok)
  - Firewalls

Requirements and Constraints
Regulatory and Legal Compliance: CALEA

http://www.andoverks.com/images/pages/N411/CALEA GoldStandard.png

- Law enforcement agency can require property manager / ISP to track specific user's online activities
  - Electronic surveillance (originally intended for VoIP, expanded in 2004 for Internet data traffic)
  - Requires valid warrant for some (headers) or all (full data) traffic
- Problems
  - Based on client MAC address (easy to spoof or use disposable Wi-Fi dongle)
  - Internet traffic generally encrypted via SSL (headers tell you "who" but not content)
  - Consumer devices, and many SMB devices, do not have capability (network owner subject to large fines if they are not compliant)
- More info: http://www.calea.org/

Security Challenges

What We Like to Think We Have

Fig: Security officers at a checkpoint at O'Hare International Airport in Chicago, Illinois

Source: http://www.independent.co.uk/news/world/americas/leaked-us-security-documents-reveal-how-to-spot-a-terrorist-trying-to-board-a-plane-10145842.html

Security Challenges

What We Actually Have

http://www.imperialnetsolutionis.com/

Security Challenges
The Ugly Truth

- Consumer-grade and/or poorly implemented SMB equipment
  - No VLANs
  - No segregation of guest, staff, security, and appliance networks
  - Firewall: Limited to NAT
  - No wired or wireless client isolation
- No protection from disgruntled current or former employees
  - WPA2 Passphrase not changed when employees leave
  - Untraceable access to resources

Security Challenges
Guest Networks: Encryption

- Open Authentication
  - Want users to get online easily
- Why not use WPA2 Personal: actually decreases value
  - Requires customers to ask staff for the passphrase – adds unnecessary staff overhead and customer aggravation
  - Signs with passphrase prominently displayed

http://noupe.com/img/ror/make_use_of_auth.jpg

- Ludicrously weak passphrases
  - Most common: “password”
  - Next most common: establishment name
- WPA2 Personal is Insecure
  - If you know the passphrase and capture the 4 way handshake, you can decrypt someone else’s traffic (Sources: CWSP, CompTIA Security+)
- Usually no client isolation on wired part of network – requires switch ACL rules

WPA2 on a guest network isn’t actually secure! It is only annoying!

Security Challenges
Guest Networks: Client Isolation

- Client isolation must be throughout network
  - Within an AP: Most APs have the ability to block clients within an AP
  - Between APs: Some APs provide filtering functionality to block traffic between APs
  - Wired clients (e.g. hotels/dorms): Generally not covered by Wi-Fi vendor solutions. Must be handled via switch and router ACL rules
- Blog: http://www.emperorwifi.com/2015/07/enhancing-wi-fi-security-with-switch.html

http://jmmphotoblog.files.wordpress.com/2011/06/bw-ecopyof-the-old-prison-in-deer-lodge-049.jpg

Security Challenges
Staff Networks: Wi-Fi Sense(less) (1)

- Microsoft Windows 10 stores and shares your SSID & passphrase
  - Shares with all of your Facebook, Skype, & Outlook contacts
  - When a friend connects automatically, information is shared with all of their Facebook, Skype, & Outlook contacts
  - Decision to share is up to the user, not the network administrator
  - Network admin can only prevent by adding "_optout" to the SSID

http://cdn.wccftech.com/wp-content/uploads/2015/02/Windows-10.png

Security Challenges
Staff Networks: Wi-Fi Sense(less) (2)

- Designed for home networks, impacts SMB networks relying on WPA2 Personal
  - Passphrase not directly shared
  - But allowing automatic connection compromises staff network security
  - Say goodbye to PCI-DSS and HIPAA compliance
- Client isolation by Windows Firewall
  - Windows 10 “friend” cannot be seen from network, but can see rest of your network
- Blog: http://www.emperorwifi.com/2015/06/wi-fi-sense-how-microsoft-has.html

http://cdn.wccftech.com/wp-content/uploads/2015/02/Windows-10.png

Security Challenges
Staff Networks: Why Not Use Enterprise Security?

- WPA2 Enterprise
  - Most small businesses do not have the equipment, knowledge or manpower
  - A lot of overhead to build/maintain RADIUS database and get devices to work
  - Rare to see WPA2 Enterprise used in practice in SMB
- Private Pre-Shared Key
  - Most enterprise AP vendors still don't offer it (though with Windows 10 maybe that changes)
  - Still have to maintain a user / device database
  - May be appropriate for staff networks, but impractical for guest and appliance / IoT networks

http://www.cloudsoftwareprogram.org/rs/371/e9c4455d-a317-4f4c-9f70-108d736bae98/b4f/filename/cloud-security.jpg

Other Challenges

What You'll NEVER See in Small Enterprise (1)

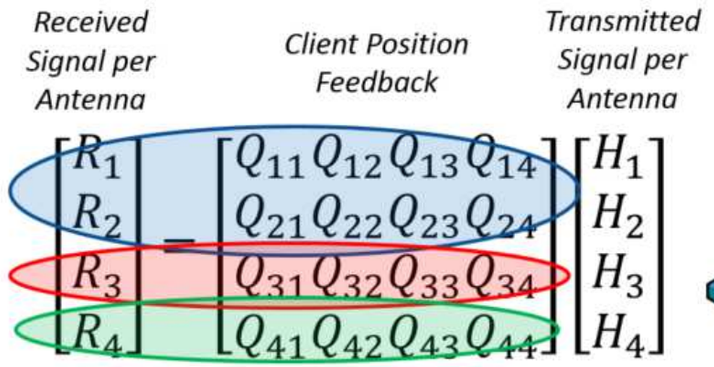
- Wi-Fi Alliance Certification
  - Irrelevant in this space: Installers and users either not aware or don't care
  - Nobody willing to pay the price premium for the certification
  - Most consumer and IoT appliances won't support anyway
- Hotspot 2.0 / Passpoint
  - Not a priority for cellular carriers: Individual networks are too small and fragmented for the cellular carriers to care about this market
  - Not a priority feature for SMB vendors (who are solely focused in this space)

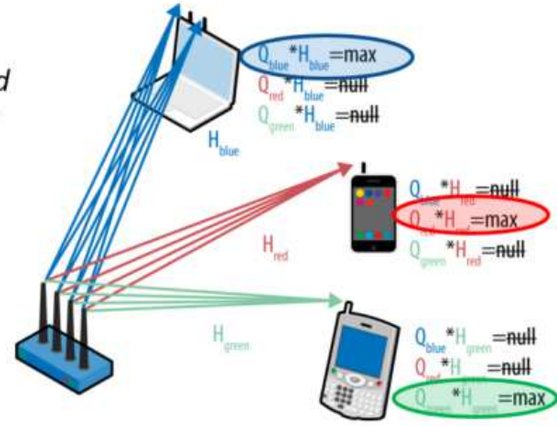
http://www.wi-fi.org/sites/default/files/images/logos/WFA_CERTIFIED_Flat_Web_LR.png

Other Challenges

What You'll NEVER See in Small Enterprise (2)

- Multi-User MIMO (MU-MIMO)
  - Only useful for very dense client environments
  - Clients must be ≥ 802.11ac wave 2
  - Clients must be spatially separated
  - Clients must be at similar connection speeds (MCS)





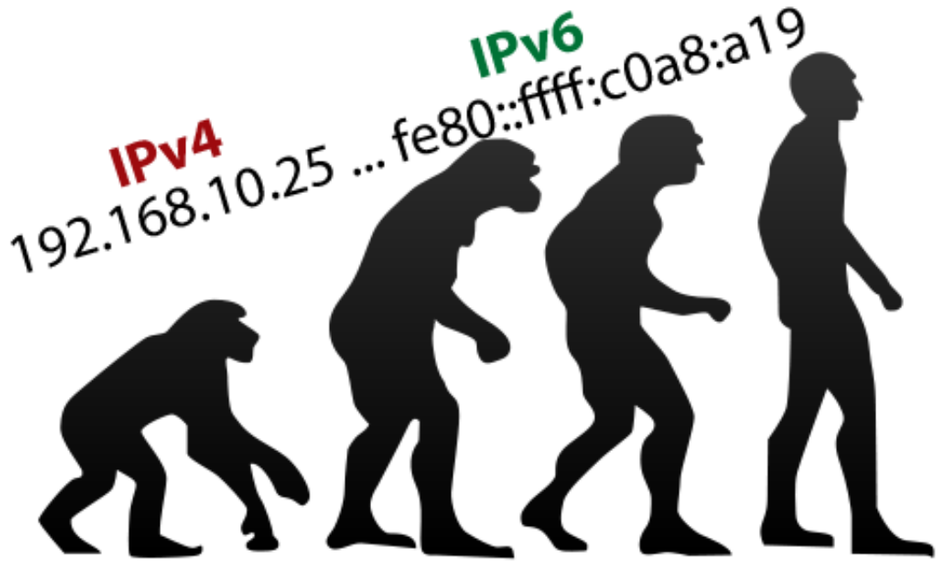
http://orm-chimera-prod.s3.amazonaws.com/1234000001739/images/easg_0418.png

- Blog post: http://www.emperorwifi.com/2015/06/the-elephant-in-room-will-mu-mimo-work.html

Other Challenges

What You'll NEVER See in Small Enterprise (3)

- IPv6
  - Installers and users don't understand it
  - Not needed for private networks
  - At most, you'll eventually see on WAN side (IPv4 to IPv6 encapsulation by router / modem)
- WIPS / WIDS
  - Too expensive
  - Too complex - basic security sufficient (though often lacking)
- Mobile Device Management (MDM)



https://dougvitale.files.wordpress.com/2013/03/ipv6-evolution.png?w=700

Other Challenges

What You'll NEVER See in Small Enterprise (4)

- Site Surveys
  - CWNAs and CWDPs know the value
  - Nobody else in the Small Enterprise wants to pay for them up front
- Site Walkthrough
  - Focused on cabling paths
  - Little to no RF measurements
  - Small deployments: Not done; figured out on the fly
- Predictive modeling
  - Good news: Number of requested models increasing
  - Bad news: Customer expects the heat maps and design for free from the installer or AP vendor.
  - Ugly news: Never verified with a site survey, unless there are major problems

Customers never want to pay for up-front design services.

Other Challenges
What You WILL See in Small Enterprise


http://www.imperialnetsolutions.com

- Bad-Fi:
  - http://www.bad-fi.com by @heyeddie
- 40 MHz Channels on 2.4 GHz
- Auto-channel and auto-power
  - Your own APs are your greatest source of interference and performance problems
  - Blog: http://www.emperorwifi.com/2015/08/an-explanation-of-channel-and-transmit.html
- Poor security and lack of VLAN isolation
  - Blog: http://www.emperorwifi.com/2015/05/how-operators-can-make-hotspots-and.html

Other Challenges
Technical Opportunities

- Most interference is internal, not external
  - Most CCI comes from your own APs
  - Don’t have other people operating Wi-Fi networks in your immediate space
  - Controlled with static channel planning (both bands)
- Don’t need latest technology
  - Most clients are smartphones / tablets (1x1:1 or 2x2:2)
  - 802.11n 2x2:2 is adequate for most small enterprises
- 802.11ac: 80 MHz Channels on 5 GHz works well!
  - Few high density areas, so few dense AP deployments
  - DFS avoidance (generally) not an issue
  - 5-6 channels to work with (80 MHz sweet spot)
- Point-to-(multi)point in high demand
  - Easy and cheap to interconnect buildings
  - High use in security / surveillance applications

Imperial Initiatives: EnGenius

Certification and Pre-Sales Services

- Vendor Certification Program
  - 1-2 day on-site training course for installers, resellers, and dealers
  - Deep dive into Wi-Fi design and best practices
  - Detailed review of network setup, monitoring, and troubleshooting of EnGenius equipment
  - Hands-on training with point-to-point links, switches, and access points (both provisioning and troubleshooting)

- Pre-Sales Design Services
  - Predictive modeling
  - Point-to-(multi)point design
  - Work with dealer and end customer to define
    - Bill of Materials (BoM)
    - AP models / locations
    - Switch infrastructure
    - Critical settings (channel / power)

Imperial Initiatives: Little Devices

Startup: Purpose-Built IT for Small Business

- Simple, Integrated SMB IT
  - Designed from ground-up for small business market
  - Fully integrated: Not disparate hardware and cloud services
- Automated Best Practices
  - No IT expertise required to deploy or maintain
  - Seamlessly coordinated networking and security
  - Next-generation storage and backup
  - Guided installation / diagnostics
- Product Launch: Q1-2016

Key Services

- Enterprise-Class Wi-Fi Networking
- Next-Generation Storage & Backup
- Secure Remote Access

Core Platform Tenets

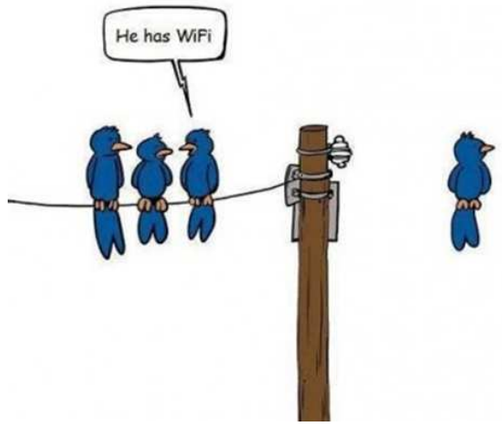
- End-to-End Security
- Hybrid Cloud & Onsite HW Solution
- Built for Reliability and Easy to Deploy

Worry about your business. Not your IT.

Sold & supported exclusively by local SMB IT partners. No up-front hardware costs.

Challenges of the Small Enterprise
Conclusions

- The small enterprise market
  - Large and growing segment
  - Some unique and some non-unique technical challenges
  - Challenges and opportunities
- Most of the enterprise solutions are not geared to this market
  - Cost
  - Complexity
  - Focus



http://dobrador.com/wp-content/uploads/2012/05/40462096622521213_mRYKn3oq_f.jpg

- Success requires understanding and focusing on the requirements and constraints of this market
  - Separate networks for guests, staff, and devices / IoT
  - Regulation and compliance
  - Security
  - Budget

Challenges of the Small Enterprise

Jason D. Hintersteiner, CWNA, CWDP, CWAP

President and Chief Technology Officer

Imperial Network Solutions, LLC

Twitter: @EmperorWiFi

Blog: http://www.emperorwifi.com