Wireless LAN Design and Troubleshooting

David Allred
Photon, Inc.
allred@photoninc.com

MACTECH

$$\nabla f = \mathbf{a}_r \frac{\partial f}{\partial r} + \mathbf{a}_\theta \frac{1}{r} \frac{\partial f}{\partial \theta} + \mathbf{a}_\phi \frac{1}{r \sin \theta} \frac{\partial f}{\partial \phi}$$

$$\nabla \cdot \mathbf{F} = \frac{1}{r^2} \frac{\partial}{\partial r} (r^2 F_r) + \frac{1}{r \sin \theta} \frac{\partial}{\partial \theta} (F_\theta \sin \theta) + \frac{1}{r \sin \theta} \frac{\partial F_\phi}{\partial \phi}$$

$$\nabla \times \mathbf{F} = \mathbf{a}_r \frac{1}{r \sin \theta} \left(\frac{\partial}{\partial \theta} (F_\phi \sin \theta) - \frac{\partial F_\theta}{\partial \phi} \right)$$
$$+ \mathbf{a}_\theta \frac{1}{r} \left(\frac{1}{\sin \theta} \frac{\partial F_r}{\partial \phi} - \frac{\partial}{\partial r} (r F_\phi) \right)$$
$$+ \mathbf{a}_\phi \frac{1}{r} \left(\frac{\partial}{\partial r} (r F_\theta) - \frac{\partial F_r}{\partial \theta} \right)$$

$$\nabla^2 f = \frac{1}{r^2} \frac{\partial}{\partial r} \left(r^2 \frac{\partial f}{\partial r} \right) + \frac{1}{r^2 \sin \theta} \frac{\partial}{\partial \theta} \left(\sin \theta \frac{\partial f}{\partial \theta} \right) + \frac{1}{r^2 \sin^2 \theta} \frac{\partial^2 f}{\partial \phi^2}$$

Overview

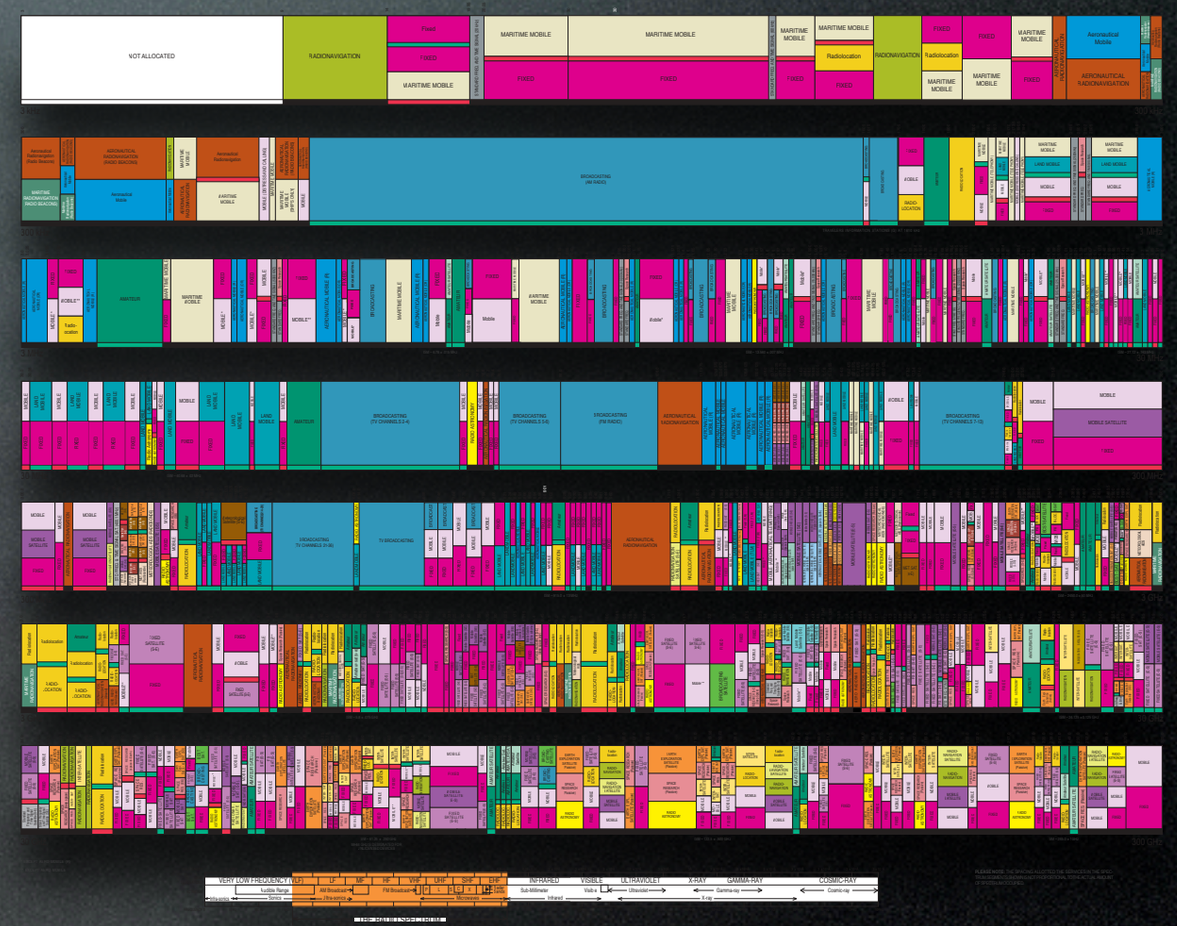
- Some Points to Consider
- Coverage
- Troubleshooting
- Testing
- Security
- References

It’s Radio

- It’s Different
- It Keeps Going
- Invented 1894 - J.C. Bose
- Invented 1896 - Marconi

Shared Resource

- Regulated
- FCC
- Part 15



Radio Communications Act of 1934

Laws of Physics

- Regularly Rewritten by Lawyers
- and Marketing Departments

Reflection
Refraction
Attenuation

Attenuation

- Distance
- Absorption
- Measuring Power
- The Decibel (dB)
- dBm - 1 mW Reference

dB

- 20 • log (Power Ratio)
- 3 dB - Double
- 10 dB - Ten Times

An example:

- 74 dBm is ...

0 dBm = 1 mW
- 30 dBm = 1 μW
- 60 dBm = 1 nW
- 70 dBm = 100 pW
- 80 dBm = 10 pW
- 77 dBm = 20 pW
- 74 dBm = 40 pW

39.91 pW

$$P_r = P_t + G_t + G_r + 20\log_{10}\left(\frac{\lambda}{4\pi R}\right)$$

Friis Equation

- There's An App For That

Nuclear Safety

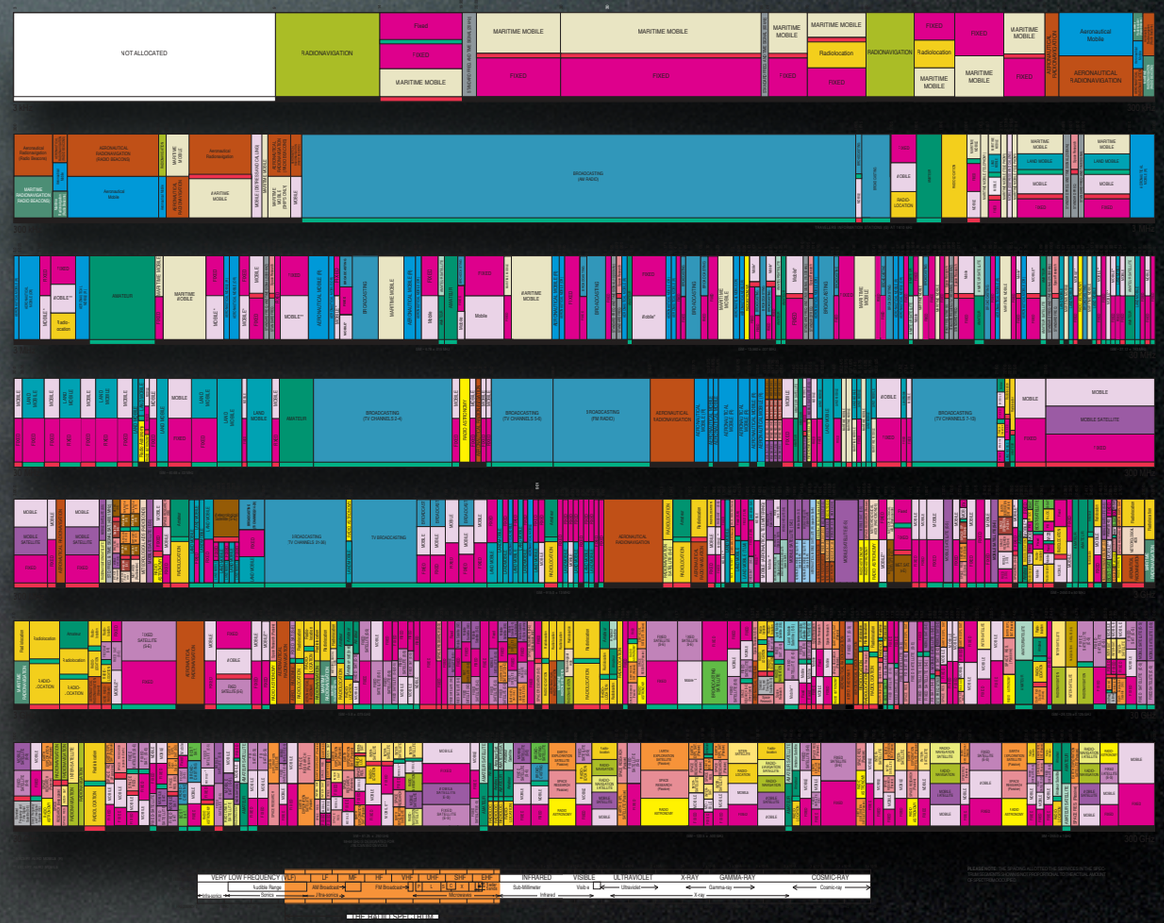
- Time
- Distance
- Shielding

Interference

- Shared Resource
- Primary User Allocation
- Part 15 Device

Industrial, Scientific, and Medical

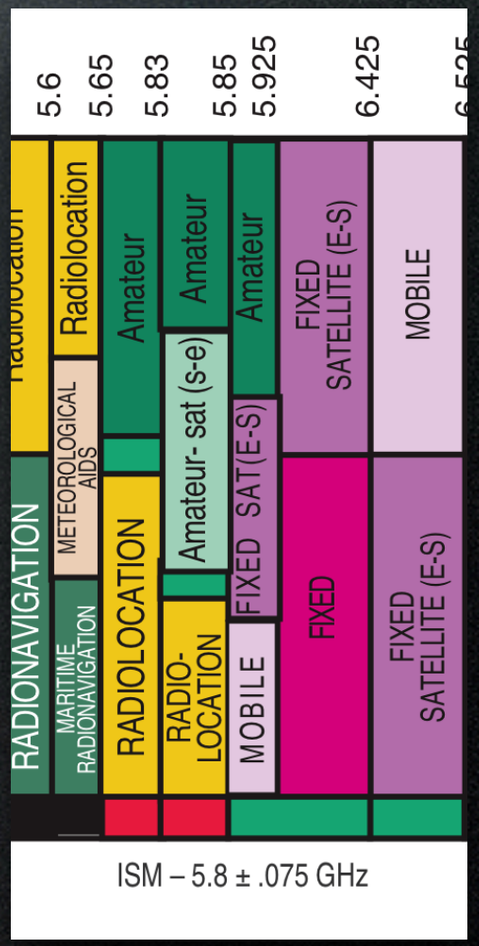
- 2.4 GHz
- 5 GHz



Industrial, Scientific, and Medical

- 2.4 GHz
- 5 GHz

ISM – 2450.0 ± 50 MHz



ISM – 5.8 ± .075 GHz

Interference Sources

- Microwave Oven
- Cordless Phone
- Other Wireless Devices
  - Baby Monitors
  - Wireless Cameras
- Bluetooth
- Time, Distance, and Shielding

Network Topology

- Subnets
- Traffic Segregation
- Department or Group
- Guest Network
- Outside the Firewall

Coverage Bandwidth and Load

Coverage

Distance Is Limited

- Part 15
- Laws of Physics
- Friis Equation

Increase Coverage

- More Access Points
- Design of a Cellular Network
  - Cell Size
  - Overlap
  - Channel Selection
- Four Color Map Theorem

Hidden Node Problem

- Carrier Sense
- Packet Collision
- Handshaking Protocols

Exposed Node Problem

- Carrier Sense
- Transmit Inhibit

Repeaters

- Decrease Bandwidth
- Hidden Node Problem
- Exposed Node Problem

Antenna Patterns

- Directional Instead of Omni-Directional
  Squeeze the Balloon
- Difficult To Do Correctly
  (easy to screw up)
- No Increase in Power
  Part 15 Limits
- Can Exacerbate Other Problems
  Hidden Node and Exposed Node

Laws of Physics

Bandwidth and Load

- Congestion
- Number of Clients
- Client Bandwidth Requirements
- Future Needs
- New Devices
- The Connected Refrigerator

Frequency Considerations

- 2.4 GHz
- 5 GHz

2.4 GHz

- 802.11b and 802.11g
- Channels 1-11
- Automatic Channel Selection
  - Don't Do It
- Spread Spectrum
- Allow a Guard Band
- 4 Channel Separation

5 GHz

- 802.11a
- Wide Channel Option
- Diversity
- MIMO

802.11n

- Increase Channel Width
  from 20 Mhz to 40 MHz
- Increase Data Rate
  from 54 Mb/S to 600 Mb/S
- 5 GHz Mode
- 2.4 GHz Mode
- Interference to Other Devices

Performance

- Is It Working ?
- What Should We Expect For Performance ?
- What Is Normal Performance ?

Bandwidth

- Only the worst link counts
  - Bottleneck Router
- Expected Bandwidth
- Actual Bandwidth
- Path being tested
- Shared Bandwidth
- Test Under Load

Latency

- Round-Trip Time (RTT)
- All links count
- Bandwidth Latency Product
  The maximum amount of data in the connection
- TCP Adaptive Behavior

Measure and Record Normal Performance

- Simple Tests
- Bandwidth
- Latency
- Advanced Testing
- WiFi Performance Tools

Troubleshooting

- Use your standard troubleshooting techniques
- Wireless in one link in a long chain

Troubleshooting

- What's The Real Problem ?
- Interference
- Congestion
- Signal Strength

Troubleshooting

- Access Point Logs
- Client Logs

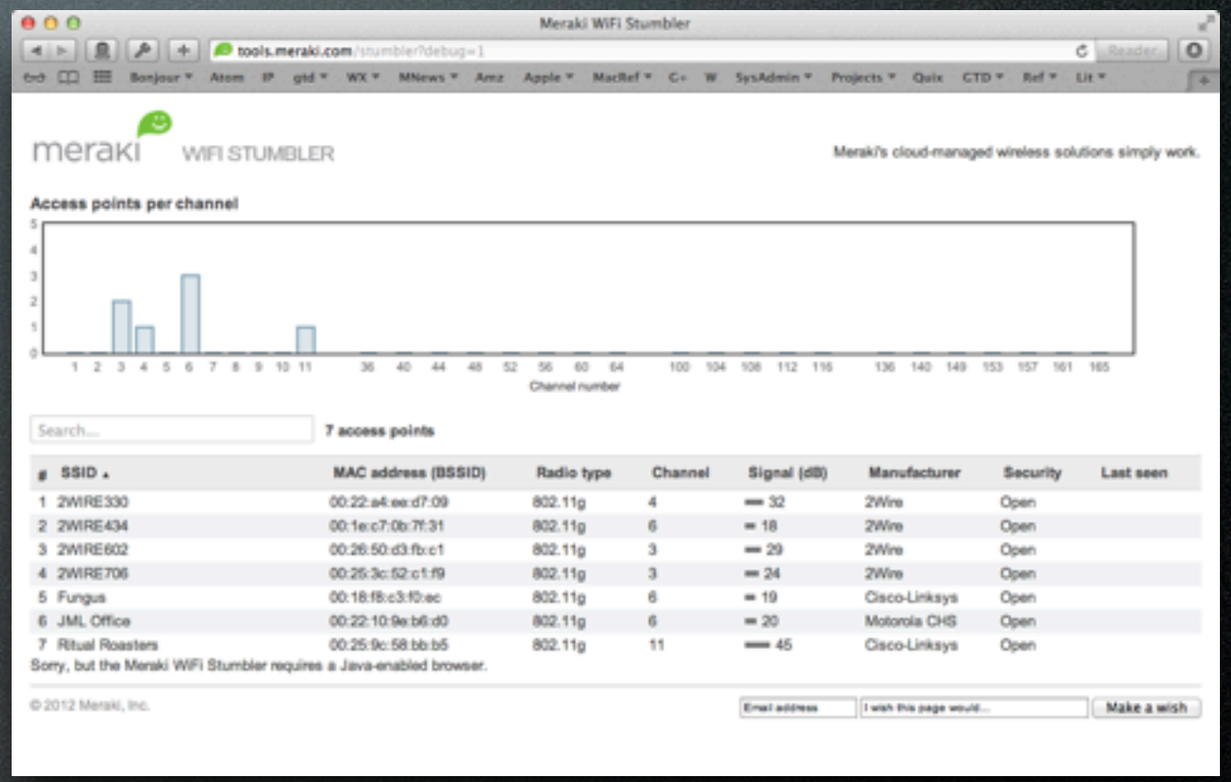
Wireless Testing Hardware

- Your own MacBook Pro
- Outboard WiFi Adapter
  Linksys WUSB300N
- A dedicated Mac or PC
- Real Test Equipment
- Fluke AirCheck WiFi Tester
  (sn.im/photon8)

Wireless Testing Software

- Meraki WiFi Stumbler

  (sn.im/photon10)



Wireless Testing Software

- KisMAC

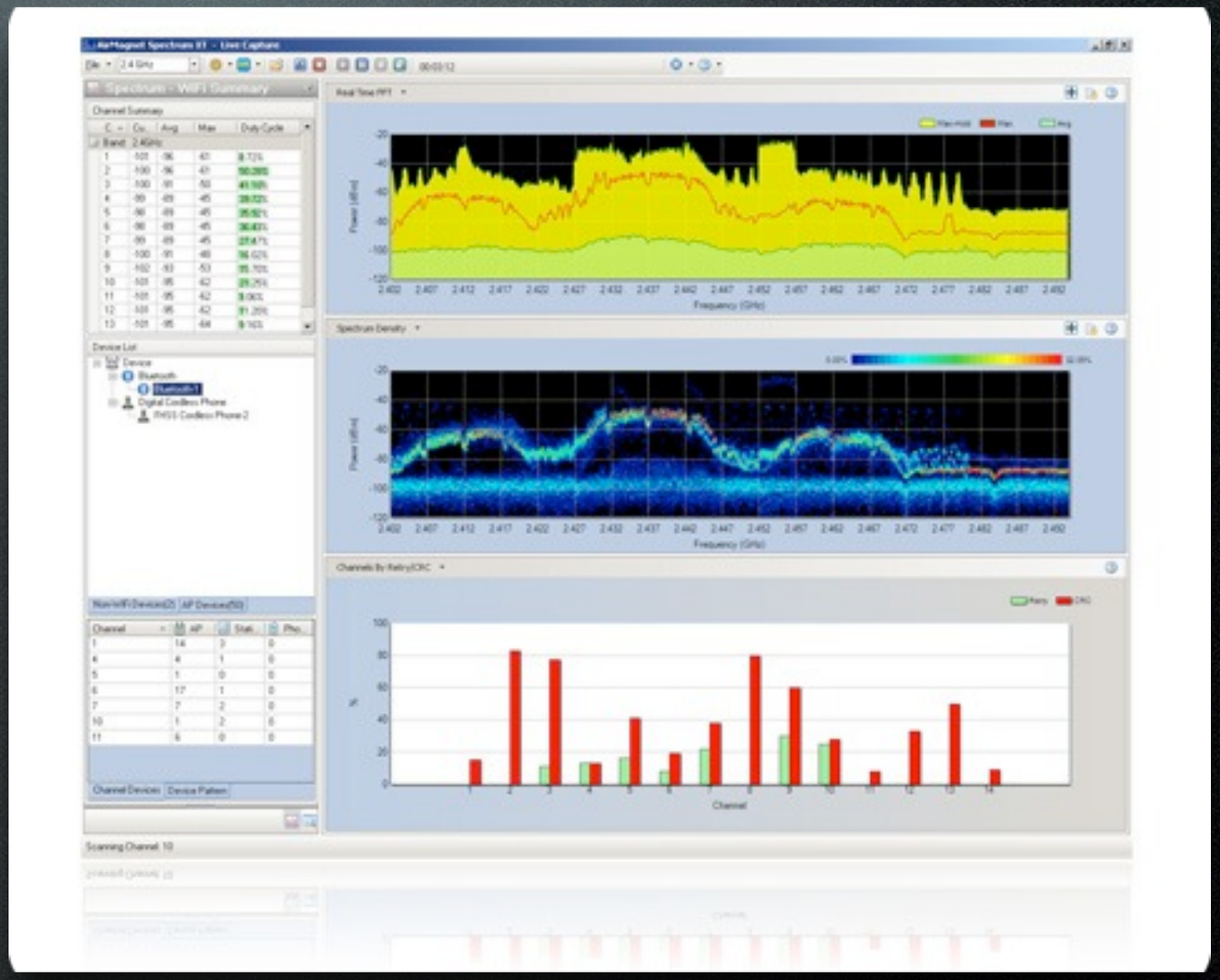
  (sn.im/photon13)

- Mac Implementation of Kismet

Wireless Testing Software

- Fluke AirMagnet

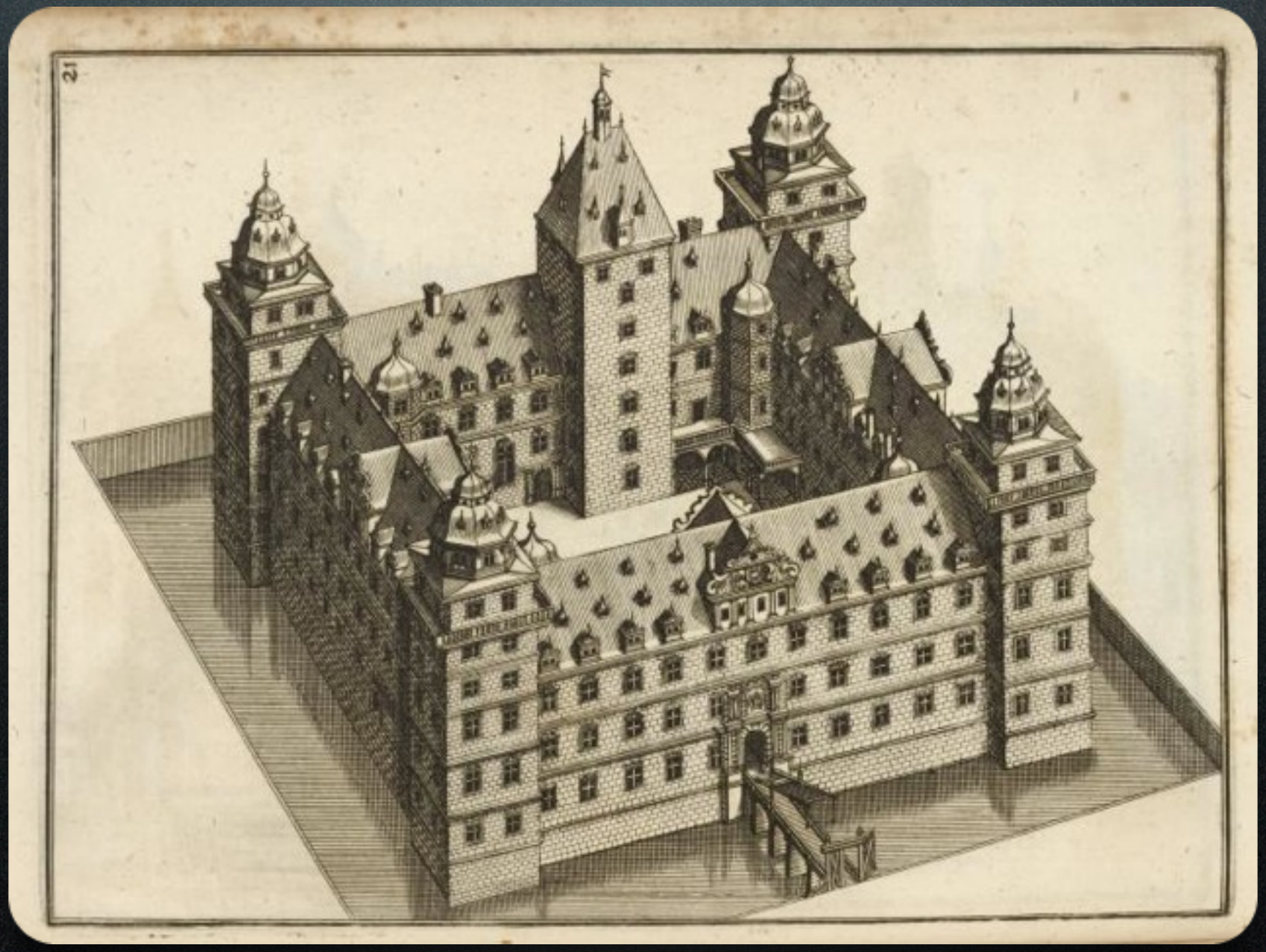
(sn.im/photon7)



Security

It’s Radio

- The Laws of Physics - again
- It Radiates and You Can’t Stop It



Build a Moat

Hide the Network

- Don't Do It
- Hidden SSID
- Isn't Hidden
- Another thing that you need to load into every client

Transmitter Power Control

- Make Interception Difficult
- Reduce the size of your cells to match coverage requirements

MAC Address Access Control

- Don’t Do It
- Spoofing
- Another thing that you need to load into every client

WEP

- Broken
- Don't Use It
- Unless You Are Setting Up a Honeypot

WPA and WPA2

- Wi-Fi Protected Access
- TKIP - Temporal Key Integrity Protocol
- MIC - Message Integrity Check
- EAP - Extensible Authentication Protocol

EAP

- 40 Versions Available
- TLS - Transport Layer Security
- EAP-TLS-Transport Layer Security
- EAP-TTLS - EAP-Tunnel Transport Layer Security
- PEAP - Protected Extensible Authentication Protocol
- LEAP - Lightweight Extensible Authentication Protocol

Physical Security

If They Can Touch It, They Can Hack It

Security

What You Don't Know Can Hurt You

References

- Information From Your Vendors
- Reference Materials
- Training
- Operating Manuals

References

- Apple AirPort Networks 2009

  http://manuals.info.apple.com/en_US/Apple_AirPort_Networks_Early2009.pdf

  sn.im/photon5

- Introduction to Wireless for Artists

References

- Cisco
- Internetworking Technology Handbook
  http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook
  sn.im/photon6
- Enterprise Mobility 4.1 Design Guide
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html
  sn.im/photon11
- Internetwork Design Guide
  http://docwiki.cisco.com/wiki/Internetwork_Design_Guide
  sn.im/photon4

References

- Wikipedia
  - Good for IT
  - Sometimes Weak Engineering
- Wikipedia - Invention of Radio

  http://en.wikipedia.org/wiki/Invention_of_radio

  sn.im/photon12

Q & A

- Call or Write
- photoninc.com
- allred@photoninc.com
- sn.im/photon4 through photon12